

Data Processing Addendum
(Last Updated November 2022)

This **DATA PROCESSING ADDENDUM**, including its schedules and appendices ("**Addendum**") is entered into as of the **Effective Date** (as defined below), by Talend and the party entering into the Agreement with Talend that refers to this addendum ("**Customer**"). This Addendum forms part of the agreement between Talend and Customer governing the contractual relationship between Talend and Customer (the "**Agreement**"). In the course of the Agreement, Talend may process (as defined below) personal data (as defined below) on behalf of Customer. This Addendum sets out the terms that apply when personal data of the Customer is processed by Talend under the Agreement, and Talend and Customer shall comply with these with respect to any processing of personal data of Customer under the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and take precedence.

Whereas, this Addendum consists of the following sections:

1. The Data Protection Terms and Conditions;
2. Schedule A: Description of Processing; and
3. Annex: The Standard Contractual Clauses (including Annex I).

Whereas, this DPA has been pre-signed on behalf of Talend. Annex I has been pre-signed by Talend, Inc. as the data importer. Please note that the contracting entity under the Agreement may be a different entity to Talend, Inc.

Whereas, in order to execute this Addendum, Customer must:

1. Complete the information in the signature box and sign the Data Protection Terms and Conditions on page 4 of this Addendum;
2. Complete the information and signature boxes of the Annex, (including Annex I)
3. Send the completed and signed Addendum to Talend by email, indicating the Customer's name, to legal@talend.com.

Whereas, Customer and Talend (the "**Parties**") now wish to enter into the Data Processing Addendum as further described below.

Now Therefore, in furtherance of the foregoing and upon due consideration resulting from the Parties' compliance with Applicable Data Protection Laws, the adequacy and receipt of which is hereby acknowledged, the parties agree as follows as of the date of this Addendum:

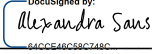








Data Protection Terms and Definitions



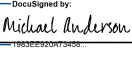

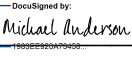



1. **Definitions:** In this Addendum, the following terms shall have the following meanings:
 - 1.1. **"controller", "processor", "data subject", "processing" (and "process") and "special categories of personal data"** shall have the meanings given in Applicable Data Protection Law.
 - 1.2. **"personal data"** shall mean any information that (i) identifies or relates, directly or indirectly, to a natural person, or (ii) the relevant Applicable Data Protection Law otherwise defines as personal data or a similar term.
 - 1.3. **"Applicable Data Protection Law"** shall mean "Data Protection Laws and Regulations" shall mean all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time, including (without limitation) the following laws or regulations and any successor legislation, to the extent applicable to the processing of Protected Data:
 - a) the GDPR and laws implementing or supplementing the GDPR;
 - b) the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR");
 - c) the CCPA
 - d) the Canadian Personal Information Protection and Electronic Documents Act;
 - e) the Singapore Personal Data Protection Act;
 - f) the Australian Privacy Act;
 - g) the Brazilian LGPD;
 - h) the Japan Act on the Protection of Personal Information;
 - i) the China Personal Information Protection Law; and
 - j) the UK Data Protection Act of 2018.
 - 1.4. **"Standard Contractual Clauses"** shall mean the standard contractual clauses, as approved by the European Commission in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, in the form attached at the Annex to this Addendum.
 - 1.5. **"Talend"** means the Talend entity which is a party to this Addendum, as specified in the applicable Agreement between Talend and Customer.
2. **Relationship of the parties:** Customer (the controller) appoints Talend as a processor, or service provider, to process the personal data that is the subject of the Agreement and as more particularly described in Schedule A (the **"Data"**). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.
3. **Lawfulness of the Data:** Customer hereby represents and warrants that Customer complies with the requirements of the Applicable Data Protection Law in collecting and transferring the Data to Talend and permitting Talend to act as a processor of the Data, including any additional requirements applicable to specific categories of information, such as national identifiers, special categories of personal data, or sensitive personal data. In particular, Customer shall make all disclosures and obtain all consents necessary to allow: (i) Customer to disclose, provide or make available the Data to Talend in compliance with Applicable Data Protection Law; and (ii) Talend to process, store, retain, use, disclose, and otherwise deal with the Data in accordance with the Agreement (including this Addendum) and with the Applicable Data Protection Law.
4. **Purpose and Confidentiality limitation:** Talend shall treat the Data as Confidential Information, as defined in the Agreement. Talend shall process, store, retain, use, or disclose the Data as a processor, or service provider, in accordance with the use and confidentiality obligations set out in the Agreement, and in accordance with documented instructions from Customer, as more particularly described in Schedule A (the **"Permitted Purpose"**). Where otherwise required by the Applicable Data Protection Law, Talend shall notify Customer prior to such processing unless Talend is prohibited by law from doing so. Talend shall inform Customer if in its opinion an instruction of Customer infringes Applicable Data Protection Law. Talend shall not sell the Data, nor process, store, retain, use, or disclose the Data (i) for any purposes other than the Permitted Purpose, or (ii) outside of the direct business relationship between Talend and Customer. Talend certifies that it understands these restrictions and will comply with them.

