European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

RECORD NO: 26

WEB CONFERENCING

Record 26 of processing operation "Web conferencing"	
Date of last update	27/2/24
Name and contact details of controller	ENISA, Corporate Support Services Unit, IT, it-helpdesk [at] enisa.europa.eu
Name and contact details of DPO	dataprotection [at] enisa.europa.eu
Name and contact details of Joint Controller	N/A
Name and contact details of processor	CISCO - for the provision of the Webex teleconference platform. ENISA has purchased the service under the European Commission's DG DIGIT SIDE II Framework Contract. A specific Data Processing Agreement (DPA) has been signed between ENISA and the processor CISCO. Microsoft for the Provision of MS Teams service. ENISA has purchased the service under the DIGIT Framework Contract DI-7880. The data controller of the processing operation is ENISA – Corporate Support Services/IT Sector.The data processor is Microsoft Ireland operations Ltd that provides the Microsoft Teams platform via an Interinstitutional Licensing Agreement (ILA) with the European Commission (to which ENISA is also party). A specific Data Processing Agreement has been signed between the European and Microsoft under the ILA that is also applicable for the processing of personal data via the Teams platform.
Purpose of the processing	To support ENISA's internal and external communication, as well as the organisation of ENISA's online conferences and events. In particular, two web conferencing tools are used: i)Cisco Webex online service. ii) Microsoft Teams. The tools are in more detail used for the following purposes: a) Internal and external communication (Webex and MS Teams): the purpose of the processing operation is to allow communication and collaboration between the Agency staff (calls, meetings, chats), Commission staff and externals (contractors, researchers etc.). b) b)Federation with other EU Agencies (MS Teams): the purpose of the processing operation is to allow communication and collaboration between the Agency staff and staff in other EU Agencies. A directory of contact data is made available, so that ENISA staff can contact colleagues to MS Teams. c) Federation with public providers (MS Teams): the purpose of the processing operation is to allow communication and collaboration between the Agency staff and external MS Teams contacts. A directory of contact data is made available, so that ENISA staff can contact colleagues to MS Teams. d) Organisation of online conferences and events (only Webex and MS Teams): the purpose of the processing is to support the organisation of ENISA's online events and conferences.
Description of data subjects	ENISA staff, staff of federated partners with whom ENISA has an agreement, external (to ENISA) collaborators, contractors, etc. communicating with ENISA staff members, participants in ENISA's online conferences, events, webinars, meetings (upon invitation)

Description of data categories	For Webex: a) Host registration information: name, email address password. These data are processed by CISCO (processor) in order to provide for the registration of the host in a specific meeting. b) Meeting host information: meeting host, meeting site URL, start/end time. These data are processed by CISCO (processor) for billing purposes. c) User generated information: meeting and call recordings, transcriptions of call recordings, uploaded files. These data are processed by CISCO in order to provide the service and are deleted after the end of the meeting. The meeting host has access to these data and can store them locally (e.g. in case that call recording is activated). d) Analytics data: IP address, user agent identifier, hardware type, operation system type and version, client MAC address, meeting session information, call attendee information (including email address, IP address, username, phone number), etc. These data are processed by CISCO for analytics purposes. e) In addition, for the provision of Single Sign On (SSO) the following attributes of ENISA's Active Directory are synced with CISCO WebEx: uid, email, first name, last name, time stamp. For MS Teams: The following types and categories of personal data are being processed with the use of the MS Teams platform. a) User data (for all registered users, i.e., ENISA staff members and externals): · Profile data (e.g., account info, email address, profile picture, phone number) · Meeting content i. Audio and video ii. Possible screen share iii. Thechat 1. One-on-one chat. Retention period is 7 days 2. MS Teams private chat. Retention period is 60 days 3. MS Teams channel chat. Retention period is 60 days iv. Possible shared files v. Possible audio and video recordings vi. Possible transcript · Voicemail · Content within a MS Teams chat or channel i. Possible shared files ii. Audio and video iii. Possible screen share iv. Possible audio and video recordings v. Possible transcripts Call history (A detailed history of the phone calls, which allows to each user to go back and review their own call records). b) Service-Generated Data This is data generated my Microsoft through operation of the service, like use or performance data. Call quality data (this includes call and meeting data available to the ENISA system administrator in order to troubleshoot issues with meeting quality and service usage). This also includes technical and connection data to be used for example to provide Outlook calendar links. (e.g., IPs, device identifiers). c) Technical Support Data Means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by, or on behalf of, ENISA through an engagement with Microsoft to obtain Professional Services or Support. This may include information collected over phone, chat, e-mail, or web form. It may include description of problems, files transferred to Microsoft to resolve support issues, automated

