Panasonic

DATA PROTECTION ADDENDUM

This Data Protection Addendum, including the Standard Contractual Clauses and the Schedules ("**DPA**") is incorporated by reference as part of the Trial Agreement (or other agreement for the purchase or provision of Panasonic's services on a trial and/or limited-term basis, hereinafter collectively the 'Agreement") entered into by and between Customer and Panasonic Avionics Corporation, a company incorporated under the laws of Delaware with offices at 3347 Michelson Drive, Suite 100, Irvine, California, 92612, United States ("**Panasonic**" or "**Processor**"). This DPA is effective as of the effective date of the Agreement, will replace any terms previously applicable to the processing and security of Customer Data, and will apply for the duration of the Agreement, unless otherwise agreed in writing. Notwithstanding the foregoing, Panasonic will continue to secure Personal Data in accordance with the terms of this DPA for so long as Panasonic has access to such Personal Data.

RECITALS

Under the Agreement Panasonic provides services to Customer (the "**Services**") that may entail the processing of Personal Data (as defined in this DPA).

The parties wish to ensure that adequate safeguards are in place for the processing of Personal Data in accordance with applicable laws, including Applicable Privacy and Data Protection Laws and Regulations.

The parties therefore agree as follows:

1. For the purposes of this DPA, the definitions are as follows:

   A. "**Processor**" or "**Service Provider**" means a person or organization that processes Personal Data on behalf of, and in accordance with, the instructions of a Controller, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose Personal Data on his or her behalf.

   B. "**Applicable Privacy and Data Protection Laws and Regulations**" means all laws and regulations, including but not limited to the laws and regulations of the European Union, the European Economic Area and its member states, Switzerland, the United Kingdom, and the United States, including federal as well as state laws in California and other states, applicable to the Processing of Personal Data under the Agreement.

   C. "**Controller**" or "**Business**" means the natural or legal person or organization who determines the purposes and means of the processing of Personal Data.

   D. "**Data Exporter**" means the entity who provides Personal Data and Processing instructions to the Processor, Subprocessor, or Sub-subprocessor for Processing on behalf of the Data Exporter;

E. "**Data Importer**" means the Processor, Subprocessor, or Sub-subprocessor who agrees to receive from the Data Exporter Personal Data intended for Processing on the Data Exporter's behalf after the transfer in accordance with the Data Exporter's instructions;

F. "**Data Subject**" or "**Consumer**" means the identified or identifiable person to whom Personal Data relates.

G. "**Personal Data**" means personal data, personal information, or equivalents as defined in Applicable Privacy and Data Protection Laws and Regulations. In the absence of Applicable Privacy and Data Protection Laws and Regulations, "Personal Data" shall mean any information in any form or format, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer.

H. "**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

I. "**Processing**" means any operation, or set of operations, which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

J. "**Subprocessor**" means the entity Processing Personal Data on behalf of the Processor.

K. "**Sub-subprocessor**" means the entity Processing Personal Data on behalf of the Subprocessor.

L. "**Transfer**" means to disclose or otherwise make Personal Data available to a third party (including to any affiliate or Sub-subprocessor), either by physical movement of the Personal Data to a third party or by enabling access to the Personal Data by other means.

M. "**Transfer Clauses**" means Module 2 (controller to processor) of the Standard Contractual Clauses approved by European Union Commission Decision of 4 June 2021.

2. This DPA and the Agreement constitute Customer's initial written instructions regarding Panasonic's processing of Personal Data in relation to the Services. Customer may issue additional or alternative instructions provided that such instructions are agreed in writing between Customer and Panasonic.

3. Customer provides general written authorization for Panasonic's use of Sub-processors in provision of Services. Customer hereby consents to the sub-processing of Personal Data by Panasonic's Sub-processors listed at https://www.panasonic.aero/subprocessors/. In order to receive notice of Panasonic's appointment or replacement of a Sub-processor, Customer may

subscribe to notifications through the portal at https://www.panasonic.aero/subprocessors/ and Panasonic shall, to the extent required by applicable law, provide the subscriber with notification of a new Sub-processor(s) before authorizing such Sub-processor(s) to process Personal Data. Customer may object to Panasonic's use of a new Sub-processor by notifying Panasonic in writing within thirty (30) days after receipt, which notice shall include a detailed explanation of the objection and a reasonable period of time to respond to and address the same.

4. The following terms apply to Panasonic's processing of Personal Data for purposes of providing Services pursuant to the Agreement:

   a. Panasonic shall process the Personal Data as a Processor/Service Provider only (i) as needed to provide the Services as set forth in the Agreement or Schedule A of this DPA, (ii) in accordance with the instructions that it has received from Customer, including with regards to any Transfers, and (iii) as needed to comply with law (in which case, Panasonic shall provide prior notice to Customer of this legal requirement, unless that law prohibits this disclosure); Panasonic shall not sell Personal Data, nor retain, use or disclose Personal Data for any other purpose other than the specific purpose of performing the Services, including any purpose outside of the direct business relationship between the parties.

   b. Notwithstanding the limitations in clause 3(a), Panasonic may, to the extent consistent with Panasonic's role as a Processor/Service Provider, process the Personal Data as necessary to (i) retain and employ sub-processors, subject to the requirements in Section 2, (ii) build or improve the quality of Panasonic's services, provided such use does not include building or modifying data subject profiles that will be used to provide services to another business or to correct or augment data acquired from another source, (iii) detect, prevent, and investigate data security incidents that may impact Personal Data or systems processing Personal Data, (iv) detect, prevent, and investigate fraudulent or illegal activity, or (v) comply with Panasonic's legal obligations.

   c. Customer instructs Panasonic to anonymize or aggregate Personal Data so that it no longer constitutes personal data (or comparable data type under applicable privacy and data protection laws and regulations governing the processing of Personal Data) so that Panasonic may use such data to provide the Services. Panasonic shall take reasonable steps to confirm that such anonymized or aggregated Personal Data cannot be associated with a particular individual or household. Panasonic shall not attempt to, and shall prohibit all subcontractors processing such anonymized or aggregated data from attempting to, reidentify anonymized or aggregated data. Panasonic may use such anonymized or aggregate Personal Data for any purpose, including but not limited to producing aggregated statistics, aggregated user data, and de-identified data. Panasonic shall not disclose such data in a manner that may reasonably identify Customer absent consent from Customer.

