DATA PROCESSING ADDENDUM

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

IF YOU ARE USING THE SERVICES 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.

This Data Processing Addendum (**"DPA")** is entered into by and between **SingleStore, Inc.,** a Delaware corporation ("**SingleStore"**) and the person or entity placing an order for or accessing the Services ("**Customer**"). SingleStore and Customer are individually referred to as "**Party**" and collectively as "**Parties**".

The Parties entered into the Underlying Agreement for SingleStore to provide Customer with Services which require that SingleStore Processes Personal Data on behalf of Customer. This DPA, together with its Appendices, specifies the obligations of the Parties when SingleStore is acting as a Processor.

Modifications to this DPA: From time to time, SingleStore may modify this DPA. Unless otherwise specified by SingleStore, changes become effective for Customer upon renewal of the then-current Subscription Term or entry into a new Order Document 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 Order Document, as applicable, referencing this DPA.

In this DPA, SingleStore will act as a Processor (or sub-processor) and Customer will act as a Controller or as a Processor on behalf of a third-party controller ("Third-Party Controller"). SingleStore may also process certain data about Customer or its users, such as contact and billing information, as a Controller in accordance with SingleStore's privacy notice available at https://www.SingleStore.com/privacy-notice. For the avoidance of doubt, this DPA does not apply to Personal Data (defined below) such as contact, billing, or other information provided by Customer to SingleStore or collected by SingleStore from Customer in SingleStore's role as a Controller (defined below) in order to provision the Services for Customer.

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 SingleStore shall Process Customer Personal Data only on behalf of Customer and at all times only in accordance with the purposes of the Underlying Agreement and this DPA.

1.2 Within the scope of the Underlying Agreement and this DPA, each Party shall be responsible for complying with its respective obligations as Controller and Processor under Applicable Data Protection Laws.1.3 Customer shall ensure its Processing instructions are lawful and that the

Processing of Customer Personal Data by SingleStore in accordance with such instructions will not violate Applicable Data Protection Laws. In particular, with regard to European Data Protection Law, Customer shall ensure that there is a lawful basis in respect of SingleStore's Processing of Customer Personal Data and Data Subjects have been provided with sufficient information to meet the requirements of Article 13/14 of the GDPR/UK GDPR in respect of such Processing (or the equivalent provisions in the Swiss Data Protection Laws).

1.4 The subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are documented in Appendix A to this DPA.

2. Processing Instructions

2.1 The Parties agree that the Underlying Agreement, including this DPA, sets out the exclusive and final instructions to SingleStore for all Processing of Customer Personal Data and, if applicable, include and are consistent with all instructions from Third-Party Controllers. Any additional requested instructions require the prior written agreement of the Parties.

2.2 SingleStore shall promptly inform Customer if, in SingleStore's opinion, a Customer instruction infringes Data Protection Laws or SingleStore cannot meet requirements under Applicable Data Protection Laws. Where applicable, Customer shall be responsible for any communications, notifications, assistance, or authorizations that may be required in connection with a Third-Party Controller.

2.3 SingleStore shall have no obligation to assess the contents or accuracy of Customer Personal Data, including to identify information subject to any legal, regulatory, or other requirement. Customer is responsible for making an independent determination as to whether its use of the Services will meet Customer's requirements and legal obligations under Applicable Data Protection Laws.

2.4 SingleStore shall not be liable for any DP Losses arising from or in connection with any Processing made in accordance with Customer's instructions following Customer's receipt of any information provided by SingleStore in this Section 2.

2.5 For the avoidance of doubt, SingleStore has the right to process and analyze any Customer Personal Data in an anonymous or deidentified format, as permitted by Applicable Data Protection Laws, for the purposes of developing and improving SingleStore's products and services and for its own analytics and product improvement processes.

3. SingleStore Personnel

SingleStore will take appropriate measures to restrict its personnel from Processing Customer Personal Data without authorization. SingleStore will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection, and data security, pursuant to Applicable Data Protection Laws.

