DATA PROCESSING AGREEMENT

THIS DATA PROCESSING AGREEMENT forms part of the Travel Services Agreement (the "**Main Agreement**") between Company ("**Company"**) and Travel Incorporated ("**Service Provider"**) located at 4355 River Green Parkway, Duluth, GA 30096 under which Service Provider provides services to the Company. The Company and Service Provider are referred to in this Addendum as "**Parties**" and individually as a "**Party**".

1. Definitions

Unless otherwise defined below, all capitalized terms used in this Addendum have the same meaning given to them in the Main Agreement and/or exhibits thereto.

"Data Controller" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller.

"European Data Protection Laws" means the European Union's General Data Protection Regulation (EU) 2016/679 (the "**GDPR**") and its national implementations in the EEA and Switzerland, and the UK General Data Protection Regulation (the "**UK GDPR**"), each as applicable and as amended or replaced from time to time.

"Data Protection Laws" means all local, state, national and/or foreign laws, treaties and/or regulations (as any of the foregoing may be amended or replaced from time to time) applicable to the protection and Processing of Personal Data (including, without limitation, European Data Protection Laws, the California Consumer Privacy Act (as amended by the California Consumer Privacy Act), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act and the Virginia Consumer Data Protection Act).

"Data Subject" means the person to whom the Personal Data relates.

"EEA" means the European Economic Area.

"Personal Data" means any data (whether referred to as personal data, personal information or another term) (A) that relates to (i) an identified or identifiable natural person or, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data under applicable Data Protection Laws), or (B) that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, use of, or access to, Personal Data transmitted, stored or otherwise Processed.

"Processing" or **"Process"** means any operation or set of operations performed on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

"Services" are those products, services, and other deliverables provided under the Main Agreement.

"Standard Contractual Clauses" means (i) the standard contractual clauses (the "**EU SCCs**") for the transfer of personal data to processors established in third countries authorized by and annexed to the European Union Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and any amendments or replacements of such EU SCCs, pursuant to the GDPR, and (ii) the international data transfer agreement (the "**UK IDTA**") and the international data transfer addendum (the "**UK Addendum**") authorized by the UK Information Commissioner's Office and effective 21 March 2022, and any amendments or replacements of such UK IDTA and UK Addendum, pursuant to Section 119A of the UK GDPR.

"Subprocessor" means a third-party entity engaged by Service Provider, but not specifically required or mandated by Company, as a subcontractor to Process Personal Data under this Addendum.

"Valid Transfer Mechanism" means a data transfer mechanism permitted by European Data Protection Laws as a lawful basis for transferring Personal Data to a recipient outside of the EEA, Switzerland or the UK, which may include, without limitation, the Standard Contractual Clauses or certification under any program established between or among the governments of the EU, Switzerland, the UK and/or the U.S. for purposes of ensuring adequate protection for data transfers (including any successor programs to the EU-U.S. Privacy Shield Program, the Swiss-U.S. Privacy Shield Program, and the EU-U.S. Data Privacy Framework).

2. Processing Personal Data

2.1. Scope and Role of the Parties. This Addendum applies to the Processing of Personal Data by Service Provider in the course of providing Services under the Main Agreement. For the purposes of this Addendum: (i) Company is the Data Controller; (ii) with respect to Personal Data for which Company is the Data Controller, Service Provider is the Data Processor Processing such Personal Data on Company's behalf; (iii) with respect to Personal Data for which Company is a Data Processor for a third party Data Controller, Service Provider is a sub-processor to Process Personal Data on the Data Controller's behalf. For simplification purposes, Service Provider is hereinafter referred to as a Data Processor for scenario (ii) and (iii) above. To the extent Service Provider acts as a Data Processor to a third party Data Controller, (a) any notifications given by the third party Data Controller to Company will be conveyed to Service Provider insofar as they relate to the Services provided by Service Provider; and (b) any instructions given by Company to Service Provider relating to the Processing of Personal Data are the instructions given by the third party Data Controller.

2.2. Instructions for Processing. Service Provider shall Process Personal Data in accordance with Company's instructions. Company instructs Service Provider to Process Personal Data to provide Services in accordance with the Main Agreement and this Addendum. Company may provide additional instructions to Process Personal Data. If Service Provider believes that an additional instruction provided by Company violates applicable Data Protection Laws, it shall inform Company accordingly. Service Provider shall Process Personal Data obtained hereunder from Company solely for purposes of fulfilling Service Provider's obligations under the Main Agreement.

2.3. Data Authorization. In addition, Company acknowledges and agrees that for Service Provider to fulfill its services hereunder and the Main Agreement, Service Provider may from time to time need to provide Personal Data concerning Company and its travelers to third party technology providers and other service providers who assist Service Provider with various aspects of the services. These third parties are called Subprocessors in this DPA and Service Provider will remain responsible for their proper handling of any Personal Data of Company or its travelers.

