# DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms a part of the Master Cloud Services Agreement found at https://www.databricks.com/mcsa or other superseding written agreement between you ("**you**" or "**Customer**") and Databricks, Inc. ("**Databricks**") that governs your use of the Covered Databricks Services (in either case, the "**Agreement**").

By signing this DPA or executing an Agreement that explicitly states that this DPA is incorporated into the Agreement by reference, 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 any Affiliates who are authorized to use the Covered Databricks Services. If you are entering into this 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 DPA. All capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement.

This DPA, including the Standard Contractual Clauses found in Annex C, has been pre-signed by Databricks. Upon the earlier of (i) the execution of an Agreement that explicitly states that this DPA is incorporated into the Agreement by reference; and (ii) Databricks' receipt of a validly completed DPA by email directed to dpa@databricks.com, this DPA will become legally binding, provided that the pre-signed version of this DPA will be null and void if any changes are made to it beyond Customer completing any required sections in Annex A and the needed basic contact information in the Standard Contractual Clauses and signature boxes.

## 1. DEFINITIONS

1.1 **"Applicable Data Protection Laws"** means data protection and privacy laws and regulations applicable to Databricks' provision of the Covered Databricks Services to its customers generally, including, without limitation the GDPR and CCPA, without regard to Customer's particular use of the Covered Databricks Services.

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

1.3 "**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. Covered Databricks Services do not include Databricks Powered Services (as listed in the Cloud Provider Directory located at databricks.com/cloud-provider-directory) or Non-Databricks Services.

1.4 "**Customer Data**" means the data, other than Customer Instructional Input, made available by Customer and its Authorized Users for processing within the Platform Services or Support Services.

1.5 **"Customer Personal Data"** means the personal data made available by Customer for processing by, or use within, the Covered Databricks Services.

1.6 "**Customer Instructional Input**" means information other than Customer Data that Customer inputs into the Platform Services to direct how the Platform Services process Customer Data, including without limitation the code and any libraries (including third party libraries) Customer utilizes within the Platform Services.

1.7 **"GDPR"** 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).

1.8 "**Standard Contractual Clauses**" means the Standard Contractual Clauses (controller to processor) promulgated by the EU Commission Decision 2010/87/EU attached as Annex C.

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

1.10 "**Sensitive Data**" means any unencrypted (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 GPS location of a particular individual; (v) any "special" or "sensitive" categories of data as those terms are defined according to the GDPR; or (vi) or any similar category under other Applicable Data Protection Laws. For the purposes of the prior sentence, "unencrypted" means a failure to utilize industry standard encryption methods to prevent Databricks, the Platform Services, and Databricks' personnel, including any subcontractors, from accessing the relevant data in unencrypted form.

1.11 **"Subprocessor"** means any third party engaged by Databricks (including any Databricks Affiliate) to process Customer Personal Data on behalf of Customer.

1.12 **"System"** means any application, computing or storage device, or network.

1.13 **"Usage Data"** means usage data and telemetry collected by Databricks relating to Customer's use of the Platform Services. Usage Data may occasionally contain queries entered by an Authorized User but not the results of those queries.

1.14 The terms "**controller**," "**data subject**," "**processor**," "**process**," "**processing**," and "**personal data**" have the meanings given to them in Applicable Data Protection Laws. The term controller includes 'businesses' (as defined in the CCPA), the term data subject includes 'consumers' (as defined in the CCPA), the term processor includes 'service providers' (as defined in the CCPA), and the term personal data includes 'personal information' (as defined in the CCPA) to the extent the rights and obligations in this DPA apply under the CCPA.

## 2. DATA PROCESSING

2.1 **Applicability.** This DPA is made effective as of the date it is mutually executed (the "**DPA Effective Date**") and except as set forth in Section 2.5, applies only to the extent that Databricks processes Customer Personal Data on behalf of Customer as a processor in the course of providing the Covered Databricks Services.

2.2 **Party Roles.** As between the parties, Customer is either the controller or processor of Customer Personal Data and Databricks is the processor or subprocessor of Customer Personal Data.

2.3 **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it in the exercise of its rights or performance of its obligations under the Agreement or this DPA, including Applicable Data Protection Laws. 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 DPA. Databricks will not 'sell' (as such term is defined in the CCPA) Customer Personal Data.

