DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms a part of the Databricks Terms of Service found at https://www.databricks.com/termsofservice, unless Subscriber has 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**").

By signing the DPA, Subscriber 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 (defined below) who are authorized to use the 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. In that case, "**Subscriber**" will refer to that company or other legal entity. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Databricks Services under the Agreement, Databricks may process certain Personal Data (such terms defined below) on behalf of Subscriber and where Databricks processes such Personal Data on behalf of Subscriber the Parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

HOW TO EXECUTE THIS DPA

0. If you are an Azure Databricks user, please STOP and reach out to us at privacy@databricks.com.
1. This DPA consists of two parts: the main body of the DPA, and Annexes A, B and C (including Appendices 1, 2 and 3).
2. This DPA has been pre-signed on behalf of Databricks. The Standard Contractual Clauses in Annex C have been pre-signed by Databricks, Inc. as the data importer. This DPA will be null and void if any changes are made to it beyond filling out the sections described in 3, below.
3. To complete this DPA, Subscriber must:
    a. Complete the information in the signature box and sign on Page 9.
    b. Complete the information as the data exporter on Pages 10 and 14.
    c. Complete the information in the signature box and sign on Pages 19, 20, 21 and 24.
4. Send the completed and signed DPA to Databricks by email, indicating the URL(s) on the Subscriber welcome page (e.g., https://dbc-0000aaa0-a0aa.cloud.databricks.com/?o=1234567890123456) or the Subscriber's workspaceId(s) (the value following ?o= in the URL(s)), to dpa@databricks.com.

Upon receipt of the validly completed DPA by Databricks at this email address, this DPA will become legally binding.

HOW THIS DPA APPLIES TO SUBSCRIBER AND ITS AFFILIATES

If the Subscriber entity signing this DPA is a party to the Agreement, this 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 DPA. If the Subscriber entity signing this DPA has executed an Order Form with Databricks pursuant to the Agreement, but is not itself a party to the Agreement, this 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 DPA. If the Subscriber entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Subscriber entity who is a party to the Agreement executes this DPA.

1. DEFINITIONS

1.1 **"Affiliate"** means, with respect to the identified party, any entity that is directly or indirectly controlled by, controlling or under common control with such party.

1.2 **"Applicable Data Protection Laws"** means all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable, EU Data Protection Law.

1.3 "**Authorized Person(s)**" means any person who processes Personal Data on Databricks' behalf, including Databricks' employees, officers, partners, principals, contractors and Subprocessors.

1.4 "**Customer Data**" has the meaning given to it in the Agreement, including without limitation Personal Data.

1.5 **"Data Subject"** means an individual to whom the Personal Data relates.

1.6 "**Databricks Group**" means Databricks, Inc. and its Affiliates.

1.7 "**Databricks Services**" means the Subscription Services and other services Databricks provides under an Agreement.

1.8 **"EU Data Protection Law"** means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data (the "**Directive**"); and (ii) on and after 25 May 2018, 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) ("**GDPR**").

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

1.10 "**Personal Data**" means information relating to an identified or identifiable natural person ("**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 personally identifiable information.

1.11 "**Privacy Shield**" means the EU-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 dated July 12, 2016 (as may be amended, superseded, or replaced).

1.12 "**Privacy Shield Principles**" means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of 12 July 2016 pursuant to the Directive, details of which can be found at www.privacyshield.gov/eu-us-framework.

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

1.14 "**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; or (iv) any "special" or "sensitive" categories of data as those terms are defined according to EU Data Protection Law 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 and its personnel, including any subcontractors, from accessing the relevant data in unencrypted form.

1.15 **"Subprocessor"** means any third party (including any Databricks' Affiliate) engaged by Databricks to process any Customer Data that may contain Personal Data on behalf of Subscriber or who may receive Personal Data provided by Subscriber through the Subscription Services pursuant to the terms of the Agreement.

1.16 "**Subscription Services**" has the meaning given to it in the Agreement.

1.17 "**Usage Data**" means usage data collected by Databricks relating to the use of the Subscription Services by Subscriber.

1.18 The terms "**Controller**", "**Processor**," and "**processing**," have the meanings given to them in Applicable Data Protection Laws. If and to the extent that Applicable Data Protection Laws do not define such terms, then the definitions given in EU Data Protection Law will apply.

