Temporal Technologies Inc.
Data Processing Addendum

Effective as of October 10, 2024

This Data Processing Addendum (the "**DPA**"), including its Exhibits, forms a part of the Order Form and Terms of Service or other written agreement entered into by the Parties (the "**Agreement**") between Temporal Technologies Inc. ("**Temporal**") and Customer ("**Customer**") (Customer together with Temporal the "**Parties**") and defines how Temporal and Customer agree to treat Personal Data (as defined below) that is contained in Customer Data.

1. **Definitions**.
    a. "**Agreement**" means, as applicable, the Terms of Service ("ToS"), or similar commercial agreement by and between Temporal and Customer with respect to the Service.
    b. "**Applicable Privacy Law**" the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**") and 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**") (together, collectively, the "**GDPR**"), each as applicable, and as may be amended or replaced from time to time.
    c. "**Customer Data**" means any data, information or other material provided, uploaded, or submitted by Customer to the Service in the course of using the Service.
    d. "**Customer Personal Data**" means the Personal Data that is included in the Customer Data that Temporal processes on Customer's behalf.
    e. "**Data Subject**" has the meaning given to it in the Applicable Privacy Law.
    f. "**European Economic Area**" or "**EEA**" means the Member States of the European Union together with Iceland, Norway and Liechtenstein.
    g. "**International Data Transfer**" means any disclosure of Personal Data by an organization subject to Applicable Privacy Law to another organization located outside the EEA and the UK;
    h. "**Temporal Security Policy and Privacy Guidelines**" means the security standards attached to, and incorporated into, this DPA as Annex 2.
    i. "**Personal Data**" has the meaning given to it in the Applicable Privacy Law.
    j. "**Personal Data Breach**" has the meaning given to it in the Applicable Privacy Law.
    k. "**Processing**" has the meaning given to it in the Applicable Privacy Law, and "**Process**" will be interpreted accordingly.
    l. "**Service**" means the Temporal services received by Customer as set forth in the corresponding ordering document agreed to in writing by Temporal.
    m. "**Standard Contractual Clauses**" means the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), C/2021/3972, OJ L 199, 7.6.2021, p. 31–61, as amended or replaced from time to time, available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en;
    n. "**Subprocessor**" has the meaning given to it in the Standard Contractual Clauses.
    o. "**Subprocessor List**" means the list of Subprocessors currently authorised by Temporal to process Customer Personal Data.
    p. "**ToS**" means Temporal's standard terms and conditions with respect to the Services available at the following URL: www.temporal.io/tos
    q. **"UK Addendum**" means the addendum to the Standard Contractual Clauses issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022), available at: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.
    r. **"U.S. State Privacy Laws**" means, collectively, all U.S. state privacy laws and their implementing regulations, as amended or superseded from time to time, that apply generally to the processing of individuals' Personal Data and that do not apply solely to specific industry sectors (e.g., financial institutions), specific demographics (e.g., children), or specific classes of information (e.g., health or biometric information). State Privacy Laws include the following:
        (i) California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (California Civil Code §§ 1798.100 to 1798.199) ("CPRA");
        (ii) Colorado Privacy Act (Colorado Rev. Stat. §§ 6-1-1301 to 6-1-1313) ("ColoPA");

(iii) Connecticut Personal Data Privacy and Online Monitoring Act (Public Act No. 22-15) ("CPOMA");
(iv) Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 to 13-61-404) ("UCPA"); and
(v) Virginia Consumer Data Protection Act (Virginia Code Ann. §§ 59.1-575 to 59.1-585) ("VCDPA").

2. Scope and Application. This DPA shall apply when Customer Personal Data is transferred to Temporal from any Customer or Customer's affiliates who are subject to the Applicable Privacy Law. In this context, Customer may act as "controller" and Temporal may act as "processor" respectively with respect to the Customer Personal Data.