2.4. Compliance with Laws. Company shall comply with Data Protection Laws applicable to Company in its role as a Data Controller Processing Personal Data. Service Provider shall comply with Data Protection Laws applicable to

Service Provider in its role as a Processor Processing Personal Data. For the avoidance of doubt, Company is not responsible for complying with Data Protection Laws directly applicable to Service Provider as a Data Processor.

3. Subprocessors

3.1. Use of Subprocessors. Service Provider may engage Subprocessors to Process Personal Data. Service Provider shall ensure that any such Subprocessor has entered into a written agreement requiring the Subprocessor to abide by terms no less protective as to Personal Data than those provided in this Addendum. Upon Company's request, Service Provider will make available to Company a summary of the Personal Data Processing activities of any such Subprocessor. Service Provider shall be liable for the acts and omissions of any Subprocessors to the same extent as if the acts and omissions were performed by Service Provider.

3.2. Notification of Subprocessors. Service Provider shall give Company prior written notice of the appointment of any Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. Service Provider shall not engage or disclose Personal Data provided by Company under the Main Agreement to any proposed Subprocessor except with the prior written consent of Company.

3.3. Objection to Subprocessors. If, within thirty (30) calendar days of receipt of notification of a proposed Subprocessor engagement, Company notifies Service Provider in writing of any objections (on reasonable grounds) to the proposed engagement, Service Provider shall not appoint and shall not disclose Personal Data provided by Company under the Main Agreement to the proposed Subprocessor until reasonable steps have been taken to address the objections raised.

4. Data Center Location and Data Transfers

4.1. Storage of Personal Data. Personal Data will be hosted in data centers located in the United States, the UK or a country in the EEA, unless the Parties otherwise expressly agree in writing.

4.2. Access to and Transfer of Personal Data. Notwithstanding Section 4.1, in order to provide the Services, Service Provider and its Subprocessors will only access Personal Data from (i) countries in the EEA; (ii) countries formally recognized by the European Commission as providing an adequate level of data protection ("**Adequate Countries**"); (iii) the UK; and (iv) the United States and other non-Adequate Countries, provided that Service Provider makes available to Company a Valid Transfer Mechanism and that, with respect to access by Subprocessors, the requirements of Section 3 are met.

5. Rights of Data Subjects

5.1. Correction, Deletion, or Restriction. Service Provider will, as necessary to enable Company or a third party Data Controller to meet its obligations under applicable Data Protection Laws, either (i) provide Company or the third party Data Controller with its own functionality or ability to correct or delete Personal Data or restrict its Processing; or (ii) if technically possible, at Company's specific request, make such corrections, deletions, or restrictions on Company's or the third party Data Controller's behalf if such functionality or ability is not available to Company or the third party Data Controller (with the choice between (i) and (ii) being at Company's discretion). Service Provider is responsible for notifying any Subprocessors of correction, deletion, or restriction request, to the extent such a request is applicable.

5.2. Access to Personal Data. To the extent a Data Subject's Personal Data is not accessible to Company or the third

party Data Controller, Service Provider will, as necessary to enable Company or a third party Data Controller to meet their obligations under applicable Data Protection Laws, provide reasonable assistance to make such Personal Data available to Company or the third party Data Controller.

5.3. Handling of Data Subject Requests. For the avoidance of doubt, Company or the third-party Data Controller is responsible for responding to Data Subject requests for access, correction, deletion, or restriction of that person's Personal Data ("**Data Subject Request**"). If Service Provider receives a Data Subject Request, Service Provider shall promptly redirect the Data Subject to Company.

5.4. Data Portability. For the avoidance of doubt, Company or the third-party Data Controller is responsible for responding to Data Subject's data portability requests. To the extent a Data Subject's Personal Data is not accessible to Company or the third party Data Controller, Service Provider will, as necessary to enable Company or the third party Data Controller to meet their obligations under applicable Data Protection Laws, provide such Personal Data extract in a structured, commonly used and machine-readable format.

6. Government Access Requests

Unless prohibited by applicable law or a legally binding request of law enforcement, Service Provider shall promptly notify Company of any request by government agency or law enforcement authority for access to or seizure of Personal Data.

7. Service Provider Personnel

Service Provider shall take reasonable steps to require screening of its personnel who may have access to Personal Data and shall require such personnel to receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data. All Service Provider personnel that handle Personal Data on behalf of Company are required to sign confidentiality agreements with Service Provider. Such confidentiality obligations shall survive termination of employment.

8. Security

8.1. Security Program. Service Provider shall implement appropriate and reasonable technical and organizational measures designed to protect Personal Data against unauthorized access or disclosure or accidental or unlawful destruction, loss, or alteration. Such measures shall be appropriate to (i) the size, scope, and type of Service Provider's business; (ii) the type of information that Service Provider will Process; and (iii) the need for security and confidentiality of such information.