2. PURPOSE; OWNERSHIP OF DATA

2.1 Subscriber and Databricks have entered into the Agreement pursuant to which Subscriber is being provided Databricks Services, including the Subscription Services. In using the Subscription Services, Subscriber may submit through the Subscription Services or otherwise provide access to Databricks certain Customer Data. Additionally, when using the Subscription Services, Databricks will collect Usage Data. When such Customer Data or Usage Data contains Personal Data, it will be subject to the terms and conditions of this DPA.

2.2 As between the Parties, all Customer Data processed under the terms of this DPA and the Agreement shall remain the property of Subscriber. Under no circumstances will any member of the Databricks Group act, or be deemed to act, as a "Controller" (or equivalent concept) of the Customer Data processed within the Subscription Services under any Applicable Data Protection Laws. Usage Data, except to the extent such Usage Data contains Personal Data collected from Subscriber, is and shall remain the property of Databricks.

3. SUBPROCESSING

3.1 Subscriber agrees that Databricks may appoint Subprocessors to assist it in providing the Databricks Services by processing Personal Data solely for the purpose of providing the Databricks Services, provided that such Subprocessors:

(a) agree to act only on Databricks' instructions when processing the Personal Data (which instructions shall be consistent with Subscriber's processing instructions to Databricks); and

(b) (ii) agree to protect the Personal Data to a standard consistent with the requirements of this DPA, including by implementing and maintaining appropriate technical and organizational measures to protect the Personal Data they Process consistent with the Security Standards described in Annex B.

3.2 Databricks remains fully liable for any breach of this DPA or the Agreement(s) that is caused by an act, error or omission of such Subprocessor.

3.3 Databricks shall maintain an up-to-date list at www.databricks.com/subprocessors (also available upon request to privacy@databricks.com) of all Subprocessors used in the provision of the Databricks Services who may have access to or process (a) Customer Data (which may contain Personal Data) or (b) other Personal Data received by Databricks from Subscriber through the Subscription Services under the Agreement. Prior to the addition or change of any Subprocessors, Databricks shall provide notice to Subscriber, which may include by updating the Subprocessor list on the website listed above, not less than 30 days prior to the date on which the Subprocessor

shall commence processing Personal Data. It is Subscriber's responsibility to check this website for changes.

3.4 In the event that Subscriber objects to the processing of its Personal Data by any newly appointed Subprocessor as described in Section 3.3, it shall inform Databricks in writing within 10 calendar days after notice has been provided by Databricks. In the event that Subscriber objects on reasonable grounds relating to the protection of Personal Data Databricks will either, at Databricks option (a) work with Subscriber to address Subscriber's reasonable objections and thereafter proceed to use the Subprocessor to perform such processing; (b) instruct the Subprocessor to cease any further processing of Subscriber's Personal Data, which may result in new Subscription Services features enabled by the Subprocessor not being available to Subscriber; or (c) allow Subscriber to terminate this Agreement (and any related services agreement with Databricks) immediately and provide it with a pro rata reimbursement of any sums it may have paid in advance for Subscription Services to be provided but not yet received by Subscriber.

3.5 Subscriber acknowledges that any third party services that may be linked to or used within the Databrick Services ("**Non-Databricks Services**") are governed solely by the terms and conditions and privacy policies of such Non-Databricks Services, and 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 Personal Data) or any interaction between Subscriber 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 Subscriber's enablement, access or use of any such Non-Databricks Services, or Subscriber'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 Agreement.

4. COOPERATION

4.1 Subscriber acknowledges that the Subscription Services provide Subscriber with a number of controls that Subscriber may use to retrieve, correct, delete or restrict Customer Data, which Subscriber may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Subscriber is unable to access the relevant Customer Data within the Subscription Services using such controls or otherwise, Databricks shall reasonably cooperate with Subscriber (at Subscriber's request and expense) to enable Subscriber (or its third party Controller) to respond to any requests, complaints or other communications from Data Subjects and regulatory or judicial bodies relating to the processing of Personal Data under the Agreement(s), including requests from Data Subjects seeking to exercise their rights under Applicable Data Protection Laws (a 'data subject request' or "**DSR**") insofar as this is possible. In the event that any such DSR, complaint or communication is made directly to Databricks, Databricks shall promptly pass such communication on to Subscriber and shall not respond to such communication without Subscriber' express authorization. For the avoidance of doubt, the foregoing shall not prohibit Databricks from communicating with a Data Subject if it is not reasonably apparent on the face of the communication to which customer of Databricks the DSR relates.

