Your use of the Adventure software service is governed by the terms and conditions of the agreement under which you obtained the services.

For clients who purchase or renew a subscription services from Adventure Res, LLC, your use is governed by the Master Software as a Service agreement ("SAAS") and other documents that the SAAS incorporates. The following are the licensing term exhibits included in the our SAAS.

# Exhibit B – Vendor and Agent Terms of Use

Clients may give access to Vendor Users for the purpose of providing information to allow the Vendor to fulfill the terms of the Client-Vendor agreement. Agent Users may be granted access to the online Agent Portal for the purpose of creating referral bookings.  Vendor and Agent users will be subject to the same terms within the Master SAAS Agreement, Data Processing Agreement (Exhibit D), CCPA Addendum (Exhibit E), Privacy Policy for Client Data (Exhibit G), and Data Security (Exhibit H) as any other Authorized User.

    A. Authorized Vendor and Agent User Conditions to Use. As a condition to access and use of a Platform, (i) each Authorized User shall agree to abide by the terms of Adventure Res' Authorized User Conditions to Use.

    B. Software Restrictions. Vendor or Agent will not, directly or indirectly (i) reverse engineer, decompile, disassemble or otherwise attempt to discover or derive the source code, object code or underlying structure, ideas, know-how or algorithms relevant to a Platform or any software, documentation or data related to a Platform ("Software"); (ii) modify, translate, or create derivative works based on a Platform or any Software; (iii) use a Platform or any Software for timesharing or service bureau purposes or other computer service to a third party; (iv) modify, remove or obstruct any proprietary notices or labels; or (v) use any Software or a Platform in  any manner to assist or take part in the development, marketing or sale of a product potentially competitive with such Software or Platform. Client shall take all reasonable measures to prevent any Authorized User or third party from engaging in or continuing to engage in any of the foregoing activities.  For the avoidance of doubt, Software and the Services, including all user- visible aspects of the Services, are the Confidential Information of Adventure Res, and Client will comply with the Master SAAS Section 5 with respect thereto.

# Exhibit D – Data Processing Agreement

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between Adventure Res LLC., ("Company" or "Data Processor") and  Client ("Data Controller"). Company and Client are sometimes referred to jointly as the "parties" or singularly as a "party."

WHEREAS

1) The Client acts as a Data Controller.
2) The Client wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.
3) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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).

4) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1) **Definitions and Interpretation**
   a) Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:
   b) "Contracted Processor" means a Subprocessor;
   c) "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
   d) "EEA" means the European Economic Area;
   e) "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
   f) "GDPR" means EU General Data Protection Regulation 2016/679, as amended, replaced or superseded from time to time;
   g) "Data Transfer" means:
       (i) a transfer of Guest's Personal Data from the Company to a Contracted Processor; or
       (ii) an onward transfer of Guest's Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);
   i) "Guest's Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Client pursuant to or in connection with the Principal Agreement;
   j) "Services" means the services the Company provides.
   k) "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.
   l) The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2) **Processing of Company Personal Data**
   a) Processor shall:
       i) comply with all applicable Data Protection Laws in the Processing of Guest's Personal Data; and
       ii) not Process Guest's Personal Data other than on the relevant Company's documented instructions.
   b) The Company instructs Processor to process Guest's Personal Data solely in accordance with this Agreement and the Principal Agreement.
   c) Processor will ensure that Sub-Processors only Process Personal Data for the sole and exclusive purpose of providing the Services to Company. Processor will not sell Personal Data and will ensure that Sub-Processors do not sell Personal Data. Processor will indemnify and hold Company harmless from and against any and all claims, damages, losses, and liabilities arising from: (i) any violation of this Agreement by Processor or its employees, Subprocessors, or agents; (ii) any action by Processor or its employees, Subprocessors, or agents in violation of

applicable Data Protection Laws; or (iii) any Personal Data Breach.

3) **Processor Personnel**
Processor shall ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Guest's Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Guest's Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4) **Security**
   a) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Guest's Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
   b) In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5) **Subprocessing**
   a) Processor shall not appoint (or disclose any Guest's Personal Data to) any Subprocessor unless required or authorized by the Company.