   d. The parties agree that the Services are provided by Panasonic to effectuate the business purposes of Customer. Panasonic is prohibited from using or disclosing the information for any purpose other than for the purposes of providing the Services and as permitted under the Agreement;

e. Panasonic shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

f. Panasonic shall safeguard Personal Data processed for the Services by implementing the technical and organizational measures set forth in Schedule B;

g. Taking into account the nature of the Processing performed under the Agreement, Panasonic shall reasonably assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising the data subject's rights;

h. Where Customer requests that Panasonic assist with the fulfilment of Customer's obligations to respond to requests from data subjects to exercise their rights, Customer agrees to issue such request to Panasonic in writing and at least ten (10) business days prior to the deadline for responding to such requests under Applicable Privacy and Data Protection Laws and Regulations, unless a shorter time frame is required under Applicable Privacy and Data Protection Laws and Regulations, in which case Customer will notify Panasonic as soon as reasonably possible of such request;

i. Taking into account the nature of Processing performed under the Agreement and the information available to Panasonic, will assist Customer for the fulfillment of Customer's obligations to comply with the rights of Data Subjects, data protection impact assessments, and prior consultation with the competent Supervisory Authorities. Customer shall make a written request for any assistance referred to in this DPA. Panasonic may charge Customer no more than a reasonable fee to perform such assistance, as set forth in a quote to be mutually accepted by the parties. If Customer does not agree with the quote, the parties shall reasonably cooperate to find a feasible solution.

j. Panasonic shall comply with (and shall reasonably assist Customer to comply with) the obligations under Applicable Privacy and Data Protection Laws and Regulations regarding Personal Data Breaches;

k. At the Customer's discretion, Panasonic shall delete or return all the Personal Data Processed for the provision of Services under the Agreement to Customer after the end of the provision of Services relating to Processing, and delete existing copies unless applicable laws require retention of the Personal Data;

l. Panasonic shall provide Customer with all information reasonably necessary to demonstrate Panasonic's compliance with the obligations under this DPA and Applicable Privacy and Data Protection Laws and Regulations, including inspections, conducted by Customer or another auditor Customer selects, provided that:

    i. Customer or person undertaking the audit on behalf of Customer shall give reasonable notice to Panasonic and shall use all reasonable efforts to avoid and minimise any damage, injury or disruption to Panasonic's premises, equipment, personnel and business;

    ii. Panasonic shall not, unless required by law, be required to provide:

        1. access to its premises;

2. any information to any individual without reasonable evidence of that individual's identity and authority;

3. access or information outside normal business hours; or

4. assistance in relation to more than one audit in any calendar year, unless an additional audit is required by applicable law or is reasonably in light of material and genuine concerns as to Panasonic's compliance with the DPA; and

m. Panasonic shall promptly inform Customer if, in Panasonic's opinion, Customer's instruction violates Applicable Privacy and Data Protection Laws and Regulations.

n. Other than to the United States, Panasonic shall not Transfer any Personal Data internationally where such Transfer would be considered a Restricted Transfer or similar concept under Applicable Privacy and Data Protection Laws and Regulations without Customer's prior written consent.

o. Panasonic shall promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. Panasonic shall notify Customer without undue delay in the event of any Personal Data Breach. Customer must notify Panasonic without undue delay after becoming aware of a Personal Data Breach involving Personal Data Processed in association with Panasonic's provision of services under the Agreement.

5. The Parties agree to comply with Applicable Privacy and Data Protection Laws and Regulations with respect to the Processing of Personal Data in association with the Agreement. To the extent applicable, the Parties agree to comply with the jurisdiction specific provisions set forth in Schedule C.

6. This DPA is hereby incorporated by reference into the Agreement. The parties do not intend that anything in this DPA will be construed to cancel or negate any obligation in the Agreement, but supplements the Agreement for the purposes of personal data processing. To the extent any Agreement conflicts with this DPA, this DPA will control.

Panasonic

SCHEDULE A: Description of Processing

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the Customer*]

1. Name: Customer

   Address: The address for Customer stated in the Agreement.
   Contact person's name, position, and contact details: The contact details for Customer as stated in the Agreement or otherwise provided by the Customer.
   Activities relevant to the data transferred under these Clauses: Processing Personal Data for the purposes of providing, supporting, and improving the Services.
   Signature and date: The parties agree that execution of the Agreement constitutes execution of this Schedule by both parties.
   Role (controller/processor): Controller

Data importer(s):

1. Name: Panasonic Avionics Corporation

   Address: 3347 Michelson Drive, Suite 100, Irvine, California, 92612, United States
   Contact person's name, position, and contact details: The contact details for Panasonic as stated in the Agreement. Panasonic's privacy team can be contacted at privacy@panasonic.aero.
   Activities relevant to the data transferred under these Causes: Processing Personal Data for the purposes of providing, supporting, and improving the Services.
   Signature and date: The parties agree that execution of the Agreement constitutes execution of this Schedule by both parties.
   Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- The data subject may include Customer's employees, and Customer airline passengers.

Categories of personal data transferred

Any Personal Data that is provided to Panasonic by, on behalf of, or at the instruction of the Customer for the purposes of providing the Services, which may include:

- First and Last name
- Contact information (e.g. email address)
- IP Address
- Device and System Attributes
- Telemetry Data
- Airline and Aircraft Information
- Arrival and Departure Information
- Flight Information

- In-Flight Media Access Record

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.

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous

Nature of the processing

Analysis, storage, and other Services as described in the Agreement, DPA, or other documentation

Purpose(s) of the data transfer and further processing

Panasonic shall Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in this DPA, and as further instructed by Customer in its use of the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Panasonic shall Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter of Personal Data transferred to Sub-processors is Customer Personal Data, which is transferred to Sub-processors to provide, support, and improve the Services, as outlined in the agreements between Customer and Panasonic.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority shall be the supervisory authority which is competent to supervise the activities of the Data Exporter.

Panasonic

SCHEDULE B

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Panasonic has implemented the following technical and organizational measures as part of its Security Program:

1. Security Awareness and Training. A mandatory privacy and security awareness and training program for all members of Panasonic's workforce (including management).
2. Access Controls. Policies, procedures, and logical controls: (i) to limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons with a genuine need-to-know; (ii) to prevent those workforce members and others who should not have access from obtaining access; and (iii) to remove access in a timely basis in the event of a change in job responsibilities or job status.
3. Physical and Environmental Security. Controls that provide reasonable assurance that physical access to facilities where Personal Data is stored, including physical servers, is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes. These controls include: (i) logging and monitoring of unauthorized access attempts to Panasonic's facilities by security personnel; (ii) camera surveillance systems at critical internal and external entry points of Panasonic's facilities; (iii) systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and (d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.
4. Government Access to Personal Data. Policies and procedures to be followed regarding access requests to Personal Data issued by Government Agencies which should, as a matter of principle (i) be evaluated and reviewed on a case-by-case basis; and (ii) only allow for the disclosure of Personal Data to Government Agencies pursuant to a valid court order or with the data subject's consent, except in defined circumstances.

5. Data Incident Procedures. A data incident response plan that includes procedures to be followed in the event of any actual or reasonably suspected unauthorized use of, loss of, access to or disclosure of Personal Data.

6. Contingence Planning. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Personal Data or production systems that contain Personal Data.

7. Audit Controls. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information.

8. Data Integrity. Policies and procedures to ensure the confidentiality, integrity, and availability of Personal Data and protect it from disclosure, improper alteration, or destruction.