4.2 If Databricks receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other public or judicial authorities) seeking the disclosure of Personal Data, Databricks shall not disclose any information but shall promptly notify Subscriber in writing of such request, and reasonably cooperate with Subscriber if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.

4.3 To the extent Databricks is required under Applicable Data Protection Laws, Databricks will assist Subscriber (or its third party Controller), at Subscriber's request and expense, to conduct a data protection impact assessment and, where legally required, consult with applicable data protection

authorities in respect of any proposed processing activity that present a high risk to Data Subjects. Subscriber shall be responsible for any costs arising from Databricks' provision of such assistance.

4.4 At Subscriber's written request, Databricks will make reasonable efforts to provide Subscriber with all information necessary to demonstrate its compliance with EU Data Protection Law.

4.5 If the Applicable Data Protection Laws and corresponding obligations related to the processing of Personal Data originating in the EEA change, the Parties shall discuss in good faith any necessary amendments. Additionally, if reasonably required by Subscriber, Databricks shall enter into a Business Associate Agreement to enable Subscriber to comply with its obligations under HIPAA/HITECH ACT ("**BAA**"). Databricks may charge additional fees for the entering into a Business Associate Agreement.

5. DATA ACCESS & SECURITY MEASURES

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

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 Personal Data ("**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. Subscriber agrees that Databricks' implementation of the Security Measures identified at **Annex B** shall be deemed to be sufficient for the purposes of complying with its obligations under this Section, as of the date of this DPA, provided that Databricks shall review the Security Measures on at least an annual basis**.**

6. SECURITY INCIDENTS

6.1 In the event of a Security Breach, Databricks shall inform Subscriber 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 Subscriber may reasonably require to fulfil Subscriber'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 Subscriber up-to-date about all developments in connection with the Security Breach.

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

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 (including, without limitation, Service Organization Controls No. 2 (SOC2) in accordance with auditing standards in the Statements on Standards for Attestation Engagements No. 16 (SSAE16)) or such other alternative standards that are substantially equivalent to ISO 27001 ("**Report**").

7.2 Databricks will respond in a commercially reasonable timeframe to any requests for additional information or clarification from Subscriber related to such Report. The Report will constitute Databricks' Confidential Information under the confidentiality provisions of the Agreement.

7.3 At Subscriber's written request, Databricks will provide Subscriber with copies of its Report so that Subscriber can reasonably verify Databricks' compliance with the security and audit obligations under this Agreement.

8. DATA PROCESSING AND TRANSPORT

8.1 Databricks will at all times provide an adequate level of protection for the Personal Data, wherever processed, in accordance with the requirements of Applicable Data Protection Laws. Subscriber acknowledges that Databricks and its Subprocessors may maintain data processing operations in countries that are outside of the EEA and Switzerland. As such, both Databricks and its Subprocessors may process Personal Data in non-EEA and non-Swiss countries. This will apply even where Subscriber has agreed with Databricks to use cloud instances of the Subscription Services located in the EEA if such non-EEA processing is necessary to provide support-related or other services requested by Subscriber.

8.2 Databricks shall process Personal Data (i) submitted to Databricks by Subscriber through the Subscription Services only as a Processor acting on behalf of Subscriber (whether as Controller or itself a Processor on behalf of third party Controllers); and (ii) in accordance with Subscriber's documented instructions as set forth in this DPA, the Agreement(s) or as otherwise necessary to provide the Subscription Services; *provided that* Databricks shall inform Subscriber if, in its opinion, Subscriber'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.

8.3 Subscriber acknowledges that the Subscription Services are data-type agnostic, and that Databricks does not have any knowledge of the actual data or types of data contained in the Customer Data. Accordingly, Subscriber shall notify Databricks prior to providing any Sensitive Data. Databricks may impose additional requirements on Subscriber prior to the use of the Subscription Services by Subscriber to process any Sensitive Data, which may include additional fees.

8.4 Where Databricks processes Personal Data under this DPA that is subject to EU Data Protection Laws, Databricks shall:

(a)
  (1) provide at least the same level of protection to such Personal Data as is required by the Privacy Shield Principles;
  (2) comply with its obligations as a data processor set forth in the Model Clauses attached as Annex C, including the appendices attached thereto, and subject to the interpretations set forth in Appendix 3;

(b) promptly notify Subscriber if it makes a determination that it can no longer meet its obligations under Section 8.4(a) above, and in such event, to work with Subscriber and

promptly take all reasonable and appropriate steps to stop and remediate (if remediable) any processing until such time as the processing meets the level of protection as is required by Section 8.4(a); and

(c) promptly cease (and procure all Subprocessors promptly cease) processing such Personal Data if in Subscriber' sole discretion, Subscriber determines that Databricks has not or cannot correct any non-compliance with Section 8.4(a) above in accordance with Section 8.4(b) within a reasonable time frame.