2.4 **Instruction to Process**. Databricks shall process Customer Personal Data pursuant to Customer's use of the Covered Databricks Services and Customer's documented instructions as set forth in this DPA and the Agreement(s) and as otherwise necessary to provide the Covered Databricks Services (together "**Processing Instructions**"). Customer's Processing Instructions shall comply with Applicable Data Protection Laws, including but not limited to providing all applicable notices to and gaining proper consents from its data subjects. Databricks shall inform Customer if it determines that Customer's Processing Instructions infringe any Applicable Data Protection Law. Databricks may refuse further processing of personal data that it believes to be in violation of any law or regulation, including any Applicable Data Protection Laws.

2.5 **Usage Data.** Databricks may collect Usage Data. Databricks is the controller of Usage Data and shall process Usage Data in accordance with Applicable Data Protection Laws. Notwithstanding the foregoing, Databricks will not share (other than with Subprocessors or third parties providing services to Databricks who agree to terms at least as restrictive regarding the processing of Usage Data as

those set forth herein) or publicly make available any Usage Data that identifies Customer or its users, data subjects, or customers, nor use any Usage Data in a manner that derives its value from Customer Personal Data. Without limiting the foregoing, Databricks will not 'sell' (as such term is defined in the CCPA) any Usage Data that contains personal data subject to the CCPA.

## 3. PLATFORM ARCHITECTURE

3.1 **Shared Responsibility Deployment.** Certain components of the Platform Services are under Customer's control. Each party must undertake technical and organizational security measures in order to protect Customer Data under such party's control. Without limiting the foregoing, Customer acknowledges and agrees that it is responsible for (i) protecting the security of credentials used to access the Platform Services; (ii) securing and managing the Customer-provided cloud provider environment into which Customer directs Databricks to deploy the portion of the Platform Services known as the "data plane" and any Customer System (with such steps to include without limitation the regular rotation of access keys and other industry standard steps to preclude unauthorized access); and (iii) any security or other issues resulting from any Customer Instructional Input, and Customer expressly assumes the risks associated with the foregoing responsibilities.

3.2 **Data Agnostic.** Customer solely chooses what Customer Data (including any Customer Personal Data) it processes in the Covered Databricks Services. Customer acknowledges that Databricks will be generally unaware of the types of or details regarding the Customer Data processed within the Covered Databricks Services.

3.3 **Sensitive Data.** Customer will not provide or process Sensitive Data in the Covered Databricks Services without Databricks' prior written approval (which approval may be set forth in an applicable Order Form).

3.4 **No Data Backup.** Databricks and the Covered Databricks Services do not provide backup services or disaster recovery for Customer Data. It is Customer's obligation to backup Customer Data and Customer Instructional Input.

## 4. SUBPROCESSING

4.1 **Authorization.** Customer agrees that Databricks may appoint Subprocessors to assist it in providing the Covered Databricks Services. Customer authorizes the use of the Subprocessors listed at www.databricks.com/subprocessors as of the DPA Effective Date ("**Subprocessor List**").

4.2 **Databricks Subprocessor Obligations**. Databricks (i) shall enter into a written agreement with its Subprocessors which includes data protection and security measures no less protective of Customer Personal Data than the Agreement and this DPA, including without limitation the requirement that such Subprocessors process Customer Personal Data no more than as Databricks is permitted to under the Processing Instructions and (ii) remains fully liable for any breach of this DPA or the Agreement that is caused by an act, error or omission of such Subprocessor to the extent Databricks would have been liable for such act, error or omission had it been caused by Databricks.

4.3 **Subprocessor Changes.** Prior to the addition of any new Subprocessor, Databricks shall provide notice to Customer, which may include updating the Subprocessor List, not less than 30 calendar days prior to the date on which the Subprocessor shall commence processing Customer Personal Data. Databricks will provide a mechanism for Customer to receive notifications of changes to the Subprocessor List (which may include without limitation the provision of an RSS feed).

4.4 **Subprocessor Objections.** Customer may reasonably object on data protection grounds to Databricks' use of a new Subprocessor by notifying Databricks in writing within 10 calendar days after notice has been provided by Databricks. In the event of Customer's timely objection on such reasonable grounds, Databricks will either: (i) work with Customer to address Customer's objections to its reasonable satisfaction; (ii) instruct the Subprocessor to not process Customer Data; provided that Customer acknowledges this may result in new or improved Covered Databricks Services features not being

available to Customer; or (iii) notify Customer of its option to terminate this DPA and the Agreement. Customer shall have 14 calendar days in which to exercise its option to terminate the Agreement after receiving notice of a right to terminate. If Customer timely exercises its right to terminate, Databricks will provide Customer with a pro rata reimbursement of any prepaid, but unused, fees as of the date Customer notifies Databricks of its choice to exercise such right.

