Cisco Webex and GDPR

Thomas Flambeaux, Cisco Webex privacy consultant
tflambea@cisco.com
Data Protection officer certified: CIPP-E, DP Institute and PECB

Abstract

- In this session, we will first do a refresh on the General Data Protection Regulation (GDPR), as well as updates on some recent developments: SCHREMS II, European Data Protection Board (EDPB) guidelines, the Google Analytics case.

- Second, we will cover what Cisco Webex offers to help our customers ensure GDPR compliance in terms of data localization and migration, privacy features, processes, privacy engineering and certifications.

The objective of this session is for attendees to get comfortable deploying Cisco Webex solutions when it comes to their obligations towards GDPR as data controllers.

Agenda

- GDPR Refresh and SCHREMS II Ruling

- Cisco Webex Assets

- Conclusion

GDPR Refresh and SCHREMS II Ruling

Foundation of Privacy in European Union

- Universal Declaration of Human Rights (1948) …non (legally) binding, not a treaty

- European Convention on Human rights (1953)…very few countries ratified

- Council of Europe Convention on Automatic Processing of Personal information (1981)

  1st legally binding text in Data Protection area ….few states signed

- Data Protection and free flow directive (1995)

- General Data protection Regulation (2018)

GDPR Key Points

- Harmonization of the EU privacy landscape and catch up on technologies

- No obligations to store personal data in EU

- NEW: portability right, accountability (register) also for processors, Privacy by Design and Default

	Date	Amount	Company
LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.
IRELAND	2022-09-05	405,000,000	Meta Platforms, Inc.
IRELAND	2023-01-04	390,000,000	Meta Platforms Ireland Limited
IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited
IRELAND	2021-09-02	225,000,000	WhatsApp Ireland Ltd.
FRANCE	2021-12-31	90,000,000	Google LLC
FRANCE	2021-12-31	60,000,000	Facebook Ireland Ltd.
FRANCE	2021-12-31	60,000,000	Google Ireland Ltd.
FRANCE	2019-01-21	50,000,000	Google LLC
GERMANY	2020-10-01	35,258,708	H&M Hennes & Mauritz Online Shop A.B. & Co. KG

Terminology

Data Transfers from the European Economic Area (EEA)

1) Adequacy decision
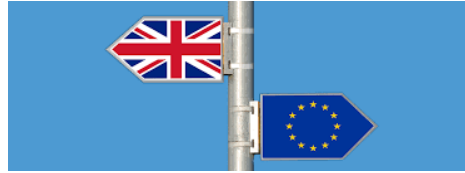
2) Appropriate safeguards

Model Clauses: Template issued by the European Commission

- ✓ Cisco offers model clauses as part of the Master Data Protection Agreement (MDPA)

Binding Corporate Rules (BCR) – Internal rules for transfers of personal data within the same corporate group

- ✓ Cisco owns BCR for controllers and applied for BCR for Processors

SCHREMS II Ruling

- The EU–US Privacy Shield invalidated due to access to EU citizens data by US authorities was disproportionate and subjects lacked a redress mechanism

- The US Privacy Shield no longer has an adequacy decision

- Data transferred to 3rd party countries via model clauses or BCRs with supplementary measures documented by the European Data Protection Board (EDPB) in spring 2021

Google Analytics

- Austrian DPA declared that NETDOKTOR in violation of the GDPR by using Google Analytics in January 2022

- Google supplementary measures (transparency reports, encryption...), were insufficient, to prevent re-identification, by Google or the U.S. government.

- DPAs rejected risk-based approach ...that the GDPR recognizes in recital 76 *"The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined"*

- Only the technical inability to access personal data in plain is adequate under problematic foreign laws, CNIL (France) proposed use of a proxy and 15 "sovereign" alternatives

EU-US Data Privacy Framework

- President Biden signed the Executive Order 14086 (October 2022) which implements:
  - ✓ Binding safeguards to limit access by data by US intelligence authorities to what is necessary and proportionate to protect national security
  - ✓ Establishment of an independent and impartial redress mechanism

- Adequacy drafted by the European Commission -> for EU Member States vote (by summer 2023)

- "Adequacy based on this Executive order will NOT satisfy the European Court of Justice" Max Schrems ……. SCHREMS III ?

