Confluent European Financial Services Regulatory Positions Statement

Introduction

Confluent acknowledges that Customer imposes operational standards and regulatory requirements onto certain of its suppliers. These mandated requirements are typically a result of regulatory requirements imposed or governed by the regulatory authorities including the European Banking Authority, Financial Conduct Authority, and the Prudential Regulation Authority (together the "**Regulators**") (the "**Regulations**").

This document is designed to assist Customer within the scope of the Regulations to consider the Guidelines on Outsourcing Arrangements (the "**EBA Outsourcing Guidelines**") and how they apply to Customer's utilization of Confluent's Cloud Service offering ("**Confluent Cloud Service**") pursuant to the Confluent Cloud Terms of Service ("**ToS**").

The focus is on Section 13 (Contractual Phase) of the EBA Outsourcing Guidelines. The EBA Outsourcing Guidelines replace the Committee of European Banking Supervisors (CEBS) guidelines on outsourcing that were issued in 2006. The EBA Outsourcing Guidelines also replace the EBA's Recommendations on Outsourcing to Cloud Service Providers published in 2018.

Below sets out Confluent's position in respect of Customer's compliance obligations with respect to the Regulations..

This document includes the following components:

1. Confluent's Compliance with minimum Control Obligations
2. A summary of Confluent's EBA Financial Services Addendum with Amazon
3. EBA Outsourcing Guidelines – Key Requirements

Confluent has also prepared an EBA Outsourcing Guidelines Cloud Offering Mapping document which addresses all requirements set out in Section 13 of the EBA Guidelines in turn. If you wish to receive a copy of this document, please contact your Confluent Cloud account representative.

Confluent's Compliance with Minimum Control Obligations

The Regulations impose a series of minimum control standards which are often captured by Customers in the form of policies or minimum control obligations. Below we set out Confluent's compliance standards and Policies in the context of the Confluent Cloud Service.

(a) Confluent's Compliance Standards:

a. Confluent's Compliance Standards

The Confluent Cloud Service is currently GDPR and CCPA ready, ISO 27001, PCI DSS, HIPPA, and SOC 1, SOC 2, and SOC 3 compliant. Further details of the compliance standards that Confluent Cloud offers can be found on the Confluent Trust and Security page which can be found at the following links:

https://www.confluent.io/trust-and-compliance/
https://docs.confluent.io/current/cloud/faq.html#what-compliance-standardsdoes-ccloud-offer.

b. Confluent has implemented an information security program which is designed to provide the same level of protection as evidenced by:

1. its security controls verified by its external auditors in its current System Organization Controls 1, Type 2 report and its current System Organization Controls 2, Type 2 Report (for availability/security and confidentiality);
2. its current certification under ISO 27001; and
3. its current compliance under PCI DSS.

Confluent conducts regular audits in respect of its Cloud offering (details are set out below).

Confluent shall provide a copy of its latest SOC 2 Report (last updated in March 2020) and its ISO 27001 Certificate to Customer on prior written request provided Customer is subject to adequate confidentiality obligations with Confluent.

(b) Privacy and Security:

Data Processing Addendum for Customers: The basis on which the parties process personal data is set out in Confluent's Data Processing Addendum for Customers (the "**DPA**"). Our DPA is tailored to Confluent's cloud offering and fulfills processing requirements under GDPR and CCPA. The DPA is incorporated into the Confluent Cloud Terms of Service and is located here.

Confluent Cloud Security Addendum: Confluent will use commercially reasonable administrative, physical, and technical safeguards designed to prevent unauthorized access, use or disclosure of Customer's content, as more fully described in the Confluent Cloud Security Addendum located here.

Privacy: Confluent has established and published a Privacy Policy which can be accessed on our corporate website here.

(c) Proper Business Conduct:

Confluent has taken adequate measures to ensure business, security, and privacy compliance and compliance with Confluent's internal policies, which contain substantially similar regulations to provide for integrity and proper business conduct, including but not limited to:

- Anti-Bribery Policy;
- Acceptable Use Policy;
- Information Security Policy;
- Modern Slavery Policy; and
- Privacy Policy;

(d) Business Continuity Program.

Confluent has a comprehensive Business Continuity Plan ("BCP") in place intended to help our organization respond to and recover from a business disruption. The BCP coordinates all of our business disruption preparation efforts, including impact identification/analysis, plan development, and testing. Key Elements of the BCP include:

- Incident Management/BCP Team and Structure;
- Business Impact Analysis & Threat Assessment;
- Data Back-Up & System Recovery Strategy;
- Mission Critical Functions, People, & Systems;
- Alternate Communications-Employee & Client Strategy;
- Alternate Physical Location-Work-site Strategy;
- Critical Vendor-Service Providers & Strategy; and
- Functional Recovery Procedures & Supporting Documentation.

