BY ACCEPTING THIS DATA PROCESSING ADDENDUM OR ACCESSING OR USING THE SERVICE, YOU ARE AGREEING TO THE TERMS AND CONDITIONS OF THIS DATA PROCESSING ADDENDUM.

IF YOU ARE USING ANY SERVICE AS AN EMPLOYEE, AGENT, OR CONTRACTOR OF A CORPORATION, PARTNERSHIP OR SIMILAR ENTITY, THEN YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO SIGN FOR AND BIND SUCH ENTITY IN ORDER TO ACCEPT THE TERMS OF THIS AGREEMENT. THE RIGHTS GRANTED UNDER THIS AGREEMENT ARE EXPRESSLY CONDITIONED UPON ACCEPTANCE BY SUCH AUTHORIZED PERSONNEL.

The Parties entered into an underlying agreement for Customer’s use of SingleStore’s offering(s) ("Underlying Agreement") which requires that the Processor accesses and Processes Personal Data. This agreement together with its exhibit (together the "Data Processing Agreement" or "DPA") specify the obligations of the Parties when SingleStore is acting as Processor.

Modifications to this Agreement: From time to time, SingleStore may modify this Data Processing Addendum. Unless otherwise specified by SingleStore, changes become effective for Customer upon renewal of the then-current Subscription Term or entry into a new Service Order Form after the updated version of this DPA goes into effect. SingleStore will use reasonable efforts to notify Customer of the changes through communications via Customer’s Account, email or other means.

The “Effective Date” of this DPA is the date which is the earlier of (a) Customer’s initial access to any Service through any online provisioning, registration or order process or (b) the effective date of the first Service Order Form, as applicable, referencing this DPA.

This DPA is entered into by and between SingleStore, Inc., a Delaware corporation ("SingleStore" or "Processor") and the person or entity placing an order for or accessing the Service ("Customer" or "Controller"). Processor and Controller are individually referred to as “Party” and collectively as “Parties”. In consideration of the terms and conditions set forth below, the parties agree as follows:

1. Scope of contract and Distribution of Responsibilities

1.1 The Parties agree that, for Processing Personal Data, the Parties shall be Controller and Processor.

1.2 Processor shall Process Personal Data only on behalf of Controller and at all times only in accordance with this Data Processing Agreement.

1.3 Within the scope of the Underlying Agreement, each Party shall be responsible for complying with its respective obligations as Controller and Processor under Data Protection Laws.
2. Processing Instructions

2.1 Processor will Process Personal Data in accordance with Controller’s instructions. This Data Processing Agreement contains Controller’s initial instructions to Processor. The Parties agree that Controller may communicate any change in its initial instructions to the Processor by way of written notification to the Processor and that Processor shall abide by such instructions. The Processor shall maintain a secure, complete, accurate and up to date record of all such individual instructions.

2.2 For the avoidance of doubt, any instructions that would lead to processing outside the scope of this Data Processing Agreement (e.g. because a new Processing purpose is introduced) will require a prior agreement between the Parties and, where applicable, shall be subject to the contract change procedure under the Underlying Agreement.

2.3 Where instructed by Controller, Processor shall correct, delete or block Personal Data.

2.4 Processor shall promptly inform the Controller in writing if, in Processor’s opinion, an instruction infringes Data Protection Laws and provide an explanation of the reasons for its opinion in writing.

2.5 Processor shall not be liable for any DP Losses arising from or in connection with any processing made in accordance with Controller’s instructions following Controller’s receipt of any information provided by Processor in this Section 2.

3. Processor Personnel

Processor will restrict its personnel from Processing Personal Data without authorization. Processor will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security, pursuant to applicable law.

4. Disclosure to Third Parties; Data Subjects Rights

4.1 Processor will not disclose Personal Data to any third party (including any government agency, court, or law enforcement) except as set forth in this Data Processing Agreement or with written consent from Controller or as necessary to comply with applicable mandatory laws. If Processor is obliged to disclose Personal Data to a law enforcement agency or third party, Processor agrees to give Controller reasonable notice of the access request prior to granting such access, to allow Controller to seek a protective order or other appropriate remedy. If such notice is legally prohibited, Processor will take reasonable measures to protect the Personal Data from undue disclosure as if it were Processor’s own confidential information being requested and shall inform Controller promptly as soon as possible if and when such legal prohibition ceases to apply.

