DATA PROCESSING ADDENDUM
(Online Version June 25, 2025)

THIS DATA PROCESSING ADDENDUM ("DPA") sets out the parties roles and responsibilities in processing personal data under, forms part of, and is subject to, the Master Subscription Agreement, or other written agreement (the "Agreement") entered between Jitterbit, Inc. and the legal entity referenced as 'Customer' thereunder and is effective as of the date last signed on the Agreement ("Effective Date").

TERMS AND CONDITIONS. The parties hereby agree to the following:

1. **Definitions and Interpretation.**

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

"Customer Data" has the meaning set forth in the Agreement;

"Customer Personal Data" means any Customer Data that is Personal Data;

"Data Authority" (or "Authority")" means the local government agency responsible for Data Protection Laws implementation in the jurisdiction;

"Data Protection Laws" means all applicable data protection, privacy and electronic marketing legislation, including the (1) California Consumer Privacy Act of 2018 ("CCPA"), California Privacy Rights Act of 2020, any implementing regulations (altogether "CA Law"), any (2) applicable national legislation implementing Directive 95/46/EC and Directive 2002/58/EC, GDPR (and any related national legislation), the UK GDPR and the Data Protection Act 2018 ("UK GDPR") and any replacement or repealing legislation, and any regulations issued relating to the same;

"EEA" means the European Economic Area but excluding the UK;

"GDPR" means the Regulation (EU) 2016/679;

"Jitterbit Platform" has the meaning set forth in the Agreement;

"Hosted Jitterbit Platform" means the Jitterbit Platform hosted by Jitterbit;

"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 attached hereto; 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. The "UK EU Addendum" means the UK SCC Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner in accordance with s119A of the Data Protection Act 2018 on 2 February 2022. In the event that only the UK SCCs apply, then the International Data Transfer Agreement shall apply and be incorporated herein.

"Personal Data" means any personal data processed by Jitterbit on behalf of Customer pursuant to the Agreement;

"Sub-Processor" means any processor appointed by Jitterbit to assist with Jitterbit's processing of Customer Personal Data. The Sub-Processor for a particular Jitterbit Service is specified in the Jitterbit Service Annex referenced in Annex I.

"UK GDPR" has the meaning as defined in section 3 of the Data Protection Act 2018.

1.2 For the purposes of this DPA the terms business, business purpose, controller, data subject, personal data, process, processing, processor, pseudonymization, service provider, and sharing shall have meanings attributed to them consistent with applicable Data Protection Laws.

1.3 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. Terms not defined herein shall have the meaning set forth in the Agreement.

2. **Acknowledgement of Roles.** The parties acknowledge Jitterbit is the processor and service provider with respect to Personal Data.

3. **Data Processing Obligations.**

3.1. Customer Instructions. Jitterbit shall process Customer Personal Data only as necessary to fulfill its obligations under the Agreement or in accordance with Customer's express written instructions documented in this DPA, the Agreement and via Customer's use of the Jitterbit Platform, hosted services, other services as described on an order form, and related support and professional services provided by Jitterbit (the " Services"); and will not process Customer Personal Data for any other purposes.

3.2. Obligation of Confidentiality. 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.

3.3. Sub-Processors.

a) 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. The current list of Jitterbit Sub-Processors is attached hereto as Annex III. 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 3. Jitterbit will be responsible for the acts and omissions of its Sub-Processors.

b) Jitterbit will notify Customer designated administrator users via email if it adds or removes Sub-processors at least thirty (30) days' prior to allowing such Sub-processor to process Customer Personal Data.

c) Right to Object. Customer may object in writing to Jitterbit's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss the matter in good faith with a view to achieving resolution. 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 the applicable Agreement including this DPA.

3.4. Jitterbit will provide all reasonable assistance to Customer to enable Customer to comply with its obligations under Data Protection Laws in respect of Customer Personal Data, including assisting Customer in complying with a data subject's rights to access, amend and transfer; and on termination or expiration of the Agreement, unless required sooner in performance of the Services, promptly delete all Customer Personal Data.

