DOMO SERVICES DATA PROCESSING ADDENDUM
(U.S. STATES)

This Domo Services Data Processing Addendum ("U.S. State DPA") forms a part of the Domo Software as a Service Agreement between Subscriber and Domo, Inc. ("Domo") or other written agreement between Domo and Subscriber for the purchase of services from Domo (the "Agreement"). This DPA reflects the parties' agreement with regard to the Processing of Personal Data in accordance with the requirements of the State Privacy Laws. All capitalized terms not defined herein will have the meaning set forth in the Agreement.

In the course of providing the Subscription Services, Technical Support Services, and/or Professional Services to Subscriber pursuant to the Agreement (collectively, the "Services"), Domo may Process Personal Data on behalf of Subscriber. Domo and Subscriber agree to comply with the following provisions with respect to any Personal Data.

1. DEFINITIONS

For the purposes of this U.S. State DPA:

"State Privacy Laws" means, collectively, all U.S. state privacy laws and their implementing regulations, as amended or superseded from time to time, that apply generally to the processing of individuals' Personal Data and that do not apply solely to specific industry sectors (e.g.,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:

(a) 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");
(b) Colorado Privacy Act (Colorado Rev. Stat. §§ 6-1-1301 to 6-1-1313) ("ColoPA");
(c) Connecticut Personal Data Privacy and Online Monitoring Act (Public Act No. 22-15) ("CPOMA");
(d) Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 to 13-61-404) ("UCPA"); and
(e) Virginia Consumer Data Protection Act (Virginia Code Ann. §§ 59.1-575 to 59.1-585) ("VCDPA").

"Personal Data" means "Personal Data" or "Personal Information" as those terms are defined in the State Privacy Laws.

"Share," "Shared," and "Sharing" have the meaning defined in the CPRA.

"Sale" and "Selling" have the meaning defined in the State Privacy Laws.

"Controller" means "Controller" or "Business" as those terms are defined in the State Privacy Laws.

"Processor" means "Processor," "Service Provider," or "Contractor" as those terms are defined in the State Privacy Laws.

"Consumer" has the meaning defined in the State Privacy Laws.

"Processing," "Process," and "Processed" have the meaning defined in the State Privacy Laws.

"Subscriber Personal Data" means Personal Data uploaded by or on behalf of Subscriber to the Services, or otherwise provided by Subscriber to, Domo to provide the Services. Subscriber Personal Data does not include Personal Data independently collected by Domo as a Controller as described in Domo's Privacy Statement (available at https://www.domo.com/company/privacy-policy), including, but not limited to, Personal Data provided by Subscriber to register a user account to use Domo's Services.

In the event of a conflict in the meanings of defined terms in the 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 Domo's Processing of Subscriber Personal Data for the nature, purposes, and duration set forth in Annex I.

2.2. Roles of the Parties. For the purposes of the Agreement and this U.S. State DPA, Subscriber is the party responsible for determining the purposes and means of Processing Subscriber Personal Data as the Controller and appoints Domo as a Processor to Process Subscriber Personal Data on behalf of Subscriber for the limited and specific purposes set forth in Annex I.

2.3. Obligations at Termination. Upon termination of the Agreement, except as set forth therein or herein, Domo will discontinue Processing and delete Subscriber Personal Data in its or its subcontractors and sub-processors possession without undue delay. Domo may retain Subscriber 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 Domo will take appropriate steps designed to ensure the confidentiality of all such Subscriber Personal Data.

3. COMPLIANCE

3.1. Compliance with Obligations. Domo, its employees, agents, subcontractors, and sub-processors (a) will comply with the obligations of the State Privacy Laws as applicable to Domo or its subcontractors or subprocessors in performance of the Services, (b) will provide the level of privacy protection required of Processors by the State Privacy Laws, (c) will provide Subscriber with all reasonably requested assistance to enable Subscriber to fulfill

its own obligations under the State Privacy Laws, and (d) understand and will comply with the terms of this U.S. State DPA. Upon Subscriber's request, Domo will make available to Subscriber all reasonably requested information in Domo's possession necessary to demonstrate Domo's compliance with this Section 3.1.

3.2. Compliance Assurance. Subscriber has the right to take reasonable and appropriate steps to ensure that Domo uses Subscriber Personal Data consistent with Subscriber's obligations under applicable State Privacy Laws.

