Data Processing Agreement (DPA)

This Data Processing Agreement including its Attachments ("***DPA***") between TUNE, Inc. ("***Supplier***") and the entity that receives any Supplier Products from Supplier (the "***Customer***") pursuant to a written or electronic agreement which governs the provision of those Supplier Products (the "***Agreement***") shall apply to the extent that (i) Supplier Processes Personal Data on behalf of the Customer, and (ii) either the Agreement expressly incorporates this DPA by reference or the parties sign this DPA.

This DPA is supplemental to, and forms an integral part of, the Agreement and is effective upon the earlier of signature or its incorporation into the Agreement, which incorporation may be specified in the Agreement or an executed amendment to the Agreement. In case of any conflict or inconsistency between the terms of the Agreement and this DPA, this DPA shall take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

The term of this DPA shall follow the Term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

1. Definitions

"California Personal Information" means Personal Data that is subject to the CCPA.

"Canadian Privacy Laws" means the data protection laws applicable in Canada and/or its provinces, in each case as hereinafter amended, supersede, or replaced, including:

(i) The Personal Information Protection and Electronic Documents Act of 2000 ("***PIPEDA***");

(ii) In Quebec: the Act to Modernize Legislative Provisions As Regards the Protection of Personal Information, also known as Law 25 (formally known as Bill 64), and the Act Respecting the Protection of Personal Information in the Private Sector, CQLR P-39.1, which is amended thereby (collectively "***Law 25***");

(iii) In Alberta: the Personal Information Protection Act [of Alberta] ("***PIPA Alberta***"); and

(iv) In British Columbia: the Personal Information Protection Act [of British Columbia] ("***PIPA BC***").

"Consumer," "Business," "Sell" and ***"Service Provider"*** shall have the meanings given to them in the CCPA.

"*Controller*" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"*Data Protection Laws*" means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, US Data Privacy Laws, and Canadian Data Privacy Laws; in each case to the extent applicable and as amended, repealed, consolidated or replaced from time to time.

"*Data Subject*" means the individual to whom Personal Data relates.

"*European Data*" means Personal Data that is subject to European Data Protection Laws.

"*European Data Protection Laws*" means data protection laws applicable in the European Union, the European Economic Area ("**EEA**") and/or their member states, Switzerland and the United Kingdom, in each case as hereinafter amended, superseded, or replaced, including:

(i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("***GDPR***");

(ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC;

(iii) Applicable national implementations of (i) and (ii); the Data Protection Act of 2018; and GDPR as it forms part of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (collectively "***UK GDPR***"); and

(iv) Swiss Federal Act on Data Protection of 19 June 1992 (as amended 25 September 2020) and its Ordinance ("***FADP***").

"*Instructions*" means the written, documented instructions issued by Customer to Supplier and directing the same to perform a specific or general action with regard to Personal Data.

"*Onward Transfer*" means a transfer of Personal Data from a third-party, such as a Processor, to a fourth-party, such as a Sub-Processor, or beyond.

"*Permitted Affiliates*" means any of Customer's Affiliates (as defined under the Agreement):

(i) That are permitted to use the Products pursuant to the Agreement, but have not signed their own separate agreement with Supplier;

(ii) For whom Supplier Processes Personal Data; and

(iii) That are subject to Data Protection Laws.

"*Personal Data*" means any information provided by or collected on behalf of Customer relating to an identified or identifiable individual where such information is protected under applicable Data Protection Laws as personal data, personal information, personally identifiable information, or any equivalent thereof.

"*Personal Data Breach*" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Supplier and/or its Sub-Processors in connection with the provision of the Products, subject to any limitations, exclusions, exceptions, or safe harbors provided for by applicable Data Protection Laws. "Personal Data Breach" shall not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems, except to the extent that this sentence conflicts with the terms of applicable Data Protections Laws.

"*Processing*" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms "Process", "Processes" and "Processed" will be construed accordingly.

"*Processor*" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

"Products" means the goods and services provided by Supplier to Customer under the Agreement.

