Maestro AI – Data Processing Addendum

This Data Processing Addendum ("DPA") supplements the Master Services Agreement (the "Agreement") entered into by and between the individual, entity, or other person identified as the customer on the signature page of this DPA ("Customer") and Maestro AI, Inc. ("Company"), and is effective of even date therewith. Any terms not defined in this DPA shall have the meanings set forth in the Agreement. In the event of a conflict between the terms and conditions of this DPA and the Agreement, the terms and conditions of this DPA shall control to the extent necessary to comply with Data Protection Laws (as defined below).

1. Definitions

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "CCPA" means the California Consumer Privacy Act of 2018, as codified at California Civil Code Sections 1798.100 through 1798.199.100, and its associated regulations, and as amended by the California Privacy Rights Act of 2020, and as subsequently further amended from time to time.

1.3 **"**Data Controller**"** means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. With respect to Personal Data subject to the CCPA, the term Data Controller shall be read to mean entities that would qualify as a "business" subject to the CCPA.

1.4 **"**Data Processor**"** means the entity which Processes Personal Data on behalf of the Data Controller. With respect to Personal Data subject to the CCPA, the term Data Processor shall be read to mean entities that would qualify as a "service provider" subject to the CCPA.

1.5 "Data Protection Law(s)" means all local, state, national and/or foreign data protection and privacy laws, treaties and/or regulations applicable to the collection, use, transfer, storage, correction, disclosure, deletion, and other Processing of Personal Data under this DPA, including, where applicable, U.S. Data Protection Law(s) and European Data Protection Law(s).

1.6 "Data Subject" means a natural person who has been or is identified or identifiable, directly or indirectly, by reference to (i) one or more identifiers such as a name, an identification number, location data, an online identifier and/or (ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. With respect to Personal Data subject to the CCPA, the term Data Subject shall be read to mean persons who would qualify as a "consumer" entitled to exercise certain rights related to his or her Personal Data under the CCPA.

1.7 "European Data Protection Law(s)" means all EU and U.K. laws, rules, regulations or other legislation applicable (in whole or in part) to the Processing of Personal Data under the Agreement (such as Regulation (EU) 2016/679 (the "GDPR"), the U.K. GDPR (defined below), and the Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA"); the national laws of each EEA member state and the U.K. implementing any EU directive applicable (in whole or in part) to the Processing of Personal Data (such as Directive 2002/58/EC); and any other national laws of each EEA member state and the U.K. applicable (in whole or in part) to the Processing of Personal Data; in each case as amended or superseded from time to time.

1.8 "Instruction(s)" means a direction made in writing, either in textual form (e.g. by e-mail) or by using a software or online tool by or on behalf of Customer to Company with respect to the Processing of Personal Data.

1.9 "Personal Data" means any information that (i) is provided by or on behalf of Customer to Company (directly or indirectly) for Processing under the Agreement, (ii) relates to a Data Subject, and (iii) is governed by Data Protection Legislation. Where the CCPA applies, 'personal data' includes "personal information" as defined by the CCPA.

1.10“Process” or “Processing” means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.11“Security Incident” means a breach and/or a suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed by Company.

1.12 “Services” means, collectively, those products and/or services to be provided by Company to Customer pursuant to the Agreement.

1.13“Sub-Processor” means a third party engaged by or on behalf of a Data Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Data Controller.

1.14“Standard Contractual Clauses” means those terms set forth in the European Commission’s Implementing Decision of 4.6.2021 on standard contractual clauses, selecting Module Two between controllers and processors in any case where Company is a Data Controller, and Module Three between processors in any case where Company is a Data Processor, under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council dated June 4, 2021, and any replacement, amendment or restatement of the foregoing issued by the European Commission on or after the effective date of this DPA.

1.15“U.K. GDPR” means the GDPR, as it forms part of the domestic law of the United Kingdom by virtue of Section 3 of the European Union (Withdrawal) Act 2018.

1.16 "U.S. Data Protection Law(s)" means all U.S. state and federal laws, rules, regulations, or other legislation applicable to the Processing of Personal Data under the Agreement, which may include (without limitation) the CCPA, the Colorado Privacy Act, the Connecticut Personal Data Privacy and Online Monitoring Act, the Montana Consumer Data Privacy Act, the Oregon Consumer Data Privacy Act, the Tennessee Information Protection Act, the Texas Data Privacy and Security Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act, in each case as amended or superseded from time to time.