5. **Security:** Talend shall implement appropriate technical and organizational measures to protect the Data from (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Data (a "**Security Incident**"). Talend has implemented the technical and organizational security measures described in Annex II of this Addendum. Talend retains the right to modify or update these security practices at its discretion provided that such modification and update does not materially decrease the overall security of the Data for the duration of the Agreement.
6. **Security incidents:** Upon becoming aware of a confirmed Security Incident, Talend shall inform Customer without undue delay and shall provide timely information and cooperation as Customer may require in order for Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) the Applicable Data Protection Law. Talend shall further take all such measures and actions as are reasonably necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer updated on all material developments in connection with the Security Incident.
7. **Sub-processing:** Talend shall subcontract any processing of the Data to a third-party subcontractor ("**Sub-processor**") in accordance with the Applicable Data Protection Law. Talend remains responsible to the Customer for the provision of all applicable schedules. Customer hereby consents to Talend engaging third party Sub-processors in connection with the processing of the Data, and acknowledges and agrees that Talend Affiliates (as defined in the Agreement) may be retained by Talend as Sub-processor. Talend will impose data protection terms on its Sub-processor to the same standard provided for by the Agreement. Prior to the addition of any new Sub-processor, Talend shall provide notice to Customer, which may include updating the Sub-processor list on the Talend website and/or posting the update to the community section of its website. Customer may object to Talend's addition or replacement of a sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Talend will either not appoint or replace the sub-processor or, if this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).
8. **Cooperation and data subjects' rights:** Talend shall provide reasonable and timely assistance (including by appropriate technical and organizational measures) to Customer at Customer's expense to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, opt out of the sale of the data, and data portability, as applicable); and (ii) any other correspondence, inquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, inquiry, or complaint is made directly to Talend, Talend shall promptly inform Customer providing full details of the same.
9. **European Specific Provisions:**
 - 9.1. Cross-Border Data transfer requirements. To the extent Talend processes or accesses Data related to residents of the EEA or Switzerland from a country that has not been determined by the European Commission as providing adequate protection for personal data, the Standard Contractual Clauses shall be deemed incorporated by reference hereto as the Annex. In the event of a conflict between the terms and conditions of the Annex and the Agreement or this Addendum, the terms and conditions of the Annex shall supersede and take precedence. Customer expressly acknowledges and agrees that Talend may process or access Data from the countries in which the Sub-processors are located.
 - 9.2. Standard Contract Clauses U.K. and Switzerland Transfers. For transfers of Personal Data from the United Kingdom, and/or transfers of Personal Data from Switzerland subject exclusively to the Data Protection Laws and Regulations of Switzerland ("Swiss Data Protection Laws"), (i) general and specific references in the Standard Contractual Clauses to GDPR or EU or Member State Law shall have the same meaning as the equivalent reference in the Data Protection Laws and Regulations of the United Kingdom ("UK Data Protection Laws") or Swiss Data Protection Laws, as applicable; and (ii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under UK Data Protection Laws or Swiss Data Protection laws, as applicable.
 - 9.3. Data Protection Impact Assessment. If Talend believes or becomes aware that its processing of the Data related to data subjects resident of the European Economic Area is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall promptly inform Customer and provide Customer with all such reasonable assistance as Customer may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

