

DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) amends and forms part of the written agreement between **Customer** and Momentum Labs, Inc. (“**Momentum**”) (collectively, “**the parties**”) for the provision of services to Customer (the “**Agreement**”). This DPA prevails over any conflicting term of the Agreement but does not otherwise modify the Agreement.

1. Definitions

1.1. In this DPA:

- a) “**Controller**”, “**Data Subject**”, “**Processing**” (related terms such as “Process” and “Processed” shall have corresponding meanings), “**Processor**”, “**Service Provider**”, “**Supervisory Authority**”, and “**Third Party**” have the meaning given to them in Data Protection Law (as defined below);
- b) “**Customer Data**” means what is defined in the Agreement as “Customer Data”;
- c) “**Data Protection Law**” means the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”) and all other Data Protection Laws of the European Union, the European Economic Area (“**EEA**”), and their respective Member States, Switzerland and the United Kingdom (“**UK**”); (ii) certain U.S. federal and state privacy laws, including the California Consumer Privacy Act as amended by the California Privacy Rights Act (California Civil Code § 1798.100) (“**CCPA**”); and (iii) all laws implementing or supplementing the foregoing;
- d) “**Data Subject Rights**” means all rights granted to Data Subjects by Data Protection Law, such as the right to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making;
- e) “**Restricted Data Transfer**” means any international transfer of Personal Data that would be prohibited under Data Protection Law in the EEA or UK without implementation of additional safeguards such as Standard Contractual Clauses.
- f) “**Personnel**” means any natural person acting under the authority of Momentum;
- g) “**Personal Data**” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with a particular Data Subject or Consumer (as defined in the CCPA, to the extent applicable), or such equivalent concept as defined under applicable Data Protection Laws.
- h) “**Personal Data Breach**” means the unauthorized destruction, loss, control, alteration, disclosure of, or access to, Personal Data for which Momentum is responsible, to the extent that the incident constitutes a reportable “data breach”, “personal data breach”, “breach of the security of the system”, or other similar term as defined under Data Protection Law. Personal Data Breaches do not include unsuccessful access attempts or attacks that do not compromise the confidentiality, integrity, or availability of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- i) “**Sell**” means to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Personal Data to a Third Party for monetary or other valuable consideration.
- j) “**Sensitive Data**” means any type of Personal Data that is designated as a sensitive or special category of Personal Data, or otherwise subject to additional restrictions under Data Protection Law or other laws to which the Controller is subject;
- k) “**Services**” means the services and/or products to be provided by Momentum to Customer under the Agreement. The Services shall also include any required, usual, appropriate or acceptable methods to perform activities related to the Services, including (a) carrying out the Services or the business of which the Services are a part, (b) carrying out any benefits, rights

and obligations related to the Services, (c) maintaining records relating to the Services, and (d) complying with any legal or self-regulatory obligations related to the Services;

- l) **“Share”** means to share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Personal Data to Third Parties for targeted advertising to an individual based on Personal Data obtained from the individual's activity across non-affiliated or distinctly-branded websites, applications, or services;
- m) **“Subprocessor”** means a Processor engaged by a Processor to carry out Processing on behalf of a Controller;
- n) **“Standard Contractual Clauses”** means (i) the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the **“EU SCCs”**), and (ii) where the UK GDPR applies, the EU SCCs as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018 (the **“UK SCCs”**).

1.2. Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

2. Scope and Roles

- 2.1. This DPA applies only to the extent that Momentum Processes Personal Data that is subject to applicable Data Protection Law in the course of providing the Services pursuant to the Agreement.
- 2.2. If Data Protection Law applies to the Processing of Personal Data, the parties agree that Momentum shall Process Personal Data only as a Processor acting on behalf of Customer and, with respect to CCPA and other applicable U.S. state privacy laws, as a Service Provider, in each case, regardless of whether Customer acts as a Controller or as a Processor on behalf of a third-party Controller with respect to Personal Data.
- 2.3. The subject matter, nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set out in **Annex I**, which is an integral part of this DPA.

3. Instructions

- 3.1. Momentum will only Process Customer Data to provide the Services to Customer.
- 3.2. It is the parties' intent that Momentum is a Service Provider, and Momentum certifies that it will not (a) Sell or Share Customer Data; (b) Process Customer Data outside the direct business relationship between the parties or for any purpose other than to provide the Services in accordance with the Agreement, unless required or authorized by Data Protection Law; or (c) combine the Customer Data that Momentum receives from or on behalf of Customer with personal data that Momentum collects or receives from another person.
- 3.3. Customer's instructions are documented in **Annex I**, the Agreement, and any applicable statement of work.
- 3.4. Customer may issue additional instructions to Momentum as it deems necessary to comply with Data Protection Law. Such instructions must be provided to Momentum in writing and acknowledged in writing by Momentum as constituting instructions for purposes of this DPA, and Momentum may charge a reasonable fee to comply with any such additional instructions.
- 3.5. The parties acknowledge and agree that the disclosure of Customer Data by the Customer to Momentum does not form part of any monetary or other valuable consideration exchanged between the parties.

