ADVISORY SERVICES DATA PROCESSING ADDENDUM

This Advisory Services Data Processing Addendum, including its annexes and the Standard Contractual Clauses, ("**Advisory Services DPA**"), effective as of the date both parties have executed this Advisory Services DPA (the "**Effective Date**"), forms a part of the Databricks Master Cloud Services Agreement concurrently entered into between the parties, unless you ("**you" or "Customer**") have entered into a superseding written master subscription agreement with Databricks, Inc. ("**Databricks**"), in which case, it forms a part of such written agreement (in either case, the "**Agreement**"). This Advisory Services DPA applies solely to the Databricks Advisory Services (as defined below) and not to any processing undertaken in the context of the Databricks Platform Services as defined below.

The parties agree as follows:

By signing the Advisory Services DPA or executing an Agreement that explicitly states that this Advisory Services DPA (including the Standard Contractual Clauses) is incorporated by reference, Customer enters into this Advisory Services DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws, in the name and on behalf of any Authorized Affiliates (defined below). If you are entering into this Advisory Services DPA on behalf of a company (such as your employer) or other legal entity, you represent and warrant that you have the authority to bind that company or legal entity to this Advisory Services DPA. In that case, "**Customer**" will refer to that company or other legal entity. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. For the purposes of this Advisory Services DPA only, and except where otherwise indicated, the term "Customer" shall include Customer and its Authorized Affiliates.

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

1. DEFINITIONS

1.1 **"Affiliate"** means an entity that directly or indirectly Controls, is Controlled by, or is under common Control with such 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 Databricks Advisory Services to its customers generally without regard to Customer's particular use of the Databricks Advisory 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 Databricks Advisory Services.

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

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

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

1.7 **"Customer Personal Data"** means Customer Data that is protected as personal data or personal information under Applicable Data Protection Laws**.**

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

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

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

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

1.12 **"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).

1.13 **"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.

1.14 **"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.

1.15 "**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 physical location of a particular individual or (v) any "special" or "sensitive" categories of data as those terms are defined according to 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 and Databricks' personnel, including any subcontractors, from accessing the relevant data in unencrypted form.

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

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

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

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

2. PURPOSE; SCOPE

2.1 Customer and Databricks have entered into the Agreement pursuant to which Customer is being provided Databricks Advisory Services. The parties acknowledge and agree that it is the expectation of both parties that (a) the purpose of the Agreement is **not** for Databricks to process Customer Personal Data on behalf of Customer or any Customer Affiliates; and (b) that, accordingly, Customer agrees that it will not intentionally grant Databricks access to Customer Personal Data or where access to Customer Personal Data is required for Databricks to perform the Databricks Advisory Services, Customer will limit Databricks access to Customer Personal Data to the extent necessary to perform the Databricks Advisory Services and such access shall happen solely within the Customer's environment and on systems controlled by Customer.

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

2.3 Accordingly, if Databricks processes any such Customer Personal Data, Databricks shall process Customer Personal Data (i) only as a Processor or sub-processor acting on behalf of Customer (whether as Controller or itself a Processor on behalf of third party Controllers); and (ii) in accordance with Customer's documented instructions as set forth in this Advisory Services DPA, the Agreement(s) or as otherwise necessary to provide the Databricks Advisory Services (together "**Processing Instructions**"). Customer shall ensure that its Processing Instructions comply with Applicable Data Protection Laws. Databricks shall inform Customer if, in its opinion, Customer's Processing Instructions infringe any law or regulation; in such event, Databricks is entitled to refuse processing of Personal Data that it believes to be in violation of any law or regulation. Without limiting the foregoing, Databricks will not 'sell' Customer Personal Data (as such term is defined in the CCPA).

2.4 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 or sub-processor pursuant to this Advisory Services 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 Databricks Advisory 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 and Customer shall be solely responsible for forwarding any notifications received from Databricks under this Advisory Services DPA (including the Standard Contractual Clauses) to the relevant controller where appropriate. Notwithstanding the foregoing, Databricks shall be entitled to follow the instructions of any third party controller of Customer Personal Data instead of Customer's if Databricks reasonably believes this is legally required in the circumstances.

2.5 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.

2.6 For the avoidance of doubt, and notwithstanding anything to the contrary in the Agreement or this Advisory Services DPA, this Advisory Services DPA does not apply to the Databricks Platform Services, which are subject to, with respect to the Databricks Platform Services directly provided by Databricks, a separate agreement between Customer and Databricks (including the DPA incorporated therein), and with respect to the Azure Databricks Platform Services, an agreement between Customer and Microsoft Corporation.

2.7 Databricks obligations set forth in this Advisory Services 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 2.3 directly to Databricks, including instructions from its Authorized Affiliates;

(b) Customer shall be responsible for Authorized Affiliates' compliance with this Advisory Services DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations in this Advisory Services 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. SUBPROCESSING

3.1 Notwithstanding anything to the contrary in the Agreement, Customer provides a general authorization for Databricks to appoint Subprocessors to assist it in providing the Databricks Advisory Services including the Subprocessors listed at www.databricks.com/subprocessors ("**Subprocessor List**"), provided that:

(a) such Subprocessors are bound to a written agreement which includes data protection and security measures no less protective of Customer Personal Data than the Agreement and this Advisory Services DPA;

(b) agree to act only on Databricks' instructions when processing the Customer Personal Data (which instructions shall be consistent with Customer's Processing Instructions to Databricks); and

(c) agree to protect the Customer Personal Data to a standard consistent with the requirements of this Advisory Services DPA, including by implementing and maintaining appropriate technical and organizational measures to protect the Customer Personal Data they process consistent with the Security Standards.

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

3.3 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).

