databricks

DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Annexes and the Standard Contractual Clauses ("**DPA**"), forms an integral part of the Databricks Master Cloud Services Agreement, or any other written agreement that governs Customer's use of the Databricks Services (as defined below) entered into between the entity identified as the "Customer" in the signature block below ("**Customer**") and Databricks, Inc. ("**Databricks"**) (the "**Agreement**"), and applies solely to the extent that Databricks processes any Personal Data (defined below) in connection with the Databricks Services. By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. For the purposes of the DPA only, and except where otherwise indicated, the term "Customer" shall include Customer and its Authorized Affiliates.

1. DEFINITIONS

1.1. **"Applicable Data Protection Laws"** means all data protection and privacy laws and regulations applicable to the processing of Personal Data under the Agreement, including (where applicable) European Data Protection Laws and the CCPA.

1.2. **"Authorized Affiliate**" means a Customer Affiliate who is authorized to use the Databricks Services under the Agreement and who has not signed their own separate "Agreement" with Databricks.

1.3. **"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 Code § 1798.100, *et seq.)*, as may be amended, superseded or replaced from time to time.

1.4. "**Customer Content"** means, if not defined within the Agreement, all data input into or made available by Customer for processing within the Databricks Services or generated from the Databricks Services.

1.5. **"Databricks Services"** means the Platform Services and/or any other services (e.g. Advisory or Support Services) provided directly by Databricks to Customers under the Agreement.

1.6. **"European Data Protection Laws"** means (a) Regulation 2016/679 (General Data Protection Regulation) ("**EU GDPR**"); (b) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); and (c) the Swiss Federal Data Protection Act and its implementing regulations ("**Swiss Data Protection Act**"); in each case as may be amended, superseded or replaced from time to time.

1.7. **"Personal Data"** means any 'personal data' or 'personal information' contained within Customer Content or provided to Databricks for processing under the Agreement by or on behalf of Customer in the provision of the Databricks Services.

1.8. **"Restricted Transfer"** means a transfer (directly or via onward transfer) of personal data that is subject to European Data Protection Laws to a third country outside the European Economic Area, United Kingdom and Switzerland which is not subject to an adequacy determination by the European Commission, United Kingdom or Swiss authorities (as applicable).

1.9. **"Security Addendum"** means the security addendum found at Databricks.com/legal/security-addendum.

1.10. **"Security Breach"** means a breach of security leading to an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

1.11. **"Standard Contractual Clauses"** or **"SCCs"** means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as may be amended, superseded or replaced from time to time.

1.12. **"Subprocessor"** means any other processor engaged by Databricks (including any Databricks Affiliate) to process Personal Data.

1.13. **"UK Addendum"** means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioners Office under S.119 (a) of the UK Data Protection Act 2018, as updated or amended from time to time.

1.14. The terms **"controller"**, **"data subject"**, **"supervisory authority"**, **"processor"**, **"process"**, **"processing"**, **"personal data"**, and **"personal information"** shall have the meanings given to them in Applicable Data Protection Laws. The term "controller" includes "business", the term "data subject" includes "consumers", and the term "processor" includes "service provider" (in each case, as defined by the CCPA).

2. PROCESSING OF PERSONAL DATA

2.1. **Scope and Roles of the Parties.** This DPA applies when Personal Data is processed by Databricks as a processor or subprocessor in its provision of the Databricks Services to Customer, who will act as either a controller or processor of Personal Data.

2.2. **Customer Processing.** Customer shall have sole responsibility for the accuracy and quality of Personal Data, and for providing any notices and obtaining any consents, permissions and rights required to enable Databricks to process Personal Data. Customer shall ensure that its instructions and processing of Personal Data comply with Applicable Data Protection Laws.

2.3. **Databricks Processing.** Databricks shall process Personal Data only in accordance with Customer's documented lawful instructions. For these purposes, Customer instructs Databricks to process Personal Data for the following purposes: (a) processing in accordance with the Agreement and any applicable Order Form(s); (b) processing initiated by Customer and Authorized Users in their use or configuration of the Databricks Services; and (c) processing to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement. Databricks is not responsible for determining if Customer's instructions are compliant with applicable law. However, Databricks shall notify Customer in writing if, in its reasonable opinion, the Customer's processing instructions infringe Applicable Data Protection Laws and provided that Customer acknowledges that Personal Data may be processed on an automated basis in accordance with Customers' use of the Databricks Services, which Databricks does not monitor.

