DATA PROCESSING AGREEMENT

This data processing agreement is between Atolio, Inc. (the "**Data Processor**") and you and/or the entity you represent ("**Data Controller**") and incorporates the terms and conditions set out in the Schedules attached hereto (the "**Agreement**"). This Agreement is subject to the Master Subscription Agreement.

Each Data Controller has appointed the Data Processor to provide services to the Data Controller(s). As a result of its providing such services to the Data Controller(s), the Data Processor will store and process certain personal information of the Data Controller(s), in each case as described in further detail in Schedule 2 (*Processing Details*).

The Agreement is being put in place to ensure that the Data Processor processes each Data Controller's personal data on the Data Controller's instructions and in compliance with Applicable Data Protection Laws.

The parties to this Agreement hereby agree to be bound by the terms and conditions in the attached Schedules as applicable with effect from the date of Data Controller's first use of the services or, if applicable, the date of the Master Subscription Agreement (the "**Effective Date**").

SCHEDULE 1
STANDARD TERMS FOR PROCESSING AGREEMENT

BACKGROUND:

(a) Each Data Controller wishes to appoint the Data Processor to Process Personal Data, as further described in Schedule 2 (*Processing Details*).

(b) This Agreement is being put in place to ensure that the Data Processor processes each Data Controller's Personal Data on the Data Controller's instructions and in compliance with the Applicable Data Protection Laws (as defined below).

1. Definitions

1.1 For the purposes of this Agreement, the following expressions bear the following meanings unless the context otherwise requires:

"**Applicable Data Protection Laws**" means (a) the General Data Protection Regulation 2016/679 (the "**GDPR**"); (b) the Privacy and Electronic Communications Directive 2002/58/EC; (c) the UK Data Protection Act 2018 ("**DPA**"), the UK General Data Protection Regulation as defined by the DPA as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (together with the DPA, the "**UK GDPR**"), and the Privacy and Electronic Communications Regulations 2003; and (d) the California Consumer Protection Act, as amended by the California Privacy Rights Act, and regulations promulgated thereunder ("CCPA"); (e) the Colorado Privacy Act ("CPA"); (f) the Connecticut Data Privacy Act ("CTDPA"); (g) the Utah Consumer Privacy Act ("UCPA"); (h) the Virginia Consumer Data Protection Act ("VCDPA") and (i) any relevant law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding instrument which implements any of the above or which otherwise relates to data protection, privacy or the use of personal data, in each case as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time;

"**Controller to Processor Clauses**" means (i) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021, specifically including Module 2 (Controller to Processor); and (ii) in respect of transfers of Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner, in each case as amended, updated or replaced from time to time;

"**Data Subject**" shall have the meaning given in the relevant Applicable Data Protection Laws;

"**Master Subscription Agreement**" means the Master Subscription Agreement available at https://www.atolio.com/msa/ or, if applicable, the Master Subscription Agreement entered into by the Data Controller(s) and the Data Processor on or around the date of this Agreement;

"**Personal Data**" means all Personal Data or Personal Information (as defined by the relevant Applicable Data Protection Laws) that is subject to the relevant Applicable Data Protection Laws from time to time;

"**Process**", "**Processed**" or "**Processing**" shall have the meaning given in the relevant Applicable Data Protection Laws;

"**Processor to Processor Clauses**" means, as relevant, (i) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021 specifically including Module 3 (Processor to Processor); (ii) in respect of transfers of Personal Data subject to the UK GDPR, the International Data Transfer

Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner, in each case as amended, updated or replaced from time to time;

"**Regulator**" means a data protection supervisory authority which has jurisdiction over a Data Controller's Processing of Personal Data; and

"**Third Country**" means (i) in relation to Personal Data transfers subject to the GDPR, any country or territory outside of the scope of the data protection laws of the European Economic Area, excluding countries or territories approved as providing adequate protection for Personal Data by the European Commission from time to time; and (ii) in relation to Personal Data transfers subject to the UK GDPR, any country or territory outside of the scope of the data protection laws of the UK, excluding countries or territories approved as providing adequate protection for Personal Data by the relevant competent authority of the UK from time to time.

