Cisco Unity Connection

This Privacy Data Sheet describes how Cisco Unity Connection (CUC) processes personally identifiable information (“personal data”).

1. Overview of Cisco Unity Connection Capabilities

Cisco Unity Connection (“CUC” or the “Service”) is s a robust unified messaging and voicemail solution that provides users with flexible message access options and IT with management simplicity. Cisco makes the Service available to companies or persons (“Customer,” “you” or “your”) who purchase it for use by their authorized users (each, a “user” or “end user”). Cisco Unity Connection lets Customers and users access and manage messages from an email inbox, web browser, Cisco Jabber, Cisco Unified IP Phone, smartphone, or tablet. Unity Connection also provides flexible message access and delivery format options, including support for voice commands and speech-to-text transcription. For more details on the core capabilities of Cisco Unity Connection, see Cisco Unity Connection.

Cisco does not host or operate this product on the Customer’s behalf. Consequently, Cisco does not process or host any personal data that is described in this Privacy Data Sheet, unless technical support requires it.

2. Personal Data Processing

The table below lists the categories and types of personal data processed by Cisco Unity Connection and describes why it processes such data.

Personal Data Category	Types of Personal Data	Purpose of Processing
End User Information	• Name (First, Last, Initial) • Title • Alias/Login ID • Corporate Email ID • Corporate Phone Number and Directory URI • Department and Manager • Billing ID, Employee ID • SMTP address, Display Name • Office Address and Timezone • Language • Extension • Login Password / PIN • Notification Settings • User’s Greetings • Voice Name • Last login IP Address	• Easy Directory search based on Name • Authentication and authorization • Users use alias to sign-in to the Cisco Personal Communications Assistant (user self-care portal) • Administrators use alias to sign-in to Cisco Unity Connection administration (web-based admin portal) • Provide the Service • Directory URI, Corporate phone number as an alternate extension for login through Telephone User Interface (TUI) • Billing and accounting purposes • SMTP address to identify the user in an SMTP-enabled client. Display name is played to the called party if voice name is not recorded for the user. • Login Password/PIN to authenticate access to voicemail through Vendor Web Portal / TUI • Service notifications, including SMTP and HTML notification of new voice mail • Greetings to be played to the caller • For logging and debugging purposes
Voicemail Information	• Recorded Voicemail • Voicemail Transcription	• Provide the Service

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 Service. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data.

3. Cross-Border Transfers

Cisco Unity Connection is not hosted or operated by Cisco. Accordingly, Cisco does not make any cross-border transfer of personal data to host or operate Cisco Unity Connection on behalf of its Customers.

4. Access Control

Customers and users can access personal data processed by the Service as described in the table below:

Personal Data Category	Who has access	Purpose of the access
End User Information	Cisco Unity Connection Administrator (Customer)	• Administrator can add, delete, edit, and view all user's configuration information such as Name, ID, Email ID, Corporate Phone Number, Manager's email ID, Department, Directory URI, Extension and Language. • Administrator can also add users and update existing configurations. • Administrator can view, edit and maintain user's configurations like login credentials, voice greetings and voice names.
	User	• End user can view and manage their own user Information through the Self-Care Portal. However, they cannot view the configuration information of other users. • A user can view and manage their login credentials, voice greetings and voice names.
Voicemail Information	Cisco Unity Connection Administrator (Customer)	• Administrator can delete a user account which results in deleted messages for that user. • Administrator can set time-based purging of voicemails.
	User	• Users can access, view, play, delete voicemails and transcriptions.

5. Data Portability

The Service allows administrators to import and export all End User and Voicemail Information.

6. Data Deletion & Retention

Retentions periods for the personal data collected by the Service are listed in the following table:

Personal Data Category	Retention Period	Reason for Retention
End User Information	Set by Cisco Unity Connection Administrator (Customer)	Administrator retains the End User Information for a period of time in accordance with the Customer's policy and legal business requirements.
Voicemail Information	Set by Cisco Unity Connection Administrator (Customer)	Administrator retains the Voicemail Information for a period of time in accordance with the Customer's policy and legal business requirements.

7. Personal Data Security

The Security measures employed to the personal data collected by the Service are listed in the following table:

Personal Data Category	Personal Data Security
End User Information	The Roles and Access Control Group assignment ensures only the administrator can access End User Information within Cisco Unity Connection.
Voicemail Information	The Roles and Access Control Group assignment ensures only users can access the Voicemail Information within Cisco Unity Connection.

Additional information about the encryption is summarized in the following table:

Personal Data Category	Type of Encryption
End User Information (excluding PINs and passwords as discussed below*)	Encrypted in transit but not at rest
Voicemail Information	By default, traffic between endpoints and the CUC server is not encrypted in transit or at rest. However, the Customer can change the configuration so that this data is encrypted in transit, but not at rest.

* When user profiles are synchronized to the Service from a Customer's Active Directory, the Service will not store passwords; instead, the Customer's active directory or IdP server will be used to authenticate end users for the Service. In the case where a Customer adds a user to CUC directly, passwords for that user will be hashed and stored locally on the CUC server. PINs, which can also be created by end users, will also be hashed and stored locally on the CUC server.

8. Third Party Service Providers (Sub-processors)

Cisco Unity Connection is not hosted or operated by Cisco. Accordingly, Cisco is not responsible for any third-party service providers the Customer might utilize to operate Cisco Unity Connection.

9. Information Security Incident Management

Breach and Incident Notification Processes
Cisco Unity Connection is not hosted or operated by Cisco. Accordingly, Information Security Incident Management is the responsibility of the Customer and not Cisco. The Cisco Product Security Incident Response Team (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 Emergency Response details the process for reporting security incidents.

10. Certifications and Compliance with Privacy Laws

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.

11. General Information and Privacy 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.