DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its annexes and the Standard Contractual Clauses, ("**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**").

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. For the purposes of the DPA only, and except where otherwise indicated, the term "Customer" shall include Customer and its Authorized Affiliates.

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, incorporating the Standard Contractual Clauses, has been pre-signed by Databricks. This DPA (including the Standard Contractual Clauses herein) will become legally binding upon (a) the mutual execution of a non-pre-signed version or (b) with respect to the pre-signed version (i) if Customer's Agreement explicitly incorporates this DPA by reference, the execution of such Agreement; or (ii) if Customer's Agreement does not explicitly incorporate a data processing agreement or Customer later executes this pre-signed DPA, Databricks' receipt of a validly completed DPA sent by email to dpa@databricks.com ("**DPA Effective Date**"), 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 signature boxes.

1. DEFINITIONS

1.1 "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity. "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests (as measured on a fully-diluted basis) then outstanding of the entity in question. The term "**Controlled**" will be construed accordingly.

1.2 "**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 without regard to Customer's particular use of the Covered Databricks Services (except to the extent the obligation specified hereunder is Customer's obligation, in which case such term shall include such laws specific to Customer's particular uses).

1.3 "**Authorized Affiliate**" means a Customer Affiliate who is authorized under the Agreement to use the Covered Databricks Services.

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

1.5 "**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.

1.6 "**Customer Content**" means, if not defined within the Agreement, the data and code made available through the Platform Services or Support Services by Customer and its Authorized Users for processing within the Platform Services or Support Services.

1.7 "**Customer Personal Data"** means the personal data made available by Customer in Customer Content.

1.8 "**GDPR**" means, unless a specific version is indicated, all of the EU GDPR, the UK Data Protection Laws and the Swiss Data Protection Act.

1.9 "**Restricted Transfer**" means a transfer (directly or via onward transfer) of personal data that is subject to the GDPR, UK Data Protection Laws or Swiss Data Protection Act 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).

1.10 "**Security Addendum"** means the security addendum found at databricks.com/security-addendum (or such other location as Databricks may provide, and as may be updated from time to time in accordance with this Platform Schedule).

1.11 "**Security Breach"** means a breach of security leading to any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored or otherwise processed by Databricks. A Security Breach shall not include an unsuccessful Security Breach, which is one that results in no unauthorized access to Customer Personal Data or to any Databricks equipment or facilities storing the Customer Personal Data, and could include (without limitation) pings and other broadcast attacks of firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

1.12 "**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; or (v) any "special" or "sensitive" or other similar categories of data as those terms are defined according to the GDPR or any 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.

1.13 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021.

1.14 "**Subprocessor"** means any third party engaged by Databricks (including any Databricks Affiliate but not including any Databricks employees, contractors or consultants) to process Customer Personal Data on behalf of Customer.

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

1.16 **"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 Action 2018, as updated or amended from time to time.

1.17 "**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.

1.18 The terms "**controller**," "**data subject**," "**supervisory authority**", "**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, 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 (including as described in **Annex A** of this DPA).

2.2 **Party Roles.** As between the parties, Databricks shall process Customer Personal Data only as a processor acting on behalf of Customer who acts as a controller or a processor of Customer Personal Data. To the extent any Usage Data is considered personal data under Applicable Data Protection Laws, Databricks is the controller of such data and shall process such data in accordance with the Agreement and Applicable Data Protection Laws.

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.**

(a) Databricks shall process Customer Personal Data in accordance with Customer's documented lawful instructions as set forth in this DPA and the Agreement(s) and as otherwise necessary to provide the Covered Databricks Services (together "**Processing Instructions**"). Additional instructions outside the scope of the Processing Instructions (if any) require prior written agreement between the parties. Customer shall ensure that its Processing Instructions comply with Applicable Data Protection Laws. Taking into account the nature of the processing, Customer agrees that it is unlikely Databricks can form an opinion on whether the Processing Instructions violate Applicable Data Protection Laws. If Databricks forms such an opinion, it shall, unless prohibited from doing so under applicable laws, inform Customer, in which case, Customer is entitled to withdraw or modify its Processing Instructions. Databricks may without penalty refuse further processing of personal data under this DPA that it believes to be in violation of any law or regulation, including any Applicable Data Protection Laws.

(b) Where Customer is itself a processor of the Customer Personal Data acting on behalf of another third party controller (or on behalf of other intermediaries of the ultimate controller): (i) Customer represents and warrants to Databricks that the Processing Instructions and its actions with respect to Customer Personal Data, including its appointment of Databricks as a processor pursuant to this DPA, reflect and do not conflict with the instructions of such third parties; (ii) Customer agrees at Databricks' request to serve as the sole point of contact for Databricks with regard to such third parties; (iii) Databricks need not interact directly with (including seeking authorizations directly from) any such third party (other than through the regular provision of the Covered Databricks Services to the extent required by the Agreement); and (iv) where Databricks would (including for the purposes of the SCCs) otherwise be required to provide information, assistance, co-operation or anything else to such third party controller, Databricks may provide it solely to Customer as the sole point of contact. Notwithstanding the foregoing, Databricks shall be entitled to follow the instructions of third party with respect to Customer Personal Data instead of Customer's if Databricks reasonably believes this is legally required in the circumstances.

(c) Taking into account the nature of the processing, Customer agrees that it is unlikely that Databricks would become aware that Customer Personal Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if Databricks becomes aware that Customer Personal Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. Databricks provides certain controls and functionality within the Platform Services to enable the

Customer to correct Customer Personal Data that is inaccurate or outdated. It is Customer's responsibility to make any necessary corrections.

2.5 **Usage Data.** Notwithstanding anything to the contrary in this Agreement, Databricks may collect and use Usage Data to develop, improve, support, and operate its products and services. Databricks may not share any Usage Data that includes Customer confidential information with a third party except (a) in accordance with the Agreement, or (b) to the extent the Usage Data is aggregated and anonymized such that Customer and Customer's Authorized Users cannot be identified.

2.6 **Authorized Affiliates.** Databricks obligations set forth in this DPA shall also extend to Authorized Affiliates, subject to the following conditions:

(a) Customer must exclusively communicate any additional Processing Instructions requested pursuant to Section 2.4 directly to Databricks, including instructions from 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 in this DPA shall be considered the acts and/or omissions of Customer; and

(c) Authorized Affiliates shall not bring a claim directly against Databricks. If an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against Databricks ("**Authorized Affiliate Claim**"): (i) 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 (ii) 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.

3. PLATFORM ARCHITECTURE

3.1 **Shared Responsibility Deployment.** Certain components of the Platform Services are under Customer's control as further described in the Agreement. Each party shall be responsible for implementing appropriate technical and organizational security measures in order to protect Customer Content under its control, which for Databricks shall be the implementation of the Security Measures set forth in Section 6.2. 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 'Customer 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 Content, and Customer expressly assumes the risks associated with the foregoing responsibilities.

3.2 **Data Agnostic.** Customer solely chooses what Customer Content (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 Content 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 Databricks Services do not provide backup services or disaster recovery for Customer Content. Databricks does provide functionality within the Platform Services that may permit Customer to backup certain Customer Content on its own. It is Customer's obligation to backup any Customer Content if desired.

4. SUBPROCESSING

4.1 **Authorization.** Customer provides a general authorization for Databricks to appoint Subprocessors to process Customer Personal Data, including those Subprocessors listed at www.databricks.com/subprocessors ("**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 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 not less than 30 calendar days prior to the date on which the Subprocessor shall commence processing Customer Personal Data. 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 (which mechanisms will include at a minimum email).

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 relating to data protection, Databricks will either: (i) work with Customer to address Customer's objections to its reasonable satisfaction; (ii) instruct the Subprocessor to not process Customer Content (including any Customer Personal 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 this DPA and the Agreement after receiving notice of a right to terminate. If Customer timely exercises its right to terminate the Agreement, 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 Content (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 and relates to Customer Personal Data ("**DSR**"), Databricks shall promptly pass on such communication to Customer. Customer is responsible for responding to and complying with any DSR. The Covered Databricks Services include controls that Customer may use to assist it to respond to a DSR. If Customer is unable to access any relevant Customer Personal Data that is under Databricks' control 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.

