Headset Customer Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of, and is subject to, the written or electronic terms of service or subscription agreement(s) and order(s) between **Headset** and **Customer** for Customer's purchase of Services from Headset that reference this DPA (the "**Agreement**"). This DPA shall be effective on the effective date of the Agreement ("**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions.

"**Affiliate**" has the meaning set forth in the Agreement.

"**California Consumer Privacy Act**" or "**CCPA**" means the California Consumer Privacy Act of 2018, upon the effective date thereof and as may be amended from time to time.

"**Customer Personal Data**" means any data which (i) qualifies as "Personal Data" "Personal Information" "Personally Identifiable Information" or any substantially similar term under Data Protection Laws and (ii) is processed on behalf of Customer by Headset under the Agreement.

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data, also known as a "Business" under the CCPA.

"**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller, also known as a "Service Provider" under the CCPA.

"**Data Protection Laws**" means all data protection and privacy laws applicable Processing of Customer Personal Data by Headset under this DPA, including, where applicable, the CCPA.

"**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

"**Data Subject Request**" means a request from a Data Subject that identifies Customer and seeks to exercise the Data Subject's right to access, rectify, erase, transfer or port Customer Personal Data, or to restrict the processing of Customer Personal Data.

"**Services**" means the services provided by Headset to Customer pursuant to the Agreement.

"**Purposes**" shall mean (i) Headset's provision of the Services in accordance with the Agreement, including processing initiated by Authorized Users in their use of the Services, and (ii) further documented, reasonable instructions from Customer.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data.

"**Sub-processor**" means any third-party Data Processor engaged by Headset or its Affiliates to Process Customer Personal Data.

2. Scope and Applicability of this DPA. This DPA applies where and only to the extent that Headset Processes Customer Personal Data on behalf of Customer as a Data Processor in the course of providing the Services.

3. Roles and Scope of Processing.

3.1 **Role of the Parties**. As between Headset and Customer, Customer is either the Data Controller of Customer Personal Data, or if Customer is acting on behalf of a third-party Data Controller, then a Data Processor, and Headset shall Process Customer

Personal Data only as a Data Processor acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined therein.

3.2 **Customer Instructions**. Customer instructs Headset to process, including, if applicable, transfer internationally, Customer Personal Data for the Purposes and in accordance with this DPA and Data Protection Laws. Headset shall not retain, use or disclose the Customer Personal Data for any purpose other than the Purposes or as otherwise expressly permitted by Customer or Data Protection Laws. The parties agree that the Agreement (including this DPA) sets out Customer's complete and final instructions to Headset for the Processing of Customer Personal Data. Any processing outside the scope of these instructions will require prior written agreement between Customer and Headset.

3.3 **Customer Processing of Personal Data**. Customer represents, warrants and covenants that it (including, as applicable its personnel and affiliates): (i) will comply with Data Protection Laws with respect to its processing of Customer Personal Data; (ii) will make appropriate use of the Services to ensure a level of security appropriate to the particular content of the Customer Personal Data, such as pseudonymizing or backing up Customer Personal Data; (iii) it is and it will remain will remain duly and effectively authorized to give the instructions set out in the Agreement, this DPA or as Customer otherwise provides; and (iv) has obtained and will continue to obtain all consents, permissions and rights necessary under Data Protection Laws for Headset to lawfully process Customer Personal Data for the Purposes.

3.4 **Details of Data Processing.**

(a) Subject matter: The subject matter of the processing under this DPA is the Customer Personal Data.

(b) Duration: Notwithstanding expiry or termination of the Agreement, this DPA will remain in effect until, and will automatically expire upon, deletion of all Customer Personal Data as described in this DPA.

(c) Purpose: Headset shall process Customer Personal Data only for the Purposes or as instructed by the Customer in this DPA.

(d) Nature of the Processing: Headset's provision of the Services described in the Agreement.

(e) Categories of Data Subjects: The categories of Data Subjects to which Customer Personal Data relate are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Prospects, customers, business partners and vendors of Customer (who are natural persons);

(ii) Employees or contact persons of Customer's vendors; and/or

(iii) Employees, agents, advisors, freelancers of Customer (who are natural persons).

(f) Types of Personal Data: The types of Customer Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Identification and contact data (name, address, date of birth, gender, contact details); and/or

(ii) Employment details (job title, geographic location, area of responsibility).

4. Sub-processing.

4.1 **Authorized Sub-processors**. Customer specifically authorizes Headset to engage the Sub-processors listed **here** (the "**Sub-processor List**") for the purposes of performing the Services on Headset's behalf.

4.2 **Sub-processor Obligations**. Headset shall enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Customer Personal Data as Headset's obligations in this DPA to the extent applicable to the nature of the services provided by such Sub-processor.