4.5 **Non-Databricks Services**. Customer acknowledges that any third party services (other than Subprocessors) that may be linked to or used within the Platform Services (e.g., Customer may use GitHub to backup Customer's notebooks) and that Customer may choose to use at its option ("**Non-Databricks Services**") are governed solely by the terms and conditions and privacy policies of such Non-Databricks Services. Databricks does not endorse, is not responsible or liable for, and makes no representations as to any aspect of such Non-Databricks Services, including, without limitation, their content or the manner in which they handle your Customer Data (including Customer Personal Data) or any interaction between Customer and the provider of such Non-Databricks Services. Databricks is not liable for any damage or loss caused or alleged to be caused by or in connection with Customer's enablement, access or use of any such Non-Databricks Services, or Customer's reliance on the privacy practices, data security processes or other policies of such Non-Databricks Services. The providers of Non-Databricks Services shall not be deemed Subprocessors for any purpose under this DPA.

## 5. COOPERATION

5.1 **Data Subject Requests.** If Databricks receives a request from a data subject seeking to exercise their rights under Applicable Data Protection Laws that identifies Customer ("**DSR**"), Databricks shall promptly pass such communication on to Customer. The Covered Databricks Services include controls that Customer may use to assist it to respond to a DSR. Customer is responsible for responding to and complying with any DSR. If Customer is unable to access any relevant Customer Personal Data that is under Databricks' control using the controls within the Covered Databricks Services, Databricks shall reasonably cooperate with Customer to enable Customer to respond to the DSR.

5.2 **Government Inquiries.** If Databricks receives a subpoena, court order, warrant or other legal demand from law enforcement or public or judicial authorities seeking the disclosure of Customer Data, Databricks shall, to the extent permitted by applicable laws, promptly notify Customer in writing of such request and reasonably cooperate with Customer to limit, challenge or protect against such disclosure.

5.3 **Assistance.** Databricks will (i) at Customer's request and expense assist Customer to conduct a data protection impact assessment and, where legally required, consult with applicable data protection authorities; and (ii) respond to reasonable requests for additional information if necessary for Customer to demonstrate its compliance with Applicable Data Protection Laws.

## 6. DATA ACCESS

6.1 **Confidentiality**. Databricks shall ensure that any person it authorizes (including Databricks' employees, contractors and Subprocessors) to process Customer Data is subject to a duty of confidentiality substantially as protective of Customer Data as this DPA and the Agreement.

6.2 **Security Measures.** Databricks will implement and maintain appropriate technical and organizational security measures to preserve the security, availability, integrity and confidentiality of Customer Data in accordance with the Databricks security measures attached here as Annex B ("**Security Measures**"). Databricks may update its Security Measures, provided that any updates shall not materially diminish the overall security of Customer Data or the Covered Databricks Services. Customer must review the Security Measures prior to providing Databricks with access to Customer Data to determine that the Security Measures meet the Customer's requirements and obligations under Applicable Data Protection Laws.

## 7. SECURITY BREACH

7.1 **Breach Notifications.** In the event of a Security Breach, Databricks shall provide written notice to Customer without undue delay and in no event later than seventy-two (72) hours after becoming aware of the Security Breach and will provide updates to Customer, including the type of data affected and the identity of affected person(s) as soon as such information becomes known to Databricks. Databricks will reasonably cooperate with Customer as required to fulfill Customer's obligations under Applicable Data Protection Laws. Databricks shall take such measures and actions as are appropriate to remedy or mitigate the effects of the Security Breach.

7.2 **Communications**. The decision whether to provide notification, public/regulatory communication or a press release (each, a "**Notification**") concerning the Security Breach shall be solely at Customer's discretion, but the content of any Notification that names Databricks or from which Databricks' identity could reasonably be determined shall be, except as otherwise required by applicable laws, subject to the prior approval of Databricks, which approval shall not be unreasonably withheld, conditioned or delayed, and provided that conditioning of the Notification on Databricks' approval shall not prevent Customer from complying with Applicable Data Protection Laws.

## 8. AUDITS

8.1 **Audits.** Databricks will utilize an independent third-party security professional to audit its Security Measures. Such audit will be performed (i) at least annually; and (ii) according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001 ("**ISMS Certification**").

8.2 **Reports**. At Customer's written request no more than once per year, Databricks will provide Customer with (i) its most current ISMS Certification; and (ii) a report from the audit 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**"). The Report and any summaries thereof will constitute Databricks' Confidential Information.