3. Data Processing.

a. Instructions for Data Processing. Temporal will process Customer Personal Data only in accordance with Customer's lawful instructions and in compliance with the Agreement, and will not process Customer Personal Data for any purpose other than to provide the Service. Processing outside of the scope of the Agreement will require the prior written agreement of the parties on the additional instructions for Processing.
b. Required Consents. Where required by Applicable Privacy Law, Customer represents and warrants that it has obtained and/or will obtain all necessary consents and permissions required for the transfer of Customer Personal Data to, and Processing of Customer Personal Data by, Temporal in accordance with the Agreement.
c. Compliance with Laws. Each party will comply with all applicable laws, rules, and regulations (including all applicable data protection law) in its performance of this DPA.
d. Data Exports. Customer represents and warrants that it has first obtained all necessary consents under Applicable Privacy Law with respect to the Processing or transfer of Customer Personal Data originating from inside the EEA and the UK.
e. U.S. State Processing. If Temporal processes Personal Data governed by U.S. State Privacy Laws on behalf of Customer in its provision of the Services, Exhibit A shall apply to Temporal's processing of such Personal Data.

4. Security Responsibilities of Temporal.

a. Security Measures. Temporal shall implement and maintain appropriate technical and organizational security measures designed to protect the security, integrity and confidentiality of the Customer Personal Data described in the Temporal Security Policy and Privacy Guidelines. The Customer acknowledges that the Temporal Security Policy and Privacy Guidelines are appropriate in relation to the risks associated with Customer's intended Processing, and will notify Temporal prior to any intended Processing for which Temporal's security measures may not be appropriate.
b. Temporal Personnel. Temporal shall restrict access by Temporal personnel to Customer Personal Data (i) to only those personnel who need to access the Customer Personal Data in order to provide the Service; (ii) provided that said personnel authorized to process Customer Personal Data are subject to an obligation of confidentiality; and (iii) as set out in the Temporal Security Policy and Privacy Guidelines.
c. Records. Temporal shall maintain relevant records with respect to Temporal's information security practices, and shall provide copies of such records as reasonably required by Customer to verify Temporal's compliance with this DPA.
d. Audit by Customer. Customer (or its third party independent auditors) may audit Temporal's compliance with the security measures set out in the Temporal Security Policy and Privacy Guidelines. Any such audit: (i) will be subject to Customer giving reasonable prior written notice to Temporal, and not conducted more than once per calendar year; (ii) will be performed at Customer's sole expense; and (iii) will be carried out by Customer in such a way as to mitigate any disruption to Temporal's business.
e. Personal Data Breach Notification. Temporal will notify Customer without undue delay after becoming aware of a Personal Data Breach involving Customer Personal Data. If Temporal's notification is delayed, it will be accompanied by reasons for the delay. Any such notification shall not be construed as an acknowledgement by Temporal of any fault or liability with respect to the unauthorised access.

5. Subprocessors.

a. Authorised Subprocessors. Customer agrees that Temporal may use Subprocessors to fulfill its obligations under the Agreement. Customer hereby consents to Temporal's use of Subprocessors listed in Annex 3 to this Data Protection Agreement. Before Temporal authorises any new Subprocessor to process Customer Personal Data, Temporal will update the published Subprocessor List or

will otherwise notify Customer in writing of the identity of any new Subprocessor. Customer may object in writing to the use of any new Subprocessor within fifteen (15) days of the publishing of a new Subprocessor list, provided that the written objection includes reasonable grounds for the objection. If Temporal elects to use any new Subprocessor Customer previously objected to pursuant to this Section 5, Customer may terminate the ToS by providing Temporal written notice of termination prior to the date Temporal begins to use such Subprocessor.

b. Subprocessor Obligations. Where Temporal authorises a Subprocessor to process Customer Personal Data as described in this section 5, Temporal will enter into a written agreement with each such Subprocessor that contains provisions that are consistent to those contained in this DPA. Except as set forth in this DPA or as otherwise authorised in writing by Customer, Temporal will not permit any Subprocessors to process Customer Personal Data.

6. International Data Transfers

a. Customer hereby authorizes Temporal to perform International Data Transfers to any country deemed adequate by the European Commission or the competent authorities, as appropriate; on the basis of adequate safeguards in accordance with Applicable Privacy Law; or pursuant to the Standard Contractual Clauses referred to in Section 6.b and 6.c.

b. By signing this DPA, Customer and Temporal conclude Module 2 (controller-to-processor) of the Standard Contractual Clauses and, to the extent Customer is a Processor on behalf of a third-party controller, Module 3 (Processor-to-Subprocessor) of the Standard Contractual Clauses, which are hereby incorporated and completed as follows: the "data exporter" is Customer; the "data importer" is Temporal; the optional docking clause in Clause 7 is implemented; Option 2 of Clause 9(a) is implemented and the time period therein is 15 days; the optional redress clause in Clause 11(a) is struck; Option 1 in Clause 17 is implemented and the governing law is the law of Ireland ; the courts in Clause 18(b) are the Courts of Dublin, Ireland; Annex I, II and III to Module 2 of the Standard Contractual Clauses are Annex 1, 2 and 3 to this DPA respectively.