4. Customer Affiliates

4.1 SingleStore's obligations set forth in this DPA also extend to Authorized Affiliates, subject to the following conditions:

(a) Customer is solely and exclusively responsible for communicating any Processing instructions on behalf of its Authorized Affiliates;

(b) Customer shall be responsible for its Authorized Affiliates' compliance with this DPA and all acts or omissions by its Authorized Affiliates with respect to Customer's obligations under this DPA; and

(c) if an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding, or other form of complaint or proceeding against SingleStore ("**Authorized Affiliate Claim**"), Customer must bring such Authorized Affiliate Claim directly against SingleStore on behalf of such Authorized Affiliate, unless Applicable Data Protection Laws require the Authorized Affiliate be a party to such claim, and all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Underlying Agreement, including any aggregate limitation of liability.

5. Disclosure to Third Parties; Data Subjects Rights

5.1 SingleStore will not disclose Customer Personal Data to any third party (including any government agency, court, or law enforcement agency) except as set forth in this DPA or with written consent from Customer, or as necessary to comply with applicable laws.

5.2 If SingleStore is obliged to disclose Customer Personal Data to any government agency, court, law enforcement agency, or any other government or public authority, or any third party pursuant to legal process ("Third-Party Demand"), SingleStore will attempt to redirect the Third-Party Demand to Customer. Customer agrees that SingleStore can provide information to such third party to the extent reasonably necessary to redirect the Third-Party Demand to Customer. If SingleStore cannot redirect the Third-Party Demand to Customer, then SingleStore shall, to the extent legally permitted to do so, provide Customer reasonable notice of the Third-Party Demand as promptly as is feasible under the circumstances to allow Customer to seek a protective order or other appropriate remedy.

5.3 In case Customer receives any request or communication from a Data Subject which relates to the Processing of Customer Personal Data ("**Request**"), SingleStore shall provide Customer with all necessary cooperation, information, and assistance ("**Assistance**") in relation to any such Request where instructed by Customer.

5.4 Where SingleStore receives a Request, SingleStore shall (i) not directly respond to such Request, (ii) forward the request to Customer without undue delay, and (iii) provide Assistance according to further instructions from Customer.

6. Assistance

6.1 Where a Data Protection Impact Assessment ("**DPIA**") or similar assessment is required under Applicable Data Protection Laws for the Processing of Customer Personal Data, SingleStore shall, upon request, provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation to carry out a DPIA or similar legally required assessment 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.

6.2 Customer shall pay SingleStore's reasonable charges mutually agreed between the Parties for providing the assistance in Section 6, to the extent that such assistance is not reasonably able to be accommodated within the normal provision of the Services.

7. Information Rights and Audit

7.1 SingleStore shall, in accordance with Applicable Data Protection Laws, make available to Customer on request in a timely manner such information as is necessary to demonstrate

compliance by SingleStore with its obligations under Applicable Data Protection Laws and this DPA.

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

7.3 Customer may request an audit of SingleStore's applicable controls, including an on-site inspection of its facilities. Such a request shall be in writing and include an audit plan, and both the request and audit plan will be provided to SingleStore at least six (6) weeks in advance of the proposed commencement date of the audit (or such shorter period as required by law or by a Supervisory Authority). The written request and audit plan shall set out the proposed scope, duration, and start date of the audit. SingleStore will review the audit plan and will notify Customer within two (2) weeks of receiving the audit plan if it agrees with the plan or if it has any objections in respect of the same. SingleStore and Customer shall mutually agree to the details of the audit. SingleStore will work cooperatively with Customer to agree on a final audit plan, and Customer's request for an audit shall be reasonable and proportional to the nature and complexity of the Services provided by SingleStore to Customer.

7.4 Any report or information produced as a result of the audit shall be considered the confidential information of SingleStore and may only be shared with a third party (including a Third-Party Controller) with SingleStore's prior written agreement. Customer must provide SingleStore with any audit reports or information generated pursuant to any audit at no charge, unless prohibited by applicable law. Customer shall keep the audit reports confidential and may use the audit reports only for the purposes of meeting its audit requirements under Applicable Data Protection Laws.