3.5. Jitterbit shall not be required to delete Customer Personal Data to the extent (i) Jitterbit is required by applicable law or order of a government/regulatory body to retain some or all the Customer Personal Data; and/or (ii) Customer Personal Data archived on back-up systems, which Customer Personal Data Jitterbit shall securely isolate and protect from any further processing, except to the extent required by applicable law.

3.6. In the event that Jitterbit receives any complaint, notice or communication from either the Authority or a data subject which relates to the processing of Customer Personal Data or to either party's compliance with Data Protection Laws, Jitterbit shall notify Customer without undue delay, and it shall provide Customer and the Authority if applicable with full cooperation and assistance in relation to any such complaint, notice or communication.

3.7. Security Breach. Jitterbit will notify Customer without undue delay upon becoming aware of any unauthorized or unlawful processing, loss of, damage to or destruction of any Customer Personal Data processed by Jitterbit's applications.

3.8. Records. Jitterbit will maintain all appropriate records of processing carried out in respect of Customer Personal Data in accordance with GDPR.

3.9. Jitterbit will notify Customer if it believes a Customer instruction may infringe applicable Data Protection Laws, or if it can no longer meet its obligations hereunder as a result of changes in applicable Data Protection Laws. Jitterbit will

upon request by Customer, provide information demonstrating its compliance with this Clause 3.

3.10. Technical Measures. Jitterbit will take appropriate technical and organizational measures against the unauthorized or unlawful processing of Customer Personal Data, and against the accidental loss or destruction of, or damage to Customer Personal Data while processed by the Hosted Jitterbit Platform ("Security Measures") specified in Annex 2.

3.11. Processing in Accord with Applicable Data Protection Laws. Jitterbit will not share, retain, use or disclose Customer 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 CCPA, the Agreement and this DPA including as described in Annex 1 (the "Purpose"). Jitterbit will not combine Customer Personal Data received from Customer with data it directly receives from consumers or others to the extent prohibited by Data Protection Laws. Notwithstanding the foregoing, Customer agrees that Jitterbit may engage other "Service Providers" to assist in performing its obligations to Customer hereunder, in accordance with Data Protection Laws, subject to written terms comparably protective of the Personal Data as this section and the procedures for Sub-Processors under Section 3.3 above.

3.12. Onward Data Transfers, Model Clauses.

a) 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. To the extent that Jitterbit processes any Customer Personal Data protected by EU Data Protection Laws under the Agreement and/or that originates from the EEA, to a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties agree to rely on the Model Clauses to provide adequate protection for any Customer Personal Data in accordance with Annex IV as referenced in this DPA.

b) UK Standard Contractual Clauses: For Customers in the UK, references to the GDPR in the Addendum will be deemed to be references to the applicable UK regulations (e.g., the UK GDPR and Data Protection Act 2018) and the then current UK Standard Contractual Clauses will apply, in accordance with Annex IV .

c) For onward transfers from Jitterbit to its Sub-processors, Customer consents to such onward transfers provided Jitterbit and relevant sub-processors enter into a written agreement which imposes materially the same obligations on the sub-processors as are imposed on Jitterbit under the Model Clauses.

d) If and as necessary to affect the transfer of Customer Personal Data as directed by Customer or established by Customer API policies and procedures in the Hosted Jitterbit Platform, or to provide the Services, Jitterbit may process, access, direct Customer Personal Data anywhere in the world as indicated by Customer through its use of the Platform.

3.13. 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.

3.14. Jitterbit will not disclose or provide access to Customer Data to any government agency, except as necessary to comply with law, or a valid and binding order of a law enforcement agency, including a subpoena or court order. If a law enforcement agency sends Jitterbit a demand for Customer Data, Jitterbit will attempt to redirect the request to Customer, which may include providing basic Customer contact information. If compelled to disclose Customer Data to a law enforcement agency, Jitterbit will give Customer notice of the demand to permit Customer to seek a protective order or other remedy unless legally prohibited from doing so.