4.2 In case Controller receives any request or communication from Data Subjects which relates to the Processing of Personal Data ("Request"), Processor shall provide the Controller with full
cooperation, information and assistance ("Assistance") in relation to any such Request where instructed by Controller.

4.3 Where Processor receives a Request, Processor shall (i) not directly respond to such Request, (ii) forward the request to Controller within thirty (30) days of identifying the Request as being related to the Controller and (iii) provide Assistance according to further instructions from Controller.

5. Assistance

5.1 The Processor assists the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR taking into account the nature of Processing and the information available to the Processor

5.2 Where a Data Protection Impact Assessment ("DPIA") is required under applicable Data Protection Laws for the Processing of Personal Data, Processor shall provide upon request Controller with reasonable cooperation and assistance needed to fulfill Customer’s obligation to carry out a DPIA related to Customer’s use of the Services, to the extent that Customer does not otherwise have access to the relevant information and such information is available to SingleStore.

5.3 The Controller shall pay the Processor reasonable charges mutually agreed between the parties for providing the assistance in Section 5, to the extent that such assistance is not reasonably able to be accommodated within the normal provision of the Services.

6. Information Rights and Audit

6.1 Processor shall, in accordance with Data Protection Laws, make available to Controller on request in a timely manner such information as is necessary to demonstrate compliance by Processor with its obligations under Data Protection Laws.

6.2 SingleStore has obtained third-party certifications and audits set forth on our security page. Upon Controller’s written request and subject to the confidentiality obligations set forth in the Underlying Agreement, SingleStore will make available to Controller a copy of SingleStore’s then most recent third-party certifications or audits, as applicable.

6.3 Processor shall, upon reasonable notice, allow for and contribute to inspections of the Processor’s Processing of Personal Data, as well as the TOMs (including data processing systems, policies, procedures and records), during regular business hours and with minimal interruption to Processor’s business operations. Such inspections are conducted by the Controller, its affiliates or an independent third party on Controller’s behalf (which will not be a competitor of the Processor) that is subject to reasonable confidentiality obligations.

6.4 Controller shall pay Processor reasonable costs of allowing or contributing to audits or inspections in accordance with Section 6.3 where Controller wishes to conduct more than one audit or inspection every 12 months. Processor will immediately refer to Controller any requests
received from national data protection authorities that relate to the Processor’s Processing of Personal Data.

6.5 Processor undertakes to cooperate with Controller in its dealings with national data protection authorities and with any audit requests received from national data protection authorities. Controller shall be entitled to disclose this Data Processing Agreement or any other documents (including contracts with subcontractors) that relate to the performance of its obligations under this Data Processing Agreement (commercial information may be removed).

7. Data Incident Management and Notification

In respect of Customer data incident Processor shall:

7.1 notify Controller of a Personal Data Breach involving Processor or a subcontractor without undue delay (but in no event later than 72 hours after becoming aware of the incident);

7.2 make reasonable efforts to identify the cause of such incident and take those steps as Processor deems necessary and reasonable in order to remediate the cause of the incident to the extent that it is within SingleStore’ reasonable control.

7.3 provide reasonable information, cooperation and assistance to Controller in relation to any action to be taken in response to a Personal Data Breach under Data Protection Laws, including regarding any communication of the Personal Data Breach to Data Subjects and national data protection authorities.

The obligations contained in Section 7 should not apply to data incidents that are caused by Customer or Customer’s users.

8. International Data Transfer

8.1 Data that SingleStore processes for the Customer as a Processor may be stored in the EU or outside of the EU depending on the SingleStore product.