2.4. **Details of Processing.** The details of the processing of Personal Data by Databricks are set out in Annex A to the DPA.

3. CONFIDENTIALITY

3.1. **Personnel.** Databricks shall ensure that any employees or personnel it authorizes to process Personal Data is subject to an appropriate duty of confidentiality.

4. SUBPROCESSING

4.1. **Authorization.** Customer provides a general authorization to Databricks use of Subprocessors to process Personal Data in accordance with this Section, including those Subprocessors listed at www.Databricks.com/subprocessors ("**Subprocessor List**").

4.2. **Subprocessor Obligations.** Databricks shall (i) enter into a written agreement with its Subprocessors, which includes data protection and security measures no less protective of Personal Data than the Agreement and this DPA; and (ii) remain fully liable for any breach of the Agreement and this DPA that is caused by an act, error or omission of its Subprocessors to the extent that Databricks would have been liable for such act, error or omission had it been caused by Databricks.

4.3. **Subprocessor Changes.** At least thirty (30) calendar days prior to the date on which any new Subprocessor shall commence processing Personal Data, Databricks shall update the Subprocessor List and provide Customer with notice of that update. Such notice will be sent to individuals who have signed up to receive updates to the Subprocessor List via the mechanism(s) indicated on the Subprocessor List.

4.4. **Subprocessor Objections.** Customer may object to Databricks' appointment of a new Subprocessor on reasonable grounds relating to data protection by notifying Databricks in writing at privacy@databricks.com within ten (10) calendar days after receiving notice pursuant to Section 4.3. In such event, Databricks shall either: (a) work with Customer to address Customer's objections to its reasonable satisfaction; (b) instruct the Subprocessor to not process Personal Data; or (c) notify Customer of its option to terminate the Agreement and this DPA within fourteen (14) calendar days. If Customer exercises its right to terminate the Agreement and this DPA, Databricks will provide Customer with a pro rata reimbursement of any prepaid, but unused fees.

5. ASSISTANCE

5.1. **Data Subject Requests.** Customer is responsible for responding to and complying with data subject requests ("**DSR**"). The Databricks Services include controls that Customer may use to assist it to respond to DSR. If Customer is unable to access or delete any Personal Data using such controls, Databricks shall, taking into account the nature of the processing, reasonably cooperate with Customer to enable Customer to respond to the DSR. If a data subject sends a DSR to Databricks directly and where Customer is identified or identifiable from the request, Databricks will promptly forward such DSR to Customer and Databricks shall not, unless legally compelled to do so, respond directly to the data subject except to refer them to the Customer to allow Customer to respond as appropriate.

5.2. **Data Protection Impact Assessments**. Databricks will provide commercially reasonable assistance to Customer (at Customer's expense) with respect to any legally required data protection impact assessment relating to the processing or proposed processing of Personal Data in connection with the Databricks Services and any related required consultation with supervisory authorities.

5.3. **Legal Requests.** If Databricks receives a subpoena, court order, warrant or other legal demand from law enforcement or any public or judicial authority seeking the disclosure of Personal Data, Databricks will attempt to redirect the governmental body to request such Personal Data directly from Customer. As part of this effort, Databricks may provide Customer's basic contact information to the governmental body. If compelled to disclose Personal Data to a governmental body, then Databricks will give Customer reasonable notice of the legal demand to allow Customer to seek a protective order or other appropriate remedy, unless Databricks is legally prohibited from doing so.

6. SECURITY

6.1. **Security Measures.** Databricks has implemented and will maintain appropriate technical and organizational security measures as set forth in the Security Addendum ("**Security Measures**"). The Security Measures are subject to technical progress and development and Databricks may update the Security Measures, provided that any updates shall not materially diminish the overall security of Personal Data or the Databricks Services. Databricks may make available certain security controls within the Databricks Services that Customer may use in accordance with the Documentation.

