



Eurojust record of processing activity

Record of processing personal data activity, based on Article 31 of 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

Part I –Article 31 Record (this part is publicly available)

Nr.	Item	Description
WebEx cloud solution for the hosting of non-confidential Eurojust Video Conferences and Meetings		
1.	Last update of this record	04/01/2021
2.	Reference number [For tracking, please contact the DP Office for obtaining a reference number.]	
3.	Name and contact details of controller [Use functional mailboxes, not personal ones, as far as possible - this saves time when updating records and contributes to business continuity.]	<u>Head of Information Management Unit</u> <u>(mchanfreau@eurojust.europa.eu)</u>
4.	Name and contact details of DPO	<u>dpo@eurojust.europa.eu</u>
5.	Name and contact details of joint controller (where applicable) [If you are jointly responsible with another EUI or another organisation, please indicate so here (e.g. two EUIs with shared medical service). If this is the case, make sure to mention in the description who is in charge of what and whom people can address for their queries.]	N/A
6.	Name and contact details of processor (where applicable) [If you use a processor (contractor) to process personal data on your behalf, please indicate so (e.g. 360° evaluations, outsourced IT services or pre-	EMEAR Privacy Officer, Cisco Systems, Inc. Haalerrbergweg 13-19, 1101 CH, Amsterdam-Zuidoost The Netherlands

Nr.	Item	Description
	employment medical checks).]	Email address: privacy@cisco.com
7.	<p>Purpose of the processing</p> <p>[Very concise description of what you intend to achieve; if you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).]</p>	<p>The purpose of the processing is to provide a Video Conferencing solution to be used for meetings and events organised by Eurojust where non-operational, non-confidential, nor sensitive data (operational or administrative) are discussed or disclosed.</p>
8.	<p>Description of categories of persons whose data are processed and list of data categories</p> <p>[In case data categories differ between different categories of persons, please explain as well.]</p>	<p>1) Eurojust Staff Members managing the back-end/configuration portal (Back Office, Front Office)</p> <ul style="list-style-type: none"> • 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. <p>2) Eurojust Staff Members managing the meeting (Back Office, Front Office, Hosts and Co-Hosts¹)</p> <ul style="list-style-type: none"> • 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

¹ A Host or Co-host is the member of the organising Unit/Desk/Department in charge of managing the meeting

Nr.	Item	Description
		<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Host Name • Meeting Site URL • Meeting Start/End Time • Screen Resolution • Join Method <p>*Data collected for Performance, Troubleshooting, and Diagnostics. ** Data collected for Analytics</p> <p style="text-align: center;">3) For external participants joining a WebEx meeting</p> <p>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:</p> <ul style="list-style-type: none"> • 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* <ul style="list-style-type: none"> • Number of Meetings** <p>* Data collected for Performance, Troubleshooting, and Diagnostics ** Data collected for Analytics</p>
9.	<p>Time limit for keeping the data</p> <p>[Indicate your administrative retention period including its starting point; differentiate between categories of persons or data where needed (e.g. in selection procedures: candidates who</p>	<p>Data listed in point 1) above:</p> <p>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</p>

Nr.	Item	Description
	made it onto the reserve list vs. those who did not).]	<p>maintained for 7 years as part of Cisco’s business record and to comply with Cisco financial and auditing policies.</p> <p>Additionally, data shared for troubleshooting purposes (as identified in the list above) with the Cisco Technical Support are kept for 10 years.</p> <p>Data listed in point 2) above:</p> <p>The data will be visible by Eurojust Staff Members managing the meeting (Back Office, Front Office, Hosts and Co-Hosts) for 31 calendar days, after which it will be automatically removed from the WebEx back end.</p> <p>The data will be retained by Cisco 3 years from the termination of the active subscription of the service by Eurojust, after which it will be automatically deleted by Cisco.</p> <p>Additionally, data shared for troubleshooting purposes (as identified in the list above) with the Cisco Technical Support are kept for 10 years, , after which it will be automatically deleted by Cisco.</p> <p>Data listed in point 3) above:</p> <p>The data will be visible by Eurojust Staff Members managing the meeting (Back Office, Front Office, Hosts and Co-Hosts) for 31 calendar days, after which it will be automatically removed from the WebEx back end.</p> <p>The participants’ data will be retained by Cisco 3 years from the termination of the active subscription of the service by Eurojust, after which it will be automatically deleted by Cisco.</p>
10.	<p>Recipients of the data</p> <p>[Who will have access to the data within Eurojust? Who outside Eurojust will have access? Note: no need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).]</p>	<p>a) User Support b) Back Office c) Hosts and Co-Hosts of the meetings 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 to 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</p>

Nr.	Item	Description
		<p>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.</p>
11.	<p>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</p> <p>[E.g. processor in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult DPO for more information on how to ensure safeguards.]</p>	<p>Yes, billing data and data shared with Cisco Technical Services for troubleshooting and incident resolution are sent to the Cisco Data Centers located in the United States of America.</p> <p>Data for troubleshooting and incident resolutions might also be shared, if needed, with the WebEx sub-processor Skyes, located in Costa Rica, and IBM (Bulgarian branch).</p>
12.	<p>General description of security measures, where possible.</p> <p>[Include a general description of your security measures that you could also provide to the public.]</p>	<p>All the data collected are partly encrypted as described below:</p> <ul style="list-style-type: none"> • Data listed in section 1) above are encrypted in transit. • Data listed in section 2) above are encrypted in transit. • Data listed section 3) above are encrypted in transit and at rest. • All password listed under point 1) are encrypted in transit and at rest. <p>Full details of the security measures in place are described in the attachments below.</p>
13.	<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:</p> <p>[While publishing the data protection notice is not strictly speaking part of the record, doing so increases transparency and adds no administrative burden, since it already exists.]</p>	