c. By signing this DPA, Customer and Temporal conclude the UK Addendum, which is hereby incorporated and applies to International Data Transfers outside the UK. Part 1 of the UK Addendum is completed as follows: (i) in Table 1, the "Exporter" is Customer and the "Importer" is Temporal, their details are set forth in this DPA, and the Agreement; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are the Standard Contractual Clauses referred to in Section 6.b of this DPA; (iii) in Table 3, Annexes 1 (A and B) to the "Approved EU SCCs" are Annex 1, 2, 3 to this DPA respectively; and (iv) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.

d. If Temporal's compliance with Applicable Privacy Law relating to International Data Transfers is affected by circumstances outside of Temporal's control, including if a legal instrument for International Data Transfers is invalidated, amended, or replaced, then Customer and Temporal will work together in good faith to reasonably resolve such non-compliance. In the event that additional, replacement or alternative Standard Contractual Clauses or UK Standard Contractual Clauses are approved by supervisory authorities, Temporal reserves the right to amend the Agreement and this DPA by adding to or replacing, the Standard Contractual Clauses or UK Standard Contractual Clauses that form part of it at the date of signature in order to ensure continued compliance with Applicable Privacy Law.

e. Supplementary Measures. In respect of any International Data Transfer, the following supplementary measures shall apply:

(i) As of the date of this Addendum, Temporal has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Customer Personal Data is being exported, for access to (or for copies of) Personal Data ("Government Agency Requests");

(ii) If, after the date of this Addendum, Temporal receives any Government Agency Requests, Temporal shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Temporal may provide Customer's basic contact information to the government agency. If compelled to disclose Temporal's Personal Data to a law enforcement or government agency, Temporal shall give Customer reasonable notice of the demand and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Temporal is legally prohibited from doing so. Temporal shall not voluntarily disclose Customer Personal Data to any law enforcement or government agency. Customer and Temporal shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Customer Personal Data pursuant to this Addendum should be suspended in the light of such Government Agency Requests; and

(iii) The Customer and Temporal will meet regularly to consider whether:
(1) the protection afforded by the laws of the country of Temporal to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;
(2) additional measures are reasonably necessary to enable the transfer to be compliant with the Applicable Privacy Laws; and
(3) it is still appropriate for Customer Personal Data to be transferred to Temporal, taking into account all relevant information available to the Parties, together with guidance provided by the supervisory authorities.
(iv) If Applicable Privacy Laws require the Customer to execute the Standard Contractual Clauses applicable to a particular transfer of Customer Personal Data to Temporal as a separate agreement, Temporal shall, on request of the Customer, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Customer to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant applicable Data Protection Laws.
(v) If either (i) any of the means of legitimizing transfers of Customer Personal Data outside of the EEA or UK set forth in this Addendum cease to be valid or (ii) any supervisory authority requires transfers of Customer Personal Data pursuant to those means to be suspended, Temporal agrees to amend the means of legitimizing transfers or alternative arrangements with Customer, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Applicable Privacy Laws.

7. Cooperation.

a. Temporal shall notify Customer of any requests received directly by Temporal from Data Subjects and shall provide to Customer such reasonable assistance as is required for Customer to comply with such Data Subject requests. Temporal shall only respond directly to such Data Subject requests on receiving Customer's written request and consent, provided that (to the extent permitted by Applicable Privacy Law) Customer shall be responsible for all reasonable costs arising from Temporal's provision of such assistance.
b. To the extent required under Article 28(3) GDPR, Temporal will assist Customer to comply with Articles 35 & 36 GDPR; in particular, upon reasonable request, Temporal will assist Customer to carry out data protection impact assessments and to consult where necessary with data protection authorities.
c. Following Customer’s request, Temporal shall destroy all Customer Personal Data in its possession. This requirement shall not apply to the extent that Temporal is required by any applicable law to retain some or all of the Customer Personal Data, in which case, Temporal shall use reasonable efforts to isolate and protect the Customer Personal Data from any further Processing except to the extent required by such law. Temporal may charge a reasonable fee for assistance under this Section 7.