10. CCPA. CCPA Compliance. For purposes of the CCPA, Customer is either a Business, Service Provider, or Contractor and Talend is either a Service Provider or Contractor. Talend shall not: (a) sell the Personal Data; (b) retain, use, share, or disclose personal data for any purpose other than for the specific purpose of performing the Services; (c) retain, use, share, or disclose the personal data for a commercial purpose (as defined by the CCPA) other than providing the Services; (d) retain, use, share, or disclose the personal data outside of the direct business relationship between Talend and Customer; or (e) unless to provide the Services or for an authorized business purpose, combine personal data with personal data from another Data Subject. Talend certifies that it understands these restrictions and will comply with them. In the event Talend suspects that Talend is unable to comply with its obligations under the CCPA, it will immediately notify Customer in writing.
11. Deletion or return of Data: Upon termination or expiry of the Agreement, Talend shall (at Customer's election) destroy or return to Customer all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for processing). This requirement shall not apply to the extent that Talend is required by the Applicable Data Protection Law to retain some or all of the Data.
12. Audit: Customer acknowledges that Talend is regularly audited against SOC 2 and 3 standards by independent third-party auditors. Upon request, Talend shall supply a summary copy of its audit report(s) to Customer, which reports shall be subject to the confidentiality provisions of the Agreement. Talend shall also respond to any written audit questions submitted to it by Customer, provided that Customer does not exercise this right more than once per year or in a manner that (i) disrupts Talend's normal business operations, or (ii) causes Talend to breach any obligation of confidentiality to a third party, whether imposed by regulation or contract.
13. Miscellaneous:
- 13.1. Headings. Clause and other headings in this Addendum are for convenience of reference only and will not constitute a part of or otherwise affect the meaning or interpretation of this Addendum.
- 13.2. Entire Agreement. This Addendum (including all schedules and appendices thereto) and any Agreement between the Parties constitute the entire agreement between the Parties relating to the subject matter of this Addendum and supersede all prior agreements, understandings, negotiations and discussions of the Parties in relation to the subject matter of this Addendum.
- 13.3. Severability. The provisions of this Addendum are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability will affect only such phrase, clause or provision, and the rest of this Addendum will remain in full force and effect.
- 13.4. Notices. Any notice or other communication under this Addendum given by either party to the other will be deemed to be properly given if given in writing and delivered in person or facsimile, if acknowledged received by return facsimile or followed within one day by a delivered or mailed copy of such notice, or if mailed, properly addressed and stamped with the required postage, to the intended recipient at its address specified below the signatures on this Agreement, or by electronic mail to the email addresses agreed to between the Parties. Either party may from time to time change its address for notices under this Section by giving the other party notice of the change in accordance with this Section 12.3.
- 13.5. Third-Party Rights. The provisions of this Addendum will endure to the benefit of and will be binding upon the Parties and their respective successors and assigns.
- 13.6. Modifications. The parties may by agreement rescind or vary this Agreement without the consent of any other person.
- 13.7. Counterparts. This Addendum may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument. Execution of an Agreement incorporating the terms of this Addendum shall be deemed to be execution of this Addendum including all attachments.
- 13.8. Governing Law. This Addendum will be governed by and construed in accordance with the governing law of the applicable Talend entity provided in the Agreement, without regard to its conflict of laws principles, except to the extent that Applicable Data Protection Law(s) require otherwise, in which event this Addendum will be governed in accordance with Applicable Data Protection Law(s).

