CONFLUENT

DATA TRANSFERS IN CONNECTION TO CONFLUENT CLOUD

FREQUENTLY ASKED QUESTIONS

Confluent is closely monitoring the developments regarding the invalidation of the Privacy Shield by the European Court of Justice ("ECJ"), including the new set of Standard Contractual Clauses adopted by the European Commission. Our customers can remain reassured that they can continue to use Confluent Cloud in compliance with European, Swiss and UK privacy laws.

This is a living-document which is made available to assist in answering questions raised by our customers when evaluating Confluent's cloud services, which is subject to the terms and conditions of the Confluent Cloud Terms of Services and to the Data Processing Addendum ("DPA"), unless different contractual terms have been agreed.

1. What did the ECJ rule in the judgment of "*Schrems II*"?

The main takeaway from the decision is that the EU-US Privacy Shield Framework was invalidated by the ECJ and is no longer considered a valid mechanism for transfers of personal data originating from the European Economic Area ("EEA") to the United States, due mainly to concerns over US surveillance law. The EU-US Privacy Shield Framework was one of the ways that organizations could lawfully transfer personal data from the European Economic Area, Switzerland and the United Kingdom (Europe) to the United States under EU privacy laws. At the same time, the ECJ concluded that the Standard Contractual Clauses (the "SCCs") issued by the European Commission for the transfer of personal data to data processors established outside of the EEA remain valid. However, the ECJ also declared that before transferring personal data from the EEA to a non-EEA country, organizations relying on the SCCs must ensure that the personal data transferred will be protected to a standard which is "essentially equivalent" with EU data protection. This involves assessing the relevant aspects of the legal system of the recipient country that may impinge on the effectiveness of the protections under the SCCs.

On June 4th, 2021, following the Schrems II decision, the European Commission has adopted a new set of SCCs, taking into account the GDPR and including new protections for the management of government access requests. Per the European Commission's guidance adopting the new SCCs, agreements made with the "old" SCCs continue to remain valid until the end of 2022. Agreements executed as of September 27th, 2021 should contain the new SCCs.

2. How does this decision affect Confluent?

Confluent does not employ the Privacy Shield Framework as a means to receive transfers of personal data in the US from our customers in the EEA. We currently use the SCCs in all our DPAs with our subprocessors. We will continue to operate in this fashion in accordance with applicable laws. We are committed to protecting the personal data that we process on behalf of our customers, and we take our obligations under privacy laws seriously. We will continue to monitor developments and guidance issued by data protection authorities to comply with privacy laws.

We take responsibility for our subprocessors, including any potential delta that may exist between the terms in our DPA with our customers and the terms in our DPAs with our subprocessors, as per the terms outlined in our DPA. Several of our subprocessors previously used the EU-US Privacy Shield Framework as their assurance of an adequate level of protection for the transfer of data. Our subprocessors have since updated their DPAs to include the SCCs and we are currently working on implementing the new SCCs and any additional safeguards where necessary with all our subprocessors.

3. Do we need to update our DPA to include the SCCs?

We will incorporate the new SCCs into our agreements in accordance with the transition periods specified by the European Commission. This means that starting on September 27th, 2021, our new contracts will contain the new SCCs. Per the European Commission's guidance, agreements made with the "old" SCCs will remain valid until December 27th, 2022, and Confluent will work with its existing customers to implement the new SCCs quickly and in any event, before that deadline.

4. Can access to data and information transmitted to the Cloud Service by Customer be limited to certain territories or countries?

If one of our customers has a specific requirement to keep message data produced by a topic and transmitted through Kafka ("Customer Data") residing within the EEA, such customer can select via the Cloud Service a data center location in the EEA. Upon selection of a data center in the EEA, that Customer Data will be stored and physically located in a data center based in the EEA. Regardless of the location of a data center, Confluent will at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of applicable data protection laws.

5. Is Confluent an "*electronic communication service provider*" as defined in 50 U.S.C. § 1881(b)(4), that could render Confluent directly subject to 50 U.S.C. § 1881a (= FISA 702)?

The Schrems II decision focussed on concerns that US government agencies can, in certain circumstances, compel US-based service providers to disclose EEA personal data in a way that is not "essentially equivalent" with EEA data protection rules.

