Cisco Registered Envelope Service

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Registered Envelope Service.

1. Overview of Cisco Registered Envelope Service Capabilities

Cisco Registered Envelope Service ("CRES") helps customers secure their email communications. This service allows a customer to send encrypted messages via registered envelopes. The registered envelope is an encrypted email which may also be password-protected. If the envelope is password-protected, it can only be opened by authorized recipients who authenticate themselves. For more information about CRES, please see: https://www.cisco.com/c/en/us/products/security/registered-envelope-service/index.html?CCID=c000156&DTID=odicdc000016.

CRES processes certain personal data of its users. The following paragraphs describe which personal data Cisco processes to deliver CRES services, the location of that data and how it is secured in accordance with privacy principles, laws and regulations.

2. Personal Data Processing

The table below lists the personal data used by CRES to carry out the services and describes why we process that data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Customer Contact Information	• Name • Email address	Product administration: Creating an account, validating license entitlements, general product support and administration.
Email Envelope Header	• Sender • Recipient	• Verify Customer registration and license entitlement • Troubleshooting customer issues
Email Data Header	• From • To • Subject • Reply-to Headers (including CC/BCC) • Name/Title of Attachment (but not the content of the Attachment)	• Identify the From, To, Subject, Envelope Recipient (e.g., jsmith@company.com) • Troubleshooting customer issues
Encryption Key	• Unique Encryption Key per user	Unique message identifier used to allow appropriate sender and recipient to open encrypted message.
IP Address	• IP Address of end-user's device	Used to maintain user session connectivity to the service and audit reporting
Encrypted Envelope	• Full email in encrypted format	Optional cloud storage for customers of encrypted envelope if customer enables the "Easy Open" feature. Cisco is not able to decrypt the envelope.

3. Cross-Border Transfers

Cross border transfers occur with respect to customer account information, and data processed by CRES. When a new customer purchases a CRES subscription, that customer's account information is always created, processed and stored in the United States. All subsequent data from such customer that is associated with the CRES product function (i.e. Email Envelope Header, Email Data Header, Encryption Keys, IP Address data and if email storage is enabled, the Encrypted Envelope) will be processed in the United States, as the third party cloud hosting providers used by CRES are located in the United States only, as follows:

Data Center	Description	Location
Equinix	The Equinix infrastructure for the CRES cloud is a co-location data center that runs in the following region:	California, USA
Switch	The Switch infrastructure for the CRES cloud is a co-location data center that runs in the following region:	Nevada, USA

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

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

4. Access Control

Personal Data Category	Who has access	Purpose of the access
Customer Contact Information	Customers	Product administration: Creating an account, validating license entitlements, general product support and administration.
	Cisco Employees – Cisco Sales Administration, Licensing Operations, CRES Operations and Support staff only	
Email Envelope Header Email Data Header	Customer Administrator	Product Administration; Auditing; Report generation
	Cisco Dev Operations	CRES configuration and troubleshooting. and maintenance
IP Address	Cisco Dev Operations	CRES troubleshooting and maintenance.
Encrypted Envelope Encryption Key	Cisco Dev Operations	CRES troubleshooting and maintenance

5. Data Deletion & Retention

Personal Data Category	Retention Period	Reason for Retention
Customer Contact Information	Currently retained until delete requested	Administrative purposes
Email Envelope Header Email Data Header Encryption Key	10 years	Service delivery Note: Customer has the ability to lock Encryption Keys or set the Encryption Keys to expire (e.g. create a policy to expire Keys on an automatic basis).
IP Addresses	90 days	Auditing
Encrypted Envelope	Configurable up to 15 days	To provide a method for mobile devices to open envelopes w/o the need for an application or software on the device.

Deletion

After the ten (10) year retention period expires, CRES will automatically purge all Email Envelope Headers, Email Data Headers and Encryption Keys from CRES. Encryption Keys that are set to lock or expire are still subject to the ten (10) year deletion period; they will not be deleted sooner. Notwithstanding the foregoing, customers may open a Cisco TAC request to request that Cisco delete their CRES user accounts. Customers cannot delete the IP addresses that are part of the audit log. CRES will purge IP Addresses after the expiration of the retention period listed above.

6. Personal Data Security

Personal Data Category	Type of Encryption
Customer Contact Information	Data at rest disk level (SAN encryption) Data in motion (TLS encryption)
Email Envelope Header	Data at rest disk level (SAN encryption) Data in motion (TLS encryption)
Email Data Header	Data at rest disk level (SAN encryption) Data in motion (TLS encryption)
Encrypted Envelope	Data at rest (payload encrypted using AES-256) Data at rest (key stored on the key server is hashed value of encryption key and the salt combined)
Encryption Key	Data at rest disk level (SAN encryption) Data in motion (TLS encryption)
IP Address	Data at rest disk level (SAN encryption) Data in motion (TLS encryption)

7. Third Party Service Providers (Sub-processors)

Cisco partners with third party cloud hosting providers who contract to provide the same level of data protection and information security that you can expect from Cisco.

Sub-processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Equinix	Email Envelope Header Email Data Header Encryption Key IP Address	CRES leverages the Equinix data center to help provide a global service footprint, security assurance, service elasticity and resilience to CRES.	California, U.S.A.	ISO 27001, SSAE 18 SOC 1 Type II, SOC 2 Type II.
Switch	Email Envelope Header Email Data Header Encryption Key IP Address	CRES leverages the Switch data center to help provide a global service footprint, security assurance, service elasticity and resilience to CRES	Nevada, U.S.A.	SSAE 18 SOC I Type 2, SOC II Type 2

8. Information Shared by Customer for Support

If a customer contacts the Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from CRES that is provided by the customer. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data. Cisco does not process this data for any other purpose than to assist the customer to

resolve issues. For more information, please refer to the TAC Support Essentials Privacy Data Sheet.

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 and Compliance with Privacy Laws

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 and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation and other privacy laws around the world.

Cisco leverages the following privacy transfer mechanisms related to the lawful use of data across jurisdictions:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

11. General Information and GDPR 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 of this Privacy Data Sheet, please see https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html.