6.2. **Security Breach Notification.** In the event of a Security Breach, Databricks will (a) notify Customer in writing without undue delay and in no event later than seventy-two (72) hours after becoming aware of the Security Breach; and (b) promptly take reasonable steps to contain, investigate, and mitigate any adverse effects resulting from the Security Breach. Databricks will reasonably cooperate with and assist Customer with respect to any required notification to supervisory authorities or data subjects (as applicable), taking into account the nature of the processing, the information available to Databricks, and any restrictions on disclosing the information (such as confidentiality).

7. AUDITS AND RECORDS

7.1. **Audit Program.** Databricks uses external auditors to verify the adequacy of its security measures with respect to its processing of Personal Data. Such audits are performed (a) at least once annually; (b) according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; and (c) by independent third party security professionals selected by Databricks. Such audits result in the generation of a confidential audit report ("**Audit Report**").

7.2. **Audit Report.** At Customer's written request, and no more than once every twelve (12) months, Databricks will provide Customer with a copy of the Audit Report so that Customer can verify Databricks' compliance with this DPA. The Audit Report shall be considered Databricks' confidential information and subject to the confidentiality provisions of the Agreement. To the extent that the Audit Report is deemed insufficient by a supervisory authority, Customer may request an on-site audit, subject to the additional terms in Section 7.3.

7.3. **Onsite Audit**. An on-site audit shall be conducted by Customer (a) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Databricks Services used by Customer; (b) up to one time per year with at least three weeks' advance written notice; and (c) during Databricks normal business hours, under reasonable duration and shall not unreasonably interfere with Databricks' day-to-day operations. Further, before any on-site audit commences, Customer and Databricks shall mutually agree upon the scope, timing, duration of the audit and costs for which Customer shall be responsible.

8. TRANSFER OF PERSONAL DATA

8.1. **Restricted Transfers.** Where the transfer of Personal Data to Databricks is a Restricted Transfer, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form an integral part of the Agreement in accordance with Annex B of this DPA.

8.2. **Alternative Transfer Mechanisms**. If and to the extent that a court of competent jurisdiction or a supervisory authority with binding authority orders (for whatever reason) that the measures described in this DPA cannot be relied on to lawfully transfer Personal Data to Databricks, the parties shall reasonably cooperate to agree and take any actions that may be reasonably required to implement any additional measures or alternative transfer mechanism to enable the lawful transfer of such Personal Data. Additionally, in the event Databricks adopts an alternative transfer mechanism (including any successor version of the Privacy Shield), such alternative transfer mechanism shall apply instead of the SCCs described in Section 8.1 of this DPA (but only to the extent such alternative transfer mechanism complies with applicable European Data Protection Laws and extends to the territories to which Personal Data is transferred).

9. BACKUP, DELETION & RETURN

9.1. **No Backups.** The Databricks Services do not include backup services or disaster recovery for Personal Data. Databricks does provide functionality within the Databricks Services that may permit Customer to backup certain Personal Data on its own. It is the Customer's obligation to backup any Personal Data if desired.

9.2. **Deletion.** The Databricks Services include controls that Customer may use at any time during the term of the Agreement to retrieve or delete Personal Data. Subject to the terms of the Agreement, Databricks will delete Personal Data from the Databricks Services when Customer uses such controls to send an instruction to delete.

9.3. **Termination.** Upon termination or expiration of the Agreement and following Customer's written request, Databricks will delete or assist Customer in deleting any Personal Data within its possession or control within thirty (30) days following such request.

10. CCPA Compliance

10.1. Databricks shall not process, retain, use, or disclose Personal Data for any purpose other than for the purposes set out in the Agreement, DPA and as permitted under the CCPA. Databricks shall not sell or share information as those terms are defined under the CCPA.

11. GENERAL

11.1. The parties agree that this DPA shall replace any existing data processing addendum, attachment, exhibit or standard contractual clauses that the parties may have previously entered into in connection with the Databricks Services.

11.2. This DPA may not be modified except by subsequent written agreement of the parties.

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

11.4. Databricks' obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions: (a) Customer is solely responsible for communicating any processing instructions on behalf of its Authorized Affiliates; (b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate 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 otherwise against Databricks ("**Authorized Affiliate Claim**"), Customer must bring such Authorized Affiliate Claim directly against Databricks 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 Agreement, including any aggregate limitation of liability.