2. Scope of DPA; Processing of Data

2.1 Scope of DPA: This DPA applies to the Processing of Personal Data by Company in the course of providing the Services to Customer. The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data and categories of Data Subjects, are described in Appendix I to this DPA. As between the parties, Customer is the Data Controller and Company is the Data Processor of Personal Data. To the extent that any Personal Data provided by Customer is subject to European Data Protection Laws, such Personal Data shall be Processed in accordance with Section 6 of this DPA. To the extent that any Personal Data provided by Customer is subject to the CCPA, such Personal Data shall be Processed in accordance with Section 10 of this DPA. To the extent that any Personal Data provided by Customer is subject to U.S. Data Protection Laws other than the CCPA, such Personal Data shall be Processed in accordance with Section 11 of this DPA.

2.2 Instructions for Processing. Company shall Process the Personal Data strictly in accordance with Customer’s documented Instructions. Customer hereby instructs Company to Process Personal Data only as necessary to provide the Services in accordance with the Agreement (including this DPA). Customer may provide additional Instructions to Company to Process Personal Data from time to time at Customer’s discretion. In no event shall Company Process Personal Data for its own purposes or those of any third party.

2.3 Customer Obligations.

2.3.1 While this DPA is in effect, Customer shall at all times be responsible for:

(i) Complying with applicable Data Protection Law, including but not limited to providing notice to Data Subjects and obtaining the consent of Data Subjects where required for purposes of Customer's own Processing of Personal Data, in Customer's use of Company's Services, and in enabling Company to process the Personal Data pursuant to the terms of the Agreement and this DPA;

(ii) Processing Personal Data, and providing instructions to Company for the Processing of Personal Data, in compliance with any and all applicable Data Protection Laws;

(iii) Ensuring that its instructions to Company comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the Processing of Personal Data in accordance with Customer's instructions will not cause Company to be in breach of the Data Protection Laws; and

(iv) Verifying the accuracy, quality, and legality of the Personal Data provided to Company by or on behalf of Customer, the means by which Customer acquired any such Personal Data, and the instructions it provides to Company regarding the Processing of such Personal Data.

2.3.2 Customer shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith.

2.3.3 Customer represents and warrants to Company that Customer has obtained the Personal Data in accordance with the requirements of applicable Data Protection Laws, and that Customer is and will at all times during the term of the Agreement and this DPA remain duly and effectively authorized to have the right to transfer Personal Data to Company for Processing in accordance with the Agreement and this DPA.

2.4 Company's Obligations.

2.4.1 While this DPA is in effect, Company shall at all times be responsible for:

(i) Processing Personal Data in a manner consistent with the terms and conditions set forth in this DPA, the Agreement, and/or any other lawful and documented instructions provided by Customer;

(ii) Complying with all Data Protection Laws applicable to Company in its role as a Data Processor Processing Personal Data;

(iii) Ensuring that any person authorized by Company to Process Personal Data (including Company's employees, agents and subcontractors) shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to Process such Personal Data who is not under such a duty of confidentiality;

(iv) Promptly notifying Customer if an instruction, in Company's opinion, infringes applicable Data Protection Laws or the guidance, instructions, or orders provided by an applicable Authority (as defined in Section 4); and

(v) Otherwise assisting Customer in meeting its obligation to adopt adequate technical and organizational measures to ensure security of Processing to the extent required by applicable Data Protection Laws.

2.4.2 To the extent Customer requires Company's assistance to meet its obligations under Article 35 and 36 of the GDPR to carry out a data protection impact assessment and prior consultation with the competent supervisory authority (as defined in Appendix III) related to Customer's use of the Services, and taking into account the nature of the Processing and the information available to Company, Company shall provide Customer with reasonable and timely assistance with any data protection impact assessments as required by applicable Data Protection Law and, where necessary, consultations with data protection authorities.

3. Deletion or Return of Personal Data.

Customer shall notify Company of its election to have Personal Data returned or deleted within thirty (30) days of termination or expiry of the Agreement (or such other period as may be specified therein). If Customer makes a timely election, Company shall return or delete Personal Data pursuant to the election within sixty (60) days. Company may delete all Personal Data after the thirty (30) day period (or such other period specified, as applicable). This requirement shall not apply to the extent that Company is required by applicable laws to retain some or all of the Personal Data, in which event Company shall isolate and protect the Personal Data from any further Processing except to the extent required by such law, shall only retain such Personal Data for as long as it is required under applicable laws, and shall continue to ensure compliance with all Data Protection Laws during such retention.

