

DATA TRANSFER ADDENDUM

This Data Transfer Addendum, including the Standard Contractual Clauses (“**DTA**”), applies to any master cloud services agreement or other written agreement between the entity identified as “**Customer**” below and Databricks, Inc. (“**Databricks**”) that governs Customer’s use of the Covered Databricks Services (the “**Agreement**”). Customer enters into this DTA on behalf of itself and, to the extent required under European Data Protection Laws, in the name and on behalf of its Authorized Affiliates. For the purposes of the DTA only, and except where otherwise indicated, the term “Customer” shall include Customer and its Authorized Affiliates. All capitalized terms not defined in this DTA shall have the meaning set forth in the Agreement.

This DTA has been pre-signed by Databricks and shall become legally binding on Databricks’ receipt of a validly completed DTA, provided that the DTA shall be null and void if any changes are made to it beyond Customer completing Annex A and the signature box (“**Effective Date**”).

Background

Customer has engaged Databricks to provide the Covered Databricks Services in accordance with the Agreement, in connection with which the parties acknowledge and agree that Customer transfers Customer Personal Data to Databricks. Accordingly, the parties wish to amend the Agreement by incorporating this DTA (including the Standard Contractual Clauses) to ensure that the transfer of Customer Personal Data by Customer to Databricks complies with European Data Protection Laws.

Agreed Terms

In consideration of the mutual promises set out in this DTA, the parties hereby agree as follows:

1. The following terms shall have the following meanings:
 - (a) “**European Data Protection Laws**” “**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Data Protection Act and its implementing regulations (“**Swiss Data Protection Act**”); in each case as may be amended, superseded or replaced from time to time.
 - (b) “**Covered Databricks Services**” means the Platform Services directly provided by Databricks and any other Databricks Services that Databricks provides to Customer that require the processing by Databricks of Customer Personal Data on Customer’s behalf.
 - (c) “**Customer Personal Data**” means the personal data made available by Customer for processing by, or use within, the Covered Databricks Services.
 - (d) “**Europe**” means the European Economic Area (“**EEA**”), the United Kingdom (“**UK**”) and Switzerland.
 - (e) “**Security Addendum**” means the security addendum found at databricks.com/security-addendum.
 - (f) “**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.
 - (g) “**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.
2. **Standard Contractual Clauses.** The parties agree that, to the extent the transfer of Customer Personal Data to Databricks involves a transfer to a country outside Europe that does not provide an adequate level of protection for personal data (within the meaning of applicable European Data

Protection Laws), the Standard Contractual Clauses shall be deemed incorporated by reference and form an integral part of the Agreement as set out herein. The Standard Contractual Clauses shall apply from the Effective with respect to transfers of Customer Personal Data that, in the absence of the application of the Standard Contractual Clauses, would cause either party to breach European Data Protection Laws.

- (a) In relation to transfers of Customer Personal Data protected by the GDPR, the SCCs shall apply as follows:
- (1) the Module Two terms shall apply where Customer is the controller and the Module Three terms shall apply where Customer is a processor of Customer Personal Data;
 - (2) in Clause 7, the optional docking clause shall apply and Authorized Affiliates may accede to the SCCs under the same terms and conditions as Customer, subject to the mutual agreement of the parties;
 - (3) 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 the Agreement;
 - (4) in Clause 11, the optional language shall not apply;
 - (5) in Clause 17, option 1 shall apply and the SCCs shall be governed by Irish law;
 - (6) in Clause 18, disputes shall be resolved before the courts of Ireland; and
 - (7) Annex I and Annex II shall be deemed completed with the information set out in Annex A to this DTA and the Security Addendum respectively.
- (b) In relation to transfers of Customer Personal Data protected by UK Data Protection Laws, the SCCs as implemented by Section 2(a) shall apply with the following modifications:
- (1) 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 Agreement;
 - (2) Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex A to this DTA and the Security Addendum respectively, and Table 4 shall be deemed completed by selecting “neither party”; and
 - (3) any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.
- (c) In relation to transfers of Customer Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented by Section 2(a) shall apply with the following modifications:
- (1) 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;
 - (2) references to “EU”, “Union”, “Member State” and “Member State law” shall be replaced with references to “Switzerland” and “Swiss law”;
 - (3) references to the “competent supervisory authority” and “competent courts” shall be replaced with references to the “Swiss Federal Data Protection Information Commissioner” and “competent Swiss courts” and the SCCs shall be governed by the laws of Switzerland.

3. **Clarifications to the Standard Contractual Clauses.** 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 SCCs:
 - (a) where Customer is itself a processor of Customer Personal Data acting on behalf of a third party controller and Databricks would (including for the purposes of the SCCs) 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 Clauses 8.5 and 16(d) of the SCCs shall be provided by Databricks to Customer only upon Customer's written request; and
 - (c) for the purposes of Clause 15(1)(a) of the SCCs, Databricks shall notify Customer and not the relevant data subjects in case of government access requests and Customer shall be solely responsible for notifying the relevant data subjects as necessary.

4. **Alternative Transfer Mechanism.** To the extent that Databricks adopts an alternative data export mechanism, including any new version of or successor to the Privacy Shield ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead of the Standard Contractual Clauses described in this DTA but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Laws and extends to territories to which Customer Personal Data is transferred.

