Cisco Spark
Privacy DataSheet

This Privacy DataSheet describes the processing of personal data (or personal identifiable information) by Cisco Spark.

1 Overview of Cisco Spark

Cisco Spark (the "Service") is an app-centric, cloud-based service made available by Cisco to companies or persons ("Customers," "you," or "your") who purchase it for use by their authorized users ("user"). Cisco Spark provides a complete collaboration suite for your team to create, meet, message, make calls, and share, regardless of whether they are together or apart—in one continuous workstream before, during, and after meetings. For a detailed description of Cisco Spark, please see the Cisco Spark Offer Description.

Because Cisco Spark enables collaboration among its users, if you choose to purchase Cisco Spark, you will be asked to provide your personal data in order to use the Service. The following paragraphs describe Cisco's processing of personal data in connection with the delivery of Cisco Spark, the location and transfers of that data, and how it is secured in accordance with privacy principles, laws, and regulations. Cisco will use your personal data consistent with this Privacy DataSheet. Note that this Privacy DataSheet is a supplement to the Cisco Privacy Statement.

2 Personal Data Processing

If you are a user and your employer is the Customer that purchased the Service, all of the information described in this Privacy DataSheet is subject to your employer's policies regarding access, use, monitoring, deletion, preservation, and export of information associated with the Service. This may include access to the keys used to encrypt or decrypt your User-Generated Information. If you are a user and also the Customer (*e.g.*, you as an individual subscribed to the Service), and you used your personal email address when signing up for the Service, your employer's policies will not apply to the data that you share while using the Service. Your account is identified by your email address, so if you sign up for the Service for your personal use, Cisco recommends that you use your personal email address. If you want to change your email address, you can do so via this link: link/doc

If Customers or users communicate with users in other companies through the Service, any information posted is shared with the users in those Spark spaces and the information associated with those communications will be subject to the space's creator's corporate policies regarding access, use, monitoring, deletion, preservation, and export of information. For example, If you communicate with a Cisco user through the Service, those communications, including your User-Generated Information, may be subject to access, monitoring, use, deletion, preservation, and export by Cisco. The tables below list the categories of personal data processed by Cisco Spark and describe why we process such data.

Spark Meeting and Messaging

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Activation Codes • Display Name • Email Address • First Name • Last Name • Password • Company Name • Billing Contact Name • Organization ID • Universal Unique Identifier	We use Registration Information to: • Enroll you in the Spark Meeting and Messaging Service • Display your user avatar identity to other users • Notify you about features and updates • Understand how the Service is used • Send you Cisco marketing communications • Make improvements to the Service and other Cisco products and services • Provide you remote access support • Authenticate and authorize access to your account
Host and Usage Information	• Device Name • Geolocation • IP Address • User Agent Identifier • Operating System Type and Version • Client Version • IP Addresses Along the Network Path • MAC Address • Time Zone • Domain Name • Activity Logs	We use Host and Usage Information to: • Understand how the Service is used • Diagnose technical issues • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service • Respond to Customer support requests
User-Generated Information	• Spaces Activity (date, time, person engaged and the activity) • Messages (content, sender, recipients, date, time, and read receipts) • Content Shared (files, file names, sizes and types) • Whiteboard Content • Meetings and Calls Information (title, invitation content, participants, link, date, time, duration and quality ratings) • Voicemails • Presence (user status) • Recordings (when feature becomes available)	We use User-Generated Information to: • Provide the Service, an important component of which is a persistent history of your interactions with other users

Personal Data Category	Types of Personal Data	Purpose of Processing
Information Collected Related to Optional Features	• Geographic Location	If you choose to enable optional location-sharing, we will collect your geographic location when you send a message or share content in a space. We collect this information so that it can be shared with other users in the space.
	• Calendar and Contact Information on Your Mobile Device	If you choose to use the Service on your mobile device, upon sign-up you will have the option of sharing your calendar and/or contacts with the Service mobile application. This calendar and contact information is accessed only by the application locally on your mobile device and is not shared with Cisco unless and until: • you interact with a contact from your mobile device contact list using the Service, in which case we collect information only about that user. The Service mobile application uses this information to make it easier for you to connect with your contacts. • you create a space from a calendar event using the Service, in which case, we collect the information in the meeting invitation, including the date, time, duration and meeting participants
	• Information Collected by Cookies, Local Storage, and Other Browser Storage Technologies	When you use the Service in your web browser, we use cookies, local storage, and other browser storage technologies to ensure that you can stay logged into the Service until you choose to log out and to improve the performance of the Service. These technologies may store Registration Information, Host and Usage Information. Cookies are always sent using transport encryption.