8.5 Databricks acknowledges that Subscriber may disclose this DPA and any relevant privacy or data protection provisions of the Agreement(s) to the US Department of Commerce, European Data Protection Authorities, or any other US or EU judicial or regulatory body with jurisdiction (each, a "**Data Regulatory Authority**") upon their request, provided that for the avoidance this DPA shall remain Confidential Information subject to the restrictions in the Agreement notwithstanding any requirement to share it with a Data Regulatory Authority.

9. OBLIGATIONS OF SUBSCRIBER

Subscriber acknowledges that Databricks does not provide data backup services, and that it is Subscriber's obligation to backup any Customer Data that Subscriber may process through the Subscription Services. As part of Subscriber receiving the Databricks Services under the Agreement, Subscriber agrees and declares as follows:

(i) that the processing of Personal Data by Subscriber, including instructing processing by Data Processor in accordance with this Agreement, is and shall continue to be in accordance with all the relevant provisions of the Applicable Data Protection Laws, particularly with respect to the security, protection and disclosure of Personal Data;

(ii) that if processing by Data Processor involves any Sensitive Data, Subscriber has collected such Sensitive Data in accordance with Applicable Data Protection Laws;

(iii) that Subscriber will inform its Data Subjects as legally required:

(a) about its use of data processors to Process their Personal Data, including Data Processor; and

(b) that their Personal Data may be processed outside of the European Economic Area;

(iv) that it shall respond in reasonable time and to the extent reasonably practicable to enquiries by Data Subjects regarding the processing of their Personal Data by Subscriber, and to give appropriate instructions to Data Processor in a timely manner; and

(v) that it shall respond in a reasonable time to enquiries from a Data Regulatory Authority regarding the processing of relevant Personal Data by Subscriber.

10. DELETION & RETURN

Upon Subscriber' request upon termination or expiry of the Agreement, Databricks shall destroy all Personal 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 Personal Data, in which event Databricks shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

11. GENERAL

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

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

11.3 This DPA may not be modified except by a subsequent written instrument signed by both Parties.

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 the Parties agree that the terms of this DPA shall prevail. Notwithstanding the foregoing, if there is any conflict between this 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 ("**HIPAA Data**"), then the BAA shall prevail to extent the conflict relates to such HIPAA Data.

11.6 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, 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. Without limiting either of the parties' obligations under the Agreement, Subscriber agrees that any regulatory penalties incurred by Databricks in relation to the Subscriber Personal Data that arise as a result of, or in connection with, Subscriber's failure to comply with its obligations under this DPA or any Applicable Data Protection Laws shall count toward and reduce Databricks' liability under the Agreement as if it were liability to the Subscriber under the Agreement.

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

11.8 This DPA and the Model Clauses 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 DPA and agrees to be bound by them.

Subscriber: _____	**Databricks, Inc.**
By: _____	By: DocuSigned by: Scott Starbird B26A3291A9E6477...
Name: _____	Name: Scott Starbird
Title: _____	Title: Director, Legal
Address:	Date: 23-May-2018
_____	
_____	
_____	
_____	
Date: _____	

ANNEX A

DETAILS OF THE PROCESSING

Description of Data Exporter

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

As between the Parties, Subscriber shall be the Data Controller of certain Personal Data provided to Databricks related to its use of the 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):

Categories of data
The personal data transferred concern the following categories of data (please specify):

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 Subscription Services to process any 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 Subscription Services shall be deemed an instruction to Databricks to process such data.

ANNEX B

SECURITY MEASURES

This Annex describes the technical and organizational security measures and procedures Databricks, Inc. ("**Databricks**") shall maintain to protect the security of Personal Data created, collected, received, or otherwise obtained during the performance of the Databricks Services (as defined in the Agreements).