"*Standard Contractual Clauses*" or "**SCCs**" means, for the processing of Personal Data that is subject to the GDPR, the standard contractual clauses approved pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021, as available at http://data.europa.eu/eli/dec_impl/2021/914/oj, as they may be amended, superseded, or replaced. For the Processing of Personal Data that is subject to the UK GDPR, the Standard Contractual Clauses also include the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as available at https://ico.org.uk/for-

organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/, as it may be amended, superseded, or replaced (the "**UK Addendum**").

"*Sub-Processor*" means any third-party engaged by Supplier to carry out specific Processing activities in accordance with the Instructions and subject to further limitations set forth in this DPA.

"*Third Country*" means, for the Processing of Personal Data that is subject to the GDPR, UK GDPR, or FADP, a country that is not a member of the EEA, United Kingdom, or Switzerland, respectively, and not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws).

"US Privacy Laws" means the data protection laws applicable in the United States of America and/or its states, in each case as hereinafter amended, supersede, or replaced, including:

(i) In **California**: the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (the "**CCPA**");

(ii) In **Colorado**: the Colorado Privacy Act (the "**CoPA**");

(iii) In **Connecticut**: the Connecticut Personal Data Privacy and Online Monitoring Act (the "**CPDP**");

(iv) In **Utah**: the Utah Consumer Privacy Act, which goes into effect on December 31, 2023 (the "**UCPA**"); and

(v) In **Virginia**: the Virginia Consumer Data Protection Act (the "**VCDPA**").

2. Roles of the Parties

a. Under European Data Protection Laws. With respect to European Data that is Processed under this DPA, the parties acknowledge and agree that Supplier is a Processor and Customer is either (i) a Controller, or (ii) a Processor acting on behalf of a Controller that is not a party to the Agreement or this DPA.

b. Under the CCPA. With respect to California Personal Information, the parties acknowledge and agree that Customer is a Business and Supplier is a Service Provider, unless and only to the extent that Attachment 1, Section A identifies any purposes for which Supplier Processes Personal Data as a 'third party' as that term is defined under the CCPA ("***CCPA Third Party***"), in which case Supplier is a CCPA Third Party.

c. Under US Privacy Laws, except the CCPA. With respect to Personal Data that is Processed under this DPA and governed by US Privacy Laws except the CCPA, the parties acknowledge and agree that Supplier is a Processor and Customer is either (i) a Controller, or (ii) a Processor acting on behalf of a Controller that is not a party to the Agreement or this DPA

d. Under Canadian Privacy Laws. With respect to Personal Data that is Processed under this DPA and governed by Canadian Privacy Laws, the parties acknowledge and agree that (i) Supplier Processes Personal Data on behalf of Customer and assumes the obligations under applicable Canadian Privacy Laws that apply to that role, and (ii) Customer, through its Instructions to Supplier, determines the purposes and means of the Processing of Personal Data and assumes the obligations under applicable Canadian Privacy Laws that apply that role.

3. Customer Responsibilities

a. Compliance with Laws. Customer shall be responsible for complying with all its obligations under applicable Data Protection Laws and shall inform Supplier without undue delay if it is not able to comply with its responsibilities under this sub-section (a) or applicable Data Protection Laws. In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that it shall be solely responsible for:

(i) the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data;

(ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes);

(iii) ensuring it has the right to transfer, or provide access to, the Personal Data to Supplier for Processing in accordance with the terms of the Agreement (including this DPA);

(iv) ensuring that its Instructions to Supplier regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and

(v) complying with all laws (including Data Protection Laws) applicable to any content created, sent or managed through the Products, including those relating to obtaining consents (where required) to send communications, the content of the communications, and its communication deployment practices.

b. Instructions. The parties agree that the following constitutes Customer's complete and final Instructions to Supplier in relation to the Processing of Personal Data: (i) the terms of the Agreement and this DPA, including the Attachments hereto, (ii) direction from Customer through its use of the Products in accordance with the Agreement, and (iii) this general authorization by Customer which hereby permits Supplier to use Personal Data for any business operations incident to providing the Products to Customer. Additional instructions outside the scope of the Instructions must be agreed to according to the process for amending the Agreement or this DPA, where applicable.

c. Security. Customer is responsible for independently determining whether the data security provided for in the Products adequately meets its obligations under applicable Data Protection Laws. Customer is also responsible for its secure use of the Products, including protecting account access to the Products and the security of Personal Data in transit to and from the Products (including the secure backup or encryption of any such Personal Data).

