Cisco Security Awareness

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Security Awareness.

1. Overview of Cisco Security Awareness Capabilities

Cisco Security Awareness is designed to help promote and apply effective cybersecurity common sense by modifying end user behavior. It empowers employees to work smarter and safer. This cloud delivered subscription provides comprehensive simulation, training and reporting so employee progress can be continually monitored and tracked. Cisco Security Awareness helps your organization remain safe with engaging and relevant computer based content with various simulated attack methods.

2. Personal Data Processing

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

Personal Data Category	Types of Personal Data	Purpose of Processing
Business Contact Information	• Name • Email address	• The name is used to contact the user, provide management reports, assign courses and other activities related to the delivery of awareness activities and phishing simulation. • The email address is used to communicate with the user when there is a new awareness activity assigned to them, deliver reminder notices and send phishing simulation email.
Phishing Simulator Data	• User IP Address • Browser Type • Operating System • User phish click behavior	• Incorporated into reports generated by the Security Simulation Platform. This information is required for troubleshooting issues and reporting on browsers and operating systems used by the users during the phishing simulation. This information helps organizations identify users who may be using software that is obsolete and no longer supported by the vendor.

3. Cross-Border Transfers

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
Business Contact Information	Customer	• Security administration and operations • Manage access lists • Deliver notifications • Reporting • Deploying awareness and phishing simulation activities • Troubleshooting and support
	Cisco	• The name is used to contact the user, provide management reports, assign courses and other activities related to the delivery of Cisco Security Awareness activities including the phishing simulation. • The email address is used to communicate with the user when there is a new Security Awareness activity assigned to them, deliver reminder notices and send phishing simulation email.
Phishing Simulator Data	Customer	• Security administration and operations • Reporting • Troubleshooting and support
	Cisco	Incorporated into reports generated by the Security Simulation Platform • Security administration and operations • Reporting • Troubleshooting and support

5. Data Portability

- Business Contact Information: Data portability is not required. The Security Awareness Platform is not the primary source for this data; the Business Contact Information is supplied by Customer.
- Phishing Simulator Data: Phishing Simulator Data can be exported in the form of reports to be processed or imported into other systems.

6. Data Deletion & Retention

Personal Data Category	Retention Period	Reason for Retention
Business Contact Information	• Retention: Duration of contract with Customer unless otherwise requested by Customer. • Deletion: Data is deleted fourteen (14) days after contract deletion or upon Customer request.	• Retention: Provide historical data on delivered activities. • Where the Customer has purchased the Security Awareness Platform, Cisco will process the data provided by the Customer for the purpose of providing Customer and Customer's employees access to a web-based Security Awareness Platform. • Where the Customer has purchased the Security Simulation Platform, Cisco will process the data provided by the Customer for the purpose of providing Customer and Customer's employees access to a Security Simulation Platform.

Phishing Simulator Data	• Retention: Duration of contract with Customer unless otherwise requested by Customer. • Deletion: Data is deleted fourteen (14) days after contract deletion or upon Customer request.	• Retention: Provide historical data on delivered activities.

7. Personal Data Security

Personal Data Category	Type of Encryption
Business Contact Information	Microsoft Azure encryption mechanisms for data at rest and all communications are secured in transit via HTTPS.
Phishing Simulator Data	Microsoft Azure encryption mechanisms for data at rest and all communications are secured in transit via HTTPS.

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 service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
• Terranova Worldwide Corporation (www.terranovasecurity.com)	• Business Contact Information • Phishing Simulator Data	• Cisco utilizes Terranova Worldwide Corporation. (www.terranovasecurity.com) as a third-party provider for Cisco Security Awareness. Where Cisco refers to Cisco employees in this data sheet, this includes authorized employees of Terranova Worldwide Corporation.	• Microsoft Azure Canada, EU
• Microsoft Azure	• Business Contact Information Phishing Simulator Data	Cisco Security Awareness is hosted in Canada or EU. Please see https://azure.microsoft.com/en-ca/overview/trusted-cloud/compliance/ for information on Azure compliance/certifications.	• Canada • EU (Ireland)
• SendGrid	• Business Contact Information	These services are located in the United States and are used for sending email messages to participants of awareness activities.	• USA
• JangoSMTP	• Business Contact Information	These services are located in the United States and are used for sending phishing simulator email messages to participants.	• USA
• Sendinblue	• Business Contact Information	These services are located in France and are used for sending email messages to participants of awareness and phishing activities in Europe.	• EU (France)
• MicroAge	• Business Contact Information	Managed Support Services for Servers.	• Canada

9. 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.

10. 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. 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. See Section 3, above.

In addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security.

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