4.3 **Changes to Sub-processors.** Where required by Data Protection Law, Headset shall provide Customer with reasonable prior notice if it intends to make any additions to the list of Subprocessors. Customer may object, in writing, to Headset's appointment of the new Sub-processor within thirty (30) days of receipt of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss Customer's concerns in good faith with a view to achieving resolution. If Customer can reasonably demonstrate that the new Sub-processor is unable to process Customer Personal Data in compliance with the terms of this DPA and Headset cannot provide an alternative Sub-processor, or the parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer, as its sole and exclusive remedy, may terminate the Order Form(s) with respect only to those aspects of the Services which cannot be provided by Headset without the use of the new Sub-processor by providing written notice to Headset. Headset will refund Customer any prepaid unused fees of such Order Form(s) following the effective date of termination with respect to such terminated Services.

5. **International Transfer.** Customer acknowledges and agrees that Headset and its Sub-processors may provide the Services from any state, province, country or other jurisdiction. Headset and its Sub-processors may transfer and process Personal Data anywhere in the world where Headset or its Sub-processors maintain data processing operations. Headset will at all times provide an adequate level of protection for the Personal Data processed, in accordance with the requirements of Data Protection Law**.**

6. **Security.**

6.1 **Security Measures**. Headset shall implement and maintain appropriate technical and organizational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data. Headset provides more information about its standard security practices in the Headset Security Policy found at https://www.Headset.io/company/legal ("**Security Policy**"). Customer is responsible for reviewing the information made available by Headset relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws. Headset may review and update its Security Policy from time to time, provided that any such updates shall not materially diminish the overall security of the Services or Customer Personal Data.

6.2 **Confidentiality of Processing**. Headset shall ensure that any person who is authorized by Headset to process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

7. **Customer Audit Rights.**

7.1 To the extent required by Data Protection Laws and upon written request from Customer:

Headset shall make available to Customer the information in Headset's control which is necessary to demonstrate Customer's compliance with Data Protection Laws.

If the information provided by Headset is insufficient to demonstrate such compliance, then Customer may also send a written request for an audit (including inspection) of the data processing facilities within Headset's control. Following receipt by Headset of such request, Headset and Customer shall mutually agree in advance on the details of the audit, including reasonable start date, scope and duration of, security and confidentiality controls applicable to, any such audit and the third-party who will conduct the audit ("Auditor"). Headset may charge a fee (rates shall be reasonable, taking into account the resources expended by Headset) for any such audit. The reports, audit, and any information arising therefrom shall be Headset's Confidential Information.

7.2 Where the Auditor is a third-party, the Auditor may be required to execute a separate confidentiality agreement with Headset prior to any audit of Headset, and Headset may object in writing to such Auditor, if in Headset's reasonable opinion, the Auditor is not suitably qualified or is a direct competitor of Headset. Any such objection by Headset will require Customer to either appoint another Auditor or conduct the audit itself. Expenses incurred by Auditor in connection with any review of Reports or an audit, shall be borne exclusively by the Auditor.

8. Return or Deletion of Data. Upon Customer request, and to the extent required by the Agreement and Data Protection Laws, Headset shall delete the Customer Personal Data in Headset's possession or control. Headset shall not be required to delete Customer Personal Data to the extent Headset is required by applicable law or order of a governmental or regulatory body to retain some or all of the Customer Personal Data. Where Headset is required to retain Customer Personal Data as set forth in the preceding sentence, then Headset will notify Customer of such requirement, to the extent legally permitted.

9. Security Incident Response.

9.1 **Security Incident Reporting.** If Headset becomes aware of a Security Incident, Headset shall notify Customer without undue delay, and in any case, where feasible, notify Customer within seventy-two (72) hours after confirmation of the Security Incident. Headset shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.2 **Security Incident Communications.** As it comes available, Headset shall provide Customer timely information about the Security Incident, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by Headset to mitigate or contain the Security Incident, the status of Headset's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Headset's communications with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Headset of any fault or liability with respect to the Security Incident.

10. Cooperation.

10.1 **Data Subject Requests.** As the Data Controller, Customer understands that they are ultimately responsible for complying with any Data Subject Request. To the extent legally permitted, if Headset receives a Data Subject Request, Headset shall direct the Data Subject to the Customer in the first instance. In the event Customer is unable to facilitate the Data Subject Request, Headset shall, on Customer's request and at Customer's reasonable expense, address the Data Subject Request, as acquired under the applicable data protection law.

10.2 **Data Protection Impact Assessments.** Headset shall provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

10.3 **Government Inquiries.** If compelled to disclose Customer Personal Data to a law enforcement or governmental entity, then Headset will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Headset is legally permitted to do so.

11. Relationship with the Agreement.

11.1 The parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment or exhibit that the parties may have previously entered in connection with the Services.

11.2 Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the processing of Customer Personal Data.

11.3 Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of Headset and Headset's Affiliates shall be subject to any exclusions on damages and aggregate limitations on liability set out in the Agreement. Without limiting Headset's obligations under the Agreement, each Customer agrees that any regulatory penalties incurred by Headset in relation to the Customer Personal Data that arise as a result of, or in connection with, Headset's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Headset's liability under the Agreement as if it were liability to Customer under the Agreement.

11.4 In no event shall this DPA or any party restrict or limit the rights of any Data Subject or of any competent supervisory authority.

11.5 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.