8. Limitation of Liability. IN NO EVENT SHALL TEMPORAL BE LIABLE FOR ANY LOST DATA, LOST PROFITS, BUSINESS INTERRUPTION, REPLACEMENT SERVICE OR OTHER SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR INDIRECT DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THEORY OF LIABILITY. TEMPORAL’S LIABILITY FOR ALL CLAIMS ARISING UNDER THIS DPA, WHETHER IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE AMOUNT OF FEES PAID OR PAYABLE BY CUSTOMER UNDER THE AGREEMENT DURING THE TWELVE (12) MONTH PERIOD PRECEEDING THE CLAIM.

9. General.

a. Termination. This DPA will terminate automatically upon termination of the Agreement.
b. Conflict. In the event of a conflict between the Agreement and this DPA, the terms of this DPA will take precedence to the extent of the conflict. In the event of a conflict between the Standard Contractual Clauses and the remaining terms of this DPA, the Standard Contractual Clauses will take precedence to the extent of the conflict. Nothing in this DPA modifies the Standard Contractual Clauses or affects any third party's rights under the Standard Contractual Clauses.

Annex 1 to the Data Processing Addendum

DESCRIPTION OF THE TRANSFER

A. LIST OF PARTIES

Data Exporter:

- Name: As designated by Customer in the Order Form to the Agreement.
- Address: As designated by Customer in the Order Form to the Agreement.
- Contact person's name, position, and contact details: As designated by Customer in the Order Form to the Agreement.
- Activities relevant to the data transferred under these Clauses: Customer receives Temporal's Services as described in the Agreement, and Temporal processes Customer Personal Data in that context.
- Signature and date: By entering into this Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.
- Role (controller/processor): Controller or Processor on behalf of Third-Party Controller.

Data Importer:

- Name: Temporal Technologies Inc.
- Address: 1915 140th Ave NE, Suite D3-1335, Bellevue, WA 98005
- Contact person's name, position and contact details: Mike McBryde, Head of Security, mike.mcbryde@temporal.io
- Activities relevant to the data transferred under these Clauses: Temporal provides its Services to Customer as described in the Agreement and processes Customer Personal Data in that context.
- Signature and date: By entering into this Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.
- Role (controller/processor): Processor on behalf of Customer, or Subprocessor on behalf of Third-Party Controller.

B. DESCRIPTION OF INTERNATIONAL DATA TRANSFER

- Categories of Data Subjects whose Personal Data is transferred:

#	**Category of Data Subjects**
1.	*Customer employees using Temporal*
2.	*Other individuals that the Customer chooses to use the Service.*

- Categories of Personal Data transferred:

#	**Category of Personal Data**
1.	*IP addresses*
2.	*Names*
3	*Email addresses*
4.	*Browser information*
5.	*Other arbitrary Customer information stored in the Service*

- The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis): *On a continuous basis.*
- Nature of the Processing: *The Personal Data will be processed and transferred as described in the Agreement.*
- Purpose(s) of the data transfer and further Processing: *The Personal Data will be transferred and further processed for the provision of the Services as described in 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: *Personal Data will be retained for as long as necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Data Protection Law.*
- For transfers to (sub-) processors, also specify subject matter, nature and duration of the Processing: *For the subject matter and nature of the Processing, reference is made to the Agreement and this DPA. The Processing will take place for the duration of the Agreement.*

C. COMPETENT SUPERVISORY AUTHORITY

- The competent authority for the Processing of Personal Data relating to Data Subjects located in the EEA is the Supervisory Authority of Ireland.
- The competent authority for the Processing of Personal Data relating to Data Subjects located in the UK is the UK Information Commissioner.

Annex 2 to the Data Processing Addendum
Temporal Security Policy and Privacy Guidelines

Technical and Organizational Security Measures

Measures of pseudonymisation and encryption of customer data
We decouple user code and workflow state, meaning that no customer code is executed in the Temporal SaaS environment. All workflow data access happens on the customer side. At their discretion, customers may encrypt their data on the customer side before it is sent to Temporal Technologies' systems, with no loss of functionality. All customer data is encrypted at rest with industry-standard encryption.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
Temporal Technologies enforces the rule of least privilege for all systems, based on employee role. Access lists are audited quarterly. Access to all systems is through SSO with MFA enabled, with access deleted or suspended on termination of employment. Temporal Technologies does not use customer workflow data for any purpose other than delivery of service.

