
cisco
You make possible

Cisco Webex and GDPR

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

BRKCOL-1797

cisco Live!
Barcelona | January 27-31, 2020

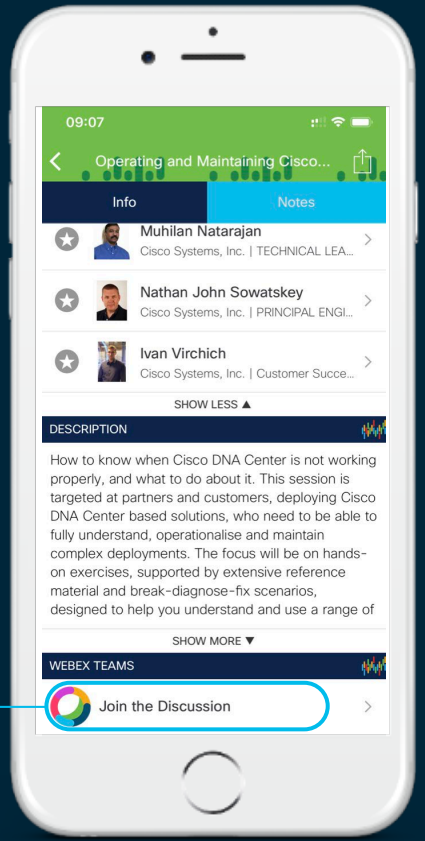
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

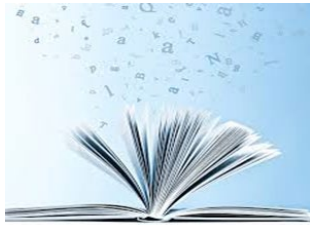


Agenda

- GDPR refresh
- GDPR what is new and next?
- Cisco Webex and GDPR
- Conclusion

GDPR Refresh

Terminology 1/2



- *Regulations* have binding legal force throughout every Member State and enter into force on a set date in all the Member States.
- *Directive* describes results to be achieved but each Member State is free to decide how to transpose into national laws.
- *Controller*: Entity that determines the purposes and means of the processing of personal data, ultimately responsible for compliance
- *Processor*: engaged by controller on his behalf to process data on given purpose (storage, encryption..), collection, accessing,.... or destruction
- *Data subject* : Individual Controller/Processor get personal data from

Terminology 2/2

- *Personal Data*: Any information identifying (directly or indirectly) a natural person Also known as Personal identifiable information (PII)

- *DPA* : Data protection authority, public entity enforcing data protection laws Handle subject complaints , advise and authorize processing revealing high risks , audit controllers and processors, corrective powers: warnings, ban processing, suspend transfers , order to comply with subject requests

- *DPO* : Data protection officer: coordinator , not liable

- *EEA*: European economic area, includes EU countries and also Iceland, Liechtenstein and Norway. It allows them to be part of the EU's single market

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 PII (1981)

Principles (see appendix) in 1995 directive and the GDPR

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

- Data Protection and free flow directive (1995)

Processing must be necessary, adequacy for data transfer, extra requirements for special categories

Applies to controllers established in EU, representative for those processing in EU , Mandates DPA in each member state

General Data Protection Regulation

GDPR replaced the 1995 directive and its local implementations

- Harmonization
- Time to catch up on technology!
- Better protect EU citizens privacy

TECH

Apple apologizes for listening to Siri conversations

PUBLISHED WED, AUG 28 2019-11:10 AM EDT | UPDATED WED, AUG 28 2019-11:47 AM EDT

On Facebook, 65% of French people targeted on their sexual, political or religious orientation

By Elisa Braun | Update the 05/03/2018 at 13:30 / published the 05/03/2018 at 11:51

A study conducted by Spanish researchers analyzes the extent of this practice

GDPR takeaways

- No obligations to store personal data in European Union
- NEW: portability right, accountability (register), Data protection by design and default…
- Data breaches to be notified to lead DPA within 72 hours
- More obligations for Processors