A summary Overview of Confluent's Business Continuity and Disaster Recovery Program can be provided to customers on prior written request, provided an NDA is in place between Confluent and Customer.

(e) Modern Slavery Act Compliance:

Confluent declares to be opposed to child labor, human trafficking, and modern slavery, and upholds respect, ethics, and knowledge while dealing with Customer. Confluent complies with its Modern Slavery Statement which is made available here.

(f) Customer's Minimum Control Obligations

Please note that Confluent is unable to actively monitor for changes in individual customers' security controls requirements nor to adjust and implement potential changes imposed by Customer. Confluent complies with its own minimum standards and policies as further set out above.

(g) Confluent Compliance with Confluent Policies

Confluent agrees to comply with the Confluent Policies, notify Customer as soon as reasonably practicable on becoming aware of any material breaches which directly pertain to Customer and its Agreement with Confluent, and to maintain evidence of compliance with these policies.

Confluent agrees to make available such evidence to Customer upon request by Customer, provided there are appropriate confidentiality obligations in place between Customer and Confluent. Confluent keeps up to date and accurate records and documentation demonstrating your compliance with the Confluent Policies.

(h) Regulatory Changes

Confluent agrees that, if a change is required to the Agreement as a direct result of changes to the Regulations which mandate such a change, then Confluent will discuss in good faith and negotiate any required amendments to the Agreement mandated by the Regulations.

Customer shall have the limited right to terminate this Agreement and any applicable Order Form upon thirty (30) days' written notice to Confluent in the event that such termination is explicitly required by an applicable regulatory authority to which Customer is subject, provided (i) Customer shall provide Confluent with written evidence to demonstrate that such termination is required and (ii) Customer shall not be entitled to a refund of any Fees paid under the applicable Order Form.

Confluent EBA Financial Services Addendum with Amazon and Financial Services Addendum: United Kingdom with Amazon Web Services, Inc. ("AWS")

Confluent has entered into the following agreements with AWS which supplement the AWS Customer Agreement between Confluent and AWS governing Confluent's use of AWS' cloud offering to provide the Confluent Cloud Service:

I. EBA Financial Services Addendum;

II. Financial Services Addendum: United Kingdom,

together the "**Addenda**"

The Addenda apply where Confluent uses AWS Services to provide the Confluent Cloud Service which is subject to the regulatory oversight of the Regulator under applicable law provided Customer (or Customer's end client if applicable) is a regulated entity and is subject to applicable Regulation (as set out above). Confluent shall provide Customer with a copy of the Addenda on prior written request provided such information shall be subject to adequate obligations of confidentiality between the parties.

To the extent required by applicable Law, Regulation, Regulator, or appropriate Regulated Entity, Confluent confirms that it shall, to the extent permitted under the Addenda, assist Customer (and where applicable its clients) in exercising any of the rights available to it under the Addenda for the benefit of Customer.

EBA Outsourcing Guidelines – Key Requirements

1. Service Defaults

Confluent and Customer are each obligated to report possible or actual service defaults promptly. Confluent will promptly notify Customer in writing of the nature, extent, and impact of any possible or actual material service default of the Confluent Cloud Service which directly relates to Customer, or any other event that may or will prevent Confluent from providing the Confluent Cloud Service to Customer in accordance with the Agreement.

Confluent will where requested in writing also agree to assist Customer with the preparation and implementation of rectification plans required by the Customer and provide the reasonable assistance and information necessary for Confluent rectification of service defaults.

2. Investigation and Audit

- **Disciplinary Proceedings.** Upon written request by Customer, to the extent legally permissible, Confluent shall provide details to Customer if it becomes aware of any disciplinary proceedings or investigation by any Regulatory Authority against Confluent, Customer, or any of their respective officers or employees. Confluent does not have an active process to trigger notifications to Customer that Confluent becomes the subject of any such proceedings or investigation.
- Audit. Where required by Regulation to confirm the compliance of the Confluent Cloud Services and to fulfil Customer's obligations under applicable law as set out in the applicable Regulation, the parties shall in good faith:

  a. appoint a mutually agreed independent third party auditor;

  b. agree on the reasonable basis under which Confluent may permit Customer or any Regulator to access on provision of reasonable notice during normal business hours Confluent's premises, relevant records, and all documentation as may be required in order to complete any audit, review, inspection, site visit, or similar event ("Audit") (which may relate to an Audit of Confluent or Customer).

