Data Protection Addendum

This Data Protection Addendum ("**DPA**") forms a part of the Master Services Agreement or other separate written agreement (the "**Agreement**") by and between Mozart Data, Inc. ("**Mozart**") and the customer named in the Agreement (the "**Customer**"), which incorporates this DPA by reference. Capitalized terms not defined in this DPA are defined in the Agreement.

1. **Definitions**.

1.1. "**Audit**" and "**Audit Parameters**" are defined in Section 9.3 below.

1.2. "**Audit Report**" is defined in Section 9.2 below.

1.3. "**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 Processing of Personal Data.

1.4. "**Customer Instructions**" is defined in Section 3.1 below.

1.5. "**Customer Personal Data**" means Personal Data in Customer Data (as defined in the Agreement).

1.6. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("**CCPA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

1.7. "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

1.8. "**EEA**" means European Economic Area.

1.9. "**Personal Data**" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

1.10. "**Processing**" and inflections thereof refer to any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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

1.12. "**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Customer Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination or (iii) where FADP applies, a transfer of Customer Personal Data from Switzerland to any other country that is not subject to an adequacy determination.

1.13. "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data being Processed by Mozart.

1.14. "**Specified Notice Period**" is 48 hours.

1.15. "**Subprocessor**" means any third party authorized by Mozart to Process any Customer Personal Data.

1.16. "**Subprocessor List**" means the list of Mozart's Subprocessors as identified on Schedule 5 (Subprocessors).

2. Scope and Duration.

2.1. **Roles of the Parties**. This DPA applies to Mozart as a Processor of Customer Personal Data and to Customer as a Controller or Processor of Customer Personal Data.

2.2. **Scope of DPA**. This DPA applies to Mozart's Processing of Customer Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

2.3. **Duration of DPA**. This DPA commences on the Effective Date of the Agreement and terminates upon expiration or termination of the Agreement (or, if later, the date on which Mozart has ceased all Processing of Customer Personal Data).

2.4. **Order of Precedence**. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) any Standard Contractual Clauses or other measures to which the parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms), (2) this DPA and (3) the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

3. Processing of Personal Data.

3.1. **Customer Instructions.**

(a) Mozart will Process Customer Personal Data as a Processor only: (i) in accordance with Customer Instructions or (ii) to comply with Mozart's obligations under applicable laws, subject to any notice requirements under Data Protection Laws.

(b) "**Customer Instructions**" means: (i) Processing to provide the Service and perform Mozart's obligations in the Agreement (including this DPA) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Agreement.

(c) Details regarding the Processing of Customer Personal Data by Mozart are set forth in Schedule 1 (Subject Matter and Details of Processing).

(d) Mozart will notify Customer if it receives an instruction that Mozart reasonably determines infringes Data Protection Laws (but Mozart has no obligation to actively monitor Customer's compliance with Data Protection Laws).

3.2. **Confidentiality**.

(a) Mozart will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.

(b) Mozart will ensure personnel who Process Customer Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

3.3. **Compliance with Laws.**

(a) Mozart and Customer will each comply with Data Protection Laws in their respective Processing of Customer Personal Data.

(b) Customer will comply with Data Protection Laws in its issuing of Customer Instructions to Mozart. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Mozart to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects.

3.4. **Changes to Laws**. The parties will work together in good faith to negotiate an amendment to this DPA as either party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

4. Subprocessors.

4.1. **Use of Subprocessors.**

(a) Customer generally authorizes Mozart to engage Subprocessors to

Process Customer Personal Data. Customer further agrees that Mozart may engage its Affiliates as Subprocessors.

(b) Mozart will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (ii) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Mozart to breach any of its obligations under this DPA.

4.2. **Subprocessor List**. Mozart will maintain an up-to-date list of its Subprocessors, including their functions and locations, as specified in the Subprocessor List.

4.3. **Notice of New Subprocessors**. Mozart may update the Subprocessor List from time to time. At least 30 days before any new Subprocessor Processes any Customer Personal Data, Mozart will add such Subprocessor to the Subprocessor List and notify Customer through email.

