CONFLUENT CLOUD OFFERING MAPPING

EBA Outsourcing Guidelines

This document is intended to aid financial institutions within the scope of the European Banking Authority's mandate ("**institutions**") to consider the Guidelines on Outsourcing Arrangements (the "**EBA Outsourcing Guidelines**") in the context of Confluent's Cloud offering and the Confluent Cloud Terms of Service ("**ToS**"). The main focus is on Section 13, Contractual Phase of the EBA Outsourcing Guidelines. Below is commentary to support addressing the guidelines. If you have an existing Confluent Cloud agreement and would like to understand how this document applies to your agreement, please contact your Confluent account executive.

Note. The EBA Outsourcing Guidelines superseded the Committee of European Banking Supervisors (CEBS) guidelines on outsourcing (2016) and the EBA's Recommendations on Outsourcing to Cloud Service Providers (2018).

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
1	**13 Contractual phase**		
2	74 The rights and obligations of the institution, the payment institution and the service provider should be clearly allocated and set out in a written agreement	Confluent clearly allocates the rights and obligations in the ToS and ancillary information, as set out below.	N/A
3	75 The outsourcing agreement for critical or important functions should set out at least:		
4	a. a clear description of the outsourced function to be provided;	The Cloud services are clearly outlined and described here. Refer to the Cloud ToS which can be found here	Definitions
5	b. the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the institution or payment institution;	Refer to the ToS.	Term and Termination
6	c. the governing law of the agreement;	Refer to the Confluent Cloud ToS.	Governing Law
7	d. the parties' financial obligations;	Refer to your Confluent Cloud ToS.	Orders, Fees and Related
8	e. whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in Section 13.1 that the sub-outsourcing is subject to;	Please see commentary on Section 13.1 at (rows 21-35).	

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
9	f. the location(s) (i.e. regions or countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the institution or payment institution if the service provider proposes to change the location(s);	**Locations** Customer Content is stored in the available Cloud Service region(s) determined and selected by Customerin its configuration of the Cloud service.	Cloud Service Location, Obligations of the data exporter, Obligations of the data importer (Cloud Security Addendum and Data Processing Agreement)
10	g where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in Section 13.2;	Please see commentary on Section 13.2 (rows 36-40).	.
11	h. the right of the institution or payment institution to monitor the service provider's performance on an ongoing basis;	Customers can monitor Confluent's performance of the Services on an ongoing basis using Confluent Cloud Status link—https://status.confluent.cloud/. Customer can also subscribe for updates. Please see below regarding Cloud Service Level Agreement.	Service Level Agreement.
12	i. the agreed service levels, which should include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;	For more information regarding Service Level Agreement, please see: https://www.confluent.io/confluent-cloud-uptime-sla/	Uptime Service Level Agreement
13	j. the reporting obligations of the service provider to the institution or payment institution, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;	Confluent will provide information concerning incidents that materially impact Confluent's ability to perform the Services in accordance with the relevant SLAs. For more information, please see Confluent Cloud Status—https://status.confluent.cloud/	Uptime Service Level Agreement, Availability and Disaster Recovery
14	k. whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;	RConfluent maintains insurance coverage against a number of identified risks. This is not explicitly referenced in the ToS, but a summary of Confluent's insurance coverage can be made available to customers on a confidential basis following a written request.	Insurance
15	l. the requirements to implement and test business contingency plans;	Confluent has implemented a business continuity plan for the Services, review and test the plan at least annually, and ensure the plan remains current with industry standards.	Availability and Disaster Recovery.

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
16	m. provisions that ensure that the data that are owned by the institution or payment institution can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;	Customers retain all intellectual property rights in their data. Confluent will enable customers to access and export their data throughout the duration of the Agreement. Please see commentary on Section 13.4 (row 75). **N.B.** Neither of these commitments are disapplied in the event of Confluent's insolvency. Confluent does not have the right to terminate for Confluent's own insolvency but customers can elect to terminate. In the unlikely event of Confluent's insolvency, customers can refer to these commitments when dealing with the appointed insolvency practitioner.	Intellectual Property Ownership, Term and Termination.
17	n. the obligation of the service provider to cooperate with the competent authorities and resolution authorities of the institution or payment institution, including other persons appointed by them;	Confluent will cooperate with competent authorities and resolution authorities exercising their audit, information, and access rights.	Cooperation with supervisory authorities.
18	o. for institutions, a clear reference to the national resolution authority's powers, especially to Articles 68 and 71 of Directive 2014/59/EU (BRRD), and in particular a description of the 'substantive obligations' of the contract in the sense of Article 68 of that Directive;	To the extent that customers are institutions (as defined above) and thus are subject to the EBA Outsourcing Guidelines, Confluent will to the extent necessary include additional terms in Customer agreements providing that Confluent will continue to provide Services during resolution as required by the national resolution authority (BRRD), subject to Customer's continued compliance with the terms of the agreement (including continued payment of fees).	S9.4 DPA or 12.4 ToS
19	p the unrestricted right of institutions, payment institutions and competent authorities to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function, as specified in Section 13.3;	Please see commentary on Section 13.3 (rows 41-66).	
20	q termination rights, as specified in Section 13.4.;	Please see commentary on Section 13.4 (rows 67-77)..	
21	**13.1 Sub-outsourcing of critical or important functions**		
22	76. The outsourcing agreement should specify whether or not sub-outsourcing of critical or important functions, or material parts thereof, is permitted.	Confluent will provide customers with information about the organizations that assist with subprocessing arrangements in regards to Services. Please see commentary on Section 13.1 (row 26). 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/. Please see Section 4 of the Confluent Customer DPA.	Subprocessing