11.5. In the event of any conflict between this DPA and any data privacy provisions set out in any agreements between the parties relating to the Databricks Services, the parties agree that the terms of this DPA shall prevail, provided that if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses control and take precedence. If there is any conflict between this DPA and a Business Associate Agreement entered into between the parties ("**BAA**"), then the Business Associate Agreement shall prevail to the extent of any conflict solely with respect to any PHI (as defined in such BAA).

11.6. Notwithstanding anything to the contrary in the Agreement or this DPA and to the maximum extent permitted by law, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA (including all Annexes hereto), the SCCs or any data protection agreements in connection with the Agreement (if any), 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 DPA, including all Annexes hereto. Customer agrees that any regulatory penalties incurred by Databricks that arise in connection with Customer's failure to comply with its obligations under this DPA or any Laws or regulations including Applicable Data Protection Laws shall reduce Databricks' liability under the Agreement as if such penalties were liabilities to Customer under the Agreement.

11.7. This 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.

11.8. The obligations placed upon each party under this DPA and the Standard Contractual Clauses shall survive so long as Databricks processes Personal Data on behalf of Customer.

[SIGNATURE PAGE FOLLOWS]

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

Customer:________________________	**Databricks, Inc.**
By:______________________________	By:______________________________
Name:___________________________	Name: Scott Starbird
Title:_______________________________________	Title: General Counsel, Public Affairs and Strategic Partnerships
Date:____________________________	Date:______________________
Contact Person:__________________________	
Contact Title:______________________________	
Contact Email:____________________	

ANNEX A

DESCRIPTION OF THE PROCESSING / TRANSFER

ANNEX 1(A): LIST OF PARTIES	
Data exporter	**Name of the data exporter:** The entity identified as the “Customer” in the Agreement and this DPA. **Contact person’s name, position and contact details:** The address and contact details associated with Customer's Databricks account, or as otherwise specified in this DPA or the Agreement. **Activities relevant to the data transferred:** The activities specified in Annex 1(B)below. **Signature and date**: See front end of the DPA. **Role (Controller/Processor):** Controller (for Module 2) or Processor (for Module 3).
Data importer	**Name of the data importer:** Databricks, Inc. **Contact person’s name, position and contact details:** Scott Starbird, General Counsel, Public Affairs and Strategic Partnerships, dpa@databricks.com **Activities relevant to the data transferred:** The activities specified in Annex 1.B below. **Signature and date**: See front end of the DPA. **Role (Controller/Processor):** Processor
ANNEX 1(B): DESCRIPTION OF THE PROCESSING / TRANSFER	
Categories of data subjects whose personal data is transferred:	Data subjects include individuals about whom data is provided to Databricks via the Databricks Services (by or at the direction of Customer), which shall include: ____ ____ ____ ____ ____ ____ IF CUSTOMER HAS NOT FILLED OUT THE ABOVE SECTION: Customer shall be deemed to have declared that the categories of data subjects include: (a) individual contacts, prospects, customers, business partners and vendors of Customer (who are natural persons); (b) employees or contact persons of Customer’s prospects, customers, business partners and vendors; (c) employees, agents, advisors, freelancers of Customer (who are natural persons); (d) Customer’s Authorized Users or (e) other individuals whose personal data is included in Customer Content.
Categories of personal data transferred:	The types of Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to: ____ ____ ____ ____ ____ ____

	IF CUSTOMER HAS NOT FILLED OUT THE ABOVE SECTION: Customer shall be deemed to have declared that the types of Personal Data may include but are not limited to the following types of Personal Data: (a) name, address, title, contact details; and/or (b) IP addresses, cookies data, location data; and (c) any other personal data processed in the course of the Services as Customer Content.
Sensitive data transferred (if appropriate)	Subject to any applicable restrictions and/or conditions in the Agreement and this DPA, Customer may include 'special categories of personal data' or similarly sensitive personal data (as described or defined in Applicable Data Protection Laws) in Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purposes of uniquely identifying a natural person, data concerning health and/or data concerning a natural person's sex life or sexual orientation.
Frequency of the Transfer	Continuous or one-off depending on the services being provided by Databricks.
Nature, subject matter and duration of the processing:	<u>Nature</u>: Databricks provides a cloud-based unified data analytics platform and related services, as further described in the Agreement. <u>Subject Matter</u>: Personal Data. <u>Duration</u>: The duration of the processing will be for the term of the Agreement and any period after the termination or expiry of the Agreement during which Databricks processes Personal Data.
Purpose(s) of the data transfer and further processing:	Databricks shall process Personal Data for the following purposes: (a) as necessary for the performance of the Databricks Services and Databricks' obligations under the Agreement (including the DPA), including processing initiated by Authorized Users in their use and configuration of the Databricks Services; and (b) further documented, reasonable instructions from Customer agreed upon by the parties (the "**Purposes**").
Period for which the personal data will be retained:	Databricks will retain Personal Data for the term of the Agreement and any period after the termination of expiry of the Agreement during which Databricks processes Personal Data in accordance with the Agreement.

