Everest Group®

SUPPLIER DATA PROTECTION ADDENDUM

This Supplier Data Protection Addendum ("**DPA**" or "**Addendum**") is hereby incorporated by reference into the agreement between the applicable Everest Group entity/entities and the applicable Supplier entity/entities (the "**Agreement**"). By entering into the Agreement, this DPA is agreed to by the parties and the parties are deemed to have signed this DPA. This DPA supplements the agreement between Everest Group and Supplier into which it is incorporated by reference ("Agreement").

1. Definitions.

Any capitalized term used but not defined in this Addendum has the meaning provided to it in the Agreement.

"**Affiliate**" means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with a Party.

"**Applicable Data Protection Law(s)**" refers to all laws and regulations applicable to either party's processing of personal data under the Agreement including, as applicable, the laws and regulations of the United States, the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, including as applicable the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the California Consumer Privacy Act of 2018 ("CCPA").

"**controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"**personal data**" means any information relating to an identified or identifiable natural person ("**data subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**processor**" means the Party to this Agreement that processes personal data on behalf of the controller. The term Processor as used herein is equivalent to the term "Processor" as used in the GDPR, and the term "Service Provider" as used in the CCPA.

"**processing"** (and "process") means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated 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.

"**Privacy Policy**" means the applicable then current Everest Group Privacy Notice available at https://www.everestgrp.com/privacy-notice/ ; or Privacy Notice For Applicants, Employees And Contractors - Everest Group (everestgrp.com).

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

"**UK GDPR**" means the GDPR as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018

"**Supplier Data**" means any personal data Everest Group receives from Supplier under the Products and/or Services.

"**Security Incident**" means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Everest Group Data.

"**Products and/or Services**" means Supplier's products and/or services as outlined in the Agreement.

"**Standard Contractual Clauses**" has the meaning set forth in Schedule 3 (Cross Border Transfer Mechanisms) of this Addendum.

"**sub-processor**" means any third-party engaged by Supplier to process Everest Group Processor Data.

"**Third Party Request**" means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.

"**Everest Group Controller Data**" means any personal data that Supplier processes as a controller subject to Section 2.2 and 4.

"**Everest Group Data**" means any data Supplier received from Everest Group during the provision of the Products and/or Services, including Personal Data. Everest Group Data includes Everest Group Controller Data and Everest Group Processor Data.

"**Everest Group Processor Data**" means any Everest Group Data that is not Everest Group Controller Data.

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "controller", "processor", "profiling", "personal data", and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies.

Controller and Processor

2. Roles of the Parties.

2.1 Supplier as a processor of Everest Group Data. The parties acknowledge and agree that with regard to the processing of Everest Group Processor Data, Everest Group is a controller and Supplier is a processor. Supplier will process Everest Group Processor Data in accordance with Everest Group's instructions as set forth in Section 5 (Everest Group Instructions).

2.2 Supplier as a Controller of Everest Group Data. The parties acknowledge that Supplier may act as an independent controller of Everest Group Data where necessary to provide the Products and/or Services under an applicable Statement of Work or Purchase Order (and for clarity, not as a joint controller with Everest Group). Where Supplier processes Everest Group Controller Data, it shall only do so (a) as set forth in an applicable Statement of Work or Purchase Order and as necessary to provide the Products and/or Services to Everest Group; (b) as necessary to comply with applicable law or regulation, including Applicable Data Protection Law; and (c) as otherwise agreed in writing between the parties.

2.3 Everest Group as a Controller of Supplier Data. The parties acknowledge and agree that with regard to the processing of Supplier Data, Supplier is a controller and Everest Group is an independent controller, not a joint controller with Supplier. Everest Group will process Supplier Data as permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the Privacy Policy.

3. Processing Purpose Limitation. Supplier shall complete Annexure 1 (Details of Processing) and further specify the nature and purpose of the processing, the processing activities, the duration of the processing, the types of personal data and categories of data subjects. Supplier shall not Process Everest Group Data for any purpose of processing other than as indicated in Annexure 1 without the prior written permission of Everest Group. If Supplier is designated as a Processor in Section 2.1 above, the Parties acknowledge and agree that Annexure 1 reflects Everest Group's written instructions regarding the Processing of Everest Group Data in connection with the Agreement.

