

SCHEDULE P – THAILAND LAW REQUIREMENTS

(Version 9 – 2 February 2026)

1. Right to audit and access

With reasonable prior written notice to the Supplier, the Supplier shall allow Citi, its regulators (including but not limited to the Bank of Thailand, the Anti-Money Laundering Office of Thailand) or any person appointed by them and/or its internal and external auditors to (i) access any report and finding made on the Supplier in connection with the Services performed for Citi; (ii) access to the business premises of the Supplier in the exercise of its right herein; (iii) inspect, examine and audit the Supplier's operations and records in relation to the Services provided by the Supplier under the Agreement including but not limited to the internal controls and the confidentiality and security system; and (iv) obtain and make copies of reports, documents of transactions and information stored or processed by the Supplier in connection with the Services pursuant to the Agreement. If the inspection, audit, and access require any consent from any regulatory body, the Supplier shall ensure that all consent is obtained, and necessary actions have been conducted, in order that the inspection process is able to be carried out properly.

2. Information Security

The Supplier agrees and undertakes, and shall procure all its personnel, to segregate Citi's data from its own data and data of any other entity and to stipulate a data access right of the Supplier's personnel strictly to protect confidentiality of Citi and its clients' information. The Supplier undertakes that it has sufficient technical and organizational safety measures to protect security, confidentiality, and privacy of Citi and its clients' information and has notified the data security measures to its personnel and related persons.

3. Transition Services

Upon termination of any Service, the Supplier shall return, destroy or delete all confidential information and personal information of Citi or its clients previously given (including without limitation, information incorporated in computer software or held in electronic storage media, together with any analyses, compilations, studies, reports or other documents or materials containing any such confidential information or personal information, as are in the possession or control of the Supplier) subject to the legal requirements for retention of records. The Supplier shall certify in writing to Citi within 30 days of the termination of the Services that it has not retained any such confidential information or personal information in any form whatsoever.

4. Thailand Personal Data Protection Act B.E. 2562

To the extent the Personal Data Protection Act B.E. 2562 ("PDPA"), and other applicable Thai laws and regulations relating to personal data protection including any notifications, sub-regulations, any guidelines or specific order issued by the Office of Personal Data Protection Committee of Thailand ("OPDPC") under the PDPA (collectively called "**Personal Data Protection Laws**") applies to both parties in its

provision of services, the Supplier shall comply or use its best effort to comply with the requirements of the Personal Data Protection Laws when collecting, holding, processing, using, or transferring personal data which is collected and disclosed by Citi from Thailand under this Agreement (“**Thai Personal Data**”) including but not limited to the following:

- a. The Supplier shall use appropriate technology and organizational measures, reasonably required by Citi or as required under the Personal Data Protection Laws, to protect the personal data collected, sent, transferred, stored and/or otherwise processed by the Supplier under this Agreement with it. In the case of a Personal Data breach incident that causes, or which may cause, damage to Thai Personal Data (“**Data Breach**”), the Supplier must immediately, and within 72 (seventy-two) hours, notify such Data Breach to Citi, in writing, with at least the following information about the Data Breach:

- Brief information relating to the nature and the category of Data Breach (including the nature and the number of Thai Data Subjects, the nature and the number of relevant personal data, and detail of Data Breach;
- Impacts that may arise as a result of Data Breach; and
- Measures used to prevent, stop or rectify Data Breach or to provide remedy for damages.

A Data Breach means a breach of security measures which causes loss, accessibility, usage, alteration, modification, or disclosure of Thai Personal Data without authorization or unlawfully, whether or not by intention, deliberation, negligence, unauthorized or unlawful acts, commission of computer offences, cyber treats, error or accidents, or any other causes. The Data Breach includes confidentiality breach, integrity breach and availability breach.