- Fines

4 % of turnover (or 20 million euros) for infringements to principles, subject rights, transfers…

2 % (or 10 million euros) anything else including data breaches

- Member states can derogate (56 articles) and implement exemptions (appendix)

Cross-border Transfers (1/2): Adequacy decision

Transferring PII outside EEA is prohibited without an adequate level of protection

- Commission will assess: Rule of law, human rights, fundamental freedoms, DPA independency and review the decision every 4 years
- USA, New Zealand, Japan (first since GDPR)….: have adequacy decision

For the USA the adequacy is achieved via Privacy Shield

- Framework between EU commission and US department of commerce
- Replaced Safe Harbor ,declared illegal by European Court of Justice
- Self registration for US companies (about 5 000) , privacy policies to be published
- Annual review by the EU commission

Cross-border Transfers (2/2)

Not on the list, not trusting Privacy shield to transfer to the USA

Model Clauses (aka Standard Contractual Clauses)

- Description of organizational security
- Template from EU commission, if using your own need for a DPA approval
- Annexes describing the data exporter and importer, processing activities, safeguards
- Once signed , the company outside EEA is considered safe to receive personal data

Binding Corporate Rules

Internal rules to transfer personal data within the same corporate group to entities worldwide.

- Considered as the highest standard :appropriate safeguards outside EU, adequate, aligned with EU standards
- To be approved by all DPAs in the European Union

GDPR what is new and next?

GDPR potential evaluation

Article 97 instructs the Commission, by May 25, 2020, to evaluate and eventually amend GDPR

Comments from member states delegation ,October 2019:

- Priority to revise child consent
- Obligation to handle complaints (Article 77) obstructs the DPA efficiency
- Suggested candidates for an adequacy finding: Singapore, Colombia, Mexico, South Africa, Serbia and Dubai International Financial Centre
- Higher fines not based on the turnover of only the undertaking concerned, but of the entire group example in appendix

GDPR business impact and requests

The multistakeholder expert group identified challenges for the commission:

- Need exception for small and medium businesses
- Notice has to be both concise and comprehensive…
- Documentation efforts, extra costs: policies-DPO-subject access requests (SAR)-staff trainings-external counsel, legacy IT systems revamp…
- Need EDPB guidance for unfounded-excessive and time consuming SAR: looking in back ups, legacy systems, all emails, video footage…
- GDPR and new technologies? Blockchain, big data or Artificial Intelligence

European Data Protection Board

- Members from DPAs and EU commission
- Assure consistency by publishing guidelines : consent, portability, accreditation of certification bodies , territorial scope . Goal is to clarify GDPR
- Lead efforts for EU-wide codes (per vertical) and certification ART 40-43
- Review adequacy decision and send back opinion to commission
- Binding decision if dispute arises between DPAs and if DPA does not request a consistency opinion issued by the EDPB

Is encrypted data still personal data?

- Is encrypted data still personal for a party that does not hold the decryption key?
- Need for EDPB guidance on encryption technologies and key storage methods that, if used, would make the data no longer personal if not in possession of the key
- Encryption is neither pseudonymization nor anonymization but could we consider encrypted data without the key as anonymized and with the key as pseudonymized?
- Anonymized data is out of the GDPR scope

Recital 26: anonymized data is no longer person data because it has been rendered unidentifiable. Pseudonymized data, however, should be considered identifiable where it could be attributable to a natural person

BREXIT

Once the United Kingdom leaves the EU, it becomes a third party country

In case of a no deal ,there will be a transition period to reach adequacy, adequacy decision to be made by the end of 2020

The British DPA (ICO) has indicated that they will

1. Allow entities to continue to use EU Model Clauses
2. Recognize Binding Corporate Rules certifications.

Data Protection bill passed on May 23rd 2018 aligned with GDPR

Virtual assistant

- The Hamburg DPA issued Google with legal requirements for its Google Assistant to comply with GDPR .Those assistants are often incorrectly activated and that transparent information about that risk is therefore required to process audio data. The legal basis is to obtain an informed consent of the user.