4. **Compliance**. Each party shall comply with its obligations under Applicable Data Protection Law(s), and this Addendum, when processing personal data. Supplier additionally warrants that Supplier obtained all necessary rights, consents, and permissions to collect, process, share, use and transfer Supplier Data as contemplated in this Agreement, including but not limited to, Everest Group's marketing, sales and recruiting purposes. Upon request, Supplier shall make available any and all records, disclosures or documentation relating to such consents or other authorisations obtained by Supplier.

Supplier as a Processor of Everest Group Data

5. **Everest Group Instructions**. Everest Group appoints Supplier as a processor to process Everest Group Processor Data on behalf of, and in accordance with, Everest Group's instructions (a) as set forth in the Agreement, this Addendum and as necessary to provide the Products and/or Services to Everest Group, and (b) as otherwise agreed in writing between the parties. Supplier is prohibited from (1) selling personal data; (2) retaining, using, or disclosing personal data for any purpose other than for the specific purpose of performing the Products and/or Services, or processing personal data for any commercial purpose other than providing the Products and/or Services; (3) retaining, using, or disclosing personal data outside of the direct business relationship between Everest Group and Supplier. Supplier certifies that it understands these prohibitions and will comply with them.

6. **Confidentiality.**

6.1 Responding to third-party requests. In the event any third-party request is made directly to Supplier in connection with Supplier's processing of Everest Group Processor Data, Supplier will promptly inform Everest Group and provide details of the same, to the extent legally permitted. Supplier will not respond to any Third-Party Request without Everest Group's prior consent, except as legally required to do so or to confirm that such Third-Party Request relates to Everest Group.

6.2 Confidentiality obligations of Supplier Personnel. Supplier will ensure that any person it authorizes to process Everest Group Data has agreed to protect personal data in accordance with Everest Group's confidentiality obligations in the Agreement.

7. **Subcontracting.** Should Everest Group provide a written authorization for Supplier to engage sub-processors to process Everest Group Processor Data, any such authorization is conditioned on the following requirements:
   a. Supplier provides Everest Group with an up-to-date list of all Supplier sub-processors prior to allowing any sub-processor to process personal data. Supplier shall give notice of any change in sub-processors at least thirty (30) days prior to any such change to privacy@everestgrp.com.
   b. Supplier certifies that it has entered into a written contract with sub-processor that includes terms substantially similar to this Addendum in which Supplier imposes data protection terms that require sub-processors to protect the personal data to the standard required by this Addendum and Applicable Data Protection Law(s).
   c. Everest Group may request a copy of such agreement between Supplier and any sub-processor and may withhold consent to the use of such sub-processor if Supplier does not provide such agreement or such agreement does not contain sufficient protection of Everest Group Data. Supplier may redact such agreement prior to sharing with Everest Group to the extent necessary to protect its trade secrets or confidential information.
   d. Supplier remains liable for any breach of this Addendum that is caused by an act, error or omission of its sub-processor.
   e. Everest Group may object to Supplier's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds. In such an event, the parties shall discuss commercially reasonable alternative solutions in good faith. If the parties cannot reach resolution, Supplier will either not appoint or replace the sub-processor or, if this is not possible, Everest Group may suspend or terminate the Agreement.

f. Supplier conducts appropriate due diligence on its sub-processors.

8. **Data Subject Rights.** To the extent Everest Group, in its ordinary use of the Products and/or Services, does not have the ability to address a data subject's request to exercise their rights under Applicable Data Protection Law(s), Supplier shall, upon Everest Group's request, provide commercially reasonable assistance to Everest Group in resolving any such data subject request.

9. **Impact Assessments and Consultations.** Supplier shall provide reasonable cooperation to Everest Group in connection with any data protection impact assessment or consultations with supervisory authorities that may be required under Applicable Data Protection Law(s).