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
23	77. If sub-outsourcing of critical or important functions is permitted, institutions and payment institutions should determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e. a material part of the critical or important function) and, if so, record it in the register.	Confluent determines if a subprocessing function is a critical or important function. Confluent will provide all the information required in the subprocessing register for our subcontractors.	Subprocessing
24	78. If sub-outsourcing of critical or important functions is permitted, the written agreement should:		
25	a specify any types of activities that are excluded from sub-outsourcing;	Please see commentary on Section 13.1 (row 22).	
26	b. specify the conditions to be complied with in the case of sub-outsourcing;	Confluent will provide information concerning subprocessors, advance notice of changes to subprocessors, and give Customers the ability to terminate their Agreement over concerns about a new subprocessor.	Subprocessing
27	c. specify that the service provider is obliged to oversee those services that it has subcontracted to ensure that all contractual obligations between the service provider and the institution or payment institution are continuously met;	Confluent will oversee the performance of all subprocessor obligations and ensure subprocessors comply with respective Customer Agreements	Subprocessing, Disclosure of subprocessor agreements
28	d. require the service provider to obtain prior specific or general written authorisation from the institution or payment institution before sub-outsourcing data;	Confluent will comply with obligations under the GDPR regarding authorization for subprocessing.	Subprocessing
29	e. include an obligation of the service provider to inform the institution or payment institution of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of subcontractors and to the notification period; in particular, the notification period to be set should allow the outsourcing institution or payment institution at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect;	Customers will be informed of a subprocessor change in order to allow a risk assessment to be performed before the change comes into effect. Confluent will provide Customers with reasonable prior notice on its website if it intends to make any changes to its subprocessors.	Subprocessor Updates
30	f ensure, where appropriate, that the institution or payment institution has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;	Customers 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 an event, the parties will discuss such concerns in good faith with a view to achieving resolution. N.B., The European Banking Authority acknowledges that explicit consent is "overly burdensome" in the context of cloud outsourcing.	Subprocessor Updates

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
31	g ensure that the institution or payment institution has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the institution or payment institution or where the service provider sub-outsources without notifying the institution or payment institution.	Customers may suspend or terminate their respective Agreement if a resolution cannot be met.	Subprocessor Updates
32	79. Institutions and payment institutions should agree to sub-outsourcing only if the subcontractor undertakes to:		
33	a comply with all applicable laws, regulatory requirements and contractual obligations; and	Confluent contractually requires subprocessors to follow the standard required EU Data Protection Laws to facilitate Confluent's compliance with its obligations to its customers.	Subprocessor Obligations
34	b grant the institution, payment institution and competent authority the same contractual rights of access and audit as those granted by the service provider.	Subprocessing does not diminish Customers' ability to oversee the service or the competent authority's ability to supervise the Customer. Confluent will ensure subprocessors comply with the information, access, and audit rights provided to Customers and competent authorities.	Subprocessing
35	80 Institutions and payment institutions should ensure that the service provider appropriately oversees the sub-service providers, in line with the policy defined by the institution or payment institution. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to a material increase of risk, including where the conditions in paragraph 79 would not be met, the institution or payment institution should exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.	Please see commentary on Section 13.1 (row 27, 30-31).	
36	**13.2 Security of data and systems**		
37	81. Institutions and payment institutions should ensure that service providers, where relevant, comply with appropriate IT security standards.	Confluent hires accredited third parties to perform audits and to attest to various compliance standards and certifications annually including: • SSAE 18 SOC 1 Type II, SOC 2 Type II, and SOC 3 • Payment Card Industry Data Security Standards (PCI-DSS) – Confluent can support PCI data that is message-level encrypted by Customer • CSA Star Level 1 Attestation • ISO 27001 certification Further details can be found on the Confluent Trust and Security Compliance Page here.	Confluent Security Compliance, Certifications, and Third-party Attestations