4.4. **Objection to New Subprocessors.**

(a) If, within 30 days after notice of a new Subprocessor, Customer notifies Mozart in writing that Customer objects to Mozart's appointment of such new Subprocessor based on reasonable data protection concerns, the parties will discuss such concerns in good faith.

(b) If the parties are unable to reach a mutually agreeable resolution to Customer's objection to a new Subprocessor, Customer, as its sole and exclusive remedy, may terminate the Order for the affected Service for convenience and Mozart will refund any prepaid, unused fees for the terminated portion of the term of a Subscription.

5. Security.

5.1. **Security Measures.** Mozart will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against Security Incidents, in accordance with Mozart's Security Measures referenced in the Agreement and as further described in Schedule 2 (Technical and Organizational Measures). Mozart will regularly monitor its compliance with its Security Measures and Schedule 2 (Technical and Organizational Measures).

5.2. **Incident Notice and Response.**

(a) Mozart will implement and follow procedures to detect and respond to Security Incidents.

(b) Mozart will: (i) notify Customer without undue delay and, in any event,

not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Mozart's reasonable control.

(c) Upon Customer's request and taking into account the nature of the applicable Processing, Mozart will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws.

(d) Customer acknowledges that Mozart's notification of a Security Incident is not an acknowledgement by Mozart of its fault or liability.

(e) Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3. **Customer Responsibilities.**

(a) Customer is responsible for reviewing the information made available by Mozart relating to data security and making an independent determination as to whether the Service meets Customer's requirements and legal obligations under Data Protection Laws.

(b) Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

6. Data Protection Impact Assessment. Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to Mozart, Mozart will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Customer's use of the Service, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

7. Data Subject Requests.

7.1. **Assisting Customer**. Upon Customer's request and taking into account the nature of the applicable Processing, Mozart will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Service).

7.2. **Data Subject Requests**. If Mozart receives a request from a Data Subject in relation to the Data Subject's Customer Personal Data, Mozart will notify Customer and advise

the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

8. Data Return or Deletion.

8.1. **During Subscription**. During the term of a Subscription, Customer may, through the features of the Service or via written request to Mozart, access, return to itself or delete Customer Personal Data.

8.2. **Post Termination.**

(a) Following termination or expiration of the Agreement, Mozart will, in accordance with its obligations under the Agreement, delete all Customer Personal Data from Mozart's systems.

(b) Deletion will be in accordance with industry-standard secure deletion practices. Mozart will issue a certificate of deletion upon Customer's request.

(c) Notwithstanding the foregoing, Mozart may retain Customer Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Mozart will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data and (y) not further Process retained Customer Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

9. Audits.

9.1. **Mozart Records Generally**. Mozart will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request, make available to Customer any records reasonably necessary to demonstrate compliance with Mozart's obligations under this DPA and Data Protection Laws.

9.2. **Third-Party Compliance Program**.

(a) Mozart will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Customer upon Customer's written request at reasonable intervals (subject to confidentiality obligations).

(b) Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.

(c) Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 9.3 (Customer Audit) below.

9.3. **Customer Audit**.

(a) Subject to the terms of this Section 9.3, Customer has the right, at Customer's expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with Mozart that is consistent with the Audit Parameters (an "**Audit**").

(b) Customer may exercise its Audit right: (i) to the extent Mozart's provision of an Audit Report does not provide sufficient information for Customer to verify Mozart's compliance with this DPA or the parties' compliance with Data Protection Laws, (ii) as necessary for Customer to respond to a government authority audit or (iii) in connection with a Security Incident.

(c) Each Audit must conform to the following parameters ("**Audit Parameters**"): (i) be conducted by an independent third party that will enter into a confidentiality agreement with Mozart, (ii) be limited in scope to matters reasonably required for Customer to assess Mozart's compliance with this DPA and the parties' compliance with Data Protection Laws, (iii) occur at a mutually agreed date and time and only during Mozart's regular business hours, (iv) occur no more than once annually (unless required under Data Protection Laws or in connection with a Security Incident), (v) cover only facilities controlled by Mozart, (vi) restrict findings to Customer Personal Data only and (vii) treat any results as confidential information to the fullest extent permitted by Data Protection Laws.