Security and Audits

10. **Return or Deletion of Everest Group Data.** Upon Everest Group's request or upon termination of the Agreement, Supplier agrees, at Everest Group's option, to either deliver to Everest Group or destroy in a manner that prevents Everest Group Data from being reconstructed, any Everest Group Data and any copies in Supplier's control or possession. Such delivery or destruction shall occur as soon as practicable and in any event within fifteen (15) business days after the effective date of such termination or the date of Everest Group's request. Upon reasonable notice and if requested by Everest Group, Supplier shall provide Everest Group with a certificate by an officer of compliance with this Section. This Section shall survive termination of the Agreement.

11. **Security.**

11.1 Security Measures. Each party has implemented appropriate technical and organizational measures for ensuring the security of the personal data being processed and will maintain the technical and organizational security measures as set forth in the Agreement. Additional information about the technical, physical and organizational security measures to protect personal data is set forth in Schedule 1 (Technical, Physical and Organizational Security Measures).

11.2 Security Incident Notification. Supplier shall, to the extent permitted by law, immediately notify Everest Group of any reasonably suspected or actual Security Incident. Notices of a Security Incident should be given within 72 hours to Everest Group at security@everestgrp.com. The notice shall summarize in reasonable detail the nature and scope of the Security Incident (including the nature of the data and data subjects impacted) and the corrective action already taken or to be taken by Supplier. The notice shall be timely supplemented in the detail reasonably requested by Everest Group, inclusive of relevant forensic reports. Unless prohibited by an applicable statute or court order, Supplier shall also notify Everest Group of any third-party legal process relating to any Security Incident, including, but not limited to, any legal process initiated by any governmental entity.

11.3 Security Incident Remediation. Supplier shall promptly take all necessary and advisable corrective actions, and shall, at its sole cost and expense, assist Everest Group in investigating, remedying, providing notices required by law and taking any other action Everest Group deems necessary regarding any Security Incident and any dispute, inquiry or claim concerning any Security Incident. Supplier shall use best efforts to remedy any Security Incident immediately but no later than within thirty (30) days of discovery of a Security Incident. Supplier's failure to remedy any Security Incident in a timely manner will be a material breach of the Agreement.

11.4 Required Breach Notices. Supplier acknowledges that it is solely responsible for the confidentiality and security of the personal data in its possession, custody or control, or for which Supplier is otherwise responsible. Everest Group will decide on whether any notice of breach is legally required to be given to any person, and if so, the content of that notice. Supplier will bear all costs of the notice. If Everest Group reasonably determines that the Security Incident is likely to have substantial adverse impact on Everest Group's relationship with its customers or associates or otherwise substantially harm its reputation, Everest Group may terminate the Agreement.

12. **Audits.** Subject to reasonable notice, Supplier shall provide Everest Group an opportunity to conduct a privacy and security audit of Supplier's security program and systems and procedures that are applicable to the Products and/or Services. Audits will occur annually or following notice of a security incident. If the audit reveals any vulnerability, Supplier shall correct such vulnerability at its sole cost and expense. Supplier shall use best efforts to correct all vulnerabilities immediately. Supplier's failure to complete corrections in a timely manner will be a material breach of the Agreement.

13. Contacts and Notices

13.1 Any notices under this Agreement are to be addressed to the other party as follows:

To Everest Group

To:	With a copy to:
Everest Global, Inc FAO of: Legal (Privacy & Data Protection) 12770 Merit Drive, Suite 800, Dallas, TX 75251 e-mail to mailbox privacy@everestgrp.com and copy to legal@everestgrp.com	**Everest Business Advisory India Pvt Ltd** FAO of: Legal (Privacy & Data Protection) Spaze Platinum Tower, 1st Floor, Sector-47, Sohna Road, Gurgaon, 122001 **Everest Group Consulting Limited** FAO of: Legal Department (Privacy & Data Protection) 27/28 Eastcastle Street, London, United Kingdom, W1W 8DH

To Processor

To:	With a copy to:
As provided in the Agreement or Purchase Order	As provided in the Agreement or Purchase Order

13.2 The contact details of the data protection officer or other authorized representatives for data protection matters of the Processor are as follows: As provided in the Agreement or Purchase Order