7.5 Where Customer has retained a third-party auditor to conduct an audit pursuant to Section 7.3 or review written documentation provided by SingleStore to Customer pursuant to Sections 7.1 or 7.2, such auditor may be required to execute a separate confidentiality agreement with SingleStore prior to any review of any information provided by SingleStore, or prior to commencing an audit of SingleStore. Further, SingleStore may object in writing to any auditor retained by Customer if in SingleStore's reasonable opinion the auditor is not suitably qualified or there is a conflict of interest. Any such objection will require Customer to either appoint another auditor or conduct the audit or review itself.

7.6 SingleStore may charge a reasonable fee for any audit conducted by Customer, taking into account the resources expended by SingleStore. Except as prohibited by applicable law, any audit of SingleStore's applicable controls shall be limited to no more than once every twelve (12) months..

7.7 SingleStore undertakes to cooperate with Customer in its dealings with a Supervisory Authority or other legal authority, and with any audit requests received from a Supervisory Authority or other legal authority.

8. Data Incident Management and Notification

8.1 SingleStore shall implement appropriate technical and organizational measures to ensure that Customer Personal Data is subject to a level of security appropriate to the risks arising from the Processing by SingleStore or its sub-processors by meeting the information security standards set out in Appendix B.

8.2 If SingleStore becomes aware of a Personal Data Breach involving SingleStore or one of its sub-processors with regard to Customer Personal Data, SingleStore shall:

a) notify Customer without undue delay, but in no event later than 72 hours after becoming aware of the incident;

b) make reasonable efforts to identify the cause of such incident and take those steps as SingleStore deems necessary and reasonable in order to remediate the cause of the incident to the extent that it is within SingleStore's reasonable control;

c) provide reasonable information, cooperation, and assistance to Customer in relation to any action to be taken in response to a Personal Data Breach under Applicable Data Protection Laws, including regarding any communication of the Personal Data Breach to Data Subjects and a Supervisory Authority or other legal authorities.

8.3 SingleStore's notification shall be sent to the email address registered by Customer within the Service for such purposes or, where no such email is registered, Customer acknowledges that the means of notification shall be at SingleStore's reasonable discretion.

8.4 The obligations contained in this Section 8 do not apply to Personal Data Breaches that are caused by Customer or Customer's users.

9. International Data Transfer

9.1 Customer Personal Data that SingleStore Processes for Customer as a Processor may be stored in or outside the EEA, UK, or Switzerland depending on the SingleStore product.

9.2 Where there is a Restricted Transfer, the following applies:

a) the Standard Contractual Clauses are incorporated into this DPA and deemed executed by each of the Parties acting on their own behalf and on behalf of their affiliates (where applicable) without the need for any further signature from either Party. If there is any conflict between the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses shall prevail;

b) the Standard Contractual Clauses shall cease to apply to the Processing of Customer Personal Data if and to the extent that the relevant transfer of Customer Personal Data ceases to be a Restricted Transfer and will re-apply if and to the extent that the relevant transfer becomes a Restricted Transfer again.

UK interpretation of Standard Contractual Clauses

9.3 For the purposes of any Restricted Transfer(s) that are made by a data exporter established in the UK, the Standard Contractual Clauses shall be deemed to be amended (and/or insofar as possible will be interpreted) so that they operate to provide appropriate safeguards to the transfer(s) in accordance with Articles 46 of the UK GDPR and shall be read mutatis mutandis as appropriate.

9.4 The Parties agree that this Section 9 incorporates the UK Addendum to the European Commission Standard Contractual Clauses issued by the ICO under or pursuant to section 119A(1) of the Data Protection Act 2018 (replaced and updated as necessary) and that, by entering into this DPA, the requirements of that addendum are binding on the Parties in accordance with Clause 12 of that addendum. Pursuant to section 19 and Table 4 of the UK Addendum, the Parties agree that the data exporter and data importer may end the UK Addendum as set out in Section 19 of the UK Addendum.