- The Luxembourg DPA had "raised privacy concerns" last summer with Amazon over the retention of audio files recorded on its Alexa voice assistant

Model clauses

Max Schrems 2 court case

- Does FISA -the U.S. law on the access of national security agencies to non nationals PIIs- break EU data protection laws?
- The advocate General's (AG) opinion declared them valid and stressed the "soundness" of the safeguards to compensate for the inadequacy of the 3rd country's laws or legal system Ruling in early 2020

The EU commission will update model clauses to align them with GDPR and introduce new requirements in relation to government access: companies will have to mitigate those impacts.

First draft in January for open consultation

Privacy shield

- In 2018 European Parliament voted a resolution calling its suspension complaining about the lack of proportionality of US government access to EU citizens data
- In the 2019 review , the commission *noted that the US continues to ensure an adequate level of protection for PII transferred from the EU to the participating US companies and stressed the positive appointments of key oversight and redress bodies, such as the Ombudsperson*

- Quadrature du net case , ruling in 2020

Companies denounced by Snowden are certified…

In the Max Schreems 2 case, the AG *"doubts" the ability of the Ombudsperson mechanism* and has *"certain doubts" as to conformity of the Privacy Shield* decision to Article 45 (transfers on the basis of an adequacy decision)

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…

Cisco Webex and GDPR

GDPR recommendations

- Pseudonymization and encryption of personal data
- Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing system and services
- Minimization and retention
- No explicit requirements for products and services but encourages data protection by design and by default
- Approved transfer mechanisms

Governance...Cisco Privacy data sheets 1/2

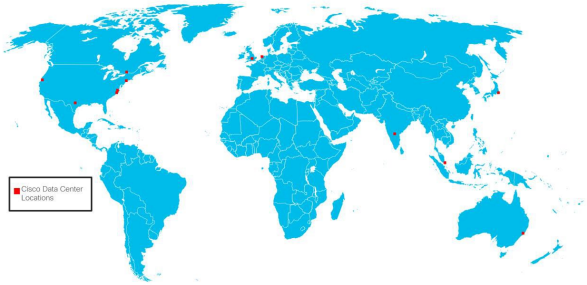
Crucial for the data controller :Accountability

Register , should DPA investigate

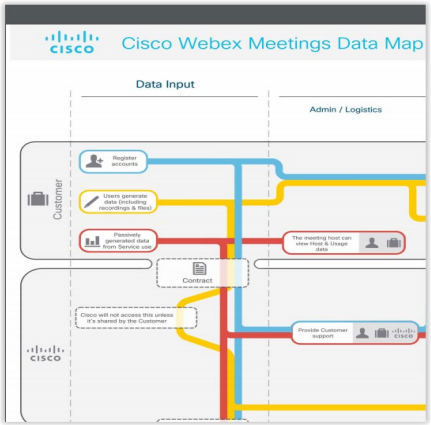
- What personal information is collected?
- For how long? What purpose? Who has access?

Subject access requests

- Right to delete and Portability

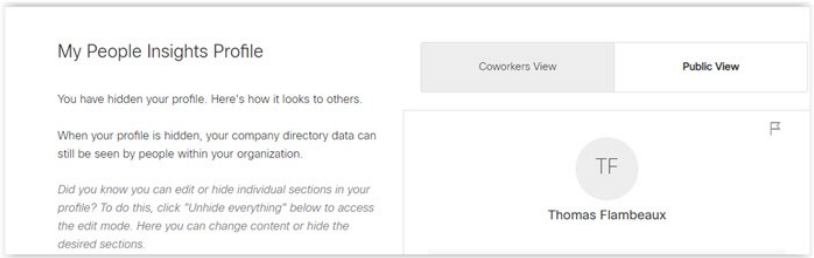


- Data center locations , transfer mechanisms
- Certifications , encryption overview
- Reduce sales cycle and help feature adoption



Governance...Cisco Privacy data sheets 2/2

- Regular updates: People Insights displays publicly available information and company directory data. Users can edit or hide its content (people.webex.com) Company directory data is only visible to people within your organization.