International Provisions

14. **Cross-Border transfer.** To the extent Everest Group's use of the Products and/or Services requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e., the European Economic Area, the United Kingdom or Switzerland) to a recipient in locations outside of that jurisdiction, the parties hereby incorporate, and agree to comply with, the Standard Contractual Clauses of June 4, 2021 ("**SCCs**") approved by the European Commission. In such case:
    a. Module 1 (Controller to Controller) of the SCCs shall apply if Supplier is designated as a Controller under Section 2.2 above.
    b. Module 2 (Controller to Processor) of the SCCs shall apply if Supplier is designated as a Processor under Section 2.1 above.
    c. The parties will complete Annex 1, and agree to Schedule 1 and 2, of this Agreement in lieu of the Annexes to the SCCs.

d. The competent supervisory authority for purposes of the SCCs is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).
e. The Parties represent that they do not believe the laws and practices in any country to which Everest Group Personal Data is transferred for purposes of the Agreement will prevent Supplier from fulfilling its obligations under this Agreement or the SCCs.

Miscellaneous

15. **Cooperation and Data Subject Rights.** In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable) or (b) any Third-Party Request relating to the processing of personal data conducted by the other party as a controller, such party will promptly inform such other party in writing. The parties agree to cooperate, in good faith, as necessary to respond to any Third-Party Request and fulfill their respective obligations under Applicable Data Protection Law

16. **Conflict.** In the event of any conflict or inconsistency among the Agreement, this Addendum, or any applicable Statement of Work regarding Supplier's privacy and security obligations, the provision more protective of personal data shall control.

17. **Entire Agreement.** This Addendum supersedes and replaces all prior proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between Everest Group and Supplier.

This Agreement is entered into and becomes a binding part of the Principal Agreement with effect from the date hereof.

Annexure 1

DETAILS OF PROCESSING

1. **Nature and Purpose of the processing.**

Supplier or Everest Group, as applicable, will process personal data as necessary to, respectively, provide or obtain the benefit of the Products and/or Services. The supplier does not sell Everest Group personal data and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

2. **Processing Activities**. Personal data will be subject to the processing activities necessary for the provision or to obtain the benefit of the Products and/or Services, as applicable.

[Further details of activities to be provided by the Supplier in the SOW/PO]

3. **Duration of the processing**. The period for which personal data will be retained will be for the duration of the Agreement, or earlier, if so, requested by Everest Group. Where Supplier, as controller, provides personal data to Everest Group as an independent controller in connection with the Agreement, the personal data shall be retained for as long as necessary for Everest Group to obtain the benefit of the Products and/or Services.

4. **Categories of Data Subjects**. Everest Group's employees, customers, end users, sales leads or job candidates. [Further details any other Data Subject category to be provided by the Supplier in the SOW/PO]

5. **Categories of Personal Data**. Supplier or Everest Group, as applicable, process such categories of personal data as necessary to provide or receive the benefit of the Products and/or Services, including, without limitation, the categories of personal data specified in the Agreement, Statement of Work or Purchase Order and may include the names, email addresses and other contact details of data subjects.

6. **Sensitive Data or Special Categories of Data**. [List of Sensitive data if required to be processed under the Agreement to be provided by the Supplier in the SOW/PO]

7. **Processing locations**. The parties shall only process personal data in the countries as agreed upon in a separate signed writing between the parties.

8. **For transfers to Supplier's sub-processors**, the subject matter, nature, and duration of the processing for each approved sub-processor is as necessary for the provision of the Products and/or Services.

SCHEDULE 1

Cross-border transfer - Standard Contractual Clause(s)

1. Data Exports or Transfers from the European Union/European Economic Area (EU/EEA) to Third Countries

The "2021 SCCs" means the Standard Contractual Clauses as approved by the European Commission Implementing Decision 2021/914 of 4 June 2021 available at Standard contractual clauses for international transfers (europa.eu).