4. **Customer Obligations.**

4.1. Customer 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; and (ii) 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.

4.2. 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.

4.3. 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.

4.4. No Assessment of Customer Data. 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. 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.

4.5. The Customer Data transmitted by Customer's use of the Jitterbit Platform is determined solely by Customer and may include, without limitation, Personal Data. Customer understands and agrees: (a) the provisions in this DPA and the Agreement about processing Personal Data by Jitterbit shall not be construed as requiring Jitterbit to undertake monitoring activities or be responsible for Customer or User initiated actions taken in connection with usage of the Jitterbit Platform, except as required to act on those Customer or User initiated actions in the normal course of providing access to the Jitterbit Platform; and (b) Customer shall, in its use of the Jitterbit Platform, only submit (and ensure that Users submit) instructions to Jitterbit that comply with applicable Data Protection Laws and Regulations.

5. **Data Protection Officer**. 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.

6. **Audit**

Jitterbit shall make available to the Customer all information reasonably necessary to demonstrate compliance with its obligations under this DPA and the Data Protection Laws including Article 28 of the GDPR, and shall allow for and contribute to remote inspections and documentary reviews, conducted by the Customer or another auditor mandated by the Customer (the "Auditor"), subject to the following conditions:

6.1. Customer shall provide Jitterbit with at least sixty (60) days' prior written notice of any intended audit or inspection, specifying the scope, purpose, and proposed methodology (e.g. documentary review, remote interviews) with a finalized audit scope and evidence request list provided in writing at least [thirty (30) days] prior to such audit. Jitterbit shall then propose a reasonable timeline for providing the requested information or interviews ..

6.2. Audits shall be conducted no more than once every twelve (12) months, unless a Personal Data Breach affecting the Customer's data has occurred, or the Customer has a reasonable and demonstrable belief of a material breach of this DPA by Jitterbit, or as required by a competent supervisory authority. Audits shall be conducted, on a non-interference basis, during normal business hours, by Customer. Customer or its third party auditors shall comply with all reasonable security and confidentiality guidelines and other policies of Jitterbit with respect to the remote audit and shall take reasonable measures to prevent unnecessary disruption to Jitterbit 's operations. The length of the audit shall not exceed twenty (20) hours.

6.3. The scope of any audit shall be strictly limited to Jitterbit's data processing activities directly relevant to the

services provided to the Customer under the Master Services Agreement and this DPA. This includes, but is not limited to, Jitterbit's organization and technical measures implemented within its cloud environment and its internal processes for managing and securing data. It shall not extend to other customers' data, Jitterbit's confidential business information unrelated to data processing obligations, or areas already adequately covered by recent third-party certifications or audit reports provided by Jitterbit, as mutually agreed.

6.4. Customer shall ensure that any Auditor appointed is suitably qualified and experienced and is subject to strict confidentiality obligations equivalent to or stronger than those set out in this DPA. Jitterbit reserves the right to object to an Auditor if the Auditor is a direct competitor of Jitterbit or poses a demonstrably significant conflict of interest, provided such objection is reasonable and communicated promptly to the Customer.

6.5. Audits shall be conducted through remote means, including (i) provision of documentation (relevant policies, procedures, security documentation, access logs, and other records upon reasonable request), (ii) video conferencing (remote interviews with relevant personnel (e.g. DPO, security lead, engineers) to discuss data protection practices, security controls, and incident response procedures), (iii) review of third-party certifications and reports (Jitterbit shall provide its most recent relevant certifications (e.g. IS 27001, ISO 27701, SOC 2 Type II reports) pertaining to its information security and privacy management systems, and its cloud environment controls where applicable. The Customer acknowledges that these reports provide independent assurance of Jitterbit's adherence to industry best practices

6.6. The Customer acknowledges and agrees that Jitterbit's obligations concerning the security of Customer Data, including Customer Personal Data processed within the AWS environment are subject to AWS's Shared Responsibility Model, whereby AWS is responsible for the security of the cloud, and Jitterbit is responsible for security in the cloud. Jitterbit's audit obligations hereunder relate to its security in the cloud responsibilities.