Swiss interpretation of Standard Contractual Clauses

9.5 The Parties agree that the Standard Contractual Clauses shall be read according to all applicable requirements under Swiss Data Protection Laws and shall be read mutatis mutandis as appropriate. In particular, the Parties agree that in relation to any transfers of Customer Personal Data from Switzerland, the Standard Contractual Clauses shall be read in conjunction with the FDPIC's decision and commentary on "*the transfer of personal data to a country with an inadequate level of data protection based on recognized standard contractual clauses and model contracts*", dated 27th August 2021.

10. Particulars of the Standard Contractual Clauses

10.1 For the purposes of Standard Contractual Clauses optional Clause 7 (Docking clause), Clause 7 is included in the Standard Contractual Clauses.

10.2 For the purposes of Clause 9 of the Standard Contractual Clauses (Use of sub-processors), the parties choose Option 2: General Written Authorisation, and the advance time period for informing Customer of a change in Sub-processor is ten (10) Business Days.

10.3 For the purposes of Clause 11 of the Standard Contractual Clauses (Redress) sub-clause (a), the optional clause is deleted.

10.4 For the purposes of Clause 13 of the Standard Contractual Clauses (Supervision), the parties choose Option (a).

10.5 For the purposes of Clause 17 of the Standard Contractual Clauses (Governing law), the parties choose Option 1, and the parties agree that this shall be the law of Ireland.

10.6 For the purposes of Clause 18 of the Standard Contractual Clauses (Choice of forum and jurisdiction) sub-clause (b), the parties choose the courts of Ireland.

10.7 The information required by Annex I Part A of the Standard Contractual Clauses (List of parties) can be found in the Underlying Agreement. The information required by Annex I Part B of the Standard Contractual Clauses (Description of transfer) can be found in Appendix A of this DPA. The information required by Annex I Part C of the Standard Contractual Clauses (Competent supervisory authority) is the Irish Data Protection Commissioner.

10.8 For the purposes of Annex II of the Standard Contractual Clauses and unless otherwise specified in the Underlying Agreement, the description of the technical and organizational measures for the security of Customer Personal Data are set out at Appendix B to this DPA.

10.9 For the purposes of Annex III of the Standard Contractual Clauses the information is set out in the Sub-processor Schedule (available from SingleStore on request).

11. CCPA Compliance

11.1 SingleStore will not: (i) sell or share (as the terms "sell" and "share" are defined under the CCPA) Customer Personal Data; (ii) use, retain, or disclose Customer Personal Data outside of its direct business relationship with Customer; (iii) use, retain, or disclose Customer Personal Data for any other purpose (including any other commercial purpose) other than as set forth in the Underlying Agreement and DPA, except as required by applicable law; or (iv) combine Customer Personal Data with Personal Data that it (a) receives from or on behalf of third parties or (b) collects from its own interactions with Data Subjects unrelated to the Services.

11.2 SingleStore grants Customer the right to take reasonable and appropriate steps to ensure that SingleStore uses Customer Personal Data in a manner consistent with Customer's obligations under the CCPA. SingleStore further grants Customer the right, upon notice, to take reasonable and appropriate steps to remediate any unauthorized use of Customer Personal Data. SingleStore will notify Customer if it can no longer meet its obligations under the CCPA or any regulations promulgated pursuant to the CCPA.

12. Term and Termination

12.1 This DPA becomes effective from the Effective Date and shall continue to operate for the duration of the Underlying Agreement.

