Cisco SD-WAN Cloud

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco SD-WAN Cloud.

Cisco SD-WAN Cloud is a cloud-based enterprise networking solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Cisco SD-WAN Cloud 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 SD-WAN Cloud in order to provide its functionality.

1. Overview of SD-WAN Capabilities

The Cisco SD-WAN solution is a software defined wide area network (SD-WAN) solution that allows customers to (i) orchestrate network policies and manage their network from a centralized console, and (ii) segregate the management, control, and orchestration layers from the device transport layer. This enables network policy, control, and orchestration to be performed across the entire network of compatible Cisco routers (physical or virtual) in a secure and extensible manner.

SD-WAN customer data is stored based on how the solution is deployed. As a result, Cisco only stores customer data from SD-WAN when a Customer deploys SD-WAN in a Cisco-Hosted Cloud or uses a SaaS feature of the solution such as VNalytics or the Cisco SD-WAN Self Service Portal. If a Customer deploys SD-WAN on a private or third party cloud, SD-WAN data is not accessible to Cisco unless the Customer uses the aforementioned SaaS features or specifically opts to share such data with Cisco, for example, for troubleshooting or support purposes.

Other than the personal data described in this Privacy Data Sheet, the data collected by the Cisco SD-WAN Cloud consists of network traffic metadata and non-personal Systems Information (i.e., configuration data, logs, device health, application usage data, edge usage data, product usage data). Network traffic information remains at the routing transport layer and is not sent to Cisco’s Cloud.

2. Personal Data Processing

The table below lists the personal data processed by Cisco SD-WAN Cloud to provide its services and describes why the data is processed.

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Types of Personal Data</th>
<th>Purpose of Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator Log-In Information</td>
<td>• Sys Admin Username, Email, and Password or • Cisco Single Sign-on (i.e., SmartAccount), pursuant to which any personal data is processed through the Smart Account service. (For more information, see <a href="https://www.cisco.com/c/dam/en_us/about/ding_business/trust-center/docs/cisco-smart-software-license-privacy-data-sheet.pdf">https://www.cisco.com/c/dam/en_us/about/ding_business/trust-center/docs/cisco-smart-software-license-privacy-data-sheet.pdf</a>)</td>
<td>• Provision of the service (i.e., authenticate authorized users of the solution), audit logs for vManage (SD-WAN management platform), troubleshooting, and support. Note: Except where required by law or enabled by Customer, this data is stored locally and not accessible by Cisco. • Audit logs for vManage for incident response for certified versions of the SD-WAN solution (e.g., FedRAMP, SOC2), if Customer elects to use those versions. • Audit logs for Cisco SD-WAN Self Service Portal (SSP) whereby Customer may view audit logs detailing users who have modified Customer overlay via SSP.</td>
</tr>
</tbody>
</table>
3. Data Center Locations
Cisco SD-WAN Cloud leverages third party cloud hosting providers to provide services globally.

The following table shows where these data centers are located, for reference purposes only. Please note that specific data center locations may change over time and this Privacy Data Sheet will be updated to reflect those changes if they occur.

<table>
<thead>
<tr>
<th>Data Center Locations</th>
<th>Data Centers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia, Germany, United States</td>
<td>• For the vAnalytics feature, customers choose one of the following region-specific data centers appropriate for their environment.</td>
</tr>
<tr>
<td>Australia, Brazil, Germany, India, Ireland, Japan, Singapore, United States</td>
<td>• For the Cisco-Hosted SD-WAN Cloud, customers choose one of the following region-specific data centers appropriate for their environment.</td>
</tr>
</tbody>
</table>

4. Cross-Border Data Transfers Mechanisms
Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- Binding Corporate Rules
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5. Access Control
The table below lists the personal data used by Cisco SD-WAN Cloud to carry out the service, who can access that data, and why.

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Who has access</th>
<th>Purpose of the access</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator Log-In Information</td>
<td>Cisco</td>
<td>• Upon customer providing access, provide troubleshooting and technical support for the service&lt;br&gt;• Provision of the service&lt;br&gt;• Communicate service and product updates to customer</td>
</tr>
<tr>
<td></td>
<td>Customer</td>
<td>• Use the service (i.e., authenticate authorized users of the solution)</td>
</tr>
<tr>
<td>End User Device Identifiers</td>
<td>Cisco</td>
<td>• Providing the optional vAnalytics service (i.e., analytics and insights to network and application performance)</td>
</tr>
<tr>
<td></td>
<td>Customer</td>
<td>• Use of the optional vAnalytics service (i.e., analytics and insights to network and application performance)</td>
</tr>
</tbody>
</table>
6. Data Portability
Customer (or a managed service provider (MSP) in the MSP context) is able to download and transfer audit logs and network statistic data.

7. Data Deletion & Retention
The table below lists the personal data used by Cisco SD-WAN Cloud, the length of time that data needs to be retained, and why we retain it.

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Retention Period</th>
<th>Reason for Retention</th>
</tr>
</thead>
</table>
| System Administrator Log-In Information   | • During customer’s active Cisco SD-WAN subscription, plus 3 years thereafter | • Customer’s use of the service  
• Provide troubleshooting and technical support for the service  
• Insights and analytics                                                              |
| End User Device Identifiers               | • During customer’s active Cisco SD-WAN subscription, plus 1 year thereafter | • Customer’s use of the services  
• Insights and analytics                                                                |

Note: Any data retained longer than stated above is anonymized and used for product improvement purposes only.

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.

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Security controls and measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator Log-in Information</td>
<td>Encrypted at rest with AES-256 algorithm. Encrypted in transit with TLS 1.2.</td>
</tr>
<tr>
<td>End User Device Identifiers</td>
<td>Encrypted at rest with AES-256 algorithm. Encrypted in transit with TLS 1.2.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Sub-processor</th>
<th>Personal Data</th>
<th>Service Type</th>
<th>Location of Data Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>• Sys Admin Username and Password</td>
<td>Hosting infrastructure services</td>
<td>Customers choose the region-specific data center appropriate for their environment (Australia, Brazil, Germany, India, Ireland, Japan, Singapore, USA).</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>• Sys Admin Username and Password</td>
<td>Hosting infrastructure services</td>
<td>Customers choose the region-specific data center appropriate for their environment (Australia, Brazil, Germany, India, Ireland, Japan, Singapore, USA).</td>
</tr>
</tbody>
</table>
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), 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.

11. 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. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

- **EU-US Privacy Shield Framework**
- **Swiss-US Privacy Shield Framework**

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security.

12. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will ask for 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
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.

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.