Confluent Cloud
Data Processing Addendum

Last Updated: February 17th, 2023

This Data Processing Addendum ("**DPA**"), forms part of the Confluent Cloud Terms of Services or other written or electronic terms of service or subscription agreement ("**Agreement**") between the Confluent entity which entered into the Agreement ("**Confluent**") and the **Customer** signatory thereto. 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.

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) "**CCPA**" means Title 1.81.5 California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended by the California Privacy Rights Act of 2020 ("**CPRA**") or otherwise, or superseded from time to time.

(d) "**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.

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

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

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

(h) **"EU GDPR"** means 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(i) "**GDPR**" means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

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

(k) **"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 Personal Data to a third party for monetary or valuable consideration.

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

(m) "**Subprocessor**" means any 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.

(n) **"UK GDPR"** means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

(o) The terms "**Business**", "**collect**", "**Consumer**", "**Controller**", "**Data Subject**", "**Processor**," "**process**,", "**processing**" and "**Personal Data**", and "**Service Provider**" have the meanings given to them in applicable Data Protection Laws.

2. Scope of this DPA

This DPA applies where and only to the extent that Confluent processes Customer Personal Data on behalf of Customer in the course of providing Services to the Customer pursuant to the Agreement. The DPA does not apply where Confluent determines the purpose and means of the processing of Personal Data.

3. Roles and Scope of Processing

3.1 Role of the Parties. As between the parties, Customer may act as Controller and/or Processor of Customer Personal Data and Confluent may act as Processor and/or subprocessor of Customer Personal Data. Nothing in the Agreement or in this DPA shall prevent Confluent from using or sharing any data where Confluent determines the purposes and means of the processing of such data.

3.2 Customer as Controller of Customer Personal Data. If Customer is Controller of Customer Personal Data, Customer agrees that (i) it will comply with its obligations as a Controller under Data Protection Laws in respect of its processing of Customer Personal 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 Personal Data pursuant to the Agreement and this DPA.

3.3 Customer as Processor of Customer Personal Data. If Customer is Processor of Customer Personal Data, Customer warrants on an ongoing basis that the relevant Controller has authorized: (i) Confluent's processing of Customer Personal Data as outlined in this DPA and in Exhibit A; (ii) Customer's appointment of Confluent as another processor; and (iii) Confluent's engagement of Subprocessors as described in Section 5 below. To the extent required by applicable Data Protection Laws, Customer will immediately forward to the relevant Controller any notice provided by Confluent in connection to this DPA.

3.4 Customer Instructions. Confluent will process Customer Personal 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) 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 certifies that it understands the restrictions in this Section 3.4 and will comply with such restrictions.

3.5 Details of Data Processing

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

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

(c) Purpose of the processing. Performance of the Services.

(d) Nature of the processing: Confluent will use and otherwise process Customer Personal Data only in accordance with Customer's documented instructions and as described and subject to the terms of the Agreement and this DPA.

(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 Personal Data. Personal data processed under this DPA include Customer Personal Data. Customer acknowledges that it solely chooses the nature and types of Customer Personal Data and that Confluent will be generally unaware of the details of Customer Personal Data processed within the Services.

4. Data Transfers

4.1 Data Storage and Processing Facilities. Customer Personal Data will only be deployed in the geographic location(s) that Customer specifies via the Service (the "**Deployment Region**"). Customer is solely responsible for any transfer of Customer Personal Data caused by Customer's subsequent designation of other Deployment Regions. Confluent may process Customer Personal 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 Personal Data processed, in accordance with the requirements of applicable Data Protection Laws.

4.2 Cross-Border Transfers. Where the transfer of Customer Personal Data is from the EEA, Switzerland or the United Kingdom to a territory which has not been recognized by the European Commission as providing an adequate level of protection for Customer Personal Data on the basis of Article 45 GDPR (or in the case of transfers from the United Kingdom, by the United Kingdom Government), Confluent agrees to process that Customer Personal Data in compliance with the provisions outlined in Exhibit A hereto, which forms an integral part of this DPA.