9. Storage and Transmission Security. Security measures to guard against unauthorized access to Personal Data that is being transmitted over a public electronic communications network or stored electronically. Such measures include requiring encryption of any Personal Data in transit as well as stored on desktops, laptops or other removable storage devices.

10. Segmentation. Measures ensuring the segmentation of Personal Data from data of others.

11. Assigned Security Responsibility. Assigning responsibility for the development, implementation, and maintenance of its Security Program, including: (i) designating a security official with overall responsibility; and (ii) defining security roles and responsibilities for individuals with security responsibilities.

12. Testing. Maintain compliance and regularly testing the key controls, systems and procedures of its Security Program to validate that they are properly implemented and effective in addressing the threats and risks identified. These requirements and testing include includes: (i) internal risk assessments; (ii) ISO 27001; (iii) Service Organization Control 1 (SOC1) and Service Organization Control 2 (SOC2) (or industry-standard successor reports); (iii) PCI-DSS; (iv) PA DSS; (v) MPAA/TPN – STAR.

13. Monitoring. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes: (i) reviewing changes affecting systems handling authentication, authorization, and auditing; (ii) reviewing privileged access to Panasonic's production systems; and (iii) engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

14. Change and Configuration Management. Maintaining policies and procedures for managing changes Panasonic makes to production systems, applications, and databases. Such policies and procedures shall include: (i) a process for documenting, testing and approving the patching and maintenance of the Service; (ii) a security

patching process that requires patching systems in a timely manner based on a risk analysis; and (iii) a process for Panasonic to utilize a third party to conduct web application level security assessments.

15. Program Adjustments. Panasonic shall monitor, evaluate, and adjust, as appropriate, its security measures in light of: (i) any relevant changes in technology and any internal or external threats to Panasonic or the Personal Data; (ii) security and data privacy regulations applicable to Customer and/or Panasonic; and (iii) Panasonic's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

16. Devices. All laptop and desktop computing devices utilized by Panasonic and any Sub-processors when accessing Personal Data shall: (i) be equipped with a minimum of AES256 bit full hard disk drive encryption; (ii) have virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and (iii) maintain virus and malware detection and prevention software so as to remain on a supported release.

Panasonic

SCHEDULE C

JURISDICTION-SPECIFIC CLAUSES

I. Argentina

A. The following provisions shall apply to all Transfers of Personal Data, directly or by onward Transfer, from a Data Exporter in Argentina.

B. For the avoidance of doubt, "Applicable Privacy and Data Protection Laws and Regulations" includes the Personal Data Protection Act, Argentinean Law 25,326 ("Act No. 25,326") and any complementary regulation.

C. Personal Data shall consist of the categories of information and only be processed, used and/or further communicated to third parties by Data Importer exclusively in accordance with the categories and purposes outlined in Schedule A, or as otherwise agreed by the Data Exporter and Data Importer.

D. Data Importer shall only Process Personal Data on instructions from Data Exporter and for the purposes specified in Schedule A or as otherwise agreed by the Data Exporter and Data Importer and will not communicate Personal Data to any third party, even for storage purposes, except: (i) where such disclosure, transfer or access is mandated by Applicable Privacy and Data Protection Laws and Regulations (subject to Data Importer providing Data Exporter with prompt written notice of such requirement to transfer or disclose, unless such notice is prohibited by Applicable Privacy and Data Protection Laws and Regulations); or (ii) where Data Exporter approves Data Importer's disclosure and/or transfer granting access of Personal Data to a third party; provided that such third party shall, prior to any such disclosure, have entered into terms at least as restrictive as this Agreement and such agreement shall be provided to Data Exporter promptly upon request.

E. Data Importer shall comply with any and all dispositions of the Argentine Data Protection Authority, the "Agency of Access to Public Information" ("AAPI").

F. Transfer of Personal Data to jurisdictions that provide an adequate level of data protection. The following provisions shall apply to all transfers of Personal Data where the Data Importer is located in a jurisdiction with legislation that provides an adequate level of data protection according to Disposition 60 E/2016 of the AAPI, as may be amended or supplemented from time to time.

(a) Data Importer must follow the recommendations of Disposition 47/2018, that detail the "Security Measures to be implemented for the processing and conservation of personal data" and its amendments.

(b) Data Importer acknowledges and accepts the rights of the Data Subjects (as defined by Act No. 25,326) of the transferred Personal Data under the Argentine Regulations on Personal Data Protection. The Data Subjects shall be able to

exercise those rights directly before Data Importer or Data Exporter at the choice of the Data Subjects.

(c) Data Importer shall furnish the AAPI with information regarding the Processing of the transferred Personal Data when required and allow it, as required under Applicable Privacy and Data Protection Laws and Regulations, to carry out audits or inspections with the same scope with which it would have been able to audit or inspect Data Exporter's premises; this includes the AAPI's right to carry out inspections of the Data Importer's premises. Data Importer shall promptly notify Data Exporter prior to any audit or inspection to be carried out by the AAPI.

(d) Data Exporter states that any international transfer of Personal Data to the Data Importer provided for in this Agreement shall be carried out in compliance with the Argentine Regulations on Personal Data Protection.

(e) Data Importer and Data Exporter agree that, in the case of a transfer of Personal Data controlled by Data Exporter in Argentina to Data Importer, this Agreement shall be governed by the laws of the Republic of Argentina. If required under Applicable Privacy and Data Protection Laws and Regulations, any conflict or controversy in relation thereto shall be settled by the Courts of the City of Buenos Aires. The Data Importer expressly accepts to be subject to the application of the Argentine laws and the exclusive jurisdiction of the Argentine courts where applicable as set forth in this Clause.

G. Upon termination or expiration of this Agreement, or if Data Importer fails to comply with the obligations under Act N° 25.326, Data Importer shall destroy the Personal Data in its possession, except where Data Exporter explicitly authorizes Data Importer to retain the Personal Data, in which case the Personal Data shall be stored with appropriate security measures for no more than two (2) years after this Agreement has terminated or expired.

II. Australia

A. The following provisions apply to all transfers of Personal Data controlled by Data Exporter in Australia.

B. For the avoidance of doubt, "Applicable Privacy and Data Protection Laws and Regulations" includes the Australian Privacy Act 1988 (Cth), as amended from time to time, including the Australian Privacy Principles or any equivalent privacy principles that take their place.

C. When collecting, using, disclosing and storing Personal Data provided by or on behalf of the Data Exporter, the Data Importer must comply with the Australian Privacy Principles.

D. To the extent Data Importer discloses Personal Data to a third party, Data Importer shall enter into an agreement with such third party that contains terms no less stringent than those described under this Agreement.

Data Importer shall only Process Personal Data for the purposes specified in Schedule A, or as otherwise agreed by the Data Exporter and Data Importer.

III. Brazil

A. The following provisions apply to all transfers of Personal Data controlled by Data Exporter in Brazil.

B. For the avoidance of doubt, "Applicable Privacy and Data Protection Laws and Regulations" includes the General Data Protection Law, Brazilian Law 13.709/2018, which came into effect August 2020 and may be amended from time to time ("LGPD"), and binding regulations issued by the Brazilian National Data Protection Agency.