4. Law Enforcement Requests.

4.1 Company's Notice Obligations. If Company receives notice from any law enforcement, regulatory, judicial or governmental authority (each an "Authority") that such Authority wishes to obtain access to any or all of the Personal Data, whether on a voluntary or a mandatory basis, then Company shall (unless legally prohibited as part of a mandatory legal compulsion that requires disclosure of Personal Data to such Authority): (a) promptly notify Customer of such Authority's data access request; (b) inform the Authority that any and all requests or demands for access to Data should be notified to or served upon Customer in writing; and (c) not provide the Authority with access to the relevant Personal Data unless and until authorized by Customer.

4.2 Conditions upon Company's Disclosure Obligations. If, at any time while this DPA is in effect, Customer comes under a legal prohibition or a mandatory legal compulsion that prevents it from complying with its obligations under Section 4.1 in full, Customer shall use reasonable and lawful efforts to challenge such prohibition or compulsion. If Customer makes a disclosure of Customer's Personal Data to an Authority (whether with Customer's authorization or due to a mandatory legal compulsion), Customer shall only disclose such Personal Data to the extent Customer is legally required to do so.

5. Authorized Sub-Processors

5.1 List. A list of Company's current Sub-Processors is available at https://www.getmaestro.ai/subprocessors (the "List"). As of the date of this DPA, and continuing throughout the term of the Agreement, the List sets forth the up-to-date details of the Processing activity/ies that each such Sub-Processor performs or will perform for Company in the performance of the Services, and the location of Processing for each Sub-Processor.

5.2 Customer's General Authorization. By executing this DPA, Customer hereby:

5.2.1 Acknowledges and agrees that (i) the Sub-Processors set forth in the List are authorized to access and to Process Customer’s Personal Data in connection with the Services and (ii) from time to time, Company may engage additional third parties as Sub-Processors for the purpose of providing the Services, including without limitation the Processing of Personal Data.

5.2.2 Consents to the transfer by Company of Customer’s Personal Data to each of the Sub-Processors identified on the List, as updated from time to time in accordance with Section 5.3 of this DPA, as necessary to provide Customer with Services pursuant to the Agreement; and

5.2.3 Provides general written authorization to Company to engage additional third parties as Sub-Processors as necessary to perform the Services, subject to the terms set forth in Section 5.3 below.

5.3 Engaging Additional Sub-Processors. If Company engages, or wishes to engage, or removes or wishes to remove, any Sub-Processors from the List following the date of the Agreement, such engagement shall be subject to the terms set forth below:

5.3.1 At least ten (10) days before enabling any third party other than currently authorized Sub-Processors to access or participate in the Processing of Personal Data, Company will:

(i) Add the proposed Sub-Processor to the List in a manner compliant with Section 5.3.1(ii);

(ii) The entry of each proposed Sub-Processor shall include (a) the entity name of such Sub-Processor, (b) the Processing activities for which the Sub-Processor was engaged, (c) the location of such Sub-Processor’s Processing activities, and (d) the date on which the proposed Sub-Processor was added to the List, and shall be highlighted or otherwise visually marked within the List as a new entry; and

(iii) Notify Customer in accordance with Company’s notice obligations under the Agreement that the List has been updated to reflect a new removal/addition.

5.3.2 If Customer objects to Company's appointment of a Sub-Processor on reasonable grounds relating to the protection of the Personal Data, Customer may reasonably object to such an engagement on legitimate grounds by informing Company in writing within ten (10) days of receipt of the aforementioned notice by Company. Customer’s objection shall be sent to privacy@getmaestro.ai and explain the reasonable grounds for Customer’s objection. If Customer does not object to the engagement of a third party in accordance with this Section 5.3.2 within ten (10) days of notice by Company, Company will deem Customer to have authorized the new Sub-Processor and that third party will be deemed an authorized Sub-Processor for the purposes of this DPA.

5.3.3 If Customer timely objects to the engagement of a third party in accordance with Section 5.3.2, the parties will discuss Customer’s concerns in good faith and use commercially reasonable efforts to achieve a resolution. Should no resolution be reached, either Company will not appoint the Sub-Processor, or (should Company choose to retain the objected-to Sub-Processor) Customer may elect to suspend or discontinue the affected Services by providing written notice to Company. Termination shall not relieve Customer of any fees owed to Company under the Agreement, nor any other obligations of Customer which are intended to survive the Agreement.

