

Data Protection Addendum

This Data Protection Addendum (“**Addendum**”) will become effective as of the date the Addendum is executed by both Parties. The “**Parties**” means each of the following: (i) Cloudera, Inc., located at 395 Page Mill Road, 94306 CA, Palo Alto, USA (“**Vendor**”), acting on its own behalf and as agent for each Vendor Affiliate (as defined hereinafter); and (ii) the entity named on the signature page hereto (“**Company**”), acting on its own behalf and as agent for each Company Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

WHEREAS:

(A) Vendor and Company have previously entered into a separate written services agreement, subscription agreement, or other relevant agreement (the “**Agreement**”) which involve Processing of Personal Data of Data Subjects subject to Data Protection Laws in the context of services provided under the Agreement.

(B) This Addendum is hereby attached to and incorporated into the Agreement between Vendor and Company.

(C) In accordance with Data Protection Laws, the Parties enter into this Addendum which shall govern the Processing of Personal Data of Data Subjects subject to Data Protection Laws in the context of services provided under the Principal Agreement.

NOW, THEREFORE, in consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum. Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 “**Applicable Laws**” means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 “**Company Affiliate**” means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 “**Company Group Member**” means Company or any Company Affiliate;

1.1.4 “**Company Personal Data**” means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member pursuant to or in connection with the Agreement;

- 1.1.5 **"Contracted Processor"** means Vendor or a Subprocessor;
- 1.1.6 **"Data Exporter"** means Company;
- 1.1.7 **"Data Importer"** means Vendor;
- 1.1.8 **"Data Protection Laws"** means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country, applicable to the Processing of Company Personal Data;
- 1.1.9 **"EEA"** means the European Economic Area;
- 1.1.10 **"EU Data Protection Laws"** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
- 1.1.11 **"GDPR"** means EU General Data Protection Regulation 2016/679;
- 1.1.12 **"Restricted Transfer"** means:
 - 1.1.12.1 a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or
 - 1.1.12.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 5.4.3 or 11 below;
- 1.1.13 **"Services"** means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Agreement in accordance with the terms and conditions set forth in the Agreement;
- 1.1.14 **"Standard Contractual Clauses"** means the contractual clauses set out in Annex 3, amended as indicated (in square brackets and italics) in that Annex and under section 12.4;
- 1.1.15 **"Subprocessor"** means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Agreement; and
- 1.1.16 **"Vendor Affiliate"** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Vendor and each Vendor Affiliate shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company Group Member's documented reasonable instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor or the relevant Vendor Affiliate shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Company Personal Data.

2.2 Each Company Group Member:

2.2.1 instructs Vendor and each Vendor Affiliate (and authorises Vendor and each Vendor Affiliate to instruct each Subprocessor) to:

2.2.1.1 Process Company Personal Data; and

2.2.1.2 in particular, transfer Company Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Agreement; and

2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 2.2.1 on behalf of each relevant Company Affiliate.

2.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Either party may make reasonable amendments to Annex 1 by written notice to the other party from time to time as the parties reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this Addendum.

3. Vendor and Vendor Affiliate Personnel

Vendor and each Vendor Affiliate shall take reasonable steps to ensure that access to the Company Personal Data by its employees, agents or contractors is strictly limited to those individuals who need to know / have access the relevant Company Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such

individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

- 4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of Company Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Vendor and each Vendor Affiliate shall in relation to the Processing of Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. Such technical and organizational measures are attached hereto as Annex 2 and Company, taking into account the nature of the Processing of Company Personal Data, hereby acknowledges and agrees that such measures represent appropriate technical and organizational security measures with respect to the Processing of Company Personal Data pursuant to this Addendum.

5. Subprocessing

- 5.1 Each Company Group Member authorises Vendor and each Vendor Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Agreement.
- 5.2 Vendor and each Vendor Affiliate may continue to use those Subprocessors already engaged by Vendor or any Vendor Affiliate as at the date of this Addendum (the “**Approved Subprocessors**”), subject to Vendor and each Vendor Affiliate in each case as soon as practicable meeting the obligations set out in section 5.4. The Approved Subprocessors are identified in the list set out in Annex 4 to this Addendum.
- 5.3 Vendor shall give Company prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within 15 calendar days of receipt of that notice, Company notifies Vendor in writing of any objections (on reasonable grounds) to the proposed appointment:
- 5.3.1 Vendor shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor;
- 5.3.2 Vendor may decide to carry on providing the Services to Company without use of the proposed Subprocessor; and
- 5.3.3 where such a change cannot be made within 30 calendar days from Vendor's receipt of Company's notice, notwithstanding anything in the Agreement, Company may by written notice to Vendor with immediate effect terminate the portion of the Agreement that relates to the Services which require the use of the proposed Subprocessor.
- 5.4 With respect to each Subprocessor, Vendor or the relevant Vendor Affiliate shall:
- 5.4.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by this Addendum;

