

RECORD OF PERSONAL DATA PROCESSING ACTIVITY according to Article 31 of Regulation (EU) 2018/1725

▶ Web Conference Service (Cisco Webex)

Contents

General information.....	1
Description and Purpose of the Processing	2
Data Subject's Rights.....	3
Categories of Data Subjects & Personal Data	4
Categories of Recipients & Data Transfers.....	7
Automated Decision Making.....	9
Retention Period & Security Measures.....	9

General information

Introduction
EIOPA, as a European Authority, is committed to protect individuals with regard to the processing of their personal data in accordance with Regulation (EU) No 2018/1725 (further referred as the Regulation) ¹ .
Contact Details of Data Controller(s)
Fausto Parente, Executive Director Westhafenplatz 1, 60327 Frankfurt am Main, Germany fausto.parente@eiopa.europa.eu
Contact Details of the Data Protection Officer
Eleni Karatza Westhafenplatz 1, 60327 Frankfurt am Main, Germany dpo@eiopa.europa.eu
Contact Details of Processor
EIOPA's Team/Unit/Department responsible for the processing: IT Unit Contact: IT-DPC@eiopa.europa.eu

¹ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Description and Purpose of the Processing

Description of Processing
<p>The overall rationale and underlying reason for the processing is documented in EIOPA’s IT Strategy, which calls on the IT Unit to deliver digital services to enable EIOPA’s policies and to support EIOPA’s internal administration.</p> <p>EIOPA uses the Cisco Webex Meetings service, a cloud-based web and video conferencing solution made available by Cisco and managed by CANCOM, to organise and host web meetings for internal and external participants (further referred as “the service”).</p> <p>The service enables individuals and virtual teams to collaborate on mobile devices or video systems in real time. It supports in meetings, events, training, and support services.</p> <p>The processing operation starts upon the registration to the service:</p> <ul style="list-style-type: none"> • when a meeting attendee joins a Webex meeting; • when a host (ie, meeting organiser) profile is created (this applies to EIOPA staff only). <p>The organiser of the meeting can take the decision of a local meeting recording, and in such scenario a recording alert is visible and available to all participants. The recording shall be explicitly announced to the participants ahead of the meeting. Participants can object to being recorded by notifying the organiser.</p> <p><u>Technical means:</u></p> <p>Cisco uses two data centres in Europe to provide their services: Amsterdam and Frankfurt am Main.</p> <p>Additionally, in EIOPA’s configuration model set up with Cisco, data are not shared with third countries, with the exception of billing and analytics data which may be sent and stored in a US data centre. This data may include personal data, e.g. on the conference host.</p> <p>Data sent to the cloud are encrypted at rest and in transit.</p> <p>Personal data will not be used for any purposes other than the performance of the activities specified above. Otherwise you will be informed accordingly. Detailed information is available in Cisco’s Privacy Data Sheet.</p>
Purpose (s) of the processing
<p><input checked="" type="checkbox"/> Staff administration</p> <p><input checked="" type="checkbox"/> Relations with external parties</p> <p><input type="checkbox"/> Procurement and accounting</p> <p><input type="checkbox"/> Administration of membership records</p> <p><input type="checkbox"/> Auditing</p> <p><input checked="" type="checkbox"/> Information administration</p> <p><input checked="" type="checkbox"/> Other (please give details):</p> <p>Personal information is collected in order to:</p> <ul style="list-style-type: none"> • identify conference host and participants to ensure the normal operation of the Webex service; • identify potential improvements and technical deficiencies of the service;