4. Supplier Obligations

a. Compliance with Instructions. Supplier shall only Process Personal Data for the purposes described in this DPA, including Attachment 1, or as otherwise agreed within the scope of Customer's lawful Instructions, except where and to the extent otherwise permitted by applicable law. Supplier is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer's industry that are not generally applicable to Supplier.

b. Conflict of Laws. If Supplier becomes aware that it can no longer meet its obligations under the applicable Data Protection Laws or Process Personal Data in accordance with Customer's Instructions due to a legal requirement under any applicable law, Supplier will:

(i) promptly notify Customer of that legal requirement to the extent permitted by the applicable law; and

(ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as Customer issues new Instructions with which Supplier is able to comply. If this provision is invoked, Supplier will not be liable to Customer under the Agreement for any failure to provide the applicable Products until such time as Customer issues new lawful Instructions with regard to the Processing.

c. Technical and Organizational Measures. Supplier shall implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Attachment 2 (*Technical and Organizational Measures*) to this DPA. Notwithstanding any provision to the contrary, Supplier may modify or update the contents of Attachment 2 at its discretion provided that such modification or update does not result in a material degradation in the technical and organizational measures set forth therein.

d. Confidentiality. Supplier shall ensure that any personnel whom Supplier authorizes to Process Personal Data on its behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

e. Personal Data Breaches. In the event that Supplier becomes aware of any Personal Data Breach, Supplier will notify Customer without undue delay, and in any case within any time period set forth in applicable Data Protection Laws. Customer hereby agrees that Supplier may, in its discretion, provide any legally required notices of Personal Data Breaches to applicable authorities and/or affected Data Subjects, provided that Customer shall have the right to propose commercially reasonable edits to any such notices; otherwise, if Supplier defers to Customer to provide any such notices then Supplier shall provide Customer with such reasonable assistance as necessary to enable Customer to provide any such notices. Customer may, at its own effort and expense, send any notices that are not required by applicable law.

f. Deletion or Return of Personal Data. Supplier will delete or return all Personal Data (including copies thereof) Processed pursuant to this DPA on termination or expiration of the Products in accordance with the procedures and timeframes set out in the Agreement, save that this requirement shall not apply to the extent Supplier is required by applicable law to retain some or all of the Personal Data, or to Personal Data that Supplier has archived on back-up systems, which data Supplier shall securely isolate and protect from any further Processing and delete in accordance with its deletion practices.

g. Demonstration of Compliance. Supplier shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and applicable Data Protection Laws and shall allow for and contribute to audits, including inspections by Customer, in order to assess compliance with this DPA and applicable Data Protection Laws. Customer acknowledges and agrees that it shall exercise its audit and inspection rights under this DPA by instructing Supplier to supply, on a confidential basis, (i) a summary copy of an independently validated report of its security programs (e.g. SOC 2, Type II Report), along with copies of any related policies and other documentation, or its hosting provider's security programs and related policies and documentation if Supplier does not host the Personal Data itself, or (ii) if Supplier does not have such a report, written responses to all reasonable requests for information made by Customer necessary to confirm Supplier's compliance with this DPA, along with copies of any related policies and other documentation. Customer shall not exercise this right to audit and inspect more than once per calendar year.

f. Supplier Assistance to Customer. To the extent required by applicable Data Protection Laws, Supplier shall assist Customer with Customer's obligations under those applicable Data Protection Laws. Such assistance may be provided through Product functionality, in which case Customer agrees to utilize such functionality before asking Supplier for further assistance.

