



### 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
<b>Core International Crime Evidence Database (CICED) - Eurojust Analysis Solution (analysis tool(s))</b>		
1.	<b>Last update of this record</b>	27/11/2023
2.	<b>Reference number</b>  [For tracking, please contact the DP Office for obtaining a reference number.]	<b>IMU-20</b>
3.	<b>Name and contact details of controller</b>  [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.	<b>Name and contact details of DPO</b>	<a href="mailto:dpo@eurojust.europa.eu">dpo@eurojust.europa.eu</a>
5.	<b>Name and contact details of joint controller (where applicable)</b>  [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.]	Members of College, Liaison Prosecutors, and Representative of Denmark – for receiving the output (via the current CMS) of the analysis done in the analysis tools by Casework Unit and for further processing in the context of the specific investigation(s) for which they provide support to the NAs.

Nr.	Item	Description
6.	<p><b>1/ Name and contact details of processor (where applicable)</b></p> <p>[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).]</p> <p><b>2/ Persons processing under the authority of the controller according to Article 30 of Regulation (EU) 2018/1725 ('internal processors')</b></p>	<p>2/- User Support for the creation of the accounts in Active Directory.</p> <p>- Staff members of the Digital Infrastructure Sector in the Information Management Unit, duly authorised by the College for:</p> <ol style="list-style-type: none"> <li>1) granting access to the environment where the analysis tools are located;</li> <li>2) accessing the analysis database (which contains operational data) as system administrator to offer technical support.</li> </ol> <p>- Application Managers in the Information Management Unit for granting access to the analysis tools via the groups created in the Active Directory.</p> <p>- Staff members from the CWU (CICED team members), duly authorised by the College, for uploading and analysing contributions/operational data received.</p>
7.	<p><b>Purpose of the processing</b></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 processing of administrative data is:</p> <ul style="list-style-type: none"> <li>• Creating and managing the accounts to be used to access the analysis tools required to analyse data and to provide reports in the context of the CICED implementation in Eurojust.</li> <li>• Analysing and resolving technical issues.</li> <li>• Detecting performance issues.</li> <li>• Identifying failing components.</li> <li>• Detecting and identifying unauthorised access to systems.</li> <li>• Monitoring and detecting external security threats to the infrastructure or persons at Eurojust.</li> </ul> <p>The joint controllers will be processing operational personal data received in accordance with Article 4(1)(j) of the Regulation 2022/838 which provides Eurojust with an explicit legal basis to preserve, store and analyse evidence related to 'core international crimes' ('CIC') and foresees the establishment of a separate 'automated data management and storage facility' as a temporary derogation to the obligation to process operational data in the Case Management System (Article 80(8)).</p>
8.	<p><b>Description of categories of persons whose data are processed and list of data categories</b></p> <p>[In case data categories differ between different categories of persons, please explain as well.]</p>	<p>Administrative personal data:</p> <ol style="list-style-type: none"> <li>1) Eurojust post-holders from Digital Infrastructure Sector, Casework Unit and authorised members of the ND/LD/DKRP</li> </ol> <p>- Name</p>