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

Databricks will (i) when any Personal Data is under its control, comply with the measures identified below with respect to such 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 Personal Data is processed or used. This is accomplished by Databricks or its cloud services provider (e.g., Amazon Web Services or Microsoft Azure 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 card-keys;
- logging and monitoring access to data centers where Personal Data is hosted; and
- securing data centers where 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 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 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 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 Personal Data;
- allocation of individual client machines and/or users to specific functions;
- monitoring capability in respect of individuals who delete, add or modify Personal Data
- conducting audits, at least yearly, of authorization profiles;
- procedures limiting the release of 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 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 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 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 work station) 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 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 Personal Data may only be processed in accordance with written instructions issued by Subscriber. This is accomplished by:

- binding policies and procedures for Databricks' employees;

- maintaining agreements with external entities responsible for the protection or processing of 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 Personal Data is protected from accidental destruction or loss. This is accomplished by:

- enabling Subscriber to backup Subscriber'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 Subscriber authorize the restoration of backups (if any), held by Databricks.

ANNEX C

MODEL CLAUSES

Standard Contractual Clauses (processors)

Name of the data exporting organisation: _____

Address: _____

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organisation:

a _____
(the "**data exporter"** or **"Subscriber"**)

And

Name of the data importing organisation: Databricks, Inc.

Address: 160 Spear Street, Suite 1300, San Francisco, CA 94105

Tel.: 866-330-0121; fax: 866-330-0121; e-mail: legal@databricks.com

a Delaware corporation
(the "**data importer"** or **"Databricks"**)

each a "party"; together "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: Director, 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

Signature DocuSigned by: Scott Starbird B26A3291A9E6477...

(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
B26A3291A9E6477...

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 Annex B

DATA EXPORTER
Name: _____
Authorised Signature ……

DATA IMPORTER
Name: Scott Starbird
Authorised Signature ……

DocuSigned by:
Scott Starbird
B26A3291A9E6477...

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

Where the EU Controller-to-Processor Model Clauses ("Clauses") apply pursuant to Section 8 of this Data Processing Addendum, then 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. When used below, the terms "data exporter" and "data importer" shall have the meaning given to them in the Clauses.
Nothing in the interpretations below is intended to vary or 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. For the avoidance of any doubt, in no event shall any party limit its liability with respect to any data subject rights under the Clauses.

Clause 4(h): Obligations of the data exporter regarding non-disclosure requirements
Data exporter agrees that these Clauses constitute data importer's Confidential Information under the confidentiality provisions of the data importer's Agreement and may not be disclosed by data exporter to any third party without data importer's prior agreement (other than to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8).

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

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.

2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, 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.

3. If the data exporter intends to suspend the transfer of personal data and/or terminate these 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").

4. 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 instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. The parties acknowledge that data importer uses external auditors to verify the adequacy of its security measures, including the security of the physical data centres from which data importer provides its data processing services. 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 data importer's selection and expense; and

   d. will result in the generation of an audit report affirming that data importer's data security controls achieve industry standards (including, without limitation, Service Organization Controls No. 2 (SOC2) in accordance with auditing standards in the Statements on Standards for Attestation Engagements No. 16 (SSAE16)) or such other alternative standards that are substantially equivalent to ISO 27001 ("Report");

2. Data importer shall provide responsive and detailed information to data exporter's requests for information (including any requests by data exporter under instruction from data subjects), which may include responses to relevant information security and audit questionnaires;

3. At data exporter's written request, data importer will provide data exporter with copies of the Report so that data exporter can reasonably verify data importer's compliance with the security and audit obligations under the Clauses. The Report will constitute data importer's Confidential Information under the confidentiality provisions of the Agreement (as defined in the DPA).

4. Data exporter agrees to exercise its audit right under Clause 5(f) by instructing data importer to execute the audit measures as described in this Appendix. Should a Data Regulatory 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 conducted no more than annually unless the data exporter reasonably believes the 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 the 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 these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward subprocessing by the data importer.

2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out below, which collectively ensure that the onward subprocessor will provide adequate protection for the personal data that it processes:

a. any onward subprocessor must agree in writing: (i) to only process personal data in the European Economic Area or another country that the European Commission has formally declared to have an "adequate" level of protection in accordance with the requirements of EU Data Protection Law; or (ii) to process personal data on terms equivalent to these Clauses or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities and whose scope extends to transfers of personal data from the territories in which the data exporter is established; and

b. data importer must restrict the onward subprocessor's access to personal data only to what is strictly necessary to perform its subcontracted data processing services to data importer (which shall be consistent with the instructions issued to data importer by data exporter) and data importer will prohibit the onward subprocessor from processing the personal data for any other purpose.

DATA EXPORTER
Name: _____
Authorised Signature ……

DATA IMPORTER
Name: Scott Starbird
Authorised Signature ……

DocuSigned by:
Scott Starbird
B26A3291A9E6477...