5. Data Subject Requests

As part of Supplier's obligation under Section 4(f) above, where required by applicable Data Protection Laws, Supplier will assist Customer with Customer's obligation to respond to requests from data protection authorities and Data Subjects that seek to exercise their rights under applicable Data Protection Laws ("***Data Subject Requests***"). All Data Subject Requests must provide sufficient information for Supplier to verify the identity of the Data Subject. Customer shall reimburse Supplier for any commercially reasonable costs that arise from any such assistance that is in addition to that which Supplier normally provides to its customers.

If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to Supplier, Supplier will, to the extent that Supplier can identify Customer as the source of the Personal Data in question through its standard due diligence processes, promptly inform Customer of such Data Subject Request and will advise the Data Subject to submit their request to Customer. Customer shall otherwise be solely responsible for responding to any Data Subject Requests.

6. Data Protection Assessments

To the extent required by applicable law, Supplier will provide reasonable assistance to Customer to enable Customer to conduct and document data protection assessments, provided that the required information is reasonably available to Supplier, and Customer does not otherwise have access to the required information.

7. Sub-Processors

Customer agrees that Supplier may engage Sub-Processors to Process Personal Data on Customer's behalf. Customer hereby approves, as Sub-Processors, the entities on the list of Sub-Processors located at https://mkt.tune.com/tune-data-subprocessors.html. Any desired changes to the list of Sub-Processors must follow the amendment process set forth in Section 11(a) of this DPA.

Where Supplier engages Sub-Processors, Supplier will execute a written agreement with any Sub-Processor that imposes data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors. Supplier will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause Supplier to breach any of its obligations under this DPA.

8. International Processing

Customer acknowledges and agrees that Supplier may Process Personal Data on a global basis as necessary to provide the Products in accordance with the Agreement. Supplier shall ensure such transfers are made in compliance with the requirements of applicable Data Protection Laws.

9. Additional Provisions for European Data

a. Scope. This Section 9 (Additional Provisions for European Data) shall apply only with respect to European Data. In the event that the terms and conditions in this Section 9 conflict with those in the other sections of this DPA, the terms and conditions in this Section 9 shall take precedence.

b. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent required by European Data Protection Laws, Supplier will provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities, provided that the required information is reasonably available to Supplier, and Customer does not otherwise have access to the required information.

c. Transfer Mechanisms for Cross Border Transfers.

(i) Supplier shall not transfer, or permit any of its Sub-Processors to transfer, European Data to any Third Country, unless it first takes all such measures as are necessary to ensure the transfer will be made in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that has (A) a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, (B) achieved binding corporate rules authorization in accordance with European Data Protection Laws, or (C) executed appropriate standard contractual clauses as adopted or approved in accordance with applicable European Data Protection Laws and conducted any requisite data transfer impact assessments in conjunction therewith.

(ii) The Standard Contractual Clauses will apply if, and only to the extent that, Personal Data is transferred, either directly or via Onward Transfer, to any Third Country, (each a "***Cross Border Transfer***").

(A) With respect to Cross Border Transfers from the EEA or Switzerland to a Third Country, the iteration of the Standard Contractual Clauses set forth in Part 1 (EEA/Swiss Transfers) of Attachment 3 shall apply.

(B) With respect to Cross Border Transfers from the United Kingdom to a Third Country, the iteration of the Standard Contractual Clauses set forth in Part 2 (UK Transfers) of Attachment 3 shall apply.

(iii) Notwithstanding Section 9(c)(ii), the Standard Contractual Clauses will not apply to a Cross Border Transfer if Supplier has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Cross Border Transfers.

(iv) If and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict.

10. Additional Provisions for California Personal Information

a. Scope. This Section 10 (Additional Provisions for California Personal Information) shall apply only with respect to California Personal Information. In the event that the terms and conditions in this Section 10 conflict with those in the other sections of this DPA, the terms and conditions in this Section 10 shall take precedence.

b. Responsibilities as a Service Provider. The parties agree that when Supplier is acting as a Service Provider (see Section 2(b)) Supplier will process California Personal Information strictly for the limited purposes set forth in Attachment 1 of this DPA and as otherwise permitted by the CCPA, including the permitted purposes set forth in the 'business purpose' definition in Section 1798.140(e) (the "***Business Purposes***").

