Cisco Spaces

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

Cisco Spaces is a cloud-based SaaS offering solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data by Cisco Spaces 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 Spaces in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

Cisco Spaces (formerly Cisco DNA Spaces) uses MAC address-based location data to gain insights into the behavior of end user devices and network- connected objects in any place with wireless connectivity, allowing customers to make informed business decisions, optimize operations, and improve experiences. Cisco Spaces brings together multiple location-based services capabilities in a unified platform and user interface (the "Service").

For a detailed overview of Cisco Spaces, please visit the Cisco Spaces website here:
https://www.cisco.com/c/en_in/solutions/enterprise-networks/dna-spaces/index.html

2. Personal Data Processing

The table below lists the personal data processed by the "See", "Act" and "Extend" Tiers of Cisco Spaces to provide its services and describes why the data is processed.

See Tier

Personal Data Category	Type of Personal Data	Purpose of Processing
System Administrator Log-in Information	• First name and last name • E-mail address	• Use the Service (i.e., authenticate authorized users of the solution)
End User Information	• MAC Address • Employee Username[1] • Userid of End User[2] • IP Address	• Use the Service (i.e., End User behavior tracking (such as visit duration, approximate location), device behavior tracking (such as status, temperature))

Act Tier

Personal Data Category	Type of Personal Data	Purpose of Processing
System Administrator Log-in Information	• First name and last name • E-mail address	• Use the Service (i.e., authenticate authorized users of the solution)
End User Information	• MAC Address (collected by default) • Employee Username[1] • Userid of End User[2] • IP Address • Customer has option to enable via captive portal collection and	• Use the Service (i.e., enable captive portal authentication, End User behavior tracking, (such as visit duration, approximate location) device behavior tracking (such as status, temperature)) • Deliver personalized content to End-users • Utilize analytics on the part of Customer

	processing of additional types of Personal Data, such as: ○ First name and last name ○ Gender ○ E-mail address ○ Phone number ○ Title ○ Zip code ○ Business tag (Customer assigned labels/categories for End-users) ○ CPF (Brazil identity number) ○ Age range ○ Social media network ID ○ In addition to other categories of available ○ Location data that may be designated by Customer	

Extend Tier

Extend Tier enables Customer to designate types of location data generated under DNA Spaces for transmission and use by third party services vendors ("Partner") with whom Customer has contracted with for other services. Customer must consent to the use of the location data by each applicable Partner through the DNA Spaces App Center portal ("App Center"), which introduces Customer and Partners, and enables transmission of location data through the Cisco Firehose API ("API"). Use of Customer Personal Data accessed by Partner through the API will be subject to privacy terms entered into by Partner and Customer. Cisco does not access or process the location data including Personal Data through the App Center function itself.

Personal Data Category	Type of Personal Data	Purpose of Processing
System Administrator Log-in Information	• First name and last name • E-mail address	• Use the Service (i.e., authenticate authorized users of the solution)
End User Information	• MAC Address (collected by default) • Employee Username[1] • Userid of End User[2] • IP Address • Customer has option to enable via captive portal collection and processing of additional types of Personal Data, such as: ○ First name and last name ○ Gender ○ E-mail address ○ Phone number ○ Title ○ Zip code ○ Business tag (Customer assigned labels/categories for End-users) ○ CPF (Brazil identity number) ○ Age range ○ Social media network ID	• Use the Service (i.e., enable captive portal authentication, End User behavior tracking, (such as visit duration, approximate location) device behavior tracking (such as status, temperature)) • Deliver personalized content to End-users • Utilize analytics on the part of Customer

[1] Basically, it's the identity that we get from the Wireless controllers during 802.1x authentication. In some instances, only when the Customer enables it, the employee usernames of End Users are collected and assigned a pseudonymized unique user identifier. This data is then used to derive some of the metrics in the far-right column in the above table.

[2] Basically, it's the identity that we get from the Wireless controllers during 802.1x authentication. In some instances, only when the Customer enables it, userids of End Users are collected. For some configurations, the userids may be hashed (anonymized) if required. This is used to map End User to the applicable device.

