DATA PROCESSING AND SECURITY ADDENDUM (NON-PLATFORM SERVICES)

This Data Processing and Security Addendum ("**Services DPA**"), effective as of the date both parties have executed this Services DPA (the "**Effective Date**"), forms a part of the Databricks Master Services Agreement concurrently entered into between the parties, unless you ("**Customer**") have entered into a superseding written master subscription agreement with Databricks, Inc. ("**Databricks**"), in which case, it forms a part of such written agreement (in either case, the "**Agreement**").

By signing the Services DPA or executing an Agreement that explicitly states that this Services DPA is incorporated by reference, Customer enters into this Services DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws, in the name and on behalf of any Affiliates (defined below) who are authorized to receive Databricks Services. If you are entering into this Services DPA on behalf of a company (such as your employer) or other legal entity, you represent and warrant that you have the authority to bind that company or legal entity to this Services DPA. In that case, "**Customer**" will refer to that company or other legal entity. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

If the Customer entity signing this Services DPA is a party to the Agreement, this Services DPA is an addendum to and forms part of the Agreement. In such case, the Databricks entity that is party to the Agreement is party to this Services DPA. If the Customer entity signing this Services DPA has executed an Order Form with Databricks pursuant to the Agreement, but is not itself a party to the Agreement, this Services DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Databricks entity that is party to such Order Form is party to this Services DPA. If the Customer entity signing this Services DPA is neither a party to an Order Form nor the Agreement, this Services DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this Services DPA.

1. DEFINITIONS

1.1 **"Affiliate"** means, with respect to the identified party, any entity that is directly or indirectly controlled by, controlling or under common control with such party.

1.2 **"Applicable Data Protection Laws"** means all worldwide data protection and privacy laws and regulations applicable to Customer Data in question, including, where applicable and without limitation, EU Data Protection Law and the California Consumer Privacy Act of 2018.

1.3 "**Authorized Person(s)**" means any person who processes Customer Data or Customer Data on Databricks' behalf under the Agreement, including Databricks' employees, officers, partners, principals and Subcontractors.

1.4 "**California Consumer Privacy Act of 2018**" or "**CCPA**" means Cal. Civ. Code § 1798.100, *et seq.*, as amended.

1.5 "**Customer Data**" means the data and information Customer makes available to Databricks under the Agreement for the purposes of permitting Databricks to perform the Databricks Services, provided that Customer Data does not include data contained within the Platform Services except to the limited extent an Authorized Person is asked to perform actions against such data.

1.6 "**Customer Data**" means any Customer Data that is Personal Data .

1.7 **"Data Subject"** means the identified or identifiable natural person to whom the Customer Data relates, including 'consumers' (as defined in the CCPA) where applicable.

1.8 "**Databricks Services**" means, for the purposes of this Services DPA, the Professional Services and/or Training Services Databricks provides under an Agreement, excluding for the avoidance of doubt the Platform Services.

1.9 "**EEA**" means, for the purposes of this Services DPA, the European Economic Area and its member states, including for the avoidance of doubt the United Kingdom, and Switzerland.

1.10 **"EU Data Protection Law"** means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**").

1.11 "**Personal Data**" means information relating to an identified or identifiable **Data Subject**; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. For the avoidance of doubt, Personal Data includes, where applicable, personally identifiable information and personal information (as defined in the CCPA).

1.12 "**Platform Services**" means the Databricks software as a service platform.

1.13 "**Privacy Shield**" means the EU-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 dated July 12, 2016 (as may be amended, superseded, or replaced).

1.14 "**Privacy Shield Principles**" means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of 12 July 2016 pursuant to the Directive, details of which can be found at www.privacyshield.gov/eu-us-framework.

1.15 **"Security Breach"** means a breach of security leading to any accidental, unauthorized or unlawful loss, disclosure, destruction, alteration, or access to Customer Data.

1.16 "**Sensitive Data**" means any (i) bank, credit card or other financial account numbers or login credentials, (ii) social security, tax, driver's license or other government-issued identification numbers, (iii) health information identifiable to a particular individual; (iv) information that could reasonably be used to determine the physical location of a particular individual or (v) any "special" or "sensitive" categories of data as those terms are defined according to EU Data Protection Law or any similar category under other Applicable Data Protection Laws.

1.17 **"Subcontractor"** means any third party (including any Databricks' Affiliate) engaged by Databricks to perform the Services, including to the extent such third party is engaged to process any Customer Data on behalf of Customer (such Subcontractors, "**Subprocessors**").

The terms "**Controller**", "**Processor**," "**process**," and "**processing**," have the meanings given to them in Applicable Data Protection Laws. The term Controller also includes 'businesses' (as defined in the CCPA) and the term Processor includes 'service providers' (as defined in the CCPA) to the extent the rights and obligations described herein apply under the CCPA. If and to the extent that Applicable Data Protection Laws do not define such terms, then the definitions given in EU Data Protection Law will apply.

