CONTROLLER-TO-CONTROLLER DATA PROCESSING AGREEMENT

(December 2022)

This Controller-to-Controller Data Processing Agreement ("DPA") forms part of the Master Services Agreement between Macro Labs, Inc. ("PodRoll") and Customer (each individually a "Party" and collectively the "Parties") and all further agreements executed under it (collectively, the "Agreement") pursuant to which PodRoll provides certain services to Customer. This DPA is effective as of the execution date of the Agreement. If there is a conflict between any provision in this DPA and any provision in the Agreement, this DPA will control.

1. Definitions

(a) **"CCPA"** means the California Consumer Privacy Act of 2018, including as amended or replaced.

(b) **"Controller"** has the meaning as provided for in the GDPR.

(a) "**Data Protection Laws"** means all applicable and binding privacy and data protection laws and regulations, including (i) such laws and regulations of the European Union ("EU"), the European Economic Area ("EEA") and their Member States, Switzerland, and the United Kingdom ("UK"), as applicable to the processing of Personal Data under the Agreement including (without limitation) the GDPR, the UK GDPR, the Swiss the FADP and Member State laws; and (ii) the CCPA, as applicable to the processing of Personal Data hereunder.

(c) **"Data Subject"** has the meaning as provided for in the GDPR.

(d) **"Data Subject Request"** means a request or complaint from (or on behalf of) a Data Subject exercising his or her rights under the Data Protection Laws.

(e) "**Personal Data**" has the meaning as provided for in the GDPR.

(f) **"Personal Data Breach"** has the meaning as provided for in the GDPR.

(g) "**Processing**" has the meaning set out in the GDPR (and "**Process**" and **"Processed"** when used in relation to the Processing of Personal Data, shall be construed accordingly).

(h) "**Security Measures"** means the requirements regarding the security of the Personal Data, including the Shared Personal Data, as set out in the Data Protection Legislation (including, in particular, the measures set out in Article 32(1) of the GDPR (taking due account of the matters described in Article 32(2) of the GDPR)) as applicable.

(i) **"Shared Personal Data"** shall have the meaning as set forth herein in Section 3.

(j) **Standard Contractual Clauses"** or "**SCCs"** means Commission Implementing Decision (EU) 2021/914 of 4 Jun 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016i/679 of the European Parliament and of the Council (referencing Module One: Transfer Controller to Controller), as such standard contractual clauses are available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, and as may be amended or replaced by the European Commission from time to time.

(k) **"Swiss FADP"** means the Federal Act on Data Protection of June 19, 1992 (DPA) of Switzerland and its implementing ordinances.

(j) **"Supervisory Authority"** means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, board or other body responsible for administering Data Protection Legislation.

(k) **"UK GDPR"** means the GDPR as incorporated into UK law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019.

(l) **"UK Transfer DPA"** means the International Data Transfer DPA to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office (Version B1.0, in force as of 21 March 2022).

Terms defined in the Agreement shall have the same meaning when used in this DPA, unless otherwise defined in this DPA. Terms defined in the Data Protection Laws shall have the same meaning when used in this DPA, unless otherwise defined in this DPA.

2. Status of the Parties

The Parties are considered separate Controllers with each Party independently determining the purpose and means of processing Personal Data, including Shared Personal Data, held under its control and in accordance with its Privacy Policy or equivalent privacy statement and applicable Data Protection Laws. For avoidance of doubt, the Parties expressly state that they do not intend to enter into a Joint-Controller relationship as described in Article 26 of the GDPR.

3. Shared Personal Data

(a) Customer agrees to make available certain Personal Data to PodRoll as set forth in Section 5 of the Agreement, specifically IP addresses and user agent data of Customer's end users ("Shared Personal Data"). The Shared Personal Data is Confidential Information pursuant to Section 4 of the Agreement.

(b) The Parties agree that PodRoll may Process Shared Personal Data for its own purposes, including to provide services for the benefit of other customers.

