DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("DPA") forms part of, and is subject to, the Master Subscription Agreement, or other written or electronic terms of service or subscription agreement entered between the parties listed on the Order Form.

This DPA is entered into as of the date of latest signature of the Order Form (the "Effective Date") by Jitterbit Inc., or any of its Affiliates (including Wevo Tecnologia S.A. "Wevo") as set forth in an Order Form, a Delaware corporation with principal offices at 1101 Marina Village Parkway, Suite 201, Alameda, CA 94501 ("Jitterbit") and the Company described in the Order Form ("Customer"). When Wevo is listed in the Order Form, this DPA is between Customer and Wevo Tecnologia S.A, an Affiliate of Jitterbit Inc.

RECITAL

Customer and Jitterbit are parties to an existing Master Subscription Agreement, terms of service or other written agreement under which Jitterbit provides various services and processes personal data on behalf of Customer (the "Agreement"). The parties wish to set out their roles and responsibilities in respect of personal data processed under the Agreement, pursuant to the below General Terms and Conditions, which will supplement the Agreement with respect to the subject matter of this Data Processing Addendum. For the mutual promises exchanged herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree the following.

1. GENERAL TERMS AND CONDITIONS

1.1 Definitions and Interpretation For the purposes of this Data Processing Addendum the following terms have the following meanings:

1. "Agreement" has the meaning given to it in the Recital.
2. "Customer Data" has the meaning set forth in the Agreement.
3. "Customer Personal Data" means any Customer Data that is Personal Data, and may include CA Personal Data as defined in section 6.2(2) below.
4. "Data Authority" (or "Authority")" means the local government agency responsible for Data Protection Laws implementation in the jurisdiction.

5. “Data Protection Laws” means all applicable data protection, privacy and electronic marketing legislation.
6. “Jitterbit Platform” means the Jitterbit Platform hosted by Jitterbit, according to the definitions set forth in the MSA.
7. “Personal Data” means any personal data processed via the Jitterbit Platform on behalf of Customer pursuant to the Agreement.
8. “Sub-Processor” means any processor appointed by Jitterbit to assist with Jitterbit's processing of Customer Personal Data.
9. “Third Party Applications” has the meaning set forth in the Agreement.

For the purposes of this DPA the terms controller, data subject, personal data, process, processing, processor and pseudonymization shall have the meanings attributed to them according to the applicable law of the region where the Agreement is signed. Where Customer and Jitterbit have more than one agreement, references to the Agreement are to all agreements in place between the parties under which Jitterbit processes Customer Personal Data using the Hosted Jitterbit Platform on behalf of Customer.

1.2 Acknowledgement of Roles The parties acknowledge Jitterbit is the processor with respect to Personal Data.

1.3 Data Processing Obligations Jitterbit shall process Customer Personal Data only as necessary to fulfill its obligations under the Agreement, to maintain and administer the Jitterbit Platform, or in accordance with Customer's express written instructions documented in this DPA or the Agreement and via Customer’s use of the Jitterbit Platform, hosted services, other services as described in an order form, and related support and professional services provided by Jitterbit (the “Services”). Jitterbit will not process Customer Personal Data for any other purposes. Jitterbit will require any person who is authorized by Jitterbit to process Customer Personal Data to be under an appropriate obligation of confidentiality, whether such obligation arises contractually or pursuant to statutory duty.

2. SUB-PROCESSORS AND SECURITY

2.1 Sub-Processors

1. Customer agrees Jitterbit may engage Sub-processors in the course of its obligations under the Agreement, to process Customer Personal Data on Customer's behalf.
2. The current list of Jitterbit Sub-Processors is defined in Annex III.
3. Jitterbit shall have a written agreement with each Sub-Processor with terms comparably protective of Customer Personal Data as the applicable terms of this Clause 2.
4. Jitterbit will be responsible for the acts and omissions of its Sub-Processors.
5. Jitterbit will notify Customer designated administrator users via email if it adds or removes Sub-processors at least (30) days' prior to allowing such Sub-processor to process Customer Personal Data.
6. Customer may object in writing to Jitterbit's appointment of a new Sub-processor within fifteen (15) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection.
7. In such event, the parties will discuss the matter in good faith with a view to achieving resolution.
8. If Jitterbit cannot provide an alternative Sub-processor for a Sub-processor who either works in conjunction with Jitterbit to provide Services, or provides Jitterbit cloud infrastructure, and is unable to deliver the Services without either the new Sub-Processor, or an alternative Sub-processor, Customer, as its sole and exclusive remedy, may elect to terminate any current order form by providing Jitterbit 30-days written notice .