- b. The Supplier agrees to promptly cooperate with Citi to ensure its compliance with the legal obligations as required under the PDPA, including the Thailand entity’s obligation to notify the Data Breach to the Thai supervisory authorities.
- c. Where the Supplier is a data processor, under PDPA, the Data Processing Agreement is required to be entered into between the data controller and the data processor in which both parties agree to the terms as set forth below.
 - i. Where the Supplier is designated as a processor in the Agreement, Customer and Customer Affiliates, as relevant, will be the controller(s), and the Supplier will be the processor, when processing Thai Personal Data in the course of the Supplier providing Services to Customer or Customer Affiliates under the Agreement. The Parties acknowledge and agree that references to 'Customer' in this document shall mean the Customer Affiliate(s) that are controllers of the Thai Personal Data being processed by Supplier (or its Sub-processors) as processors. The Parties acknowledge and agree that a description of the Thai Personal Data processed by Supplier as a processor under this Agreement is set out in **Annex 1 (Data Processing Description)** hereof, and contains at least

the following information: (i) the subject-matter of the processing; (ii) the duration of the processing; (iii) the nature and purpose of the processing; (iv) the types of personal data processed; and (v) the categories of data subjects in relation to the personal data processed.

ii. **Data Processor Terms.** In this context, the Supplier shall procure that its Personnel (including its Sub-processors) processing Thai Personal Data shall, at no additional cost to:

- (1) process the Thai Personal Data solely for the Permitted Purposes in accordance with Customer's instructions and otherwise in accordance with the provisions hereof;
- (2) without prejudice to the Agreement, promptly advise Customer of any notices, requests or queries from data subjects, any data protection supervisory authority or any law enforcement authority, for Customer to resolve;
- (3) promptly provide such information and assistance to Customer as Customer may require to allow it to comply with: (a) the rights of data subjects under Data Protection Laws (including, taking into account the nature of the processing, appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to data subject requests to exercise such rights); (b) notices, requests or queries served or raised by any data protection supervisory authority or any law enforcement authority; (c) (taking into account the nature of the processing and the information available to Supplier) requirements to conduct data protection impact assessments and to consult with data protection supervisory authorities in relation to data processing; and (d) to facilitate timely resolution of any matter arising hereunder or any investigation;
- (4) without prejudice to the duty of care and use restrictions of the Agreement and any protective measures herein, implement (and update from time-to-time as needed) appropriate technical, organisational and security measures (including any specific security measures notified by Customer) to protect Personal Data from and against unauthorised or unlawful processing and against accidental loss, destruction, damage, disclosure or alteration, and provide Customer with a written detailed description of such measures promptly upon request from time-to-time;
- (5) without limiting the foregoing, follow best industry practice (including background checks and ongoing training) to ensure: (a) the reliability of the Supplier's Personnel (including its Sub-processors) who may have access to Customer Personal Data; and (b) that such measures include the ability to retrieve promptly any Customer Personal Data in such format and on such media as Customer reasonably requests;
- (6) put in place a contract with any Sub-processor who has been approved pursuant to use of sub-processors containing provisions

in favour of Customer which are equivalent to those in this Appendix, including sufficient guarantees in respect of the appropriate technical and organisational measures governing the processing to be carried out, and procure the right for Customer to perform an ISA on such Sub-processors;

- (7) provide any information requested by Customer to demonstrate Supplier's compliance with the obligations set out herein;
 - (8) maintain written records of all categories of Thai Personal Data processing activities carried out on behalf of Customer containing the information prescribed in applicable Data Protection Laws including PDPA;
 - (9) upon the expiry or termination of this Agreement and/or any Work Order under which Thai Personal Data will be processed, promptly arrange for the secure return or destruction of Thai Personal Data as notified by Customer in writing at the relevant time and delete existing copies of the Thai Personal Data, unless Thai law and all any applicable Data Protection Laws require storage of the Thai Personal Data, in which case the Parties will work together to ensure that this requirement is met;
 - (10) notify Customer immediately if, in the Supplier's opinion, an instruction for the processing of Customer Personal Data infringes Applicable Law; and
 - (11) not process, disclose or allow access to Thai Personal Data except on Customer's express instructions or where processing is required by applicable Data Protection Laws including PDPA to which the Supplier is subject, provided that the Supplier notifies Customer of that legal requirement before processing (which, for the avoidance of doubt, includes disclosure) the Thai Personal Data (unless that law prohibits the Supplier from doing so on important grounds of public interest). The Supplier shall provide Customer with reasonable cooperation in Customer's efforts to resist the processing or obtain a protective order (at Customer's request and expense), and shall process only the portion of Thai Personal Data that is required to be processed under the relevant applicable Data Protection Laws including PDPA.
- d. Where the Thai Personal Data is disclosed or transferred internationally to, by, or on behalf of the Supplier, the Supplier including its affiliates and its subcontractors, shall comply with the PDPA's requirements regarding cross-border transfer with respect to Thai Personal Data. The Supplier agrees to enter into an agreement, an undertaking, or relevant standard contractual clauses that are required or will be required for the purpose of Citi's compliance with the PDPA's requirements regarding cross-border transfer, such as third-party beneficiary conditions and security measures requirements, including but not limited to the below sections.