Measures for ensuring the ability to restore the availability and access to customer data in a timely manner in the event of a physical or technical incident
Temporal Technologies maintains a business continuity and disaster recovery plan that is tested yearly.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
Temporal Technologies conducts regular external audits (SOC 2 Type II) to ensure ongoing effectiveness. Temporal Technologies conducts a yearly risk assessment, which drives the prioritization of initiatives. Temporal Technologies conducts an external full-scope pentest at least annually.

Measures for user identification and authorisation
Temporal Technologies routes all authentication through corporate-controlled SSO, with MFA enabled. Temporal Technologies enforces the rule of least privilege for all systems, based on employee role.

Measures for the protection of data during transmission
Temporal Technologies ensures encryption in transit for all communications between customers and the service itself using industry standard protocols. Temporal Technologies encrypts all customer data in transit inside our service using industry-standard mutually authenticated TLS. Temporal Technologies supports private network connections to the service.

Measures for the protection of data during storage
Temporal Technologies encrypts all data at rest with cloud native encryption for ephemeral and persistent data stores using cloud provider's object storage. Additionally, customers may encrypt their data before it is sent to Temporal systems with no loss of functionality.

Measures for ensuring physical security of locations at which customer data are processed
Physical access to customer data processing locations is the responsibility of cloud providers. Temporal Technologies validates semi-annually that all subprocessors have sufficient physical security controls, including access controls, visitor logs, video security and alarm systems, backup power, and environmental monitoring.

Measures for ensuring events logging
Temporal Technologies logs relevant events to a central security information and event management system. Temporal employees monitor events, and automated alerts are sent to 24/7 oncall.

Measures for ensuring system configuration, including default configuration
Temporal Technologies manages all deployments through automated, repeatable processes driven by infrastructure as code tooling.

Measures for internal IT and IT security governance and management
Temporal Technologies ensures effective internal IT and IT security governance and management by implementing an information security management program that is informed by the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Measures for certification/assurance of processes and products
Temporal Technologies ensures assurance of products and processes by conducting third party audits of the service according to the 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Type II Report as issued by the American Institute of Certified Public Accountants. Upon request Temporal Technologies will share or provide evidence that a third party audit was conducted.

Measures for ensuring data minimisation
Temporal Technologies processes only that data which is relevant and necessary for the provision of services.

Measures for ensuring data quality
Temporal Technologies ensures data quality by ensuring that such details are up to date, reviewing data regularly, and following data deletion practices.

Measures for ensuring limited data retention
Temporal Technologies retains customer data currently in process until the end of contract; this is necessary to the service we provide. Customer data that is no longer in processing (e.g. kept for historical purpose) are deleted automatically, based on a retention setting configurable by the customer. All customer data is deleted upon contract termination. Backups are retained for 30 days.

Measures for ensuring accountability
Temporal Technologies ensures accountability through logging of access activity. Such logs are retained indefinitely, and can be reviewed to ensure that any access is proportionate and appropriate. Temporal Technologies does not allow non-employees access to customer data or production systems. All Temporal Technologies employees are required to abide by our data protection policies, any violation of which will result in disciplinary procedures.

Measures for allowing data portability and ensuring erasure
Temporal Technologies supports migration of all data in customer's accounts out of Temporal Cloud and into any other Temporal system, including OSS instances hosted by the customer. Customers can configure their own retention period for historical data, and can halt any currently running processing.

Annex 3 to the Data Processing Addendum
List of Subprocessors

#	**Name**	**Address**	**Description of the Processing (including a clear delimitation of responsibilities in case several sub-processors are authorized**
1	Amazon AWS	440 Terry Ave N, Seattle, WA 98109	Infrastructure
2	Google GCP	967 North Shoreline Blvd, Mountain View, CA 94043	Infrastructure (for Namespaces launched in GCP regions)
3	Datastax	2755 Augustine Dr. 8th Floor Santa Clara, CA 95054	Database as a service
4	Auth0	10800 NE 8th St #700, Bellevue, WA 98004	User authentication service
5	Elastic	88 Kearny St Floor 19 San Francisco, CA 94108	Business data monitoring and analysis (for Namespaces launched in GCP regions)
6	WorkOS, Inc.	548 Market Street #86125, San Francisco, CA 94104	Customer identity and access management platform

EXHIBIT A

U.S. STATE PRIVACY LAW DATA PROCESSING ADDENDUM

Pursuant to the Agreement between Customer on behalf of itself and its affiliates ("**Company**"), and Temporal Technologies, Inc. ("**Vendor**") the Parties hereby adopt this U.S. State Privacy Law Data Processing Addendum ("**U.S. State DPA**") for so long as Vendor processes Personal Data on behalf of Company. This U.S. State DPA prevails over any conflicting terms of the Agreement.