2.2 Security and Technical Measures Jitterbit will maintain appropriate technical and organizational measures to safeguard Customer Personal Data processed by the Hosted Jitterbit Platform ("Security Measures"). Such Security Measures are specified in the Security Measures referenced in Annex II. They include where appropriate and if possible:

1. The pseudonymization and encryption of Customer Personal Data.
2. Requiring that all individuals, parties, employees, or other entities with access to Customer Personal Data are bound by industry standard confidentiality obligations.
3. The ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident.
4. A process to regularly evaluate the effectiveness of the Security Measures.

Jitterbit will notify Customer without undue delay (and in any event within 72 hours) upon confirming a Security Incident involving Customer Personal Data processed by the Jitterbit

Platform. Jitterbit will promptly provide reasonable assistance to Customer to comply with any lawful request from Customer requiring Jitterbit to access, amend, transfer or delete Customer Personal Data in accord with its obligations under applicable Data Protection Laws.

3. CUSTOMER OBLIGATIONS

3.1 Processing of Personal Data. Customer agrees (i) it will comply with its obligations under Data Protection Laws in respect of its processing of Personal Data, including any obligations specific to its role as a Data Controller, and any processing instructions it issues to Jitterbit. It has provided notice and obtained or will obtain all consents and rights necessary under Data Protection Laws from any individuals or entities whose information is included in the Customer Data for Jitterbit to process Personal Data and provide the Services pursuant to the Agreement and this DPA. If Customer is itself a Data Processor, Customer warrants to Jitterbit that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Jitterbit as another Data Processor, have been authorized by the relevant Data Controller to the extent required under applicable law.

3.2 Platform Usage and Security

1. Customer is responsible for its use of the Jitterbit Platform, including making appropriate use of the Jitterbit Platform to ensure a level of security appropriate to the risk in respect of the Customer Personal Data, securing its account authentication credentials, managing its data back-up strategies, and protecting the security of Customer Personal Data when in transit to and from the Jitterbit Platform and taking any appropriate steps to securely encrypt or backup any Customer Personal Data uploaded to the Jitterbit Platform.
2. Customer will utilize any self help features available in the Jitterbit Platform to access the Customer Personal Data.
3. Jitterbit has no obligation to protect Customer Personal Data Customer elects to store or transfer outside of Jitterbit and its Sub-Processors' systems, for example, offline or on-premises storage.
4. Customer acknowledges and agrees that Jitterbit will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements.

5. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to a Security Incident.

4. AUDITS AND REVIEWS

Customer acknowledges and agrees that Jitterbit is regularly audited by independent third-party auditors and/or internal auditors with respect to its security policy. Jitterbit shall keep reasonably detailed, accurate and up-to-date records, documents and/ or electronic data relating to the processing of Customer Personal Data by Jitterbit and to the measures taken by Jitterbit. All copies of such Records (including any Reports, as defined below) are Jitterbit's Confidential Information under the Agreement.

Jitterbit shall permit Customer and its third-party representatives, on reasonable prior written notice, no more than once annually, to receive electronic copies of the audit information in the form of summary reports, audit sheets or table of contents ("Report(s)") that provides reasonable information on Jitterbit's compliance with its security policies within the scope of the audit without compromising Jitterbit's security. Customer may remotely review all Records related to the processing of Customer Personal Data by Jitterbit for assessing Jitterbit's compliance with its obligations under this DPA. Such review rights may be exercised only once in any calendar year during the Term. Customer shall conduct any such review in a prompt manner so as not to interfere in Jitterbit business operations.