5.4 Obligations of Sub-Processors. Company will enter into a written agreement with each Sub-Processor, imposing on the Sub-Processor data protection obligations that are substantially the same as those imposed on Company under this DPA with respect to the protection of Personal Data. Company will remain fully liable to Customer for any breach of this DPA that is caused by an act, error or omission of any Sub-Processor’s obligations under such agreement.

5.5 Disclosure of Sub-Processor Agreements. For purposes of clause 9(c) of the Standard Contractual Clauses, Customer acknowledges that Company may be restricted from disclosing Sub-Processor agreements to Customer, but Company agrees to use reasonable efforts to request any Sub-Processor to disclose the Sub-Processor agreement to Customer and will provide (on a confidential basis) all Sub-Processor information reasonably possible without breaching any obligations of confidentiality Company may have to the Sub-Processor.

6. International Transfers of Personal Data

6.1 Location of Processing. Company is located in the United States and Processes Personal Data in the United States. The parties acknowledge and agree that, for Company to perform Services for Customer pursuant to the Agreement, Customer shall transfer (directly or indirectly) Personal Data to Company in the United States.

6.2 Terms Applicable to Processing of EU/U.K/Swiss Personal Data. With respect to Personal Data provided by Customer that is subject to European Data Protection Law, the parties agree to abide by and Process the Personal Data pursuant to the terms set forth hereunder (provided, if and to the extent a Permitted Affiliate relies on the Standard Contractual Clauses for the transfer of Personal Data subject to European Data Protection Law, any references to "Customer" in this Section 6 include such Affiliate):

6.3 The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and are an integral part of this DPA, subject to further specification as described below and in Appendices III, IV, and V to this DPA. For the purposes of the descriptions in the Standard Contractual Clauses:

6.3.1 Company agrees that it is the "data importer" and Customer is the "data exporter" (notwithstanding that Customer may itself be located outside the EEA/U.K. and/or a Processor acting on behalf of a third-party Data Controller);

6.3.2 The Agreement, together with this DPA, represents Customer's complete and final documented Instructions as of the effective date for the Processing of Personal Data;

6.3.3 Appendix I (Processing Particulars) and Appendix II (Specific Security Measures) of this DPA shall form Annex I and Annex II of the Standard Contractual Clauses, respectively;

6.3.4 Option 2 under clause 9 of the Standard Contractual Clauses will apply with respect to any Sub-Processor engaged by Company under this DPA. For purposes of clause 9(a) of the Standard Contractual Clauses, Company has Customer's general authorization for the engagement of Sub-Processor(s) from the List (as defined in Section 5.1 and updated from time to time in accordance with Section 5.3), which shall be amended from time to time in accordance with the terms of the Agreement, this DPA, and all applicable Data Protection Laws.

6.3.5 To the extent that the Standard Contractual Clauses permit the selection of modules and clauses, the parties agree to the following modules and clauses:

(i) The Docking Clause option under clause 7 of the Standard Contractual Clauses shall apply.

(ii) The parties agree that the audits described in clause 8.9 of the Standard Contractual Clauses shall be carried out in accordance with the audit provisions detailed in Section 8 of this DPA.

(iii) The option under clause 11 (Redress) of the Standard Contractual Clauses shall not apply.

6.3.6 It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. Accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict with respect to Personal Data Processed pursuant to the Standard Contractual Clauses. In no event does this DPA restrict or limit the rights of any Data Subject or of any competent supervisory authority (as defined in Appendix III).

7. Rights of Data Subjects.

7.1 Responses to Data Subjects. Customer is responsible for responding to requests from Data Subject requests to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making with respect to Personal Data (such requests individually and collectively "Data Subject Request(s)").

7.2 Company's Obligations Regarding Data Subject Requests. If Company receives a Data Subject Request in relation to Customer's Personal Data, Company will promptly inform Customer providing full details of the same and shall not respond to the communication unless specifically required by law or authorized by Customer.

7.3 Customer's Obligations Regarding Data Subject Requests. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of Processing, or withdrawal of consent to Processing of any Personal Data are communicated to Company, and for ensuring that a record of consent to Processing is maintained with respect to each Data Subject; provided that Company shall provide all reasonable and timely assistance to enable Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under applicable Data Protection Law; and (ii) any other correspondence received from a regulator or public authority in connection with the Processing of the Personal Data.