	○ In addition to other categories of available location data that may be designated by Customer	

Spaces Connector On-premise solution
Cisco Spaces collects and uses the personal data as part of its operation such as MAC address and Username through Connector on-prem solution from the customer locations. Cisco Spaces Connector supports optional hashing of Username and/or MAC address on the connector. For IP addresses, there is an option to skip sending IP addresses to Cisco Spaces.

Spaces Connector has gone through CSDL Self-Assessment Certification process (Cisco Secure Development Lifecycle) which supports in meeting Cisco's security requirements in order to make the solution and Cisco more secure. CSDL takes care of all industry best standard controls for On-prem applications.

As part of CSDL, Spaces Connector uses Cisco Secured Linux and Cisco Cloud9 team that provides hardened base images. The Cisco Secured Linux includes OS Hardening, Kernel Hardening, protection against malware insertion and execution.

Cisco Secured Linux is a Security & Trust Organization (STO) program that provides a means for product teams to quickly and efficiently incorporate foundational security into their products and achieve security requirement compliance.

Smart Workspaces
The Smart Workspaces solutions, including the Digital Signage app, do not require personal data by default. Interactions with the web application are anonymous. Cisco Spaces does not know any details about the individual that interacts with the application. Telemetry, such as people counts and environmental sensors, are all anonymous and computed on partner devices outside of the Cisco Spaces platform.

Optionally, a customer can integrate Office 365 or Google Calendar either directly through the Cisco Spaces platform or through Webex Hybrid Calendar in Control Hub. Cisco Spaces collects meeting schedules, meeting name, room name, the host's name, and the host's email address.

Rich Maps
The underlying architecture of the Smart Workspaces solutions is the Location Hierarchy (a hierarchy of nodes of buildings, floors, etc.) and Rich Maps, which provide sub-floor level metadata that can be used for context throughtout Cisco Spaces.

The process to create Rich Maps involves a customer uploading their facility CAD files (i.e. architectural and furniture drawings), which Cisco Spaces uses Artificial Intelligence (AI) and Machine Learning (ML) techniques to extract objects and IDs from the files. Cisco Spaces processes CAD files into Rich Maps in partnership with Pointr. Only visible layers (i.e. not hidden or frozen) are read by the Spaces conversion program and only data that the customer chooses to share. If the room names/IDs include identifying information for occupants of those workspaces, then that data is processed and stored. However, that data can also be overwritten using the Rich Map Editor in the Cisco Spaces Dashboard setup pages.

Other System Information
Cisco Spaces also collects "System information" to assist Cisco with understanding product usage and enabling product improvements.

Cisco Spaces Collects telemetry data such as Device Mac Address, Network data is collected such as location data includes Network SSID, Client Device Location Details (X, Y), Network Hierarchy including Campus / Building / Floor Identity, connected AP details.

Through Connector 2.x and 3.x, Cisco Spaces collects the other telemetry data such as AP mac address, RSSI value, ipv4, ipv6, SSID, AP name from the user locations.

Third Party Integrations
Cisco Spaces not integrated with other Cisco products. However, Cisco Spaces is integrated with third-party products includes HubSpot, Pendo, Pointr, Kontakt.io. Cisco is not responsible for customer data once it leaves Cisco Spaces for a non-Cisco product. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party.

The Table below lists Third Party Integrations.

Third Party Products	Description	Type of Personal Data	Purpose
HubSpot	HubSpot is a cloud-based, inbound marketing & CRM platform that allows businesses to transform the way that they market online and helps companies build customer experiences. It does this by bringing together a variety of easy-to-use tools/functionalities and allowing teams to manage all their activities in one place.	• First name and last name • E-mail address	Cisco Spaces is sending the Spaces account details. Customers will submit their contact information as updated in this Table in web form through the dnaspaces website (https://spaces.cisco.com)
Pendo	Pendo is a cloud platform that deliver better product experiences for happier and more productive users.	• E-mail address	Cisco Spaces is sending customer account details and personal information as updated in this Table.
Pointr	Pointr is a partner and Cisco Spaces shares Floor CAD files, which do not contain PII, with them to process into returned code. Cisco Spaces is integrating with Pointr via APIs.	No PII	Shares Floor CAD files, which do not contain PII, with with Pointr to process into returned code.
Kontakt.io	API Integration between Spaces and "Edge device manager" and Kontakt.io infrastructure Manager web portal to apply / manage configuration of Bluetooth low energy (BLE) floor beacons.	No PII	Cisco Spaces is sending IoT Telemetry data to Kontakt.io via the Firehose.