10. Cross-Border Transfers/Region-Specific Terms.

10.1. **Cross-Border Data Transfers.**

(a) Mozart (and its Affiliates) may Process and transfer Customer Personal Data globally as necessary to provide the Service.

(b) If Mozart engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

10.2. **Region-Specific Terms**. To the extent that Mozart Processes Customer Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.

[*Remainder of page intentionally blank*]

Schedule 1: Subject Matter and Details of Processing

Customer / 'Data Exporter' Details

Name:	As provided in the Agreement
Contact details for data protection:	As provided in the Agreement
Main address:	As provided in the Agreement
Role:	Controller

Mozart / 'Data Importer' Details

Name:	Mozart Data, Inc.
Contact details for data protection:	support@mozartdata.com
Main address:	Mozart Data 750 N San Vicente Blvd Suite 800W West Hollywood CA, 90069
Mozart activities:	Provision of the service described in the Agreement
Role:	Processor

Details of Processing

Categories of Data Subjects:	Customer's users, customers, prospective customers, employees, suppliers, business partners, and such other Data Subjects as determined by Customer in Customer's use of the Service.

Categories of Customer Personal Data:	Contact details, business related information, online identifiers, HR related information, account credentials, access logs, and such other Personal Data as determined by Customer in Customer's use of the Service.
Sensitive Categories of Data and additional associated restrictions/safeguards:	N/A
Frequency of transfer:	Continuous throughout the provision of the Service.
Nature of the Processing:	All operations such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means), etc.
Purpose of the Processing:	The provision of the Services in accordance with the Agreement.
Duration of Processing / retention period:	Personal Data will be retained during the term of the Agreement and will be deleted in accordance with the terms thereof.
Transfers to Subprocessors:	The subject matter of the Processing is Customer Personal Data, the nature of the Processing is the performance of the Services under the Agreement and as detailed above and the duration of the Processing is the term of the Agreement.

Schedule 2: Technical and Organizational Security Measures

Mozart maintains a suite of Information Security Policies and Procedures as a framework for continuous improvement of security. A part of these is Mozart's Technical and Organizational Security Measures will include, but not be limited to, the following:

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of Mozart's information security program.
2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Mozart's organization, monitoring and maintaining compliance with Mozart's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.
3. Data security controls which include at a minimum, but may not be limited to, logical segregation of access to data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available and industry standard encryption technologies for Personal Data that is:
    a. transmitted over public networks (i.e. the Internet) or when transmitted wirelessly; or
    b. at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives).
4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access when employment terminates or changes in job functions occur).
5. Password controls designed to manage and control password strength, expiration, and usage.
6. Use of data centers that enforce physical and environmental security controls designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
7. Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to Mozart's technology and information assets.
8. Incident response procedures designed to allow Mozart to investigate, respond to, mitigate and notify of events related to Mozart's technology and information assets.
9. Network security controls that provide for the use of firewalls, intrusion detection systems, and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
10. Vulnerability assessment and threat protection technologies, including file integrity monitoring, malware detection, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
11. Secure development procedures based on secure system engineering principles, including the use of version control, restrictions on changes to third-party packages, and security testing designed to ensure the security of the applications that are produced.

12. Business continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Mozart may update or modify such Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

Schedule 3: Cross-Border Transfer Mechanisms

1. **Definitions**. Capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

1.2. "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022.

1.3. In addition:

"**Designated EU Governing Law**" means:	The law of the EU Member State where Customer is headquartered
"**Designated EU Member State**" means:	The EU Member State where Customer is headquartered

1.4. **EU Transfers**. Where Customer Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:

1.5. The EU SCCs are hereby incorporated by reference as follows:

(a) Module 2 (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and Mozart is a Processor of Customer Personal Data;

(b) Module 3 (Processor to Processor) applies where Customer is a Processor of Customer Personal Data (on behalf of a third-party Controller) and Mozart is a Processor of Customer Personal Data;

(c) Customer is the "data exporter" and Mozart is the "data importer"; and

(d) by entering into this DPA, each party is deemed to have signed the EU SCCs (including their Annexes) as of the Effective Date of the Agreement.

