Cisco Technical Assistance (TAC) Service Delivery

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco TAC.

1. Overview Cisco TAC Delivery Capabilities

Cisco's Support Services Technical Assistance Center (TAC) is a global organization that provides around-the-clock, award-winning technical support services online and over the phone. TAC offers customer support for all Cisco products/services using a global follow-the-sun support model. Our TAC teams support thousands of service requests every day, as well as supply best-in-class hardware support, repair, and replacement from one of our 1,100 depots.

As part of our TAC services support process, service requesters may be required to provide certain personal data. These data are limited to business contact details provided by the requester and used for the purposes of providing the support required.

Customer Case Attachment Data (including text, audio, video or image files), which are either provided to Cisco by a customer in connection with the customer's use of Cisco products or services, or data developed by Cisco at the specific request of a customer, is subject to the following security controls:

- Authentication
- Access control
- Login/activity logging and monitoring
- Data masking
- Data encryption, both at rest and in transit
- Transport and storage for physical data

2. Personal Data Processing

The tables below list the personal data used by Cisco TAC to carry out the services and describe why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
TAC Support Information	• Name • Email Address • Phone Number of the Employee Appointed to Open the Service Request • Authentication Information (exclusive of passwords) • Information About the Condition of the System • Registry Data About Software Installations and Hardware Configurations • Error-Tracking File	We use TAC Support Information to: • Provide remote access support • Review quality of the support service • Perform analysis of the service solution
Customer Case Attachment	Cisco TAC does not intentionally collect or process personal data via Customer Case Attachments. We instruct customers to provide the least amount of personal data possible. However, unsolicited personal data may be contained in the files provided by customers. For illustrative purposes only, the list below includes the types of data that may be processed for Customer Case Attachments for the purpose of providing support: • Device Configuration (e.g., running config and startup config, SNMP Strings (masked); Interface description • Command Line Interface (CLI) (i.e., Show Commands, such as Show Version) • Product Identification Numbers • Serial Numbers • Host Names • Sysdescription (has device location) • IP Addresses • Operating System (OS) Feature Sets • OS Software Versions • Hardware Versions • Installed Memory • Installed Flash • Boot Versions • Chassis Series • Slot IDs • Card Types • Card Families • Firmware Versions • MAC Address • SNMP MIBs (ACLs, CDP)	We use Customer Case Attachments to: • Provide remote access support • Perform analysis of the service solution

3. Cross-Border Transfers

Cisco TAC leverages a Customer Relationship Management (CRM) case management system to deliver our services and capture TAC Support Information. This system is a customized instance on the SalesForce.com (SFDC) platform known as Support Case Manager (SCM) and utilizes a numerical Service Request (SR) case assignment process. Cisco TAC SR case details and associated case notes within Cisco's CRM system are stored at the Salesforce.com (SFDC) data center, which physically resides in Washington DC, USA.

Customer Case Attachments (including detailed system logs, etc.) uploaded by customers are housed in a single data repository hosted by Amazon Web Services (AWS -US East, North Virginia Region). The AWS instance, known internally as CX Files, maintains robust data security and governance controls, including authentication, authorization, role-based access controls, encryption in transit and at rest, login logging and monitoring, and activity logging and monitoring. CX Files is wholly maintained by the Cisco Customer Care IT / Crypto team and the storage location is not shared with any other AWS customers, nor with any other team within Cisco.

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

4. Access Control

Personal Data Category	Who has access	Purpose of the access
Cisco TAC Support Information	Customer/Partner	Work with Cisco to resolve their support case
	Cisco Support Personnel	Work with Customer to resolve their support case. Access based on functional responsibility.
Customer Case Attachments*	Customer/Partner	Work with Cisco to resolve their support case
	Cisco Support Personnel	Work with Customer to resolve their support case. Access based on functional responsibility.

**As stated above, Customer Case Attachment Data (including text, audio, video or image files), which are either provided to Cisco by a customer in connection with the customer's use of Cisco products or services, and/or data developed by Cisco at the specific request of a customer, are subject to the above-mentioned security controls.*

5. Data Portability

Cisco TAC allows customers to export both their Service Request (SR) case data and Case Attachments related to cases for which they have been granted access. Partners who have been enabled by the customer and assigned to a specific contract, may also view, upload and/or download data on the customer's behalf.

6. Data Deletion & Retention

Cisco TAC Service Request (SR) case data that has been in CLOSED status for 10 years + 1 day or more is automatically purged from our key repositories on a nightly basis. Case data is all data captured as part of the service request process, including all Case Notes and Customer Case Attachments.

Customers may request deletion of personal data retained by Cisco TAC by submitting a request via privacy portal. If you require deletion of any other data outside of the timelines stated above, please contact your sales representative. In each instance, Cisco will endeavor to delete the requested data from its systems at the earliest possible time and will do so unless the data is required to be retained by Cisco.

Cisco retains data to ensure efficient support in case of recurring issues and to comply with Cisco audit policies related to business records of services provided to Customers (i.e., legitimate business purposes).

7. Personal Data Security

Cisco Services has received ISO 27001:2013 (Information Security) re-certification from TUV (a copy of the new certificate is available here).

Personal Data processed by	Type of Encryption
TAC Support Information	Encrypted in transit, and at rest after reaching Cisco.
Customer Case Attachments	Encrypted in transit, and at rest after reaching Cisco.

8. Third Party Service Providers (Sub-processors)

Cisco engages sub-processors that provide the same level of data protection and information security that you can expect from Cisco. A current list of contracted sub-processors for the Cisco TAC Delivery service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Aricent (India) **Estarta (Jordan)** **IBM (Bulgaria)** **Sykes (Costa Rica and Colombia)** **Concentrix (USA)**	TAC Support Information Customer Case Attachments	Delivery support on behalf of Cisco Systems, Inc.	• Gurgaon, India • Amman, Jordan • Sofia, Bulgaria • San Jose, Costa Rica and Barranquilla, Columbia • California, USA
Salesforce.com (USA)	Customer Relationship Management (CRM)	Hosting/Storage	• Washington, DC, USA
Amazon Web Services (USA)	Customer Case Attachments	Hosting/Storage	• US East, Northern Virginia

9. Information Security Incident Management

Breach and Incident Notification Processes
The Data Protection & Privacy team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

10. Certifications and Compliance with Privacy Laws

The Security and Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. Cisco and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation (GDPR) and other privacy laws around the world.

Cisco leverages the following privacy transfer mechanisms related to the lawful use of data across jurisdictions:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

In addition to complying with our stringent internal standards, Cisco also continually maintains third-party validations to demonstrate our commitment to information security. Cisco Customer Experience (CX) has received the following certifications:

- ISO 27001

11. General Information and GDPR FAQ

For more general information related to Cisco's Technical Services, please visit the Technical Services section Cisco.com.

For more general information and FAQs related to Cisco's Security Compliance Program and Cisco's GDPR readiness please visit The Cisco Trust Center.

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.