  c. Confluent shall also where required provide reasonable assistance to Customer (or where applicable its clients) in respect of any Audit which requires Confluent to exercise its rights with AWS under the Addenda.

  d. **Penetration and Vulnerability Testing.** Confluent conducts regular penetration and vulnerability testing of its systems which relate to the provision of the Confluent Cloud Service and agrees to provide Customer with remediation reports under NDA, which will show the original number of issues found and the number of issues remediated.

  e. If any Audit reveals that Confluent has materially failed to perform its obligations under the Agreement, then relevant provisions of the Agreement and point 2 above will apply and Confluent may be required to rectify these activities as Service Defaults.

  f. Customer shall comply with Confluent's reasonable directions in respect of relevant safety, security, or other reasonable policies when undertaking any Audit and Confluent's nominated representative may be present at the Audit.

  g. As set out above, Confluent also agrees to provide Customer with such reasonable co-operation and information as may be required by Customer to fulfil regulatory reporting requirements for Customer and where applicable its clients (for example, SOC 2 reports).

4. Termination and Exit Assistance

a. **Termination.** Customer's clients often require Customer to cooperate in a smooth handover of services to third parties or the Customer's client in cases of termination or expiry of the agreement between Customer and its client. Provided Customer continues to comply pay any fees applicable in respect of the Agreement and continues to comply with its terms, Confluent agrees to provide all reasonable information and assistance required by Customer, including but not limited to granting an extension of any licences required by Customer or its client for the period of time required to effect the handover of Customer's or client's data to another third party service provider.

b. **Exit Assistance Document.** Confluent has prepared an Exit Assistance strategy document to assist Customer in transferring Customer data from a Confluent Cloud Managed cluster to an on-premise Open Source version of Apache Kafka once Customer terminates the Confluent Cloud Services Agreement with Confluent (or an alternative solution of Customer choice).

   The goal of this Exit Assistance document is to effect the smooth handover of services to third parties or the clients of Customer in cases of termination or expiry of the agreement between Customer and Confluent. This document covers, inter alia:

   i. material elements of transfer of responsibilities;

   ii. how data and Content (as defined in the Agreement) of Client or Customer (as applicable) shall be transitioned from the Confluent Cloud Service to a third party or the Client, including details of the processes, documentation, data transfer; and

   iii. scope of any exit assistance services to be provided after notice to terminate has been given.

c. Customer and its clients, where applicable, must be able to readily access all Data related to the Confluent Cloud Service while the Agreement is in full force and effect. Confluent agrees to ensure that Customer can do so in accordance with the terms of the Agreement (including for the avoidance of doubt its service level agreement obligations).

d. To the extent the terms of open source licenses applicable to Open Source Software require Confluent to make an offer to provide source code or related information in connection with the Open Source Software, such offer is made to Customer.

e. Provided the Customer continues to comply with the terms of the Agreement, including Customer continuing to pay the applicable fees in respect of the Confluent Cloud Service, the Customer (on behalf of the Client) may specify that the exit assistance services to be provided by Confluent and Customer shall be entitled to extend the term of the Agreement between Confluent and Customer for a further maximum period of twelve (12) months for the transition to be completed. Confluent agrees to comply with any extended assistance period requested by the Customer.

5. Data and Intellectual Property Rights

a. Under the Agreement (specifically the Confluent Customer DPA), Customer may provide data (which may include 'Personal Data' as defined in the Agreement), drawings, and documents. in various formats which may belong to Customer; Customer's clients; or the end-customer of Customer's clients and which may or may not be the intellectual property of those parties ("Data"). Confluent may alternatively collect this Data its via a subcontractor if required by the Agreement. Confluent agrees to comply with the following statements:

   i. The Data and/or intellectual property belonging to (i) either party; (ii) a Customer's client; or (iii) a Customer's client's end-customer before the commencement date of the Agreement or not created in the course of or in connection with the Agreement shall remain the exclusive property of the entity or individual owning it;

ii. Any modifications made as part of the Subcontracted Services to Data or any intellectual property owned by Customer, its end-consumer, or its client's end-customer shall also be owned by the relevant entity or individual which owned the Data or intellectual property rights prior to modification;

iii. Confluent is an Open Source company and it accordingly incorporates open source software into the software or services Confluent provides, including the Confluent Cloud Service. Customer hereby acknowledges that Confluent Cloud is a cloud native, elastically scalable data streaming service based on Apache Kafka (Open Source).

iv. Except where set out in the Agreement, Confluent will not use the name or any marks of any of Customer's Clients without prior written consent from either Customer or the applicable Client.