- Just updated with facial recognition, attendee data, billing data

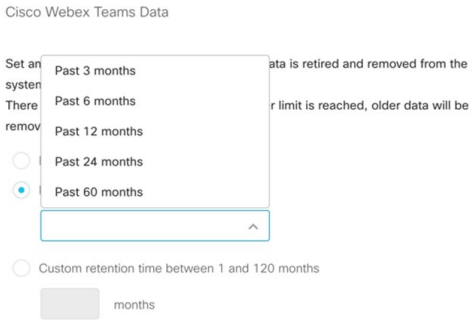
Effectiveness of measures....Cisco Secure Development Lifecycle

- Product security baseline :requirements , list in appendix
- Data flows identification ,threat identifications and mitigation
- Integrity and authenticity (FIPS 140-3 requirements)
- Best Practices Guidelines for each OS ,signed images , no backdoor
- Obtaining security fixes via contract from 3rd parties
- Robustness check: network protocols ,file systems, digital media
- Duplicate Hacker Attacks using a set of open source tools

Minimization ....Retention policy

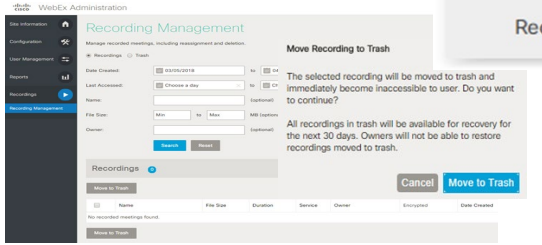
Webex Teams

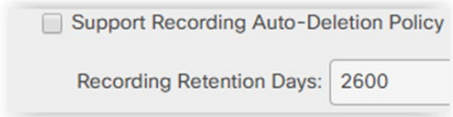
- Default Retention Period : Indefinite (Subject to storage limits)
- Configurable Retention Period : 1 to 120 months (pro pack)



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

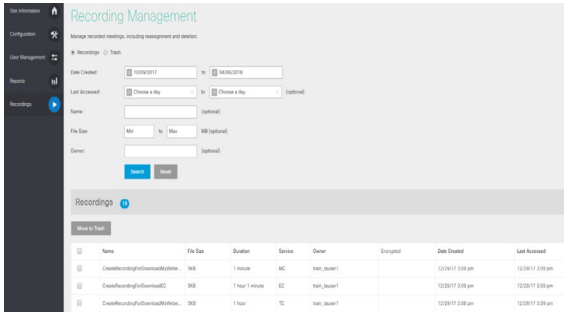




Security...Encryption

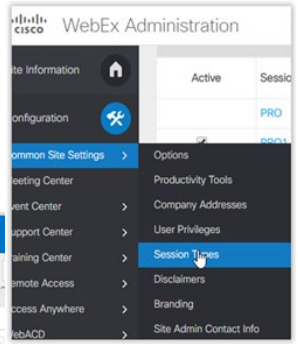
Recordings

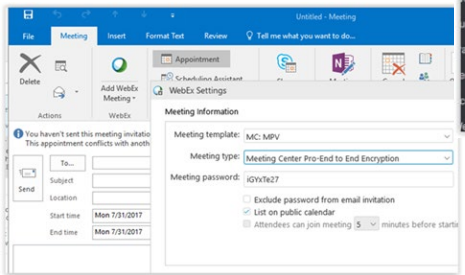
- Recording are automatically encrypted with AES 256 bit keys and stored in encrypted form (since WBS32.13)



Meetings

- Limitations no support for: Join before host, cloud based recordings ,web app (webRTC) and video endpoints
- Supports Mobile clients
- Session type (op-request)





Security.....by design!