Customer shall first review Jitterbit's most recent third-party audit summary report. Only if Customer reasonably demonstrates that such report does not contain information necessary to verify compliance, or following a confirmed Security Incident, may Customer (at its sole cost, under customary non-disclosure agreements, during standard business hours, and upon at least 30 days' advance written notice) conduct a remote security audit , provided such audit does not disrupt business operations or compromise multi-tenant systems. Customer shall be responsible for all costs incurred by Customer and Jitterbit's reasonable billable expenses (at Jitterbit's then-current professional services rates) associated with assisting Customer in any audit.

5. ARTIFICIAL INTELLIGENCE (AI) AGENTS

5.1 Disclaimer of Liability for AI Integrations

Customer may utilize the Jitterbit Platform to build integrations that connect with or utilize artificial intelligence agents ("AI Agents"). Customer acknowledges and agrees that Jitterbit acts solely as the technical integration layer connecting these endpoints. Jitterbit does not control, monitor, govern, or train these AI Agents. Jitterbit explicitly disclaims any and all liability for the outputs, actions, or data processing behaviors of AI Agents utilized by the Customer. This includes, but is not limited to, liability for AI "hallucinations," biased outputs, API overages, unauthorized autonomous data transfers, or data exfiltration initiated by the AI Agent's behavior. Customer remains solely responsible for ensuring that its configuration and use of AI Agents complies with all applicable Data Protection Laws, security standards, and its own internal data governance policies.

6. REGION-SPECIFIC DATA PROTECTION TERMS

6.1 United Kingdom and European Union (GDPR) Requirements

This section applies when Customer Personal Data is subject to UK and/or EU Data Protection Laws.

1. **Definitions:** For the UK: the UK GDPR and the Data Protection Act 2018. “UK GDPR” has the meaning as defined in section 3 of the Data Protection Act 2018.
   For the EU: Any applicable national legislation implementing Regulation (EU) 2016/679 (and any related national legislation).
2. **Designated Data Protection Officer:** “Designated Data Protection Officer” or “DDPO” shall mean an authorized representative of Jitterbit with sufficient awareness of Jitterbit's processing of Personal Data. The Jitterbit DPO will act as a point of contact for Customer and have as part of his/her responsibilities the obligation to respond to Customer queries on Jitterbit's processing of Personal Data. The contact details of the Jitterbit DPO are available at: https://www.jitterbit.com/privacy-policy.
3. **Data Impact Assessment:** In the event that Customer reasonably determines that any processing activity related to Jitterbit's processing of Customer Personal Data is likely to result in high risk to the rights and freedoms of a data subject, Jitterbit shall reasonably cooperate, at Customer’s expense, in Customer’s conducting a data protection impact

assessment of such processing activity, with such impact assessment to be conducted in a manner so as not to interfere with Jitterbit business operations.

4. **Records:** Jitterbit will maintain all appropriate records of processing carried out in respect of Customer Personal Data in accordance with GDPR.
5. **Model Clauses and Transfers:** "Model Clauses" means the current applicable version of the Standard Contractual Clauses for Controller to Processor or Processor to Processor, as approved by the European Commission, as incorporated herein (Annex IV). For Customers in the UK, "Model Clauses" means the Controller to Processor or Processor to Processor clauses approved by the UK Information Commissioner's Office. In the event that both EU and UK SCCs will apply, the UK EU Addendum shall apply and be incorporated herein. Customer authorizes the transfer of the personal data to Jitterbit and sub-processors located outside the EEA where such transfer is required in connection with the provision of Services and/or is necessary in the normal course of business. The parties agree to rely on the Model Clauses to provide adequate protection for any Customer Personal Data in accordance with Annex IV as attached to this DPA.

6.2 United States (CCPA/CPRA) Requirements

This section applies when Customer Personal Data is subject to US and California privacy laws.