13. Deletion or Return of Customer Personal Data

13.1 Customer may export all Customer Personal Data prior to the termination of Customer's account. In any event, following the termination of Customer's Account, (i) subject to (ii) and (iii) below and the Underlying Agreement, Personal Data will be retained for a period of seven (7) days from such termination within which Customer may contact SingleStore to export Customer Personal Data; (ii) where Customer does not use custom mailbox and uses the e-mail feature, if available within the Service(s), e-mails forming part of Personal 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, SingleStore reserves the right to delete all Personal Data in the normal course of operation except as necessary to comply with SingleStore's legal obligations, maintain accurate financial and other records, resolve disputes, and enforce its agreements. Personal Data cannot be recovered once it is deleted.

13.2 Customer may instruct SingleStore to delete the Personal Data at any time.

14. Miscellaneous

14.1 In case of any conflict, the provisions of this DPA shall take precedence over the provisions of any other agreement with SingleStore.

14.2 The limitation of liability stated in the Underlying Agreement shall apply to the breach of the DPA.

14.5 Any supplementary agreements or amendments to this DPA must be made in writing and signed by both Parties.

14.6 Should individual provisions of this DPA become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this DPA.

15. Definitions

“Applicable Data Protection Laws” means all data protection and privacy laws and regulations applicable to the processing of Personal Data pursuant to the Underlying Agreement and DPA, including European Data Protections Laws and the CCPA.

“Authorized Affiliate” means a Customer Affiliate who is authorized to use the Services pursuant to the Underlying Agreement and that has not signed its own separate agreement with SingleStore.

“CCPA” means the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 *et seq.*), as may be amended, superseded, or replaced from time to time.

“Controller” means an entity that determines the purposes and means of the Processing of Personal Data, and shall include the meaning given to it in European Data Protection Laws and includes “business” as that term is defined by the CCPA.

"Customer Personal Data” means Personal Data:

a) supplied to SingleStore by, or on behalf of Customer; and/or

b) obtained by, or created by, SingleStore on behalf of Customer in the course of delivery of Services.

For clarity, Customer Personal Data does not include Personal Data such as contact, billing, or other information provided by Customer to SingleStore or collected by SingleStore from Customer in SingleStore’s role as a Controller in order to provision the Services for Customer.

“Data Subject” means the identified or identifiable natural person to whom Customer Personal Data relates, and shall include the meaning given to it under European Data Protection Laws, and includes “consumer” as that term is defined by the CCPA.

“European Data Protection Laws” shall mean the GDPR and any applicable EU Member State national laws implementing or supplementing the GDPR, the UK Data Protection Laws, and the Swiss Data Protection Laws.

“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 SingleStore;

iii) the costs of compliance with investigations by a data protection authority or any other relevant legal or regulatory authority or agency.

“**EEA**” means European Economic Area.

“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.

“**ICO**” means the UK Information Commissioner’s Office.

“Personal Data” means any information relating to an identified or identifiable natural person and includes similarly defined terms in Applicable Data Protection Laws, including but not limited to, the definition of “personal information” in the CCPA.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data, and shall include the meaning given to it under European Data Protection Laws.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, or dissemination, and shall include the meaning given to it under European Data Protection Laws (the terms **"Process"**, **"Processes"**, and **"Processed"** shall be interpreted accordingly).

"Processor" means an entity that Processes Personal Data on behalf of a Controller, and shall include the meaning given to it under European Data Protection Laws.

"**Restricted Country**" means a country, territory or jurisdiction which is not considered by the EU Commission (or in respect of Customer Personal Data transfers caught by the requirements of UK Data Protection Laws or Swiss Data Protection Laws, the relevant UK and/or Swiss governmental or regulatory body as applicable) to offer an adequate level of protection in respect of the processing of Personal Data pursuant to Article 45(1) of the GDPR/UK GDPR (or equivalent provisions in the Swiss Data Protection Laws);

"**Restricted Transfer**" means a transfer of Customer Personal Data from an entity whose processing of Customer Personal Data under the DPA is caught by the requirements of the European Data Protection Laws, to an entity that processes the relevant Customer Personal Data in a Restricted Country.

"Standard Contractual Clauses" means the standard contractual clauses 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 (Module 2 Controller to Processor), as supplemented by Section 10 of this DPA.