- Encryption at rest : on device, on server
- In transit: media
- Any content: messages, files , AES256 in GCM mode
- Search on encrypted content
- Key server can be deployed on premise

- Logical and physical separation of functional components into micro services: content, keys, indexer...
- Identity Services holding real user Identity. All the other components only use 128-bit Universally Unique Identifier (UUID) : pseudonymization

See BRKCOL-2795 - Webex Teams Security in depth

Incident.....Cisco Product Security Incident Response Team : PSIRT

- Manages the receipt, investigation, and public reporting of security vulnerability information related to Cisco products

Cisco.com	http://www.cisco.com/security/
Email	cust-security-announce@cisco.com
RSS	http://tools.cisco.com/security/center/rss.x?i=44
Cisco PSIRT openVuln API	https://developer.cisco.com/site/PSIRT/
Cisco Notification Service	http://www.cisco.com/cisco/support/notifications.html

The European DPAs made clarifications on **data breaches**

- State of the art algorithm+ key not compromised

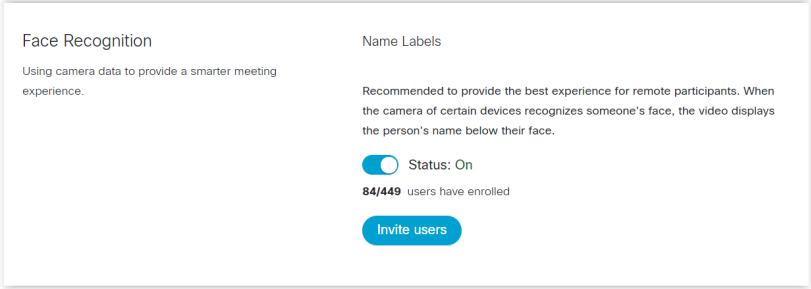
→ No need to notify data subjects

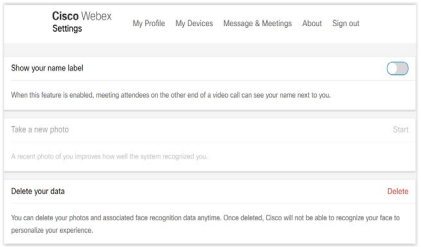
- State of the art algorithm+ key not compromised + proper backup

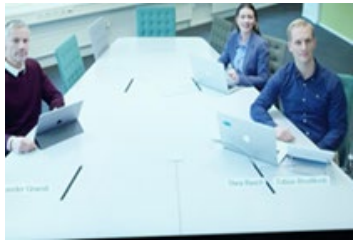
→ No need to notify the DPA !!

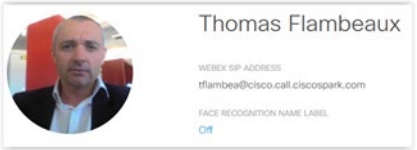
Facial recognition.....Explicit consent

- Disabled by default
- Once administrator enables it, the user can then opt-in to enable the Feature
- Must take a picture at opt-in.
- Feature vector (image based) are used for a given org only and retained as long as the feature is enabled and can be deleted at any time by user.
- Feature vectors for all users are deleted upon customer's discontinuation of the service.









