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.

1. 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.
"Data Protection Laws" means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement.

"EEA" means the European Economic Area.

"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").

"Model Clauses" means Annex A, the Standard Contractual Clauses for Controller-to Processor transfers, as approved by the European Commission in Decision 2021/914, attached to and forming part of this Addendum.

"Personal Data" means any information relating to an identified or identifiable natural person.

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

"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.

"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.

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

"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.

2. 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.

3. 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.
4. **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/](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/](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).

5. **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](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.

6. **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.

7. **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.

8. 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.

9. 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.

10. 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.
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) for the transfer of personal data to a third country.

(b) The Parties:

(i) The 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 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

(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 organisational 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 (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.

8.7 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

(a) 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 thirty (30) 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. 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.
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.

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

(a) 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.
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.

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.

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.

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.

The Parties agree that if one Party is held liable under paragraph (e), 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.

The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

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.

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;

(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.
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).

(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. 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 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.).

(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.

15.1 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.

(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.
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).

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 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.

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. 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.

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**

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

(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.
APPENDIX TO STANDARD CONTRACTUAL CLAUSES

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

The data exporter is the legal entity that is identified as “Customer” in the DPA. Customer is the Controller.

Data importer(s):

The data importer is Confluent, Inc. Confluent, Inc. provides a distributed real-time data streaming platform online which processes personal data upon the instruction of the data exporter in accordance with the terms of the Clauses. Confluent is the Processor.
B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Data subjects include the individuals about whom data is provided to Confluent via the Services (as defined in the DPA) by (or at the direction of) data exporter.

Categories of personal data transferred:

Depending on Customer’s use of the Services, Customer may elect to transfer any of the following categories of the following categories in the personal data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, phone number, first name, last name, initials, email address, gender, date of birth, social media identifiers, emergency contact details), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example MAC address);
- Profiling (for example click streams, browsing logs, IP-addresses, domains, apps installed, log data, or profiles based on marketing preferences);
• HR and recruitment data (for example recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);

• Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);

• Citizenship and residency information (for example citizenship, naturalization status, nationality, immigration status, passport data, details of residency or work permit);

• Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority; or

• Any other personal data identified in Article 4 of the GDPR.

**Sensitive data (if applicable):**

Data exporter may submit special categories of data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person’s sex life or sexual orientation, or data relating to criminal convictions or offences). Data exporter is responsible for ensuring a level of data protection commensurate with the sensitivity of the Message Content it uploads to the Cloud Service including, without limitation, an appropriate level of message-level encryption, according to the terms of the Confluent Cloud Security Addendum.

**The frequency of the transfer:**

Data processing will be on a continuous basis for the period specified in the Agreement to which these Clauses are annexed. Such period will automatically terminate upon the deletion by the data importer of all data processed pursuant to the DPA.
**Nature of the processing:**

Confluent will use and otherwise process Customer Data only in accordance with Customer’s documented instructions and as described and subject to the following: (a) to provide Customer the Services, (b) for Confluent’s legitimate business operations incident to delivery of the Services; and (c) if otherwise permitted by applicable Data Protection Laws and/or by the Standard Contractual Clauses.

**Purpose(s) of the data transfer and further processing:**

Performance of the Services

**The period for which the personal data will be retained:**

Data importer will delete Customer Data upon expiration or termination of data exporter’s use of the Services, in accordance with the terms applicable to the DPA.

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

Data importer utilizes subprocessors to provide limited services on data importer’s behalf, such as storage of Customer Data pursuant to Customer’s instructions. Any such subprocessor will be permitted to obtain Customer Data only to deliver the Services the data importer has retained them to provide, and they are prohibited from using Customer Data for any other purpose.

**C. COMPETENT SUPERVISORY AUTHORITY**

The competent supervisory authority is the Member State in which the data exporter is established.
ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The technical and organizational measures, internal controls, and information security routines set forth in the Confluent Cloud Security Addendum available at https://www.confluent.io/legal/confluent-cloud-security-addendum and the Confluent Cloud Security Controls available at https://www.confluent.io/legal/confluent-cloud-security-controls are hereby incorporated into this Annex II by this reference and are binding on the data importer as if they were set forth in this Annex II in their entirety.