3.3. Compliance Monitoring. Domo will arrange for a qualified and independent assessor to conduct an assessment, at least annually and at the Domo's expense, of Domo's policies and technical and organizational measures in support of the obligations under this U.S. State DPA using an appropriate and generally accepted control standard or framework and assessment procedure for such assessments (e,g, SOC2). Subscriber consents to such assessment. Upon Subscriber's written request, and subject to the confidentiality obligations set forth in the Agreement, Domo shall provide a report of such assessment.

3.4. Compliance Remediation. Domo shall promptly notify Subscriber if it determines that it can no longer meet its obligations under applicable State Privacy Laws. Upon receiving notice from Domo in accordance with this Section 3.4, Subscriber may direct Domo to take reasonable and appropriate steps to stop and remediate unauthorized use of Subscriber Personal Data.

3.5. Security. Each party will implement and maintain no less than commercially reasonable security procedures and practices, appropriate to the nature of the information, to protect Subscriber Personal Data from unauthorized access, destruction, use, modification, or disclosure. See Annex II for additional details.

4. RESTRICTIONS ON PROCESSING

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

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

4.3. Subcontractors; Sub-processors. A current list of Domo's subcontractors and sub-processors who may Process Subscriber Personal Data is available at https://www.domo.com/company/subprocessors. At this location, Subscriber may sign-up to receive notice of any intended changes concerning the addition or replacement of subcontractors or sub-processors. Further, Domo will ensure that its subcontractors or sub-processors who Process Subscriber Personal Data on Domo's behalf agree in writing to the same or equivalent restrictions and requirements that apply to Domo in this U.S. State DPA and the Agreement with respect to Subscriber Personal Data, as well as to comply with the applicable State Privacy Laws.

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

5. CONSUMER RIGHTS

5.1. To the extent Subscriber, in its use of the Services, does not have the ability to address such requests itself, Domo will provide commercially reasonable assistance to Subscriber for the fulfillment of Subscriber's obligations to respond to State Privacy Law-related Consumer rights requests regarding Subscriber Personal Data.

5.2. Where applicable, Subscriber will inform Domo of any Consumer request made pursuant to the State Privacy Laws that Domo must comply with. Subscriber shall provide Domo with the information necessary for Domo to comply with the request.

6. DEIDENTIFIED DATA

6.1. In the event that Subscriber discloses or makes available Deidentified data (as such term is defined in the State Privacy Laws) to Domo, Domo will not attempt to reidentify the information.

7. SALE OF DATA

7.1. 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.

8. EXEMPTIONS.

8.1. Notwithstanding any provision to the contrary of the Agreement or this U.S. State DPA, the terms of this U.S. State DPA will not apply to Domo's Processing of Subscriber Personal Data that is exempt from applicable State Privacy Laws.

9. CHANGES TO APPLICABLE PRIVACY LAWS.

9.1. 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 State Privacy Laws.

10. LIMITATION OF LIABILITY

10.1. Each party's liability to the other party or its Affiliates arising out of or related to this U.S. State DPA is subject to the cap on liability set forth in the Agreement. Neither party will be liable to the other party or its Affiliates for indirect, consequential, incidental, special, punitive, or exemplary damages, or lost profits or loss of business arising out of or related to this U.S. State DPA, whether based in contract, tort (including, without limitation, negligence), or any other theory of liability, and even if the party is apprised in advance of the likelihood of such damages or such damages could have reasonably been foreseen.

ANNEX I

PROCESSING DETAILS

Categories of Personal Data Processed:

Subscriber may submit Personal Data to the Services, the extent of which is determined and controlled by the Subscriber in its sole discretion except as limited by the Agreement, and which may include, but is not limited to the following categories of Personal Data:

- Name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- Government issued identification data
- Professional life data
- Personal life data
- Connection data
- Location data

Nature of the Processing:

Subscribers will be able to view, manipulate, and create visualizations of the Personal Data via the Services provided by Domo pursuant to the Agreement.

Purpose(s) of the Processing

The purpose of the Processing is the provision of the Services by Domo to Subscriber and Affiliates of Subscriber.