Future of Uncertainty and Contradictions

- Adequacy decision for the US?

- DPA decisions (not risks-based) and EDPB guidelines (localization) "vs" the spirit of GDPR.
  EU Court of Justice (in SCHREMS II ruling) also did not require that additional safeguards provide a 100 % guarantee access can never occur....

- Sovereign offerings?

Cisco Webex Assets

Cisco Webex and Supplementary Safeguards?

Aligned with EDPB guidelines and included in our Master Data Protection Agreement:

- Localization

- Transparency

- Certifications

- Technical safeguards

Localization: Webex Data Residency Program

European customers data stored and processed in the European Union (Frankfurt and Amsterdam)

- Analytics, Identity, Content

- Meetings, messaging and calling

- Billing is now stored in EU

- Migration programs

See PSO-COL-2311 Webex achieves full data residency in EU

Localization: In Meeting Traffic (media)

Private meeting on video mesh

- Media kept on-premise, signaling to cloud

- Can cascade among nodes

- Only scheduled meetings

This is a private meeting. You can join it only from the Webex Teams app or from an authenticated video system in the host organization.

Disable Global Distributed meeting

- On request (Webex Customer success team)

- No overflow to other regions possible !

CISCO *Live!*

Transparency: Cisco Reports and Principles

- Trustportal.cisco.com

- Every 6 months since 2014!

- Notifies customer unless applicable law prohibits it, challenges requests that prohibit notification

- Challenges any request that would put Cisco in breach of privacy laws in another country except if disclosing data will prevent imminent death or serious physical harm to an individual.

From Jan 2022	To Jun 2022

All Countries

Total Data Demands

71

- 0
- 1-25
- 25-50
- 50+

Responses

Disclosed 45

Rejected 13   No data found 13

Content Demands
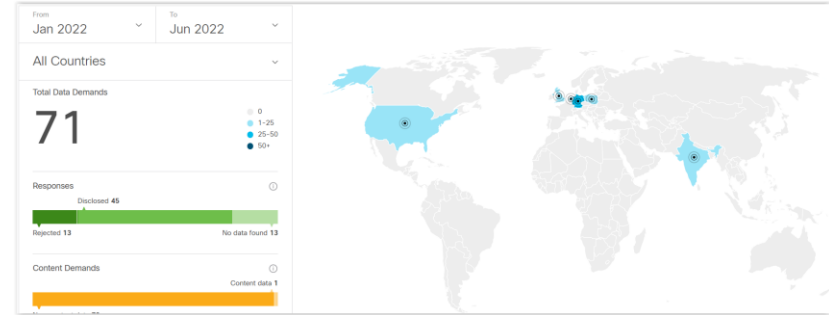
Content data 1

Percent Disclosed - US and International Demands Combined

Jan 1st-June 30th, 2022	Total	% Disclosed
Content Demands Received	1	0%
Non-Content Demands Received	70[2]	64%

CISCO Live!

Transparency: Privacy Data Sheets/Maps

Personal data and Webex in great detail

Since early 2018

Latest Update

- From 3 years to 13 months retention policy for the host and usage data of Webex Meetings at the org level

- Breakdown of data Webex processes as a controller and as a processor

Certifications (EU relevant ones)

	Meetings	Messaging	Calling	Contact Center
ISO 27001 and extensions 27017/27018 and 27701	✅	✅	✅	✅
SOC 2 Type II (report under NDA)	✅	✅	✅	✅
C5 (Germany)	✅	✅	✅	✅
ENS (Spain)	✅	✅	✅	
AGID (Italy)	✅	✅	✅	
EU Cloud Code of Conduct (Level 2)	✅	✅	✅	

"Such standards will bring trust to DPA, partner and customers"

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

ISO
ISO 27701

Very useful building block in a data-protection certification mechanism" **iapp**

EU Cloud Code of Conduct

- Uncertainty for companies due to numerous GDPR vague provisions
  An approved code of conduct (Art. 40 GDPR) is a solution, optional though

- Concretize requirements of GDPR article 28 for practical implementation
  within the cloud – must at all time comply with all the controls

- First code approved by EDPB and the EU commission, in May 2021

Cisco Webex meetings, messaging and calling adhere to the EU CCoC Level 2

Cloud CoC Content and Benefits

- More than 80 controls on contract, liability, law enforcement requests, complaint, audits, breaches, confidentiality, lawful processing, sub processors ….for the best practices