Prevent Data leakage.....Single Sign-On

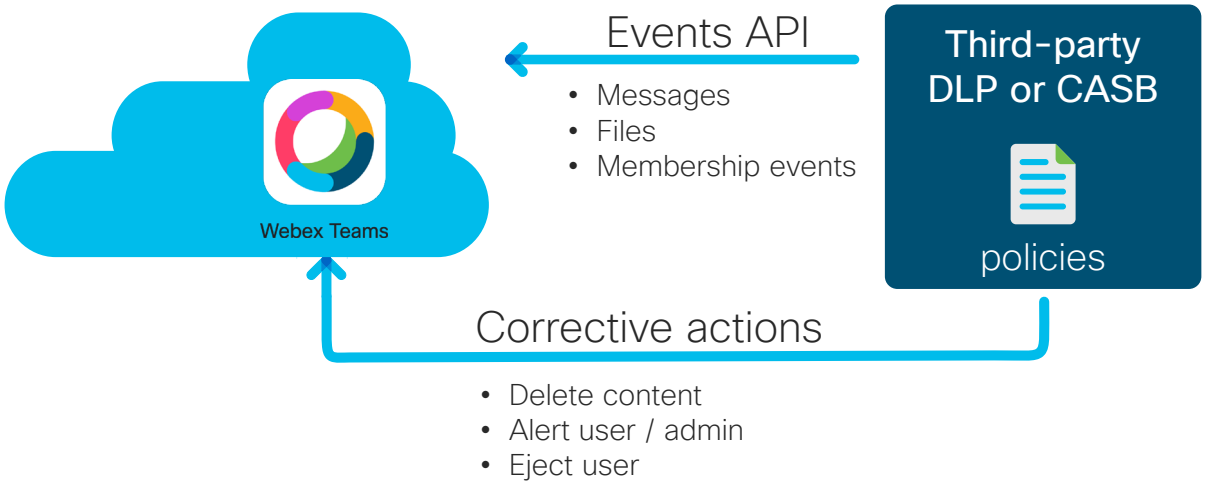
Stronger authentication with SSO

- Restricted set of devices
- Restricted access from corporate network
- Multi-factor authentication :Cisco DUO

See BRKUCC-3444 - Authentication and Authorization in Collaboration Deployments

Prevent Data leakage……Events APIs

- Expand policies (email, instant messaging…) into messaging
- DLP: Data loss Protection , CASB: Cloud Access Security Broker



skyhigh

cisco Cisco Cloudlock

paloalto NETWORKS

Symantec

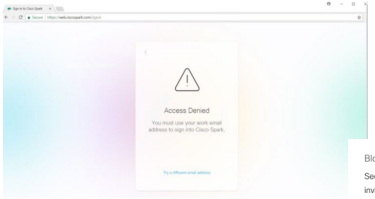
AGAT

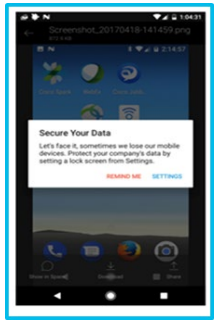
VERINT verba

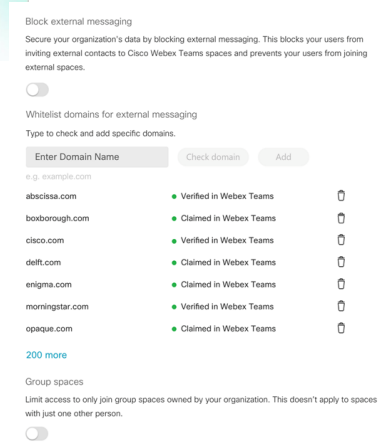
netskope

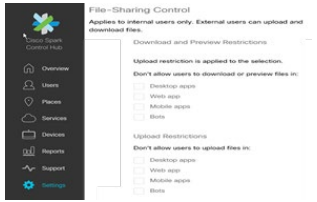
Data leakage…Administrator controls

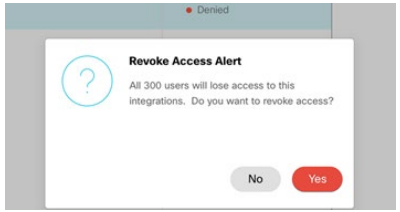
- Block non corporate accounts from company network (TLS inspection)
- Block external communications Messages, inviting external: only for new spaces
- Enforce PIN lock
- Integration management; policy and capability to allow/deny specific integrations
- Disable file preview (download only)
- File sharing controls (per platform)