Spark Call

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• SIP Identifier • Phone Number • Directory Extension • Direct Line • Voicemail Box Number • Voicemail PIN • Device Activation Codes • Email Address • Name • Profile Picture • Password	We use Registration Information to: • Enroll you in the Spark Call Service • Display Caller ID • Notify you about features and updates • Understand how the Service is used • Send you Cisco marketing communications • Make improvements to the Service and other Cisco products and services • Enable Directory Services within your organization • Provide you remote access support • Authenticate and authorize access to your account • Route calls to your users and places • Allow internal and external dialing • Allow you to activate your IP Phones • Access your voicemail • Respond to Customer support requests
Host and Usage information	• Device Name • Geolocation • IP Address • Mobile Type • MAC Address • Time Zone • Universal Unique Identifier • Domain Name • Activity Logs	We use Host and Usage Information to: • Understand how the Service is used • Diagnose technical issues • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service • Respond to Customer support requests
User-Generated Information	• Recordings • Transcripts • Voicemail	We use User-Generated Information to: • Provide the Service, enabling collaboration among users in different locations • Provide customized Music On Hold

Personal Data Category	Types of Personal Data	Purpose of Processing
		• Provide voicemail and voicemail transcription services Note: We route audio and video call content and screen sharing content between call participants but we do not retain or store the content

Spark Care

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Activation Codes • Display Name • Email Address • First Name • Last Name • Password • Company Name • Billing Contact Name • Organization ID • Universal Unique Identifier	We use Registration Information to: • Provide you remote access support • Authenticate and authorize access to the Spark Care Service
Host and Usage information	• IP Address	We use Host and Usage Information to: • Understand how the Service is used • Diagnose technical issues • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service • Respond to Customer support requests

Spark Depot (APIs)

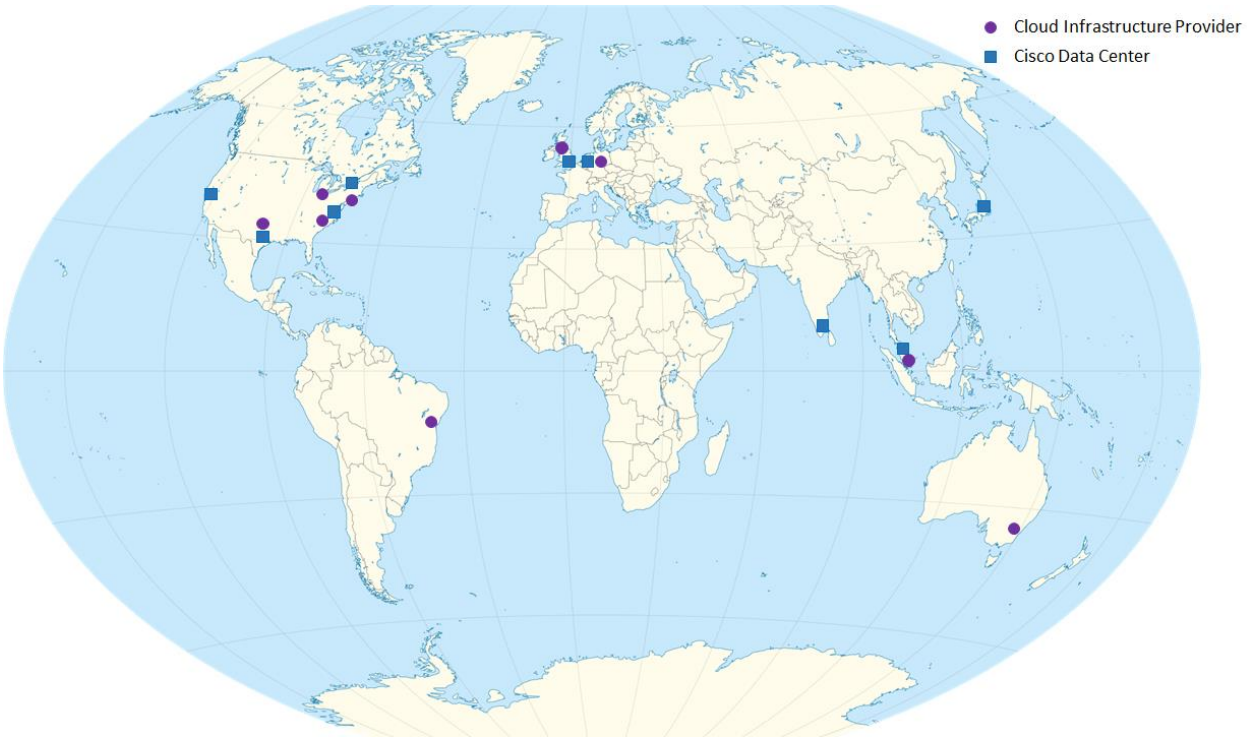
Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Activation Codes • Display Name • Email Address • First Name • Last Name • Password • Company Name • Billing Contact Name • Organization ID • PIN • SIP Identifier • Phone Number • Directory Extension • Voicemail Box Number	We use Registration Information to: • Authenticate and authorize access to the Spark Depot • Notify you of features and updates • Understand how the Service is used • Provide you remote access support • If you choose to use Spark Depot to add a third-party integration or bot to your Spark space, the third party may share information and content associated with your third-party service or application account with us. We do not receive or store your passwords for these third-party services or applications, although we do store authentication tokens associated with them.
Host and Usage information	• Device name • Geolocation • IP Address • Mobile Type • MAC Address • Time Zone • Universal Unique Identifier • Domain Name • Activity Logs	We use Host and Usage Information to: • Provide the Service • Diagnose technical issues • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service • Respond to Customer support requests