(i) As a Service Provider, Supplier shall not:

(A) combine the California Personal Information that the Supplier receives from, or on behalf of, the Customer with California Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, provided that the Supplier may combine California Personal Information to perform any Business Purposes permitted under the CCPA, and may also aggregate, deidentify, or anonymize California Personal Information so it no longer meets the California Personal Information definition, and may use such aggregated, deidentified, or anonymized data for its own research and development purposes or for any other purpose that is not prohibited under the CCPA;

(B) sell or share California Personal Information (as defined in the CCPA);

(C) retain, use, or disclose California Personal Information for any purpose, including any commercial purpose, other than for the Business Purposes or as otherwise permitted by the CCPA; or

(D) retain, use, or disclose California Personal Information outside of the direct business relationship between Customer and Supplier, unless permitted by the CCPA.

(ii) As a Service Provider, Supplier shall:

(A) comply with all applicable obligations imposed by the CCPA;

(B) provide the same level of privacy protection as is required by the Customer under the CCPA;

(C) implement reasonable security procedures and practices appropriate to the nature of the California Personal Information received to protect the California Personal Information from unauthorized or illegal access, destruction, use, modification, or disclosure;

(D) promptly comply with any Customer request or instruction requiring the Supplier to provide, amend, transfer, or delete California Personal Information, or to stop, mitigate, or remedy any unauthorized processing;

(E) provide the Customer with reasonable and appropriate steps to (1) stop and remediate unauthorized use of California Personal Information and (2) ensure that Supplier uses the California Personal Information in a manner consistent with the Customer's obligations under the CCPA; and

(F) notify Customer immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA; specifically, the Supplier must notify the Customer within seven (7) business days if it receives a verifiable consumer request under the CCPA.

c. Responsibilities as a CCPA Third Party. The parties agree that when Supplier is acting as a CCPA Third Party (see Section 2(a)) Supplier will process California Personal Information strictly for the limited purposes set forth in Attachment 1 of this DPA, including any Business Purposes and any CCPA Third Party purposes as identified therein, and as otherwise permitted by the CCPA (the "***CCPA Third Party Purposes***").

(i) As a CCPA Third Party, Supplier shall:

(A) Only use the California Personal Information for the CCPA Third Party Purposes;

(B) Comply with all applicable obligations imposed by the CCPA;

(C) Provide the same level of privacy protection as is required by the Customer under the CCPA;

(D) Implement reasonable security procedures and practices appropriate to the nature of the California Personal Information received to protect the California Personal Information from unauthorized or illegal access, destruction, use, modification, or disclosure;

(E) Permit the Customer to take reasonable and appropriate steps to (1) stop and remediate unauthorized use of California Personal Information and (2) ensure that the Supplier uses the California Personal Information in a manner consistent with the Customer's obligations under the CCPA; and

(F) Notify Customer immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA, including any request to opt out of the sale or sharing of Personal Data; specifically, the Supplier must notify the Customer within seven (7) business days if it receives a verifiable consumer request under the CCPA.

d. Certification. Supplier certifies that it understands and will comply with the restrictions set out in Section 9(b) (*Responsibilities as a Service Provider*) and Section 9(c) (*Responsibilities as a CCPA Third Party*).

11. General Provisions

a. Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 4(a) (*Compliance with Instructions*), or Section 4(c) (*Technical and Organizational Measures*), Supplier reserves the right to make any updates and changes to this DPA or list of Sub-Processors, and that any such modifications become effective thirty (30) days after the date that Supplier either (1) notifies Customer that the updated DPA or list of Sub-Processors has been posted to a particular URL, or (2) distributes the updated DPA or list of Sub-Processors to any known point-of-contact for Customer. Customer is responsible for reviewing and becoming familiar with the updated DPA or list of Sub-Processors. If, prior to the effective date of the updated DPA or list of Sub-Processors, Customer notifies Supplier of its objection to any modification of the DPA or list of Sub-Processors, then Supplier shall either (i) negotiate with Customer in good faith to resolve any such objection, or (ii) upon thirty (30) days' notice to Customer, terminate the DPA and any portion of the Agreement that governs Products which are dependent upon its execution. If Supplier exercises its right to terminate pursuant to the terms of this Section, Customer shall be entitled to a pro-rata refund of any Fees already paid by Customer for the affected Products, calculated from the effective date of any such termination.

b. Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

c. Limitation of Liability. Each party's liability, and where applicable, each of Customer's Affiliates' liability, taken in aggregate, arising out of or related to this DPA, including the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, shall be subject to the limitations and exclusions of liability set out in the Agreement. In no event shall either party's liability be limited with respect to any individual Data Subject's data protection rights under this DPA(including the Standard Contractual Clauses) or otherwise.

d. Governing Law. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

12. Parties to this DPA

a. Permitted Affiliates. Customer enters into this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Permitted Affiliates, thereby establishing a separate DPA between Supplier and each such Permitted Affiliate. Each Permitted Affiliate agrees to be bound by the obligations under this DPA. For the purposes of this DPA only, the term "Customer" shall include Customer and such Permitted Affiliates.

b. Authorization. The legal entity entering into this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

c. Remedies. Except where applicable Data Protection Laws require a Permitted Affiliate to exercise a right or seek any remedy under this DPA against Supplier directly by itself, the parties agree that: (i) solely the Customer entity that is the contracting party to the Agreement shall exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all communication with Supplier under the DPA and shall be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

TUNE, Inc.

By: 

Name: Cameron Stewart

Title: Portfolio Manager, Digital Marketing

Email Contact: legal@tune.com

Date: February 16, 2024

Attachment 1 - Details of Processing

A. Nature and Purpose of Processing
Supplier will Process Personal Data for the limited and specific purposes identified in the Agreement, including as necessary to provide the Products pursuant to the Agreement, as further specified in an Order Form or SOW, and as further instructed by Customer in its use of the Products.

B. Duration of Processing
Subject to the "Deletion or Return of Personal Data" section of this DPA, Supplier will Process Personal Data for the duration of the Agreement only, unless otherwise agreed in writing. Notwithstanding the foregoing and subject to applicable Data Protection Laws, Supplier may continue to retain Customer's Personal Data for as long as necessary to comply with Supplier's legal and regulatory obligations; to enable fraud monitoring, detection and loss prevention activities; to comply with Supplier's tax, accounting, and financial reporting obligations; and where required by Supplier's contractual commitments to third-parties. Any such processing that extends beyond the term of the Agreement shall be done in accordance with the terms of this DPA and any applicable Data Protection Laws.

C. Categories of Data Subjects
Customer may provide Personal Data relating to the following categories of Data Subjects to Supplier in the course of using the Products, or incident to the use thereof, the extent of which is determined and controlled by Customer in its sole discretion:

Customer's employees, contractors, collaborators, customers, partners, prospects, suppliers and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to Customer's end users.

D. Categories of Personal Data
Customer may provide the following categories of Personal Data to Supplier in the course of using the Products, or incident to the use thereof, the extent of which is determined and controlled by Customer in its sole discretion:

- Contact Information (e.g. name, email address, phone number, online user name(s), telephone number, IP Address, user agent, and similar information).
- Financial Information, including bank account and credit card information
- Any other Personal Data submitted by, sent to, or received by Customer, Customer's Partners, Customer's Advertisers or Customer's end users, via the Products.

E. Special categories of data (if appropriate)
The parties do not anticipate processing special categories of Personal Data or sensitive personal information, as those terms are defined under applicable Data Privacy Laws.

F. Processing operations
Personal Data will be Processed in accordance with the Agreement and this DPA and may be subject to the following Processing activities:

a. Storage and other Processing necessary to provide, maintain and improve the Products provided to Customer; and/or

b. Disclosure in accordance with the Agreement, this DPA, and/or as compelled by applicable laws.

