Cisco SD-WAN

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

1. Overview of Cisco SD-WAN Capabilities

Cisco SD-WAN is a software defined wide area network solution that allows users to (i) orchestrate network policies and manage networks from a centralized console, and (ii) segregate the management, control, and orchestration layers from the routing transport layer so that network policy, control, and orchestration can be performed across the entire network of router devices in a secure and extensible manner.

Other than the personal data described in this Privacy Data Sheet, all data collected by Cisco SD-WAN consists of network traffic data and non-personal telemetry data (i.e., configuration data, logs, device health). Users’ network traffic remains at the routing transport layer and is not sent to the cloud. See link for more information https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/index.html.

2. Personal Data Processing

Users may sign into the user interface for the solution through the following methods:

- Non-Cisco Single Sign-on (i.e., Radius or Tacacs), pursuant to which any personal data is processed through the user’s designated third party SSO operator.

- Cisco Single Sign-on (i.e., SmartAccount), pursuant to which any personal data is processed through the Smart Account service. (For more information, see https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-smart-software-license-privacy-data-sheet.pdf.)

- Username and password to access and use Cisco SD-WAN. Usernames and passwords are retained in the customer’s SD-WAN account, hosted by Cisco. Cisco has access to and processes such personal data (unless the username and password are used by a group, which is not advised). This use is more particularly described below.

IP addresses and other unique identifiers are not captured by Cisco SD-WAN during the sign-on process.

3. Cross-Border Transfers

Cisco SD-WAN leverages third party cloud services. The following table shows where these data centers are located, for reference purposes only. (Note that data center locations may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.)

| Destination Country | Customers choose the region-specific data center appropriate for their environment (Australia, Brazil, Germany, India, Ireland, Japan, Singapore, USA). |

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
- EU Standard Contractual Clauses
4. Access Control

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Who has access</th>
<th>Purpose of the access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data provided by user in its username</td>
<td>Product Support Team (Cisco TAC, Cisco business unit escalation team, Cisco business unit engineering team)</td>
<td>Support for customer initiated issues.</td>
</tr>
<tr>
<td></td>
<td>Customers</td>
<td>To access and manage their own data and use of Cisco SD-WAN.</td>
</tr>
<tr>
<td>Personal data provided by user in its password</td>
<td>Customers</td>
<td>To access and manage their own data and use of Cisco SD-WAN.</td>
</tr>
</tbody>
</table>

5. Data Deletion & Retention

**Retention**

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Retention Period</th>
<th>Reason for Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The period in which a customer has an active Cisco SD-WAN subscription, plus 60 days after the expiration or termination of the subscription.</td>
<td>To authenticate the user.</td>
</tr>
<tr>
<td>Password</td>
<td>The period in which a customer has an active Cisco SD-WAN subscription, plus 60 days after the expiration or termination of the subscription.</td>
<td>To authenticate the user.</td>
</tr>
</tbody>
</table>

**Deletion**

Customers have the ability to delete their personal data through their account settings; Cisco does not have the ability to take this action on customer's behalf while the customer has an active Cisco SD-WAN subscription. However, 60 days after expiration or termination of a customer's Cisco SD-WAN subscription, Cisco automatically deletes the customer's entire Cisco SD-WAN controller, including personal data stored therein.

6. Personal Data Security

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Type of Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Database in which personal data is stored is encrypted; personal data is not transmitted out of the database.</td>
</tr>
<tr>
<td>Password</td>
<td>Database in which personal data is stored is encrypted; personal data is not transmitted out of the database.</td>
</tr>
</tbody>
</table>

7. Third Party Service Providers (Sub-processors)

Cisco partners with service providers who contract to provide the same level of data protection and information security that you can expect from Cisco.

<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>Username and Password</td>
<td>Host</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>Username and Password</td>
<td>Host</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>
8. 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.

9. 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 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](#)
- [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 Services has received the following certifications:

- [ISO 27001](#)

10. General Information and GDPR FAQ

For more general information and FAQs related to Cisco’s Security Compliance Program and Cisco’s GDPR readiness please visit [The Cisco Trust Center](#).