1. **Definitions:** When in the US: the California Consumer Privacy Act of 2018 ("CCPA"), California Privacy Rights Act of 2020, any implementing regulations ("CA Law"),.
2. **Processing Restrictions:** Jitterbit may not share, retain, sell, use or disclose Customer Data that contains "Personal Information" as that term is defined under the California Consumer Privacy Act of 2018 ("CCPA") (referred to hereafter as "CA Personal Data") for any purpose other than for performing the Services in accordance with Customer instructions and its rights or its obligations as a Service Provider under CA Law, the Agreement and this DPA (the "Purpose"). Jitterbit will not combine CA Personal Data from different sources. Jitterbit acknowledges that it is a Service Provider under the CCPA/CPRA and will comply with all restrictions and obligations placed on a Service Provider under the CCPA/CPRA.
3. **Service Providers:** Notwithstanding the foregoing, Customer agrees that Jitterbit may engage other "Service Providers" as provided for under CA Law to assist in performing its obligations to Customer hereunder, in accordance with CA Law, subject to written

terms comparably protective of the CA Personal Data as this section and the procedures for Sub-Processors under Section 2.1 above.

4. **Data Retention and Destruction:** Jitterbit will retain CA Personal Data only for as long as reasonably necessary for the Purpose, or as required by applicable laws. Upon termination of the Agreement, or upon Customer's written request, if earlier, Jitterbit will destroy CA Personal Data pursuant to the Agreement, unless legal obligations require Jitterbit to store CA Personal Data.
5. **Consumer Requests:** If Jitterbit, directly or indirectly, receives a request submitted by a Consumer (as defined under the CCPA) to exercise a right it has under the CCPA in relation to the Consumer's CA Personal Data, Jitterbit will provide a copy of the request to Customer. Customer will be responsible for handling and communicating with the Consumer regarding any such requests. Jitterbit will notify Customer in the event it makes a determination that it can no longer meet its obligations under CA Law.

6.3 Latin America (LGPD) Requirements

This section applies when Customer Personal Data is subject to Brazilian and Latin American privacy laws.

1. **Definitions:** When in Latin America: the General Data Protection Law, number 13.709/18 (LGPD) from Brazil. CD/ANPD Resolution No. 19/2024
2. The Processor shall process Personal Data exclusively in accordance with the documented instructions of the Controller, including with regard to transfers of Personal Data to third countries or international organizations, unless required to do so by applicable Brazilian law, specifically the General Data Protection Law (LGPD - Law No. 13.709/2018). In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
3. The Processor shall implement and maintain technical, administrative, and organizational measures appropriate to the risk to ensure a level of security of the Personal Data, protecting it against unauthorized access, destruction, loss, alteration, communication, or any form of improper or unlawful processing. Furthermore, the Processor ensures that persons authorized to process the Personal Data (including employees and contractors) have committed themselves to confidentiality through

legally binding agreements or are under an appropriate statutory obligation of confidentiality.

4. In the event of a confirmed Security Incident involving the Controller's Personal Data, the Processor shall notify the Controller without undue delay, after becoming aware of the incident. The notification shall include, to the extent possible: (a) a description of the nature of the incident; (b) the categories and approximate number of Data Subjects affected; (c) the likely consequences; and (d) the measures taken or proposed to mitigate the effects. The Processor shall fully cooperate with the Controller in investigating the incident and assisting with any required notifications to the Regulatory Agency of the jurisdiction.
5. If a Data Subject makes a direct request to the Processor, the Processor shall promptly forward such request to the Controller and shall not respond directly unless explicitly authorized by the Controller.
6. Upon termination of the provision of processing services, the Processor shall, at the choice of the Controller, securely delete or return all Personal Data to the Controller, if such return is possible. The Processor shall delete existing copies, provided that such deletion occurs in accordance with the retention schedule in Annex I and upon Customer's written request confirm that it has done so, unless the retention of the Personal Data is expressly required by Brazilian law or regulatory obligation, in which case the Processor shall isolate and protect such data from any further processing.

7. TERM, TERMINATION AND GENERAL PROVISIONS

7.1 Term and Termination This DPA shall remain in effect until the termination of the Agreement. If Jitterbit processes Customer Personal Data under one or more agreements in addition to the Agreement, this DPA shall terminate upon expiry of the last agreement between the parties to expire or terminate.

