Cisco Technical Assistance (TAC) Service Delivery

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

Cisco will process personal data from customers in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data processed by Cisco TAC in order to provide its functionality.

1. Overview

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 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

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

2. Personal Data Processing

The table below lists the personal data processed by Cisco TAC to provide its services and describes why the data is processed.

Personal Data Category	Type 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) • Work organization and responsibilities • Current employer name	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:	We use Customer Case Attachments to: • Provide remote access support • Perform analysis of the service solution

	• 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)	

3. Data Center Locations

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 data repository hosted by Amazon Web Services (AWS - US East Region, Northern Virginia), and replicated for resiliency to another AWS data repository (AWS - US West Region - Oregon). 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.

Infrastructure Provide Locations
Amazon Web Services (AWS) - US East (Northern Virginia) Region
Amazon Web Services (AWS) - US West (Oregon) Region
SalesForce.com (SFDC) – Washington D.C., USA

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses
- EU-U.S. Data Privacy Framework and the U.K. Extension to the EU-U.S. Data Privacy Framework
- Swiss-U.S. Data Privacy Framework

5. Access Control

The table below lists the personal data used by Cisco TAC to carry out the service, who can access that data, and why.

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.

6. 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.

7. Data Retention

The table below lists the personal data used by Cisco TAC the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
TAC Support Information and Customer Case Attachments	10 Years + 1 day	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).

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Personal Data Category	Security controls and measures
TAC Support Information	• Data encryption, in transit • Authentication • Access control • Login/activity logging and monitoring • Data masking
Customer Case Attachments	• Data encryption, both at rest and in transit • Authentication • Access control • Login/activity logging and monitoring

	• Data masking

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Salesforce.com (USA)	TAC Support information	Hosting/Storage	Washington, D.C., USA

10. 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), the Advanced Security Initiatives Group (ASIG), and Cisco Legal.

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.

11. Certifications and Compliance with Privacy Requirements

The Security & 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. The service is built with security and privacy in mind and is designed so that it can be used by Cisco Customers in a manner consistent with global security and privacy requirements.

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

- ISO/IEC 27001:2013

12. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, data portability and / or deletion of the personal data processed by the Service as well as object to processing.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirect to their employer for a response.

Requests can be made by submitting a request via:

1) the Cisco Privacy Request form
2) by postal mail:

Chief Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES		
Americas Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES	**APJC Privacy Officer** Cisco Systems, Inc. Bldg 80, Lvl 25, Mapletree Biz City, 80 Pasir Panjang Road, Singapore, 117372 SINGAPORE	**EMEA Privacy Officer** Cisco Systems, Inc. Haarlerbergweg 13-19, 1101 CH Amsterdam-Zuidoost NETHERLANDS

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco's US-based third-party dispute resolution provider. Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoriteit Persoonsgegevens.

13. General Information

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

This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement. To the extent this document differs from the Cisco Online Privacy Statement, this document will take precedence. If there is a difference in translated, non-English versions of this document, the U.S.-English version will take precedence.

Cisco frequently evolves and updates its offerings. Cisco Privacy Data Sheets are subject to change, and are reviewed and updated on an annual basis, or as reasonably needed to reflect a material change in the processing of Personal Data. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.

To receive email notifications of updates to the Privacy Data Sheet, click the "Subscribe" link in the upper right corner of the Trust Portal.