2. PURPOSE; SCOPE

2.1 Customer and Databricks have entered into the Agreement pursuant to which Customer is being provided Databricks Services. The parties acknowledge and agree that it is the expectation of both parties that (a) the purpose of the Agreement is **not** for Databricks to process Personal Data on behalf of Customer or any Customer Affiliates; and (b) that, accordingly, Customer agrees that it will limit Databricks' access to Personal Data to the extent necessary to perform the Databricks Services.

2.2 Section 2.1 notwithstanding, this Services DPA shall apply where and **only** to the extent that Databricks processes Customer Data on behalf of Customer as a Processor in the course of providing Databricks Services pursuant to the Agreement.

2.3 Accordingly, if Databricks processes any such Customer Personal Data, Databricks shall process Customer Personal Data (i) only as a Processor acting on behalf of Customer (whether as Controller or itself a Processor on behalf of third party Controllers); and (ii) in accordance with Customer's documented instructions as set forth in this Services DPA, the Agreement(s) or as otherwise necessary

to provide the Databricks Services; *provided that* Databricks shall inform Customer if, in its opinion, Customer's processing instructions infringe any law or regulation; in such event, Databricks is entitled to refuse processing of Personal Data that it believes to be in violation of any law or regulation. Without limiting the foregoing, Databricks will not 'sell' Customer Data (as such term is defined in the CCPA).

2.4 For the avoidance of doubt, and notwithstanding anything to the contrary in the Agreement or this Services DPA, this Services DPA does not apply to the Databricks Platform Services, which are subject to, with respect to the Databricks Platform Services on Amazon Web Services, an agreement between Customer and Databricks, and with respect to the Azure Databricks Platform Services, an agreement between Customer and Microsoft Corporation.

3. SUBCONTRACTING

3.1 Notwithstanding anything to the contrary in the Agreement, Customer agrees that Databricks may appoint Subcontractors to assist it in providing the Databricks Services, provided that:

(a) such Subcontractors are bound to a written agreement substantially as protective of Customer Data and Personal Data as the Agreement and this Services DPA;
(b) agree to act only on Databricks' instructions when processing the Customer Data or Customer Data (which instructions shall be consistent with Customer's processing instructions to Databricks); and
(c) agree to protect the Customer Data and Customer Data to a standard consistent with the requirements of this Services DPA, including by implementing and maintaining appropriate technical and organizational measures to protect the Customer Data and Customer Data they process consistent with the Security Standards.

3.2 Databricks remains fully liable for any breach of this Services DPA or the Agreement that is caused by an act, error or omission of such Subcontractors to the extent Databricks would have been liable for such act, error or omission had it been caused by Databricks.

3.3 Additionally, while it is not the intention of either party that such Subcontractors process Personal Data on behalf of Customer, to the extent Databricks becomes aware that a Subcontractor processes or may process Personal Data during the performance of the Databricks Services, Databricks will notify Customer that such Subcontractor is acting as a Subprocessor. In the event that Customer objects to the processing of Customer Data by any such Subcontractor, it shall inform Databricks in writing within 10 calendar days after notice has been provided by Databricks. In the event that Customer timely objects on reasonable grounds relating to the protection of Customer Data Databricks will either, at Databricks option (a) appoint a different Subcontractor reasonably acceptable to Customer to act as a Subprocessor; or (b) instruct the Subcontractor to not process Customer Data.

4. COOPERATION

4.1 Databricks will promptly notify Customer if it becomes aware that it is acting as a processor for any Customer Data or otherwise has been provided any Customer Data by Customer. The parties agree that, unless otherwise mutually agreed by the parties, Databricks may at its option delete any Customer Data in order to no longer be deemed a processor of Customer. Additionally, at Customer's written request and expense, Databricks will make reasonable efforts to assist Customer with compliance with Applicable Data Protection Laws to the extent applicable to the performance of the Databricks Services by Databricks.

4.2 If Applicable Data Protection Laws and corresponding obligations related to the processing of Personal Data change, the parties shall discuss in good faith any necessary amendments to this Services DPA and/or the Agreement.

5. DATA ACCESS & SECURITY MEASURES

5.1 Databricks shall ensure that any Authorized Person is subject to a duty of confidentiality (whether a contractual or statutory duty) and that they process Customer Data (including any Customer Data contained therein) only for the purpose of delivering the Databricks Services under the Agreement(s) to Customer.

5.2 Databricks will implement and maintain appropriate technical and organizational security measures to protect against Security Breaches and to preserve the security, availability, integrity and confidentiality of Customer Data ("**Security Measures**") and will review such Security Measures on at least an annual basis. Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

6. SECURITY INCIDENTS

6.1 In the event of a Security Breach, Databricks shall inform Customer without undue delay and provide written details of the Security Breach, including the type of data affected and the identity of affected person(s) as soon as such information becomes known or available to Databricks.

6.2 Furthermore, in the event of a Security Breach, Databricks shall:

(a) provide timely information and cooperation as Customer may reasonably require to fulfill Customer's data breach reporting obligations under Applicable Data Protection Laws; and

(b) take such measures and actions as are appropriate to remedy or mitigate the effects of the Security Breach and shall keep Customer up-to-date about all developments in connection with the Security Breach.