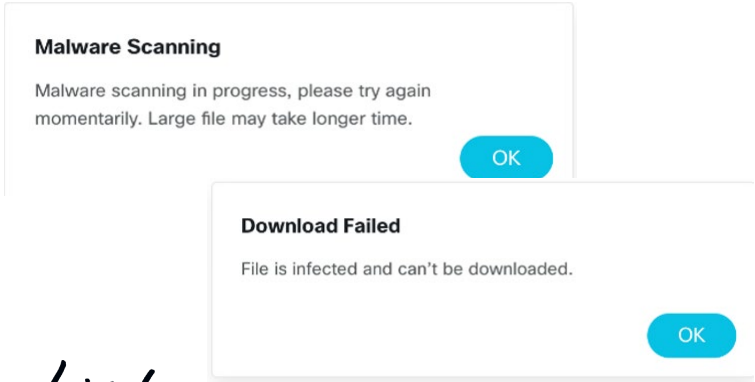


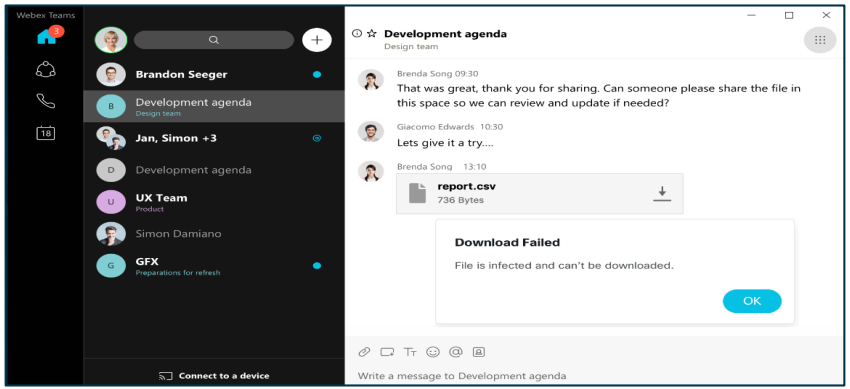




Data leakage.....Anti-Virus and malware

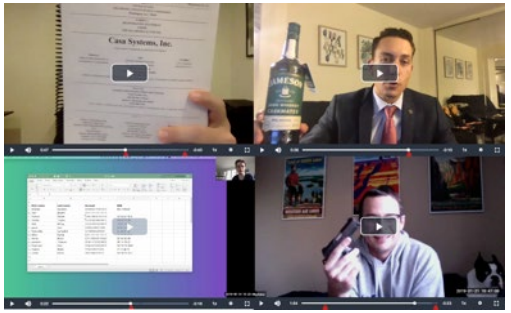
- Scanning and blocking of infected files and unsafe URL's
- Administrator control to turn-off and turn-on scanning , Scan logs (CSV)

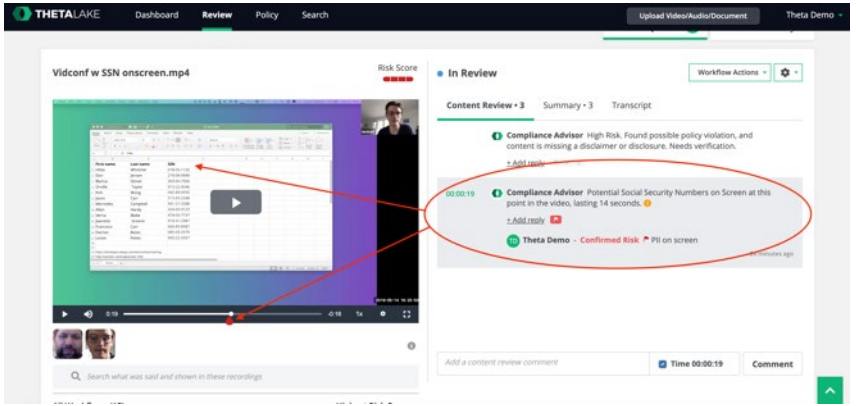




Data leakage…..Recordings compliance

- Platform to manage, detect and flag compliance issues.
- Automatically analyzes shown, shared, spoken, written, and whiteboard content when a new Webex Meeting recording is created.





THETALAKE

cisco Live!

