Cisco Intersight® Platform

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by the Cisco Intersight® Platform ("Intersight").

Intersight provides system management capabilities that allow IT organizations to analyze, simplify, and automate their data center and public cloud environments through an intuitive user portal.

Cisco will process personal data from Intersight 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 Intersight in order to provide its functionality.

1. Overview

Intersight provides customers 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 the prior generations of tools. Intersight integrates with Cisco UCS®, HyperFlex®, and select third-party solutions, allowing for remote deployment, configuration, and ongoing maintenance.
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.

This privacy data sheet applies to the Intersight platform, inclusive of Infrastructure Services, as more fully described in the Cisco Intersight Platform Offer Description. Addendum One to this privacy data sheet describes the processing of personal data (or personal identifiable information) when using Intersight Virtual Appliance, which can be operated in two modes - Connected Virtual Appliance (CVA) or Private Virtual Appliance (PVA).

Note, Intersight may also be integrated with third-party products and services. Cisco is not responsible for customer data once it leaves Intersight for a non-Cisco product or service. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party.

2. Personal Data Processing

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

Personal Data Category[1]	Type of Personal Data	Purpose of Processing
Account information	• Cisco.com ID • First and last name • Email address • User ID	We use account information to: • Perform account creation and product activation • Log in to the service[2] • Cross-domain identity management[3] • 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 • Enable trials of Intersight functionality
User credentials	• System generated key, tied to an individual user of the service.	User credentials are used to authenticate and authorize access to the service.
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

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, switches, and network management systems in the data center or edge locations and not be connected to an individual's device.

Data Category[1]	Types of Data	Purpose of Processing

Inventory and configuration data	• Configuration data
	  ○ Hardware inventory
	  ○ Firmware inventory
	  ○ User labels
	  ○ IP addresses
	  ○ Domain names
	  ○ Server configuration inventory
	  ○ Workflow configuration
	  ○ Workflow logs
	  ○ Licensing data
	  ○ Configuration policies
	  ○ API keys, OAuth2 tokens
	  ○ OS software image meta-data
	  ○ Events and alarms
	• Server service contract
	  ○ Billing and 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
		• Understand how the service is used

[1] If customer integrates other applications, additional personal data may be processed.

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

[3] If the customer enables the use of SCIM (System for Cross-domain Identity Management), the personal data related to SCIM is processed in the United States.

Host and usage information	• Host provisioning data
	  ○ OS version
	  ○ IP addresses
	  ○ Driver version
	  ○ Server version
	  ○ Device identifiers
	• 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 and usability of the service
		• Help optimize the client experience

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. Cisco TAC, as a global service, may need to move customer tech support data to a different region for troubleshooting and analysis. The Intersight default setting for tech support is to allow collection of incident information. To turn this off, see Disabling Tech Support Bundle Collection. Only an account administrator can modify the setting.

3. Data Center Locations
Customers must select a geographic region (United States or European Union) during Intersight account creation. The account region determines where Cisco stores data from managed devices (also referred to as claimed targets), even if those devices are located outside of the region. However, Cisco stores Inventory and configuration data (see the table in section 2 above) from all unclaimed devices in the United States. Once a customer who selected the European Union region claims a device for management by Intersight, Cisco purges that device's data from the United States data center (Inventory and configuration data is then processed in the EU data center). Cisco retains purged data in a backup system for up to 30 days. Customer 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 stored in the account region. Encrypted Customer feedback may be stored in Cisco data centers globally. As footnote 3 in section 2 above notes, if a customer enables SCIM, Cisco processes that Account information in the United States (even for customers who select the European Union).

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

Cisco also offers an on-premises software Virtual Appliance as an alternative to the Intersight SaaS platform, allowing implementation of most Intersight functionality within a customer's data center. See Addendum One to this Privacy Data Sheet for information regarding the Intersight Virtual Appliance processing of data.

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

Personal Data Category	Who has Access	Purpose of the Access
Account 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
User credentials	Customer	• Authenticate and authorize access to the service
Customer feedback, when provided by an individual ("Participant") using Intersight	Limited group of Cisco engineers and support staff	• Respond to Participant communications. Diagnose technical issues and conducting statistical and technical analysis to improve the usability and technical performance of the service
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 usability and technical performance of the service

6. Data Portability

Data portability requirements are not applicable to Intersight.