8.2 SingleStore may also process certain data about Customer or its users as a data controller, including in countries outside of the EU, in accordance with SingleStore privacy notice available at https://www.SingleStore.com/privacy-notice

8.3 Where there is international transfer of Personal Data to the Processor in countries which do not ensure an adequate level of data protection the following applies

   a) The Parties enter into Standard Contractual Clauses (Exhibit 1) for the transfer of Personal Data in countries which do not ensure an adequate level of data protection in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals. The Standard Contractual Clauses will apply to Personal Data originating from Controller (who, for the purposes of the Standard Contractual Clauses shall be deemed the "Data Exporter") that is processed by Processor (who, for the purposes of the Standard Contractual Clauses shall be deemed the "Data Importer"). If there is any conflict between the
Standard Contractual Clauses and this Data Processing Agreement, the Standard Contractual Clauses shall prevail.

b) At Controller’s request, the Standard Contractual Clauses shall be replaced and the Parties shall execute new standard contractual clauses for transfers to data processors in third countries adopted pursuant to Art. 46 (2) c) or d) GDPR.

c) If and as long as the country where Personal Data is transferred to a country which is subject to an adequacy decision according Article 45 (3) GDPR, no Standard Contractual Clauses are required. Once the adequacy decision is repealed or suspended, a) and b) shall automatically apply.

9. Reference to Provisions of the Standard Contractual Clauses

For the technical and organizational measures (TOMs), reference is made to and Annex II of the Standard Contractual Clauses.

For sub-processing, reference is made to Annex III of the Standard Contractual Clauses. In event of objection by the Controller to the appointment or replacement of any sub processor, Processor will either not appoint or replace the sub processor or, if this is not possible, Controller may suspend or terminate the Service(s) (without prejudice to any fees incurred by Controller prior to such suspension or termination).

10. Term and Termination

10.1 This Data Processing Agreement becomes effective upon signature. It shall continue to be in full force and effect as long as Processor is processing Personal Data according to Exhibit 1 Annex I and shall cease automatically thereafter.

10.2 The Controller may terminate the Data Processing Agreement as well as the Underlying Agreement for cause, at any time upon reasonable notice or without notice, as selected by Controller, if the Processor is in material breach of the terms of this Data Processing Agreement.

10.3 Where amendments are required to ensure compliance of this Data Processing Agreements with Data Protection Laws, the Parties shall agree on such amendments upon request of Controller and, for the avoidance of doubt, with no additional costs to Controller. Where the parties are unable to agree upon such amendments, either party may terminate the Underlying Agreement and this Data Processing Agreement with 90 days written notice to the other party.

11. Deletion or Return of Personal Data

Controller may export all Customer Data prior to the termination of the Customer's Account. In any event, following the termination of the Customer's Account, (i) subject to (ii) and (iii) below and the Underlying Agreement, Customer Data will be retained for a period of fourteen (14) days from such termination within which Controller may contact Processor to export Customer Data;
(ii) where the Controller does not use custom mailbox and uses the e-mail feature, if available within the Service(s), e-mails forming part of Customer Data are automatically archived for a period of three (3) months; and (iii) logs are archived for a period of thirty (30) days in the log management systems, post which logs are retired to a restricted archived cold storage for a period of eleven (11) months (each a "Data Retention Period"). Beyond each Data Retention Period, Processor reserves the right to delete all Customer Data in the normal course of operation except as necessary to comply with Processor's legal obligations, maintain accurate financial and other records, resolve disputes, and enforce its agreements. Customer Data cannot be recovered once it is deleted.

12. Miscellaneous

12.1 In case of any conflict, the provisions of this Data Processing Agreement shall take precedence over the provisions of any other agreement with Processor.

12.2 The limitation of liability stated in the Underlying Agreement apply to the breach of the Data Processing Agreement.

12.3 No Party shall receive any remuneration for performing its obligations under this Data Processing Agreement except as explicitly set out herein or in another agreement.

12.4 Where this Data Processing Agreement requires a "written notice" such notice can also be communicated per email to the other Party. Notices shall be sent to the contact persons set out in Exhibit 1 Annex I.