2. Conditions of Processing

2.1 This Agreement governs the terms under which the Data Processor is required to Process Personal Data on behalf of the Data Controller(s).

3. Data Processor's Obligations

3.1 The Data Processor shall only process Personal Data under the Master Subscription Agreement for the limited and specific purpose of performing the services provided for in the Master Subscription Agreement, and at all times in compliance with Applicable Data Protection Laws, and shall provide the same level of privacy protection as is required by Applicable Data Protection Laws. The Data Processor shall notify the Data Controller without undue delay if the Data Processor makes a determination that it can no longer meet its obligations under Applicable Data Protection Laws. To the extent required by Applicable Data Protection Laws, the Data Controller shall have the right to take reasonable and appropriate steps to help ensure that the Data Processor uses the Personal Data in a manner consistent with the Data Controller's obligations under Applicable Data Protection Laws and stop and remediate any unauthorized use of the Personal Data.

3.2 The Data Processor shall only retain, use, disclose, and otherwise Process Personal Data on behalf of the Data Controller(s) and in accordance with, and for the business purposes set out in the documented instructions received from the Data Controller(s) unless required to Process such Personal Data by applicable law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller(s) of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest

3.3 To the extent required by Applicable Data Protection Laws, the Data Processor is prohibited from selling the Personal Data; sharing the Personal Data for cross-context behavioral advertising purposes; retaining, using, or disclosing the Personal Data outside of the direct business relationship between Data Processor and Data Controller; and combining the Personal Data received from Data Controller with any Personal Data that may be collected from Data Processor's separate interactions with the individual(s) to whom the Personal Data relates or from any other sources.

3.4 The Data Processor shall ensure that its personnel authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.5 The Data Processor shall implement reasonable and appropriate technical and organisational measures to protect the Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure, taking into account the nature of the Personal Data, the state of the art, the costs of implementation and the nature, scope, context and purpose of the Processing as set out in Schedule 3, or otherwise agreed and documented between the Data Controller and Data Processor from time to time.

3.6 The Data Processor shall without undue delay notify the relevant Data Controller(s) about any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data belonging to the Data Controller(s) or any accidental or unauthorised access or any other event affecting the integrity, availability or confidentiality of the Personal Data belonging to the Data Controller(s) (with further information about the breach provided in phases as more details become available).

3.7 The Data Processor shall upon written request from any Data Controller from time to time provide that Data Controller with such information as is reasonably necessary to demonstrate compliance with the obligations laid down in this Agreement.

3.8 Upon reasonable request of Data Controller, the Data Processor shall make available to Data Controller all information in its possession necessary to demonstrate the Data Processor's compliance with its obligations under Applicable Data Protection Laws. The Data Processor shall allow and cooperate with reasonable assessments by the Data Controller or the Data Controller's designated auditor, at the Data Controller's expense, of the Data Processor's compliance with its obligations under this Agreement and Applicable Data Protection Laws. The Data Controller shall be permitted to conduct such an assessment no more than once every twelve months, upon thirty days' advance written notice to the Data Processor, and only after the parties come to agreement on the scope of the audit. As an alternative to an audit performed by or at the direction of the Data Controller, the Data Processor may arrange for a qualified and independent auditor to conduct, at the Data Processor's expense, an assessment of the Data Processor's policies and technical and organizational measures in support of its obligations under Applicable Data Protection Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessments, and will provide a report of such assessment to the Data Controller upon reasonable request. Notwithstanding the foregoing, in no event shall the Data Processor be required to give the Data Controller access to information, facilities, or systems to the extent doing so would cause the Data Processor to be in violation of confidentiality obligations owed to other customers or its legal obligations.

