Cisco Intersight

This privacy data sheet describes the processing of personal data (or personally identifiable information) by Cisco Intersight™.

1. Overview of Cisco Intersight capabilities

Cisco Intersight is a management platform delivered as a service with embedded analytics for Cisco® and third-party IT infrastructure. This platform offers an intelligent level of management that enables IT organizations to analyze, simplify, and automate their environments in more advanced ways than prior generations of tools. Cisco Intersight has deep integration with Cisco UCS®, HyperFlex™, APIC, DCNM, Services Engine, Pure Storage FlashArray and VMware vCenter systems, allowing for remote deployment, configuration, and ongoing maintenance. The core capabilities of Cisco Intersight are described here: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_intersight_offer_description.pdf.

Cisco Intersight processes certain personal data of its users. The following sections describe which personal data Cisco processes to deliver its services, the location of that data, and how it is secured in accordance with privacy principles, laws, and regulations.

2. Personal data processing

The table below lists the personal data used by Cisco Intersight to carry out its services and describes why we process that data.

Personal data category*	Types of personal data	Purpose of processing
Registration information	• Cisco.com ID • First name • Last name • Email address • User ID	We use registration information to: • Perform account creation and product activation • Log in to the service** • Provide customer support • Authenticate and authorize access to the service • Provide updates on the status and availability of the service • Provide opt-In marketing/sales contact
Customer feedback, when provided by an individual ("Participant") using Intersight	• Participant name • Participant email • Indication whether the Participant is open to follow-up on their feedback	We use feedback from Participants to: • Improve the product • Provide customer support • Identify and resolve product bugs • Follow up with Participants on their feedback

*If the customer integrates other applications, additional personal data may be processed.

**If the customer utilizes a single sign-on or identity provider service, the personal data processed for logging into the account may differ.

The data in the table below may potentially be connected to an individual's account and therefore be personal data, but for the most part is expected to relate only to servers, storage systems, and network management systems in the data center or edge locations, and not be connected to an individual's device.

Data category	Types of data	Purpose of processing
Inventory and configuration data	• Configuration data ◦ Hardware inventory ◦ Firmware inventory ◦ User labels ◦ IP addresses ◦ Server configuration inventory ◦ Workflow configuration ◦ Licensing data ◦ Configuration policies ◦ API keys, OAuth2 tokens ◦ OS software image meta-data • Server service contract ◦ Billing address ◦ Shipping address ◦ Purchase order number ◦ Contract coverage ◦ Warranty information	We use inventory and configuration information to: • Provide the service and associated features • Support contracts for the service • Provide technical support • Detect common vulnerabilities and exposures on the servers claimed by the service
Host and usage information	• Session information ◦ Session ID ◦ Creation timestamp ◦ Update timestamp • Host provisioning data ◦ OS version ◦ IP addresses ◦ Driver version ◦ Server version • Monitoring data ◦ Session date and time ◦ Screens viewed ◦ Actions taken ◦ UI analytics ◦ Alarms ◦ System health data ◦ Audit records ◦ Time-series statistics ◦ Tech support bundles	We use host and usage information to: • Understand how the service is used • Diagnose technical issues • Conduct statistical and technical analysis to improve the technical performance of the service

Intersight users also have the option to upload identification tags, either directly via a file or via orchestrator integrations (UCSD, etc.), and can use Intersight APIs to integrate Intersight with Cisco and/or third-party applications. It is possible, but not recommended, that an administrator / Intersight user could add personal data within the tags (for example, the name of the individual associated with an asset, IP address, or process). With use of Intersight applications, APIs, or other integrations to come, Intersight may incorporate and process additional personally identifiable information.

Technical support assistance

If a customer reaches out to Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from the Intersight service. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data.

3. Cross-border transfers

When a customer purchases a subscription of Cisco Intersight, the customer's information (both the data relating to the customer's employees who are in contact with Cisco to procure and administer the product on behalf of the customer, and the data processed through Cisco's delivery of its services to customers) is processed and stored in the United States. A cross-border transfer occurs if a customer's account and contact information is transmitted to Cisco from outside the United States and if the personal data described in Section 2 is transmitted to Cisco Intersight from outside of the United States. Cisco Intersight is hosted in the United States.

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

Personal data category	Who has access	Purpose of the access
Registration information	Cisco Intersight support team	Support of the service and product improvement
	Customer	Based on the policy of an individual customer for the use of personal data
Inventory and configuration data	Limited group of Cisco engineers, support staff, and licensing operations	Validating license entitlement and providing general product support and operations
	Customer	Product administration and operation
Host and usage information	Limited group of Cisco engineers and support staff	Diagnose technical issues and conducting statistical and technical analysis to improve the technical performance of the service

5. Data deletion and retention

Personal data category	Retention period	Reason for retention
Registration information	The data is purged from the service upon customer request at termination of service	Creating an account, product enablement, product usage notifications, training, and support
Inventory and configuration data	• As long as the Intersight account is active • Configuration data is retained for 30 days after deletion of the Intersight account	• Product features and recommendations • Support for recreating customer accounts
Host and usage information	• As long as the Intersight account is active • Host and usage data is retained for 30 days after deletion of the Intersight account	• Conducting statistical and technical analysis to improve the technical performance of the service

6. Personal data security

Cisco Intersight adopts technical and organizational security measures as required by law and by industry standards to protect your personal data from unauthorized access, use, or disclosure. We only partner with service providers who contract to provide the same level of information security that you can expect from Cisco. Below is additional information about our encryption architecture.

Personal data category	Type of encryption
Registration information	Encrypted in transit and at rest
Inventory and configuration data	Encrypted in transit and at rest in block and object data stores
Host and usage information	Encrypted in transit and at rest in block and object data stores

7. Third-party service providers (sub-processors)

Cisco Intersight does not use sub-processors to process personal data.

8. Information security incident management

Breach and incident notification processes

The Data Protection and Privacy team within Cisco's Security and 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

Cisco's 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. See section 3, "Cross-border transfers," above.

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

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.

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.

11. Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

12. Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-741197-01 03/20