C. Data Exporter shall process Personal Data in compliance with the Brazilian General Data Protection Law, and shall only issue instructions to Data Importer for processing such Personal Data that comply with the LGPD.

D. Data Importer shall carry out the processing of Personal Data according to the instructions provided by Data Exporter or as otherwise permitted by Applicable Privacy and Data Protection Laws and Regulations.

E. Data Exporter shall transfer Personal Data outside of Brazil in compliance with Chapter V of the LGPD. To the extent transfers of such data are reliant on a transfer mechanism approved by the Brazilian National Data Protection Agency, such as standard contractual clauses, the Parties agree to adopt an approved transfer mechanism to safeguard such transfers in compliance with the LGPD. In the absence of approved transfer mechanisms, Data Importer commits to provide a standard of protection to Personal Data that is comparable to that which is required of Data Exporter in compliance with the LGPD.

IV. China

A. The following provisions apply to all transfers of Personal Data controlled by Data Exporter in China. Personal Data shall mean data that is "personal data" or "important data" within the meaning of Applicable Privacy and Data Protection Laws and Regulations in China, including the China Cyber Security Law, China Personal Information Protection Law, China Data Security Law, and other applicable laws, regulations, and departmental rules in China, as each may be amended or superseded from time to time.

B. Data Exporter will not transfer Personal Data to a place outside of China to the extent that doing so is prohibited by Applicable Privacy and Data Protection Laws and Regulations. Data Exporter shall obtain any and all appropriate consents and make any and all notifications required under Applicable Privacy and Data Protection Laws and Regulations and meet any other requirements under Applicable Privacy and Data Protection Laws and Regulations for lawful transfers of Personal Data to a place outside of China.

C. Data Exporter warrants and undertakes that Personal Data have been collected, Processed and stored in accordance with the laws applicable to Data Exporter in China. In the case of a transfer of Personal Data from Data Exporter to a territory outside China, it is the responsibility of Data Exporter to obtain the governmental security assessment, standard contractual clauses record-filing, or certification required under Data Protection Laws in China for lawful transfers of Personal Data to a place outside of China. To the extent the transfer shall be subject to the standard contractual clauses issued by the Cyberspace Administration of China or other separate agreement requirements as applicable, the standard contractual clauses or separate agreement required will be incorporated into this Agreement. In the event of any conflict of terms with respect to processing of personal data, the standard contractual clauses or separate agreement required shall prevail with respect to the conflicting provisions.

D. Data Exporter warrants and undertakes that it has conducted a personal information security impact assessment on the intended cross-border transfer of the Personal Data to Data Importer in accordance with the Applicable Privacy and Data Protection Laws and Regulations in China.

E. Data Importer shall Process and use Personal Data received for purposes as consented to by data subjects or as otherwise permitted under Applicable Privacy and Data Protection Laws and Regulations.

F. Data Importer shall maintain the security and confidentiality of Personal Data and ensure that the level of protection of Personal Data is not lower than the Applicable Privacy and Data Protection Laws and Regulations in China.

G. Data Importer shall avoid providing or transferring the Personal Data to any third party, except when authorized by Data Exporter and consented to by data subjects (including to subcontractors subject to the same obligations as Data Importer) or when required by applicable law (e.g., when lawfully requested by competent authorities).

H. Data Importer shall update Personal Data according to any instructions from Data Exporter.

I. Data Importer shall make Personal Data accessible to Data Exporter upon reasonable request and provide Data Exporter with information concerning Data Importer's security controls from time to time upon request.

V. European Economic Area

A. The terms below shall have the following meanings ascribed to them for the purposes of this Section V:

(a) "**Europe**" means the European Economic Area;

(b) "**European Data Protection Laws**" means any applicable laws of Europe that relate to the Processing of Personal Data under this Agreement.

(c) "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016.

To the extent that any Data Exporter transfers Personal Data subject to European Data Protection Laws, either directly or via onward transfer, to a Data Importer located in a country that does not ensure an adequate level of protection within the meaning of European Data Protection Laws, the Parties agree to comply with the terms of the Transfer Clauses, which are hereby incorporated into this Agreement by reference.

B. For the purposes of the Transfer Clauses, the following additional provisions shall apply:

(a) the names and addresses of those Data Exporter(s) and Data Importer(s) shall be considered to be incorporated into the Transfer Clauses;

(b) The Parties' signature to this Agreement shall be considered as signature to the Transfer Clauses.

(c) Clause 7 (Docking Clause) shall apply.

(d) Option 2 under paragraph (a) of Clause 9 (Use of sub-processors) shall apply and "[Specify time period]" be replaced with "thirty (30) business days".

(e) The option under Clause 11 (Redress) shall not apply.

(f) For the purposes of paragraph (a) of Clause 13 (Supervision), the Data Exporter shall be considered as established in an EU Member State.

(g) The governing law for the purposes of Clause 17 (Governing law) shall be the law of the Republic of Ireland.

(h) The courts under Clause 18 (Choice of forum and jurisdiction) shall be the courts of Dublin, Republic of Ireland.

(i) The contents of Schedule A shall form Annex I to the Transfer Clauses

(j) The supervisory authority competent to supervise the activities of Data Exporter shall act as competent Supervisory Authority for the purposes of Annex I.C of the Transfer Clauses.

(k) The contents of Schedule B shall form Annex II of the Transfer Clauses (Technical and organisational measures including technical and organisational measures to ensure the security of the data).

VI. Hong Kong

A. For the avoidance of doubt, Applicable Privacy and Data Protection Laws and Regulations includes the Personal Data (Privacy) Ordinance (Cap. 486), including all regulations thereunder, as amended from time to time.

VII. Israel

A. The following provisions apply to all transfers of Personal Data controlled by Data Exporter in Israel.

B. For the avoidance of doubt, Applicable Privacy and Data Protection Laws and Regulations includes the Protection of Privacy Law 1981 including all regulations there under, including, but not limited to, Privacy Protection Regulations (Data Security), 2017, and the Privacy Protection Regulations (Conditions for Data Storage and Security and Public Sector Data Sharing), 1986, as amended from time to time.