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
38	82. Where relevant (e.g. in the context of cloud or other ICT outsourcing), institutions and payment institutions should define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.	Confluent implements layered security controls designed to protect and secure Confluent Cloud customer data. We incorporate multiple logical and physical security controls including access management, least privilege, strong authentication, logging and monitoring, vulnerability management, bug bounty programs, and many others. To learn more about our security controls for Confluent Cloud, please see: • Confluent Cloud Security Addendum • Confluent Cloud whitepaper • Confluent Cloud public documentation	Privacy and Security
39	83. In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, institutions and payment institutions should adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations.	Content is stored in the available Cloud Service region(s) specified by Customers in their setup and configuration of the Cloud service. Please see commentary on Section 13 (row 9).	Cloud Service Location
40	84. Without prejudice to the requirements under the Regulation (EU) 2016/679, institutions and payment institutions, when outsourcing (in particular to third countries), should take into account differences in national provisions regarding the protection of data. Institutions and payment institutions should ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the institution or payment institution (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).	Confluent implements layered security controls designed to protect and secure Confluent Cloud customer data. Please see commentary on Section 13.2 (rows 37-38). See our Confluent Customer Data Processing Addendum here for more information. Please also see the Confluent Cloud Trust and Compliance Page.	Privacy and Security, Confluent Cloud Customer Data Processing Addendum and Security Addendum
41	**13.3 Access, information and audit rights**		
42	85. Institutions and payment institutions should ensure within the written outsourcing arrangement that the internal audit function is able to review the outsourced function using a risk-based approach.	To the extent that customers are institutions (as defined above) and thus are subject to the EBA Outsourcing Guidelines, Confluent will to the extent necessary include additional terms in Customer agreements to ensure that the institution has the ability to review reasonable documentation relating to any outsourced function within our Services.	Obligations of data importer, Cooperation with supervisory authority

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
43	86. Regardless of the criticality or importance of the outsourced function, the written outsourcing arrangements between institutions and service providers should refer to the information gathering and investigatory powers of competent authorities and resolution authorities under Article 63(1)(a) of Directive 2014/59/EU and Article 65(3) of Directive 2013/36/EU with regard to service providers located in a Member State and should also ensure those rights with regard to service providers located in third countries.	Confluent accepts the information gathering and investigatory powers of competent authorities under the relevant EU Directives.	Cooperation with supervisory authority
44	87. With regard to the outsourcing of critical or important functions, institutions and payment institutions should ensure within the written outsourcing agreement that the service provider grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following:	To the extent that customers are institutions (as defined above) and thus are subject to the EBA Outsourcing Guidelines, Confluent will to the extent necessary include additional terms in Customer agreements to grant audit, access, and information rights to institutions, competent authorities (including resolution authorities), and both their appointees in respect of Confluent's premises.	Obligations of data importer, Cooperation with supervisory authority Confluent Cloud Security Addendum
45	a. full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and	Please see commentary on Section 13.3 (row 44).	
46	b. unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.	Please see commentary on Section 13.3 (row 44).	
47	88. For the outsourcing of functions that are not critical or important, institutions and payment institutions should ensure the access and audit rights as set out in paragraph 87 (a) and (b) and Section 13.3, on a risk-based approach, considering the nature of the outsourced function and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. Institutions and payment institutions should take into account that functions may become critical or important over time.	Please see commentary on Section 13.3 (row 42).	

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
48	89. Institutions and payment institutions should ensure that the outsourcing agreement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by them, competent authorities or third parties appointed by them to exercise these rights.	Please see commentary on Section 13.3 (row 42).	
49	90. Institutions and payment institutions should exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.	Institutions will determine the audit frequency and scope. Confluent can discuss further details with institutions.	Obligations of data importer, Cooperation with supervisory authority Confluent DPA Section 6
50	91. Without prejudice to their final responsibility regarding outsourcing arrangements, institutions and payment institutions may use:		
51	a. pooled audits organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider;	Confluent can discuss further details with institutions around pooled audits.	Obligations of data importer, Cooperation with supervisory authority
52	b. third-party certifications and third-party or internal audit reports, made available by the service provider.	Please see commentary on Section 13.2 (row 37).	
53	92. For the outsourcing of critical or important functions, institutions and payment institutions should assess whether third-party certifications and reports as referred to in paragraph 91(b) are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these reports over time.	This is an institution responsibility.	
54	93. Institutions and payment institutions should make use of the method referred to in paragraph 91(b) only if they:		
55	a. are satisfied with the audit plan for the outsourced function;	Please see commentary on Section 13.2 (row 37).	
56	b. ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the institution or payment institution and the compliance with relevant regulatory requirements;	Please see commentary on Section 13.2 (row 37).	
57	c. thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete;	Please see commentary on Section 13.2 (row 37).	