7. Data Deletion and Retention

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

Type of Personal Data	Retention Period	Reason for Retention
Account information and User Credentials	• As long as the Intersight account is active Account information and User credential data are retained for up to 30 days after deletion of the Intersight account	• Creating an account, product enablement, product usage notifications, training, and support. Maintaining a record of customer licensing
Inventory and configuration data	• As long as the Intersight account is active Inventory and Configuration data are retained for up to 30 days after deletion of the Intersight account	• Product features and recommendations • Support the customer in recreating accounts
Customer feedback, when provided by an individual ("Participant") using Intersight	• As long as the Intersight account is active Customer feedback data is retained for up to 30 days after deletion of the Intersight account	• Product features and recommendations • Provide customer support • Identify and resolve product bugs • Follow up with Participants on their feedback
Host and usage information	• Except for session information, as long as the Intersight account is active, Host and usage information is retained for up to 30 days after deletion of the Intersight account	Conducting statistical and technical analysis to improve the technical performance of the service
Session information stored within FullStory*	• Session information shared with FullStory is retained for up to two years	• Product features and recommendations • Support improvements to the product, including bug identification and resolution
*** No customer data is shared with or processed by FullStory for customers who have selected the EU geographic region.**		

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.

Below is additional information about our encryption architecture.

Personal Data Category	Security Controls and Measures
Account information	Encrypted in transit and at rest
User Credentials	Encrypted in transit and at rest
Customer feedback, when provided by an individual ("Participant") using Intersight	Encrypted in transit and at rest in block and object data stores
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

9. Sub-processors

Intersight engages service providers that act as sub-processors of personal data and contract to provide the same level of data protection and information security provided to you by Cisco. The current list of sub-processors is set out below. Sub-processors may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.

Sub-processor	Personal Data*	Service Type	Location of Data Center
Amazon Web Services	All data categories in section 2 above, which is encrypted in transit and in rest.	Infrastructure Provider	United States, Germany
Sentry.io**	Account and host and usage information, which is encrypted in transit and in rest.	Error tracking and support	United States
FullStory**	Account and host and usage Information, which is encrypted in transit and in rest.	Support	United States

*** Cisco controls encryption keys.**
**** Neither Sentry.io nor FullStory act as sub-processors for customers who select the EU geographic region.**

10. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security 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 Requirements

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.

Further, in addition to complying with our stringent internal standards, Cisco also continually maintains third-party validations to demonstrate our commitment to information security. Intersight has received the following certifications:

- ISO/IEC 27001:2013
- ISO/IEC 27017:2015
- SOC 2 Type 2, SOC 3
- CSA CSTAR Level 1
- FIPS 140-2 Compliance

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 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 redirected to their employer for a response. Requests can be made by submitting a request via:

1) Cisco's Privacy Request form
2) by postal mail:

<table>
<tr><td colspan="3">Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td>EMEA Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost NETHERLANDS</td></tr>
</table>

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 Autoritiet 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.

Addendum One: Intersight Virtual Appliance

This Addendum describes the processing of personal data (or personal identifiable information) when using the Intersight Virtual Appliance, which can be operated in two modes, as a Connected Virtual Appliance (or "CVA") or as a Private Virtual Appliance (or "PVA").

This Addendum One to the Cisco Intersight Platform Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Intersight Virtual Appliance Overview

Cisco Intersight Virtual Appliance delivers the management features of Intersight in an easy to deploy VMware OVA, Microsoft Hyper-V Server VM, and KVM hypervisor on Linux, that allows you to control what system details leave your premises. The virtual appliance form factor enables additional data locality, security, or compliance needs that are not completely met by intersight.com.

CVA delivers the management features of Intersight while allowing you to control what system details leave your premises. CVA deployment requires a connection back to Cisco and Intersight services for automatic updates and access to services for full functionality.

PVA delivers the management features of Intersight and allows you to ensure that no system details leave your premises as PVA operates with no connection back to Cisco. The PVA does require creation of an appliance account on https://intersight.com. For both PVA and CVA, the appliance account processes some data as described below and in the Cisco Intersight Platform Privacy Data Sheet above. The CVA may also make use of an appliance account if a user opts for manual updates.

2. Personal Data Processing and the Virtual Appliance

If a customer uses the CVA it functions in a connected mode and requires connectivity to hosted Intersight services. The table below lists the personal data processed by Intersight in creating an appliance account and, for CVA automatic updates and access to services on Intersight.com, and describes why the data is processed.

Personal Data Category[4]	Type of Personal Data	Purpose of Processing
Account information	• Cisco.com ID • First name and Last name • Email address • User ID • User credentials	We use account information to: • Perform SaaS account creation and product activation to claim appliance into the SaaS account • Log in to the service[5] • Cross-domain identity management[6] • Authenticate and authorize access to the SaaS account • Provide customer support

[4] If customer integrates other applications, additional personal data may be processed.

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

[6] If customer enables the use of SCIM (System for Cross-domain Identity Management), the personal data related to SCIM is processed in the United States.