The Data Importer shall: (i) meet all the conditions for Personal Data retention, storage and Processing, which apply to personal data in Israel; (ii) take sufficient steps to ensure the privacy of the Personal Data subjects; (iii) apply adequate data security requirements to applicable Personal Data; (iv) process the Personal Data in accordance with the safeguards outlined in Schedule B; (v) logically segregate the Personal Data from information obtained from unaffiliated third parties or information obtained for other purposes; (vi) appoint an officer responsible for data security; (vii) periodically audit and make reports to the Data Exporter with respect to Personal Data processing activities and compliance with this Agreement; (viii) coordinate and permit periodic audits by the Data Exporter (or a mutually agreed upon third party who will execute a confidentiality agreement), including on-site inspections and, to the extent possible, automated monitoring over the processing activities of the Data Importer; (ix) ensure that the Personal Data will not be transferred to a third party, whether in the Data Importer's jurisdiction, or elsewhere, other than to approved service providers that provide at least the same level of privacy protection as is required by this Agreement; (x) only Process Personal Data for the purposes specified in Schedule A and, or as otherwise agreed by the Data Exporter and Data Importer; (xi) refrain from illicit collection of Personal Data or from use of Personal Data in an illicit database; (xii) investigate and report to the Data Exporter any suspected breach of the integrity or security of the Personal Data and take any necessary remedial action; (xiii) conduct reasonable background checks for personnel with access to Personal Data; (xiv) upon termination of the Agreement or in accordance with Data Exporter's instructions, destroy or return Personal Data in its possession; and (xv) indemnify the Data Exporter for any cost, charge, damages, expenses or loss arising out of any third-party claim alleging damage as a result of any breach of Data Importer's obligations under this Agreement; provided, however, (a) the Data Exporter promptly notifies the Data Importer of such a claim and (b) the Data Importer is provided the possibility to cooperate with the Data Exporter in the defense and settlement of the claim.

VIII. Japan

A. The following provisions apply to all transfers of Personal Data controlled by Data Exporter in Japan.

B. For the avoidance of doubt, Applicable Privacy and Data Protection Laws and Regulations includes the Act on the Protection of Personal Information (Act No. 57 of 2003, as amended).

C. Data Importer shall not Process Personal Data for purposes other than those specified in Schedule A, or as otherwise agreed by the Data Exporter and Data Importer (for the purpose of this section, the "**Utilization Purposes**") without the prior written consent of the Data Exporter. Data Exporter represents that it has notified all applicable Data Subjects of the Utilization Purposes to the extent required by Data Protection Laws.

D. Data Importer and Data Exporter agree that Data Exporter shall collect all consents from Data Subjects required by Data Protection Laws, including without limitation for (1) the collection of any "**Special Care-Required Personal Information**" (as defined by Applicable Privacy and Data Protection Laws and Regulations) and (2) any disclosures of Personal Data made by Data Exporter to third parties, subject to Clause G below.

E. The Data Importer shall keep the Personal Data accurate and up-to-date within the scope necessary to achieve the Utilization Purposes, and shall delete any Personal Data that becomes unnecessary to achieve a Utilization Purpose or other legitimate business purpose. For the avoidance of doubt, it is not necessary to delete Personal Data where applicable laws require the Data Importer to retain it.

F. The Data Importer shall have in place appropriate technical and organizational measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, leakage, alteration, and unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

G. The Data Importer shall exercise the necessary and appropriate control and supervision over its officers, employees, and vendors to securely manage the Personal Data received.

H. The Data Importer shall not disclose Personal Data to any third party except: (i) where such disclosure, transfer or access is mandated by Applicable Law; or (ii) where Data Exporter consents to the disclosure of Personal Data to the third party; or (iii) as permitted in Clause I, below. In the event that Data Importer discloses Personal Data to a third party, Data Importer shall impose contractual obligations upon the third party that are no less restrictive than the terms set forth in this Agreement.

I. In the case where Data Importers entrust the handling of the Personal Data to a third party pursuant to Clause H above, they shall exercise necessary and appropriate control and supervision over the entrustees to ensure the safety of such Personal Data, as stated in Clause F above, and they shall require the entrustees comply with obligations equivalent to the obligations of the Data Importers under this Agreement, including the

obligations in this section. The Data Importers shall be responsible for any breach by the entrustees (and any subsequent entrustee) of the obligations above. For clarity, Clause I shall apply to all third party entrustees and subsequent third party entrustees.

J. To the extent required by the APPI, upon request of the Data Subject, each Data Importer shall correct, add, or delete certain Personal Data if the Data Subject can show the contents of the Personal Data are incorrect. Each Data Importer shall promptly inform the Data Subject if it has corrected, added, or deleted Personal Data, or if it has determined it does not have to do so.

K. To the extent required by the APPI, upon request of the Data Subject, each Data Importer shall disclose the information on the Personal Data stipulated under the APPI, including (i) the contents of the retained Personal Data; (ii) the name of the Data Importer; (iii) the Utilization Purposes; (iv) the procedures for responding to a request for the Personal Data; and (v) the contact information Data Subjects should use to make claims regarding the handling of the Personal Data. Each Data Importer shall promptly inform the Data Subject if it has determined it does not have to provide requested information on the contents and/or the Utilization Purposes of the Personal Data.

L. To the extent required by the APPI, each Data Importer shall delete or stop utilizing the Personal Data if the Data Subject can show that the Data Importer is using or has used such Personal Data outside of the designated Utilization Purposes or if was acquired by improper means; provided, however, that it is not required where it would be unreasonably expensive or unreasonably difficult to do so and where alternative action which would protect the Data Subject's interests can be taken. Each Data Importer shall promptly inform the Data Subject if it has deleted or stopped utilizing the Personal Data, or if it has determined it does not have to do so.

M. To the extent required by the APPI, each Data Importer shall stop providing Personal Data to a third party, if the Data Importer has provided it to a third party in violation of the restrictions related to the provisions of the Personal Data to a third party under the APPI; provided, however, that it is not required where would be unreasonably expensive or unreasonably difficult to do so and where alternative action which would protect the Data Subject's interests can be taken. Each Data Importer shall promptly inform the Data Subject if it has stopped providing the Personal Data, or if it has determined it does not have to do so.

N. If a Data Importer knows or should know that any Personal Data has been or is likely to be leaked, disclosed, accessed, destroyed, altered, lost, used without authorization, or otherwise handled in any way not permitted under this Agreement, regardless of whether or not the Data Importer is liable for such incidents, the Data Importer shall promptly inform the Data Exporter of the same in writing, and shall take any appropriate measures to prevent such incident from occurring, expanding, and recurring.

O. Utilization Purposes under this agreement include the purposes listed in Schedule A.

IX. Malaysia

A. For the avoidance of doubt, Applicable Privacy and Data Protection Laws and Regulations includes the Malaysian Personal Data Protection Act 2010, which shall include implementing measures to comply with obligations prescribed by the Malaysian Personal Data Protection Commissioner from time to time, including the Personal Data Protection Standards 2015, as may be amended or supplemented from time to time.

X. Mexico

A. The following provisions apply to all transfer of Personal Data controlled by Data Exporter in Mexico.

B. Definitions. For the purposes of this section:

(a) "Privacy Notice" shall mean a document in physical, electronic or any other format, generated by the Controller, that is made available to the Data Subject prior to the processing of the Data Subject's Personal Data, which provides the Data Subject with information regarding what Personal Data is collected about them and for what purposes.

(b) "Mexican Personal Data" shall mean Personal Data collected within Mexico under this Agreement.