- 5.4.2 ensure that the arrangement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;
- 5.4.3 provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Company may request from time to time.
- 5.5 Vendor and each Vendor Affiliate shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Vendor.

6. Data Subject Rights

- 6.1 Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing appropriate technical and organisational measures as described in section 4.1, insofar as this is possible, for the fulfilment of the Company Group Members' obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.
- 6.2 Vendor shall:
- 6.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data, except if such request relates to an opt-out request for direct marketing; and
- 6.2.2 subject to section 6.2.1 above, ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

- 7.1 Vendor shall notify Company without undue delay upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

Such notification shall as a minimum:

- describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

- communicate the name and contact details of Vendor's data protection officer or other relevant contact from whom more information may be obtained;
- describe the likely consequences of the Personal Data Breach; and
- describe the measures taken or proposed to be taken to address the Personal Data Breach

7.2 Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Vendor and each Vendor Affiliate shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

- 9.1 Subject to sections 9.2 and 9.3 Vendor and each Vendor Affiliate shall promptly and in any event within 30 of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Company Personal Data.
- 9.2 Subject to section 9.3, Company may in its absolute discretion by written notice to Vendor within 30 of the Cessation Date require Vendor and each Vendor Affiliate to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Contracted Processor. Vendor and each Vendor Affiliate shall comply with any such written request within 30 of the Cessation Date.
- 9.3 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor and each Vendor Affiliate shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.
- 9.4 Vendor shall provide written certification to Company that it and each Vendor Affiliate has fully complied with this section 9 within 30 of the Cessation Date.

10. Audit rights

- 10.1 Subject to sections 10.2 to 10.4, Vendor and each Vendor Affiliate shall make available to each Company Group Member on request all information reasonably necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any

Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

- 10.2 Information and audit rights of the Company Group Members only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

A Company Group Member may only mandate an auditor for the purposes of section 10.1 if the auditor is identified in the list set out in Annex 5 to this Addendum, as that list is amended by agreement between the parties in writing from time to time. Vendor shall not unreasonably withhold or delay agreement to the addition of a new auditor to that list.

- 10.3 Company or the relevant Company Affiliate undertaking an audit shall give Vendor or the relevant Vendor Affiliate reasonable notice of any audit or inspection to be conducted under section 10.1 and in no event less than 45 days, and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. Audits may only be conducted during the normal business hours of Vendor or Vendor Affiliate. Vendor or Vendor Affiliate need not give access to its premises for the purposes of such an audit or inspection:

10.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;

10.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or the relevant Company Affiliate undertaking an audit has given prior notice to Vendor or the relevant Vendor Affiliate that this is the case before attendance outside those hours begins; or

10.3.3 for the purposes of more than one audit or inspection, in respect of each Vendor or Vendor Affiliate, in any calendar year, except for any additional audits or inspections which:

10.3.3.1 Company or the relevant Company Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Vendor's or the relevant Vendor Affiliate's compliance with this Addendum; or

10.3.3.2 A Company Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor or the relevant Vendor Affiliate of the audit or inspection.

11. Restricted Transfers

- 11.1 Subject to section 11.3, each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate, (as "data importer") may optionally enter into the

Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

11.2 The Standard Contractual Clauses shall come into effect under section 11.1 on the later of:

11.2.1 the data exporter becoming a party to them;

11.2.2 the data importer becoming a party to them; and

11.2.3 commencement of the relevant Restricted Transfer.

11.3 Section 11.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12. General Terms

Governing law and jurisdiction

12.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

12.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

12.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

12.2 Nothing in this Addendum reduces Vendor's or any Vendor Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

12.3 Subject to section 12.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

12.4 Company or Vendor may:

12.4.1 by at least 30 (thirty) calendar days' written notice to other party from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to

Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

- 12.4.2 propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.
- 12.5 If Company or Vendor gives notice under section 12.4.1:
 - 12.5.1 Vendor and each Vendor Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 5.4.3; and
 - 12.5.2 Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 12.4.1 and/or 12.5.1.
- 12.6 If Company or Vendor gives notice under section 12.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.
- 12.7 Neither Company nor Vendor shall require the consent or approval of any Company Affiliate or Vendor Affiliate to amend this Addendum pursuant to this section 12.5 or otherwise.