1. **Definitions**. For the purposes of this U.S. State DPA:
   - 1.1. "U.S. **State Privacy Laws**" means, collectively, all U.S. state privacy laws and their implementing regulations, as amended or superseded from time to time, that apply generally to the processing of individuals' Personal Data and that do not apply solely to specific industry sectors (e.g., financial institutions), specific demographics (e.g., children), or specific classes of information (e.g., health or biometric information). U.S. State Privacy Laws include the following:
     - 1.1.1. California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (California Civil Code §§ 1798.100 to 1798.199) ("**CPRA**");
     - 1.1.2. Colorado Privacy Act (Colorado Rev. Stat. §§ 6-1-1301 to 6-1-1313) ("**ColoPA**");
     - 1.1.3. Connecticut Personal Data Privacy and Online Monitoring Act (Public Act No. 22-15) ("**CPOMA**");
     - 1.1.4. Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 to 13-61-404) ("**UCPA**"); and
     - 1.1.5. Virginia Consumer Data Protection Act (Virginia Code Ann. §§ 59.1-575 to 59.1-585) ("**VCDPA**").
   - 1.2. "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person. Where applicable, Personal Data shall be interpreted consistent with the same or similar term under U.S. State Privacy Laws.
   - 1.3. "**Share**," "**Shared**," and "**Sharing**" have the meaning defined in the CPRA.
   - 1.4. "**Sale**" and "**Selling**" have the meaning defined in the U.S. State Privacy Laws.
   - 1.5. "**Controller**" means "Controller" or "Business" as those terms are defined in the U.S. State Privacy Laws.
   - 1.6. "**Processor**" means "Processor," "Service Provider," or "Contractor" as those terms are defined in the U.S. State Privacy Laws.
   - 1.7. "**Consumer**" has the meaning defined in the U.S. State Privacy Laws.
   - 1.8. "**Processing**," "**Process**," and "**Processed**" have the meaning defined in the U.S. State Privacy Laws.
   - 1.9. "**Company Personal Data**" means Personal Data provided by Company to, or which is collected on behalf of Company by, Vendor to provide services to Company pursuant to the Agreement.
   - 1.10. In the event of a conflict in the meanings of defined terms in the U.S. State Privacy Laws, the meaning from the law applicable to the state of residence of the relevant Consumer applies.
2. **Scope, Roles, and Termination.**
   - 2.1. *Applicability* - This U.S. State DPA applies only to Vendor's Processing of Company Personal Data for the nature, purposes, and duration set forth in Annex 1 of the DPA.
   - 2.2. *Roles of the Parties* - For the purposes of the Agreement and this U.S. State DPA, Company is the Party responsible for determining the purposes and means of Processing Company Personal Data as the Controller and appoints Vendor as a Processor to Process Company Personal Data on behalf of Company for the limited and specific purposes set forth in Annex 1 of the DPA.
   - 2.3. *Obligations at Termination* - Upon termination of the Agreement, except as set forth therein or herein, Vendor will discontinue Processing and destroy or return Company Personal Data in its or its subcontractors and sub-processors possession without undue delay. Vendor may retain Company Personal Data to the extent required by

law but only to the extent and for such period as required by such law and always provided that Vendor shall ensure the confidentiality of all such Company Personal Data.

3. Compliance.

3.1. *Compliance with Obligations* - Vendor represents and warrants that Vendor, its employees, agents, subcontractors, and sub-processors (a) shall comply with the obligations of the U.S. State Privacy Laws, (b) shall provide the level of privacy protection required by the U.S. State Privacy Laws, (c) shall provide Company with all reasonably-requested assistance to enable Company to fulfill its own obligations under the U.S. State Privacy Laws, and (d) understand and shall comply with this U.S. State DPA. Upon the reasonable request of Company, Vendor shall make available to Company all information in Vendor's possession necessary to demonstrate Vendor's compliance with this subsection.