	trouble-shooters, or by accessing customer systems remotely with customer permission.d) Administrative/Billing Data Contractual, account and billing information.
Time limits (for the erasure of data)	For Webex: Meeting host information is maintained for 7 years by CISCO after termination of the service for audit purposes. User generated data are deleted by CISCO after each meeting. Analytics data are maintained by CISCO until the termination of the contract. Any locally stored user data will be deleted by the meeting host/organiser (ENISA) in accordance with its policy for events. For MS Teams: ENISA follows a data retention policy for the personal data collected (ENISA shall use minimum necessary for the accomplishment of the purpose). User data: User MS Teams channel data is stored for a period of maximum 2 months and then they are deleted. 1. One-on-one chat retention period is 7 days 2. MS Teams private chat retention period is 60 days 3. MS Teams channel chat retention period is 60 days 4. Usermessages are retained for a period of maximum 90 days when the user is deleted from MS Teams services. 5. Where Meeting Transcripts are used, they are later deleted manually by the user after taking minutes from them (e.g., by the secretaries). They are kept for maximum 2 months. 6. Meeting Recording retention period is 60 days. Service-generated Data: up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations. As per Microsoft data retention. Any Personal Data (data not included in Customer Data): Up to 180 days. As per Microsoft data retention. Administrative/billing data: If ENISA terminates the contract with Microsoft for the provision of the MS Teams service, then the relevant personal data are deleted between 90 and 180 days of this service termination.
Data recipients	For Webex: Designated staff of ENISA (meeting host/organiser) and CISCO (processor); Designated staff of ENISA IT responsible for system operation and maintenance, in case of troubleshooting or investigation of security incidents. For MS Teams: The following parties have access to the personal data: - ENISA staff responsible for the service (e.g., IT system administrators) have access to personal data such as participant information, meeting information. The access is for system operation and maintenance, troubleshooting or investigation of security incidents. By default, administrators do not have access tochannels they are not members of, although this is possible via the Compliance Console (if an admin is granted special permissions over not owned data, an alert is sent to the rest of the administrators). - Microsoft for delivering the service.What personal data does Microsoft Teams collect and for what purposes does Microsoft Teams use this data? - The MS Teams service processors (Microsoft and its online servicessub processors. These sub-processors only have access to aggregated) - The participants of an MS Teams call/meeting have access to the meeting information such as the chat, name of the meeting participants, and the content shared in the meeting.
Transfers to third countries	For Webex: In particular, Webex host meeting information and analytics data are processed by Cisco (processor) in US and UK. For UK the processing is based on the Commission's adequacy decision for UK. For processing in the US, ENISA and

	CISCO have signed the latest version of the EC Standard Contractual Clauses (SCCs) - as part of the DPA signed between ENISA and CISCO. Transfers of personal data for the provision of the Webex service may also take in US and other third countries for the provision of technical support (follow-the-sun). These transfers are also governed by the EC SCCs signed between ENISA and CISCO (and form part of the DPA between the two parties). Communication of Webex meetings is end-to-end encrypted. CISCO has approved BCRs (NL DPA as lead authority). <u>For MS Teams:</u> Transfers or personal data outside the EU/EEAUser data are stored and further processed within Microsoft data centers exclusively in EU under the Microsoft data boundary program . There is an exception in the case of certain sub-processors (see Annex 1 - Microsoft General - Online Services Sub-Processors List) where personal data may be processed in US for the provision of the service. Service generated data: generated by Microsoft and transferred to Microsoft data centers in US. Based on the Microsoft EU Data Boundary, pseudonymized service generated and diagnostic data will be stored & processed in the EU, in phase 2 - end of year 2023. Technical support data: generated by ENISA/IT and processed around the world (24/7). Based on the Microsoft EU Data Boundary, Support data will be stored in the boundary of EU with limited access to it from outside the boundary of the EU. Data Boundary Roadmap. Privacy & Security Terms.[A3] [A4] Any transfer of personal data outside the EU/EEA shall be performed in line with the ILA (between the European Commission and Microsoft) and in compliance with Chapter V EUDPR. Microsoft has been certified under the EU US Data Privacy Framework.
Security measures - General description	Webex is operated in secure servers of processor (CISCO). Applicable security policies of processor and subprocessor are in place. MS Teams is a cloud service hosted on Microsoft servers. MS Teams is a cloud-based collaboration software that follows thesecurity best practices and procedures such as:- service-level security through defence-in-depth, - customer controls within the service, - security hardening, and - operational best practices.Microsoft uses the"Supplier Security and Privacy Assurance (SSPA) program" to ensure privacy and security principles are followed by suppliers. It also uses Just In Time role-based access to access the production environment. MS Teams offers end-to-end encrypted calls for one-on-one calls. There is also the option ofend-to-end encrypted meetings via the MS Teams Premium license (that ENISA has acquired). Microsoft online services are regularly audited and its data centres follow security standards. More details can be foundhere. ENISA has fully disabled diagnostic data/telemetry in the platform and the possibility to apply E2EE will be considered on a case-by-case basis.
Privacy statement	Available on intranet for all ENISA staff. Information on the use of CISCO Webex and MS Teams is provided, whenever relevant, in privacy statements of ENISA online conferences and events.