(c) "Mexican Privacy Laws and Regulations" shall mean the Federal Law on the Protection of Personal Data Held by Private Parties ("Ley Federal de Protección de Datos Personales en Posesión de los Particulares") and all of its implementing regulations, including the Regulations of the Federal Law on the Protection of Personal Data Held By Private Parties ("Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares") and the Privacy Notice Guidelines ("Lineamientos del Aviso de Privacidad").

(d) Data Importer shall Process the Mexican Personal Data on behalf of Data Exporter in accordance with this Agreement, Mexican Privacy Laws and Regulations, the Data Exporter's Privacy Notice and other documented instructions received from Data Exporter. Data Exporter shall provide to Data Importer a copy of its latest Privacy Notice so that Data Importer may identify the main purposes for which it may process the Mexican Personal Data. Data Exporter may provide Data Importer with general or specific instructions, which shall be in accordance with Data Exporter's Privacy Notice, and be issued in writing or via e-mail, unless urgency or other special circumstances necessitate a different form (e.g. verbally), in which case Data Exporter will confirm these instructions in writing or via e-mail promptly thereafter.

(e) Data Importer shall implement security measures to protect Mexican Personal Data consistent with Schedule B of this Agreement.

(f) Data Importer will take reasonable steps to verify that its personnel involved in the Processing of the Mexican Personal Data are able to maintain the confidentiality of the Mexican Personal Data and to Process the Mexican Personal Data in accordance with the Data Exporter's Privacy Notice and Mexican Privacy Laws and Regulations.

(g) Data Importer may only transfer Mexican Personal Data to third parties as necessary to comply with a valid request made by a competent legal authority, or after receiving the written authorization of the Data Exporter to do so.

(h) Data Importer may only transfer Mexican Personal Data to third parties who agree to limit their Processing to purposes listed in the Data Exporter's Privacy Notice and this Agreement.

(i) Upon termination or expiration of the Agreement for whatever reason, Data Importer shall at, Data Exporter's request, cease Processing the Mexican Personal Data and shall confirm that any other third parties to which Data Importer has transferred the Mexican Personal Data similarly cease Processing any such data.

(j) Upon termination or expiration of the Agreement for whatever reason, Data Importer shall:

(i) provide Data Exporter with the opportunity to retrieve the Mexican Personal Data; and

(ii) upon request, provide Data Exporter with the Mexican Personal Data including all copies and back-ups.

XI. Peru

A. For the avoidance of doubt, Applicable Privacy and Data Protection Laws and Regulations includes the Personal Data Protection Law, Law 29733, which shall include implementing measures to comply with that Law, as may be amended or supplemented from time to time.

XII. Philippines

A. The following provisions apply to all transfers of Personal Data controlled by Data Exporter in Philippines.

B. For the avoidance of doubt, Applicable Privacy and Data Protection Laws and Regulations includes the Data Privacy Act of 2012 (Republic Act No. 10173), which shall include implementing measures to comply with that Act, as may be amended or supplemented from time to time.

C. Data Importer shall not Process Personal Data for purposes other than those specified in Schedule A without the prior written consent of the Data Exporter.

D. Data Importer shall implement security measures to protect Personal Data consistent with Schedule B of this Agreement.

XIII. Singapore

A. The following provisions apply to all transfers of Personal Data controlled by Data Exporter in Singapore. For the avoidance of doubt, Applicable Privacy and Data Protection Laws and Regulations includes the Personal Data Protection Act 2012 (PDPA), which shall include implementing measures to comply with that Act, as may be amended or supplemented from time to time. Data Exporter shall ensure appropriate express consent from Data Subjects has been obtained for the transfer of Personal Data from Data Importer and/or its subcontractors, unless the purpose of such transfer falls within an exception to the PDPA's consent requirements (e.g., transfers that are reasonable for the purpose of managing or terminating an employment relationship).

XIV. South Korea

A. The following provisions apply to all transfers of Personal Data controlled by Data Exporter in South Korea.

B. When Processing Personal Data provided by or on behalf of Data Exporter:

(a) The scope, classification, purposes and details of the Processing of the Personal Data shall be as described in Schedule A, or as otherwise agreed by the Data Exporter and Data Importer.

(b) Data Importer shall limit access to Personal Data to those personnel who reasonably require such access for the purposes of the Processing, and Data Importer shall establish and maintain safeguards as per Schedule B of this Agreement, including: (i) internal procedures for secure handling of Personal Data; (ii) measures to prevent illegal access to Personal Data; (iii) measures to prevent falsification of alteration of access logs; (iv) measures to securely store and transmit Personal Data (including use of encryption technology and secure server); and (v) installation of intrusion detection software (vi) the installation and regular updating of antivirus software for monitoring for and responding to intrusions by computer viruses, spyware or other malicious programs; (vii) the establishment and operation of access control procedures with respect to physical storage locations; and (viii) other measures for the protection of Personal Data that may be required under relevant rules and regulations of Korean data

protection law from time to time (as applicable to an overseas transferee of Personal Data).

(c) Data Importer shall inform Data Exporter reasonably in advance of such disclosure or transfer of Personal Data to a third-party service provider. Upon Data Exporter's request, Data Importer shall provide the following information: (a) the Processing activities to be subcontracted; (b) the identity of the third-party service provider; and (c) any changes to (a) and (b).

(d) Notwithstanding Clause (c) of this Section XIIIV, Data Importer shall not disclose or transfer to any person or entity any Personal Data unless it obtains prior consent to transfer from relevant Data Subjects or otherwise does so in accordance with applicable provisions of Korean data protection law.

(e) Data Importer shall establish and implement appropriate procedures for (i) the handling of complaints regarding invasions of privacy and (ii) the resolution of any disputes with Data Subjects.

(f) Data Importer shall be subject to (i) training and supervision by the Data Exporter with respect to the Data Importer's handling of the Personal Data, and (ii) supervision and audit by relevant Supervisory Authorities.

(g) Indemnify the Data Exporter for any and all damages, liabilities, costs and expenses arising out of any breach of the Data Importer's obligations under this Agreement or under Applicable Law.

XV. Switzerland

A. To the extent that the processing or transfer of Personal Data under this Agreement is subject to Swiss Applicable Privacy and Data Protection Laws and Regulations (or was originally transferred subject to such laws), the Transfer Clauses shall apply as applicable and shall be interpreted as follows:

(a) The Transfer Clauses shall be read and interpreted in the light of the provisions of Swiss Data Protection Laws as applicable, and so that they fulfil the intention for them to provide the appropriate safeguards as required by Swiss Applicable Privacy and Data Protection Laws and Regulations.
(b) The Transfer Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Applicable Privacy and Data Protection Laws and Regulations.
(c) In Clause 18(c) of the Transfer Clauses, "Member State" will be interpreted in such a way as to not to exclude Data Subjects in Switzerland from the possibility of bringing a claim under this Agreement before the courts in Switzerland.
(d) Part C of Annex I of the Transfer Clauses shall also include the Swiss Federal Data Protection and Information Commissioner.