- Reduces risk of being sued and enables trust in products and services: best certification you can currently get in terms of GDPR compliance

- Additional module for data transfer (in progress, to be approved by Belgian data protection authority and EDPB) to help controller to assess the privacy laws of destination countries

Privacy by design

Webex Meetings <u>does not</u>:

- Produce decisions that would result in legal or other significant effects impacting the rights of data subjects based solely by automated means.
- Sell your personal data.
- Serve advertisements on our platform.
- Track your usage or content for advertising purposes.
- Monitor or interfere with you your meeting traffic or content.
- Monitor or track user geolocation.

Pseudonymization

Technical measures

What is the point of localizing, having certifications, being transparent…if you can easily experience a breach?

Technical measures only will ultimately please data protection authorities (Google Analytics)

End to End Encryption for Meetings

- Not enabled by default

- Up to 1000 attendees (January 2023)

- Webex cannot decipher in meeting traffic

- Video endpoints support

- NSA evaluation on encryption: Webex ranked 1st

- Coming for 1-1 calls in first half 2023

See BRKCOL-2876 Securing Webex Meetings
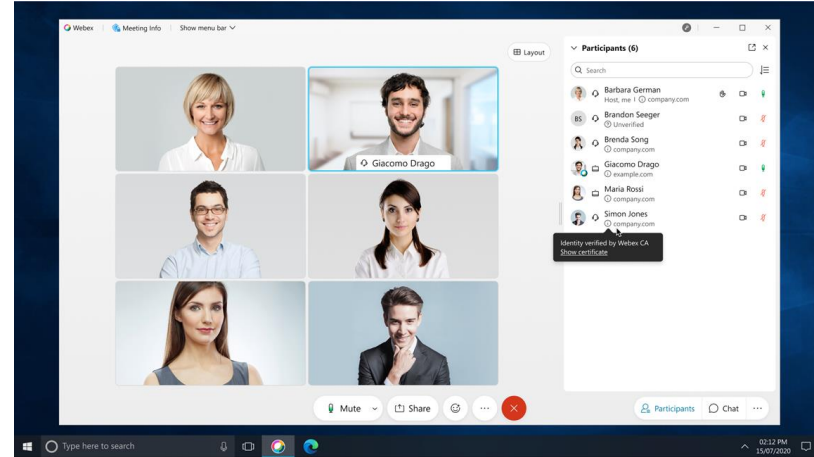
Single Sign-on (SSO) and Events APIs

Stronger authentication with SSO

- Multi-factor authentication

- Restricted set of devices

- Restricted access from corporate network

Identity as a Service

okta   ORACLE

Azure   G Suite

Centrify   Ping Identity

salesforce   onelogin
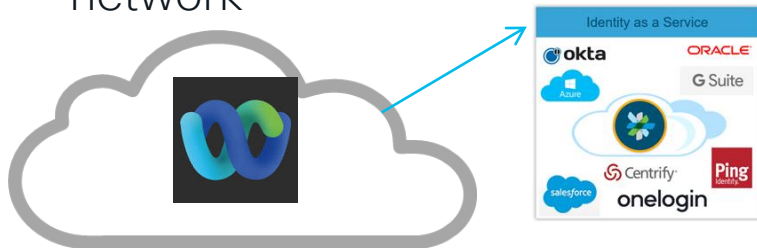
See BRKCOL-2007 Authentication, Authorization and Provisioning for Cisco Collaboration

Events APIs for webex messaging

- Events and content polled to monitor and correct user behavior, preventing the loss of sensitive data

- Lately extended to recordi and transcripts

THETALAKE   VERINT verba

cisco Cisco Cloudlock   netskope

Retention periods updated

	Standard Pack	Pro Pack
Default retention period set to a year (if unspecified)	Admin can change, from 1 day (messaging) or 1 week (meetings) to a year maximum	Customer can change from 1 week to 10 years
Put in effect	January 2023	March 2023

Deleted recordings purged after 30 days (soft delete) except if a retention period applies (hard delete)
Retention policy do not apply to recordings on legal-hold

Internal Webex Meeting Access Controls

Option 1: No external users can join Personal Room meetings and Scheduled meetings by default

Option 2: No external users can join Personal Room meetings

        Any user can join scheduled meetings

External meetings access controls

Granularity: These controls can be applied to all users , groups (templates) or individual user

Collaboration Restrictions for employees

- **Control user's experience** (20+ features toggles) for external or internal meetings for org/group/users

- **Users joining external meeting will be notified** if policy applies

- Use of personal email? Guests? **Add a token (containing Org ID) to company devices** so that restrictions apply anyway

Audio watermarking (April 2023)

- Encode meetings audio signal with unique inaudible identifiers for each participant, so leaked recordings can be easily traced back to the source.

