

EDPS record of processing activity

Record of EDPS activities processing personal data, 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.

Nr.	Item	Description
		<i>Use of video conferencing software: Cisco Jabber client</i>
1.	Last update of this record	20/03/2023
2.	Reference number	69
3.	Name and contact details of controller	<p>The European Data Protection Supervisor (EDPS) and the European Parliament (EP) - DG ITEC - Individual Equipment & Logistics Unit (EQUILOG) are separate controllers for this processing operation.</p> <p>EDPS The EDPS is controller regarding the business processing of personal data when using WebMeeting for the meetings/events it organises (this includes business choices made on the use of the features of video conferencing tool).</p> <p>For more information on the EDPS please consult our website: https://edps.europa.eu.</p> <p>Responsible department or role: the Head of the EDPS Secretariat (EDPS@edps.europa.eu).</p> <p>Contact form for enquiries on processing of personal data to be preferably used: https://edps.europa.eu/about-edps/contact_en.</p>



Nr.	Item	Description
		<p>EP EP The Individual Equipment and Logistics Unit (EQUILOG Unit) is controller regarding the technical and legal aspects that it decides upon, such as for example the contractual clauses concluded with the service provider, as well as regarding technical customisation done at ITEC level and over which EDPS does not have any control or the possibility to alter.</p> <p>According to the EP data protection notice on On-premise Web Audio and Video Conferencing Service:</p> <p><i>Controllership scope aspects</i> <i>The Individual Equipment and Logistics Unit (EQUILOG Unit) is not controller for business processing operations on the usage of video/audio/chat services by EP's entities and client EUIs' entities, acting as controllers for the use of video/audio/chat services (i.e. using video/audio/chat services for their own business purposes). These entities are responsible for the business processing of data in video/audio/chat conferences organized on the provisioned services (included choices on the use of features of the services, such as meeting recording).</i></p> <p>Responsible department or role: DG ITEC - Individual Equipment & Logistics Unit (EQUILOG), ITEC-DPO-EQUILOG@europarl.europa.eu</p> <p>For more information, please see the EP Data Protection Statement here: https://epintranet.in.ep.europa.eu/home/browse-as/it-support/it-security-data-protection/it-protection-personal-data/cisco-jabber-client.html [available only internally]</p> <p>Contact for enquiries: EP DPO - http://www.europarl.europa.eu/at-your-service/en/stay-informed/data-protection</p>
4.	Name and contact details of DPO	EDPS DPO: dpo@edps.europa.eu EP DPO: data-protection@europarl.europa.eu



Nr.	Item	Description
5.	Name and contact details of joint controller (where applicable)	N/A
6.	Name and contact details of processor (where applicable)	N/A
7.	Short description and purpose of the processing	Cisco Jabber is part of the unified communication tools available to the EDPS and provided by the EP. Cisco Jabber is a tool allowing for audio-video calls and instant messaging (chat). The purpose of the processing operation is to enable audio/video communications by EDPS staff.
8.	Description of categories of persons whose data the EDPS processes and list of data categories	<p>The EDPS processes the following categories of personal data for the provision of Cisco Jabber tool: first name, last name, work telephone, work email address, starting and ending date of the contract, type of contract (e.g. official, contractual agent, trainee).</p> <p>According to the EP data protection statement,</p> <p><i>The Cisco Jabber client uses the following categories of personal data: first name, last name, picture, phone number, email address, job title, Internet Protocol (IP) address, corporate directories contacts, personal contacts (that can be private and/or corporate), status of availability (aka 'Presence'), location, communications details and the content of the communications (processed only during the communication in order to ensure the transmission).</i></p> <p><i>Regarding the location, the user has the possibility to inform others about his/her location.</i></p> <p><i>Different natures of personal data (present in the communications themselves) may be processed in the application in order to establish and ensure the communications themselves. However, Jabber does not analyse and does not store the content of the audio/video communication.</i></p>
9.	Time limit for keeping the data	Personal data are processed by the EDPS as long as the staff member is a member of the EDPS. When a staff member leaves the EDPS, the account is disabled and scheduled for deletion. The account is kept, in the disabled state, for a maximum period of three months, after which it is deleted. All personal data are deleted when deletion of the account occurs.

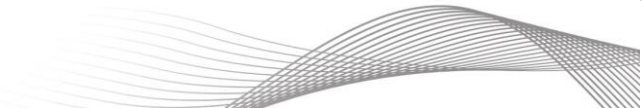


Nr.	Item	Description
		<p>According to the EP data protection statement,</p> <p><i>Personal data necessary for the transmission of an audio/video communication (content of the communication and metadata) are processed from their collection/creation until the termination of the communication, and are not stored afterwards.</i></p> <p><i>Personal data necessary for the end-user experience (e.g. Chat messages) are kept during the life cycle (from installation until de-installation or upgrade) of the Jabber client. The user can delete the chats messages at any time by pressing ‘Reset Jabber’¹, before signing into the Jabber client. Other data such as the picture or the title (i.e. gender) are synchronised from the EP corporate Directory (i.e. Active Directory) if present there.</i></p> <p><i>The call history of Jabber holds the last 200 calls.</i></p> <p><i>Personal data necessary for the support, maintenance and evolution of the system (metadata) are kept from their collection/creation up to 6 months. These data will be used for the calculation of global statistics (non-personal data results) necessary for technical reporting and monitoring.</i></p>
10.	Recipients of the data	<p><u>Access to personal data</u></p> <p>According to the EP data protection statement,</p> <p><i>Each end-user receives and sends personal data necessary for the transmission of an audio/video/text communication (including content of the communication and the related metadata to ensure the communication).</i></p> <p><i>Personal data (strictly necessary for the transmission of a communication) are transferred to the recipient end-user(s) to establish the communication.</i></p>

¹ By pressing Reset, all data stored in the local database will be erased, as well as the encryption certificate. You will need to contact ITEC Service Desk to renew your certificate in order to use the Softphone.



Nr.	Item	Description
		<p><i>The 'Availability' status is visible by all domain users unless managed via a black/white list by the end-user.</i></p> <p><i>The user can trigger activation/deactivation and auto-detection of the location data in the 'Options/Location' menu of Jabber. The location field may optionally be filled in by the user and if so, is visible by all domain users. Jabber saves each location linked to the IP address in an encrypted local database of the user profile.</i></p> <p><i>Personal contacts and groups of contacts are stored both in the local cache in an encrypted way and on the central server where they are visible by the IT administrators.</i></p> <p><i>Chat messages are stored in an encrypted local database of the user profile. They are only visible by their owner.</i></p> <p><i>Call history is stored in an encrypted local database of the user profile. It is only visible by the owner. The user can delete all (or a selection of) calls in the 'Calls' tab of Jabber with a right-click and 'Delete'.</i></p> <p><i>EP services have access to the personal data (metadata) necessary for the support, maintenance and evolution of the system.</i></p> <p><i>In case of technical issues, users might receive a message to send the report for further analysis. However, the 'send' button in the report request prompt is unavailable. In order to send the report the user would need to save and send the .zip file to ITEC Service Desk. More specifically, this would be sent to the "EXPTTEL team" (an ITEC support team in charge of communications). The sending of the report is voluntary.</i></p>
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	The EDPS does not transfer any data outside of EU and EEA.
12.	General description of security measures, where possible.	<ul style="list-style-type: none"> - Information security measures implemented by the EP. - The EDPS staff have do not have access to personal data processed via Jabber.



Nr.	Item	Description
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:	The data protection notice is available internally.