Severance

- 12.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the date the Addendum is executed by both parties set forth below.

Company

Signature _____

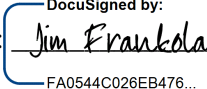
Company Name: _____

Name: _____

Title: _____

Date Signed: _____

Vendor: Cloudera, Inc.

Signature:  _____
FA0544C026EB476...

Name: Jim Frankola

Title: Chief Financial Officer

Date Signed: _____

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Company Personal Data are set out in the Agreement and this Addendum.

The nature and purpose of the Processing of Company Personal Data

Performance of services set out in the Agreement, including technical support and related communications, training, marketing activities, sales invoices, contracts and billing.

The types of Company Personal Data to be Processed

Contact details:

Company name

first name, last name, title

email address

phone number, mobile number

business mailing address

system username

network IP address

billing information

The categories of Data Subject to whom the Company Personal Data relates

Company Group Member, and their employees and staff

The obligations and rights of Company and Company Affiliates

The obligations and rights of Company and Company Affiliates are set out in the Agreement and this Addendum.

ANNEX 2: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

1. Information Security Policies and Standards

The Data Importer will implement security requirements for staff and all subcontractors, service providers, or agents who have access to Personal Data.

These are designed to:

Prevent unauthorized persons from gaining access to Personal Data processing systems (physical access control);

Prevent Personal Data processing systems being used without authorization (logical access control);

Ensure that persons entitled to use a Personal Data processing system gain access only to such Personal Data as they are entitled to access in accordance with their access rights and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control);

Ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control);

Ensure the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing (entry control);

Ensure that Personal Data are Processed solely in accordance with the Instructions (control of instructions);
Ensure that Personal Data are protected against accidental destruction or loss (availability control); and
Ensure that Personal Data collected for different purposes can be processed separately (separation control).

These rules are kept up to date, and revised whenever relevant changes are made to the information system that uses or houses Personal Data, or to how that system is organized.

2. Physical Security

The Data Importer will maintain commercially reasonable security systems at all Data Importer sites at which an information system that uses or houses Personal Data is located. The Data Importer reasonably restricts access to such Personal Data appropriately.

Physical access control has been implemented for all data centers. Unauthorized access is prohibited to the data center through 24x7 onsite staff, and security camera monitoring. Data Centre physical security is audited by an independent firm.

Surveillance camera on entry door is installed and security monitoring by building management is implemented.

3. Organizational Security

When media are to be disposed of or reused, procedures have been implemented to prevent any subsequent retrieval of any Personal Data stored on them before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures have been implemented to prevent undue retrieval of Personal Data stored on them.

Data Importer implemented security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees.

All Personal Data security incidents are managed in accordance with appropriate incident response procedures.

All sensitive data transmitted by Service Provider are encrypted while in transit and when on portable devices or media.

4. Network Security

The Data Importer maintains network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection systems, access control lists and routing protocols.

5. Access Control

Only authorized staff can grant, modify or revoke access to an information system that uses or houses Personal Data.

User administration procedures define user roles and their privileges, how access is granted, changed and terminated; addresses appropriate segregation of duties; and defines the logging/monitoring requirements and mechanisms.

All employees of the Data Importer are assigned unique User-IDs.

Access rights are implemented adhering to the “least privilege” approach.

The Data Importer implements commercially reasonable physical and electronic security to create and protect passwords.

6. Virus and Malware Controls

The Data Importer installs and maintains anti-virus and malware protection software on the system.

7. Personnel

The Data Importer implements a security awareness program to train personnel about their security obligations.

This program includes training about data classification obligations; physical security controls; security practices and security incident reporting.

Service Provider has clearly defined roles and responsibilities for the employees. Screening is implemented before employment with terms and conditions of employment applied appropriately.

Service Provider employees strictly follow established security policies and procedures. Disciplinary process will be applied if employees committed a security breach.

8. Business Continuity

The Data Importer implements appropriate disaster recovery and business resumption plans. Data Importer reviews both business continuity plan and risk assessment regularly. Business continuity plans are being tested and updated regularly to ensure that they are up to date and effective.