12.5 Any supplementary agreements or amendments to this Data Processing Agreement must be made in writing and signed by both Parties.

12.6 Should individual provisions of this Data Processing Agreement become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this agreement.

13. Definitions

"Data Protection Laws" shall mean the data protection laws of the country in which Controller is established, including the GDPR, and any data protection laws applicable to Controller in connection with the Underlying Agreement. Where the Controller is not established in an EU Member State the California Consumer Privacy Act applies in addition.

"DP Losses" means all liabilities, including:

a) costs (including legal costs);

b) claims, demands, actions, settlements, charges, procedures, expenses, losses and damages (whether material or non-material, and including for emotional distress);

c) to the extent permitted by applicable law:

i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a data protection authority or any other relevant Regulatory Authority;
ii) compensation to a Data Subject ordered by a data protection authority to be paid by Processor;

iii) the costs of compliance with investigations by a data protection authority or any other relevant Regulatory Authority.

"GDPR" shall mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data.

"Personal Data" mean any information relating to an identified or identifiable natural person as defined by the General Data Protection Regulation of the European Union ("GDPR" EC-2016/679) that is Processed by Processor as part of providing the services to Controller as described in Exhibit 1.

"Underlying Agreement" shall mean the SingleStore License Agreement (whether Managed Service or SingleStoreDB) available at https://www.SingleStore.com/legal/ or an equivalent master services agreement executed between the Parties.

"Standard Contractual Clauses/EU Standard Contractual Clauses" the standard contractual clauses set forth in Exhibit 1 for the transfer of Personal Data from a Data Controller in the European Economic Area to Processors established in third countries in the form set out in the Annex of the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as amended by incorporating the description of the Personal Data to be transferred and the technical and organizational measures to be implemented as set out in the Appendix.

"Controller", "Data Subject", "Personal Data Breach", "Processor" and "Process"/"Processing" shall have the meaning given to them in the GDPR.
Appendix A: Personal Data

This Appendix includes certain details of the Processing of the Personal Data as required by Article 28(3) GDPR or equivalent provisions of any Data Protection Law.

1. Subject matter and duration of the Processing of the Personal Data

The subject matter and duration of the Processing of the Personal Data are providing non personalized advertising media buying in the US, as set out in the Principal Agreement.

2. The nature and purpose of the Processing of the Personal Data

The Supplier shall Process the Personal Data for the purposes of providing the Services as set out in the Principal Agreement.

3. The types of the Personal Data to be Processed

[Please complete]

4. The categories of Data Subject to whom the Personal Data relates

In each case as applicable to the Services.

5. The obligations and rights of the Data Controller

The obligations and rights of the Data Controller are set out in the Principal Agreement and this Addendum.
Appendix B: SingleStore Inc Technical and Organizational Measures

a. Data Storage
SingleStore is a global company providing services through all major cloud solution providers (CSP). SingleStore Managed Service customers are able to choose from a selection of global processing and storage locations to meet their geographic and strategic needs.

b. Encryption and Key Management
SingleStore products support encryption at rest and in transit to ensure the security of customer data. Customers using SingleStore on their own infrastructure are responsible for ensuring that adequate encryption is in place. For SingleStore Managed Service encryption at rest is provided through CSP native technologies supporting AES-256 encryption and for encryption at rest TLS 1.2 is fully support, however this required customer configuration.

c. Support and Maintenance
SingleStore deploys changes to SingleStore Managed Service during scheduled maintenance windows, which are agreed upon at the point of customer onboarding. For any additional maintenance required SingleStore will contact customers directly via email to notify and agree said maintenance.