3.9 Where:

(i) a Data Subject exercises his or her rights under the Applicable Data Protection Law in respect of Personal Data Processed by the Data Processor on behalf of any Data Controller, including Data Subjects exercising rights under Applicable Data Protection Laws (such as rights to rectification, erasure, blocking, access their personal data, objection, restriction of processing, data portability, and the right not to be subject to automated decision making); or

(ii) any Data Controller is required to deal or comply with any assessment, enquiry, notice or investigation by the Regulator; or

(iii) any Data Controller is required under the Applicable Data Protection Laws to carry out a mandatory data protection impact assessment or consult with the Regulator prior to Processing Personal Data entrusted to the Data Processer under this Agreement,

then the Data Processor will provide reasonable assistance to the relevant Data Controller to enable that Data Controller to comply with obligations which arise as a result thereof.

3.10 To the extent the Data Processor Processes Personal Data in a Third Country, and it is acting as data importer, the Data Processor shall comply with the data importer's obligations set out in the Controller to Processor Clauses, which are hereby incorporated into and form part of this Agreement; the Data Controller(s) will comply with the data exporter's obligations in such Controller to Processor Clauses; and:

(i) for the purposes of Annex I or Part 1 (as relevant) of such Controller to Processor Clauses, the parties and processing details set out in Schedule 2 (*Processing Details*) shall apply, the Start Date is the Effective Date, and the signature(s) (in any form) given in connection with the execution of

the Master Subscription Agreement by a party and the dates of such signature(s) shall apply as the dated signature required from that party;

(ii) if applicable, for the purposes of Part 1 of such Controller to Processor Clauses, the relevant Addendum EU SCCs (as such term is defined in the applicable Controller to Processor Clauses) are the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021 (Module 2) as incorporated into this Agreement by virtue of this clause 3.10;

(iii) for the purposes of Annex II or Part 1 (as relevant) of such Controller to Processor Clauses, the technical and organisational security measures set out in Schedule 3 (*Technical and Organisational Measures)* shall apply and, if applicable, the technical and organisational measures adopted by relevant sub-processors as notified in the relevant sub-processor privacy notice or security documentation shall apply; and

(iv) if applicable, for the purposes of: (i) Clause 9 of such Controller to Processor Clauses, Option 2 ("General written authorization") is deemed to be selected and the notice period specified in clause 6.2 shall apply; (ii) Clause 11(a) of such Controller to Processor Clauses, the optional wording in relation to independent dispute resolution is deemed to be omitted; (iii) Clause 13 and Annex I.C, the competent supervisory authority shall be the Irish Data Protection Commission; (iv) Clause 17, Option 1 is deemed to be selected and the governing law shall be Irish law; (v) Clause 18, the competent courts shall be the Irish courts; (vi) Part 1 of such Controller to Processor Clauses, the Data Processor as Importer may terminate the Controller to Processor Clauses pursuant to Section 19 of such Controller to Processor Clauses.

3.11 The Data Controller acknowledges and agrees that the Data Processor may appoint an affiliate or third party subcontractor to Process the Data Controller's Personal Data in a Third Country, in which case the Data Processor shall execute the Processor to Processor Clauses with any relevant subcontractor (including affiliates) it appoints on behalf of the Data Controller.

4. Data Controller's Obligations

4.1 Each Data Controller warrants that: (i) the legislation applicable to it does not prevent the Data Processor from fulfilling the instructions received from the Data Controller(s) and performing the Data Processor's obligations under this Agreement; and (ii) it has complied and continues to comply with the Applicable Data Protection Laws, in particular that it has obtained any necessary consents or given any necessary notices, and otherwise has a legitimate ground to disclose the data to the Data Processor and enable the Processing of the Personal Data by the Data Processor as set out in this Agreement and as envisaged by the Master Subscription Agreement and any other services agreement in place between the parties.

4.2 Each Data Controller agrees that it will jointly and severally together with any other Data Controller, indemnify and hold harmless the Data Processor on demand from and against all claims, liabilities, costs, expenses, loss or damage (including consequential losses, loss of profit and loss of reputation and all interest, penalties and legal and other professional costs and expenses) incurred by the Data Processor arising directly or indirectly from a breach of this Clause 4.