Technical Support Assistance (TAC)

Personal Data Category	Types of Personal Data	Purpose of Processing
TAC Support Information	• First Name • Last Name • Email Address • Phone Number of the Employee Appointed to Open the Service Request • Authentication Information • Information About the Condition of the System • Registry Data About Software Installations and Hardware Configurations • Error-Tracking Files	We use TAC Support Information to: • Provide you remote access support • Review quality of the support service • Perform analysis of the service solution

3 Cross-Border Transfers

Cisco Spark leverages its own data centers as well as third-party cloud hosting providers to deliver the Service globally. These data centers are currently located in the following countries (data center locations may change from time to time and this Privacy DataSheet will be updated to reflect those changes):



Cisco Data Center Locations:
Dallas, TX, USA
San Jose, CA, USA
Washington DC, USA
Toronto, Canada
Amsterdam, Holland
Bangalore, India
London, UK

Cloud Infrastructure Provider Locations:
Chicago, Illinois, USA
Dallas, TX, USA
Los Angeles, CA, USA
New York, New York, USA
Frankfurt, Germany
Sao Paulo, Brazil
Singapore, Singapore

Cisco Spark Media Data Center Locations:
Dallas, TX, USA
San Jose, CA, USA
Washington DC, USA
Amsterdam, Holland
Frankfurt, Germany
London, UK
Sao Paulo, Brazil

Cisco Data Center Locations:	Cloud Infrastructure Provider Locations:	Cisco Spark Media Data Center Locations:
Singapore, Singapore Tokyo, Japan	Sydney, Australia	Singapore, Singapore Sydney, Australia Tokyo, Japan

Not all of the above locations are used for processing and storage for all Spark services. Storage and processing details are as follows:

Product	Processing	Storage
Spark Meeting and Messaging	US locations + Worldwide Media Data Center locations	US locations only
Spark Call	US locations only	US locations only
Spark Care	US locations only	US locations only
Spark Depot	US locations only	US locations only

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions.
In particular:

- US-EU and Swiss-US Privacy Shields
- APEC Cross Border Privacy Rules
- Cisco Master Data Protection Agreement with EU Model Clauses
- Binding Corporate Rules are currently in-process

4 Access Control

Customers and Cisco can access personal data on Cisco Spark as described in the table below.

Spark Meeting and Messaging and Spark Call

Personal Data Category	Who Has Access	Purpose of Access
Registration Information	Customer through the Cisco Spark Control Hub	Process in accordance with Customer's personal data policy
	Cisco	Support the Service in accordance with Cisco's data access and security controls process
Host and Usage Information	Customer through the Cisco Spark Control Hub	Process in accordance with Customer's personal data policy
	Cisco	Support and improvement of the Service by the Cisco Spark Support and Development Team
User-Generated Information	Customer through eDiscovery console, Events API (enables data leak prevention). Additionally, for Cisco Spark PRO Pack Customers - Encryption Keys	Process in accordance with Customer's personal data policy
	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer, and will only access in accordance with Cisco's data access and security controls process
	Other Customers (when users share with other Customers)	To the extent that users post User-Generated Information in Spark spaces that include users from other companies, those users have access to the data posted. Additionally, if users post User-Generator Information in Spark Spaces owned by other Customers, those Customers have access to this information and can use it in accordance with their own corporate data policies.