The Services:

- Domo will provide a business intelligence platform (the "Domo Platform"), delivered as a service, together with other subscription-based services, to Subscriber to support its business intelligence activities (collectively the "Subscription Services"), as described in the Agreement and applicable Service Order. The Subscription Services allow Subscriber to bring together data from various locations designated by Subscriber into the Domo Platform. Subscriber's Authorized Users will have access to the Domo Platform (subject to specific license rights and restrictions), and will be able to create connections, reports and visualizations of Subscriber Personal Data.
- Domo will also provide related technical support, and training, consulting, implementation, and other professional services related to the Subscription Services.

Duration of the Processing:

The Processing will occur throughout the duration of the Agreement.

ANNEX II

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

The parties will maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as applicable to the specific Services purchased by Subscriber and any Personal Data limitations and restrictions provided in the Agreement. Domo's technical and organizational measures are described in this Annex.

1. *Measures of pseudonymization and encryption of Personal Data:*

   - Encryption of Subscriber Personal Data in transit across external untrusted networks when using Domo APIs and services utilizing industry standard cryptography and key management practices;
   - Where technically enforced, encryption of Subscriber Personal Data and back-ups of Subscriber Personal Data at rest utilizing industry standard cryptography and key management practices;
   - Encryption of authentication credentials at rest utilizing industry standard cryptography and key management practices;
   - Additional features available for Subscriber to implement such as Bring Your Own Key to facilitate encryption of Subscriber Personal Data and backups of Subscriber Personal Data using Subscriber's own encryption keys.

2. *Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services:*

   - Maintenance of intrusion detection and prevention measures and end point security controls;
   - Utilization of anti-virus and anti-malware software against appropriate Domo information assets;
   - Installation and maintenance of firewalls intended to help protect Subscriber Personal Data accessible via the internet or from other untrusted networks;
   - Implementation and maintenance of a written, comprehensive information security program;
   - Monitoring of security controls on a regular basis to assess whether the controls are operating in a manner reasonably calculated to prevent and detect unauthorized access to or use of Subscriber Personal Data;
   - Review of the scope of security measures annually or when there is a material change in business practices that may reasonably implicate the security or integrity of Subscriber Personal Data.

3. *Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident:*

   - Maintenance of a system contingency plan and assignment of appropriate personnel to coordinate contingency planning, training and testing activities;
   - Maintenance and periodic evaluation of a written disaster recovery program that documents business impact assessments, contingency plans, and recovery procedures.

4. *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing:*

   - Monitoring of security controls on a regular basis to assess whether the controls are operating in a manner reasonably calculated to prevent and detect unauthorized access to or use of Subscriber Personal Data;
   - Review of the scope of security measures annually or when there is a material change in business practices that may reasonably implicate the security or integrity of Subscriber Personal Data.

5. *Measures for user identification and authorization:*

   - Requiring two-factor authentication for remote access into systems which house Subscriber Personal Data;
   - Blocking access to user accounts after multiple unsuccessful attempts to gain access;
   - Implementation of controls such as VPN access requirements, multi-factor authentication requirements, user access provisioning and de-provisioning tools and processes to help prevent a third party from accessing, using or disclosing Subscriber Personal Data except as specifically authorized in the Agreement or as otherwise approved by Subscriber.

6. *Measures for the protection of data during transmission:*

   - Encryption of Subscriber Personal Data in transit across external untrusted networks when using Domo APIs and services, utilizing industry standard cryptography and key management practices;

7. *Measures for the protection of data during storage:*

   - Maintenance of physical or logical separation of Subscriber Personal Data;
   - Encryption of Subscriber Personal Data and backups of Subscriber Personal Data and authentication credentials at rest;
   - Additional features available for Subscriber to implement such as Bring Your Own Key to facilitate encryption of Subscriber Personal Data and backups of Subscriber Personal Data using Subscriber's own encryption keys;
   - Installation and maintenance of firewalls intended to help protect Subscriber Personal Data accessible via the internet

or from other untrusted networks;
- Implementation of consistent hardening procedures and practices for Domo systems which access, store or connect to Subscriber Personal Data.

8. *Measures for ensuring physical security of locations at which Personal Data are Processed:*

- Maintenance of physical or logical separation of Subscriber Personal Data;
- Implementation of physical entry controls and monitoring for locations where Subscriber Personal Data is Processed, including requiring personnel accessing these locations to employ individually identifiable entry controls (such as card keys) that provide an audit trail of each entry.