<ul style="list-style-type: none"> • collect statistics used for service invoicing by the contractor; • collect representative data and conference statistics (excluding content) to improve user experience and service performance by carrying out analyses of aggregated data; • address technical support requests; • analyse the performance of technical support. <p>Personal data is accessed only when necessary for troubleshooting, performance and capacity management, analysis of performance problems, general user support, billing verification, when validating the performance of contractual conformity and for investigations as set out in the Draft Policy and Working Instructions on the Acceptable Use of EIOPA’s Information and Communications Technology Resources.</p>
<p>Lawfulness of Processing</p>
<ul style="list-style-type: none"> • Legal Basis justifying the processing: <ul style="list-style-type: none"> • Regulation (EU) 1094/2010 (EIOPA Regulation); • Policy and Working Instructions on the Acceptable Use of EIOPA’s Information and Communications Technology Resources. • Processing is necessary: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> for the performance of a task carried out in the public interest, in line with Article 5(1)(1)(a) of the Regulation, notably for the management and functioning of EIOPA <input type="checkbox"/> for compliance with a legal obligation to which the Controller is subject <input type="checkbox"/> for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract <input type="checkbox"/> in order to protect the vital interests of the data subject or of another natural person <p>Or</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Data subject has given his/her unambiguous, free, specific and informed consent, in case of audio/video recording of a conference/meeting/event

Data Subject’s Rights

<p>Information on how to exercise data subject’s rights</p>
<p>Data subjects may exercise their data privacy rights provided in Articles 17 to 24 of the Regulation (EU) 1725/2018.</p> <p>Data subjects have the right to:</p> <ul style="list-style-type: none"> • access their personal data, receive a copy of them in a structured and machine-readable format or have them directly transmitted to another controller, as well as request their rectification or update in case they are not accurate; • request the erasure of their personal data, as well as object to or obtain the restriction of their processing;

- withdraw their consent to the processing of their personal data at any time in case such processing is based solely on their consent.

For the protection of the data subjects’ privacy and security, every reasonable step shall be taken to ensure that their identity is verified before granting access, or rectification, or deletion.

Should data subjects wish to access/rectify/delete their personal data, or receive a copy of them/have it transmitted to another controller, or object to/restrict their processing, please contact IT-DPC@eiopa.europa.eu or DPO@eiopa.europa.eu.

Complaint:

Any complaint concerning the processing of the data subjects’ personal data can be addressed to EIOPA’s Data Protection Officer (DPO@eiopa.europa.eu). Alternatively, data subjects can also have at any time recourse to the European Data Protection Supervisor (www.edps.europa.eu).

Categories of Data Subjects & Personal Data

Categories of Data Subjects
<input checked="" type="checkbox"/> EIOPA permanent staff, Temporary or Contract Agents <input checked="" type="checkbox"/> SNEs or trainees <input type="checkbox"/> Visitors to EIOPA (BoS, MB, WG, Seminars, Events, other) If selected, please specify: NA <input checked="" type="checkbox"/> Providers of good or services <input checked="" type="checkbox"/> Complainants, correspondents and enquirers <input type="checkbox"/> Relatives and associates of data subjects <input checked="" type="checkbox"/> Other (please specify): <ul style="list-style-type: none"> • External collaborators, contractors, etc. communicating with EIOPA staff members; • Participants in EIOPA's online conferences/meetings and events.
Categories of personal data
<p>(a) General personal data:</p> <p>The personal data contains:</p> <input checked="" type="checkbox"/> Personal details (Registration information: name, e-mail address, password, public IP address, browser, phone number (optional), mailing address (optional), geographic region, user information included in the customer’s Active Directory (if synched), Unique User ID (UUID), etc.) <input type="checkbox"/> Education & Training details <input type="checkbox"/> Employment details <input type="checkbox"/> Financial details

Family, lifestyle and social circumstances

Other (please give details):

In order to carry out this processing operation, the following categories of personal data are collected:

1. Host and Usage Information

- IP address
- User agent identifier
- Hardware type
- Operating system type and version
- Client version
- IP addresses along the network path
- MAC address of endpoint (as applicable)
- Service version
- Actions taken
- Meeting session information (title, date and time, frequency, average and actual duration, quantity, quality, network activity, and 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 and diagnostics information