6.7. The Customer shall bear all costs associated with any audit.

7. **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.

8. **General.**
   - 8.1. Survival. Sections 3.1, 3.4, 3.5, 6.1 and 8 shall survive the termination or expiration of this DPA.
   - 8.2. 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.
   - 8.3. Except for the changes made 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. Notwithstanding the foregoing, and solely to the extent applicable to any patient, medical or other protected health information regulated by HIPAA or any similar U.S. federal or state laws, rules or regulations ("HIPAA Data"), if there is any conflict between this DPA and a Business Associates Agreement between Customer and Jitterbit ("BAA"), then the BAA shall prevail to extent the conflict relates to such HIPAA Data.
   - 8.4. 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.
   - 8.5. In the event of any conflict between the terms of this DPA and any provision of the Agreement, this DPA shall take precedence.
   - 8.6. A person who is not a party to this DPA may not enforce any of its terms against a party under this DPA.

8.7. Choice of Law, Jurisdiction. Except as provided in the Model Clauses, the choice of law and jurisdiction shall be pursuant to the Agreement.

8.8. This DPA may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

Annex I

DESCRIPTION OF DATA PROCESSING

The description of data processing services provided by Jitterbit relates to the specific features/ services of the Jitterbit Platform Customer has selected, which is reflected in Customer's Order Form, and a processing Annex is incorporated into the DPA by this reference, as applicable.

Jitterbit iPaaS	https://www.jitterbit.com/wp-content/uploads/Annex-I-Description-of-Data-Processing-Jitterbit-iPaaS-rev-11.19.2024.pdf
Jitterbit App Builder	https://www.jitterbit.com/wp-content/uploads/Annex-I-Description-of-Data-Processing-Jitterbit-App-Builder-rev-11.19.2024.pdf
Jitterbit EDI	https://www.jitterbit.com/wp-content/uploads/Annex-I-Description-of-Data-Processing-Jitterbit-EDI-rev-11.19.2024.pdf

Annex II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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.

- *For Jitterbit Platform: Jitterbit maintains the technical and organizational security measures described in the Agreement, and at https://www.jitterbit.com/security-annex-b*

Annex III

Jitterbit Harmony Platform List of Sub-Processors

https://www.jitterbit.com/wp-content/uploads/Annex-III-Jitterbit-List-of-Sub-Procesors-Rev-11.19.2024.pdf

Annex IV

STANDARD CONTRACTUAL CLAUSES

Schedule 1
EU STANDARD CONTRACTUAL CLAUSES
The EU SCCs apply to transfers from EU Countries to non-compliant countries.

SCCs: https://www.jitterbit.com/wp-content/uploads/ADDENDUM-SCCs-short-form-EU-and-UK-rev-03.09.pdf

Schedule 2
UK STANDARD CONTRACTUAL CLAUSES SHORT FORM

The EU Addendum applies to data transfers from the UK to countries where the EU SCCs also apply.

EU Addendum: https://www.jitterbit.com/wp-content/uploads/ADDENDUM-SCCs-short-form-EU-and-UK-rev-03.09.pdf

Schedule 3
UK STANDARD CONTRACTUAL CLAUSES IDTA

The International Data Transfer Agreement ("IDTA") applies only where Customer is transferring from UK to a non-compliant country, but the EU SCCs do not apply.

IDTA: Parts 1-3 https://www.jitterbit.com/wp-content/uploads/International-Data-Transfer-Agreement-IDTA-for-the-UK-Parts-1-3-rev-11.13.2024.pdf

IDTA: Part 4, UK Mandatory Clauses https://www.jitterbit.com/wp-content/uploads/IDTA-Part-4-Mandatory-Clauses-rev-10.18.2024.pdf