8. **Audit**.

8.1 Customer's Right to Review. Upon Customer's written request, Company shall make available for Customer's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the Processing of Personal Data.

8.2 Customer's Right to Audit. Company uses an external auditor to verify the adequacy of its security measures and controls for its Services. Upon written request, Company shall provide to Customer a copy of Company's most recent report from such audit ("Audit Report"), along with such other information as Customer shall reasonably request from Company for purposes of verifying Company's compliance with applicable Data Protection Laws; provided that the parties acknowledge and agree that the Audit Report constitutes Company's confidential information, and that Customer's receipt, review, and retention of the Audit Report shall be subject to confidentiality obligations of the Agreement and/or such other non-disclosure agreement as the parties may execute to cover the Audit Report. If the Audit Report and other information that Company provides to Customer is insufficient to fulfill Company's obligations under applicable Data Protection Law (such as, without limitation, Article 28(3)(h) of the GDPR in cases where Personal Data provided by Customer pursuant to this DPA includes Personal Data subject to the GDPR), then Company shall permit Customer to audit Company's compliance with this DPA, subject to Section 8.3 of this DPA.

8.3 Audit Conditions.

8.3.1 Customer shall be entitled to request an audit for purposes of reviewing Company's compliance with this DPA. Any such audit shall be conducted in accordance with this Section 8.3. Customer shall not be entitled to more than one audit of Company per calendar year, except (i) following the occurrence of a Security Incident, or (ii) following an instruction by a regulator or public authority, where Customer shall be entitled to arrange one (1) additional audit for that calendar year.

8.3.2 Customer's audit shall be limited to such documents, materials, information, systems, and/or Company staff as reasonably required to assess Company's compliance with this DPA. Customer shall engage an independent third party for purposes of the audit.

8.3.3 Company and Customer shall mutually agree in advance on the date, scope, duration, and security and confidentiality controls applicable to the audit; provided that the audit shall begin on a date that is no fewer than sixty (60) days following Company's receipt of Customer's written notice of request to audit, unless such requirement is expressly waived by Company in writing. To the extent that such procedures are necessary to assess Company's compliance with this DPA, Customer's audit may include (by way of example): a site visit (during normal office hours and with reasonable prior notice), review of Company's policies and procedures as reasonably related to the Personal

Data, inspection of Company’s data security infrastructure and procedures, and/or provision of such other documentary evidence as Customer shall reasonably request for purposes of verifying Company’s compliance with its obligations under this DPA. The audit shall be conducted in such a way as to not be unreasonably disruptive to Company’s business.

8.3.4 During the audit, Customer, and any third parties assisting Customer in the audit, shall strictly abide by Company’s rules and requirements regarding security and confidentiality with respect to Company’s property and/or any disclosures made by or on behalf of Company in the course of the audit. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits.

9. Security of Personal Data; Security Incidents.

9.1 Company’s Security Measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company shall maintain appropriate technical and organizational measures to protect the Personal Data from (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Personal Data. At a minimum, such measures shall include the security measures identified in Appendix II. For the avoidance of doubt, the parties agree that the security measures identified in Appendix II, as in effect on the effective date of this DPA, are reasonable and appropriate for the Processing of Data hereunder. Company may review and update its security measures from time to time, provided that any such updates are consistent with the requirements of this DPA and do not diminish the security of Company’s Processing activities with respect to the Data.

9.2 Company’s Obligations in the Event of a Security Incident. Upon becoming aware of a Security Incident, Company shall:

8.3.5 without undue delay, inform Customer of the Security Incident;

9.2.1 provide all such timely information and cooperation reasonably within Company’s abilities to enable Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) applicable Data Protection Law;

9.2.2 take such steps as Company in its sole discretion deems necessary and reasonable to remediate such Security Incident for Customer (to the extent that remediation is within Company’s abilities and reasonable control);

9.2.3 keep Customer informed of all material developments regarding the Security Incident; and

9.2.4 not notify any third parties of Personal Data being affected by a Security Incident unless: (a) Customer has agreed to such notification, and/or (b) notification is required to be made by Company under applicable Data Protection Law.

9.3 No Acknowledgment of Liability. Company’s obligation to report or respond to a Security Incident under Section 9.2 will not be construed as an acknowledgement by Company of any fault or liability with respect to a Security Incident.