9. *Measures for ensuring events logging:*

- Implementation of logging and alerting controls which include alerting of significant events;
- Implementation of intrusion prevention and detection systems to monitor and log system resources for potential unauthorized access and generate alerts on attempted attacks;
- Maintenance of retention policies for logs, audit trails and other documentation that provides evidence of security, systems, and audit processes and procedures related to Subscriber Personal Data.

10. *Measures for ensuring system configuration, including default configuration:*

- Ongoing monitoring and review of configurations including assessing the Domo Platform for security flaws;

11. *Measures for internal IT and IT security governance and management:*

- Maintenance of a written, proportionally comprehensive information security program consistent with applicable industry standards that includes:
    - Information security policies,
    - Access management,
    - Change management,
    - Secure System Development Lifecycle (SSDLC),
    - Physical and environmental security,
    - Incident response plans and procedures,
    - Vulnerability management,
    - Patch management,
    - Business continuity/Disaster Recovery plans,
    - Continuous monitoring,
    - Asset criticality and data classification,
    - Data retention and destruction policies,
    - Third party and software supply chain security,
    - Hiring policies,
    - Employment termination policies,
    - Security awareness,
    - Privacy policies, and
    - Data security procedures.

- Implementation of a risk management program to help address security vulnerabilities, and deploy security patches within a commercially reasonable timeframe;
- Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Subscriber Personal Data and evaluation and implementation of improvements, where necessary, of the effectiveness of the current safeguards for limiting such risks;
- Annual employee security and privacy awareness training;
- Written agreements with sub-processors who have access to Subscriber Personal Data;

12. *Measures for certification/assurance of processes and products:*

- Maintenance of an information security program in compliance with ISO 27001 and SOC 2.

13. *Measures for ensuring data minimization:*

- Implementation of data retention policies;
- Implementation of controls designed to ensure that Subscriber Personal Data is deleted consistent with applicable data retention policies;
- Restriction of personnel access to Subscriber Personal Data to authorized personnel who are subject to written confidentiality obligations and have participated in security awareness training;

14. *Measures for ensuring data quality:*

- Identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Subscriber Personal Data, and evaluation of and implementation of improvements, where necessary, to the effectiveness of the current safeguards for limiting such risks.

15. *Measures for ensuring limited data retention:*

- Implementation of data retention policies;
- Implementation of controls designed to ensure that Subscribed Data is deleted consistent with applicable data retention policies;

16. *Measures for ensuring accountability:*

- Adoption and implementation of data protection policies;
- Execution of written agreements with sub-processors who may have access to Subscriber Personal Data;
- Implementation of intrusion prevention and detection systems to monitor and log system resources for potential unauthorized access and generate alerts on attempted attacks;
- Adoption of retention policies for logs, audit trails and other documentation that provides evidence of security, systems, and audit processes and procedures related to Subscriber Personal Data;
- Annual employee security and privacy awareness training.

17. *Measures for allowing data portability and ensuring erasure:*

- Encryption of Subscriber Personal Data in transit across external untrusted networks when using Domo APIs and services utilizing industry standard cryptography and key management practices;
- Where technically enforced, encryption of Subscriber Personal Data and back-ups of Subscriber Personal Data at rest utilizing industry standard cryptography and key management practices;
- Encryption of authentication credentials at rest utilizing industry standard cryptography and key management practices.

For transfers to Sub-processors, Domo, as Processor, requires that its Sub-processors take appropriate technical and organizational measures to assist the controller and Subscriber in protecting the security, confidentiality and integrity of Personal Data uploaded to the Services as follows:

1. Relevant agreements with sub-processors include requirements for appropriate technical and organizational measures relevant to the sub-processor services provided to Domo.

2. Technical and organizational measures used to mitigate any risks associated with sub-processor access to Subscriber Personal Data in its provision of relevant sub-processor services to Domo are agreed upon with the sub-processor and documented.

3. All relevant technical and organizational measures are established and agreed upon with each sub-processor that may access, Process, or store Subscriber Personal Data.

4. A Domo security and risk review is performed for each sub-processor that may access, Process or store Subscriber Personal Data.