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 – Eurojust Infrastructure log files
Monitoring system performance, user compliance, troubleshooting and enabling ICT Security forensic investigations for internal systems and ICT services operated by Eurojust.		
1.	**Last update of this record**	**20/07/2022**
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.]	Head of IM Unit mchanfreau@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 their queries.]	Not Applicable
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°	usersupport@eurojust.europa.eu – initial troubleshooting am@eurojust.europa.eu – monitor for compliance backoffice@eurojust.europa.eu – system performance

Nr.	Item	Description – Eurojust Infrastructure log files
	evaluations, outsourced IT services or pre-employment medical checks).]	monitoring, troubleshooting and reconstruction of events
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 processing personal data are: • Analyse and resolve technical issues • Detect performance issues • Identify failing components • Detect and identify unauthorised access to systems • Ensure compliance with Eurojust regulations and policies • Efficient management of resources and planning future requirements and developments • To monitor and detect external security threats to the infrastructure or persons at Eurojust.
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.]	Data subjects with Eurojust Active Directory accounts: 1. Users with access only to e-mail • Active Directory User name, time and date of accessing Eurojust ICT devices and systems, external IP address of user devices, translated internal IP address. 2. Users with access to Eurojust internal systems and applications • Active Directory User name, time and date of accessing Eurojust ICT devices and systems, Media Access Control (MAC) address for Eurojust devices, internal IP address of the user's device, external IP address of user devices connecting to systems available from Internet, reference to resources - such as Uniform Resource Locator (URL)/ web address of internal web applications accessed by the data subject. Data subjects accessing publicly available Eurojust systems from the Internet • Active Directory User name, time and date of accessing Eurojust ICT devices and systems, external IP address of user devices, translated internal IP address, reference to resources - such as Uniform Resource Locator (URL)/ web address of the accessed system. Data subjects making use of Eurojust telephony and fax

Nr.	Item	Description – Eurojust Infrastructure log files
		• Time and Date, dialed number, dialing number, duration of the connection. Data subjects accessing Eurojust operated videoconferencing systems externally via Cisco Meeting App: • User name provided by the data subject, IP address, address of the videoconference attended by the data subject, time, date, and duration of the connection to the videoconference. Data subjects using Eurojust wireless network WLAN_IOT • User's name, user's device MAC and IP address Data subjects using Eurojust wireless network WLAN_Guest • User's device MAC and IP 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).]	Network monitoring systems – retention period is 1 year Videoconferencing systems – retention period is up to 1 year maximum (or less in case of installation of a Cisco patch) VPN – retention period is 3 months Access Control Server (ISE) – retention period is 5 days on ISE appliances itself. The logs however are forwarded to SPLUNK where they are kept for the duration of 1 year. Fax – retention period is 3 months WIFI – retention period is 1 year The retention period for Audit log is defined by the POLICY- Audit log as approved by the AD 08/03/2018.
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).]	User Support, Back Office, Application Managers
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	No

Nr.	Item	Description – Eurojust Infrastructure log files
	needed, consult DPO for more information on how to ensure safeguards.]	
12.	**General description of security measures, where possible.** [Include a general description of your security measures that you could also provide to the public.]	Log file data is protected through measures defined in Eurojust Policies and Procedures and industry best practices. Security controls
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.]	Data subjects can exercise their rights to access, rectify, object, and data portability for the data collected by Eurojust (as listed under point 8) as described in the Data protection Notice Data_Protection_Notice_Log_Processing_20