Attachment 2 - Technical and Organizational Measures

Supplier currently observes the technical and organizational measures described in this Attachment 2 to ensure an appropriate level of Personal Data protection, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of the Data Subjects.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: Supplier hosts its Cloud Services with outsourced cloud infrastructure providers. Additionally, Supplier maintains contractual relationships with vendors in order to provide the Cloud Services in accordance with our Data Processing Agreement. Supplier relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: Supplier hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: Supplier implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Supplier's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

ii) Preventing Unauthorized Product Use

Supplier implements industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: Supplier implemented a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in Supplier's source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: Supplier maintains relationships with industry recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of Supplier's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high-risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

External access to Supplier assets is restricted, following the same least privilege model, and requires two-factor authorization and authentication. External access controls are configured and monitored by Supplier IT and Security personnel.

Background checks: All Supplier employees undergo a third-party background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: Supplier makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the Supplier products. Supplier's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Supplier stores user passwords following policies that follow industry standard practices for security. Supplier has implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: Supplier designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Supplier personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Supplier maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Supplier will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to Customer will be in accordance with the terms of the DPA or Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Supplier's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Supplier operations in maintaining and updating the product applications and backend while limiting downtime.

e) Certifications

Upon request of Customer, Supplier will provide a copy of any available independently validated report of its security programs (i.e. SOC 2, Type II, ISO 27001, etc.).

Attachment 3

Part 1 – EEA/Swiss Transfers

1) The parties agree that the terms of the Standard Contractual Clauses, as supplemented by this Part 1, are hereby incorporated by reference and shall apply to the transfer of Personal Data from the EEA or Switzerland to Third Countries.

2) Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the transfer of Personal Data to a Third Country is effectuated by Customer as the Controller of the Personal Data and Supplier is the Processor of the Personal Data.

3) Module Three (Processor to Processor) of the Standard Contractual Clauses shall apply where the transfer of Personal Data to a Third Country is effectuated by Customer as the Processor of the Personal Data and Supplier is a Sub-Processor of the Personal Data.

4) The parties acknowledge that the Standard Contractual Clauses solicit input from the parties in several clauses, and the parties agree that the following responses shall apply (to Module Two and Module Three, where applicable):

    a) Clause 7 of the SCCs shall not be applicable.

    b) In Clause 9(a), Option 2 (general written authorisation) shall apply, the time period for prior notice of Sub-Processor changes shall be thirty (30) days.

    c) In Clause 11, the optional language will not apply, and Data Subjects shall not be able to lodge a complaint with an independent dispute resolution body.

    d) In Clause 17, option 1 shall apply. The Parties agree that the Standard Contractual Clauses shall be governed by the laws of the Republic of Ireland.

    e) In Clause 18(b), the parties choose the courts of the Republic of Ireland as their choice of forum and jurisdiction.

5) Annex I.A of the SCCs shall be completed as follows (for Module Two and Module Three):

    a) "**Data Exporter**":

        i) **Name:** The entity identified as "Customer" in the DPA

        ii) **Address:** The address for Customer associated with its account or as otherwise specified in the DPA or Agreement.

        iii) **Contact person's name, position and contact details:** The contact details associated with Customer's account, or as otherwise specified in the DPA or the Agreement.

        iv) **Activities relevant to the data transferred under these Clauses:** The activities specified in Attachment 1 of the DPA.

        v) **Role (controller/processor):** With respect to Module Two, Controller; with respect to Module Three, Processor.

    b) "**Data Importer**":

        i) **Name:** TUNE, Inc.

        ii) **Address:** 11350 McCormick Rd, EP3, Suite 200, Hunt Valley, MD 21031

iii) **Contact person's name, position and contact details:** Cameron Stewart, Portfolio Manager, Digital Marketing, cameron.stewart@tune.com

iv) **Activities relevant to the data transferred under these Clauses:** The activities specified in Attachment 1 of the DPA.

v) **Role (controller/processor):** With respect to Module Two, Processor; with respect to Module Three, Processor.

c) Signature and Date: By entering into the DPA, data exporter and data importer are deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.

