DATA PROCESSING AGREEMENT

(APPLICABLE TO SELLERS, GOODS AND/OR SERVICE PROVIDERS ("COUNTERPART") WHO CARRY OUT PERSONAL DATA PROCESSING ACTIVITIES ON BEHALF OF COLUMBIA ASIA SDN BHD AND/OR ITS SUBSIDIARY(S))

This Data Processing Agreement ("**DPA**") forms an integral part of the service and/or goods and/or business agreement ("**Agreement**") between the Counterpart and Columbia Asia Sdn Bhd and/or its subsidiary(s) ("**Company**") (each, a "**Party**", and together, "**Parties**"). The DPA supplements and specifies the data protection obligations of the Agreement and any related supplemental agreement (which the Parties may have already entered into or may enter into in the future).

Definitions

Unless the context otherwise requires, for the purposes of this DPA, the following terms and expressions shall have the meanings set forth below:

"**Applicable Data Protection Laws**" means all applicable data protection laws to the Processing of the Personal Data, including but not limited to the PDPA;

"**Data Controller** " shall have the meaning given to it in the PDPA;

"**Data Processor**" shall have the meaning given to it in the PDPA;

"**Data Subject**" shall have the meaning given to it in the PDPA;

"**Personal Data**" shall have the meaning given to it in the PDPA;

"**PDPA**" means the Personal Data Protection Act 2010, Personal Data Protection (Amendment) Act 2024 and its implementing regulations and any other legislation, regulations, guidelines and code of practice applicable to the Data Controller which are in force from time to time in Malaysia relating to privacy and/or the processing of Personal Data; and

"**Process**", "**Processed**" or "**Processing**" shall have the meaning given to "processing" in the PDPA.

"**Representative**" means any directors, officers, employees, consultants, contractors, subcontractors, advisors and/or agents of a Party.

1. Application of DPA

1.1 This DPA applies if the Counterpart and/or its Representative is required to Process any Personal Data on behalf of the Company and/or if any Personal Data is provided by the Company and/or its Representative to the Counterpart and/or its Representative pursuant to the Agreement. For purposes of this DPA, the Company is the Data Controller and the Counterpart is the Data Processor.

1.2 This DPA shall apply throughout the term of the Agreement (and any extension thereof).

1.3 Data Controller may terminate this DPA by giving 30 days' prior written notice to the Data Processor.

2. Data Processor's Obligations

2.1 The Data Processor shall, in relation to any Personal Data Processed in connection with the performance of its obligations under the Agreement:

2.1.1 Process the Personal Data only based on the Data Controller's documented instructions or otherwise fulfilling its obligations under the Agreement and/or this DPA;

2.1.2 ensure that any of its Representative authorised to Process the Personal Data have committed to binding contractual obligations of confidentiality with the Data Processor or are under an appropriate statutory obligation of confidentiality;

2.1.3 implement appropriate technical and organisational security measures, including, as appropriate, (i) the pseudonymisation of Personal Data, (ii) ensuring the ongoing confidentiality, integrity, availability and resilience of Processing systems and services, (iii) restoring the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, (iv) adopting current anti-virus, firewall and up to date anti-intrusion software, (v) incorporating encryption in all transmission and reception of Personal Data, and (vi) regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing. In assessing the appropriate level of security, the Data Processor shall take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed;

2.1.4 not engage any third party, including but not limited to, consultant, sub-contractor, agent or professional adviser which may receive and/or have access to Personal Data ("**Sub-Processor**"), without prior written authorisation of the Data Controller. If authorised by the Data Controller, the Data Processor shall:

(a) ensure the Data Controller is informed of any intended changes concerning the addition or replacement of a Sub-Processor, and the Data Controller shall have the right to object to such appointment and replacement;

(b) cause each Sub-Processor to execute an agreement with contractual obligations substantially similar to the obligations imposed on the Data Processor in this DPA;

(c) remain fully liable to the Data Controller for any failure of any such Sub-Processor to comply with such substantially similar data protection obligations;

2.1.5 take into account the nature of the Processing, assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to any request from the Data Subject to exercise any of his or her rights under the Applicable Data Protection Laws (including right of access, rights to correct, and withdraw consent) or any other request or query from the Data Subject, authority or third party in relation to the Processing of the Personal Data ("**Data Subject Request**"). If the Data Processor receives such Data Subject Request, it shall:

(a) notify the Data Controller immediately of the Data Subject Request (in any event not later than 24 hours) without responding to that Data Subject Request, unless it has been otherwise authorised by the Data Controller in writing to do so;

(b) provide details of the Data Subject Request and any other information the Data Controller may reasonably request, to the Data Controller within 48 hours from receipt of Data Subject Request; and

(c) provide such assistance to the Data Controller for the purposes of responding to the Data Subject Request;

2.1.6 notify the Data Controller in writing immediately (in any event within 24 hours) in the event of any actual or potential breach of the Personal Data, and shall provide

information as may be requested by the Data Controller and render full cooperation in relation to such occurrence of actual or potential breach;

