Cisco Secure Email Domain Protection

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Secure Email Domain Protection.

Cisco will process personal data from Cisco Secure Email Domain Protection 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 Domain Protection in order to provide its functionality.

1. Overview of Cisco Secure Email Domain Protection Capabilities

Cisco Secure Email Domain Protection ("Domain Protection") for external email helps prevent phishing emails from being sent using a customer domain(s). Domain Protection automates the process of implementing the email authentication standard Domain Message Authentication Reporting and Conformance ("DMARC") to better protect employees, customers and suppliers from phishing attacks using customer domain(s). This protects the customers' brand identity as well as increases email marketing effectiveness by reducing phishing messages from reaching inboxes. Domain Protection also offers an optional in bound DMARC feature for inbound emails.

For more information about Domain Protection, please see:
https://www.cisco.com/c/en/us/products/security/email-security/index.html

2. Personal Data Processing for Domain Protection

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

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Name • Address • E-mail Address • User ID	• Product administration: Creating an account, validating license entitlements, general product support and administration. • Product notifications • Product training
Email Header Data (header data from RUF failure samples) [(1)]	• Email From address • Email To address • Email Subject • Uniform Resource Identifier (URI)	• Message Failure Sample • Data used to determine the source and purpose of the inauthentic message
Sender IP	• IP address of sending mail server	• Identify legitimate and illegitimate sources of email

[(1)] Email header data is derived from DMARC authentication failure samples which typically originate from third party emails not generated by a customer. However, on rare occasions an email generated by the customer could fail DMARC authentication. In such cases, Domain Protection would receive that DMARC failure sample from the applicable email service provider. This data is deleted in accordance with Section 5. Customers can disable the DMARC authentication failure reporting (opt-out) at their own discretion.

Customer Gateway Service Reporting
Customer has the option to send numerical summaries about messages which have been processed and appear to come from Customer's domains ("RUA Data") or messages failing email authentication ("RUF Failure Samples") directly to Cisco to enhance the Domain Protection service. If a Customer chooses to share RUF Failure Samples directly with Cisco, such a configuration may transfer personal data within the RUF Failure Samples to Cisco, if applicable.

3. Personal Data Processing for Optional Inbound DMARC Feature

Inbound DMARC is an optional feature of Domain Protection that provides DMARC visibility to inbound email for domains owned by the customer. Inbound DMARC requires additional configuration and must be proactively enabled by Cisco and the customer in the Domain Protection configuration settings (e.g. opt-in). If enabled, a customer can subsequently choose to disable this feature at any time.

To leverage Inbound DMARC, a data sensor must be implemented. The Inbound DMARC sensor is available in an on-premises deployment model (the "On Premises Sensor") or a hosted deployment model where the sensor is hosted by Cisco (the "Hosted Sensor"). The table below lists the additional personal data processed by Domain Protection for the Inbound DMARC feature. For clarity, if customer uses an On Premises Sensor, Cisco does not collect the Email Metadata or Email Message Content data listed in the table below, and in that case, processing occurs at the customer premises where the On Premises Sensor is located.

Personal Data Category	Types of Personal Data	Purpose of Processing
Email Header Data and Sender IP (header data from inbound emails processed by Inbound DMARC)	• Email From header • Email "rcpt to" header • Email To header • Email Subject • Sender IP	Identify emails that are applicable for analysis by the Inbound DMARC Service
Email Metadata	• Attachment Filename • Attachment file format and presence of macros/malicious code • Attachment Hash (e.g. encrypted MDS or SHA1 format) • Uniform Resource Identifier (URI)	This data is not required for Inbound DMARC but is incidentally processed by the sensor (but is not retained). However, if the customer is utilizing the On Premises Sensor, this processing occurs on the customer's premises and the data is not collected by Cisco.
Email Message Content	• Personal data, if any, included in email message including attachments.	This data is not required for Inbound DMARC but is incidentally processed by the sensor (but is not retained). However, if the customer is utilizing the On Premises Sensor, this processing occurs on the customer's premises and the data is not collected by Cisco.

On Premises Sensor

Customers have complete control over the sensor including full "root" level access to the operating system and host application. Cisco employees cannot access an On Premises Sensor without the permission of the customer.