## 9. TRANSFER MECHANISM

Customer acknowledges that Databricks and its Subprocessors may maintain data processing operations in countries that are outside of the country in which the Platform Services are deployed. To the extent that Databricks processes on behalf of Customer any Customer Personal Data subject to the GDPR in a country that has not received a finding of adequacy by the European Commission, Databricks agrees to process such data as a "data importer" in compliance with the Standard Contractual Clauses (with Customer and/or its Affiliates as the "data exporter"), including all appendices thereto, attached as Annex C or other legally-recognized transfer mechanism.

## 10. DELETION & RETURN

The Platform Services include controls that Customer may use to retrieve or delete Customer Data. Databricks will delete Customer Data when requested by Customer by using the controls within the Covered Databricks Service provided for this purpose. Upon Customer's request upon termination or expiration of the Agreement or upon Customer's cancellation of a Platform Services workspace, Databricks will delete Customer's Platform Services workspace(s) and any Customer Data contained therein within 30 days of the cancellation of such workspace(s). Databricks may retain Customer Data where permitted by applicable law. In such event, Databricks will (i) to the extent practical, isolate such data; and (ii) protect such data from any further processing, except to the extent permitted by applicable law.

## 11. GENERAL

11.1 The parties agree that this DPA shall replace any existing DPA (including, as applicable, the Standard Contractual Clauses) the parties may have previously entered into in connection with the Covered Databricks Services.

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

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

11.4 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 Covered Databricks Services, the parties agree that the terms of this DPA shall prevail. 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).

11.5 Notwithstanding anything to the contrary in the Agreement or this DPA, 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), 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 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 the Customer under the Agreement.

11.6 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.

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

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:**_____<br><br>By:_____<br><br>Name:_____<br><br>Title:_____<br><br>Date:_____ | **Databricks, Inc.**<br><br>By: DocuSigned by: Scott Starbird D4B3FEA843844BE...<br><br>Name: Scott Starbird<br><br>Title: VP, Legal<br><br>Date: 01-Mar-2021 |

# ANNEX A

## DETAILS OF THE PROCESSING

**Description of Data Exporter**

*The data exporter is the entity identified as the "Customer" in the Data Processing Addendum in place between data exporter and data importer and to which this Annex is appended.*

*As between the parties, Customer shall be the controller of certain personal data contained in Customer Data provided to Databricks related to its use of the Covered Databricks Services.*

**Description of Data Importer**

*Databricks, the data importer, provides a cloud-based unified data analytics platform and related services.*

**Data subjects**
The personal data transferred concern the following categories of data subjects (please specify):

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.

**Categories of data**
Customer may submit personal data to the Covered Databricks Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following types of personal data:

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/or (ii) IP addresses, usage data, cookies data, location data.

**Special categories of data (if appropriate)**
The personal data transferred concern the following special categories of data (please specify):

*n/a. You may not use the Covered Databricks Services to process any Sensitive Data (including without limitation special categories of data) unless the Order Form you have executed with Databricks explicitly allows such processing.*

**Processing operations**
The personal data transferred will be subject to the following basic processing activities (please specify):

*General big data analytics processing. Any use of the Covered Databricks Services shall be deemed an instruction to Databricks to process such data.*

**ANNEX B**

**SECURITY MEASURES**

This Annex B describes the technical and organizational security measures and procedures Databricks shall maintain to protect the security of Customer Personal Data created, collected, received or otherwise obtained during the performance of the Covered Databricks Services.

Customer acknowledges that the Covered Databricks Services operate pursuant to a shared responsibility model, which requires, among other things, that Customer take certain steps such as encryption and backup with respect to its own data (which remains stored within Customer's environment under Customer's control). Additionally, Customer acknowledges its obligation under applicable law not to provide more Customer Personal Data to Databricks than is reasonably necessary to enable Databricks to perform the Covered Databricks Services.

Databricks will (i) when any Customer Personal Data is under its control, comply with the measures identified below with respect to such Customer Personal Data; and (ii) keep documentation of such measures to facilitate audits and for the conservation of evidence.

Access Control to Processing Areas

Databricks implements suitable measures designed to prevent unauthorized persons from gaining access to the data processing equipment where Customer Personal Data is processed or used. This is accomplished by Databricks or its Cloud Services Provider (e.g., Amazon Web Services):

- establishing security areas, with 24-hour security service provided by the property owner;
- protecting and restricting access paths;
- securing data processing equipment;
- establishing and documenting access authorizations for staff and third parties;
- maintaining appropriate processes applicable to the use of cardkeys;
- logging and monitoring access to data centers where Customer Personal Data is hosted; and
- securing data centers where Customer Personal Data is hosted with a security alarm system, and other appropriate physical security measures.