d. Incident Response and Notification
"Incident" means a security event that compromises the confidentiality, integrity or availability of an information asset. "Breach" means an Incident that results in the confirmed disclosure, not just potential exposure, of data to an unauthorized party.
SingleStore has an incident response plan, including a breach notification process, to assess, escalate, and respond to identified physical and cyber security incidents that impact the organization, Customers, or result in data loss. Discovered intrusions and vulnerabilities are resolved in accordance with established procedures. The incident response plan is reviewed and updated annually and more frequently as needed.
If there is a Breach involving your Customer Data, SingleStore will (A) notify you within 24 hours of discovery of the Breach, (B) reasonably cooperate with you with respect to such Breach, and (C) take appropriate corrective action to mitigate any risks or damages involved with the Breach to protect your Customer Data from further compromise. SingleStore will take any other actions that may be required by applicable law as a result of the Breach.

e. Information Security Program

Scope and Contents: SingleStore maintains a written security program that (A) complies with applicable global industry recognized information security frameworks, (B) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of data and (C) is appropriate to the nature, size and complexity of SingleStore’s business operations. SingleStore has built its information security program on the requirements of ISO 27001 and SOC 2.
Security Program Changes: SingleStore policies, standards, and operating procedures related to confidentiality, integrity and availability are made available to personnel via the corporate intranet. Security policies and procedures are reviewed, updated (as needed), and approved at least annually to maintain their continuing relevance and accuracy. Personnel are required to review and acknowledge these policies and procedures during on-boarding and annually thereafter.

Security Officer: SingleStore’s Head of Information Security and Information Security Steering Committee develop, maintain, review, and approve SingleStore’s security standards and policies.

Security Training & Awareness: All SingleStore personnel are required to complete security awareness training at least on an annual basis. SingleStore conducts periodic security awareness education and communications in relation to phishing ad other security concerns.

f. Risk Management

A security risk assessment and management process is in place to identify and remediate potential threats to SingleStore. Risk ratings are assigned to all identified risks, and remediation is managed by security personnel. Executive management is kept apprised of the risk posture of the organization. Full business risk assessments are completed at least annually.

g. Access Control

SingleStore assigns application and data rights based on user security groups and roles within its access management system. Security access requests are approved by the designated individual prior to provisioning. Security groups and roles are created based on the principle of least privilege.

SingleStore classifies informational assets in accordance with its data classification guideline.

h. User Access Management

SingleStore promptly disables application, platform and network access for terminated users upon notification of termination.

Administrator access to confidential and restricted systems, including corporate and cloud networks, is reviewed on an annual basis for appropriateness. Any inappropriate access is removed promptly.

SingleStore uses separate administrative accounts to perform privileged functions, and accounts are restricted to authorized individuals.

i. Password Management and Authentication

SingleStore uses an industry recognized access management system for users to authenticate to corporate resources. This also enforces minimum password length and complexity as well as requiring multi factor authentication on all connections.

j. Remote Access
Remote access to the corporate network is secured through a virtual private network (VPN) solution with two-factor authentication. Remote access to all corporate applications requires authentication through the access management system and with multi-factor authentication.

k. Asset Configuration and Security
Endpoint antiviruses technology is installed and activated on all SisngleStore workstations to monitor for virus and malware infections. Endpoint devices are scanned in real-time. Monitoring is in place to indicate when an anti-virus agent does not check in for prolonged periods of time. Issues are investigated and remediated as appropriate. Virus definition updates are pushed out to endpoint devices automatically as they become available.
SingleStore uses full-disk encryption on all endpoints. Endpoint devices are monitored and encrypted using industry recognized tools. IT administrators are alerted of discrepancies in security policies and settings identified from the tools. SingleStore maintains and regularly updates an inventory of corporate and cloud infrastructure assets, and systematically reconciles the asset list annually.

l. Security Testing
SingleStore has established a Threat and Vulnerability Management (TVM) program to monitor for vulnerabilities on an on-going basis.
Quarterly internal vulnerability scans are conducted using industry-recognized vulnerability scanning tools. Identified vulnerabilities are evaluated and documented within an associated ticket and remediated to address the associated risk(s).
External penetration tests are conducted by an independent third party on an annual basis to detect application security vulnerabilities. Critical and High findings from these tests are evaluated, documented, and remediated.