10. Additional Terms for CCPA Data. The provisions of this Section 10 will apply only with respect to Personal Data that is subject to the CCPA ("CCPA Data").

10.1Defined Terms of the CCPA. The terms “service provider,” “share,” and “sell”, as used in this Section 10, are as defined in Section 1798.140 of the CCPA.

10.2Obligations Regarding CCPA Data. Company acknowledges and agrees that all CCPA Data is disclosed by Customer hereunder only for those limited and specified purposes set forth in the Agreement. Company shall comply with all obligations of the CCPA applicable to service providers, and except and unless expressly permitted by law, shall:

10.2.1 Not sell or share any CCPA Data;

10.2.2 Not retain, use or disclose any such CCPA Data for a commercial purpose other than performing the Services as set forth in the Agreement with Customer, or as otherwise expressly permitted under this DPA, the Agreement, and the CCPA;

10.2.3 Not retain, use or disclose CCPA Data to any party outside of the direct business relationship between Company and Customer;

10.2.4 Promptly notify Customer if it determines at any time that it can no longer meet its obligations under applicable Data Protection Laws;

10.2.5 Cooperate with and otherwise assist Customer's reasonable and appropriate efforts to ensure that Company Processes the CCPA Data transferred in a manner consistent with each party's obligations under the CCPA;

10.2.6 Not combine the CCPA Data relating to a specific consumer with any other data about the same consumer in Company's possession and/or control, whether received from or on behalf of another person or persons or collected by Company from its own interaction(s) with the consumer;

10.2.7 Ensure that persons authorized by Company to access the CCPA Data (which may include, without limitation, Company's employees, independent contractors, Sub-Processors, agents, and other personnel) comply with all of the foregoing obligations; and

10.2.8 To the extent required by applicable Data Protection Laws, post and/or otherwise make available a legally adequate privacy notice describing its practices with respect to Personal Data.

11. Data Processing Data Obligations (U.S. Data Protection Laws). With respect to Personal Data that is subject to U.S. Data Protection Laws: Company agrees that it shall adhere to Customer's instructions in the Processing of such Personal Data, and shall assist Customer in meeting its obligations under applicable U.S. Data Protection Laws on the terms described in this DPA.

12. Miscellaneous.

12.1Termination**.** The term of this DPA will terminate automatically without requiring any further action by either party upon the later of (i) the termination of the Agreement, or (ii) when all Personal Data is removed from Company's systems and records.

12.2Survival**.** Notwithstanding Section 12.1, Company's obligations with respect to Personal Data under this DPA shall survive so long as Company and/or its Sub-Processors Process Personal Data provided by Customer.

12.3Conflict; Invalidation**.** This DPA is subject to the terms of the Agreement; provided that, in the event of inconsistencies between the provisions of this DPA and the Agreement, this DPA shall prevail with regard to the parties' data protection obligations. If any provision of this DPA is deemed invalid or unenforceable, the invalid or unenforceable provision shall be either (i) amended to ensure its validity and enforceability while preserving the parties' intentions as closely as possible; or (ii) if that is not possible, then construed in a manner as if the invalid or unenforceable part had never been included herein. Any remaining provisions of this DPA which have not been deemed invalid or unenforceable shall remain valid and in force.

12.4Change of Law**.** If there is a change in law requiring a change to this DPA in order for each party to comply with its respective obligations under applicable Data Protection Laws, the parties will in good faith (i) negotiate an amendment to this DPA implementing that change, and (ii) take such additional actions, including (without limitation) execution and delivery of additional documents to effectuate the purposes of the amendment, as shall be reasonably necessary to comply with applicable Data Protection Laws.

By signing below, each party acknowledges that it has read and understood the terms of this DPA, including each and all Appendices attached hereto, and agrees to be bound by the terms set forth herein.

COMPANY	**CUSTOMER**
Signature: ______________________________	Signature: ______________________________
Name: ______________________________	Name: ______________________________
Title: ______________________________	Title: ______________________________
Date: ______________________________	Date: ______________________________

APPENDIX I

Details of Processing

List of Parties

Data exporter(s):

Name: Customer

Address: As set forth in the Agreement, or else as provided below.

E-mail: As set forth in the Agreement, or else as provided below.

Role: Data Controller (or Data Processor, as applicable)

Data importer(s):

Name: Maestro AI, Inc.