4. Customer Responsibilities

- 4.1 Customer is responsible for the lawfulness of Personal Data Processing in connection with the Services. Customer shall (i) provide all notices and obtain all consents, permissions and rights necessary under applicable Data Protection Law for Momentum to lawfully Process Personal Data for the purposes contemplated by the Agreement; (ii) make appropriate use of the Services to ensure a

level of security appropriate to the particular content of the Personal Data; (iii) comply with all Data Protection Law applicable to the collection of Personal Data and the transfer of such Personal Data to Momentum and its Subprocessors; and (iv) ensure its Processing instructions comply with applicable laws (including applicable Data Protection Law).

5. Personnel and Subprocessing

- 5.1. Momentum will require all Personnel authorized to Process Personal Data agree to maintain the confidentiality of the data.
- 5.2. Customer authorizes Momentum to engage and disclose Personal Data to the Subprocessors identified in **Annex III** ("Subprocessor List"); and Subprocessors engaged in accordance with Section 5.3.
- 5.3. Where Momentum intends to engage any additional Subprocessor not already identified on the Subprocessor List, Momentum will notify Customer of the proposed engagement of the Subprocessor giving Customer the opportunity to object. If Customer does not make a reasonable objection to the proposed engagement within 15 days of Momentum providing notice to Customer under this Section 5.3, Customer is deemed to have authorized the engagement of such Subprocessor. If Customer objects prior to the appointment of such Subprocessor on reasonable grounds relating to the Subprocessor's ability to protect Personal Data in accordance with this DPA, Momentum will work with Customer in good faith to resolve the issue. If an alternative solution cannot be found, Customer and Momentum may agree to terminate the impacted Services, and the Customer shall pay Momentum any fees due for the Services performed prior to termination.
- 5.4. Momentum will enter into a written agreement with all Subprocessors which imposes substantially similar obligations on the Subprocessors as this DPA imposes on Momentum. Momentum will remain fully liable to the Customer for the performance of each Subprocessor's data protection obligations relating to this DPA in the event the Subprocessor fails to fulfil those obligations.
- 5.5. To the extent required by law, Momentum will provide a copy of Momentum's agreements with Subprocessors to Customer upon request. Momentum may redact commercially sensitive information before providing such agreements to Customer.

6. Restricted Data Transfers

- 6.1. In the event that the Personal Data Processed under the DPA is subject to Data Protection Law and the transfer of Personal Data to Momentum would be restricted in the absence of the Standard Contractual Clauses, the parties agree that the Standard Contractual Clauses shall be incorporated into this DPA with Customer as the "data exporter" and Momentum as the "data importer."
- 6.2. The EU SCCs are completed as follows: the optional docking clause in Clause 7 is implemented; Clause 9(a) option 2 is implemented and the time period therein is specified as thirty (30) days; the optional redress clause in Clause 11(a) is struck; the governing law in Clause 17 is the law of Ireland; the court in Clause 18(b) are the courts of Ireland; and Annex 1, 2 and 3 to the EU SCCs are the appendices of this DPA. To the extent required by Data Protection Law in the UK, Part 1, tables 1, 2 and 3 of the UK SCCs will be deemed to be completed like its equivalent provisions in the EU SCCs. For the purpose of Part 1, Table 4, the party that may end the UK SCCs in accordance with Section 19 of the UK SCCs is the importer.

7. Security and Personal Data Breaches

- 7.1. Momentum will implement and maintain technical and organizational measures in relation to the Processing of Personal Data designed to provide a level of security appropriate to the risks which may occur as a result of Processing Personal Data, and in particular the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, including the measures listed in **Annex II** (as appropriate).
- 7.2. Momentum will inform Customer without undue delay after becoming aware of a Personal Data Breach, and will provide Customer with details of the Personal Data Breach and reasonable assistance in remediating and mitigating the effects of the Personal Data Breach.

- 7.3. Momentum's notification of or response to a Personal Data Breach under Section 7.2 will not be construed as an acknowledgement by Momentum of any fault or liability with respect to the Personal Data Breach.
- 7.4. In the event of a Personal Data Breach, Customer is solely responsible for determining whether Data Protection Law requires the notification of affected individuals, regulators and other parties of the Personal Data Breach.

8. Assistance

- 8.1. Momentum will reasonably assist Customer, including by implementing appropriate technical and organizational measures, with the fulfilment of Customer's own obligations under Data Protection Law, including:
- a) complying with Data Subjects' requests to exercise Data Subject Rights;
 - b) replying to inquiries or complaints from Data Subjects;
 - c) replying to investigations and inquiries from Supervisory Authorities;
 - d) conducting data protection impact assessments, and prior consultations with Supervisory Authorities; and
 - e) providing notifications to affected individuals, regulators and other parties in connection with Personal Data Breaches.
- 8.2. Unless prohibited by Data Protection Law, Momentum will inform Customer as soon as reasonably practicable if Momentum:
- a) receives a request, complaint or other inquiry regarding the Processing of Personal Data from a Data Subject or Supervisory Authority;
 - b) receives a binding or non-binding request to disclose Personal Data from law enforcement, courts or any government body;
 - c) is subject to a legal obligation that requires Momentum to Process Personal Data in contravention of Customer's instructions; or
 - d) is otherwise unable to comply with Data Protection Law or this DPA.
- 8.3. Unless prohibited by Data Protection Law, Momentum will obtain Customer's written authorization before responding to, or complying with any requests, orders, or legal obligations referred to in Section 8.2.
- 8.4. Customer will promptly reimburse Momentum for any costs and expenses incurred by Momentum in connection with the provision of assistance to Customer under this DPA.