6) **Data Subject Rights**
   a) Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
   b) **Processor shall:**
      i) promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Guest's Personal Data; and
      ii) ensure that it does not respond to that request except on the documented instructions of Company or as required by applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7) **Personal Data Breach**
   a) Processor shall notify Company without undue delay, and in any event within 24 hours, upon Processor becoming aware of a Personal Data Breach affecting Guest's Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

   b) Processor shall cooperate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach, all at Processor's sole expense. Such remediation may include, without limitation the provision of notice concerning such occurrence to any person affected or potentially affected thereby and applicable domestic and international authorities.

8) **Data Protection Impact Assessment and Prior Consultation**
   a) Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Guest's Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9) **Deletion or Return of Company Personal Data**
   a) Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Guest's Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Guest's Personal Data.

10) **Audit Rights**
   a) Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Guest's Personal Data by the Contracted Processors.
   b) Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11) **Data Transfer**
   a) The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12) **General Terms**
   a) Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:
      i) disclosure is required by law;
      ii) the relevant information is already in the public domain.

13) **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

14) **Governing Law and Jurisdiction**

   a) This Agreement is governed by the laws of West Virginia.
   b) Any dispute arising in connection with this Agreement, which the Parties will not be able to

resolve amicably, will be submitted to the exclusive jurisdiction of the courts of West Virginia.

# Exhibit E - CCPA Service Provider
# Addendum

Adventure Res has entered into one or more agreements with the Client or one of its subsidiaries or affiliates (as applicable, "Client" under which Service Provider Company has agreed to provide services to the Client (as amended from time to time, the "Agreement"). This CCPA Service Provider Addendum (the "Addendum") forms part of the Agreement and will take effect on the service effective date of the Master SAAS.

Adventure Res and Client agree as follows:

1) **Definitions.** For purposes of this Addendum, the terms below shall have the meanings set forth below. Capitalized terms used but not otherwise defined in this Addendum have the meanings set forth in the Agreement.
   a) "CCPA" means the California Consumer Privacy Act of 2018.
   b) "Client Personal Information" means any "personal information" (as defined in the CCPA) contained within the data or set of data that the Service Provider Company "processes" (as defined in the CCPA) on behalf of Client in connection with performing Services under the Agreement.
   c) "Services" means the services and/or products provided by Service Provider Company to the Client under the Agreement, including activities that are required, usual, or appropriate in performing the Services, including to (a) carry out the Services or the business of which the Services are a part, (b) carry out the benefits, rights and obligations relating to the Services,
   (c) maintain records relating to the Services, or (d) comply with any legal or self-regulatory obligations relating to the Services.

2) **Service Provider Company Obligations.**
   a) To the extent that Service Provider Company processes the Client's Personal Information for a Business Purpose (as defined in the CCPA) under the Agreement, Service Provider Company is a "service provider" (as defined in the CCPA) and shall process the Client's Personal Information solely to provide its Services under the Agreement.
   b) Service Provider Company shall not retain, use, disclose or otherwise process Client's Personal Information for any purpose other than for performing the Services, or as otherwise permitted by the CCPA and shall return or delete all the Client's Personal Information at the conclusion of performance of the Services, or sooner if directed by the Client. Service Provider Company shall follow all Client instructions regarding the return or destruction of the Client's Personal Information.
   c) Service Provider Company shall not "sell" (as defined in the CCPA) any of the Client's Personal Information.
   d) Service Provider Company shall assist the Client in fulfilling its obligations under the CCPA to respond to individual requests related to Client's Personal Information about them, including by promptly fulfilling requests to access or delete relevant Personal Information in Service Provider Company's possession. If Service Provider Company receives a request to know or a request to delete from a consumer regarding Personal Information that the

Service Provider collects, maintains, or sells on behalf of the Client, and does not comply with the request, it shall explain the basis for the denial. The Service Provider Company shall also inform the consumer that it should submit the request directly to Client and, when feasible, provide the consumer with contact information for the Client.

 **e)** Service Provider Company shall enter into written agreements with each third party subcontractor that processes the Client's Personal Information that obligate the subcontractor to comply with terms that are at least as restrictive as those imposed on Service Provider Company under this Addendum and the Agreement, including the prohibition on the sale of the Client's Personal Information.

 **f)** Service Provider Company hereby certifies that it understands its obligations under this Addendum, and shall comply with them.

