Customer Journey Data Service

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Customer Journey Data Service.

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

Cisco will process personal data from Customer Journey Data Service 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 Journey Data Service in order to provide its functionality.

1. Overview

Customer Journey Data ("the Service") is a next-generation customer journey management service made available by Cisco or its resale partner ("Partners") to companies ("Customer", "you", "your") who purchase it for use by their authorized users to capture customer journeys of people who access contact centers ("Users") across any channel or application, identify insights, and take real-time actions to provide an excellent customer experience. This service is currently only available for Cisco's US-based Customers.

Customer Journey Data Service integrates with various Cisco products. Please see the applicable Privacy Data Sheet for details regarding processing of personal data by the Cisco product receiving/sending personal data from/to Journey Data Service.

Note, Customer Journey Data Service may also be integrated with third-party products. Cisco is not responsible for customer data once it leaves Customer Journey Data Service 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.

For more information about Journey Data Service, visit https://developer.webex-cx.com.

2. Personal Data Processing

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

Personal Data Category	Type of Personal Data	Purpose of Processing
Registration Information (Customer)	• User Profile Information • Username • Name (First, Last) • Email address • Department title • Phone number • Password	We use Registration Information to: • Deliver and provide operational support for the Service • Communicate with you on the status and availability of the Service • Notify you of features and updates • Billing and Invoicing • Customer contact enablement, incident response, and customer relationship management • Send you Cisco marketing communications • Authenticate and authorize access

User Information (User)	- Name (optional) - Phone (optional) - Email (optional) - Other Personally Identifiable Information from customer integrated data sources (Optional)	- Deliver and provide operational support/product feature for the Service - Ensure quality and training - Diagnose technical issues
Host and Usage Information	- Activity logs (e.g.API calls, application errors, API usage data).	We use Host and Usage Information to: - Understand how Service is used - Respond to support requests and diagnose problems - Conduct and provide Customer with analytics and usage information

3. Data Center Locations

Cisco uses third-party hosting providers to deliver the Service globally. The Service's data centers are currently located in the following countries (data center locations may change from time to time and this Privacy Data Sheet will be updated to reflect those changes).

Hosting Provider Locations
United States United Kingdom Germany Australia Canada

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 Journey Data Service to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Registration Information (Customer)	Customers	- View and manage users/administrators - Process in accordance with Customer's personal data policy
	Cisco	- Enable and support the Service in accordance with Cisco's data access and security controls process
User Information (User)	Customers	- View and process in accordance with Customer's personal data policy

	Cisco	• Deliver, support and improve the Service in accordance with Cisco data access and security controls process • While Cisco operates the Service, Cisco does not access or monitor this data unless it is shared with Cisco by Customer and will only do so in accordance with Cisco's data access and security controls process.
Host and Usage Information	Customers	• Usage information may be accessible to Customer when accessing, processing and analyzing User's journey data collated from the Customer's integrated data sources
	Cisco	• Support and improvement of the Service

6. Data Portability

Customer may export the Registration Information, User Information and select Host and Usage Information through APIs. Such exports will be available in an open standard format.

7. Data Deletion and Retention

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

Type of Personal Data	**Retention Period**	**Reason for Retention**
Registration Information (Customer)	Active Subscriptions: Registration Information will be retained as long as the Customer maintains an active subscription. Registration Information will be deleted upon account termination.	Registration Information is required to provide the Service. 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 complying with Cisco financial and audit policies, as well as tax requirements.
User Information (User)	User Information will be deleted upon the earlier of 1) when Customer's configured data retention period ends (see documentation for options); or 2) upon account termination. User information can also be deleted for a specific User on a per-request basis.	User Information is persistent because the Service was built to allow Customers to leverage this information over long periods of time
Host and Usage Information	Active Subscriptions: Host and Usage Information will be retained as long as Customer maintains active subscription.	Usage Information is persistent because the Service was built to allow Customers to leverage this information over long periods of time. Usage Information may be used to conduct analytics and measure statistical performance.

	Host and Usage will be deleted upon account termination.	

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.

Personal Data Category	Security Controls and Measures
Registration Information (Customer)	• Encrypted in transit and at rest • Passwords are hashed
User Information (User)	• Encrypted in transit and at rest
Host and Usage Information	• Encrypted in transit and at rest

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	Registration, User, Host and Usage Information	Data Hosting	United States United Kingdon Germany Australia Canada

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.

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.

This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement. To the extent this document differs from the Cisco Online Privacy Statement, this document will take precedence. If there is a difference in translated, non-English versions of this document, the U.S.-English version will take precedence.

Cisco frequently evolves and updates its offerings. Cisco Privacy Data Sheets are subject to change, and are reviewed and updated on an annual basis, or as reasonably needed to reflect a material change in the processing of Personal Data. 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.