5 Data Portability of User-Generated Information and Other Personal Information

Cisco Spark allows Customers to export up to 90 days of User-Generated Information using APIs provided with the Service. Users who do not have a corporate account (*e.g.*, you have an individual user account) must contact Cisco to specifically request to export up to 90 days of User-Generated Information via privacy@cisco.com. Additionally, Customers that purchase Cisco Spark PRO Pack can use the APIs that come with that service to export User-Generated Information for any period that the Customer sets, in accordance with its corporate data retention and deletion policies. The User-Generated Information posted by users who are using Cisco Spark purchased by their employer is treated as data of the employer (Cisco's Customer). Accordingly, the Customer's corporate policies will apply. If users wish to export their data, the user must consult the Customer administrator or the person within their employer authorized to make determinations regarding the disposition of Cisco Spark data belonging to the Customer. If a Customer's users post User-Generated Information into a Cisco Spark space belonging to another Customer (*e.g.*, a space created by a separate organization or user outside of your organization), you will not be able to export the data posted in that space, because that data is treated as data of the organization or user that created the space.

Both the Customer and the consumer user are able to export personal information that is held on the Cisco Spark platform. The Customer can export limited types of personal data via the Control Hub (through CSV exports) or all types of personal data except authentication tokens through APIs. Consumer users can export personal data through the APIs. There is no time restriction on exporting this data.

6 Data Deletion & Retention

Cisco Spark allows for the persistent retention of meetings and messages information shared by users. Accordingly, Customer's data is stored on the platform for 7 years while the Customer has an active subscription (subject to data storage limitations). For Customers that wish to minimize the amount of data stored on the Spark platform or customize the retention period to be longer or shorter, Cisco Spark PRO Pack includes retention settings that automatically delete data in accordance with the Customer's corporate data retention and deletion policies. After a Customer's subscription terminates or expires, its remaining encrypted User-Generated Information and personal data is retained on our platform for 7 years unless the Customer requests deletion. Customers can request deletion of personal data retained on the Cisco Spark platform by sending a request to privacy@cisco.com or opening a TAC support request. When a Customer makes a request for deletion, Cisco endeavors to delete the requested data from its systems within 30 days, unless the data is required to be retained for Cisco's legitimate business purposes. If we are required to retain certain categories of Customer data, the reason why we retain it and the retention period are described in the table below. Also, Cisco will not delete any User-Generated Information that your users have posted into a Cisco Spark space belonging to another Customer (*e.g.*, a space created by a separate organization or user outside of your organization) and will retain your user's name associated with the posting in that space, because that data is treated as data of the organization or user that created the space.

Personal Data Category	Retention Period	Reason and Criteria for Retention
Registration Information	7 years from when the Service is terminated	Data collected as part of registration, including information provided by Customers as part of Cisco's financial due diligence, constitute Cisco business records and are kept to comply with Cisco financial and audit policies, as well as tax requirements.
TAC Support Information	Until Customer requests deletion via privacy@cisco.com or by opening a TAC service request for deletion.	TAC Support Information is retained to ensure efficient support in case of recurring issues and to comply with Cisco audit policies related to business records of services provided to Customers.

Personal Data Category	Retention Period	Reason and Criteria for Retention
User-Generated Information **(excluding Voicemail for Spark Call, discussed below)**	7 years after user's last post, unless Customer (i) specifically requests deletion via privacy@cisco.com or by opening a TAC service request; or (ii) purchases Cisco Spark PRO Pack, in which case the retention period is customizable by Customer	User-Generated Information is persistent because the Service was built to allow Customers to leverage this information to collaborate with other users over long periods of time.
Voicemail for Spark Call	Unread messages are retained until the user reads the message or the user is deleted from the system. When a user reads the message, it is retained for 30 days and then deleted. When a user is deleted from the system, all associated messages (read or unread) are then deleted within 2 days. When a user deletes a message, it is deleted from the system within 1 day.	Data is retained for the time necessary to provide the associated service.
Host and Usage Information	7 years from when the Service is terminated	Information generated by instrumentation and logging systems created through the use and operation of the Service is kept as part of Cisco's record of Service delivery. Usage information used to conduct analytics and measure statistical performance is retained but pseudonymized.

7 Personal Data Security

Cisco Spark is ISO 27001:2013 certified and in accordance with those standards adopts technical and organizational security measures to protect your personal data from unauthorized access use or disclosure as required by law. Additional information about our encryption architecture is summarized in the table and paragraphs below.

Spark Meeting and Messaging and Spark Call

Personal Data Category	Type of Encryption
Registration Information	Encrypted in transit, but not at rest
Host and Usage information	Encrypted in transit, but not at rest
User-Generated Information	Encrypted end to end with Cisco holding keys on Customer's behalf unless Customer purchases the Spark PRO Pack and deploys Hybrid Data Security, which allows Customer to hold keys

The Service uses different kinds of encryption to protect different kinds of data in transit and in storage. In this section, "you" and "your" refers to the user.