3.4 Customer may reasonably object on data protection grounds to Databrick's 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 (a) work with Customer to address Customers objections to its reasonable satisfaction; or (b) instruct the Subprocessor to not process Customer Data (including any Customer Personal Data), provided that Customer acknowledges this may mean that Databricks is unable to provide all or part of the Databricks Advisory Services in accordance with the Agreement; or (c) 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 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. COOPERATION

4.1 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 Personal Data, Databricks shall, to the extent required by applicable laws promptly notify Customer of such request and reasonably cooperate with Customer to limit, challenge or protect against such disclosure.

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

5. DATA ACCESS & SECURITY MEASURES

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

5.2 Databricks will implement and maintain appropriate technical and organizational security measures to protect against Security Breaches and to preserve the security, availability, integrity and confidentiality of Customer Data in accordance with the Security Addendum ("**Security Measures**"). Such measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Databricks may update the Security Addendum and its Security Measures, provided that any updates shall not materially diminish the overall security of Customer Data or the Databricks Advisory 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.

6. SECURITY INCIDENTS

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

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

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

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

7. SECURITY REPORTS & INSPECTIONS; AUDITS

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

(a) will be performed at least annually;
(b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001;
(c) will be performed by independent third-party security professionals at Databricks' selection and expense; and
(d) will result in the generation of an audit report affirming that Databricks' data security controls achieve industry standards under Service Organization Controls No. 2 (SOC2) in accordance with AT-C 205 or such other alternative standards that are substantially equivalent to SOC 2 Type 2 ("**Report**").

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

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

8. DATA TRANSFERS

8.1 Any Restricted Transfer of Customer Personal Data from Customer to Databricks shall be governed by the Standard Contractual Clauses and UK addendum (as applicable) which shall be deemed incorporated into and form an integral part of this Advisory Services DPA in accordance with Annex B.

8.2 To the extent that Databricks adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy) ("**Alternative Transfer Mechanism**"), such Alternative Transfer Mechanism shall automatically apply instead of the Standard Contractual Clauses described in this Advisory Services 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.

9. DELETION & RETURN

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

10. GENERAL

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

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

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

10.4 In no event shall this Advisory Services 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 Service DPA (including the Standard Contractual Clauses).

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

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

10.7 Notwithstanding anything to the contrary in the Agreement or this Advisory Services 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 Advisory Services DPA (including all Annexes hereto), the Standard Contractual Clauses) 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 in 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 Advisory Services DPA, including all Annexes hereto. Customer agrees that any regulatory penalties incurred by that arise in connection with, Customer's failure to comply with its obligations under this Advisory Services 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.

10.8 In no event does this Advisory Services DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

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

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

[*signature page follows*]

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

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

ANNEX A

DESCRIPTION OF THE PROCESSING / TRANSFER

ANNEX 1(A): LIST OF PARTIES	
Data exporter	**Name of the data exporter:** the entity identified as the "Customer" in the Agreement and this Advisory Services 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 the Agreement. **Activities relevant to the data transferred:** The activities specified in Annex1.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, email: dpa@databricks.com **Activities relevant to the data transferred:** The activities specified in Annex1.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:	Databricks does not intentionally collect or process Personal Data in connection with the provision of the Databricks Advisory Services. The categories of Data Subjects that may be unintentionally processed by Databricks include individuals about whom data is provided to Databricks via the Covered Databricks Advisory 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 parties acknowledge and agree that the purpose of the Agreement is not for Databricks to process Personal Data on behalf of Customer or its Affiliates, and that Customer agrees that in connection with the performance of the Databricks Advisory Services, it will not intentionally grant Databricks' access to any Personal Data . Notwithstanding the foregoing, in the event there is unintentional access to Customer Personal Data, the categories of Personal Data shall be solely 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) and applied restrictions or safeguards	Subject to any applicable restrictions and/or conditions in the Agreement and this Advisory Services DPA, and with prior written authorization, 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 (e.g. whether the data is transferred on a one-off or continuous basis)	Continuous or one-off depending on the services being provided by Databricks.
Nature, subject matter and duration of the Processing	**Nature:** The Databricks Advisory Services include Professional Services and/or Training Services, excluding the Platform 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 Advisory Services and Databricks' obligations under the Agreement (including the DPA, and (ii) further documented, reasonable instructions from Customer agreed upon by the parties (the "**Purposes**").
Period for which the personal data will be retained, or if that is not possible the criteria used to determinate that period, if applicable:	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)

1.1 To the extent the Standard Contractual Clauses are deemed incorporated into and form an integral part of the Professional Services DPA pursuant to Section 8, they shall apply as follows:

(a) In relation to transfers of Customer Personal Data protected by the GDPR, the SCCs shall apply as follows:

(1) The Module Two terms shall apply where Customer is the controller of Customer Personal Data and the Module Three terms shall apply where Customer is a processor of Customer Personal Data;

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

(3) in Clause 9, option 2 ("general authorization") is selected and the process and time period for prior notice of Subprocessor changes is set out in Section 3 of the Professional Services DPA;

(4) in Clause 11, the optional language shall not apply;

(5) in Clause 17, option 1 shall apply and the SCCs will be governed by Irish law;

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

(7) Annex I shall be deemed completed with the information set out in Annex A of the Professional Services DPA;

(8) Annex II shall be deemed completed with the information set out in the Security Addendum.

(b) In relation to transfers of Customer Personal Data protected by UK Data Protection Laws, the SCCs as implemented by Section 1.1(a) above shall apply with the following modifications:

(1) the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the Professional Services DPA;

(2) Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex A of the Professional Services DPA and the Security Addendum, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party"; and

(3) any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

(c) In relation to transfers of Customer Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented by Section 1.1(a) above shall apply with the following modifications:

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