



Webex, Meet Safe and Secure

April 2020

“Privacy is a fundamental human right, and we need security and transparency to protect it.”



Chuck Robbins
Chairman and CEO, Cisco
February 7, 2019

Webex

Three Security Principals:

Privacy, Security and Transparency

- Committed to the **privacy** of your data
- Secure by **design** and by **default**
- Transparent about security

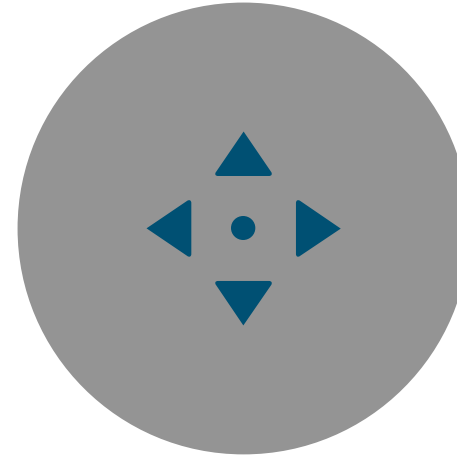
Cisco Data Protection Program



Customer &
Market Expectations



Competitive
Differentiation



Risk Landscape



Legal
Obligations

Strategic Considerations

Privacy at Cisco



Data Protection
Program



International Transfers of
Personal Data



Third-Party
Reviews

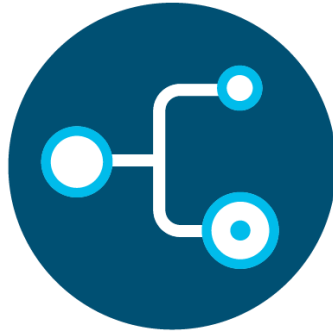
More information on:

<https://www.cisco.com/c/en/us/about/trust-center.html>
<https://youprotect.cisco.com/>

Data protection & privacy



Policies and
Standards



Identification and
Classification



Data Risk and
Organizational Maturity



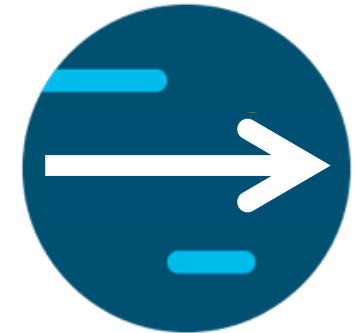
Incident
Response



Oversight and
Enforcement



Awareness and
Education



Security & Privacy
By Design

International transfers of personal data



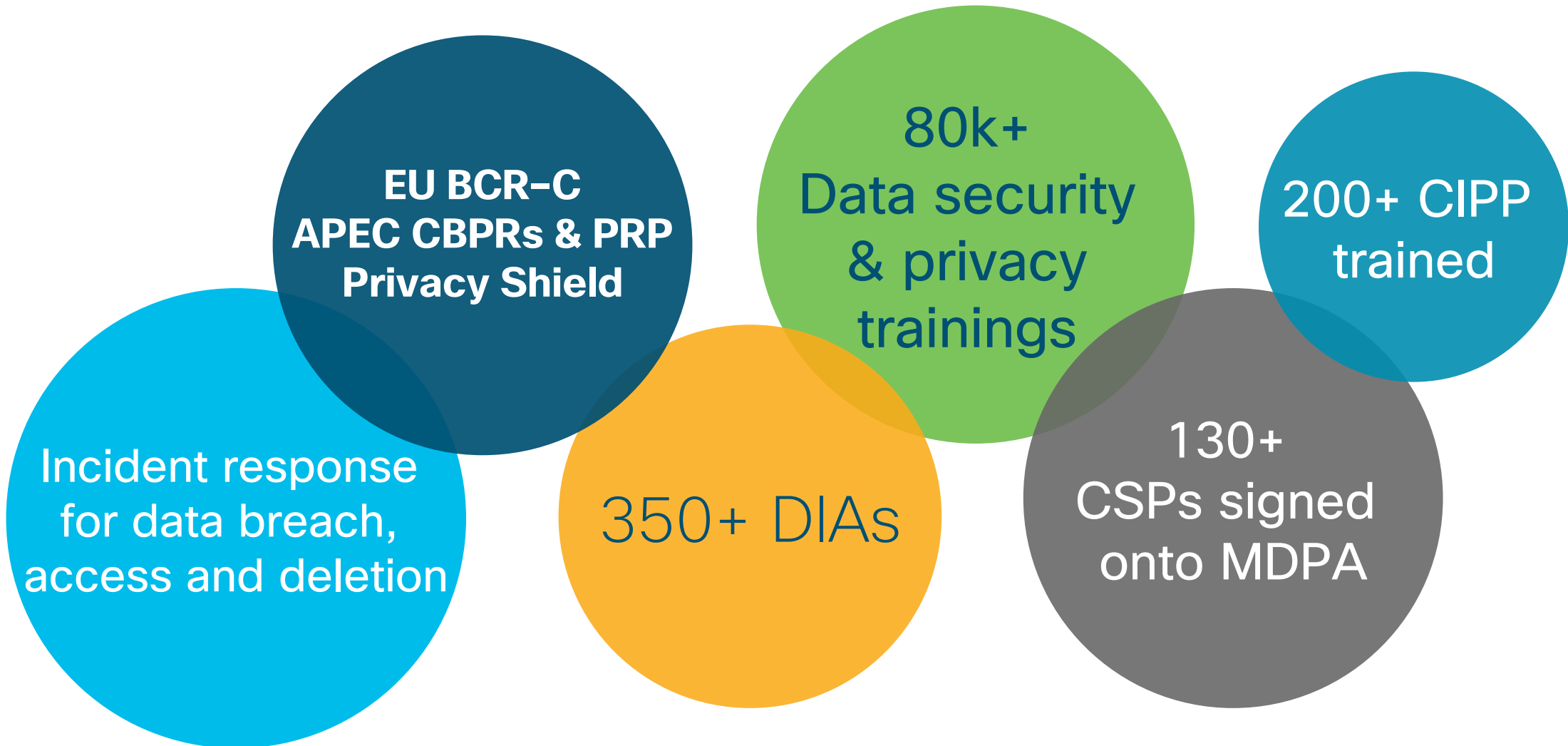
Certified under the [EU-US](#) and Swiss-US [Privacy Shield](#) frameworks

[EU Standard Contractual Clauses](#) for cloud offerings

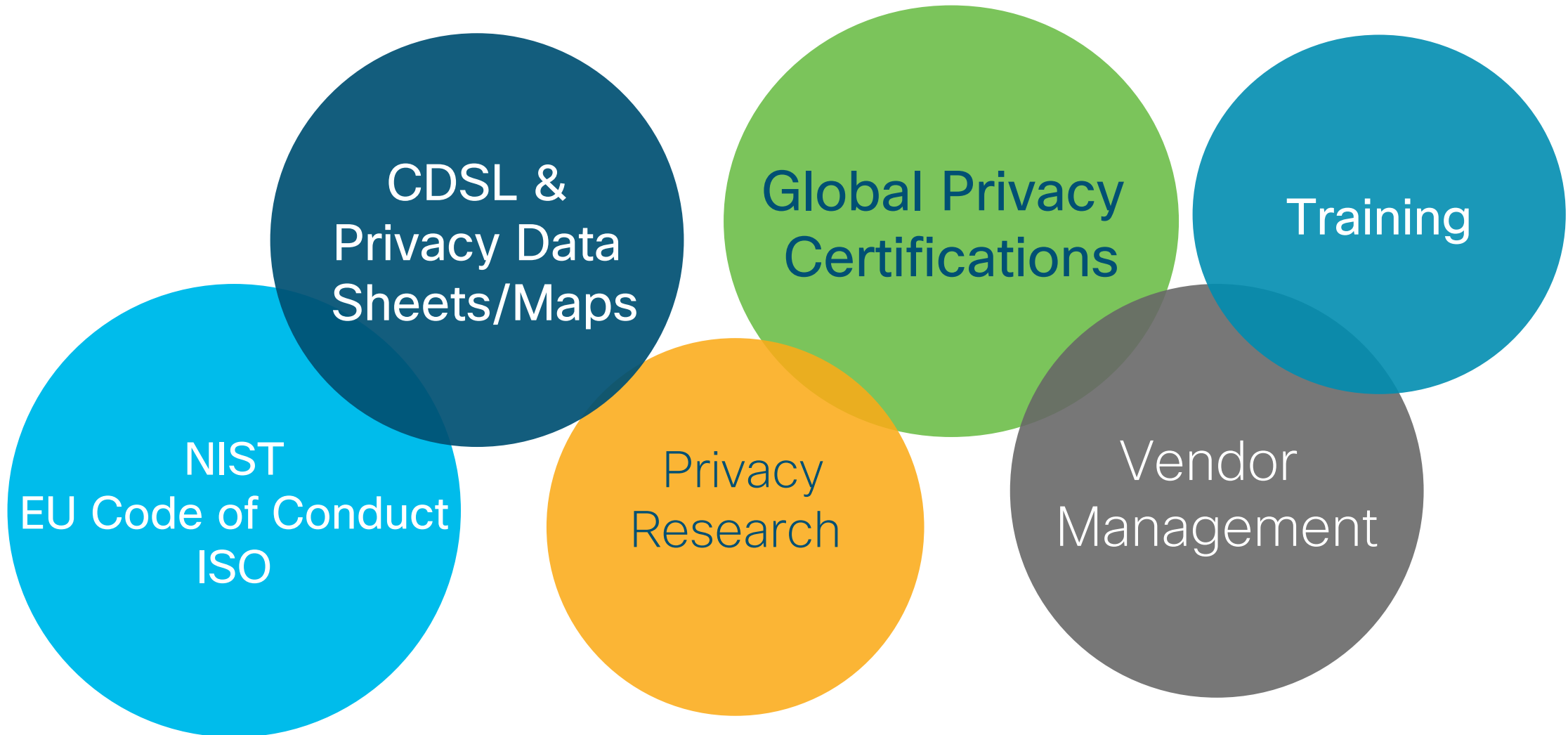
Certified under APEC Cross-Border Privacy Rules system (controller and processors)

[EU Binding Corporate Rules](#)

Cisco in numbers



Our competitive advantage



Third-Party Reviews



Cisco Webex Certifications

ISO 27001
SOC2 type II
ISO 27017-018
C5



Cisco Services Certification

ISO 27001



EU Cloud Code of Conduct



- Art. 40 GDPR
- Accountability tools which set out specific data protection rules for categories of controllers and processors (EDPB Guidelines)
- Concretises requirements of processors in a cloud environment
- GDPR offers signatories of a Code the legal benefit to prove compliance

Privacy by default & design



Secure Development Lifecycle



Embed privacy engineering into the secure development and operational lifecycle



19 Privacy Data Maps

[illegible]

Privacy Data Sheet

Cisco Webex Meetings

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

1. Overview of Cisco Webex Meetings Capabilities

Cisco Webex Meetings (the "Service" or "Webex Meetings") is a cloud-based web and video conferencing solution made available by Cisco to companies or persons ("Customers," "you," or "your") who purchase it for use by their authorized users (each, a "user"). The Service enables global employees and virtual teams to collaborate in real time from anywhere, anytime, on any mobile device or video system as though they were working in the same room. Solutions include meetings, events, training, and support services. For more information regarding the People Insights feature for Cisco Webex Meetings, please see Addendum One below. For a detailed overview of the Service, please visit the Cisco Web Conferencing [homepage](#).

Because the Service enables collaboration among its users, you may be asked to provide your personal data in order to use the Service. The following paragraphs describe Cisco's processing of personal data in connection with the delivery of the Service, the location and transfers of that data, and how it is secured in accordance with privacy principles, laws, and regulations. If you choose to purchase the Service, you will need to disclose personal data to Cisco in order to use it. Cisco will use your personal data consistent with this Privacy Data Sheet. Note that this Privacy Data Sheet is a supplement to the [Cisco Privacy Statement](#).

2. Personal Data Processing

The Service allows users to instantly connect in a way that is as personal as a face-to-face meeting. The meeting host has the option to record meetings and all users have the option to upload and preserve files shared during and outside of meetings, which may be discoverable in a legal matter. The meeting host should inform all meeting attendees prior to recording if the meeting host intends to record the meeting. If the meeting host opts not to preserve the meeting content, it disappears from the Webex Meetings platform immediately after the meeting concludes. If you are a user and your employer is the Customer that purchased the Service, all of the information described in this Privacy Data Sheet is accessible by your employer and is subject to your employer's policies regarding access, use, monitoring, deletion, preservation, and export of information associated with the Service.

Similarly, if users participate in meetings hosted by users in other companies, the meeting host will control any meeting recordings or files shared during the meeting, which will be subject to the host's corporate policies regarding access, use, monitoring, deletion, preservation, and export of information. Note, Cisco has no control over, and is not responsible or liable for the privacy of any information that you have shared with others. Even after you remove information from the Webex Meetings platform, copies of that information may remain viewable elsewhere to the extent it has been shared with others.

This Privacy Data Sheet covers the Cisco Webex Meetings Suite, Cisco Webex Events, and Cisco Webex Training. If you use the Service together with Cisco Webex Teams, see the Cisco Webex Teams Privacy Data Sheet (available on [The Cisco Trust Center](#)) for descriptions of the data that may be collected and processed in connection with those services. The table below lists the categories of personal data used by the Service and describe why we process such data.

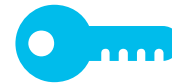
Key Differentiators



Clearly **identifies purpose** for processing



Specific information on **where data** is stored/transferred (e.g. data centers)



Protection of sensitive data at rest through service **encryptions**



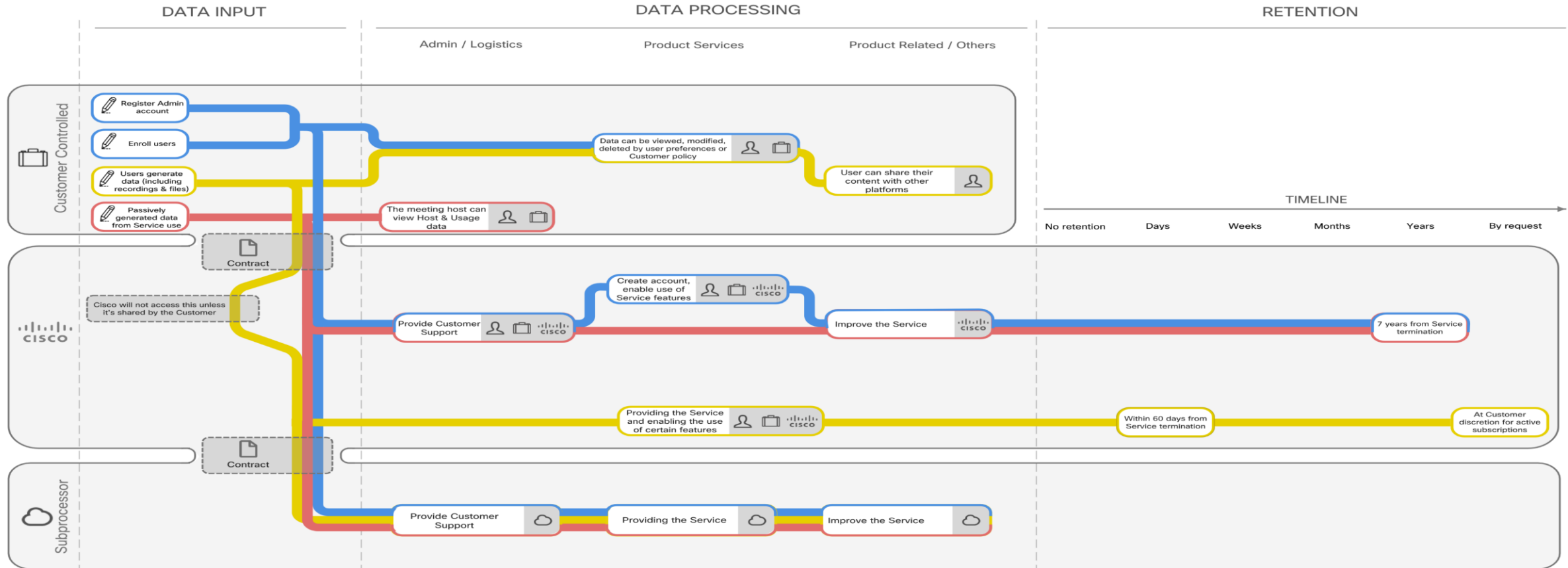
User-generated information is **automatically deleted** within 60 days after termination of service

Privacy Data Maps

All privacy data sheets and data maps are publicly accessible on trust.cisco.com

WebEx Meetings

Data Flow Process



Personal Data Processing

Registration data

Name, Email Address, Password, Public IP Address, Browser, Phone Number (optional), Mailing Address (optional), Avatar (optional), Billing Information

Hosting and usage data

IP Address, User Agent Identifier, Hardware Type, Operating System Type and Version, Client Version, IP Addresses Along the Network Path, MAC Address of Your Endpoint (as applicable), Service Version, Actions Taken, Meeting Session Information (title, date and time, frequency, average and actual duration, quantity, quality, network activity, network connectivity), Number of Meetings, Number of Screen-Sharing and Non-Screen Sharing Sessions, Number of Participants, Host Name, Screen Resolution, Join Method, Performance/Troubleshooting/Diagnostics Information

User-generated data

Meetings and Call Recordings, Uploaded Files

Access Key

Icons on the right show WHO has access
Details of access are listed in the datasheet

What's being done

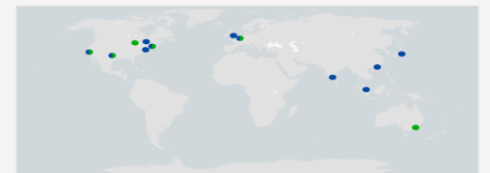


Columns show category of purpose
Row show who controls the data
Text inside indicates purpose

Cross-border transfers

• Data center locations
Amsterdam, Netherlands
Bangalore, India
California, USA
Hong Kong, China
London, UK
New York, USA
Singapore, Singapore
Texas, USA
Tokyo, Japan
Toronto, Canada
Virginia, USA

• Internet Point of Presence (IPoP) locations
Amsterdam, Netherlands
California, USA
Illinois, USA
New York, USA
Sydney, Australia
Texas, USA



What happens to User Generated Content?



Webex Teams



- Enterprise Default Retention Period : Indefinite (Subject to storage limits)
- **Configurable Retention Period** : 1 to 120 months (pro pack)
- Consumer Account Default Retention Period : 6 months

Cisco Webex Teams Data

Set an retention period for your system. There is a limit on how much data can be removed from the system. Once the limit is reached, older data will be removed.

Past 3 months
Past 6 months
Past 12 months
Past 24 months
Past 60 months

☐ Custom retention time between 1 and 120 months

months

Webex Meetings



- **No in-meeting content stored upon meeting termination**
- Event Data records for reporting and billing purposes
- Recordings stored in the cloud optionally , can be deleted **anytime**
- Bulk delete, policy

☐ Support Recording Auto-Deletion Policy

Recording Retention Days:

WebEx Administration

Recording Management

Manage recorded meetings, including reassignment and deletion.

Move Recording to Trash

The selected recording will be moved to trash and immediately become inaccessible to user. Do you want to continue?

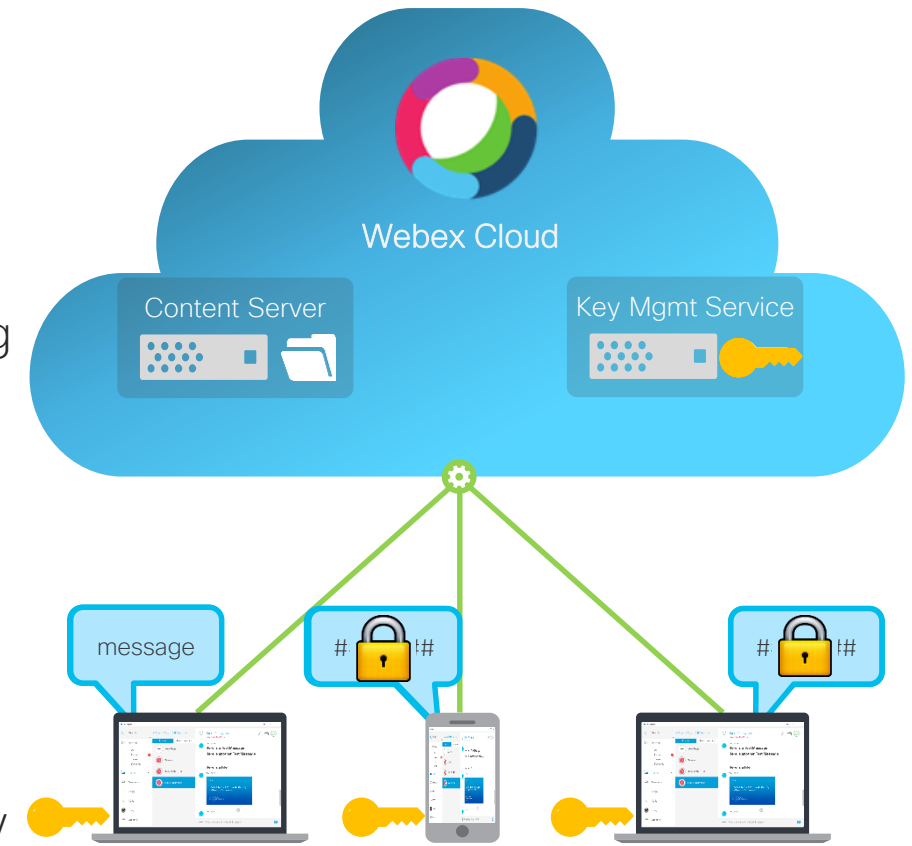
All recordings in trash will be available for recovery for the next 30 days. Owners will not be able to restore recordings moved to trash.

Name	File Size	Duration	Service	Owner	Encrypted	Date Created
No recorded meetings found.						

Webex Teams Security.....by design!



- **Encryption of data at rest** :
 - On your Apps and Devices and In the Webex Cloud
- **Encryption of data in transit**:
 - SRTP for media, TLS for signaling
- **End to End Encryption of User Generated Content (messages, files)**
 - Messages and files encrypted by the Webex Teams App before being sent to the cloud. A unique AES-256-GCM key used per space
- **Search on encrypted Teams content**
- **Logical and physical** separation of functional components into micro services: content, keys, indexer...
- Webex Teams Key server can be deployed **on premises**
- **Identity Services** hold real user Identity. All the other components only use 128-bit Universally Unique Identifier (UUID) : **pseudonymization**



AES256-GCM cipher used for content encryption

Meetings Security...Encryption

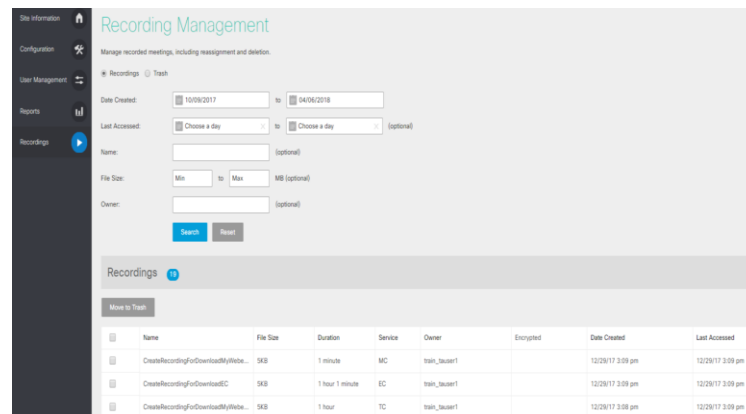


Security by default

All communications between Webex Applications, Webex Room devices and the Webex Cloud occur over TLS encrypted channels. Once a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted.

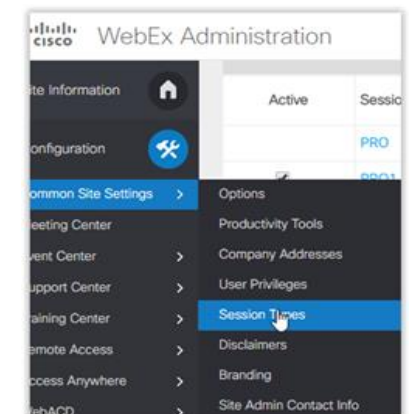
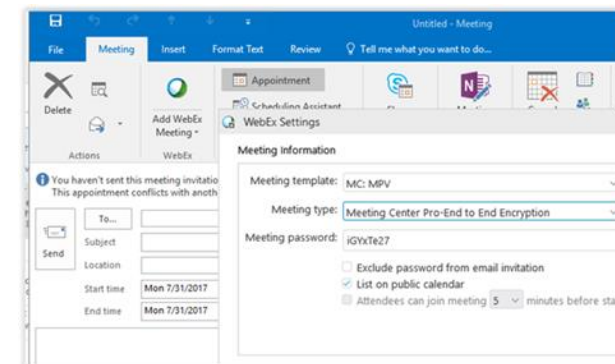
Recordings

- Recording are automatically **encrypted with AES 256** bit keys and stored in encrypted form (since WBS32.13)



End to End Encrypted Meetings

- For businesses requiring a higher level of security, Cisco Webex also provides end-to-end encryption. With this option, Cisco Webex Cloud does not decrypt the media streams.
- See [Webex Meeting Security whitepaper](#)



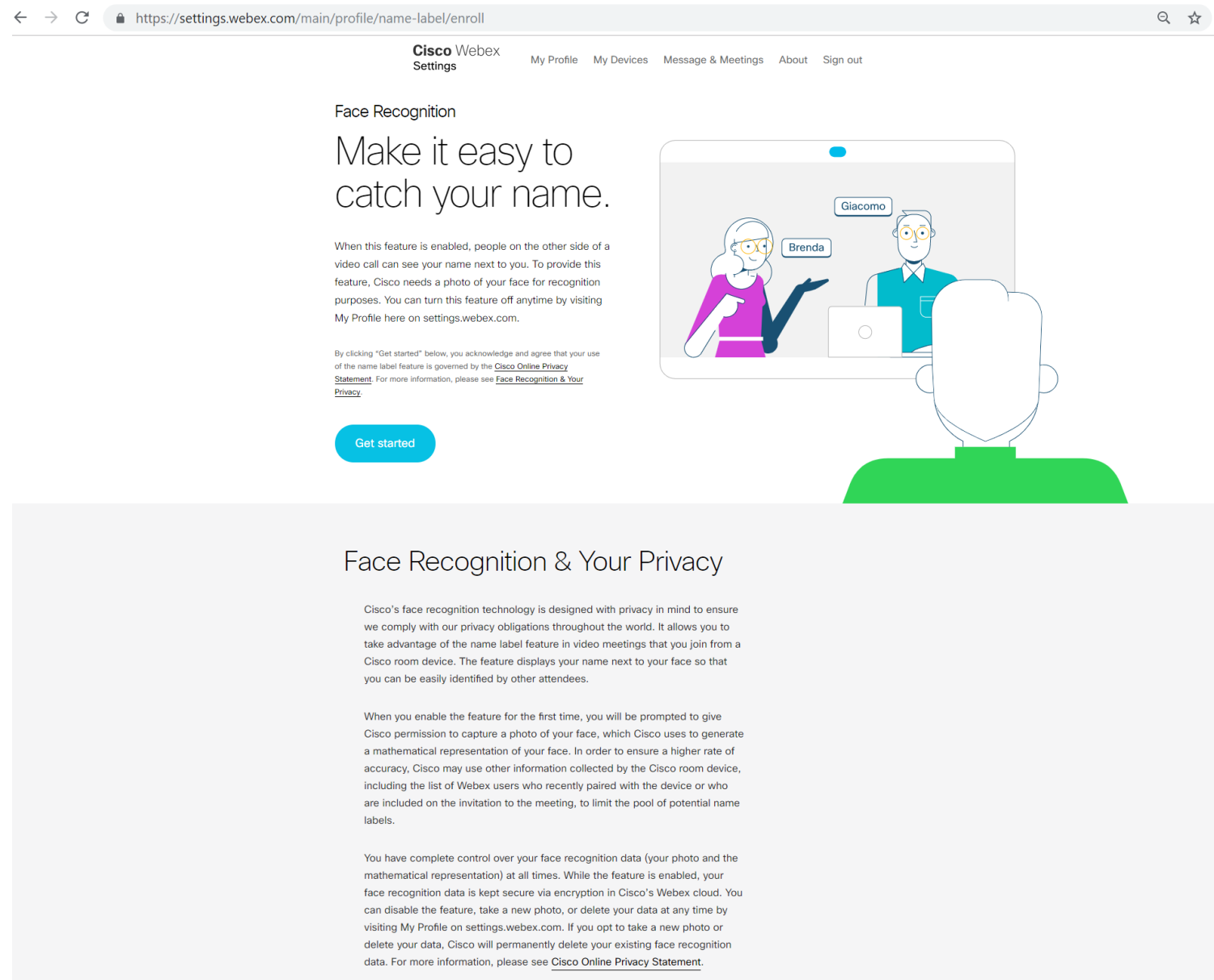
Webex: Cognitive Collaboration

[Data Handling and Privacy for Cognitive Collaboration White Paper](#)

Cognitive Collaboration examples:
Speech Recognition
Face Recognition

Cognitive Collaboration Data Privacy Principles :

- Don't retain data if you don't have to
- If you do, keep it for the shortest possible time
- Be transparent about data usage
- Provide Deletion Controls
- Empower end users



The screenshot shows the Cisco Webex Settings page for Face Recognition enrollment. The browser address bar displays <https://settings.webex.com/main/profile/name-label/enroll>. The page header includes the Cisco Webex Settings logo and navigation links: My Profile, My Devices, Message & Meetings, About, and Sign out. The main heading is "Face Recognition" with the subheading "Make it easy to catch your name." Below this, a paragraph explains that when enabled, people on the other side of a video call can see your name next to you, and that Cisco needs a photo of your face for recognition purposes. A "Get started" button is prominently displayed. To the right, an illustration shows a video call interface with two participants, Brenda and Giacomo, and a third person's back view in the foreground. Below the illustration, a section titled "Face Recognition & Your Privacy" provides detailed information about Cisco's privacy obligations, the data collected, and the user's control over their face recognition data.