6) Annex I.B of the SCCs shall be completed as follows (for Module Two and Module Three):

a) **Categories of data subjects whose personal data is transferred:** Categories of data subjects are specified in Attachment 1 of the DPA.

b) **Categories of personal data transferred:** The personal data is described in Attachment 1 of the DPA.

c) **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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:** The data exporter will transfer the sensitive Personal Data listed in Section E of Attachment 1 to the DPA (if any). To the extent that data importer receives sensitive Personal Data, data importer will apply those restrictions or safeguards that are necessary and appropriate based on applicable Data Protection Laws.

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

e) **Nature of the processing:** The nature of the processing is described in Attachment 1 of the DPA.

f) **Purpose(s) of the data transfer and further processing:** The purpose of the processing is described in Attachment 1 of the DPA.

g) **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 will be retained for the later of (i) the date upon which data exporter asks data importer to delete or destroy the Personal Data in accordance with the terms of the DPA or the Agreement, and (ii) as long as permitted by applicable Data Protection Laws.

h) **For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:** The subject matter, nature and duration of the processing are described in Attachment 1 of the DPA.

7) **Annex I.C** of the SCCs shall be completed as follows: The competent supervisory authority in accordance with Clause 13 of the Standard Contractual Clauses is the supervisory authority in the Member State stipulated in Section 4(d) of this Attachment 3.

8) Attachment 2 to this DPA (Technical and Organizational Measures) serves as **Annex II** of the SCCs.

9) Section 7 of this DPA (Sub-Processors) serves as **Annex III** of the SCCs.

Part 2- UK Transfers

1) The parties agree that the terms of the Standard Contractual Clauses, as supplemented by Part 1 above and amended by the iteration of the UK Addendum attached hereto as Exhibit 1 to Attachment 3 of this DPA, are hereby incorporated by reference and shall apply to the transfer of Personal Data from the United Kingdom to Third Countries. The Standard Contractual Clauses, together with the UK Addendum, which are deemed to be amended to the extent necessary to enable them to: (a) lawfully facilitate transfers by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to such transfers; and (b) provide appropriate safeguards for the transfer in accordance with Articles 46 of the UK GDPR.

2) This Part 2 shall (a) be read and interpreted in the light of the provisions of UK GDPR and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 of the UK GDPR, and (b) not be interpreted in a way that conflicts with rights and obligations provided for in the UK GDPR.

3) Any references to legislation, including the UK Addendum, mean that legislation, as may be amended from time to time (including consolidation, reenactment or replacement of such legislation following the Effective Date of this DPA).

4) To the extent there is any conflict between the Standard Contractual Clauses, together with the UK Addendum, and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses, together with the UK Addendum, will prevail.

Exhibit 1 to Attachment 3 – International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

Part 1: Tables

Table 1: Parties

Start date	Upon the effective date of the DPA.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: As stated in Part I, Section 5(a) of Attachment 3 to the DPA Trading name (if different): Main address (if a company registered address): As stated in Part I, Section 5(a) of Attachment 3 to the DPA Official registration number (if any) (company number or similar identifier):	Full legal name: As stated in Part I, Section 5(b) of Attachment 3 to the DPA Trading name (if different): Main address (if a company registered address): As stated in Part I, Section 5(b) of Attachment 3 to the DPA Official registration number (if any) (company number or similar identifier):
Key Contact	As stated in Part I, Section 5(a) of Attachment 3 to the DPA	As stated in Part I, Section 5(b) of Attachment 3 to the DPA
Signature (if required for the purposes of Section 2)	NOT REQUIRED	NOT REQUIRED

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: June 4, 2021 template, effective on the Start Date listed above Reference (if any): Other identifier (if any): Or ☐ 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 Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As stated in Part I, Section 5 of Attachment 3 to the DPA
Annex 1B: Description of Transfer: As stated in Part I, Section 6 of Attachment 3 to the DPA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As stated in Part I, Section 8 of Attachment 3 to the DPA
Annex III: List of Sub processors (Modules 2 and 3 only): As stated in Part I, Section 9 of Attachment 3 to the DPA

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**6: ☒ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.