# Calix Data Processing Agreement (DPA)
# Frequently Asked Questions*

May 15, 2023

The Calix Online Universal Data Processing Agreement posted on the Calix public-facing website, addresses customer concerns about Calix data processing on behalf of customers for most jurisdictions. As set forth in the DPA, where customers require separately signed standard contractual clauses to address cross-border transfers, Calix will work with customer to put these in place, at customer's request.

1. Has Calix performed a Transfer Impact Assessment (TIA) for customer representative PD (Representative PD) and customer subscriber PD (Subscriber PD) (collectively Representative PD and Subscriber PD are Customer PD) transferred to Calix?

   Yes. Calix has performed a transfer impact assessment for Representative PD and Subscriber PD that details the circumstances of the transfers, assesses the level of protection afforded to the transferred PD by the relevant laws and practices of the destination country, and documents the technical and organizational measures in place in relation to the transfer, including any supplementary measures and whether any additional procedural steps are required. Additional information regarding these Calix Data Processing Agreement FAQs is available to customer representatives in the MyCalix Trust Center (requires log-in).

2. What transfer mechanism does Calix rely upon?

   For external transfers of Customer PD, Calix relies on:
   a. the appropriate European Union Standard Contractual Clauses issued by the European Commission in June 2021 (Commission Decision 2021/914 of June 2021) (SCCs) (for transfers subject to the EU GDPR);
   b. the International Data Transfer Agreement (version A1.0) issued by the United Kingdom Information Commissioner's Office on 2 February 2022 (the "UK International Data Transfer Agreement") (for transfers subject to the UK GDPR) (for transfers between Calix and its customers); and
   c. the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner (the "UK International Data Transfer Addendum") (for transfers subject to the UK GDPR) (for transfers between Calix and its sub-processors).

   For internal transfers of Customer PD within the Calix Group, Calix and its affiliates have entered into an Intra Group Data Transfer Agreement which incorporates the SCCs and the UK International Data Transfer Addendum to the SCCs.

3. Transfers of Subscriber PD.

**Calix is not providing legal advice. Customer to seek legal advice from Customer's attorneys.*

a. *Does Calix process special categories of Subscriber PD?*

No. Calix does not process special categories of Subscriber PD.

b. *Where does Calix store Subscriber PD?*

Calix stores Subscriber PD, for customers whose subscribers are located outside the United States, in the Calix International Cloud hosted by Amazon Web Services in Quebec, Canada.

c. *Does Calix use sub-processors for Subscriber PD?*

Calix sub-processors are listed in the Calix Trust Center. Calix provides notice of new sub-processors at least 20 days prior to transferring any Subscriber PD to the sub-processor and notifies its customers of new sub-processors both by posting the new sub-processor in the Calix Trust Center and by including any new sub-processors in its quarterly release notifications to customers.

4. Transfers of Representative PD

a. *Where does Calix store and process Representative PD*? Calix stores and processes Representative PD in Salesforce, hosted within the United States and accessed by Calix employees in the countries where Calix operates.

b. *How does Calix protect Representative PD*? Calix has entered a written contract with Salesforce as processor, that includes Salesforce's standard DPA that incorporates the SCCs. Calix protects Representative PD with the measures set forth in detail in Calix's technical and organizational measures for security and the supplementary measures that Calix has implemented.

5. Has Calix implemented any supplementary measures?

All Calix employees sign a confidentiality agreement prior to joining Calix. In addition, Calix's Code of Conduct and Business Ethics requires all employees to protect confidential information that includes Customer PD. Calix requires all technicians who have standing access to Subscriber PD to take additional training on their obligation to maintain confidentiality of Subscriber PD and will audit technician access until the restrictions are automated. Any discrepancies will trigger corrective action.

Although Calix's TIA has determined that no supplementary measures are required, Calix is implementing the following two supplemental measures to further protect Representative PD and Subscriber PD.

**1. Approval process for Accessing Subscriber PD in the Calix Cloud in Canada.**

**Calix is not providing legal advice. Customer to seek legal advice from Customer's attorneys.*

a. Prior Approval Process. Before any Calix technicians (employees or contractors) outside the EEA, UK or Canada, may access Subscriber PD within the Calix Cloud, those technicians will have to follow a formal procedure that requires both internal (Calix management) approval, and external (Customer) written approval. For Calix Professional Services, this consent (for the duration of the statement of work) will be included in the statement of work. For trouble reports requiring assistance by the Calix Technical Assistance Center (TAC), the request for Customer consent will be presented during the creation of the trouble report and will be limited to the duration of the trouble report. If Customer does not consent to TAC technician access in the United States, Costa Rica, or India, that trouble report will be routed to a technician located in Poland (which could cause a delay in resolving the trouble ticket).

b. Access is time-limited. Only a small group of Calix Cloud operations and engineering technicians have standing access to Subscriber databases. Otherwise, permitted access to Subscriber PD will be limited to the length of time needed to perform the work on behalf of the Customer.

**2. Requests for Customer Data.**

a. If Calix receives a valid and binding order ("**Request**") from any governmental body ("**Requesting Party**") for disclosure of Customer PD, Calix will redirect the Requesting Party to the Customer.

b. If compelled to disclose Customer PD to a Requesting Party, Calix will:

i. promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy, if Calix is legally permitted to do so. If Calix is prohibited from notifying Customer about the Request, Calix will use reasonable and lawful efforts to obtain a waiver of the prohibition, to allow Calix to communicate as much information to Customer as soon as possible; and

ii. challenge any inappropriate Request if there are legal grounds to do so; and

c. If, after exhausting the steps in described in section 2.b, above, Calix remains compelled to disclose Customer PD to a Requesting Party, Calix will disclose the minimum amount of Customer PD necessary to satisfy the Request.

6. Does Calix recommend any language to address transfers of Subscriber PD?

Yes, for countries other than the United States and Canada.

a. Customers operating in the Australian state of New South Wales or in Switzerland will want to obtain consent from subscribers specifically to disclose subscriber data to Calix, Inc. and its sub-processors.
b. To address cross-border transfers in Customer's privacy notice, for countries outside the United States (other than Canada where Calix subscriber data is stored), Calix recommends* Customer

**Calix is not providing legal advice. Customer to seek legal advice from Customer's attorneys.*

include disclosures to Customer's subscribers in this respect. Disclosures should communicate the following:

- That personal data includes sampled network traffic data.
- That personal data about users of the residential gateway, including sampled network flow data, will be stored and processed in countries outside of the European Economic Area (EEA) or the United Kingdom (UK).
- That technicians outside EEA or UK may access personal data for the purposes of installing, configuring and troubleshooting services.
- If applicable, that you have implemented additional safeguards such as standard contractual clauses adopted by the European Commission or the UK Government to ensure the information is adequately protected.

**Calix is not providing legal advice. Customer to seek legal advice from Customer's attorneys.*