1.6. For each Module, where applicable the following applies:

(a) the optional docking clause in Clause 7 does not apply;

(b) in Clause 9, Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of this DPA, and Mozart shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with Section 4.3 of this DPA;

(c) in Clause 11, the optional language does not apply;

(d) in Clause 13, all square brackets are removed with the text remaining;

(e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Designated EU Governing Law;

(f) in Clause 18(b), disputes will be resolved before the courts of the Designated EU Member State;

(g) Schedule 1 (Subject Matter and Details of Processing) to this DPA contains the information required in Annex 1 of the EU SCCs; and

(h) Schedule 2 (Technical and Organizational Measures) to this DPA contains the information required in Annex 2 of the EU SCCs.

1.7. Where context permits and requires, any reference in this DPA to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this Section 2.

2. **Swiss Transfers**. Where Customer Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:

2.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

(a) in Clause 13, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner;

(b) in Clause 17 (Option 1), the EU SCCs will be governed by the laws of Switzerland;

(c) in Clause 18(b), disputes will be resolved before the courts of Switzerland;

(d) the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c); and

(e) all references to the EU GDPR in this DPA are also deemed to refer to the FADP.

3. **UK Transfers**. Where Customer Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:

3.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

(a) each party shall be deemed to have signed the "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119 (A) of the Data Protection Act 2018;

(b) the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Customer Personal Data;

(c) in Table 1 of the UK Addendum, the parties' key contact information is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(d) in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules and selected clauses which this UK Addendum is appended to are located above in this Schedule 3;

(e) in Table 3 of the UK Addendum:

(i) the list of parties is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(ii) the description of transfer is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(iii) Annex II is located in Schedule 2 (Technical and Organizational Measures) to this DPA; and

(iv) the list of Subprocessors is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA.

(f) in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and

(g) in Part 2: 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 section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses.

Schedule 4: Region-Specific Terms

A. **CALIFORNIA**

1. **Definitions**. CCPA and other capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA.

1.2. The definition of "Data Subject" includes "consumer" as defined under the CCPA.

1.3. The definition of "Controller" includes "business" as defined under the CCPA.

1.4. The definition of "Processor" includes "service provider" as defined under the CCPA.

2. **Obligations**.

2.1. Customer is providing the Customer Personal Data to Mozart under the Agreement for the limited and specific business purposes of providing the Service as described in Schedule 1 (Subject Matter and Details of Processing) to this DPA and otherwise performing under the Agreement.

2.2. Mozart will comply with its applicable obligations under the CCPA and provide the same level of privacy protection to Customer Personal Data as is required by the CCPA.

2.3. Mozart acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 9 (Audits) of this DPA to help to ensure that Mozart's use of Customer Personal Data is consistent with Customer's obligations under the CCPA, (ii) receive from Mozart notice and assistance under Section 7 (Data Subject Requests) of this DPA regarding consumers' requests to exercise rights under the CCPA and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

2.4. Mozart will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA.

2.5. Mozart will not retain, use or disclose Customer Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Section 2.1 of this Section A (California) of Schedule 4 or (ii) outside of the direct business relationship between Mozart with Customer, except, in either case, where and to the extent permitted by the CCPA.

2.6. Mozart will not sell or share Customer Personal Data received under the Agreement.

2.7. Mozart will not combine Customer Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA.

3. **Activity Prior to January 1, 2023**. To the extent this Section A (California) of Schedule 4 is in effect prior to January 1, 2023, Mozart's obligations hereunder that are required solely by amendments to the CCPA made by the California Privacy Rights Act regarding contractual obligations of service providers shall only apply on and after January 1, 2023.

Schedule 5: Subprocessors

Mozart uses certain Subprocessors to assist it in providing to its customers the Services as described in the DPA and the Agreement. Mozart engages the following Subprocessors to perform various functions as explained in the table below:

Subprocessor Name	Type of Service	Corporate Location	Storage Location
Snowflake, Inc.	Database Service Provider	USA	USA/EU
Fivetran, Inc.	ETL Service Provider	USA	USA/EU
Google, LLC	Cloud Service Provider	USA	USA/EU