5. Changes in Applicable Data Protection Laws

5.1 The parties agree to negotiate in good faith modifications to this Agreement if changes are required for the Data Processor to continue to process the Personal Data as contemplated by this Agreement in compliance with the Applicable Data Protection Laws or to address the legal interpretation of the Applicable Data Protection Laws, including (i) to comply with the GDPR or any national legislation implementing it, or the UK General Data Protection Regulation or the DPA, and any guidance on the interpretation of any of their respective provisions; (ii) the Controller to Processor Clauses or the Processor to Processor Clauses or any

other mechanisms or findings of adequacy are invalidated or amended, or (iii) if changes to the membership status of a country in the European Union or the European Economic Area require such modification.

6. Sub-Contracting

6.1 The Data Controller(s) hereby grants the Data Processor general written authorisation to engage the sub-processors set forth on the following site: https://atolio.com/subprocessors/.

6.2 If the Data Processor appoints a new subcontractor or intends to make any changes concerning the addition or replacement of the subcontractors, it shall provide the Data Controller(s) with seven (7) business days' prior written notice, during which the Data Controller(s) can object against the appointment or replacement. If no Data Controller objects, the Data Processor may proceed with the appointment or replacement. The Data Processor shall ensure that it has a written agreement in place with all subcontractors which contains obligations on the subcontractor which are no less onerous on the relevant subcontractor than the obligations on the Data Processor under this Agreement.

7. Termination

7.1 Termination of this Agreement shall be governed by Clause 12 (*Term and Termination*) of the Master Subscription Agreement.

8. Consequences of Termination

8.1 Upon termination of this Agreement in accordance with Clause 7 (*Termination*), the Data Processor shall, at the choice of the Data Controller:

(i) return to the Data Controller or to another data processor designated by the Data Controller all of the Personal Data and any copies thereof which it is Processing or has Processed upon behalf of that Data Controller; or

(ii) destroy all Personal Data it has Processed on behalf of the Data Controller after the end of the provision of services relating to the Processing, and destroy all copies of the Personal Data unless any European Member State law requires storage of such Personal Data; and

(iii) in each case cease Processing Personal Data on behalf of the Data Controller(s).

9. Law and Jurisdiction

This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in all respects in accordance with the laws of New York and shall be deemed to have been made in New York, and each party hereby submits to the jurisdiction of the courts of New York County, New York**.**

SCHEDULE 2

PROCESSING DETAILS

A. LIST OF PARTIES

Data controller(s)/ exporter(s):

Name: The customer who has purchased services from Data Processor.

Address: As set forth in the Master Subscription Agreement or as set forth in Data Controller's account for the services.

Contact person's name, position and contact details: As set forth in the Master Subscription Agreement or as set forth in Data Controller's account for the services.

Activities relevant to the data transferred under these Clauses: Receipt of services from Data Processor under the Master Subscription Agreement.

Role (controller/processor): Controller

Data processor/ importer(s):

Name: Atolio, Inc.

Address: 1550 Larimer St #436

Denver, CO 80202-1602 USA

Contact person's name, position and contact details:

Christine Johnson, VP Finance

christine@atolio.com

Activities relevant to the data transferred under these Clauses: Provision of services to Data Controller under the Master Subscription Agreement.

Role (controller/processor): Processor

B. PROCESSING DETAILS/ DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is processed/ transferred

Contacts of Atolio's customers.

Categories of personal data processed/ transferred

Basic contact details (i.e., name, email, phone number).

Sensitive data processed/ transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous, for the duration of the provision of the services.

Nature of the processing

Processing activities in order to provide services to Data Controller.

Purpose(s) of the data processing/ data transfer and further processing

To provide services to Data Controller.

Duration of the processing/ the period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

In accordance with the period set out in the privacy policies or as otherwise notified to data subjects by Data Controller, subject to Applicable Data Protection Laws.

For processing by/ transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

If relevant, as set out above for Data Processor.

SCHEDULE 3
TECHNICAL AND ORGANISATION SECURITY MEASURES

1. Physical Access Management

The Data Processor does not control or own the physical premises or facilities in which the Data are processed.