9. Additional Technical and Organizational Security Measures

The Data Importer implements additional Technical and Organizational Security Measures as defined in the Agreement.

ANNEX 3: STANDARD CONTRACTUAL CLAUSES

These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).

If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection *This opening recital is deleted if these Clauses are not governed by the law of a member state of the EEA.*

The gaps below are populated with details of the relevant Company Group Member:

Name of the data exporting organisation:

Address:

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

Other information needed to identify the organisation

.....
(the data **exporter (Company)**)

And

The gaps below are populated with details of the relevant Contracted Processor:

Name of the data importing organisation: Cloudera, Inc.

Address: 395 Page Mill Road, Palo Alto, California, 94306

Tel.: (888) 789-1488; fax(888) 789-1488; e-mail: dpo@cloudera.com

Other information needed to identify the organisation:

.....
(the data **importer (Vendor)**)

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.

Background

The data exporter has entered into a data processing addendum (“DPA”) with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

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; [If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words “except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data” are added.]*
- (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; [If these Clauses are not governed by the law of a Member State, the words "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" are deleted.]
- (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; *[If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.]*
- (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 or 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 (Company):

Populated with details of, and deemed signed 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.....

On behalf of the data importer (Vendor):

Populated with details of, and deemed signed on behalf of, the data importer:

Name (written out in full): Jim Frankola

Position: Chief Financial Officer

Address: 395 Page Mill Road, Palo Alto, CA 94306

Other information necessary in order for the contract to be binding (if any):

Signature .....
DocuSigned by:
Jim Frankola
FA0544C026EB476...

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

PART 1: 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.

Data exporter

The data exporter is:
Company Group Member

Data importer

The data importer is:
Vendor

Data subjects

The personal data transferred concern the following categories of data subjects:
Same as the categories of Data Subject to whom the Company Personal Data relates in Addendum ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

Categories of data

The personal data transferred concern the following categories of data:
Same as the types of Company Personal Data to be Processed in Addendum ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:
None

Processing operations

The personal data transferred will be subject to the following basic processing activities:
Same as the nature and purpose of the Processing of Company Personal Data in Addendum ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

PART 2: Business related additions to the Standard Contractual Clauses:

According to Clause 10 “Variation of the contract” of the Standard Contractual Clauses, the parties hereby agree to add the following business related terms to the Standard Contractual Clauses:

-Clause 4 “Obligations of the data exporter”, (f): For clarity, the data exporter undertakes NOT to provide any special categories of data to data importer under these Clauses.

-Clause 5 “Obligations of the data importer”, (a): The parties agree that the termination right may be executed by the data exporter only if the data importer does not cure the non-compliance within 45 days cure period after its notification.

-Clause 5 “Obligations of the data importer”, (b): The parties agree that the termination right may be executed by data exporter only if the data importer does not cure the non-compliance within 45 days cure period after its notification.

-Clause 5 “Obligations of the data importer”, (d), (iii): For clarification purposes only, this section does not apply if the data importer deals with the request in connection with the provision of its standard Customer Support Services provided under the Agreement and/or any opt-out request.

-Clause 5 “Obligations of the data importer”, (j): The parties agree that the data importer will send a copy of such subprocessor agreement upon request of the data exporter. In the event such subprocessor agreement contains commercial information, the data importer may remove such commercial information which does not relate to the processing of personal data.

-Clause 6 “Liability”: for the avoidance of doubt, the liability obligations between the data importer and the data exporter shall be as set out in the Agreement.

DATA EXPORTER (Company)

Populated with details of, and deemed to be signed on behalf of, the data exporter:

Name: _____

Title: _____


Authorised Signature: _____

DATA IMPORTER (Vendor)

Populated with details of, and deemed to be signed on behalf of, the data importer:

Name: Jim Frankola
Title: Chief Financial Officer

Authorised Signature:

DocuSigned by:

FA0544C026EB476...

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):

Same as Addendum ANNEX 2: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

ANNEX 4: LIST OF COMPANY APPROVED VENDOR SUBPROCESSOR

Approved Subprocessor and processing activities

The Approved Subcontractors to be used for processing of personal data are the companies:
posted at <https://www.cloudera.com/legal/subprocessors.html>

ANNEX 5: LIST OF MANDATED AUDITORS

To be completed if Company desires to designate a listed of mandated auditors, for purposes of any audits completed in Section 10.1:
