DATA PROTECTION NOTICE
For processing of personal data in the context of the use of WebEx meetings

1. Context and Controller
As Eurojust collects and further processes personal data, it is subject to Regulation (EU) 2018/1725 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.

Collection and processing of personal data within Eurojust system log files is under the responsibility of the Controller, who is the Head of Information Management Unit and can be contacted at mchanfreau@eurojust.europa.eu.

2. What personal information do we collect, for what purpose, under which legal bases and through which technical means?

Legal basis
The legal basis for processing of personal data are:

Regulation (EU) 2018/1725 of 23 October 2018 (a2) (a) as per recital 22, second sentence

To be able to maintain and support IT systems needed for the operation of Eurojust.

Purpose of the processing
The WebEx Meetings solution is used for organising large-scale meetings hosted by Eurojust for internal and external participants, where non-operational, non-confidential, nor sensitive data (operational or administrative) are discussed or disclosed.

Technical means
Cisco uses two Data Centres in Europe at the moment to provide their services: Amsterdam and Frankfurt.

Additionally, in the Eurojust configuration model set up with Cisco, the data are not shared with third countries, with the exception of the billing data which are sent and stored in the US Data Centre.

Types of personal data
Personal data collected and further processed are:

1) For Eurojust Staff Members managing the back-end/configuration portal (Back Office, Front Office)

- Name
- Email Address
- Password
- Public IP Address
- Browser
- Phone Number (Optional)
- Mailing Address (Optional)
- Geographic region – obtained from the IP address
- Avatar (Optional)
- Billing Information
- Unique User ID (UUID) – as generated by Cisco and encrypted.
2) For Eurojust Staff Members managing the meeting (Back Office, Front Office, Hosts and Co-Hosts)

- IP Address
- Hardware Type*
- Operating System Type and Version*
- Client Version*
- IP Addresses Along the Network Path*
- MAC Address of Client* (As Applicable)
- Service Version*
- Actions Taken
- Geographic Region – obtained from the IP address
- 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 NonScreen-Sharing Sessions
- Number of Participants**
- Participant’s name used to join the call: this information is provided by the participant, and does not need to be their real name/surname
- Participant’s email address: this information is provided by the participant, and does not need to be their real email address
- Meeting Host Information:
  - Host Name
  - Meeting Site URL
  - Meeting Start/End Time
- Screen Resolution
- Join Method

*Data collected for Performance, Troubleshooting, and Diagnostics.
** Data collected for Analytics

3) For external participants joining a WebEx meeting

For VideoConferencing systems accessed by external participants via WebEx web browser plugin, smart phone app, or any other videoconferencing tool, the following personal data are collected:

- Email addresses: this information is provided by the participant, and does not need to be their real email address
- IP address
- Username: this information is provided by the participant, and does not need to be their real name/surname.
- Phone numbers – only for those connecting via phone
- Device information*
- Hardware Type*
- Operating System Type and Version*
- Client Version*
- MAC Address of Client* (As Applicable)
- Service Version*
  - Number of Meetings**

---

1 A Host or Co-host is the member of the organising Unit/Desk/Department in charge of managing the meeting
* Data collected for Performance, Troubleshooting, and Diagnostics
** Data collected for Analytics

3. Who has access to your personal data and to whom is it disclosed?

For the purpose detailed above, access to your personal data is given to the following persons, without prejudice to a possible transmission to the bodies in charge of a monitoring or inspection task in accordance with European Union law:

Access restrictions apply based strictly on need to know basis.

   a) User Support  
   b) Back Office  
   c) Host or Co-Host of the meeting  
   d) For data listed in Section 1) and Section 2) above, and limited to the data indicated as to be collected for Performance, Troubleshooting, and Diagnostic: these data can be sent also the Cisco Technical Support, in charge of investigating and solving technical issues. In such case, a dedicated member of the Back Office Team will send the information to the Cisco Technical Support. Participants data listed under Section 3) will not be shared with Cisco Technical Support. Cisco Technical Support is located in several countries (as described in the attachment Cisco TAC Delivery Service Privacy Data Sheet). The data submitted to the Cisco Technical Support are stored on Amazon Web Services Data Centre located in North Virginia and are kept for 10 years.

4. How do we protect and safeguard your information?

The personal data collected by WebEx are encrypted as described below:

- Data listed in section 1) above are encrypted in transit.
- Data listed in section 2) above are encrypted in transit.
- Data listed in section 3) above are encrypted in transit and at rest.
- All password listed under point 1) are encrypted in transit and at rest.

Additional information on the encryption methods are included in the attached Cisco Privacy Data Sheet.

5. How can you verify, modify or delete your information?

In case you wish to verify which personal data is stored on your behalf by the Controller, have it modified, corrected, or deleted, or restrict the processing, or object to it or to exercise the right to data portability, please make use of the following email address: usersupport@eurojust.europa.eu , by explicitly describing your request. Any correction of your personal data will be taken into consideration from the data protection point of view.

Identification data of individuals can be corrected at any time.

6. How long do we keep your personal data?

The retention period is the following:

**Eurojust data described in section 1) above:**

The data are maintained as long as an active subscription with Cisco is in place. In case of termination of service with Cisco, all the data are deleted with the exception of Name, UUID, and billing information which are kept are maintained for 7 years as part of Cisco's business record and to comply with Cisco financial and auditing policies.
Additionally, data shared for troubleshooting purposes (as identified in the list above) with the Cisco Technical Support are kept for 10 years.

**Eurojust data described in section 2) above**

The data will be retained by Cisco 3 years from the termination of the active subscription of the service by Eurojust.

Additionally, data shared for troubleshooting purposes (as identified in the list above) with the Cisco Technical Support are kept for 10 years.

**Participants data described in section 3) above**

The participants' data will be retained by Cisco 3 years from the termination of the active subscription of the service by Eurojust.

7. **Contact information**

You have the right to access, rectify or erase or restrict the processing of your personal data or, where applicable, the right to object to processing or the right to data portability in line with Regulation (EU) 2018/1725.

Any such request should be directed to the Controller, by using the following email address: usersupport@eurojust.europa.eu, and by explicitly specifying your request.

You may also contact the Data Protection Officer of the Eurojust (dpo@eurojust.europa.eu).

8. **Recourse**

You have the right to lodge a complaint to the European Data Protection Supervisor (https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data.