XVI. Turkey

A. The following provisions apply to all transfers of Personal Data controlled by Data Exporter in Turkey ("Turkish Personal Data") to countries where there is not an adequate level of protection under the Law on the Protection of Personal Data No. 6698 Dated 24/03/2016 ("Law No. 6698").

B. **Controller to Processor Transfers.**

Article 1 – Obligations of Data Controller

The data controller undertakes that it has fulfilled and shall fulfill the following obligations:

a) Personal data shall be processed and transferred in accordance with Law No. 6698 and other relevant legislation.

b) The data controller shall take all kinds of necessary technical and administrative measures to provide an adequate level of security according to the category of personal data in order to prevent unlawful processing of personal data, prevent unlawful access to personal data, safeguard personal data; and shall also ensure that these measures are taken by the data processor.

c) In case the processed personal data are acquired by others through unlawful means, the data controller shall notify the data subject and the Personal Data Protection Board (hereinafter referred to as "Board") as soon as possible. The Board, if necessary, may declare such situation on its website or by other means which it deems appropriate.

d) The data controller instructs the data processor that the personal data transferred shall only be processed on behalf of the data controller and in accordance with the provisions of the contract and Law No. 6698.

e) The data controller shall promptly notify the data subject and the Board of any violation notification received from the data processor.

f) The data controller shall promptly inform the Board of any problems arising out of the fulfillment of the provisions of this contract by the data processor.

g) The data controller undertakes that the data processor has the capacity to fulfill the obligations arising from these Clauses.

h) The data controller shall have these provisions approved by the Board prior to the transfer of the personal data in accordance with Law No. 6698.

Article 2 – Obligations of Data Processor

The data processor undertakes that it has fulfilled and shall fulfill the following obligations:

a) The data processor shall take all kinds of necessary technical and administrative measures to provide an adequate level of security according to the category of personal data in order to prevent unlawful processing of personal data, prevent unlawful access to personal data and safeguard personal data.

b) The data processor shall process the personal data on behalf of the data controller in compliance with its instructions and the contract. If the data processor fails to comply with the instructions of the data controller for whatever reason, it shall inform the data controller as soon as possible. In this case, the data processor acknowledges that the data controller is entitled to suspend the data transfer and terminate the contract.

c) The data processor shall research whether there is any national regulation contrary to the contract at the contract date with regard to the personal data transferred. If it realizes the existence of such a regulation or in the event of a change in the legislation which is likely to have an adverse effect on its commitments under the contract, it shall promptly inform the data controller. In such a case, the data processor acknowledges that the data controller is entitled to suspend the data transfer and terminate the contract.

d) The data processor accepts that on the termination or expiration of this contract it shall, at the choice of the data controller, return all personal data transferred along with the backups/copies thereof to the data controller or shall destroy all the personal data. If there is any provision in the regulation that prevents the data processor from fulfilling this obligation, it shall cease the data processing activity and take all kinds of necessary technical and administrative measures in order to guarantee confidentiality of the personal data subject to transfer.

e) The data processor shall inform the data controller as soon as possible if the data processor receives any legally binding requests from a judicial authority that require disclosure of personal data to the concerned legal authority or if there is an unauthorized access to personal data.

f) The data processor shall respond as soon as practicable in due form to the enquiries from the data controller within the scope of the contract and shall comply with the decisions and opinions of the Board regarding the processing of the personal data subject to transfer.

g) The data processor acknowledges that the data controller has the authority to carry out/to have carried out inspections in order to determine whether its commitments and obligations are fulfilled or not and provides the necessary support and convenience for this purpose.

h) If the data processor should transfer the personal data to a subcontractor while performing the services under the contact, it must inform the data controller in a demonstrable manner and get its approval. The contract between the data processor and

the subcontractor must include at least the provisions of the contract between the data controller and the processor and of this letter of undertaking.

Article 3 – Common Provisions

a) In case personal data are processed on behalf of the data controller by another natural or legal person, the data controller shall be jointly liable with the data processor with regard to taking the aforesaid administrative and technical measures.

b) The data controller and the data processor shall not disclose and misuse personal data they learned contrary to the provisions of the Law No. 6698.

c) This responsibility for the data controller and the data processor is for an unlimited time.

Annex

The contents of Schedules A and B to the Agreement are incorporated by reference to this Annex to the provisions on Controller to Processor transfers.

Additional measures for sensitive data

None.

The Controller's Controller Registry Information System (VERBIS) Information as provided by the Customer

XVII. United Kingdom

A. The terms below shall have the following meanings ascribed to them for the purposes of this Section SVII:

(a) "UK" means the United Kingdom.

(b) "UK Data Protection Laws" means the UK GDPR, Data Protection Act of 2018, and all UK laws relating to the Processing, privacy, protection, or use of Personal Data.

(c) "UK GDPR" means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

B. To the extent any Data Exporter transfers Personal Data subject to UK Data Protection Laws, either directly or via onward transfer, to a Data Importer located in a country that does not ensure an adequate level of protection within the meaning of UK Data Protection

Laws, the Parties agree to the Transfer Clauses in accordance with Section V of this Schedule C as supplemented by Clause C of this Section XVII.

C. The following additional provisions shall apply so that the Transfer Clauses are suitable for providing an adequate level of protection for such transfer under UK Data Protection Laws:

(a) Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses;

(b) With respect to Section 19 of the Approved Addendum, in the event the Approved Addendum changes, neither Party may end the Addendum except as provided for in the Agreement; and

(c) Any references to the "Clauses" in the Transfer Clauses shall include the amendments set out in this Section XVII of Schedule C.

XVIII. United States

The following provisions apply to all Transfers of Personal Data from one Party (the "**Disclosing Party**") to another Party (the "**Recipient**") that are subject to the laws of California, Colorado, Connecticut, Virginia, or Utah, as described below.

A. California**.** The following provisions apply to all Transfers from a Disclosing Party to a Recipient of Personal Data, and the Processing of Personal Data by that Recipient, which is subject to the California Consumer Privacy Act of 2018 ("CCPA") as codified at Cal. Civ. Code Part 4, Division 3, Title 1.81.5 Section 1798.100 et. seq., as amended or supplemented from time to time, or the California Privacy Rights Act of 2020 ("CPRA") as codified at Cal. Civ. Code Part 4, Division 3, Title 1.81.5 Section 1798.100 et. seq. and operative January 1, 2023, as amended or supplemented from time to time ("**California Personal Data**"):

(a) to the extent the Disclosing Party discloses Deidentified data (as that term is defined under the CPRA) originally derived from California Personal Data to Recipient, or to the extent Recipient creates Deidentified data from California Personal Data received from or on behalf of the Disclosing Party, Recipient shall:

(i) adopt reasonable measures to prevent such Deidentified data from being used to infer information about, or otherwise being associated with, a particular natural person or household;

(ii) publicly commit to maintain and use such Deidentified data in a deidentified form and to not attempt to re-identify the Deidentified data,

except that Recipient may attempt to re-identify the data solely for the purpose of determining whether its deidentification processes satisfy the requirements of the CCPA or CPRA, as applicable; and

(iii) contractually obligate any recipients of the Deidentified data, including sub-processors, contractors, and other third parties, to comply with the provisions of this subdivision (a) of Section XVIII(A) of Schedule C.