13.9. This Addendum has been signed on behalf of each of the Parties by a duly authorised signatory.

FOR AND ON BEHALF OF CUSTOMER: Name of Customer: _____ Signature: _____ Name: _____ Title: _____ Date: _____	TALEND SAS Signature:  _____ <small>DocuSigned by: Alexandra Sans 64CCE4BC58C748C</small> Name: Alexandra Sans Title: Manager, Commercial Operations Date: _____
Talend Germany GmbH Signature:  _____ <small>DocuSigned by: Phillip Mothersole 40C5A7AF67AF6B3</small> Name: Phillip Mothersole Title: Order Management Specialist Date: _____	Talend Ltd (UK) Signature:  _____ <small>DocuSigned by: Didem Ilter A0720B3CF4A84AB</small> Name: Didem Ilter Title: Contracts Manager Date: _____
Talend Italy Srl Signature:  _____ <small>DocuSigned by: Benoit Dall'Alba EB7DEB94B9C0412</small> Name: Benoit Dall'Alba Title: Accounting Director Date: _____	Talend Spain SL Signature:  _____ <small>DocuSigned by: Benoit Dall'Alba EB7DEB94B9C0412</small> Name: Benoit Dall'Alba Title: Accounting Director Date: _____
Talend Netherlands BV Signature:  _____ <small>DocuSigned by: Benoit Dall'Alba EB7DEB94B9C0412</small> Name: Benoit Dall'Alba Title: Accounting Director Date: _____	Talend Sweden AB Signature:  _____ <small>DocuSigned by: Benoit Dall'Alba EB7DEB94B9C0412</small> Name: Benoit Dall'Alba Title: Accounting Director Date: _____
Talend GmbH (Switzerland) Signature:  _____ <small>DocuSigned by: Benoit Dall'Alba EB7DEB94B9C0412</small> Name: Benoit Dall'Alba Title: Accounting Director Date: _____	Talend Ltd (Ireland) Signature:  _____ <small>DocuSigned by: Benoit Dall'Alba EB7DEB94B9C0412</small> Name: Benoit Dall'Alba Title: Accounting Director Date: _____

Talend KK (Japan) Signature:  Name: Robert Purcell Title: Chief Financial Officer Date: _____	Talend Singapore Pte. Ltd. Signature:  Name: Darren Lim Title: Senior Collections Analyst Date: _____
Talend, Inc. Signature:  Name: Michael Anderson Title: Director of Revenue Operations Date: _____	Talend (Canada) Limited Signature:  Name: Michael Anderson Title: Director of Revenue Operations Date: _____
Talend Australia Pty. Ltd. Signature:  Name: Michael Anderson Title: Director of Revenue Operations Date: _____	Talend China Beijing Technology Co. Ltd. Signature:  Name: Adam Dawe Title: Senior Director of Professional Services Date: _____
Talend USA, Inc. Signature:  Name: Michael Anderson Title: Director of Revenue Operations Date: _____	Talend Data Integration Services Ltd. Signature:  Name: Michael Anderson Title: Director of Revenue Operations Date: _____
Effective Date: _____ (if blank, then the Effective Date is the last indicated date of execution)	

SCHEDULE A

Description of the Processing

This Schedule A forms part of the Agreement and the Addendum and describes the processing that Talend will perform on behalf of Customer.

Subject matter and duration of the processing	The subject matter and duration of the processing are defined in the Agreement.
Nature and purpose of the processing	The processing is for the purpose of Talend delivering the services under the Agreement.
Categories of personal data processed	The personal data processed by Talend is the data that the Customer requires Talend to process under the Agreement. It includes the following data, to the extent that it is personal data: identifying data, commercial data, economic or financial data, and data related to transactions on good and services.
Categories of data subject to which the data relates	The categories of data subject whose data will be processed by Talend under the Agreement include: Customer's customers, Customer's prospective customers, Customer's suppliers, and Customer's business contacts.

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
 - (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

- (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such

notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

[OPTION 1 INTENTIONALLY OMITTED]

- (a) **OPTION 2: GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

- (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
- (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (i) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (ii) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (iii) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (iv) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (v) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (vi) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (vii) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to

them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

[OPTION 2 INTENTIONALLY OMITTED]

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of France.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex I to the Standard Contractual Clauses

This Annex 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.