(c) Customer shall ensure that all Shared Personal Data it makes available to PodRoll has been collected in accordance with Data Protection Laws, including providing all notices and has obtained all authorizations and/or consents necessary to provide such Shared Personal Data to PodRoll.

(d) Customer agrees to pass on to PodRoll and PodRoll will honor any (i) Do Not Sale Opt Out or Do Not Sell Request (under the CCPA or other applicable law), and (ii) GDPR consent notices from Data Subjects, as applicable to any Shared Personal Data provided by Customer to PodRoll.

4. Data Protection

(a) Each Party shall maintain and abide by a publicly available Privacy Policy or equivalent privacy statement that complies with applicable Data Protection Laws.

(b) Each Party shall ensure that any person who is authorized by it to access and/or Process Shared Personal Data (including its employees, agents and sub-processors) shall be under an appropriate contractual or statutory obligation of confidentiality.

(c) Each Party shall implement and maintain appropriate technical, administrative and physical Security Measures that are designed to (i) ensure and protect the security, integrity and confidentiality of the Shared Personal Data; and (ii) protect against any unauthorized Processing, loss, use, disclosure, acquisition of or access to any Shared Personal Data.

(d) The Parties shall notify each other without undue delay of any potential or actual Personal Data Breach and/or actions taken to prevent or mitigate the effects of such Personal Data Breach. Notwithstanding the foregoing, a Party is not required to make such notice to the extent prohibited by Data Protection Laws, and a Party may delay such notice as requested by law enforcement and/or in light of the Party's legitimate needs to investigate or remediate the matter before providing notice.

(e) The Parties agree to provide reasonable assistance as may be necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner, and to enable each Party to comply with its obligations under the Data Protection Laws.

5. Data Subject Requests

(a) Data Subjects have rights under the Data Protection Laws to (inter alia) obtain certain information about and access their Personal Data, including Shared Personal Data, and to request to amend, restrict, erase or transport their Personal Data, and object to the Processing of their Personal Data.

(b) The Parties agree to provide reasonable assistance as is necessary to each other to enable the other Party to comply with Data Subject Requests and to respond to any other queries or complaints from Data Subjects.

(c) In the event of a dispute or claim brought by a Data Subject concerning the processing of Shared Personal Data against either or both Parties, the Parties will inform each other about any such disputes or claims and will cooperate with a view to settling them amicably in a timely fashion and as may be permitted by applicable law.

6. Regulatory Compliance

(a) Each Party shall reasonably assist the other Party as may be necessary to meet its obligations to any relevant Supervisory Authority.

(b) Where and when required by Data Protection Laws, each Party will provide the relevant Supervisory Authority with information related to their Processing of Shared Personal Data.

(c) If requested, each Party will assist the other Party in the event of an investigation by a relevant Supervisory Authority.

(d) To the extent the Parties are required under the Data Protection Laws, each Party will provide reasonable assistance, including consultants with relevant Supervisory Authorities, to carry out any necessary Data Protection Impact Assessments.

7. Processors and Sub-processors

(a) The Parties (as Controllers) may use Processors (and, in turn, Sub-processors) at their discretion for Processing Shared Personal Data. Any such Processing may only occur in accordance with the written instructions of the Controller.

(b) A Party engaging a Processor (and, in turn a Sub-processor) for Processing Shared Personal Data will impose, by way of contract, no less strict data protection obligations upon all Processors (and Sub-processors) as those set out in the provisions of this DPA.

(c) In addition, the Party engaging a Processor (and, in turn a Sub-processor) for Processing Shared Personal Data will remain fully liable for any acts or omissions of its Processors (or Sub-processors) that causes the Party to breach any of its obligations under this DPA or the Data Protection Laws.