5. Subprocessing

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

5.2 Subprocessor Obligations. Where Confluent authorizes any Subprocessor as described in Section 5.1 above:

(a) Confluent will restrict the Subprocessors access to Customer Personal Data only to what is necessary to assist Confluent in providing or maintaining the Services, and will prohibit the Subprocessor from accessing Customer Personal 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 Personal Data to the standard required by applicable Data Protection Laws; 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.

5.3 Subprocessor Updates. Confluent will provide Customer with a 30-day 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, within 90 days of notification, object in writing to Confluent's appointment of a new Subprocessor, provided that such objection is based on reasonable grounds relating to the processing of Customer Personal Data by the new Subprocessor. In such event, the parties will discuss such objection 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).

6. Security Measures and Security Incident Response

6.1 Security Measures. Confluent has implemented and will maintain appropriate technical and organizational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data ("**Security Measures**"). The Security Measures applicable to the Services are set forth in the Confluent Cloud Security Addendum available at https://www.confluent.io/cloud-enterprise-security-addendum and in the Confluent Cloud Security White Paper available at https://www.confluent.io/legal/confluent-cloud-security-controls, as updated or replaced from time to time in accordance with Section 6.2 below.

6.2 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.

6.3 Personnel. Confluent restricts its personnel from processing Customer Personal 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 Personal Data is under an appropriate obligation of confidentiality.

6.4 Customer Responsibilities. Without prejudice to Confluent's obligations under this DPA, and elsewhere in the Agreement, Customer is responsible for its secure use of the Services, including: (i) protecting account authentication credentials; (ii) protecting the security of Customer Personal 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 Personal 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 Personal Data uploaded to the Services.

6.5 Security Incident. In the event of a Security Incident, Confluent will notify Customer without undue delay and will provide updates to Customer. Confluent will reasonably cooperate with Customer as required to fulfill Customer's obligations under Data Protection Laws.

7. Audits

7.1 Audit Reports. Confluent uses external auditors to evaluate the continued effectiveness of its Security Measures. Upon request and at no additional cost to Customer, Confluent will provide Customer access to reasonably requested documentation evidencing such effectiveness in the form of the relevant audits or certifications listed in the Confluent Cloud Security Addendum ("**Audit Reports**"). Audit 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.

7.2 Customer Audit Rights. To the extent Customer's audit requirements under applicable Data Protection Laws cannot reasonably be satisfied through Audit Reports, documentation or compliance information Confluent makes generally available to its customers, Confluent will promptly respond to Customer's additional audit requests. Before the commencement of an audit, Customer and Confluent will mutually agree upon the scope, timing, duration, and control and evidence requirements, provided that this requirement to agree will not permit Confluent to unreasonably delay performance of the audit. To the extent needed to perform the audit, Confluent will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Personal Data by Confluent available. Neither Customer nor the third-party auditors, if any, shall have access to any data from Confluent's other customers or to Confluent systems or facilities not involved in the processing of Customer Personal Data. Customer is responsible for all costs and expenses related to such audit, including all reasonable costs and expenses for any and all time Confluent expends for any such audit.

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

9. Cooperation

9.1 Data Subject Request. The Services provide Customer with the ability to retrieve and delete Customer Personal Data. Customer may use these controls to comply with Customer's obligations under applicable Data Protection Laws, including Customer's obligations related to any requests from data subjects ("**Data Subject Requests**"). To the extent that Customer is unable to independently access the relevant Customer Personal Data using such controls or otherwise, Confluent shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to such Data Subject Requests. In the event that any such Data Subject Request is made directly to Confluent, Confluent shall, to the extent legally permitted: (i) advise the data subject to submit their Data Subject Request to Customer; (ii) promptly notify Customer; and (iii) not otherwise respond to that Data Subject Request without authorization from Customer unless legally compelled to do so. Customer will be responsible for responding to any such Data Subject Requests.