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

2. Name: Talend, Inc.

Address: 400 South El Camino Real, Ste 1400, San Mateo, CA 94402

Contact person's name, position and contact details: legal@talend.com

Activities relevant to the data transferred under these Clauses: Talend provides an open-source data integration platform that provides software and services for data integration, data management, data quality, and data integration across cloud and on-premises environments.

Signature and date: ...

DocuSigned by:
Michael Anderson
1083EE920A73458...

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

The extent of which Personal Data is provided to Talend is determined by the Talend Customer. Personal Data categories disclosed to Talend by Talend Customers may include (i) data regarding potential customers, customers, partners and other vendors of Customer, (ii) Customer personnel, agents, advisors, and freelancers, or (iii) Customer's personnel, agents, advisors, and freelancers.

Categories of personal data transferred

Talend Services provide data integration tools to Talend Customers; therefore, the categories of Personal Data Talend Customers provide Talend include non-sensitive and sensitive data from all industries. To the extent Talend operates as a Processor on behalf of Talend Customers, Talend Customers may submit Personal Data to the Services, or provide Personal Data to Vendor, which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Employment information

- Contact information (company, email, phone, physical business address)
- Identification information (drivers ID, passport, other government issued ID)
- Professional life information
- Personal life information
- Connection information including internet or electronic network activity
- Location information
- Commercial information
- Device information
- Audio/visual information

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis depending on the use of the Services by Customer.

Nature of the processing

The nature of the Processing of Personal Data by Talend is for the performance of the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

The purposes of the data transfer and further Processing by Talend is the performance of the Services pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Subject to the Deletion of Data section of the Addendum, Talend will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Subprocessor will Process Personal Data as necessary to perform the Services pursuant to the Agreement. Subprocessor will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Commission Nationale de l'Informatique et des Libertés ("CNIL"), France shall act as competent supervisory authority insofar as the relevant data transfer is governed by Regulation (EU) 2016/679.

The UK Information Commissioner's Office shall act as competent supervisory authority insofar as the relevant data transfer is governed by UK Data Protection Laws and Regulations.

The Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

APPENDIX

ANNEX II

Talend Technical and Organizational Security Measures

Talend maintains technical and organizational security program for the security, confidentiality, and integrity of the personal data it processes on behalf of its customers, as described below.

This security program applies to Talend Cloud Services. Most Talend products can also be installed and hosted on the Customer premises, in which case the Data is stored at all time within the Customer environment and systems, and is protected by the Customer's own security controls. In this setup, Customer's own technical and organizational security measures will apply to the Data.

Most Talend Cloud Services may be hosted either on Amazon Web Services (AWS) or Microsoft Azure (Azure), at the choice of the Customer. As further described hereafter, the applicable security controls depend on whether the Customer selected AWS or Azure.

Talend technical and organizational security measures are further described (i) for Talend Cloud Services, in the Talend Security Architecture Overview applicable to the specific Talend Cloud Services purchased by the Customer, and (ii) for Stitch Products, in the Stitch Compliance and Security Documentation, including the Security FAQ. These documents, as updated from time to time, are accessible respectively on Talend.com and Stitchdata.com, or upon request.

1. Security Practices

Talend security organization consists of a dedicated team of security experts distributed across the company who work closely with the Talend CISO. Their mission is to protect Talend and its customers with security best practices. This team supports all aspects of Talend business, including Talend development and operations. The responsibility of Talend security rolls up to the CISO, who also defines Talend security strategy, architecture, and program.

2. Physical Security

Talend maintains security controls to prevent unauthorized physical access to buildings and data centers and to protect its systems and software, and by extension the Talend environment, from damage, interruption, misuse, or theft. Authorizations are reviewed regularly, and access is monitored continuously.

3. Security Trainings

All Talend employees are trained on security best practices. Talend informs all employees about relevant security procedures applicable to their respective roles, and of possible consequences of breaching the security rules and procedures.