Section 702 of the U.S. Foreign Intelligence Surveillance Act (as amended) ("FISA") authorises intelligence agencies to collect foreign intelligence information about non-US persons located outside of the US and, subject to authorisation from the Foreign Intelligence Surveillance Court, can compel "electronic communications service providers" to disclose certain data they process for this purpose.

The ECJ ruled under Schrems II that FISA does not respect the minimum safeguards resulting from the principle of proportionality under EU law and cannot be regarded as limited to what is strictly necessary. Most, if not all, US-based providers of cloud-based technology solutions may fall within the scope of an "electronic communications service provider". Confluent is no different in this respect. Rest assured, we take the privacy, security and confidentiality of our customers very seriously.

To date, Confluent has not received any request from intelligence agencies pursuant to FISA.

6. Does Confluent cooperate with US authorities conducting surveillance of communications under E.O. 12.333?

The E.O. 12.333 is an executive order that authorises intelligence agencies to conduct surveillance outside of the US, and is primarily used to target traffic flowing through internet backbone providers that carry Internet traffic (i.e. telecommunications carriers). As such, Confluent is not directly subject to E.O. 12.333. In addition, and unlike FISA 702, E.O. 12.333 does not authorize the US government to require any company to disclose data, though E.O. 12.333 may be used by intelligence activities to access data overseas without the involvement of the company in question. Confluent does not cooperate in any respect with US authorities conducting surveillance under E.O. 12.3333 and has not been made aware of any direct access to our customers' data under Executive Order 12333.

7. How does Confluent handle potential access to Customer Data from third parties, in particular public and administrative authorities?

Both the new SCCs and the EDPB Recommendations indicate that organizations should assess whether laws like Section 702 of FISA apply practically to their day-to-day business operations, and not just from a pure theoretical perspective. This includes identifying whether the data importer has received any requests from government authorities or is aware of any direct access. Confluent has not received a government request for Customer Data as of the date of the publication of this document. In any event, Confluent is committed to the privacy and security of all Customer Data and has implemented steps to ensure that it will not provide, or disclose access to, Customer Data to third parties unless strictly required to do so by law.

Confluent understands that our customers should control their data. In the event third parties, in particular public and administrative authorities ("Third-Parties"), make a lawful request to Confluent for Customer Data, Confluent will attempt to redirect such a request so that the applicable customer can respond to it directly.

If Confluent is not able to redirect such request to the customer, or if Confluent knows or gains a reasonably grounded suspicion that Third-Parties have obtained or will soon obtain access to Customer Data which we hold that is subject to processing by Confluent, and such access by the Third-Parties is neither subject to a data processing agreement, nor covered by an instruction from such customer, Confluent will inform the customer of such Third-Parties' access as soon as reasonably practicable, to the extent legally permitted.

If Confluent receives a Third-Party request for Customer Data, Confluent will review each government request on a case-by-case basis and will only comply if and to the extent the request is lawful. Confluent will aim to disclose only the minimum amount of Customer Data necessary to satisfy the Third-Party's request. For purposes of keeping such disclosure by Confluent as restrict as possible, Customer 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.

In addition, Confluent will review the legality of the Third-Party's request and will challenge it if, after careful assessment, it concludes that there are reasonable grounds to consider that such request is unlawful under applicable laws.

8. For every processing operation that Confluent has control over, has Confluent implemented appropriate technical and organisational measures (see Article 32 GDPR) to prevent mass and indiscriminate processing of personal data by or on behalf of authorities in transit (such as under the "Upstream" program in the US)?

Yes, Confluent is committed to maintaining robust security measures to protect Customer Data. For instance, Confluent Cloud encrypts data in-transit and at rest using appropriate encryption standards. For the purposes of ensuring good data governance and data confidentiality, customers should securely encrypt their data prior to sending any data to Confluent. In addition, Confluent maintains several security certifications including ISO 27001 and SOC 2 type II. For further information about the technical and organisational measures implemented by Confluent, please check our Confluent Cloud Security Addendum and Confluent Cloud Security Controls.

9. Where do I get more information on the privacy, compliance & security controls adopted by Confluent?

Confluent invites you to visit our Trust & Security webpage to get more information about security controls, compliance reports and certifications acquired by Confluent. Confluent is committed to being transparent about the data we handle and how we handle it. Confluent's Privacy Policy can be found here.