- Option when scheduling, free of charge, supports E2E meetings

- Upload the media file to Control Hub (self-serve) and see the source: meeting, participant, and device thanks to this tagging
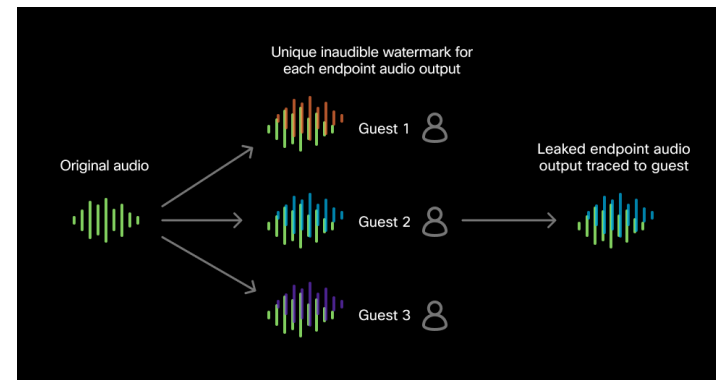
Privacy: Edit your name in meetings


- Anyone can edit his/her own name , (co)hosts can edit any attendee name

- Last edited name is seen in-meeting and post-meeting as well: chat, devices, recordings ,reports ..)

- Witness joining a meeting hosted by a court, attendee with specific title-degree…(Doctor, Minister…)
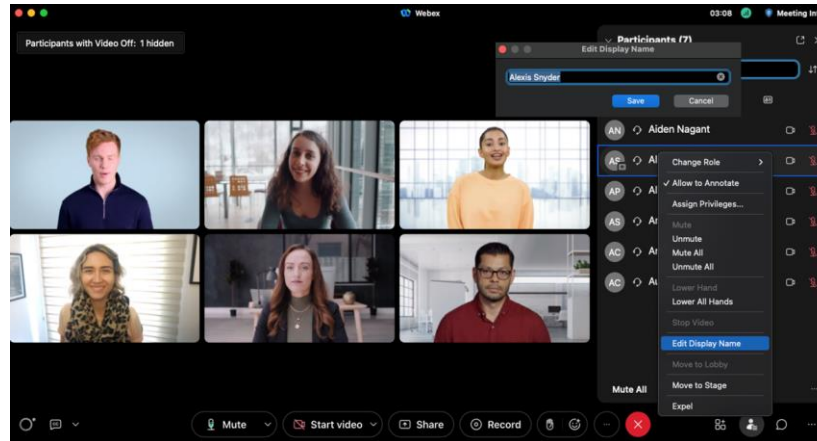
Privacy: user Host and usage information deletion

- About metadata (no E2E encryption), not about user account or conte...

- Must be a full administrator of the organization
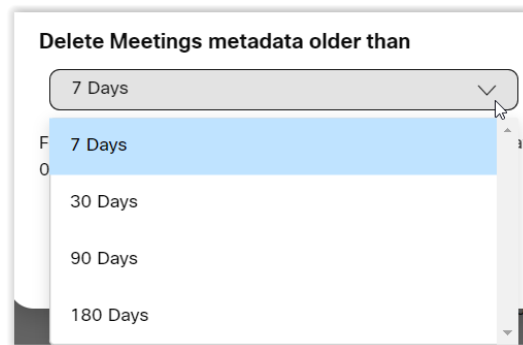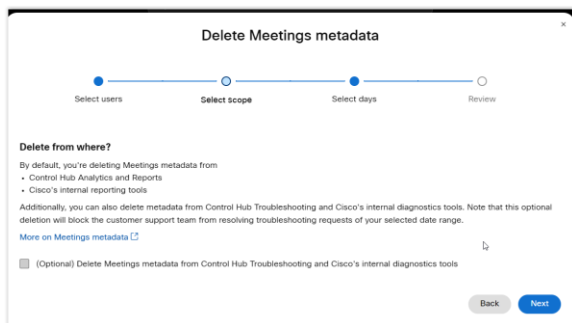
More controls for customers in the context of the GDPR when it comes to data subject requests

