Confluent Cloud
Data Processing Addendum

Updated: January 1, 2021

This Data Processing Addendum ("**DPA**"), forms part of the Confluent Cloud Subscription Agreement or other written or electronic terms of service or subscription agreement ("**Agreement**") between Confluent, Inc. ("**Confluent**") and the **Customer** signatory thereto. This DPA applies where, and to the extent that, Confluent processes Personal Data on behalf of Customer when providing Services under the Agreement. The DPA does not apply where Confluent determines the purpose and means of the processing of Personal Data. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. The parties agree that this DPA shall replace any existing DPA or other data protection provisions the parties may have previously entered into in connection with the Services.

In consideration of the mutual obligations set forth 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 DPA to the Agreement are to the Agreement as amended by, and including, this DPA.

Definitions

(a) "**Affiliate**" means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

(b) "**Agreement**" means the written or electronic agreement between Customer and Confluent for the provision of the Services to Customer.

(c) "**Control**" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "**Controlled**" will be construed accordingly.

(d) "**Customer Data**" means any Personal Data that is uploaded into Confluent Cloud for storage or hosting that Confluent processes on behalf of Customer in the course of providing Services.

(e) "**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

(f) "**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.

(g) "**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement.

(h) "**EEA**" means the European Economic Area.

(i) "**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**"); and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**").

(j) **"Model Clauses"** means Annex A, the Standard Contractual Clauses for Data Processors as approved by the European Commission in Decision 2010/87/EU, attached to and forming part of this Addendum.

(k) "**Personal Data**" means any information relating to an identified or identifiable natural person.

(l) "**Processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" will be interpreted accordingly.

(m) "**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

(n) **"Sell" or "Sale"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing or by electronic or other means, Customer Data to a third party for monetary or valuable consideration.

(o) "**Services**" means any cloud service offering provided by Confluent to Customer pursuant to the Agreement.

(p) "**Subprocessor**" means any Data Processor engaged by Confluent or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Subprocessors may include third parties or Confluent's Affiliates.

Scope of this DPA

This DPA applies where and only to the extent that Confluent processes Customer Data on behalf of Customer in the course of providing Services to the Customer pursuant to the Agreement.

Roles and Scope of Processing

3.1 *Role of the Parties*. As between Confluent and Customer, Customer is the Data Controller of Customer Data and Confluent shall process Customer Data only as a Data Processor acting on behalf of Customer.

3.2 *Customer Processing of Customer Data*. Customer agrees that (i) it will comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to Confluent; and (ii) it has provided notice and obtained (or

will obtain) all consents and rights necessary for Confluent to process Customer Data pursuant to the Agreement and this DPA.

3.3 *Confluent Processing of Customer Data*. Confluent will process Customer Data only (i) for the purpose of providing the Services and in accordance with Customer's documented lawful instructions as set forth in the Agreement and this DPA; (ii) as part of the direct business relationship between Customer and Confluent; (iii) on behalf of Customer and Confluent's other customers, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity; or (iv) as required by law, provided Confluent shall inform Customer of such legal requirement prior to commencing such processing unless prohibited by law. The parties agree that the Customer's complete and final instructions with regard to the nature and purposes of the processing are set out in this DPA. Confluent will not Sell Customer Data.

Confluent certifies that it understands the restrictions in this section 3.3 and will comply with such restrictions.

3.4 *Details of Data Processing*

(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

(b) Duration: As between Confluent and Customer, the duration of the data processing under this DPA is the term of the Agreement.

(c) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of Confluent's obligations under the Agreement and this DPA (or as otherwise agreed by the Parties).

(d) Nature of the processing: The provision of a distributed streaming platform which enables Customer to access data as real-time streams, and such other Services, as described in the Agreement.

(e) Categories of data subjects: The data subjects of Customer may include Customer's end users, employees, contractors, suppliers, and other third parties.

(f) Types of Customer Data: Personal Data that is uploaded to the Services by the Customer.

Subprocessing

4.1 *Authorized Subprocessors*. Customer agrees that in order to provide the Services, Confluent may engage Subprocessors to process Customer Data. Confluent maintains a list of its authorized Subprocessors on its website at https://www.confluent.io/sub-processors/.

4.2 *Subprocessor Obligations*. Where Confluent authorizes any Subprocessor as described in section 4.1:

(a) Confluent will restrict the Subprocessors access to Customer Data only to what is necessary to assist Confluent in providing or maintaining the Services, and will prohibit the Subprocessor from accessing Customer Data for any other purpose;

(b) Confluent will enter or has already entered into a written agreement with the Subprocessor imposing data protection terms that require the Subprocessor to protect the Customer Data to the standard required by EU Data Protection Laws and in compliance with the California Consumer Privacy Act; and

(c) Confluent will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause Confluent to breach any of its obligations under this DPA.