5. **Miscellaneous.** This DTA shall replace any equivalent provisions in the Agreement regarding the transfer of Customer Personal Data that is subject to European Data Protection Laws, including any prior or existing versions of the Standard Contractual Clauses. Except as set out in this DTA, the Agreement shall continue in full force and effect. In the event of any conflict between this DTA and the Agreement, the parties agree that the terms of this DTA shall prevail, provided that if and to the extent the Standard Contractual Clauses conflict with any provision of this DTA, the Standard Contractual Clauses control and take precedence. Any provisions excluding or limiting either party's liability under the Agreement shall apply to the liability of each party and each party's Affiliates under this DTA, including the Standard Contractual Clauses, except that they shall not apply to any claim made by a data subject pursuant to its rights as a third-party beneficiary under the Standard Contractual Clauses.

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

Customer: _____ By: _____ Name: _____ Title: _____ Date: _____ Contact Person: _____ Contact Title: _____ Contact Email: _____	Databricks, Inc. By: _____ Name: Scott Starbird Title: General Counsel, Public Affairs and Strategic Partnerships Date: _____
--	--

ANNEX A

ANNEX 1(A): LIST OF PARTIES	
Data exporter:	<p>Name of data exporter: The entity identified as “Customer” in the Agreement and this DTA</p> <p>Contact person’s name, position and contact details: The contact details associated with Customer’s Databricks account or as otherwise specified in this DTA or the Agreement.</p> <p>Activities relevant to the data transferred: The activities specified in Annex 1.B below</p> <p>Signature and date: See front end of the DTA</p> <p>Role (Controller/Processor): Controller (for Module 2) or Processor (for Module 3)</p>
Data importer:	<p>Name of data importer: Databricks, Inc.</p> <p>Contact person’s name, position and contact details: Scott Starbird, General Counsel, Public Affairs and Strategic Partnerships</p> <p>Activities relevant to the data transferred: The activities specified in Annex 1.B below</p> <p>Signature and date: See front end of the DTA</p> <p>Role (Controller/Processor): Processor</p>
ANNEX 1(B): DESCRIPTION OF THE TRANSFER	
Categories of data subjects:	<p>Data subjects include individuals about whom data is provided to Databricks via the Covered Databricks Services (by or at the direction of Customer), which shall include:</p> <p style="background-color: yellow; border: 1px dashed black; height: 40px; margin: 5px 0;"></p> <p style="background-color: yellow; border: 1px dashed black; height: 40px; margin: 5px 0;"></p> <p style="background-color: yellow; border: 1px dashed black; height: 40px; margin: 5px 0;"></p> <p>IF CUSTOMER HAS NOT FILLED OUT THE ABOVE SECTION: Customer shall be deemed to have declared that the categories of data subjects include: (i) prospects, customers, business partners and vendors of Customer (who are natural persons); (ii) employees or contact persons of Customer’s prospects, customers, business partners and vendors; (iii) employees, agents, advisors, freelancers of Customer (who are natural persons); and/or (iv) Customer’s Authorized Users; (iv) Customer’s Authorized Users or (v) other individuals whose personal data is included in Customer Content.</p>
Categories of personal data:	<p>The types of Customer Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:</p> <p style="background-color: yellow; border: 1px dashed black; height: 40px; margin: 5px 0;"></p> <p style="background-color: yellow; border: 1px dashed black; height: 40px; margin: 5px 0;"></p> <p style="background-color: yellow; border: 1px dashed black; height: 40px; margin: 5px 0;"></p> <p>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: (i) name, address, title, contact details; and (ii) IP addresses, cookies data, location data.</p>
Sensitive data (if applicable):	<p>Subject to any applicable restrictions and/or conditions in the Agreement, Customer Personal Data may include ‘special categories of personal data’ as defined by European Data Protection Laws or similarly sensitive personal data, the extent of which is determined and controlled by Customer in its sole discretion.</p>
Frequency of the transfer:	<p>Continuous or one-off depending on the services being provided by Databricks.</p>
Nature, subject matter and duration of the transfer:	<p><u>Nature:</u> Databricks provides a cloud-based unified data analytics platform and related services, as further described in the Agreement</p> <p><u>Subject Matter:</u> Customer Personal Data</p> <p><u>Duration:</u> The term of the Agreement and any period after the termination or expiry of the Agreement during which Databricks processes Customer Personal Data</p>
Purpose(s) of the transfer and further processing:	<p>Databricks shall process Customer Personal Data for the following purposes: (i) as necessary for the performance of the Covered Databricks Services and Databricks’ obligations under the Agreement (including the DTA), including processing initiated by Authorized Users in their use of the Covered Databricks Services; and (ii) further documented, reasonable instructions from Customer agreed upon by the parties.</p>
Period for which the personal data will be retained:	<p>Databricks will retain Customer Personal Data for the term of the Agreement and any period after the termination or expiry of the Agreement during which Databricks processes Customer Personal Data in accordance with the Agreement.</p>
ANNEX 1(C): COMPETENT SUPERVISORY AUTHORITY	

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