m. Logging and Monitoring
SingleStore continuously monitors application, infrastructure, network, data storage space and system performance. SingleStore utilizes a security information event monitoring system that proactively alerts based on suspicious or abnormal activities. Logs contain details on the date, time, source, and type of events. Information and works events worthy of real-time review are reviewed.

n. Change Management
SingleStore change management policies and procedures are established for requesting, testing, and approving application, infrastructure, and product related changes. All changes receive a risk score based on risk and impact criteria. Lower risk release changes generate automated change tickets and have various levels of approval based on risk score. High risk-rated changes require manual change tickets to be created and are reviewed by approvers based on change type.
Planned changes to the corporate and/or cloud production environments are reviewed regularly. Change documentation and approvals are maintained in a ticketing system (SOC: CM-1). Product development changes undergo various levels of review and testing based on change type, including security and code reviews, regression, and user acceptance testing prior to approval for deployment (SOC: CM-2). Following the successful completion of testing, changes are reviewed.
and approved by appropriate managers prior to implementation to production (SOC: CM-3). Dedicated environments separate from production exist for development and testing activities. (SOC: CM-9).

o. **Secure Development**
SingleStore has established a Software Development Life Cycle (SDLC) methodology that governs the acquisition, development, implementation, configuration, maintenance, modification, and management of infrastructure and software components. The SDLC methodology is consistent with SingleStore’s security, availability, processing integrity and confidentiality policies. Prior to the final release of a new version to the production cloud environment, code is reviewed and tested. Secure coding guidelines are established based on leading industry standards, updated as needed, and are available to personnel via the intranet. Developers receive secure coding training.

p. **Network Security**
Network perimeter defense solutions, including firewalls, are in place to monitor, detect, and prevent malicious network activity. Security operations personnel monitor items detected and take appropriate action. Firewall rule changes that meet the criteria for the corporate change management criteria follow the change management process and require approval by the appropriate approvers. SingleStore’s corporate and Cloud networks are logically segmented and firewalls monitor traffic to restrict access to authorized users, systems, and services.

q. **Third Party Security**
SingleStore assesses and manages the risks associated with existing and new vendors. SingleStore employs a risk-based scoring model for each vendor. SingleStore communicates security and confidentiality requirements and operational responsibilities to third parties through contractual agreements as necessary (e.g., Master Underlying Agreement, Non-Disclosure Agreement, Information Security Addendum, Data Processing Addendum). All vendors with access to data classified as confidential in SingleStore’s document classification scheme are reviewed at least annually using a third party vendor risk assessment tool.

r. **Physical Security**
Physical access to SingleStore offices is granted based on job responsibilities and work location. Access to offices can only be approved by appropriate personnel. Physical access is removed when access is no longer required and as a component of the employee termination process. Visitor logs are maintained for personnel visiting the offices, and visitors are required to be escorted by SingleStore personnel. Badge readers control all access within SingleStore offices. Unauthorized badge access attempts are denied and logged. Tailgating is prohibited by policy.

s. **Internal Audit**
Internal audits are aligned to SingleStore’s information security program and compliance requirements. SingleStore conducts internal control assessments to validate that controls are operating effectively. Issues identified from assessments are documented, tracked and remediated as appropriate. Internal controls related to security, availability, processing integrity and confidentiality are audited by an external independent auditor at least annually and in accordance with applicable regulatory and industry standards.

**t. Business Continuity**
SingleStore has a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) in place to manage significant disruptions to operations and infrastructure. These plans are reviewed and updated periodically and approved on an annual basis by the Head of Information Security. Business continuity exercises are conducted to evaluate the tools, processes and subject matter expertise of SingleStore in response to a specific incident. Summaries of the results of the exercises are documented and issues identified are tracked and followed up on for remediation.

**u. Human Resources Security**
SingleStore requires personnel to sign a confidentiality agreement as a condition of employment. SingleStore has a new employee hiring procedure in place to guide the hiring process, and background verification checks are completed for potential SingleStore personnel in accordance with relevant laws and regulations. SingleStore maintains a disciplinary process to take action against personnel that do not comply with company policies, including but not limited to, those put in place to meet its security,