Hosted Sensors

Hosted Sensors are provisioned in a dedicated and separate Amazon Web Services account. Hosted Sensors are not multi-tenant. Each customer gets their own Virtual Private Cloud (VPC), their own Elastic Load Balancer (ELB), and their own EC2 Autoscale Group (ASG). The underlying AWS IaaS is multitenant. Cisco engineers cannot access the Hosted Sensor EC2 instances using the root account and only authorized Cisco engineers have access to the Hosted Sensor environment. All Hosted Sensor actions are logged locally and can be reviewed with the customer. This includes evidence that each message is deleted post-processing.

4. Cross-Border Transfers

When a customer purchases a subscription to Domain Protection, that customer's information (both the data relating to the customer's employees who are in contact with Cisco to procure and administer the products on behalf of customers, and the data processed through Cisco's delivery of its services to customers) is processed and stored in the United States.

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

- Binding Corporate Rules (Controller)
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5. Access Control

Personal Data Category	Who has access	Purpose of the access
Registration Information	Customer	Granting and managing access to their own account.
	Cisco	Creating an account and validating license entitlements and general product support and operations
Email Header Data and Sender IP (header data from RUF failure samples)	Customer	Security administration and operations
	Cisco	Providing general product support and operations
Email Header Data and Sender IP (header data from inbound emails processed by Inbound DMARC)	Customer	Security administration and operations
	Cisco	Providing general product support and operations
Email Metadata (for Hosted Sensor Deployment with Inbound DMARC only)	Customer	Incidentally processed by Hosted Sensor and not retained.
	Cisco	Incidentally processed by Hosted Sensor and not retained.
Email Message Content (for Hosted Sensor Deployment with Inbound DMARC only)	Customer	Incidentally processed by Hosted Sensor and not retained.
	Cisco	Incidentally processed by Hosted Sensor and not retained.

6. Data Deletion & Retention

Personal Data Category	Retention Period	Reason for Retention
Registration Information	Subscription length [2]	Validating license entitlements and general product support and operations
Email Header Data (header data from RUF failure samples)	14 days	Data used to determine the source and purpose of the inauthentic message
Sender IP (Domain Protection) (Section 2 above)	3 years	Historical reporting capabilities

[2] Customer's registration information will be purged from Domain Protection upon request by opening a Cisco TAC case.

Sender IP (Inbound DMARC) (Section 3 above)	13 months	Historical reporting capabilities
Email Header Data (for Hosted Sensor Deployment with Inbound DMARC only)	60 days	Historical reporting capabilities
Email Metadata and Email Message Content (for Hosted Sensor Deployment for Inbound DMARC only)	Processing period only	This data is not retained once processed

7. Personal Data Security

Personal Data Category	Type of Encryption
Registration Information	Encrypted in transit (TLS) and at rest (AES 256)
Email Header Data and Sender IP (header data from RUF failure samples)	Encrypted in transit (TLS) and at rest (AES 256)
Email Header Data and Sender IP (for Hosted Sensor Deployment with Inbound DMARC only)	Encrypted in transit (TLS) and at rest (AES 256)
Email Metadata and Email Message Content (for Hosted Sensor Deployment with Inbound DMARC only)	Encrypted in transit (TLS). This data is not retained and does not come to rest in the Domain Protection cloud.

8. Third Party Service Providers (Sub-processors)

Cisco partners with service providers who 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 Cisco Domain Protection service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Agari Data, Inc.	• Registration Information • Email Header Data • Sender IP • Email Metadata and Email Message Content (for Hosted Sensor Deployment with Inbound DMARC only)	Cisco utilizes Agari Data, Inc. (www.agari.com) as a third-party provider for Domain Protection. Where Cisco refers to Cisco employees in this data sheet, this includes authorized employees of Agari Data, Inc.	United States
Amazon Web Services ("AWS")	• Registration Information • Email Header Data • Sender IP • Email Metadata and Email Message Content (for Hosted Sensor Deployment with Inbound DMARC only)	Domain Protection is hosted in the United States by Amazon Web Services (AWS). For information regarding AWS compliance/certification, please refer to documentation online at https://aws.amazon.com/compliance/.	United States (AWS U.S. West region)
Pendo	User names (i.e. email address)	Pendo (www.pendo.io) is utilized for product usage analytics.	United States (Google Cloud)

9. 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 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.

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 Laws

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:

- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework

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 redirect 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	**EMEAR 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 and GDPR FAQ

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, please go to the Personal Data Privacy section of the Cisco Trust Center.