9. Accountability

- 9.1. Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate Momentum's unauthorized use of Personal Data.
- 9.2. Momentum will inform Customer without undue delay if Momentum believes that a written instruction by Customer pursuant to this DPA, violates Data Protection Law, in which case Momentum may suspend the Processing until Customer has modified or confirmed the lawfulness of the instructions in writing.

10. Audit

- 10.1. Upon Customer's prior written request, and no more than once annually, Momentum will make available to Customer the required information reasonably necessary to demonstrate compliance with the obligations of Data Protection Law and this DPA. Momentum shall provide additional information as reasonably necessary to allow for and contribute to audits, including inspections, conducted by a Supervisory Authority, Customer or another auditor mandated by law.
- 10.2. If a third party is to conduct a Customer-requested audit, Momentum may object to the auditor if the auditor is, in Momentum's reasonable opinion, not suitably qualified or independent, a competitor of

Momentum or otherwise manifestly unsuitable. Such objection by Momentum will require Customer to appoint another auditor or conduct the audit itself.

- 10.3. The audit must be conducted during regular business hours at the applicable facility, subject to an audit plan agreed to between the parties at least two weeks in advance and may not unreasonably interfere with Momentum's business activities.
- 10.4. If Customer's requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Customer's audit request and Momentum confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.
- 10.5. Any Customer-requested audits are at Customer's expense. Customer shall reimburse Momentum for any time expended by Momentum or its Subprocessors in connection with any Customer-requested audits or inspections at Momentum's then-current professional services rates, which shall be made available to Customer upon request.
- 10.6. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports are confidential information of the parties under the terms of the Agreement.

11. Return or deletion of Customer Data

- 11.1 Thirty days after the Agreement comes to an end or expires, Momentum shall delete all Customer Data in its possession or control. This requirement shall not apply to the extent Momentum is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems (e.g., in the form of audit logs), which Customer Data Momentum must be securely isolated and protected against any further Processing, except to the extent required by applicable law. Upon request from Customer, Momentum will certify such secure deletion in writing within thirty (30) days of Customer's request. Upon request from Customer, Momentum will certify such secure deletion in writing within thirty (30) days of Customer's request.

12. Liability

- 12.1. The total combined liability of either party and its affiliates towards the other party and its affiliates, whether in contract, tort or any other theory of liability, under or in connection with Agreement and this DPA combined, will be limited to limitations on liability or other liability caps agreed to by the parties in the Agreement.

13. Confidentiality

- 13.1. Momentum will keep all Personal Data and all information relating to the Processing thereof in strict confidence.

14. Analytics

- 14.1 Customer acknowledges and agrees that Momentum may create and derive from Processing related to the Services anonymized and/or aggregated data that does not identify Customer or any natural person, and use, publicize or share with third parties such data to improve Momentum's products and services and for its other legitimate business purposes.

15. Notifications

- 15.1. Momentum will make all notifications required under this DPA as agreed to in the Agreement.

16. Modification of this DPA

- 16.1. This DPA may only be modified by a written amendment signed by both Customer and Momentum.

17. Invalidity and Severability

- 17.1. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect

any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

ANNEX I

A. LIST OF PARTIES

Customer is the Controller and the data exporter and Momentum is the Processor and the data importer.

B. DESCRIPTION OF TRANSFER

Subject Matter	Momentum's provision of workflow automation services to Customer.
Duration of the Processing	For the term of the Agreement and as required under applicable law.
Nature and Purpose of the Processing	Momentum will Process Personal Data for the purposes of providing the Services to Customer in accordance with the DPA.
Frequency of the Processing	Continuous.
Categories of Data	Data relating to individuals provided to Momentum in connection with the Services provided to Customer, including name, email address, usage data, any Personal Data captured via services the user integrates with Momentum (such as Google Calendar and Slack), and any Personal Data voluntarily shared and captured in the transcription of the recorded user's conversations.
Sensitive Data Processed	The Services are not intended to Process Sensitive Data unless otherwise agreed to in a signed amendment to this Annex.
Data Subjects	Customer's end users and authorized users.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the Irish Data Protection Commission.

ANNEX II

For a description of Momentum's security controls, please visit <https://www.momentum.io/security>.

ANNEX III

List of Subprocessors

Customer authorizes Momentum to engage the Subprocessors listed at:
<https://www.momentum.io/sub-processors>.