End-to-end encryption is used to protect messages, content, whiteboards, and meeting details. Just prior to sending a message from your client, it is encrypted on your device. (If you have opted to share your location information, that information is also encrypted.) Messages remain encrypted until they are received by other users, where they are decrypted on those user's devices. The same process is used for each whiteboard stroke, whiteboard background images, and whiteboard snapshots (with one exception listed below under media encryption). The same process is also used for content that you share, except as noted below. Push notifications are likewise end-to-end encrypted.

There are a few circumstances under which User-Generated Information is decrypted:

- For certain types of files (PDFs, Microsoft Word documents, and PowerPoint presentations), we decrypt the object in order to send it to a third party to be "transcoded" for display in a space. For example, if you upload a slide presentation into a space, it will first be encrypted on your device. When we receive the presentation on our server, we will decrypt it and send it to a third party, where individual thumbnail images of each slide will be generated. The third party will send the thumbnails and presentation back to us. We will then encrypt the thumbnails and presentation and send them to the other users in the space. The decrypted file and images are not stored; only the encrypted forms of these objects are stored.
- For bots and integrations that have not integrated with our end-to-end encryption scheme, we decrypt messages and content associated with a bot/integration before sending it to the third party supporting the bot or integration. We do not store the decrypted messages and content.
- Messages and content may be decrypted by your employer or the employers of those you communicate with using the Service. If you communicate with Cisco employees, then those messages can be decrypted by Cisco.

Media encryption is used to protect the audio, video, screen sharing data, and voicemails that you transmit during a call. When you make a call, media is encrypted from your device to our servers. It may be decrypted on our servers so that we can manage the call. It is re-encrypted before being sent to the other participants on the call unless they are connected via the public telephone network or do not support encryption. If you dial into a meeting using SIP and there is whiteboarding taking place in the meeting, we will decrypt the end-to-end encrypted whiteboard content, transcode it, and send it to you using media encryption. We do not store any call audio, video, or screen sharing data on our servers. Voicemails are encrypted from your device to our servers, decrypted to be prepared for storage, and re-encrypted in storage on our servers. Voicemails transmitted via email are not encrypted. Faxes are not encrypted.

Transport encryption (also known as HTTPS) is used to protect all connections to and from the Service other than voice/video calls. When you register for the Service, send messages, share content, write on a whiteboard, connect with third-party services or applications via integrations, send logs or screen shots to provide us with feedback, or otherwise connect to the Service, we always use transport encryption.

8 Third Party Service Providers (Sub-processors)

We may share User-Generated Information, Registration Information, Host Information, and/or Usage Information with service providers, contractors, or other third parties to assist in providing and improving the Service. The data shared may include aggregate statistics or individualized data. All sharing of information is carried out consistent with the Cisco Privacy Statement and we contract with third-party service providers that can provide the same level of data protection and information security that you can expect from Cisco. We do not rent or sell your information. A current list of Cisco Spark's third-party service providers with access to personal data can be provided upon request.

If a Customer subscribes to the Service through a Cisco partner, we may share Host and/or Usage Information about the Customer's employees' use of the Service with the partner. Customers have the option of disabling this information-sharing with Cisco partners. If a Customer chooses to purchase support for the Service through a Cisco partner, any or all of the information described in this DataSheet may be shared with the partner.

Unencrypted messages may be shared with third-party services and applications that you choose to integrate with the Service, but not with any other third parties without your permission or unless required by law.

9 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.

10 Certifications

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 has received the following certifications:

- ISO/IEX 27001:2013
- SOC 2 Type I Attestation
- The WebTrust Seal of Assurance for CA and the Web Trust Seal of Assurance for CA–SS

Additionally, the following Certifications are in-process for Cisco Spark.

- SOC 2 Type II Attestation

Customers can review the certifications under NDA. In-process certifications will be made available for review under NDA, as they are completed.

11 Corporate Quality Compliance and Certifications

Cisco holds a Global ISO 9001 Certification and ISO 14001 Registration, managed by the Corporate Quality Compliance and Certifications program, which establishes and maintains policies that ensure quality management of processes and environmental responsibilities. Visit our Quality Certifications page to understand the scope of these compliance certifications and read more information.

12 FAQs

For more information and FAQs related to Cisco Spark's technical and operational security features, please see the Spark Tech Ops and Security FAQs page and the Spark Security, Compliance, and Management page.

For more general information and FAQs related to Cisco's Security Compliance Program and Cisco's GDPR readiness please visit The Cisco Trust Center.