8. **Cross-Border Transfers**

(a) To the extent PodRoll's Processing of Shared Personal Data includes data subjects in the European Economic Area ("EE"), Switzerland and/or United Kingdom ("UK"), Customer and PodRoll acknowledge and agree that such Shared Personal Data may be transferred to third countries, including countries that are not recognized by the European Commission, UK or Switzerland as providing an adequate level of protection for Personal Data. More specifically, Customer acknowledges and agrees that Shared Personal Data may be transferred to PodRoll in the United States, which has not received an adequacy determination. Customer hereby consents to the transfer of Customer Personal Data to PodRoll in the United States as set forth herein.

(b) For Shared Personal Data of data subjects in the EEA, the Standard Contractual Clauses are implemented as follows:

- Clause 7, the "Docking Clause (Optional)", shall be deemed incorporated;
- Clause 9 is not applicable;
- The optional wording in Clause 11 shall be deemed not incorporated;
- Clause 17 and Clause 18, the governing law and forum shall be the Republic of Ireland; and
- Appendixes 1 and 2 attached hereto serve as Annexes I and II of the Standard Contractual Clauses.

(c) For Shared Personal Data of data subjects in Switzerland, the Standard Contractual Clauses (as revised herein) are implemented as follows:

- The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for the transfers exclusively subject to the Swiss FADP;
- The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the Standard Contractual Clauses shall be interpreted to include the Swiss FADP with respect to the transfers;
- References to Regulation (EU) 2018/1725 are removed;
- References to the "Union", "EU" and "EU Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses;
- In Clause 17 and Clause 18, the governing law and forum shall be Switzerland;
- Where the transfers are exclusively subject to the Swiss FADP, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the Swiss FADP; and
- Where the transfers are subject to both the Swiss FADP and the GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the Swiss FADP insofar as the transfers are subject to the Swiss FADP.

(d) For Customer Personal Data of data subjects in the UK, the UK Transfer DPA is implemented as follows:

A. Table 1: Parties

- The Start Date is the effective date of the Agreement.
- The Customer's and PodRoll's details and key contacts are provided in the Agreement.
- The parties' signatures on the Agreement constitute their signatures for purpose of this UK Transfer DPA.

B. Table 2: Selected SCCs, Modules and Selected Clauses

The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this UK Transfer DPA:

- Module in operation: Module One: Transfers Controller to Controller
- Clause 7 (docking clause): Yes.
- Clause 9: Not applicable
- Clause 11 (option): No
- Combined Personal Data: No

C. Table 3: Appendix Information

- Annex IA: The list of parties (Customer and PodRoll) is provided in the Agreement.
- Annex IB: Description of Transfer: A description of the transfer is provided in Appendix 1 of this DPA.
- Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: PodRoll's implemented security measures are described in Appendix 2 of this DPA.
- Annex III: Not applicable

D. Table 4: Ending this UK Transfer DPA when the Approved DPA Changes

Either Customer or PodRoll can end this UK Transfer DPA as set out in Section 19 therein.

(e) The Parties further agree that if the Standard Contractual Clauses or the UK Transfer DPA are updated, replaced or are no longer available for any reason, the parties will cooperate in good faith to implement updated or replacement Standard Contractual Clauses or UK Transfer DPA, as appropriate, or identify an alternative mechanism(s) to authorize the contemplated cross-border transfers.

9. Data Retention

The Parties shall retain or Process Shared Personal Data no longer than is necessary to carry out the purposes and obligations described in the Agreement, unless otherwise required to retain the Shared Personal Data for a longer period in accordance with upon a valid order of a relevant Supervisory Authority or court of competent jurisdiction.

9. Indemnification

Each Party indemnifies the other Party for any direct or indirect damages resulting from any breach of its obligations under this DPA and/or applicable Data Protection Laws.

10. Commencement; Duration; Survival

(a) This DPA shall commence on the same date the Agreement commences and shall last until the Agreement ends or for as long as PodRoll receives and Processes Shared Personal Data from Customer.