Access Control to Data Processing Systems

Databricks implements suitable measures designed to prevent the systems used for data processing from being used by unauthorized persons. This is accomplished by:

- identification of the client machine and/or the user of the Databricks systems;
- automatic disabling of user IDs when several erroneous passwords are entered and maintenance of a log file of events (i.e., monitoring of break-in-attempts);
- issuing and safeguarding credentials;
- dedication of individual client machines and/or users to specific functions where appropriate;
- implementation and maintenance of staff policies in respect of each staff member's access rights to Customer Personal Data (if any), where such policies inform staff about their obligations and the consequences of any violations of such obligations to ensure that staff will only access Customer Personal Data and resources to the extent necessary to perform their job duties;
- training staff on applicable policies, privacy duties and liabilities;
- logging and monitoring access to Customer Data; and

- use of industry standard encryption technologies.

Access Control to Use Specific Areas of Data Processing Systems

Databricks implements suitable measures designed to restrict use of its systems so that certain data is subject to additional access permissions (e.g., by user or specific authorization) and that Customer Personal Data cannot be read, copied, modified or removed without authorization. This is accomplished by:

- implementation and maintenance of staff policies in respect of each staff member's access rights to Customer Personal Data;
- allocation of individual client machines and/or users to specific functions;
- monitoring capability in respect of individuals who delete, add or modify Customer Personal Data
- conducting audits, at least yearly, of authorization profiles;
- procedures limiting the release of Customer Personal Data only to authorized persons;
- implementation and maintenance of data retention policies; and
- use of industry standard encryption technologies.

Transmission Control

Databricks implements suitable measures designed to prevent Customer Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of industry standard firewall and encryption technologies to protect data while it travels; and
- logging and monitoring of data transmissions.

Input Control

Databricks implements suitable measures designed to ensure that it is possible to check and establish whether and by whom Customer Personal Data has been input into or removed from systems. This is accomplished by:

- maintenance of an authorization policy for the input of data, and for the reading, alteration and deletion of stored data;
- authentication of authorized personnel;
- requiring individual authentication credentials such as user IDs that, once assigned, are not re-assigned to another person;
- use of protective measures for any data input into Databricks systems, including the reading, alteration and deletion of stored data;
- utilization of user credentials (passwords) of at least eight characters (or the system maximum permitted number if less than eight) and modification at first use and thereafter at least every 90 days;
- providing that entries to its cloud provider data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log-off of user IDs (requiring re-entry of the user’s password to use the relevant workstation) that have not been used for a substantial period of time;
- automatic deactivation of user authentication credentials (such as user IDs) in case the person is disqualified from accessing Customer Personal Data or in case of non-use for a substantial period of time (at least six months), except for those authorized solely for technical management; and
- electronic recording of entries.

Job Control

Databricks implements suitable measures designed to ensure that Customer Personal Data may only be processed in accordance with written instructions issued by Customer. This is accomplished by:

- binding policies and procedures for Databricks' employees;
- maintaining agreements with external entities responsible for the protection or processing of Customer Personal Data hereunder that require substantial compliance with the measures described hereunder;
- individual appointment of system administrators;
- adoption of suitable measures to register and maintain system administrators' access logs;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by Databricks and applicable laws; and
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned.

Availability Control

Databricks implements suitable measures designed to ensure that Customer Personal Data is protected from accidental destruction or loss. This is accomplished by:

- enabling Customer to backup Customer’s data by providing infrastructure redundancy options (e.g., data versioning within Amazon Web Services) to ensure data access is restorable on demand; and
- requiring that the Customer authorize the restoration of backups (if any), held by Databricks.

**ANNEX C**

**Standard Contractual Clauses (processors)**

THE PARTIES HAVE AGREED on the following Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

*Clause 1 - **Definitions***

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law***'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2 - **Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3 - **Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4 -* ***Obligations of the data exporter***

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

*Clause 5 -* ***Obligations of the data importer***

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to

inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

*Clause 6 - **Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

*Clause 7 - **Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8 - **Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9- **Governing Law***

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

*Clause 10 - **Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11 - **Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

*Clause 12-* ***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter:**
Name (written out in full): _____
Position: _____
Address: _____
Other information necessary in order for the contract to be binding (if any):

Signature……..