4.3 Subprocessor Updates. Confluent will provide Customer with reasonable prior notice on its website if it intends to make any changes to its Subprocessors. Customer may receive notifications of new Subprocessors and updates to existing SubProcessors by subscribing for updates at https://www.confluent.io/subscribe-to-sub-processor-updates/. Customer may object in writing to Confluent's appointment of a new Subprocessor, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. 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).

Security Measures and Security Incident Response

5.1 *Security Measures.* Confluent has implemented and will maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data ("**Security Measures**"). The Security Measures applicable to the Services are set forth at https://www.confluent.io/cloud-enterprise-security-addendum, as updated or replaced from time to time in accordance with section 5.2.

5.2 *Updates to Security Measures*. Customer has carried out its own review of the information made available by Confluent relating to data security and has made an independent determination that the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that Confluent may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

5.3 *Personnel*. Confluent restricts its personnel from processing Customer Data without authorization by Confluent as set forth in the Security Measures and shall ensure that any person who is authorized by Confluent to process Customer Data is under an appropriate obligation of confidentiality.

5.4 *Customer Responsibilities*. Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services in accordance with the Agreement. Customer may elect to implement technical or organisation measures in relation to Customer Data, which may include (i) protecting account authentication credentials; (ii) protecting the security of Customer Data when in transit to and from the Services; (iii) implementing measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in

a timely manner in the event of a physical or technical incident; and (iv) taking any appropriate steps to securely encrypt or pseudonymise any Customer Data uploaded to the Services.

5.5 *Security Incident Response*. Upon becoming aware of a Security Incident, Confluent will notify Customer without undue delay and will provide information relating to the Security Incident as it becomes known or as is reasonably requested by Customer. Confluent will also take reasonable steps to mitigate and, where possible, to remedy the effects of, any Security Incident.

Audit Reports

6.1 *Reports.* Customer acknowledges that Confluent is regularly audited against SSAE 18 and SOC 2 Type II standards by independent third-party auditors. Upon request, Confluent shall supply a copy of its SOC 2 audit report(s) to Customer, which reports shall be subject to the confidentiality provisions of the Agreement. Confluent shall also respond to any written audit questions submitted to it by Customer provided that Customer shall not exercise this right more than once per year.

6.2 *Customer Audits.* Customer agrees that Confluent's compliance with section 6.1 shall fulfil any audit cooperation responsibilities that may apply to Confluent under Data Protection Laws.

International Transfers

7.1 *Data Center locations*. Confluent shall store all Customer Data only in the geographic location(s) that Customer specifies via the Service. Confluent may process Customer Data anywhere in the world where Confluent, its Affiliates or its Subprocessors maintain data processing operations. Confluent will at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

7.2 *Application of Model Clauses*. The Model Clauses will apply, by incorporation into this DPA, to Customer Data that originates inside the EEA, Switzerland, or the United Kingdom and that is transferred outside the EEA, Switzerland, or the United Kingdom, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the GDPR).

7.3 *Alternative Data Export Solutions*. Notwithstanding the foregoing section 7.2, the parties agree that in the event Confluent adopts another alternative data export solution (as recognized under EU Data Protection Laws), then the alternative data export solution shall apply instead of the Model Clauses. In the event that the alternative data export solution is later determined to not constitute an adequate level of data protection under EU Data Protection Laws, the Model Clauses shall apply as the data export solution.

Return or Deletion of Data

Upon termination or expiration of the Agreement, Confluent shall (at Customer's election) delete or return to Customer all Customer Data in its possession or control in accordance with the terms of the Agreement. This requirement shall not apply to the extent Confluent is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on

back-up systems, which Customer Data Confluent shall securely isolate and protect from any further processing, except to the extent required by law.

Cooperation

9.1 *Access*. To the extent that Customer is unable to independently access the relevant Customer Data within the Services and provided that Customer has configured the Services in accordance with Confluent's recommendations, Confluent shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement when Customer is required to respond to such requests under applicable Data Protection Laws. In the event that any such request is made directly to Confluent, Confluent shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Confluent is required to respond to such a request, Confluent will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

9.2 *Law Enforcement Request*. If a law enforcement agency sends Confluent a demand for Customer Data (for example, through a subpoena or court order), Confluent will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Confluent may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then Confluent will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Confluent is legally prohibited from doing so.

9.3 *Legal Compliance*. To the extent Confluent is required under Data Protection Law, Confluent will (at Customer's expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

General

10.1 For the avoidance of doubt, any claim or remedies the Customer may have against Confluent, any of its Affiliates and their respective employees, agents and Subprocessors arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; and (iii) under applicable Data Protection Laws, including any claims relating to damages paid to a data subject, will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Customer further agrees that any regulatory penalties incurred by Confluent in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Confluent's liability under the Agreement as if it were liability to the Customer under the Agreement.