The 2021 SCCs are unmodified and will take precedence over any conflicting provisions in this DPA or the Agreement. The 2021 SCCs (i) apply to personal data transferred pursuant to the Agreement, provided, the personal data is transferred from the EU/EEA to a third country as defined by the European Commission and (ii) are hereby agreed to between the parties and deemed entered into and incorporated into this DPA by reference as if fully reproduced herein. The 2021 SCCs are completed as follows:

(a) Consistent with the GDPR, Module One (Controller to Controller) of the 2021 SCCs will apply where the transfer of personal data is from controller to controller (whether jointly or independently controlled).
(b) Consistent with the GDPR, Module Two (Controller to Processor) of the 2021 SCCs will apply where the transfer of personal data is from controller to processor.
(c) Consistent with the GDPR, Module Three (Processor to Processor) of the 2021 SCCs will apply where the transfer of personal data is from processor to processor.
(d) Consistent with the GDPR, Module Four (Processor to Controller) of the 2021 Standard Contractual Clauses will apply where the transfer of personal data is from processor to controller.
(e) With respect to the 2021 SCCs, as applicable:
    i. the optional docking provision in Clause 7 will not apply;
    ii. Option 2 will apply in Clause 9 and the time period set forth in Annex 1 of the DPA is the specified time period.
    iii. the optional language in Clause 11 will not apply;
    iv. regarding Clause 17, the governing law will be Irish law;
    v. regarding Clause 18, disputes will be resolved before the courts of Ireland;
    vi. with respect to the 2021 SCCs, as applicable, Annex I, Part A:

Data exporter(s):

Name: The entity identified as [TO BE SPECIFIED BY PARTIES AT THE TIME OF FINALISAING THE SOW] in the Agreement for Products and/or Services.

Address: The address as specified in the Agreement: [TO BE FILLED BY PARTY IDENTIFIED AS EXPORTER UNDER THE SOW]

Contact person's name, position and contact details: The contact as specified in the Agreement: [TO BE FILLED BY PARTY IDENTIFIED AS EXPORTER UNDER THE SOW]

Activities relevant to the data transferred under these Clauses: The activities as specified in Section 1 of the DPA.

Signature and date: By executing the Agreement for Products and/or Services, Exporter is deemed to have signed the Standard Contractual Clauses, including their Annexes, as of the effective date of the Agreement.

Role (controller/processor): The exporter's role as applicable and as described in the DPA.

Data importer(s):

Name: The entity identified as [TO BE SPECIFIED BY PARTIES AT THE TIME OF FINALISAING THE SOW/PO] in the Agreement for Products and/or Services.

Address: The address as specified in the Agreement: [TO BE FILLED BY PARTY IDENTIFIED AS IMPORTER UNDER THE SOW/PO]

Contact person's name, position and contact details: [TO BE FILLED BY PARTY IDENTIFIED AS IMPORTER UNDER THE SOW/PO]

Activities relevant to the data transferred under these Clauses: The activities as specified in Annex 1 of the DPA.

Signature and date: By executing the Agreement to provide Products and/or Services, Importer is deemed to have signed the Standard Contractual Clauses, including their Annexes, as of the effective date of the Agreement.

Role (controller/processor): The importer's role as applicable and as described in the DPA.

(f) with respect to the 2021 SCCs, as applicable, Annex I, Part B:

The categories of data subjects whose personal data is transferred are described in Annex 1 of the DPA.

The categories of personal data transferred are described in Annex 1 of the DPA.

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, is described in Annex 1 of the DPA.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis is described in Annex 1 of the DPA.

Nature of the processing is described in *Annex 1* of the DPA.

Purpose(s) of the data transfer and further processing is described in Annex 1 of the DPA.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that perio*d, is described in *Annex 1* of the DPA.

For transfers to (sub-)processors, also specify the subject matter, nature and duration of the processing is described in Annex 1 of the DPA.

(g) with respect to the 2021 SCCs, as applicable, Annex I, Part C:

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

(i) with respect to the 2021 SCCs, Annex II:

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. As described in Schedule 2 of the DPA.

Measures of pseudonymisation and encryption of personal data. As described in *Schedule 2* of the DPA.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services. As described in *Schedule 2* of the DPA.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. As described in *Schedule 2* of the DPA.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing. As described in *Schedule 2* of the DPA.

Measures for user identification and authorization. As described in *Schedule 2*of the DPA.

Measures for the protection of data during transmission. As described in *Schedule 2* of the DPA.

Measures for the protection of data during storage. As described in *Schedule 2*of the DPA.