6. Client Information

a. As set out in Section 5 above in relation to Data, any information provided by Customer or collected by Confluent in relation to the Services may not be owned by Confluent, but rather may be owned by its clients or their end-customers, and the clients shall be the Controller of such Data under the data protection legislation. Confluent agrees that it may be required to process Personal Data for which the Customer's clients and/or its end-customers are the Controllers in addition to Confluent Personal Data in the performance of the Services under the Agreement.

b. As set out in the DPA, Confluent's Security Addendum, and Confluent's SOC 2 documentation, Customer agrees that in order to provide the Services, Confluent may engage sub-processors to process Customer Data. Confluent maintains a list of its authorized sub-processors on its website here.

c. As set out in the Confluent DPA, Confluent may transfer and process Customer Data anywhere in the world where Confluent, its Affiliates or its Sub-processors 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. Except as set out above, Confluent shall not transfer any Data outside of the EEA without Customer's prior written consent which may be subject to certain conditions as set out in the DPA.

d. In addition, Confluent acknowledges and agrees that all information in any format of a confidential nature regarding the Clients, the Clients' end-customers (including the fact that they are our clients), shall be deemed to be confidential information of the parties for the purposes of the Agreement and shall fall within the definition of Confidential Information in the Agreement. The parties acknowledge and agree that Customer may share Confidential Information belonging to Confluent (other than pricing information – which shall only be shared with prior written consent) in accordance with the terms of the Agreement, and only confidential information which is relevant to the Agreement or the provision of the Confluent Cloud Service with the Client if required.

e. Where Customer notifies Confluent that an agreement between Customer and a Client expires or is terminated, Confluent will promptly following that notice and in accordance with the terms of the DPA return to Customer or permanently delete beyond recovery (as directed by Confluent) all Data relating to that Client, subject to Customer data retention requirements under applicable law.

7. Step-In Rights

Due to the requirements of Regulations which the Customer may be subject to, Customer or a client of Customer or its appointed agent may have certain step-in rights under its agreement with Customer in case of the occurrence of certain events which may impact the Agreement ("**Step-In Event**").

In a Step-In Event, Confluent agrees to continue to perform its obligations under the Agreement and shall not be entitled to terminate the Agreement by reason of the Step-In Event, provided the Customer or applicable client of the Customer continues at all times to comply with the terms of the Agreement (including continued payment of any applicable fees).

Customer acknowledges that Confluent is not able to differentiate between Customer or Customer's clients which are beneficiaries of the Confluent Cloud Service, and Confluent is dependent on Customer to mediate this requirement. Customer is responsible for designing and implementing its segmentation controls with respect to its clients and cooperating with Confluent throughout the Step-In Event.

Confluent acknowledges that a client of Customer may only 'step-in' in respect of the Confluent Cloud Service delivered to it personally and not in relation to any other client of Customer. Confluent shall therefore treat the client or its appointed agent as though it were Customer in relation to the provision of the Confluent Cloud Service to that client and cooperate with them and provide them with all information, assistance, access, and rights of use required for that particular client. However, Customer shall at all times ensure that information related to each client is stored separately and that information related to one particular client is not shared with Customer's other clients.

8. Confluent's Personnel Any Confluent personnel providing services to Customer in the United Kingdom are paid the London Living Wage or UK Living Wage (as applicable).

9. Assignment and Novation Confluent allows Customers to assign, novate, or transfer the Agreement as set out in the Confluent Cloud Terms of Service located here.

10. Sub-processors and Sub-Contractors.

Customer's clients may require that Confluent has transparency on the suppliers and subcontractors that Confluent utilizes in the delivery of the Services (as distinguished from the sub-processors referenced above). As set out above, Confluent provides a list of sub-processors as part of the data processor obligations in relation to sub processors here, but Confluent shall on written request provide a full list of any applicable subcontractor (that are separate from the sub-processors) that are material to Confluent's ability to deliver the Confluent Cloud Service to the Customer. This list can be provided on or within ten (10) business days of countersignature of this letter, and an updated list should be provided on an on-going basis as and when new subcontractors are appointed. As set out in the DPA, Confluent will provide Customer with reasonable prior notice on its website if it intends to make any changes to its Sub-processors. Customer may receive notifications of new Sub-processors and updates to existing Sub-Processors by subscribing for updates here.

11. Service Level Availability and Uptime

Customer can subscribe to updates regarding the Confluent Cloud Service Uptime Availability here.

12. General

Confluent will use reasonable efforts to notify Customers as soon as possible in the event of any material changes to our company structure or any change in ownership and/or control.