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 Content, 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 Content is subject to a duty of confidentiality substantially as protective of Customer Content as this DPA and the Agreement.

6.2 **Security Measures.** Databricks will implement and maintain appropriate technical and organizational security measures designed to preserve the security and confidentiality of Customer Content in accordance with the Security Addendum ("**Security Measures**"). Databricks may update the Security Addendum and its Security Measures, provided that any updates shall not materially diminish the overall security of Customer Content or the Covered Databricks Services. Customer must review the Security Measures prior to providing Databricks with access to Customer Content 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 measures and actions appropriate and reasonable 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

9.1 **Deployment Region**. Customer can specify the location(s) in which Customer's Platform Services Workspace(s) will be deployed for the Customer in accordance with the Security Addendum and Databricks will not move such Workspace(s) without the express permission of Customer.

9.2 **Restricted Transfers**. Subject to Section 9.3 below, where the transfer of Customer Personal Data to Databricks is a Restricted Transfer, such transfer shall be governed by the Standard Contractual Clauses and the UK addendum (as applicable), which shall be deemed incorporated into and form an integral part of this DPA in accordance with Annex B of this DPA.

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

10. DELETION & RETURN

The Platform Services include controls that Customer may use at any time during the term of the Agreement to retrieve or delete Customer Content. Subject to the terms of the Agreement, Databricks will delete Customer Content from the Platform Services when Customer uses such controls to send an instruction to delete. Additionally, upon Customer's written request upon termination or expiration of the Agreement or upon Customer's cancellation of a Platform Services Workspace, Databricks will delete or assist Customer in deleting Customer's Platform Services Workspace(s) and will delete any Customer Content contained therein within 30 days following the cancellation of such Workspace(s). Databricks may retain Customer Content 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 data processing addendum, attachment, exhibit or standard contractual clauses that the parties may have previously entered into in connection with the Covered Databricks Services.

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

11.3 In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a third party controller), but without prejudice to the rights or remedies available to data subjects under Applicable Data Protection Laws or this DPA (including the SCCs).

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

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 Covered 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 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:_____	**Databricks, Inc.**
By:_____ Name:_____ Title:_____ Date:_____ Contact Person:_____ Contact Title:_____ Contact Email:_____	DocuSigned by: By: Scott Starbird B26A3291A9E6477... Name: Scott Starbird Title: General Counsel, Corporate and Compliance Date: 16 May 2022

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, Corporate and Compliance, 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 Covered 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: (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 personal data transferred:	The types of Customer 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: (i) name, address, title, contact details; and/or (ii) IP addresses, usage data, cookies data, location data.
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 Customer 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 Customer 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:	Nature: Databricks provides a cloud-based unified data analytics platform and related services, as further described in the Agreement. Subject Matter: Customer Personal Data. Duration: 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 Customer Personal Data.
Purpose(s) of the data transfer and further processing:	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 DPA), 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 (the "**Purposes**").
Period for which the personal data will be retained:	Databricks will retain Customer Personal Data for the term of the Agreement and any period after the termination of expiry of the Agreement during which Databricks processes Customer 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 GDPR.

ANNEX B

STANDARD CONTRACTUAL CLAUSES (Modules 2 and 3)

1. Subject to Section 9.2 of the DPA, where the transfer of Customer 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 Customer Personal Data protected by the GDPR, the SCCs shall apply as follows:

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

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 6.2 (Security Measures) of the DPA.

b. In relation to transfers of Customer Personal Data protected by UK Data Protection Laws, the SCCs as implemented by 1(a) above will 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 Customer Personal Data protected by Swiss Data Protection Act, the SCCs as implemented by 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 Swiss Data Protection Act ;

II. and the equivalent articles or sections therein;

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

IV. 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");

V. the shall be governed by the laws of or Switzerland); and

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

2. Where the Standard Contractual Clauses apply pursuant to Section 9.2 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 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 EU SCCs shall be provided by Databricks to Customer only upon Customer's written request;; and

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.