All employees involved in the development lifecycle, from creation to deployment and operation, are guided through trainings, reviews, and drills. For trainings, reviews and drills, Talend only uses anonymous data.

4. Security Software Development

The Talend security organization is involved throughout the creation of any new product application, capability, or feature. Our security experts conduct architecture, design, and code reviews.

Talend implements a Top 10 Open Web Application Security Project (OWASP) awareness program during application development, and schedules regular internal and external audits to assess compliance with OWASP best practices.

5. Cloud workload protection and monitoring

Talend uses a combination of security services from third-party vendors to protect Talend Cloud Services.

Our security experts use external scanning tools to ensure that systems and containers are hardened, configured, and patched according to Talend guidelines and best practices.

Talend uses NIST Cybersecurity Framework as part of its global security strategy.

Our deployments leverage the built-in segmentation capabilities of AWS EC2 Security groups and Microsoft Azure Network Security groups to restrict inter-resource communication.

Talend Cloud's perimeter security is composed of (but not limited to):

- Web Application Firewall (WAF) which validates, monitors, and filters all web application and API traffic,
- Network-based intrusion detection system (IDS) and intrusion prevention system (IPS) which alerts on rogue activity and protect against threats such as zero-day attacks,
- Security information and event management system (SIEM) for monitoring and observability of system status, and performance and detection of rogue processes.

Our security experts use external scanning tools to ensure that systems and containers are hardened, configured, and patched according to Talend guidelines and best practices.

6. Authentication, authorization, and access control

Standard access

Tenant users are authenticated with their own unique credentials: username plus password.

Talend use TLS certificates issued by the Talend's approved Certificate Authority (CA) to secure and encrypt all communications between user systems and Talend. Talend supports HTTPS over TLS.

The authentication process follows the OpenID Connect standard and uses either the authorization code or the implicit flow. Once connected, a session is managed using cookies.

Administrative access

Talend Cloud Services administrative access requires management review and approval. Elevated privilege access requires the same level of approval by management.

Access to any management console, Talend Cloud Services, AWS, or Azure requires multifactor authentication (credentials plus secret keys).

Access to the management console is restricted to select members of the Talend Site Reliability Engineering (SRE) or Information Security teams. New account creation follows a strict approval process. Accounts are reviewed quarterly.

System access is provided via Kubernetes administration management.

Password management

Talend maintains a password management policy consistent with industry standard practices that all employees must comply with. It ensures the creation of strong passwords, the protection of those passwords, and the use of a corporate password manager.

All system-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed on at least a quarterly basis.

All production system-level passwords must be part of the Talend IT administered secrets server.

7. Key management

Talend applications and components obtain and use tenant-specific Master Keys from HashiCorp Vault to encrypt tenant-related data.

Front-end TLS endpoints are managed through Traefik (Edge Router running as a Kubernetes service) and Kubernetes Secrets. Private keys are generated by Talend and certificates are signed by Talend's approved Certificate Authority (CA), GoDaddy. The certificates are then published as part of the Certificate Transparency program and uploaded to Traefik configuration as Kubernetes secrets.

8. Vulnerability management

All applications are tested by Talend security experts (dynamic application security testing (DAST) and penetration tests) at least twice a year.

In addition, Talend leverages internal and third-party security services to perform external penetration tests.

Third-party penetration tests are scheduled twice a year and prior to any new Talend Cloud Services release and deployment. The penetration tests cover a wide range of security aspects of the application and address modern web best practices.

All detected vulnerabilities are logged by the Talend Quality Assurance team and analyzed by the Talend Information Security team, which then supports, tracks, and tests their remediation.

Talend follows the Security Content Automation Protocol (SCAP) framework. Vulnerabilities are rated according to the Common Vulnerability Scoring System (CVSS) v3.0 equation. Vulnerabilities are resolved depending on their severity rating and their potential impact on the infrastructure.

Third-party penetration test reports are available upon request at Talend's discretion.

