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
Use of Microsoft Teams for organising and attending non-confidential Eurojust Video Conferences and Meetings with other EU bodies and institutions and/or with External participants.		
1.	**Last update of this record**	**22/04/2025**
2.	**Reference number** [For tracking, please contact the DP Office for obtaining a reference number.]	IMU-23 (June 2025)
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.]	Head of Information Management Unit (ictprojects2@eurojust.europa.eu)
4.	**Name and contact details of DPO**	dpo@eurojust.europa.eu
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	N/A

Nr.	Item	Description
	their queries.]	
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-employment medical checks).]	**Contact details of MS EU Data Protection Officer**: South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 1 706 3117 (https://aka.ms/privacyresponse)
7.	**Purpose of the processing** [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).]	The purpose of the processing is to provide a Video Conferencing solution to be used for meetings and events organised by Eurojust or by other EU bodies, institutions or agencies (hereinafter referred to as 'EUIBAs') and/or with external parties in which Eurojust post-holders need to attend. During such meetings and events non-operational, non-confidential, nor sensitive data (operational or administrative) are discussed or disclosed.
8.	**Description of categories of persons whose data are processed and list of data categories** [In case data categories differ between different categories of persons, please explain as well.]	**1) For Eurojust post-holders managing the back-end/configuration portal (Digital Infrastructure Sector, User Support), the following data categories are processed:** • Email Address • Phone Number • Profile Picture (optional) **2) For Eurojust post-holders and College members organising and/or joining the meetings with their Microsoft Teams account, the following data categories are processed:** • Email Address • Phone Number • Profile Picture (optional) • Chat logs (kept for 30 days) * Microsoft might also collect additional technical not personal data for Performance, Troubleshooting, and Diagnostics (e.g. Browser version, Teams app version).

Nr.	Item	Description
		3) For Eurojust post-holders involved in the management of the contract with Microsoft, the following data categories are processed: • Name and Surname • Phone Number • Email address
9.	**Time limit for keeping the data** [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 made it onto the reserve list vs. those who did not).]	**Data listed in point 1) above:** The data is maintained until the user has an active account in Microsoft Teams (the account is created and managed in Azure/Entra ID). After the account is deleted, e.g. after the move or departure of the Eurojust post-holders, the data are kept for 90 days. **Data listed in point 2) above:** The data is maintained until the user has an active account in Microsoft Teams (the account is created and managed in Azure/Entra ID). After the account is deleted, e.g. after the move or departure of the Eurojust post-holders, the data are kept for 90 days. **Data listed in point 3) above:** Microsoft will retain Customer Data (used for e.g. contractual and billing purposes) for the duration of the Customer's right to use the service and until all Customer Data is deleted or returned, in accordance with the customer's instructions or the terms of the Online Services Terms. At all times during the term of the Customer's Microsoft subscription, the Customer will have the ability to access, extract, and delete Customer Data stored in the Online service. Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the Customer Data. **Other data** Chat history will remain available to the Eurojust's postholders for 30 days after the chat took place, after which the chat history will be automatically deleted. The content of the chat will not be visible to anyone aside from the users participating in the chat and will not be shared with Microsoft.

Nr.	Item	Description
10.	**Recipients of the data** [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).]	a) User Support b) Digital Infrastructure Sector
11.	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?** [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.**]**	Yes, billing data is sent to the Microsoft Data Centers located in the United States of America. Microsoft might use sub processors for commercial purposes and/or for troubleshooting of theirsystems. The list of sub-processors is available here. Based on the Service Level Agreement(SLA) with Microsoft signed by the European Commission, neither Microsoft nor their Sub processors are allowed to transfer personal data to third countries without explicit consent of the customer (Eurojust). In such cases, the personal data would be limited to the contact details of the DIS ICT Officer who contacts MS for support; no personal data of the users would be shared.
12.	**General description of security measures, where possible.** [Include a general description of your security measures that you could also provide to the public.]	All the data listed in Section 1) and 2) above is encrypted in transit and at rest. Data listed section 3) above are encrypted in transit and at rest. Additionally, data is pseudoanonymised by Microsoft. Full details of the security measures in place are described in the DPIA attached below.
13.	**For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:** [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.]	https://www.eurojust.europa.eu/document/data-protection-notice-processing-personal-data-context-use-microsoft-teams