3.2. *Compliance Assurance* - Company has the right to take reasonable and appropriate steps to ensure that Vendor uses Company Personal Data consistent with Company's obligations under applicable U.S. State Privacy Laws and Annex 2 of the DPA incorporated herein.

3.3. *Compliance Remediation* - Vendor shall notify Company no later than five business days after determining that it can no longer meet its obligations under applicable U.S. State Privacy Laws. Upon receiving notice from Vendor in accordance with this subsection, Company may direct Vendor to take reasonable and appropriate steps to stop and remediate unauthorized use of Company Personal Data.

4. Restrictions on Processing.

4.1. *Limitations on Processing* - Vendor will Process Company Personal Data solely as instructed in the Agreement and this U.S. State DPA. Except as expressly permitted by the U.S. State Privacy Laws, Vendor is prohibited from (i) Selling or Sharing Company Personal Data, (ii) retaining, using, or disclosing Company Personal Data for any purpose other than for the specific purpose of performing the Services specified in Annex 1 of the DPA, (iii) retaining, using, or disclosing Company Personal Data outside of the direct business relationship between the Parties, and (iv) combining Company Personal Data with Personal Data obtained from, or on behalf of, sources other than Company, except as expressly permitted under applicable U.S. State Privacy Laws.

4.2. *Confidentiality* - Vendor shall ensure that its employees, agents, subcontractors, and sub-processors are subject to a duty of confidentiality with respect to Company Personal Data.

4.3. *Subcontractors; Sub-processors* -Vendor's current subcontractors and sub-processors are set forth in Annex 3 of the DPA. Vendor shall notify Company of any intended changes concerning the addition or replacement of subcontractors or sub-processors. Further, Vendor shall ensure that Vendor's subcontractors or sub-processors who Process Company Personal Data on Vendor's behalf agree in writing to the same or equivalent restrictions and requirements that apply to Vendor in this U.S. State DPA and the Agreement with respect to Company Personal Data, as well as to comply with the applicable U.S. State Privacy Laws.

4.4. *Right to Object* - Company may object in writing to Vendor's appointment of a new subcontractor or sub-processor on reasonable grounds by notifying Vendor in writing within 30 calendar days of receipt of notice in accordance with Section 4.3. In the event Company objects, the Parties shall discuss Company's concerns in good faith with a view to achieving a commercially reasonable resolution.

5. Consumer Rights.

5.1. Vendor shall provide commercially reasonable assistance to Company for the fulfilment of Company's obligations to respond to State Privacy Law-related Consumer rights requests regarding Company Personal Data.

5.2. Company shall inform Vendor of any Consumer request made pursuant to the U.S. State Privacy Laws that they must comply with. Company shall provide Vendor with the information necessary for Vendor to comply with the request.

5.3. Vendor shall not be required to delete any Company Personal Data to comply with a Consumer's request directed by Company if retaining such information is specifically

permitted by applicable U.S. State Privacy Laws; provided, however, that in such case, Vendor will promptly inform Company of the exceptions relied upon under applicable U.S. State Privacy Laws and Vendor shall not use Company Personal Data retained for any purpose other than provided for by that exception.

6. Deletion of Company Personal Data

6.1. Upon direction by Company, and in any event no later than 30 days after receipt of a request from Company, Vendor shall promptly delete Company Personal Data as directed by Company, unless Vendor is required by law to retain such data, in which case Vendor shall, on ongoing basis, isolate and protect the security and confidentiality of such Personal Data and prevent any further processing except to the extent required by such law and shall destroy or return to Company all other Personal Data not required to be retained by Vendor by law.

7. Deidentified Data

7.1. In the event that Company discloses or makes available Deidentified data (as such term is defined in the U.S. State Privacy Laws) to Vendor, Vendor shall not attempt to reidentify the information.

8. Security

8.1. Vendor and Company shall implement and maintain no less than commercially reasonable security procedures and practices, appropriate to the nature of the information, to protect Company Personal Data from unauthorized access, destruction, use, modification, or disclosure.

9. Sale of Data

9.1. The Parties acknowledge and agree that the exchange of Personal Data between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Agreement or this U.S. State DPA.

10. Changes to Applicable Privacy Laws.

10.1. The Parties agree to cooperate in good faith to enter into additional terms to address any modifications, amendments, or updates to applicable statutes, regulations or other laws pertaining to privacy and information security, including, where applicable, the U.S. State Privacy Laws.