3) **No Consideration.** Notwithstanding anything in the Agreement or any order or Statement of Work entered into in connection therewith, Service Provider Company's access to the Client's Personal Information is not part of the consideration exchanged by the parties in respect of the Agreement.

4) **Duration of Addendum.** Notwithstanding the expiration of the Term of the Agreement, this Addendum will remain in effect until, and automatically expire upon, Service Provider Company's deletion or return to Client all the Client's Personal Information.

5) **Conflicts.** In the event of any conflict or inconsistency between this Addendum and the terms of the Agreement, this Addendum will control, notwithstanding any statement to the contrary in the Agreement.

# Exhibit F – Subprocessors

Adventure Res may allow third party integrators ("Integrators") to create applications and/or tools that supplement or enhance the Services (the "Integrations"). If you choose to access any such Integrations, the Integrators will access (via API) and use information you provide solely for the purpose of supplementing or enhancing the Services through the Integrations.

Adventure Res makes no warranty that Integrators will have uninterrupted service.

- Authorize.net – One of the credit card processing gateways.
- Google Analytics – We provide the ability for you to use Google Analytics for your online booking system. We also provide a series of points for the Google Tag Manager data layer.
- NMI – One of the credit card processing gateways.
- OneTrust – Adventure Res manages it use of cookies through OneTrust. Some cookies are usually only set in response to actions made by the guest which amount to a request for services, such as setting privacy preferences, logging in, or filling in forms.
- SendGrid – Some Adventure Res clients use SendGrid for transactional email processing.
- Twilio - Some Adventure Res clients use Twilio for transactional SMS processing.
- USPS – Adventure Res allows for a data correction service within the software through a USPS integration.

# EXHIBIT H – Data Security

1) **Data Breach Procedures**. Adventure Res maintains a data breach plan in accordance with the criteria set forth in Exhibit D and shall implement the procedures required under such data breach plan on the occurrence of a data breach (as defined in such plan). For the avoidance of

doubt, the data breach provisions set forth in Exhibit D are not specific to the EU or to GDPR compliance, and will apply to the Services in all cases and in all jurisdictions.

2) **Redundancy, Data Backup, and Disaster Recovery**.  Adventure Res shall maintain or cause to be maintained disaster avoidance procedures designed to safeguard the Client Data and Client's other Confidential Information, Adventure Res' Processing capability, and the availability of the Services, in each case throughout the Term and at all times in connection with its actual or required performance of the Services hereunder. Adventure Res may, from time to time, host and/or maintain a Platform using a third-party technology service provider and Client acknowledges that Adventure Res cannot offer any additional or modified procedures other than those put in place by such technology provider with respect to such technology service.

3) **Redundant Hosting and Connectivity.**

   a) **For clients who are hosted by Adventure Res:** Adventure Res shall simultaneously operate a mirror system at a hardened data center facility remote from the primary system on which the Services are hosted (the "Secondary Backup Facility"). Except for its location and housing facility, the mirror system shall: (a) be identical in all respects to the primary system; (b) have hardware and software, network connectivity, power supplies, backup generators, and other similar equipment and services that operate independently of the primary system; (c) have fully current backups of all Client Data stored on the primary system; and (d) have the ability to provide the Services in accordance with this Agreement and the Specifications during the performance of routine and remedial maintenance or any outage or failure of the primary system. Adventure Res shall operate, monitor, and maintain such mirror system so that it may be activated within [24 hours] of any failure of the Subscription Services to be Available.
   b) **For clients who host their own instance of Adventure Res on their own servers:** Client is responsible for network security, IT infrastructure, and all costs associated with hosting their own system.

4) **Data Backup**.
   a) **For both clients hosted by Adventure Res and for clients who host their own instance of Adventure Res on their own servers:** Adventure Res shall conduct or have conducted [daily] backups of Client Data and perform or cause to be performed periodic backups of Client Data and store such backup Client Data in a commercially reasonable location and manner. On written notice from Client and, in any case, on a quarterly basis, Adventure Res shall provide Client with a copy of the backed-up Client Data in such machine-readable format or as Client otherwise reasonably requests. Client shall reimburse Adventure Res for all media costs and shipping charges reasonably incurred in fulfilling Client's additional requests for copies of backed up Client Data.