(stamp of organisation)

**On behalf of the data importer:**
Name (written out in full): Scott Starbird
Position: VP, Legal
Address: 160 Spear Street, Suite 1300, San Francisco, CA 94105
Other information necessary in order for the contract to be binding (if any): not applicable

DocuSigned by:
Scott Starbird
D4B3FEA843844BE...

Signature……..

(stamp of organisation) (Databricks has no corporate stamp)

## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Please see details set forth in Annex A to the Data Processing Addendum

DATA EXPORTER
Name: _____
Authorised Signature ……

DATA IMPORTER
Name: Scott Starbird
Authorised Signature ……

DocuSigned by:
Scott Starbird
D4B3FEA843844BE...

## APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

Please see the Security Measures set forth in the DPA.

DATA EXPORTER
Name: _____
Authorised Signature ……

DATA IMPORTER
Name: Scott Starbird
Authorised Signature ……

DocuSigned by:
Scott Starbird
D4B3FEA843844BE...

## APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 3 sets out the parties' interpretations of their respective obligations under specific provisions within the Clauses, as identified below. Where a party complies with the interpretations set out in this Appendix 3, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

Nothing in the interpretations below is intended to modify the Clauses or conflict with either party's rights or responsibilities under the Clauses and, in the event of any conflict between the interpretations below and the Clauses, the Clauses shall prevail to the extent of such conflict. Notwithstanding this, the parties expressly agree that any claims brought under the Clauses shall be exclusively governed by the limitations on liability set out in the Agreement.

Clause 5(a): Suspension of data transfers and termination

1. If the data exporter intends to suspend the transfer of personal data and/or terminate the Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").
2. If after the Cure Period, the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instances where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit

1. Data exporter agrees to exercise its audit right under Clause 5(f) by instructing data importer to execute the audit measures as described in the DPA.
2. Should an applicable data protection authority finally determine that this mechanism is not legally sufficient under the Clauses:
    a. the parties agree that data exporter audits conducted pursuant to Clause 5(f) will be (i) scoped to only matters not reasonably covered by the Report, unless an applicable data protection authority determines that the scope of such audit is not legally sufficient to enable data importer to comply with its obligations under Clause 5(f); and (ii) conducted no more than annually unless (a) the data exporter reasonably believes Databricks is failing to fulfil its obligations under these Clauses; or (b) there has been a confirmed Security Breach, in which case data exporter may perform an audit at data exporter's request provided it makes such request known to data importer in writing within 30 days after being notified of a Security Breach or the occurrence of any facts giving rise to a belief data importer is failing to fulfil its obligations under these Clauses.
    b. Data exporter will endeavour to provide data importer with reasonable notice of its intent to conduct an audit and to cooperate reasonably with data importer in scheduling such audit. Data exporter will use reasonable endeavours to minimise any business disruption to data importer when conducting such audit.
    c. Any audit will be conducted at data exporter's expense and the data importer may charge reasonable day rates for any support it provides data exporter in connection with such audit (such rates to be agreed with the data importer in advance or, if no such agreement, then at the data importer's normal professional day rates). In the event that such audit reveals a material breach of these Clauses by the data importer, then the data importer shall bear the costs of such audit.
    d. Any auditor, whether internal to data exporter or a third party appointed by the data exporter, must execute a non-disclosure agreement in a form reasonably acceptable to data importer prior to accessing data importer's facilities or otherwise receiving confidential information from data importer in connection with such audit.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.
2. Accordingly, the parties agree that upon the request of data exporter, data importer shall provide all relevant information evidencing compliance with Clause 5(j). Should the information provided by data importer be insufficient to demonstrate data importer's compliance with Clause 5(j) then data importer

may provide a version of the onward subprocessor agreement with commercially sensitive and/or confidential information removed.

3. Accordingly, the parties agree that any onward subprocessor agreement or information related thereto that data importer provides to data exporter shall constitute data importer's Confidential Information under the Agreement (as defined in the DPA) and shall not be disclosed by data exporter to any third party without data importer's prior agreement.

Clause 6: Liability

1. Any claims brought under these Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations of liability set forth in the Agreement (as defined in the DPA). In no event shall any party limit its liability with respect to any data subject rights under the Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to Article 28 of the GDPR, the data exporter may provide a general consent to onward subprocessing by the data importer. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of the Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 4 of the DPA.

DATA EXPORTER
Name: _____
Authorised Signature ……

DATA IMPORTER
Name: Scott Starbird
Authorised Signature …… DocuSigned by: Scott Starbird D4B3FEA843844BE...