(b) where the Disclosing Party acts as a Business with respect to California Personal Data and Recipient acts as a Service Provider of California Personal Data (as the terms "Business" and "Service Provider" are defined under CCPA and CPRA, as applicable) to provide services pursuant to a written contract (the "**Services**"):

(i) Recipient agrees that it Processes California Personal Data as a Service Provider when providing the Services.

(ii) Recipient acknowledges that the Disclosing Party is disclosing California Personal Data in connection with the Agreement only for the limited and specific purposes of receiving the Services.

(iii) Recipient shall: (1) retain, use, disclose, or otherwise process California Personal Data solely on behalf of the Disclosing Party for the specific purpose of providing the Services or as otherwise required by law; (2) Process California Personal Data, at all times, in compliance with the CCPA and CPRA (as applicable) and the Agreement; and (3) provide the same level of privacy protection as is required by the CCPA and CPRA (as applicable).

(iv) Recipient shall not: (1) retain, use, disclose, or otherwise process California Personal Data except as necessary to provide the Services or as otherwise required by law; (2) Sell California Personal Data (as the term "Sell" is defined under CCPA and CPRA, as applicable); (3) Share California Personal Data (as the term "Share" is defined under CPRA); (4) Process California Personal Data in any manner outside of the direct business relationship between Disclosing Party and Recipient; or (5) combine any California Personal Data with Personal Data that it receives from or on behalf of any other third party or its interactions with Consumers (as the term "Consumers" is defined under CCPA and CPRA, as applicable), provided that Recipient may so combine California Personal Data for a Business Purpose (as that term is defined under CCPA and CPRA, as applicable) if directed to do so by the Disclosing Party or as otherwise expressly permitted by the CPRA.

(v) Recipient agrees to cooperate with any reasonable and appropriate audits, inspections, or other steps that the Disclosing Party deems

reasonably necessary to confirm that Recipient processes California Personal Data in a manner consistent with the Disclosing Party's obligations under the CCPA.

(vi) Disclosing Party may, upon reasonable notice to Recipient, take all reasonable and appropriate steps to prevent, stop, or remediate any unauthorized processing of California Personal Data.

(vii) Recipient agrees to immediately notify Disclosing Party in writing if it can no longer comply with the CCPA or CPRA (as applicable) or its obligations under this Agreement.

B. Colorado. The following provisions apply to all transfers from a Disclosing Party to a Recipient of Personal Data, and the processing of Personal Data by that Recipient, which is subject to the Colorado Privacy Act, Col. Rev. Stat. § 6-1-1301 et seq. ("**CPA**"), as amended or supplemented from time to time ("**Colorado Personal Data**"):

(a) to the extent the Disclosing Party discloses Deidentified data (as that term is defined under the CPA) originally derived from Colorado Personal Data to Recipient, or to the extent Recipient creates Deidentified data from Colorado Personal Data received from or on behalf of the Disclosing Party, Recipient shall:

(i) adopt reasonable measures to prevent such Deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(ii) publicly commit to maintain and use such Deidentified data in a deidentified form and to not attempt to re-identify the Deidentified data, except that Recipient may attempt to re-identify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of the CPA; and

(iii) contractually obligate any recipients of the Deidentified data, including subprocessors, contractors, and other third parties, to comply with the CPA.

(b) The Parties agree that the provisions of this Section XVIII(B) shall take effect on July 1, 2023, and shall be of no force or effect prior to that date

C. Connecticut. The following provisions apply to all transfers from a Disclosing Party to a Recipient of Personal Data, and the processing of Personal Data by that Recipient, which is subject to the Connecticut Data Privacy Act, S.B. 6 ("**CTDPA**"), as amended or supplemented from time to time ("**Connecticut Personal Data**"):

(a) to the extent the Disclosing Party discloses Deidentified data (as that term is defined under the CTDPA) originally derived from Connecticut Personal Data to

Recipient, or to the extent Recipient creates Deidentified data from Connecticut Personal Data received from or on behalf of the Disclosing Party, Recipient shall:

(i) adopt reasonable measures to prevent such Deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(ii) publicly commit to maintain and use such Deidentified data in a deidentified form and to not attempt to re-identify the Deidentified data, except that Recipient may attempt to re-identify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of the CTDPA; and

(iii) contractually obligate any recipients of the Deidentified data, including subprocessors, contractors, and other third parties, to comply with the CTDPA.

(b) The Parties agree that the provisions of this Section XVIII(C) shall take effect on July 1, 2023 and shall be of no force or effect prior to that date.

D. Virginia. The following provisions apply to all transfers from a Disclosing Party to a Recipient of Personal Data, and the processing of Personal Data by that Recipient, which is subject to the Virginia Consumer Data Protection Act, S.B. 1392 § 59.1 et seq. ("**VCDPA**"), as amended or supplemented from time to time ("**Virginia Personal Data**"):

(a) to the extent the Disclosing Party discloses Deidentified data (as that term is defined under the VCDPA) originally derived from Virginia Personal Data to Recipient, or to the extent Recipient creates Deidentified data from Virginia Personal Data received from or on behalf of the Disclosing Party, Recipient shall:

(i) adopt reasonable measures to prevent such Deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(ii) publicly commit to maintain and use such Deidentified data in a deidentified form and to not attempt to re-identify the Deidentified data, except that Recipient may attempt to re-identify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of the VCDPA; and

(iii) contractually obligate any recipients of the Deidentified data, including subprocessors, contractors, and other third parties, to comply with the VCDPA.

(b) The Parties agree that the provisions of this Section XVIII(D) shall take effect on January 1, 2023 and shall be of no force or effect prior to that date.

E. Utah. The following provisions apply to all transfers from a Disclosing Party to a Recipient of Personal Data, and the processing of Personal Data by that Recipient, which is subject to the Utah Consumer Privacy Act, S.B. 227 ("**UCPA**"), as amended or supplemented from time to time ("**Utah Personal Data**"):

(c) to the extent the Disclosing Party discloses Deidentified data (as that term is defined under the UCPA) originally derived from Utah Personal Data to Recipient, or to the extent Recipient creates Deidentified data from Utah Personal Data received from or on behalf of the Disclosing Party, Recipient shall:

(i) adopt reasonable measures to prevent such Deidentified data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(ii) publicly commit to maintain and use such Deidentified data in a deidentified form and to not attempt to re-identify the Deidentified data, except that Recipient may attempt to re-identify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of the UCPA; and

(iii) contractually obligate any recipients of the Deidentified data, including subprocessors, contractors, and other third parties, to comply with the UCPA.

(d) The Parties agree that the provisions of this Section XVIII(E) shall take effect on December 31, 2023 and shall be of no force or effect prior to that date.