Conclusion

Cisco Webex and GDPR Recap

Many features, certifications and resources to assist you with your obligations as data controllers for GDPR compliance

Resources

Cisco 2023 Data Privacy Benchmark

- Based on responses from security/privacy professionals from over 3000 organizations; anonymous

- Information on key privacy issues for organizations:

  - The importance of Transparency

  - Impact of privacy laws

  - Trust and Artificial Intelligence

  - Data Localization Requirements

- Available on trust.cisco.com

Business benefits of investing in data privacy management programs

Business Benefits of Investing in
Data Privacy Management Programs

January 2023

- Joint study by CIPL and the Privacy Center of Excellence at Cisco

- 36 CIPL members participated

- Insight into how leading global companies realize value from privacy management programs

- 56% of survey participants experienced at least $1m in benefit from investing in privacy last year

- 28% experienced over $10m in benefit

- Only 8% reported not experiencing any monetary benefit from privacy investments

- Download: https://bit.ly/3GnvkD6

REFERENCES

- Webex localization https://blog.webex.com/hybrid-work/webex-strengthens-eu-data-residency/

- Data deletion https://help.webex.com/en-us/article/l4pqoi/Delete-Webex-Meetings-host-and-usage-information-of-users-in-Control-Hub

- Data migration https://help.webex.com/en-us/article/2d73oy/Migrate-your-organization%E2%80%99s-Webex-data-to-the-European-Union-data-center-inControl-Hub

- NYOB statement on US executive order https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law

- Coming audio watermarking https://blog.webex.com/hybrid-work/webex-audio-watermarking/

- Cisco BCR-C https://www.cisco.com/c/en/us/about/trust-center/data-protection-and-privacy-policy.html

- Cisco Vulnerability policy https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html

- Cisco Webex AI and privacy https://blog.webex.com/workplace-transformation/webex-advanced-collaboration-features/

- GDPR fines https://www.enforcementtracker.com/

- NSA comparing web conferencing encryption https://media.defense.gov/2020/Aug/14/2002477670/-1/-1/0/CSI_%20SELECTING_AND_USING_COLLABORATION_SERVICES_SECURELY_SHORT_20200814.PDF

- Cisco blog on CoC https://blogs.cisco.com/security/webex-by-cisco-earns-adherence-to-the-eu-cloud-code-of-conduct

- Cisco principles for data access https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-principled-approach-to-government-requests-for-data.pdf

- MLS vetted https://hal.laas.fr/INRIA/hal-02425229

- Coming privacy by design ISO https://www.itworldcanada.com/article/privacy-by-design-to-become-an-iso-standard-next-month/521415

- EDPB guidelines https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

- NYOB 101 complaints https://noyb.eu/en/eu-us-transfers-complaint-overview

- Post SCHREMS II FAQs https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-faq-intl-transfer-personal-data-post-schrems-II.pdf
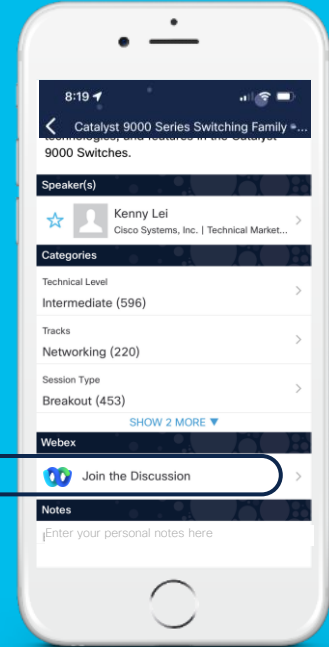
Cisco Webex App

Questions?
Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click "Join the Discussion"
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
until February 24, 2023.

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.

- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at
https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

Thank you

Thomas Flambeaux, Cisco Webex privacy consultant
tflambea@cisco.com

CISCO *Live!*

ALL IN