2. System Entry Management

The Data Processor shall take, among others, the following technical and organizational measures in order to prevent unauthorized access to the data processing systems:

- Unique user authentication via user name and password for each network and system access required (default passwords changed at 1st login)
- Use of state-of-the-art anti-virus software that includes e-mail filtering and malware detection
- Use of firewalls
- During idle times, user and administrator PCs are automatically locked
- User passwords are changed in response to signals indicating account compromise and a multi-factor authentication system is used
- Concept of least privilege, allowing only the necessary access for users to accomplish their job function. Access above these least privileges requires appropriate authorization
- Starter, mover & leaver housekeeping processes in place which covers role-based access rights
- All users have a Google Workspace account with mandatory multi-factor authentication, and access to applications is gated on the use of a Google Workspace identity
- AWS CloudTrail logs all access to all S3 buckets

3. Data Access Management

The Data Processor shall take, among others, the following technical and organizational measures in order to prevent unauthorized activities in the data processing systems outside the scope of any granted authorizations:

- User and administrator access to the network is based on a role based access rights model. There is an authorization concept in place that grants access rights to data only on a “need to know” basis
- Administration of user rights through system administrators
- Number of administrators is reduced to the absolute minimum
- AWS CloudTrail logs all access to all S3 buckets.

4. Onward Data Transfer

The Data Processor shall take, among others, the following technical and organizational measures in order to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons under their electronic transmission or during their transport or recording on data carriers and to guarantee that it is possible to examine and establish where personal data are or have had to be transmitted by data transmission equipment:

- Remote access (including during remote maintenance or service procedures) to the IT systems only via VPN tunnels or other state-of-the-art secure, encrypted connections
- Use of e-mail encryption

- Data transferred by the Data Processor is transported and saved in encrypted form in accordance with AWS policies on data transfer. The relevant areas of the data carriers are encrypted using data and hard drive encryption software
- The secure transfer modes and encryption methods are regularly updated and kept state-of-the-art (*e.g.*, according to the recommendations in the data protection manual issued by the BSI (Federal Office for Information Security))
- Secure communication session established via HTTPS and SFTP protocols across all applications / services
- Encrypted certificates utilised for authentication between the web client and the web server across all websites

5. Input Management

The Data Processor shall take, among others, the following technical and organizational measures in order to ensure that it is subsequently possible to verify and establish whether and by whom personal data have been entered into data processing systems, altered or removed:

- Access to electronic documents / applications is documented via auditable log files
- Access to physical documents is documented via protocols
- Protocolling input, modification and deletion of data by use of individual user names

6. Instructions

The Data Processor shall take, among others, the following technical and organizational measures in order to ensure that personal data which are processed on behalf of Data Controller can only be processed in compliance with Data Controller's instructions:

- Clear and binding internal policies contain formalized instructions for data processing procedures
- Unambiguous language in the underlying contracts
- Careful selection of contractors, especially with regard to data security aspects
- Internal monitoring of quality of service includes compliance with contractual arrangements
- The Data Processor's corporate network is separated from its customer services network by means of complex segregation devices

7. Availability

The Data Processor shall ensure that its Subprocessors who provide data storage services take, among others, the following technical and organizational measures in order to protect the data from accidental destruction or loss:

- Appliances for the monitoring of temperature and humidity
- Fire / smoke detectors and fire extinguishers in the areas where data is stored / processed
- Enable the local firewall on each system
- Use of state-of-the-art anti-virus software that includes e-mail filtering and malware detection
- Data recovery measures and emergency plan in place and regularly tested

8. Separation and Purpose

The Data Processor shall take, among others, the following technical and organizational measures in order to ensure that data collected for different purposes are processed separately:

- Documents that are stored physically are stored separately for each customer and the respective containers are clearly labelled

- Implementation of an authorization concept
- Strong isolation between guest virtual machines is maintained. Customers are prevented from accessing areas not assigned to them by filtering through the virtualization software