ANNEX 1(C): COMPETENT SUPERVISORY AUTHORITY

Competent supervisory authority	The data exporter's competent supervisory authority will be determined in accordance with the EU GDPR.

ANNEX B

STANDARD CONTRACTUAL CLAUSES (Modules 2 and 3)

1. Subject to Section 8.1 of the DPA, where the transfer of Personal Data to Databricks is a Restricted Transfer and Applicable Data Protection Laws require that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form part of the DPA as follows:

a. In relation to transfers of Personal Data protected by the EU GDPR, the SCCs shall apply as follows:

I. Module Two terms shall apply (where Customer is the controller of Personal Data) and the Module Three terms shall apply (where Customer is the processor of Personal Data);

II. in Clause 7, the optional docking clause shall apply and Authorized Affiliates may accede the SCCs under the same terms and conditions as Customer, subject to mutual agreement of the parties;

III. in Clause 9, option 2 ("**general authorization**") is selected, and the process and time period for prior notice of Sub-processor changes shall be as set out in Section 4.3 of the DPA;

IV. in Clause 11, the optional language shall not apply;

V. in Clause 17, option 1 shall apply and the SCCs shall be governed by Irish law;

VI. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

VII. Annex I shall be deemed completed with the information set out in Annex A to the DPA; and

VIII. Annex II shall be deemed completed with the information set out in the Security Addendum, subject to Section 6.1 (Security Measures) of the DPA.

b. In relation to transfers of Personal Data protected by the UK GDPR, the SCCs as implemented under Section 1(a) above shall apply with the following modifications:

I. the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the DPA;

II. Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex A and Annex B to the DPA and the Security Addendum respectively, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party"; and

III. any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

c. In relation to transfers of Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented under Section 1(a) above will apply with the following modifications:

I. references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;

II. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" and/or "Swiss law" (as applicable);

III. references to the “competent supervisory authority” and “competent courts” shall be replaced with references to the “Swiss Federal Data Protection Information Commissioner” and “applicable courts of Switzerland”);

IV. the SCCs shall be governed by the laws of Switzerland ; and

V. disputes shall be resolved before the competent Swiss courts.

2. Where the Standard Contractual Clauses apply pursuant to Section 8.1 of this DPA, this section sets out the parties' interpretations of their respective obligations under specific provisions of the Clauses, as identified below. Where a party complies with the interpretations set out below, that party shall be deemed by the other party to have complied with its commitments under the Standard Contractual Clauses:

a. where Customer is itself a processor of Personal Data acting on behalf of a third party controller and Databricks would otherwise be required to interact directly with such third party controller (including notifying or obtaining authorizations from such third party controller), Databricks may interact solely with Customer and Customer shall be responsible for forwarding any necessary notifications to and obtaining any necessary authorizations from such third party controller;

b. the certification of deletion described in Clause 16(d) of the SCCs shall be provided by Databricks to Customer upon Customer's written request;

c. for the purposes of Clause 15(1)(a) the SCCs, Databricks shall notify Customer and not the relevant data subject(s) in case of government access requests, and Customer shall be solely responsible for notifying the relevant data subjects as necessary; and

d. taking into account the nature of the processing, Customer agrees that it is unlikely that Databricks would become aware of Personal Data processed by Databricks is inaccurate or outdated. To the extent Databricks becomes aware of such inaccurate or outdated data, Databricks will inform the Customer in accordance with Clause 8.4 SCCs.