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
58	d. ensure that key systems and controls are covered in future versions of the certification or audit report;	Please see commentary on Section 13.2 (row 37).	
59	e. are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, reperformance/ verification of the evidence in the underlying audit file);	Please see commentary on Section 13.2 (row 37).	
60	f. are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;	Please see commentary on Section 13.2 (row 37).	
61	g. have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective; and	Institutions can request an expansion of the scope of the relevant certifications and audit reports.	Confluent Security Compliance, Certifications, and Third-party Attestations, Obligations of the data exporter
62	h. retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions.	Please see commentary on Section 13.3 (row 44).	
63	94. In line with the EBA Guidelines on ICT risk assessment under the SREP, institutions should, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes. Taking into account Title I, payment institutions should also have internal ICT control mechanisms, including ICT security control and mitigation measures.	Confluent contracts with professional penetration testing service providers at least twice per year for this service and we make a summary of the report available upon request. Additionally, we have implemented a bug bounty program and have invited a number of individuals to perform security testing against the services on a continual basis. In the event that institutions would like additional assurance, we are happy to discuss an off-cycle penetration test.	Vulnerability Management and Penetration Testing
64	95. Before a planned on-site visit, institutions, payment institutions, competent authorities and auditors or third parties acting on behalf of the institution, payment institution or competent authorities should provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.	Reasonable notice enables Confluent to deliver an effective audit to any institution (as defined above) which is subject to the EBA Outsourcing Guidelines. Notice also enables Confluent to plan the audit so that it does not create undue risk to a customer's environment or that of any other Confluent customer. Confluent recognizes that in some cases extended notice may not be possible. In these cases, we will work with the auditing party to address their needs.	Obligations of the data exporter Confluent DPA Section 6

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
65	96. When performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.	It is extremely important to Confluent that what we do with one customer should not put any other customers at risk. This applies when you perform an audit. It also applies when any other customer performs an audit. When an institution performs an audit, we will work with them to minimize the disruption to our other customers. Just as we will work with another auditing customer to minimize the disruption to the institution. In particular, we will be careful to comply with our security commitments at all times.	Obligations of the data exporter
66	97. Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the institution or payment institution should verify that whoever is performing the audit – whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf – has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the institution or payment institution reviewing third-party certifications or audits carried out by service providers.	This is an institution responsibility.	
67	**13.4 Termination rights**		
68	98. The outsourcing arrangement should expressly allow the possibility for the institution or payment institution to terminate the arrangement, in accordance with applicable law, including in the following situations:	IInstitutions may discontinue its use of Services at any time for any reason by following the process in the Confluent website interface to "Delete" an Institution's purchased Cloud Service.	Term and Termination
69	a. where the provider of the outsourced functions is in a breach of applicable law, regulations or contractual provisions;	Please see commentary on Section 13.4 (row 68).	
70	b. where impediments capable of altering the performance of the outsourced function are identified;	Please see commentary on Section 13.4 (row 68).	
71	c. where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors);	Please see commentary on Section 13.4 (row 68).	

	EBA Outsourcing Guidelines	Confluent Cloud Commentary	References for Confluent Cloud ToS
72	d. where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and	Please see commentary on Section 13.4 (row 68).	
73	e. where instructions are given by the institution's or payment institution's competent authority, e.g. in the case that the competent authority is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the institution or payment institution.	Please see commentary on Section 13.4 (row 68).	
74	99. The outsourcing arrangement should facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the institution or payment institution. To this end, the written outsourcing arrangement should:		
75	a. clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the institution or payment institution, including the treatment of data;	Customer is solely responsible for exporting Content from the Cloud Service prior to expiration or termination of this Agreement. Customer acknowledges that following termination it will have no further access to any Content. For assistance with exporting Content, please submit a Support ticket or reach out to your Account Executive. Please see the Confluent Cloud Exit Assistance Document on our Confluent Cloud Trust and Compliance Page	Term and Termination, Data Export (Confluent Customer Data Processing Addendum and Confluent Cloud Security Addendum)
76	b. set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions; and	Please see commentary on Section 13.4 (row 75).	
77	c. include an obligation of the service provider to support the institution or payment institution in the orderly transfer of the function in the event of the termination of the outsourcing agreement.	Please see commentary on Section 13.4 (row 68).	

Last updated: September 2020