Measures for ensuring physical security of locations at which personal data are processed. As described in *Schedule 2* of the DPA.

Measures for ensuring events logging. As described in *Schedule 2* of the DPA.

Measures for ensuring system configuration, including default configuration. As described in *Schedule 2* of the DPA.

Measures for internal IT and IT security governance and management. As described in *Schedule 2* of the DPA.

Measures for certification/assurance of processes and products. As described in *Schedule 2* of the DPA.

Measures for ensuring data minimization. As described in *Schedule 2* of the DPA.

Measures for ensuring data quality. As described in *Schedule 2* of the DPA.

Measures for ensuring limited data retention. As described in *Schedule 2* of the DPA.

Measures for ensuring accountability. As described in *Schedule 2* of the DPA.

Measures for allowing data portability and ensuring erasure. As described in *Schedule 2* of the DPA.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter. As described in *Schedule 2* of the DPA.

2. Data Exports or Transfers from the United Kingdom (UK) to non-EU/EEA countries

Data Exports or Transfers from the United Kingdom (UK) to non-EU/EEA countries

The "UK SCCs" means the UK's new standard form International Data Transfer Agreement ("IDTA"), and International Data Transfer Addendum (the "UK Addendum") to the new EU Standard Contractual Clauses (SCC Addendum) effective from March 21, 2022, available at international-data-transfer-addendum.pdf (ico.org.uk)

The relevant parties enter into the terms of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0) which are hereby incorporated into this agreement and completed as follows:

Table 1 – Parties: is completed as follows:

- The data exporter is Customer/Everest Group, who is acting as Controller; The entity identified as Customer in the Agreement for Products and/or Services.
- The data importer is the Supplier or Provider, who is acting as Processor
- Customer' address is the address on the first page of this agreement and its contact person for matters related to Standard Contractual Clauses is Shaili Bhandari, Data Protection Officer; Michael Peacock, IT Director Security; Email: privacy@everestgrp.com; 1-214-451-3000
- Processor's address is the address on the first page of this agreement and its contact person for matters related to Standard Contractual Clauses is the contact information as specified in the Agreement or, if none, the contact information associated with Supplier's account
- Signature and date: By executing an Agreement for Products and/or Services, Customer is deemed to have signed the Standard Contractual Clauses, including their Annexes and/or Appendices, as of the effective date of the Agreement for Products and/or Services

Table 2 - Selected SCCs, Modules and Selected Clauses: is completed as follows – select the second option (the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum) and complete as follows:

Module	**Module in operation**	**Clause 7 (Docking Clause)**	**Clause 11 (Option)**	**Clause 9a (Prior Authorisation or General Authorisation)**	**Clause 9a (Time period)**	**Is personal data received from the Importer combined with personal data collected by the Exporter?**
1	No	N/A	N/A	N/A	N/A	N/A
2	Yes	No	No	Prior Authorisation	time period set forth in Section 1 of the DPA is the specified time period	Yes
3	No	N/A	N/A	N/A	N/A	N/A
4	No	N/A	N/A	N/A	N/A	N/A

Table 3 Appendix Information: is completed as follows:

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: is completed as follows:

- The data exporter is acting as Controller; The entity identified as Customer or Everest Group in the Agreement for Products and/or Services.
- The data importer is the Supplier, who is acting as Processor; The entity identified as Supplier or Provider in the Agreement for Products and/or Services.
- Customer' address is the address on the first page of this agreement and its contact person for matters related to Standard Contractual Clauses is Shaili Bhandari, Data Protection Officer; Michael Peacock, IT Director Security; Email: privacy@everestgrp.com; 1-214-451-3000

- Processor's address is the address on the first page of this agreement and its contact person for matters related to Standard Contractual Clauses is the contact information as specified in the Agreement or, if none, the contact information associated with Supplier's account
- The transfer of Customer Personal Data relates to Customer's marketing activities
- The transfer of Personal Data relates to the Processor's activities as set out in the Agreement

Annex 1B: Description of Transfer

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Annex III: List of Sub processors (Modules 2 and 3 only):

SCHEDULE 2

TECHNICAL, PHYSICAL AND ORGANIZATIONAL SECURITY MEASURES

This Schedule 2 details the technical and organizational security measures to be taken by Supplier with respect to personal data processed in connection with the Agreement.