Nr.	Item	Description
		<ul style="list-style-type: none"> <li>- Surname</li> <li>- Email</li> </ul> <p>2) Technical logs for troubleshooting purposes available for dedicated staff members of the Digital Infrastructure Sector</p> <p>3) Access logs available to ICT Security via <a href="#">Splunk</a> for monitoring the use of the system and carry out security tasks (e.g. detect possible intrusion).</p> <p><u>Operational personal data</u> - the data analysed will be in accordance with Article 27 of Eurojust Regulation and Annex II, including the recent amendments to it, more specifically point 1(n) and point 2(f) of the revised Eurojust Regulation.</p> <p>Find below the changes in Annex II:</p> <p>(a) point 1(n) is replaced by the following:</p> <p style="padding-left: 40px;">‘(n) DNA profiles established from the non-coding part of DNA, photographs and fingerprints and, in relation to the crimes and related criminal offences referred to in Article 4(1), point (j), videos and audio recordings.’;</p> <p>(b) point 2(f) is replaced by the following:</p> <p style="padding-left: 40px;">‘(f) the description and nature of the offences involving the person concerned, the date on which and location at which the offences were committed, the criminal category of the offences, the progress of the investigations and, in relation to the crimes and related criminal offences referred to in Article 4(1), point (j), information relating to criminal conduct, including audio recordings, videos, satellite images and photographs’.</p> <p>In addition, there might be an operational need to store to a limited extent special categories of operational personal data, pursuant to Article 27(4) of the Regulation (EU) 2018/1727 and Article 76 of the Regulation (EU) 2018/1725, e.g. data revealing racial and/or ethnic origin, political opinions, religious beliefs, genetic and biometric data for the purpose of uniquely identifying a victim or a suspect, and, as applicable, a witness; and data concerning health of a victim, suspect or witness; and data concerning sexual orientation of a victim.</p> <p>The data processed in analysis tools will be operational personal data and will mainly be used for analysis purposes.</p> <p>For more information regarding the processing of operational personal data, please consult <a href="#">Data Protection Notice regarding the processing of operational personal data by Eurojust</a>.</p>

Nr.	Item	Description
9.	<p><b>Time limit for keeping the data</b></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 made it onto the reserve list vs. those who did not).]</p>	<p>Operational personal data:</p> <p>The files with the operational personal data uploaded in the analysis area in the storage solution, will be stored by Eurojust in accordance with the conditions and time limits set by Article 29 of the Eurojust Regulation, as well the provisions of Chapter IX of Regulation (EU) 2018/1725.</p> <p>The operational personal data (analysis results) listed in section 8 are kept in the system until the output is generated and shared via the CMS with the requested authorised members of the National Desks/LP/DKRP.</p> <p>Administrative personal data:</p> <p>A yearly review takes place to confirm the need for accounts and remove the unnecessary ones.</p> <p>Access logs are sent to <a href="#">Splunk</a>, where they are kept for one year to allow ICT Security to monitor the use of the system and carry out their tasks (e.g. detect possible intrusion). The analysis tools logs are kept for three years to allow sufficient time for analysing and auditing. The logs are kept in accordance with Article 88 <i>Regulation (EU) 2018/1725</i> and made available to the DPO and the EDPS upon request.</p>
10.	<p><b>Recipients of the data</b></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>Duly authorised staff of ICT Security (via Splunk) – for administrative personal data; in cases of suspicious/malicious actions and for monitoring the system for possible security threats.</p> <p>National Members/Liaison Prosecutors/ Representative of Denmark and duly authorised members of the National Desks/LP/DKRP who receives the output of the operational personal data analysis shared with them by other NDs/LPs.</p> <p>No external contractors will have access to the data in the Storage Analysis Area nor in the analysis tools.</p>
11.	<p><b>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</b></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>No.</p>

Nr.	Item	Description
12.	<p><b>General description of security measures, where possible.</b></p> <p>[Include a general description of your security measures that you could also provide to the public.]</p>	<p>All the data are stored in Eurojust premises and secured following the Eurojust Security requirements.</p>
13.	<p><b>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:</b></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>	<p>Data subjects can exercise their rights as is described in the</p> <div data-bbox="790 450 839 510" style="text-align: center;">  </div> <p>Eurojust Analysis Tools_Data_Protecti</p> <p>For administrative personal data, the data subjects can send an e-mail regarding the administrative personal data to <a href="mailto:usersupport@eurojust.europa.eu">usersupport@eurojust.europa.eu</a>.</p> <p>For operational personal data, any request from data subjects regarding their rights should be directed to Eurojust (via email <a href="mailto:dpo@eurojust.europa.eu">dpo@eurojust.europa.eu</a>) or to the national supervisory authority in the Member State of the choice. That authority shall refer the request to Eurojust without delay, and in any case within one month of its receipt.</p>