2.1.7 upon the termination or expiry of the Agreement or the DPA,

(a) securely delete or destroy all the Personal Data (including all copies thereof); and/or
(b) upon written request from the Data Controller, return all the Personal Data (including all copies thereof) to the Data Controller;

provided that the Data Processor may retain a copy of the Personal Data to the extent where required by the applicable laws;

2.1.8 make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and the Applicable Data Protection Laws, and allow the Data Controller or its authorised representative at any time upon three (3) business days' notice, access to any relevant part of the Data Processor's premises, Personal Data Processing facilities, systems (including any of its security measures), equipment and documents to enable the Data Controller or its authorised representative to inspect or audit the same for the purposes of monitoring compliance with the Data Processor's obligations under the Agreement and this DPA;

2.1.9 maintain written records of all of the categories of Processing carried out by the Data Processor on behalf of the Data Controller, including the name and contact details of any Sub-Processor and the Processing activities carried out by each Sub-Processor. The Data Controller may inspect such written records at any time by providing written notice to the Data Processor. This obligation shall survive termination or expiry of this DPA;

2.1.10 immediately inform the Data Controller if, in its opinion, any instruction given by the Data Controller infringes the Applicable Data Protection Laws;

2.1.11 The Data Processor shall implement and maintain adequate backup and restore functions to safeguard the Personal Data. These functions must ensure that, in the event of a system failure, data corruption, or loss of personal data, a complete and accurate backup is readily available to restore the data to its original state without undue delay;

2.1.12 The Data Processor shall develop, document, and maintain a clear business continuity protocol that outlines the procedures to follow in the event of any disruption, including but not limited to technical failures, natural disasters, or cyber-attacks. This protocol must ensure that the availability, integrity, and confidentiality of Personal Data are preserved at all times and that normal business operations, particularly related to the Processing of Personal Data, can be restored promptly; and

2.1.13 comply with all its obligations under the Applicable Data Protection Laws at its own cost.

2.2 In the event the Data Processor collects the Personal Data on behalf of the Data Controller, the Data Processor shall:

2.2.1 ensure that appropriate consent has been obtained from the relevant Data Subjects in accordance with the PDPA prior to collecting such Personal Data; and

2.2.2 if such Personal Data is transferred to a country outside Malaysia with the Data Controller's written consent, ensure that the recipient of such Personal Data is under

contractual obligations to protect such Personal Data to the same or higher standards as those imposed under the PDPA.

3. Personal Data Breach

3.1 In the event there is, or the Data Processor reasonably believes that there is, any improper, unauthorised or unlawful access to, use of, or disclosure of any Personal Data Processed by the Data Processor under or in connection with the Agreement and/or this DPA ("**Personal Data Breach**"), the Data Processor shall:

3.1.1 within one (1) hour after becoming aware of it, notify the Data Controller in writing all known details of such Personal Data Breach including:

(a) a description of the nature of the Personal Data Breach including where possible, the categories and approximate number of the Data Subjects and the records concerned;

(b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) a description of the likely consequences of the Personal Data Breach; and

(d) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;

3.1.2 obtain prior written consent of the Data Controller before disclosing to any third parties including the governmental authorities any information pertaining to the Personal Data Breach ; and

3.1.3 give full assistance to the Data Controller in notifying about the Personal Data Breach to the relevant authority or the Data Subject if such notification is required by the Applicable Data Protection Laws.

4. International Personal Data Transfers

The Data Processor shall not Process Personal Data outside Malaysia without the prior written approval of the Data Controller. If such transfer is necessary and approved by the Data Controller, the Data Processor shall ensure that such Process shall only take place in accordance any Applicable Data Protection Laws and in accordance with clause 2.2.2 of this DPA.

5. Remedy

Without prejudice to any other rights or remedies that the Data Controller may have, the Data Processor acknowledges and agrees that a breach of this DPA may result in irreparable harm, and damages alone may not be an adequate remedy. The Data Controller shall be entitled to the remedies of injunction, specific performance or other equitable relief for any threatened or actual breach of the terms of this DPA.

6. Compensation and Indemnity

6.1 In addition to the indemnities in the Agreement, the Data Processor agrees to indemnify and keep the Data Controller indemnified against any and all claims, damages, losses, actions, proceedings, liabilities, costs (including legal fees on a solicitor-client basis), and/or expenses incurred by the Data Controller arising directly or indirectly from a

breach of this DPA by the Data Processor or the Sub-Processor, or enforcement of any rights under it. This obligation shall survive termination or expiry of this DPA.

6.2 The Data Controller shall have the right to claim compensation from the Data Processor for any loss, damage, costs, or expenses incurred as a direct result of the Data Processor's failure to safeguard Personal Data in its custody, or as a result of any unauthorized access, disclosure, alteration, or destruction of Personal Data caused by the Data Processor's negligence, breach of its obligations herein, or failure to comply with the Applicable Data Protection Laws.

7. Compliance Timelines

The Data Processor acknowledges that if the Data Controller expressly instructs a shorter time frame or if a time frame is mandated by law to ensure compliance with the Data Processor's obligations under this DPA, then that shorter time frame will apply.

*** *The rest of this page has been intentionally left blank* ***