3. Data Center Locations

Cisco Spaces leverages third party cloud hosting providers to provide services globally.

Infrastructure Provider	Description	Location
AWS US North Virginia	Primary region for Cisco Spaces global customers	US-EAST-1
AWS US N-California	Disaster Recovery (DR) region for Cisco Spaces global customers	US-WEST-1
AWS EU Ireland	Primary region for Cisco Spaces european customers	EU-WEST-1
AWS EU Frankfurt	Disaster Recovery (DR) region for Cisco Spaces european customers	EU-CENTRAL-1
AWS Singapore	Primary region for Cisco Spaces Singapore customers. DR for Singapore is within same region on an alternate availability zone	AP-SOUTH-EAST-1

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 Spaces to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
System Administrator Log-in Information	• Customers	• Use the Service (i.e., authenticate authorized users of the Service)
	• Cisco BU Engineers (including technical support team)	• Provide technical support for the Service • Provide the Service • Communicate Service updates to Customer
End User Information	• Customers	• Use the Service (i.e., enable captive portal authentication, End User behavior tracking (such as visit duration, approximate location) and device behavior tracking (such as status, temperature), deliver personalized content to users, analytics))
	• Cisco BU Engineers • (Including technical support team)	• Improve the Service • Provide Customer assistance with reporting • Provide technical support
	• Third parties (if sharing option is chosen by Customer within the Service)	• To facilitate related Customer request

6. Data Portability

If Customer receives an end user request to port data, customer may contact Cisco technical support for Cisco Spaces (electronic mail: cisco-dna-spaces-support@external.cisco.com) to assist in preparing the data portability report.

7. Data Deletion and Retention

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

Customers can request deletion of other personal data retained on the Cisco Spaces platform by sending a request at https://privacyrequest.cisco.com/ or opening a TAC service request, and unless the personal data is required to be retained for Cisco's legitimate business purposes, Cisco endeavors to delete the requested data from its systems within 30 days. The table below describes the retention period and the business reasons that Cisco retains the personal data.

Type of Personal Data	Retention Period	Reason for Retention
System Administrator Log-in Information	For the duration of Customer's active license term to the Service, or until such time that Customer requests deletion of this data by reaching out to Cisco technical support for Cisco Spaces.	• Provide the Service • Communicate Service updates to Customer
End User Information	For the duration of Customer's active license term to the Service, or until such time that Customer requests deletion of this data by reaching out to Cisco technical support for Cisco Spaces.	• Use the Service (i.e., enable captive portal authentication, End User behavior tracking (such as visit duration, approximate location) and device behavior tracking (such as status, temperature)) • Deliver personalized content to End Users • Utilize analytics on the part of Customer

8. Personal Data Security

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

Cisco Spaces infrastructure is deployed and protected in a separate secure Amazon VPC (Virtual Private Cloud). All the data is encrypted at rest and in transit. The data is transmitted from Customer infrastructure to Cisco Spaces cloud over HTTPS/TLS. Customers can optionally choose to use RADIUS for captive portal authentication. If used, RADIUS traffic is sent over UDP to the Cisco Spaces cloud.

9. Sub-processors

Cisco partners with 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
AWS	• Log-in Information • End User Information	Third party host of the Service	United States, European Union, Singapore

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 & 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:

- SOC2 Type I Compliance
- ISO 9001:2015 Certified
- Cloud Security Alliance (CSA) STAR Level 1 Certification
- SCF Compliance (formerly CATO Compliance)
- Cisco CSDL Compliance for On-prem Cisco Spaces connector
- GDPR Compliance for Europe region

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 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) 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 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.

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