7.2 General

1. **Survival:** According to the applicable law, all clauses that are required shall survive the termination or expiration of this DPA.
2. **Superseding Effect:** The parties agree that this DPA shall replace and supersede any existing data processing agreement, addendum, attachment, or exhibit (including the

Model Clauses (as applicable) that the parties may have previously entered into in connection with the Services or the Agreement. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect.

3. **Conflict of Terms:** 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, including CA Personal Data. In the event of any conflict between the terms of this DPA and any provision of the Agreement, this DPA shall take precedence.
4. **Liability:** Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's Affiliates under this DPA shall be subject to the limitations on liability set out in the Agreement.
5. **Choice of Law:** Except as provided in Annex IV, the choice of law and jurisdiction shall be pursuant to the Agreement.

ANNEX I: DESCRIPTION OF DATA PROCESSING

A. LIST OF PARTIES

Data Exporter:

1. The Customer which has signed the Agreement.
2. Role (controller/processor): controller
3. Activities relevant to the data transferred under these Clauses: relate to exporters use of the Jitterbit Platform. The data exporter may transfer encrypted personal data pertaining to its customers ("Customer Personal Data") contained in "Customer Data", between Customer selected Endpoints in Third Party Applications. The data exporter may share employee and contractor business contact information ("Business Contact Information") with the data importer as necessary for the data importer and its subcontractors to administer the Agreement.

Data Importer:

1. The Jitterbit Entity which has signed the Agreement.
2. Email: dpo@jitterbit.com
3. Activities: Data importer is providing the services described in the Agreement. The data importer and its sub-processors host certain components of the Jitterbit Platform or Services used by the data exporter to transfer Customer Personal Data. The data importer has no knowledge of the content of the Customer Personal Data data exporter elects to transfer.

B. DESCRIPTION OF TRANSFER

1. **Categories of data subjects whose personal data is transferred:** Customer Personal Data: customers of data exporter whose data resides in one Third Party Application and which data exporter desires to transfer to another Third Party Application via the hosted Jitterbit Platform, or hosted Services. Business Contact Information: employees and contractors acting on behalf of data exporter.

2. **Categories of personal data transferred:** Customer Personal Data: any personal data that data exporter elects to transfer as between Third Party Applications. Business Contact Information: name, business title, business telephone number, business fax number, business email address, business office address, username and password to the Jitterbit Platform, in each case, belonging to the data exporter's employees or contractors.
3. **The frequency of the transfer:** Continuous.
4. **Nature of the processing:** Customer Data is processed via the hosted Jitterbit Platform in order to provide the services as described in the Agreement.
5. **The period for which the personal data will be retained:** For Jitterbit Platform: Customer Personal Data is retained for the performance of Jitterbit obligations under the Agreement and is deleted 90 days after the Agreement has expired or been terminated. For EBridge Services: Pursuant to EBridge retention policy.

ANNEX II: TECHNICAL AND ORGANISATIONAL MEASURES

1. **For Jitterbit Platform:** Jitterbit maintains the technical and organizational security measures described in the Agreement, and at https://www.jitterbit.com/security-annex-b.
2. **Sub-processors security measures:**
    - Amazon security measures are described at https://aws.amazon.com/security/
    - Pendo: https://trust.pendo.io/controls
    - Saxonica: https://www.saxonica.com/about/gdpr.xml
    - Tenable: https://www.tenable.com/trust-and-assurance
    - Elastic: https://www.elastic.co/trust
    - Microsoft Corporation: [https://azure.microsoft.com/en-us/overview/security/]
    - OpenText: [https://www.opentext.com/about/copyright-information/site-privacy]