9. Backups

Talend uses AWS or Azure services for both mirroring and long-term storage. All storage processes are automated, monitored, and tested. Mirrors and snapshots are performed twice daily.

10. Disaster recovery and business continuity

Talend maintains a disaster recovery/business continuity (DR/BC) policy that is reviewed, updated, and tested annually.

Talend operates in multiple AWS and Azure regions globally. Any Talend instance in any public cloud region can fail over to another region of the same public cloud vendor.

We are in close contact with both vendors and carefully monitor their service levels to make sure that they meet our required service levels.

Our development team spans six geographical locations: one in the US, four in Europe, and one in Asia. Every development function can be fulfilled by at least two developers.

Our operations team spans five geographical locations: two in the US, three in Europe, and one in Asia. Every operations function can be fulfilled by at least two members of the team.

11. Incident Response Process

Talend maintains a record of security breaches which includes a description of the breach, the time period, the consequences of the breach, the context surrounding the report of the breach, and the mitigation measures taken as a result of the breach.

For each security breach that is a Security Incident, notification by Talend to the Customer (as described in the “Security Incident” section above) will be made without undue delay.

12. Security certifications

Talend is SOC 2 Type 2 certified. Talend technical and organizational security measures are further described in Talend’s-current security attestation report, available upon request.

Talend uses the Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) program to assess our security practices and validate the security posture of our cloud offerings.

Please refer to the AWS and Azure websites for more details about their security certifications and compliance information.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors, subject to change from time to time:

Sub-processor	Service Provided	Data Center Location
Amazon Web Services	Cloud computing and data storage	United States Ireland Germany Japan Singapore Australia
Microsoft Azure	Cloud computing and data storage	United States
MoonshotLabs	Content delivery	United States
Gainsight	Survey provider; analytics	United States
Antidot	Content delivery	France United States
Komiko	CRM communication management	United States
Auth0	Identity Management	United States
Okta	Identity Management	United States
JIRA	Project management; issue tracking	France United States
Kryterion	Talend Service education test provider	United States
Github	Support ticket replication, troubleshooting	United States
Sendgrid	Email service provider	United States
Box	Cloud Storage	United States
Twilio	Communications technology provider	United States
Snowflake	Data storage and analytics	United States
Tableau	Data storage and analytics	United States
Salesforce	CRM; Support management	United States

Intercom	In-app messaging service	United States
Splunk	SIEM	United States
Datadog	Event logging; uptime monitoring	United States
Zuora	Payment card processor	United States
Pendo	Service usage analytics	United States
Zoom	Virtual conferencing service	United States
Webex	Virtual conferencing service	United States
Bluevoyant	Managed Security Service Provider	United States
Signal Science	Web Application Firewall	United States
Jotform	Online forms	United States
Safebase	Compliance posture web portal	United States
Docebo	Learning Management System	United States
Intellum	Learning management	United States
Google Analytics	Analytics	United States
Orca	Cloud security risk detection services	United States
Slack	Internal and external instant messaging; SafeBase authorization	United States
Onetrust	Data Subject Requests	United States
Gitguardian	Github monitoring	United States
Worldpay	Payment card processor	United States

The following Talend controlled subsidiaries and affiliates support, operate, deliver, and maintain Talend services and in the course of doing so, may process, store, or otherwise access customer data.

Subsidiary Affiliate	Location
Talend Australia Pty Ltd.	Australia
Talend Beijing Technology Co. Ltd.	China
Talend (Canada) Limited	Canada
Talend Data Integration Services Private Limited	India
Talend Germany GmbH	Germany

Talend GmbH	Switzerland
Talend, Inc.	Delaware
Talend Italy S.r.l.	Italy
Takend KK	Japan
Talend Limited	Ireland
Talend Ltd.	United Kingdom
Talend Netherlands B.V.	Netherlands
Talend Singapore Pte. Ltd.	Singapore
Talend Spain, S.L.	Spain
Talend Sweden AB	Sweden
Talend USA, Inc.	Delaware
Stitch Inc.	Delaware