"**Supervisory Authority**" shall have the meaning given to it in the GDPR/UK GDPR. For processing subject to the UK GDPR, Supervisory Authority shall mean ICO.

"**Swiss Data Protection Laws**" means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in Switzerland including the Swiss Data Protection Act 1992 and the Swiss Data Protection Act 2020 (as in force and applicable).

"**UK**" means the United Kingdom.

"**UK Data Protection Laws**" means all laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

"**UK GDPR**" means the UK GDPR as defined by section 3(10) of the UK Data Protection Act 2018.

"**Underlying Agreement**" shall mean the Customer agreement (whether Cloud Service Agreement (formerly Managed Service Agreement) or Self Managed License Agreement (formerly On Premises License Agreement)) available at https://www.SingleStore.com/legal/, or an equivalent master Service agreement executed between the Parties, including any order documents or statements of work for Service entered into between SingleStore and Customer.

Appendix A: Customer Personal Data

This Appendix includes certain details of the Processing of Customer Personal Data.

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

The subject matter of the Processing under this DPA is the Customer Personal Data. SingleStore will process the Customer Personal Data until termination of the Agreement and subsequent deletion of all Customer Personal Data as described in the Underlying Agreement and this DPA.

2. The nature, purpose and frequency of the Processing of Customer Personal Data

SingleStore will perform Processing as needed to provide the Services and to comply with Customer's Processing instructions as provided in accordance with the Underlying Agreement and this DPA. SingleStore will Process the Customer Personal Data only as needed to provide the Services and as described in this DPA. SingleStore will Process the Customer Personal Data continuously until deletion of all Customer Personal Data. Where there is a Restricted Transfer, the frequency of the transfer will be on a continuous basis.

3. The types of Customer Personal Data to be Processed

The types of Customer Personal Data are determined and controlled by Customer in its sole discretion and may include, but are not limited to identification and contact data, employment-related data, and information technology information such as IP addresses or cookies data.

4. The categories of Data Subjects to whom Customer Personal Data relates

The categories of Data Subjects to which Customer Personal Data relate are determined and controlled by Customer in its sole discretion and may include, but are not limited to, customers, business partners, vendors, or employees.

5. The period for which Customer Personal Data will be retained

The period for which Customer Personal Data will be retained is set out in Clause 13 of this DPA.

Appendix B: SingleStore, Inc. Technical and Organizational Measures

a. Personal Data Storage

SingleStore is a global company providing services through all major cloud solution providers (CSPs). SingleStore Cloud 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 Personal Data. Customers using SingleStore on their own infrastructure are responsible for ensuring that adequate encryption is in place. For SingleStore Cloud Service encryption at rest is provided through CSP native technologies supporting AES-256 encryption and for encryption at rest TLS 1.2 is fully supported, however this requires customer configuration.

c. Support and Maintenance

SingleStore deploys changes to SingleStore Cloud 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 on said maintenance.

d. Breach Response and Notification

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 DP Losses. 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 Personal Data Breach SingleStore will (A) notify you without undue delay and in any event within 72 hours of becoming aware of the Personal Data Breach, (B) reasonably cooperate with you with respect to such Personal Data Breach, and (C) take appropriate corrective action to mitigate any risks or damages involved with the Personal Data Breach to protect Customer Personal Data from further compromise. SingleStore will take any other actions that may be required by applicable law as a result of the Personal Data 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 Customer Personal 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 GRC Program Manager 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 and 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 antivirus technology is installed and activated on all SingleStore 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. SingleStore uses full-disk encryption on all managed 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 security monitoring tools that proactively alert 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 SingleStore's GRC Program Manager and Information Security Steering Committee. 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.

IN WITNESS WHEREOF, the parties intending to be bound have caused this DPA to be executed as follows:

SINGLESTORE, INC.	**CUSTOMER: _____**
By: _____	By: _____
Print: _____	Print: _____
Title: _____	Title: _____
Dated: _____	Dated: _____