Cisco Webex certifications

- ISO 27001:**consistent model** to implement, operate, monitor, review, maintain and improve an Information Security Management System (ISMS)
- ISO 27017: Security controls in the cloud / ISO 27018 :Privacy and PII controls in the cloud

- SOC 2 Type 2 reports (audit report with auditor testing and results)

Security, availability, processing integrity, confidentiality and privacy controls

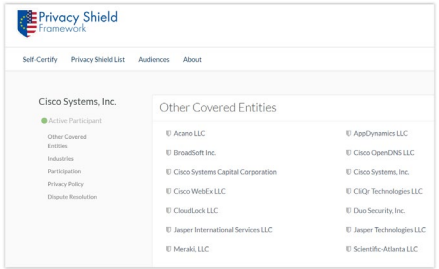
SOC 3 public report provides the system description and auditor opinion

- C5 certified (Kind of combination of ISO27001 and SOC 2 audit)

All those certifications on trustportal.cisco.com , audit reports provided under non disclosure agreement (NDA)

Cisco cross Border transfers

- Privacy Shield certified



- Model Clauses part of the master data protection agreement

- European DPAs have approved Cisco's Controller BCRs: they reviewed our global privacy policies and procedures and determined that Cisco protects customer and HR personal data in accordance with EU requirements (namely GDPR) wherever they flow within our large global organization

Sub-processors

Sub-processors provide the same level of data protection and information security that you can expect from Cisco.

We do not rent or sell your information.

Current list of Cisco Webex sub-processors with access to personal data can be provided upon request.

In our master Data protection agreement for suppliers, sub processors have obligations to embrace our model clauses

Conclusion

Cisco Webex and GDPR recap

Many features , procedures , certifications and resources to assist customers with their obligations as data controllers

CiscoPSIRT
Product Security Incident Response Team

Resources

References 1/2

- Cisco Webex Teams security and privacy https://help.webex.com/en-us/nv2hm53/Cisco-Webex-Teams-Security-and-Privacy
- List of DPA in EU http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm
- Countries with adequate level of personal data protection http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
- Safe Harbor declared illegal following Max Schrems case https://www.youtube.com/watch?v=_Ebh8X5nzac
- Global Site Backup FAQ https://collaborationhelp.cisco.com/article/en-us/DOC-19437
- ICO guidelines on Brexit https://ico.org.uk/for-organisations/data-protection-and-brexit/
- Cisco Webex ISO certifications

References 2/2

- Security FAQ Webex teams https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Webex-Teams-Security-Frequently-Asked-Questions.pdf
- Cisco Webex security white paper https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf
- Cisco Webex SSO https://collaborationhelp.cisco.com/article/en-us/g5ey83
- Cisco MDPA for customers (including Model Clauses) https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf
- Cisco MDPA for suppliers https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/mdpa-for-supplier-portal.pdf
- List of companies with BCRs https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#listofcompanies
- GDPR fines tracker http://www.enforcementtracker.com/
- EDPB blog on Facial recognition https://edps.europa.eu/node/5551

Appendix

- Slide 7:Principles: lawfulness-fairness-accuracy-retention-purpose-appropriate safeguards- subject rights-sensitive PII processing prohibited
- Slide 9:Derogation for :Processing of sensitive data; data processing in the context of employment; conducting PIAs; appropriate safeguards for data protection for archiving purposes in the public interest, scientific or historical research, or statistical purposes; access rights; automated decision-making and profiling; and data protection officers
- Slide 14: New fine system proposed by Germany: In the case of the company mentioned in the previous example, with an annual turnover of EUR 90 billion and a "daily rate" of 250 million euros, the authorities find a minor infringement, i.e., the least severe category with an associated multiplier range of one to four. The authority then multiplies the "daily rate" of 250 million euros by the one to four multiplier range. This results in a regular fine corridor of 250 million to 1 billion euros and therefore a median value of 625 million euros.
- Slide 27 CSDL Product security baselines

Administrative access security-logging and auditing-application security-operational process – Authentication and authorization –Privacy and data security – boot and system integrity – session management – cryptographic support – threat surface reduction – development process – traffic and protocol protection – hosted services hardening – vulnerability management – web security

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on 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 Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

You make **possible**