Personal Data Category[4]	Type of Personal Data	Purpose of Processing
Customer feedback, when provided by an individual ("Participant") using Intersight[7]	• 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

Upon downloading update bundles for both the PVA and the CVA, Intersight will collect the Account information used for the purposes described in the table above. Intersight also maintains audit logs that will record the download.

The data in the table below may be shared by CVA deployments and may be potentially 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[4]	Types of Data	Purpose of Processing
Inventory and configuration data	Appliance data ○ The appliance ID (Serial Number) ○ The IP address of the appliance ○ The hostname of the appliance ○ The device connector version and public key on the appliance Endpoint Data ○ Serial number and PID (to support Connected TAC) ○ UCS Domain ID ○ Platform Type ○ The endpoint target type - Cisco UCS Fabric Interconnect, Integrated Management Controller, Cisco HyperFlex System[7] ○ Firmware versions[7] ○ The IP address[7] ○ Domain names[7] ○ The hostname[7] ○ Workflow logs[7] ○ Device connector version and public key[7]	We use the information about the endpoint target to: • Provide Technical Support • Provide Proactive RMA • Device connector version, public key and other data marked with a # below are used to upgrade devices that may have an unsupported device connector version.
Host and usage information	• Monitoring data ○ Alarms[7] ○ Appliance health data ○ Appliance CPU usage ○ Appliance Memory usage ○ Appliance Disk usage ○ Service statistics • Tech support bundles[7]	We use host and usage information to: • Diagnose technical issues • Provide Technical Support • Provide Proactive RMA

3. Data Center Locations and the Virtual Appliances

When a user of a Virtual Appliance accesses Intersight, the customer's information is stored as described in Section 3 of the Intersight Privacy Data Sheet above.

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)

[7] The data is collected only in specific cases when enabled by customers or needed to provide technical support.

- 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 for the Virtual Appliance

Personal data collected by Intersight described above in Section 2 of this Addendum One are used and accessed as set forth in the table appearing in Section 5 of the body of the Intersight Privacy Data Sheet above.

6. Data Portability

Data portability requirements are not applicable to the Intersight Virtual Appliance.

7. Data Deletion and Retention

Personal data described above in Section 2 of this Addendum One that is collected by Intersight are retained and used as described in the table below.

Type of Personal Data	Retention Period	Reason for Retention
Account information and User credentials	• As long as the Intersight account is active Account information and User credentials data is retained for up to 30 days after deletion of the Intersight account	Creating an account, product enablement, product usage notifications, training, and support. Maintaining a record of customer licensing
Inventory and configuration data **(CVA only)**	• As long as the Intersight account is active Inventory and configuration data is retained for up to 30 days after deletion of the Intersight account	• Product features and recommendations
Customer feedback, when provided by an individual ("Participant") using Intersight	• As long as the Intersight account is active Customer feedback data is retained for up to 30 days after deletion of the Intersight account	• Product features and recommendations • Provide customer support • Identify and resolve product bugs • Follow up with Participants on their feedback
Host and usage information **(CVA only)**	• As long as the Intersight account is active, Host and usage information is retained for up to 30 days after deletion of the Intersight account	Conducting statistical and technical analysis to improve the technical performance of the service

8. Personal Data Security for Virtual Appliance Data on Intersight.com

Cisco has implemented appropriate technical and organizational measures for personal data collected by Intersight described above in Section 2 of this Addendum One as described in the table appearing in Section 8 of the body of the Intersight Privacy Data Sheet above.

9. Sub-processors for Virtual Appliance Data on Intersight.com

Intersight Virtual Appliance engages service providers that act as sub-processors of personal data and contract to provide the same level of data protection and information security provided to you by Cisco. The current list of sub-processors is set out below. Sub-processors may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	All data categories from section 2 above, which is encrypted in transit and in rest.*	Infrastructure Provider	United States, Germany
*** Cisco controls encryption keys.**			

10. Information Security Incident Management

Breach and Incident Notification Processes
Breach and Incident Notification Processes are the same as those for Intersight, as described in the body of this Privacy Data Sheet above.

11. Certifications and Compliance with Privacy Requirements

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

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

12. Exercising Data Subject Rights in Connection with the Virtual Appliance

Virtual Appliance users whose personal data is collected by Intersight as described in Section 2 above have the right to request access, rectification, suspension of processing, or deletion of that personal data.

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 redirected to their employer for a response.

Requests can be made by submitting a request via:

1) Cisco's Privacy Request form
2) by postal mail:

<table>
<tr><td colspan="3">Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td>EMEA Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost NETHERLANDS</td></tr>
</table>

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.