10.2 Any claims against Confluent or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms. In no event shall any

party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

10.3 To the extent reasonably necessary to comply with changes to applicable Data Protection Laws or in response to guidance or mandates issued by any court, regulatory body, or supervisory authority with jurisdiction over Confluent, Confluent may modify, amend, or supplement the terms of this DPA. Confluent will endeavour to provide prior written notice of any such changes to Customer by posting a notice on Confluent's website and in Customer's Confluent Cloud web portal, where applicable.

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

10.5 Customer acknowledges that Confluent may disclose the privacy provisions in this DPA to the U.S. Department of Commerce, the Federal Trade Commission, a European supervisory authority, or any other U.S. or EU judicial or regulatory body upon their lawful request.

10.6 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

10.7 The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.

Annex A - Model Clauses

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.

Customer is the **data exporting** organisation (the **data exporter**)

And

Confluent is the **data importing** organisation (**the data importer**)

each a "**party**"; together "**the parties**".

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. Definitions

For the purposes of the Clauses:

'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;

'the data exporter' means the controller who transfers the personal data;

'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;

'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;

'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;

'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.

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.

3. Third-party beneficiary clause

3.1 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.

3.2 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.

3.3 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.

3.4 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.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

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.

6. Liability

6.1 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.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

6.4 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.

7. Mediation and jurisdiction

7.1 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.

7.2 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.

8. Cooperation with supervisory authorities

8.1 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.

8.2 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.

8.3 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).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

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.

11. Subprocessing

11.1 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.

11.2 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.

11.3 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.

11.4 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.

12. Obligation after the termination of personal data processing services

12.1 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.

12.2 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.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Model 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 the legal entity that is identified as "Customer" in the DPA.

Data importer

The data importer is Confluent, Inc. Confluent provides a distributed streaming platform online which enables its customers to access data as real-time streams.

Data subjects

Data subjects are defined in section 3.4 of the DPA.

Categories of data

Categories of data are defined in section 3.4 of the DPA.

Special categories of data

The Service is not designed to require the submission of special categories of Personal Data except as those defined in section 3.4 of the DPA. To the extent such data is submitted to the Service, apart from those defined in section 3.4 of the DPA, it is determined and controlled by data exporter in its sole discretion.

Processing operations

The purpose of the processing is set out in section 3.4 of the DPA.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Model Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The security measures are described at https://www.confluent.io/cloud-enterprise-security-addendum.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Model Clauses and must be completed and signed by the parties.

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. The provisions of the Model Clauses shall take precedence over this Appendix, and the provisions of this Annex shall be considered as business-related clauses within the meaning of Recital 4 of Decision 2010/87/EU and shall not conflict with the Model Clauses. Subject to the above, where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Model Clauses.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's confidential information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to the Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

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

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

2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.

3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").

4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. The parties acknowledge that data importer uses external auditors to assess the adequacy of its data processing, including the security of the systems and premises used by data importer to provide data processing services.

2. The parties further acknowledge that these audits:

   (a) are performed once each year;

   (b) are comprehensively assessed against SOC 2 standards;

(c) are conducted by auditors selected by the data importer, but otherwise conducted with all due and necessary independence and professionalism; and

(d) are fully documented in an audit report that affirms the data importer's controls meet the standards against which they are assessed ("**Report**");

3. At data exporter's written request, data importer will (on a confidential basis) provide data exporter with a copy of the Report so that data exporter can verify data importer's compliance with the audit standards against which it has been assessed and these Clauses.

4. Data importer shall further provide detailed written responses (on a confidential basis) to all reasonable requests for information made by data exporter, including responses to information security and audit questionnaires, that data exporter considers necessary to confirm data importer's compliance with these Clauses.

5. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in this Appendix.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

3. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but to limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

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

2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's

compliance with the requirements set out below, which collectively ensure that the onward subprocessor will provide adequate protection for the personal data that it processes:

(a) any onward subprocessor must agree in writing:

(i) to only process personal data in the European Economic Area or another country that the European Commission has formally declared to have an "adequate" level of protection in accordance with the requirements of applicable Data Protection Laws; or

(ii) to process personal data on terms equivalent to these Clauses or pursuant to a Binding Corporate Rules approval granted by competent European data protection authorities and whose scope extends to transfers of personal data from the territories in which the data exporter is established; and

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

3. Data importer shall maintain a list of all onward subprocessors it has engaged to process personal data pursuant to these Clauses. This list shall be made available on the data importer's website as indicated in section 4 of the DPA.