Address: 216 27th Ave E, Seattle, WA, 98112-5427, United States

E-mail: As set forth in the Agreement, or else as provided below.

Role: Data Processor (or Sub-processor, as applicable)

Nature and Purpose of Processing:

Personal Data shall be Processed solely in connection with and for the purpose of providing the Services to Customer, as set forth in the Agreement.

Duration of Processing:

Personal Data shall be Processed during the term of the Agreement, and may be Processed following termination only as permitted by applicable laws, rules, and regulations.

Categories of Data Subjects:

Customer may submit Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, including (without limitation) Personal Data relating to the following categories of Data Subjects: Customer's personnel or Customer's end users (to the extent that the foregoing are natural persons).

Types of Personal Data Transferred:

Customer may submit the following categories of Personal Data, the extent of which is determined and controlled by Customer in its sole discretion:

Data Type	***Examples***
Identifiers	Unique personal identifier, online identifier, account name, and other similar identifiers.
Characteristics of Protected Classifications	Characteristics of protected classifications under Data Protection Law such as gender, date of birth, and marital status.
Commercial Information	Purchase and usage history data; financial information (account details, payment information)
Internet or Other Electronic Network Activity Information	IT information (ex: computer ID, user ID and password, log files, software and hardware inventory) IT-related data (ex: IP addresses, online navigation data, browser type, language preferences, pixel data, cookies data, web beacon data)
Geolocation Data	IP address and other similar location-related information.
Professional/Employment-Related Information	Past employers, employment title, e-mail address, and other similar identifiers.
Education information	Personal information relating to a consumer's education or academics, which is not publicly available personally identifiable information, as defined in (and subject to) the Family Educational Rights and Privacy Act.
Inferences	Inferences drawn from any of the Personal Data listed above to create a profile or summary about, for example, a Data Subject's preferences and characteristics.

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

Data is transferred on a continuous basis during the term of the Agreement and this DPA.

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

Personal Data shall be retained by Company for no longer than necessary to effect the services set out in the Agreement, subject to exemptions as set forth in the DPA.

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

Company transfers the Personal Data listed above to certain Sub-Processors (as described in the DPA) for the sole purpose of facilitating Company's provision of Services under the Agreement. Sub-Processors have been instructed to retain any Personal Data Processed by Company for no longer than necessary to render sub-processing services for Company.

APPENDIX II

TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF PERSONAL DATA

Throughout the term of the DPA, Company will implement and maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data uploaded to the Services: including, at a minimum, technical and organizational measures that are reasonably calculated to achieve the following (in each case to the extent appropriate and applicable, and taking into account the nature, scope, context and purposes of the data importer's Processing of Personal Data):

- Preventing unauthorized persons from gaining access to its systems for Processing Personal Data;
- Preventing Company's systems that Process Personal Data from being used without authorization;
- Ensuring that persons authorized to access Processing Personal Data gain access only to such Personal Data in accordance with their access rights and that, in the course of Processing, Personal Data cannot be read, copied, modified or deleted beyond the scope of the granted access rights without authorization;
- Ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified;
- Establishing an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Processing;
- Protecting Personal Data against unauthorized access or disclosure of, as well as unauthorized, unlawful or accidental loss, destruction, acquisition of, or damage;
- Ensure that Personal Data is logically separated from any data or information collected by Company for different purposes.

Company may update or modify such security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services.

APPENDIX III

COMPETENT SUPERVISORY AUTHORITY

For the purposes of any personal data subject to the GDPR or the GDPR as implemented in the domestic law of the United Kingdom by virtue of Section 3 of the European Union (Withdrawal) Act 2018), where such Personal Data is Processed in accordance with the Standard Contractual Clauses, the competent supervisory authority shall be as follows:

(i) where Customer is established in an EU member state, the supervisory authority with responsibility for ensuring Customer's compliance with the GDPR shall act as competent supervisory authority; (ii) where Customer is not established in an EU member state, but falls within the extra-territorial scope of the GDPR and has appointed a representative, the supervisory authority of the EU member state in which Customer's representative is established shall act as competent supervisory authority; or (iii) where Customer is not established in an EU member state but falls within the extra-territorial scope of the GDPR without however having to appoint a representative, the supervisory authority of the EU member state in which the Data Subjects are predominantly located shall act as competent supervisory authority.