8.2. Breach Notification. Service Provider shall promptly (and in any case not more than 72 hours of becoming aware of a Personal Data Breach) notify Company of any Personal Data Breach affecting the Personal Data that Service Provider maintains on Company's behalf. The notice will include: (i) the date or date range of the Personal Data Breach; (ii) the date the Service Provider discovered the Personal Data Breach; (iii) a description of the Personal Data Breach; (iv) the number of Data Subjects affected by the Personal Data Breach; (v) types of Personal Data involved in the Personal Data Breach; the likely consequences of the Personal Data Breach; and the steps that Service Provider has taken to investigate the Personal Data Breach, mitigate potential harm and possible adverse effects, and prevent further Personal Data Breaches. Service Provider will promptly supplement the

notice as necessary with information about the Personal Data Breach as Service Provider obtains the information, including Service Provider's assessment as to whether the Personal Data Breach is reportable under Data Protection Laws. Service Provider shall fully cooperate in the investigation of the Personal Data Breach and provide sufficient information to allow Company to meet its obligations under Data Protection Laws and under contract, if applicable. To the extent any applicable law requires that the affected Data Subjects or governmental authority be notified of a Personal Data Breach caused by Service Provider or any of its Subprocessors or with respect to IT systems under the control of Service Provider or any of its Subprocessors, Service Provider will be responsible for, at its own cost and expense, and indemnify Company for:

a. At Company's request, and where possible under law, providing such notices to Data Subjects or governmental authorities containing the information required by applicable law, Service Provider will obtain Company's prior approval of any content, form and timing of such notice;
b. Conducting any forensic and security review, investigation and audit in connection with such Personal Data Breach;
c. Providing remediation services and other reasonable assistance to such Data Subjects as (a) required under law, and (b) requested by governmental authorities; and
d. Providing full cooperation to Company in responding to such Personal Data Breach.

To the extent that Company is subject to or involved in an investigation by a governmental authority, litigation, or any inquiry, formal or informal, arising out of or related to a Personal Data Breach, Service Provider will provide full cooperation to Company in responding to such event.

9. Audit

Service Provider shall make available, upon reasonable request, information necessary to demonstrate compliance with this Addendum and, upon reasonable prior notice and mutually agreed scheduling, shall allow for reasonable audits or i inspection by Company in relation to the Processing of Personal Data under the Main Agreement.

10. Return and Deletion of Personal Data

Upon termination of the Services, Service Provider shall, at Company's option, delete or return all Personal Data to Company and delete existing copies unless applicable law requires storage of the Personal Data. In such case, Service Provider shall continue to ensure the confidentiality of all such Personal Data.

11. Indemnification; Limitations on Liability; Remedies.

Subject to the limits of liability addressed in the Main Agreement, Service Provider agrees to indemnify and hold harmless Company, its subsidiaries and related companies and their officers, directors, employees, workers and agents, from and against all claims or threats of claims, cost, losses, liabilities, expenses (including attorneys' fees) resulting from or arising out of any third party claims due to: (i) Service Provider's breach of this Addendum; (ii) a violation by Service Provider or any of its Subprocessors of Data Protection Laws; (iii) a Personal Data Breach affecting Company or its Personal Data that was caused by Service Provider or any of its Subprocessors; and (iv) any claim related to the infringement of a privacy right or other similar privacy-related action caused by Service Provider or any of its Subprocessors.

Subject to the limits of liability addressed in the Main Agreement, Company agrees to indemnify and hold harmless Service Provider, its subsidiaries and related companies and their officers, directors, employees, workers and agents, from and against all claims or threats of claims, cost, losses, liabilities, expenses (including attorneys' fees) resulting from or arising out of any third party claims due to: (i) Company's breach of this Addendum; (ii) a violation by Company of Data Protection Laws; (iii) a Personal Data Breach affecting Company or its Personal Data that was caused by Company; and (iv) any claim related to the infringement of a privacy right or other similar privacy-related action caused by Company.

Notwithstanding the foregoing or anything else in this Addendum to the contrary, the liability limits in the Main Agreement shall apply to all matters under this Addendum.

12. General Provisions

12.1. Termination. The term of this Addendum will end simultaneously and automatically with the termination of the Main Agreement.

12.2 Conflict. In the event of a conflict between the provisions of this Addendum and the Main Agreement, the provisions of the Main Agreement will prevail with regard to the Parties' data protection obligations.

12.2. Section Headings. The section headings contained in this Addendum are for reference purposes only and shall not in any way affect the meaning or interpretation of this Addendum.

12.3. Governing Law. This Addendum shall be governed by the same governing law as that of the Main Agreement.