7. SECURITY REPORTS & INSPECTIONS; AUDITS

7.1 The parties acknowledge that Databricks uses external auditors to verify the adequacy of its Security Measures. This audit:

(a) will be performed at least annually;

(b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001;

(c) will be performed by independent third-party security professionals at Databricks' selection and expense; and

(d) will result in the generation of an audit report affirming that Databricks' data security controls achieve industry standards under Service Organization Controls No. 2 (SOC2) in accordance with AT-C 205 or such other alternative standards that are substantially equivalent to SOC 2 Type 2 ("**Report**").

7.2 At Customer's written request, Databricks will provide Customer with copies of its Report so that Customer can reasonably verify Databricks' compliance with the security and audit obligations under this Agreement. The Report and any summaries thereof will constitute Databricks' Confidential Information under the confidentiality provisions of the Agreement.

7.3 Databricks will respond in a commercially reasonable timeframe to any requests for additional information or clarification from Customer related to such Report.

8. DATA TRANSPORT

8.1 To the extent that Databricks processes any Customer Data subject to EU Data Protection Law ("**EEA Data**") on behalf of Customer, the parties agree that Databricks makes available the transfer mechanisms listed below for any transfers of EEA Data from the EEA to Databricks located in a country

which does not ensure an adequate level of protection (within the meaning of Applicable Data Protection Laws) and to the extent such transfers are subject to such EU Data Protection Law:

(a) (i) Databricks will be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for EEA Data by virtue of having self-certified its compliance with the Privacy Shield; (ii) Databricks agrees to process EEA Data in compliance with the Privacy Shield Principles; (iii) if Databricks is unable to comply with its obligations under this sub-Section, Databricks will inform the Customer; and (iv) Databricks will promptly cease (and cause its Subprocessors to promptly cease) processing such EEA Data if in Customer's sole discretion, Customer determines that Databricks has not or cannot correct any non-compliance with this sub-Section in accordance with the Privacy Shield Principles within a reasonable time frame.

(b) To the extent the transfer mechanism identified in Section 8.1(a) does not apply to the transfer, is invalidated and/or Databricks is no longer self-certified to the Privacy Shield, the parties agree to mutually negotiate sufficient data protection measures or modify the Agreement so that Databricks will not act as a processor with respect to any Customer Personal Data.

9. DELETION & RETURN

Upon Customer's request upon termination or expiry of the Agreement, Databricks shall destroy all Customer Data (including Customer Data) in its possession or control. This requirement shall not apply to the extent that Databricks is required by any applicable law to retain some or all of the Customer Data (including Customer Data), in which event Databricks shall isolate and protect such data from any further processing except to the extent required by such law.

10. GENERAL

10.1 The parties agree that this Services DPA shall replace any existing Services DPA (including the Standard Contractual Clauses (as applicable)) the parties may have previously entered, solely to the extent it applies to the Databricks Services specified under this Services DPA.

10.2 This Services DPA shall be effective on the date of the last signature set forth below. The obligations placed upon Databricks under this Services DPA shall survive so long as Databricks and/or its Subcontractors processes Customer Data on behalf of Customer.

10.3 This Services DPA may not be modified except by a subsequent written instrument signed by both parties.

10.4 If any part of this Services DPA is held unenforceable, the validity of all remaining parts will not be affected.

10.5 In the event of any conflict between this Services DPA and any data privacy provisions set out in any Agreements the parties agree that the terms of this Services DPA shall prevail. Notwithstanding the foregoing, if there is any conflict between this Services DPA and a BAA applicable to any patient, medical or other protected health information regulated by HIPAA or any similar U.S. federal or state laws, rules or regulations applicable to health information, then the BAA shall prevail to the extent the conflict relates to such data.

10.6 Notwithstanding anything to the contrary in the Agreement or this Services DPA, each party's and all of its affiliates' liability, taken together in the aggregate, arising out of or related to this Services DPA, any Order or the Agreement, whether in contract, tort or under any other theory of liability, shall remain subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the Agreement and this Services DPA, including all Annexes hereto. Without limiting either of the parties' obligations under the Agreement, Customer agrees that any regulatory penalties incurred by

Databricks in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this Services DPA or any Applicable Data Protection Laws shall count toward and reduce Databricks' liability under the Agreement as if such penalties were liabilities to the Customer under the Agreement.

10.7 This Services DPA will be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Laws.

10.8 This Services DPA will terminate simultaneously and automatically with the termination or expiry of the Agreement.

[*signature page follows*]

By signing below, each party acknowledges that it has read and understood the terms of this Services DPA and agrees to be bound by them.

Customer:	**Databricks, Inc.**
_____	
By:_____	By:_____
Name:_____	Name: Scott Starbird
Title:_____	Title: VP, Legal
Address:	Date:_____
_____	
_____	
_____	
_____	
Date:_____	