Face Recognition

Make it easy to catch your name.

When this feature is enabled, people on the other side of a video call can see your name next to you. To provide this feature, Cisco needs a photo of your face for recognition purposes. You can turn this feature off anytime by visiting My Profile here on settings.webex.com.

By clicking "Get started" below, you acknowledge and agree that your use of the name label feature is governed by the [Cisco Online Privacy Statement](#). For more information, please see [Face Recognition & Your Privacy](#).

[Get started](#)

Face Recognition & Your Privacy

Cisco's face recognition technology is designed with privacy in mind to ensure we comply with our privacy obligations throughout the world. It allows you to take advantage of the name label feature in video meetings that you join from a Cisco room device. The feature displays your name next to your face so that you can be easily identified by other attendees.

When you enable the feature for the first time, you will be prompted to give Cisco permission to capture a photo of your face, which Cisco uses to generate a mathematical representation of your face. In order to ensure a higher rate of accuracy, Cisco may use other information collected by the Cisco room device, including the list of Webex users who recently paired with the device or who are included on the invitation to the meeting, to limit the pool of potential name labels.

You have complete control over your face recognition data (your photo and the mathematical representation) at all times. While the feature is enabled, your face recognition data is kept secure via encryption in Cisco's Webex cloud. You can disable the feature, take a new photo, or delete your data at any time by visiting My Profile on settings.webex.com. If you opt to take a new photo or delete your data, Cisco will permanently delete your existing face recognition data. For more information, please see [Cisco Online Privacy Statement](#).

From Privacy to Profit & Importance of Privacy



From Privacy to Profit: Achieving Positive Returns on Privacy Investments

Cisco Data Privacy Benchmark Study 2020



For every \$100 spent on Privacy, the average organization is getting \$270 in benefits



Over 70% are reporting significant privacy benefits in areas such as efficiency and company attractiveness



Organizations that are more “accountable” were twice as likely to be breach-free and had other security and financial benefits.



Eighty-two percent of organizations believe privacy certifications are important factors in the buying process today.



Key Takeaway: Data Privacy is delivering significant financial benefits beyond compliance.

Consumer Privacy Survey

The growing imperative of getting data privacy right



84% of consumers care for their own data and data of others



80% see **data privacy** as an important factor influencing their buying decisions



48% indicated they had already **switched companies** or providers because of their data policies or data sharing practices



87% of companies are experiencing **sales delays** caused by their **customers' privacy concerns**



97% of companies were **realizing benefits** such as competitive advantage or investor appeal from their **privacy investments**



Data Incident Response



Submitting a data loss incident

Prompt response to a data incident is essential to minimize the impact to Cisco, customers, and partners

How to submit data loss incident:

- 1 Visit clip.cisco.com to open a CLIP case for Data Protection and Privacy
- 2 Complete the form with as much information as you can provide
- 3 Submit the form within the tool and await follow up from member of Incident Response team

Examples of data incidents:

- Sending customer information to wrong email address
- Posting confidential content on a public website (e.g. YouTube) without proper access controls
- Using an unapproved collaboration tool in the cloud and sharing confidential information
- Sending the wrong attachment with classified information, including customer information

Keeping Cisco Safe



Gold Winner of Info Security
PG's Global Excellence
Awards®



Cyber Information Security Risk
Mitigation Marketing Campaign



Winner of the NCSA Cyber
Safety in the Workplace Award

ISO 27701



- **Privacy extension** of ISO27001 (required), same frequency
- Defines processes and provides guidance for **protecting PII on an ongoing basis**: similar to ISO 27001 but for privacy
- First ISO to reference external material :the appendix includes a section on **mapping to the GDPR articles** on controller and processor
- *“Organizations needs to bring trust to their DPA, partner and customers Such a standard will contribute strongly to this trust”* CNIL, French DPA
- Over time controllers, (sub) processors will use **same controls** which will make things easier for audits, contracts, documentation...

For more information: <https://trustportal.cisco.com/>