In relation to Personal Data that is subject to the U.K. GDPR, the competent supervisory authority is the United Kingdom Information Commissioner's Office, subject to the additional terms set forth in the International Data Transfer DPA to the EU Standard Contractual Clauses attached hereto as "Appendix V".

In relation to Personal Data that is subject to the Swiss DPA, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

APPENDIX IV

SWISS ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix IV amends the Standard Contractual Clauses with respect to transfers of Personal Data from Switzerland, to the extent that the Swiss DPA (as may be amended, superseded or replaced) apply to the Processing undertaken under the DPA.

The Standard Contractual Clauses shall be amended with the following modifications, in each case as applicable:

(i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(ii) references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

(iii) references to Regulation (EU) 2018/1725 shall be removed;

(iv) references to "EU", "Union" and "Member State" shall be replaced with references to "Switzerland";

(v) Clause 13(a) is not used and the "competent supervisory authority" shall be the Swiss Federal Data Protection Information Commissioner;

(vi) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "courts of Switzerland";

(vii) in Clause 17, the Standard Contractual Clauses shall be governed by the laws of Switzerland; and

(viii) to the extent the Swiss DPA applies to the Processing, Clause 18 shall be replaced to state: “Any dispute arising from these Clauses shall be resolved by the competent courts of Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts.”

APPENDIX V

U.K. INTERNATIONAL DATA TRANSFER ADDENDUM

This U.K. INTERNATIONAL DATA TRANSFER ADDENDUM ("**IDTA**") forms a part of the Data Processing Addendum ("**DPA**") entered into by and between Company and Customer, as attached hereto. Unless otherwise specified, all capitalized terms used in this IDTA have the meanings provided in the DPA.

1. Scope of IDTA. The obligations set forth in this IDTA apply solely to Personal Data subject to the U.K. GDPR that is Processed under the DPA ("**U.K. Personal Data**").

2. Incorporation of the U.K. DPA. The parties agree that the International Data Transfer DPA to the EU Commission Standard Contractual Clauses, as issued by the U.K. Information Commissioner's Office under s.119A (1) of the U.K. Data Protection Act 2018 ("**U.K. DPA**") is incorporated by reference into and forms a part of this IDTA as if fully set forth herein. Each party agrees that execution of the DPA (to which this IDTA is attached as an appendix and incorporated by reference) shall have the same effect as if the parties had simultaneously executed a copy of the U.K. DPA.

3. Interpretation of the Standard Contractual Clauses. For purposes of Processing U.K. Personal Data, any references in the DPA to the Standard Contractual Clauses shall be read to incorporate the mandatory amendments to the Standard Contractual Clauses set forth in the U.K. DPA.

4. DPA Terms. Tables 1 through 4 of the U.K. DPA shall be completed as follows:

   a. In Table 1 of the U.K. DPA, the "Start Date" shall be the effective date of the DPA, and the details and contact information for the "data exporter" and the "data importer" shall be as specified in Appendix I of the DPA.

   b. In Table 2 of the U.K. DPA:

      i. The version of the Standard Contractual Clauses incorporated by reference into the DPA shall be the version applicable to this IDTA.

      ii. Those provisions of the Standard Contractual Clauses applicable under Module Two (or, where Customer is a Data Processor, Module Three) shall apply to this IDTA.

      iii. The optional clauses and provisions of the Standard Contractual Clauses applicable to this IDTA shall be those clauses and provisions specified in the DPA.

   c. In Table 3 of the U.K. DPA, the information required in Annexes I (both 1A and 1B), II, and III shall be as provided in Appendices I, II, and III of the DPA, respectively.

   d. In Table 4 of the U.K. DPA, if the ICO issues any revisions to the U.K. DPA after the effective date of the DPA ("**ICO Revision**"), Customer and Company shall each have the right to terminate this IDTA in accordance with the U.K. DPA, the DPA, and the Agreement. Upon such termination of this IDTA:

      i. Company shall cease its Processing of the U.K. Personal Data; and

      ii. Each party shall follow the processes described of the DPA with respect to the Processing of U.K. Personal Data following termination.

   Notwithstanding the foregoing, termination of this IDTA in the event of an ICO Revision shall not terminate the DPA, the Agreement, and/or the obligations of either party arising thereunder with respect to Personal Data other than U.K. Personal Data, except and unless expressly agreed by and between the parties.

5. No Amendments. The terms of the U.K. DPA have not been amended in any way except as expressly stated herein.