(b) The Parties' obligations set forth in this DPA shall survive the expiration or termination (for whatever reason) of the Agreement for as long as PodRoll receives and Processes Shared Personal Data from by Customer.

11. Anonymized Data

Customer hereby grants PodRoll the right to anonymize and aggregate Shared Personal Data (the "**Anonymized Data**") and process the Anonymized Data for the purposes of statistics, usage reporting, data analytics, industry analysis, market research, and other similar purposes.

12. Miscellaneous

(a) **Governing Law and Forum.** The governing law and forum of this DPA shall be the same as set forth in the Agreement.

(b) **Counterparts.** The Parties may execute this DPA in any number of counterparts. Each counterpart is an original and all counterparts constitute one agreement binding both Parties. Facsimile and electronic signatures will be binding for all purposes.

(c) **Construction.** Neither Party has entered into this DPA in reliance on any promise, representation, or warranty not contained herein. This DPA will be interpreted according to its plain meaning without presuming that it should favor either Party.

(d) **Entire agreement.** This DPA supersedes all prior and contemporaneous communications, whether written or oral, regarding the subject matter covered in this DPA.

(e) **No further amendment**. Except as modified by this DPA, the Agreement remains unmodified and in full force and effect.

(f) **No partnership or agency**. Nothing in this DPA nor any action taken under this DPA creates a partnership, creates a principal-agent relationship, or otherwise authorizes any Party to bind the other Party.

(g) **Severability**. If any provision in this DPA is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired thereby.

APPENDIX 1

DESCRIPTION OF DATA PROCESSING

A. LIST OF PARTIES

Data exporter(s):

Name: Customer identified in the Agreement

Address: Address listed in the Agreement

Contact person's name, position and contact details: Contact information provided in the Agreement

Activities relevant to the data transferred under these Clauses: PodRoll to deliver relevant podcast recommendations to Customer's end users.

Signature and date: Customer's signature in the Agreement

Role: Controller

Data importer(s):

Name: Macro Labs, Inc. DBA PodRoll

Address: 228 Park Ave S PMB 80012 New York, NY 10003-1502

Contact person's name, position and contact details: Contact information provided in the Agreement

Activities relevant to the data transferred under these Clauses: PodRoll to deliver relevant podcast recommendations to Customer's end users.

Signature and date: PodRoll's signature in the Agreement

Role: Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Customer's end users

Categories of personal data transferred

- IP address and/or mobile device ID
- User agent data

Sensitive data 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 specialized 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

Nature of the processing

- PodRoll processes Customer Personal Data to enhance Customer's end users' podcasting experience by providing relevant recommendations of podcasts to these end users.

Purpose(s) of the data transfer and further processing

- To provide the Services to Customer pursuant to the Agreement.

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

- For the Term set forth in the Agreement.

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

- To support PodRoll's provisioning of the Services to Customer pursuant to the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

- The competent supervisory authority is the Data Protection Commission of Ireland

APPENDIX 2

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

Data Importer has implemented the following technical and organisational measures:

1. Ensure that the Personal Data can be accessed only by authorized personnel for the purposes set forth in the Agreement and this DPA;

2. Take all reasonable measures to prevent unauthorized access to the Personal Data through the use of appropriate physical and logical (passwords) entry controls, securing areas for data processing, and implementing procedures for monitoring the use of data processing facilities;

3. Build in system and audit trails;

4. Use secure passwords, network intrusion detection technology, encryption and authentication technology, secure logon procedures and virus protection;

5. Account for all the risks that are presented by processing, for example from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of Personal Data;

6. Ensure the pseudonymization and/or encryption of Personal Data, where appropriate;

7. Maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

8. Maintain the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

9. Implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data;

10. Implement measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide services to the Subscriber;

11. Provide employee and contractor training to ensure ongoing capabilities to implement these security measures; and

12. Monitor compliance with these measures on an ongoing basis.