1. Organisational/Administrative Security Measures: Supplier has implemented, and will maintain and update as appropriate throughout its Processing of Personal Data:

1.1. A written and comprehensive information security program in compliance with applicable data protection laws. The security measures shall be appropriate to the nature and risk to personal data, and in any event shall not be less stringent than those prescribed under applicable laws.

1.2. A data loss prevention program that reflects reasonable policies or procedures designed to detect, prevent, and mitigate the risk of data security breaches or identify theft, which shall include at a minimum:

1.2.1. appropriate policies and technological controls designed to prevent loss of Personal Data; and

1.2.2. a disaster recovery/business continuity plan that addresses ongoing access, maintenance and storage of Personal Data as well as security needs for back-up sites and alternate communication networks.

1.3. Policies and procedures to limit access to Everest Group's Personal Data to those who require such access to perform their roles and responsibilities in connection with the Agreement, including regular updates to such access based on changes to Supplier's personnel, policies or procedures.

1.4. Procedures to verify all access rights through effective authentication methods.

1.5. A government agency data access policy that refuses government access to data, except where such access is required by law, or where there is imminent risk of serious harm to individuals.

1.6. Policies and procedures for assessing legal basis for, and responding to, government agency requests for data.

1.7. Specific training of personnel responsible for managing government agency requests for access to data, which may include requirements under applicable Data Protection Law(s).

1.8. Processes to document and record government agency requests for data, the response provided, and the government authorities involved.

1.9. Procedures to notify Everest Group about any request or requirement for government agency access to data, unless legally prohibited.

2. Physical Security Measures

2.1. Supplier has implemented and will maintain and update as appropriate throughout its Processing of Everest Group Personal Data, appropriate physical security measures for any facility used to Process

Everest Group Personal Data and continually monitor any changes to the physical infrastructure, business, and known threats.

2.2. Supplier's servers and office spaces have a physical security program that manages visitors, building entrances, CCTVs (closed circuit televisions), and overall office security. All employees and contractors are required to have approved access cards and visitors are required to be escorted throughout those parts of the premises containing personal data.

3. Technical Security Measures: Supplier shall throughout its Processing of Everest Group Personal Data:

3.1. perform vulnerability scanning and assessments on applications and infrastructure used to Process Everest Group Personal Data.

3.2. secure its computer networks using multiple layers of access controls to protect against unauthorized access.

3.3. restrict access through mechanisms such as, but not limited to, management approvals, robust controls, logging, and monitoring access events and subsequent audits.

3.4. identify computer systems and applications that warrant security event monitoring and logging, and reasonably maintain and analyze log files.

3.5. use up-to-date, industry standard, commercial virus/malware scanning software that identifies malicious code on all of its systems that Process Everest Group Personal Data.

3.6. encrypt Everest Group Personal Data in transit.

3.7. encrypt Everest Group Personal Data at rest and solely manage and secure all encryption keys (i.e., no other third party shall have access to these encryption keys, including Sub-processors).

3.8. pseudonymizes personal data only in accordance with Everest Group's instructions.

3.9. ensures data minimisation in accordance with its instructions from Everest Group, data privacy policies and industry standards.

4. Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Everest Group. When Supplier engages a sub-processor under this Addendum, Supplier and the sub-processor enter into an agreement with data protection terms substantially similar to those contained herein. Each sub-processor agreement must ensure that Supplier is able to meet its obligations to Everest Group. In addition to implementing technical and organizational measures to protect personal data, sub-processors must a) notify Supplier in the event of a Security Incident so Supplier may notify Everest Group; b) delete data when instructed by Supplier in accordance with Everest Group's instructions to Supplier; c) not engage additional sub-processors without authorization in accordance with this Addendum; d) assist with responses to data subject requests; and e) not process data in a manner which conflicts with Everest Group's instructions to Supplier.

5. Audit. Supplier conducts regular audits to ensure compliance with its privacy and security standards Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing of personal data. Supplier maintains industry standard security certifications, subject to regular audits.