ANNEX III: LIST OF SUB-PROCESSORS

Jitterbit Harmony Platform List of Sub-Processors

Subprocessor	Location Country	Website	Purpose
Tenable	US	tenable.com	Network security
Amazon Web Services (AWS)	Global	aws.amazon.com	Cloud hosting provider
Microsoft Azure	Global	azure.microsoft.com	Cloud hosting provider
Pendo	US	pendo.io	User behavior analytics & feedback
Saxonica	UK	saxonica.com	XML & XSLT data transformation software
Elastic	US / Global	elastic.co	Search, logging, & data analytics engine
OpenText	Canada / Global	opentext.com	Information management & content integration

ANNEX IV: STANDARD CONTRACTUAL CLAUSES

1. **EU Standard Contractual Clauses**. For data transfers from the EEA to locations outside the EEA or the UK, the 2021 EU Standard Contractual Clauses will apply in the following manner. Where the applicable sections of the Standard Contractual Clauses require the data exporter and the data importer to select a module:

    1.1. Module Two of the Standard Contractual Clauses (*Transfer controller to processor*) shall apply where Jitterbit, as data importer, is acting as Customer's Data Processor; and

    1.2. Module Three of the Standard Contractual Clauses (*Transfer processor to processor*) shall apply where Customer is acting as a processor, and Jitterbit, as data importer, is acting as Customer's sub-Data Processor;

    1.3. Clause 7, the optional docking clause will not apply.

    1.4. In Clause 9(a), Option 2 ("General Written Authorisation") will apply. The notification, authorization, and applicable time period will be as set forth in Section 2.1(5) of the DPA.

    1.5. In Clause 17, Option 1 will apply. These Standard Contractual Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The parties agree that this shall be the law of the Netherlands.

    1.6. In Clause 18(b), disputes will be resolved before the courts of the Netherlands.

2. **UK Standard Contractual Clauses.** For data transfers from the United Kingdom, the applicable Model Clauses shall be the UK International Data Transfer Agreement, or the UK International Data Transfer Addendum (altogether, the "UK SCCs") as applicable. For data transfers subject to the UK SCCs, Annex I of this DPA shall apply as Annexes 1A, 1B. of the UK SCCs; and Annex II, and Annex III of this DPA shall apply as Annex II and Annex III of the UK SCCs respectively. For personal data subject to the privacy laws of the UK, references to the GDPR in the Addendum will be deemed to be references to the UK GDPR and Data Protection Act 2018, and, to the extent possible, Modules and optional clauses shall apply as set forth above in Sections 1.1, 1.2 "EU Standard Contractual Clauses."

3. **UK Standard Contractual Clauses- Applicability**. The UK SCCs will apply in the following manner:
   3.1. Table 2:
      3.1.1. Exporter Status: Customer, as exporter is a (*pick one*):
         3.1.1.1. [ ] controller [ ] processor
      3.1.2. Importer Status: Jitterbit, as importer is a (*pick one*):
         3.1.2.1. [ ] processor [ ] sub-processor
   3.2. Table 3, list of Sub-processors: see Annex III
   3.3. Table 4: both the Importer and the exporter may end the UK SCCs in accordance with the terms of the UK SCCs.
   3.4. In the event both the EU Standard Contractual Clauses and the UK SCC's apply, then the UK International Data Transfer Addendum shall apply.
   3.5. Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK SCCs and any other terms in this Addendum, or the Agreement, the provisions of the EU Standard Contractual Clauses or UK SCCs as applicable, will prevail.
   3.6. Jurisdiction. With regard to personal data subject to the data privacy laws of the UK, this Annex IV and the UK SCCs are governed by the laws of England and Wales, and any dispute arising under the UK SCCs will be resolved by the courts of England and Wales.
4. Conflict: To the extent that there is any conflict between the terms of the DPA and the Model Clauses, the relevant term(s) of the applicable Model Clauses will control.

C. BRAZILIAN STANDARD CONTRACTUAL CLAUSES (CD/ANPD RESOLUTION NO. 19/2024)

For transfers of Customer Personal Data subject to the LGPD from Brazil to locations outside Brazil:

1. Applicability: The standard contractual clauses approved by the ANPD pursuant to Resolution CD/ANPD No. 19/2024 ("Brazilian Standard Clauses") are hereby incorporated into this DPA.