Where the Supplier and/or Citi transfer Thai Personal Data of Thai Data Subjects Cross-border, under the terms and requirement of, the Notification of the Personal Data Protection Committee (PDPC) issued under PDPA dated 12 December 2023 published in the Government Gazette on 25 December 2023, the parties mutually agree to establish appropriate safeguards for the transfer and Thai Personal Data under the terms hereof:

The “**Transferor**” shall mean either the data controller or the data processor who transfer the Thai Personal Data to the transferee who reside at overseas countries; and

The “**Transferee**” shall mean either the data controller or the data processor who resides at overseas countries, and receive the Thai Personal Data from the Transferor, for the purpose of collection, use or disclose of that Thai Personal Data.

- (a) In case that the Transferee is the data processor:
 - (i) The Transferee shall collect, use or disclose of the Personal Data under the demand or on behalf of the Transferor, and under the purpose as described by the Transferor (as the controller) only;
 - (ii) The Transferee shall notify the Transferor as soon as possible in case that the Thai Data Subjects request to exercise the rights under PDPA in relation to the Thai Personal Data processed under the Agreement (if any), other than in accordance with the instruction given by the Transferor to the Transferee; and
 - (iii) The Transferee of Thai Personal Data shall return the Thai Personal Data under the contract terms to the Transferor and/or erase or dispose of the Thai Personal Data or anonymize the Thai Personal Data to make it unidentifiable, in order to remove identifying particulars of the Thai Data Subjects, in accordance with the appropriate measure as it deemed fit, and under any condition that the Transferor may describe. Once completed, the Transferee shall confirm to the Transferor in writing, the completion of deletion of the Thai Personal Data.
 - (b) In case that the Transferee of the Thai Personal Data is the Data Controller, the parties acknowledge and agree that:
 - (i) each act as separate and independent controllers for the purposes of that work and shall be responsible for it’s own compliance with its obligations as a controller under Data Protection Laws; and
 - (ii) The Transferee shall notify the breach incident under the personal data protection laws to the Transferor of the Thai Personal Data as well (in case that the transferor is also the data controller) and in that case, no later than 72 (Seventy Two) hours from the date that it had become aware of the data breach incident, except that the breach has no risk to harm or effect rights and freedom of individuals.
 - (c) Both parties have arranged, and ensure that, each party has it’s efficient and effective legal remedies to the Thai Data Subjects.
- e. The Supplier shall prepare the record of processing activities relating to Thai Personal Data, which contains at least following information as required under the Personal Data Protection Laws:

- Name and details of the Supplier and the Supplier's representative if one is appointed in Thailand.
- Name and details of the Citi affiliates whose work has been assigned to the Supplier.
- Name and details of the data protection officer of the Supplier, including address and contact information.
- Categories and manners of data processing, including Thai Personal Data being processed and purposes being served.
- Categories of business units that receive Thai Personal Data (only if the data is sent offshore from Thailand.)
- Details of security standards and measures in place.

ANNEX 1

Data Processing Description

A. LIST OF PARTIES

Customer (the data exporter):

Name:	
Address:	
Contact person's name, position and contact details:	
Data Protection Officer contact information:	
Activities relevant to the data transferred under these Clauses:	
Signature and date:	
Role of Customer (controller/processor):	

[Add more tables as needed.]

Supplier (the data importer):

Name:	
Address:	
Contact person's name, position and contact details:	
Data Protection Officer (or if none, the nearest equivalent role):	
Activities relevant to the data transferred under these Clauses:	
Signature and date:	
Role of Supplier (controller/processor):	

[Add more tables as needed.]

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	
Categories of personal data transferred:	
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	
Nature of the processing:	
Purpose(s) of the data transfer and further processing:	
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	
For transfers by Supplier to (sub-) processors, also specify subject matter, nature and duration of the processing:	

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 (Supervision) SCCs)	
---	--