9.2 Requests for Customer Personal Data. If Confluent receives a subpoena, court order, warrant or other legal demand from law enforcement or public or judicial authorities seeking the disclosure of Customer Personal Data, Confluent shall, to the extent permitted by applicable laws, promptly notify Customer in writing of such request and reasonably cooperate with Customer to limit, challenge or protect against such disclosure.

9.3 Legal Compliance. To the extent Confluent is required under applicable Data Protection Laws, 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. CCPA Compliance

10.1 Applicability. This section 10 applies to the extent Customer is a Business that is subject to the CCPA and submits Personal Information (as that term is defined under CCPA) as part of Customer Personal Data in connection with Confluent's performance of the Agreement. Customer appoints Confluent as its Service Provider to collect and process the Customer Personal Data for the purposes outlined in section 3.4.

10.2 Service Provider Commitments. Confluent will not (a) Sell Customer Personal Data; (b) retain, use, or disclose the Customer Personal Data for any purpose other than for the Business Purpose, including to retain, use, or disclose the Customer Personal Data for a commercial purpose other than providing its Services under the Agreement; (c) retain, use, or disclose the Customer Personal Data outside of the direct business relationship between Confluent and the Customer; (d) process the Customer Personal Data for targeted and/or cross context behavioural advertising; (e) combine Customer Personal Data that it receives from, or on behalf of, Customer, with Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the Consumer, if and to the extent such combination would be inconsistent with the limitations on Service Providers under the CCPA or other laws.

11. General

11.1 For the avoidance of doubt, any claim or remedies the Customer and/or its Affiliates may have against Confluent, any of its Affiliates and their respective employees, agents and Subprocessors (hereinafter "**Confluent Group**") arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) for breach of cross-border data transfers and related provisions outlined in the Standard

Contractual Clauses (to the extent applicable and as defined in Exhibit A hereto); (iii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; and (iv) 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. Such limitation of liability does not apply to any direct claim or remedies a data subject may have against Customer or Confluent. Customer further agrees that any regulatory penalties incurred by Confluent Group in relation to the Customer Personal 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.

11.2 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.

11.3 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/or in Customer's Confluent Cloud web portal, where applicable.

11.4 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.

11.5 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in Exhibit A (Cross-Border Data Transfers); (2) the terms of this DPA outside of Exhibit A; and (3) the Agreement. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

11.6 If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

EXHIBIT A

CROSS-BORDER DATA TRANSFERS

1. Definitions

(a) "**EU Standard Contractual Clauses (Controller-to-Processor)**" or **"EU SCCs (Controller-to-Processor)"** means the terms located at: http://www.confluent.io/dpa/eusccs-c2p

(b) "**EU Standard Contractual Clauses (Processor-to-Processor)**" or **"EU SCCs (Processor-to-Processor)"** means the terms located at: http://www.confluent.io/dpa/eusccs-p2p

(c) "**UK Addendum"** means the terms located at: http://www.confluent.io/dpa/uksccs-c2p

2. EU Standard Contractual Clauses

2.1 For transfers of Customer Personal Data from the EEA and/or Switzerland that are subject to Section 4.2 of the DPA:

(a) Where Customer is a controller of Customer Personal Data, the EU SCCs (Controller-to-Processor) will apply and are incorporated into the DPA by reference; and

(b) Where Customer is a processor of Customer Personal Data, the EU SCCs (Processor-to-Processor) will apply and are incorporated into the DPA by reference.

3. UK Addendum

3.1 For transfers of Customer Personal Data from the United Kingdom that are subject to Section 4.2 of the DPA, the UK Addendum will apply and are incorporated into the DPA by reference.

4. Alternative Data Export Solutions

4.1 Notwithstanding the foregoing, the parties agree that in the event Confluent adopts another alternative data export solution (as recognized under applicable Data Protection Laws), then the alternative data export solution shall apply instead of the Standard Contractual Clauses. In the event that the alternative data export solution is later determined to not constitute an adequate level of data protection under applicable Data Protection Laws, the Standard Contractual Clauses shall apply as the data export solution.