2. Invoicing information (subset of previous category)

- Host name
- Conference URL
- Conference time and duration

3. Host Registration Information

- Name
- Email address
- Password (hashed version only)
- Public IP address
- Browser
- Phone number (optional)
- Mailing address (optional)
- Avatar (optional)

- Billing information
4. User-generated Information
- Meeting and call recordings (only local by meeting organiser) – optional data
 - Uploaded files – optional data
5. Cisco Technical Support Information (TAC)
- Name/Surname of the employee appointed to open the service request
 - Email address of the employee appointed to open the service request
 - Phone number of the employee appointed to open the service request
 - Authentication information (excluding passwords)
 - Information about the condition of the system (if applicable)
 - Registry data about software installations and hardware configurations (if applicable)
 - Error-tracking files (if applicable)

The provision and collection of personal data is mandatory to meet technical requirements. If personal data is not provided (Host Registration/Host Usage/User-generated), possible consequences might be that the system cannot operate properly and therefore the participation of a user is impossible. On the other hand, missing TAC Support Information might severely impact the efficient technical support the contractor could offer.

The user-generated information, namely the recording and files shared of the conference, can be available in two ways:

- Through participation in the conference for its duration. In this case, participants may decide not to share their image or voice.
- By the local audio or video recording of the conference/meeting, which may be activated manually by the meeting organiser. Conferences/meetings are not recorded by default. When they are recorded, the explicit consent of the participants to the recording is required before the recording starts.

The chat exchanges between participants are never retained after the termination of the conference.

The list of participants' names is available for each participant for the duration of the conference. However, these names are not a unique identifier for each user. Indeed, they may not correspond to the real names of people in the conference.

(b) Special categories of personal data

The personal data reveals:

- Racial or ethnic origin, in case of virtual meetings where participants are using their camera.
- Political opinions
- Religious or philosophical beliefs
- Trade union membership

Genetic or Biometric data

Data concerning health, sex life or sexual orientation

Neither EIOPA nor Cisco can control what participants share during meetings and in conversation chats. EIOPA highly advises that users refrain from using Webex to disseminate sensitive data, e.g. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data (mental & physical), data concerning a natural person’s sex life or sexual orientation, as well as data regarding criminal convictions and offences or related security measures – which either concern themselves or another natural person.

Only in case the data subjects include in the meeting, meeting chat or documents the above-mentioned sensitive data will such data be processed.

Remark: Personal data may be processed, in particular personal data contained within the content created by individual users or groups of users, in addition to the personal data processed by Cisco Webex covered by this record. For example, this refers to documents, messages or meeting chats exchanged between members of a specific group or team. The decision on which data will be shared using Cisco Webex remains fully with the respective user. To this extent, special categories of data might be processed.

Categories of Recipients & Data Transfers

Recipient(s) of the data

Managers of data subjects

Designated EIOPA staff members

If selected, please specify: IT administrators and security officers

Relatives or others associated with data subjects

Current, past or prospective employers

Healthcare practitioners

Education/training establishments

Financial organisations

External contractors

Other (please specify):

- Designated support staff from EIOPA, CANCOM and Cisco have access to host and usage information.
- The main recipient is the conference organiser who invites all internal and/or external participants. The organiser, by service definition, is an EIOPA staff member. Participants are also recipients of all the meeting contents during the duration of the session. If the main organiser takes the decision of a local meeting recording, a recording alert is visible and available to all participants. Participants can object to being recorded by notifying the organiser.
- For monitoring or audit tasks, or in case of complaints, access may be granted to:

<ul style="list-style-type: none"> ▪ relevant EIOPA staff (e.g., the Legal Team, Data Protection Officer, Antifraud Officer, Ethics Officer, Internal Control); ▪ bodies in charge of monitoring, inspection, regulatory or judicial task in accordance with the EU legislation (e.g., the European Court of Auditors, the European Anti-Fraud Office, the EU Ombudsman, the Court of Justice of the EU); ▪ external legal service provider. <ul style="list-style-type: none"> • Potentially any EU institution/agency/body with which EIOPA conducts business. • Potentially any organisation within EU with which EIOPA conducts business (e.g. NCAs).
Data transfer(s)
<p><input checked="" type="checkbox"/> Within EIOPA or to other EU Institutions/Agencies/Bodies If selected, please specify: Within EIOPA and potentially any EU institution/agency/body with which EIOPA conducts business.</p> <p><input checked="" type="checkbox"/> To other recipients within the EU (e.g. NCAs) Potentially any organisation within EU with which EIOPA conducts business.</p> <p><input checked="" type="checkbox"/> To third countries If selected, please specify:</p> <ul style="list-style-type: none"> • User-Generated information is stored in Cisco’s data center closest to the Agency’s location, i.e. Amsterdam, Netherlands, or Frankfurt, Germany. Cisco stores the following personal data in the United States of America (USA): <ul style="list-style-type: none"> ○ Cisco Webex analytics platform data, which utilises host and usage information; ○ Billing information. • Cisco may also share data with third party service providers as indicated in the Privacy Data Sheet. <p>Detailed information on data transfers provided by CISCO Webex is available here: https://www.cisco.com/c/en/us/about/trust-center/gdpr.html</p> <p>Whether suitable safeguards have been adopted:</p> <p><input type="checkbox"/> Adequacy Decision of the European Commission²</p> <p><input checked="" type="checkbox"/> Standard Contractual Clauses (SCC)</p> <p><input checked="" type="checkbox"/> Binding Corporate Rules (BCR)</p> <p><input type="checkbox"/> Administrative Arrangements between public Authorities (AA)</p>

² Third countries for which the European Commission has issued adequacy decisions are the following: [Adequacy decisions \(europa.eu\)](#)

<input type="checkbox"/> To international organisations If selected, please specify the organisation and whether suitable safeguards have been adopted: NA
Data subjects could obtain a copy of SCC, BCR or AA here: Cisco has invested in a number of transfer mechanisms to enable the lawful use of data outside the European Economic Area such as EU Binding Corporate Rules and EU Standard Contractual Clauses . For further information, please also read the Cisco Webex Privacy Statement .

Automated Decision Making

Automated Decision-making, including profiling
A decision is taken in the context of this processing operation solely on the basis of automated means or profiling: <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes In case of an automated decision-making or profiling, please explain: NA

Retention Period & Security Measures

Retention period
How long will the data be retained? <ul style="list-style-type: none">• Host and usage information: 3 years from when the service is terminated in a pseudonymised format;• Invoicing information: 7 years maximum;• Host registration information: 7 years after contract termination (EIOPA can request early deletion to privacy@cisco.com or open a service request);• User-generated information: meeting duration (unless local recording by the meeting host takes place);• TAC Support Information: up to 10 years (EIOPA can request early deletion to privacy@cisco.com or open a service request).• The content of the video/audio conference (documents, links, files etc.) will be deleted after the termination of the session, unless they are downloaded/saved by the meeting organiser or a specific recording of the meeting takes place. Specific recordings of the meetings are deleted from Webex after the termination of the session and saved and retained in EIOPA's ICT infrastructure in accordance with EIOPA security and document management policies. The chat messages exchanged among participants during a meeting are deleted after the meeting/session is ended/terminated.

- Amazon cloud (AWS) collected data: data will be deleted within 15 days of the meeting.

Please also see the [Privacy Data Sheet](#).

For further processing envisaged beyond the original retention period for historical, statistical or scientific purposes, please specify whether the personal data will be anonymised:

No

Yes

Technical & organisational security measures taken

Several technical and organisational measures have been adopted in order to ensure the optimum security of the documents and personal data collected in the context of the procedures described in section "Description and purpose of the processing".