



### 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>Eurojust Digital Storage Solution</b>		
1.	<b>Last update of this record</b>	14/03/2023
2.	<b>Reference number</b> [For tracking, please contact the DP Office for obtaining a reference number.]	
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	Duly authorised members of College, Liaison Prosecutors, Representative of Denmark – for reading the files received from the Eurojust Digital Transfer Solution, which are saved in the Digital Storage Solution. Each College member, Liaison prosecutor, representative of Denmark will only have access to the files saved under their own country folder.

Nr.	Item	Description
	their queries.]	
6.	<p><b>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>Duly authorised staff members of the Back Office–folders creation and permissions granting and technical troubleshooting</p> <p>User Support for the creation of the accounts in Active Directory.</p> <p>Duly authorised staff members from the CWU – for downloading the files from the Eurojust Digital Transfer Solution to the Digital Storage Solution</p> <p>Authorised members of the National Desks/LP/DKRP for the storing the operational personal data in the folders of their own country.</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 administrative data is:</p> <ul style="list-style-type: none"> <li>• Create and manage the accounts and folders to be used to store file in the context of the CISED implementation in Eurojust,</li> <li>• Analyze and resolve technical issues,</li> <li>• Detect performance issues,</li> <li>• Identify failing components,</li> <li>• Detect and identify unauthorized access to systems,</li> <li>• Monitor and detect 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 (Article 80(8)) 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.</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</p>	<p>Administrative personal data:</p> <p><b>1) Eurojust post-holders from Back Office and Casework Unit</b></p> <ul style="list-style-type: none"> <li>- Name</li> </ul>

Nr.	Item	Description
	persons, please explain as well.]	<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 Back Office team.</p> <p>Regarding the <u>operational personal data</u> - the data stored 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>
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>The files with the operational personal data uploaded in the Eurojust Digital Storage Solution will be stored by Eurojust for only as long as is necessary for the performance of its tasks and in accordance with the conditions and time limits set by Article 29 of the Eurojust Regulation.</p> <p>The data listed in section 8 are kept in the system until the users no longer need access to the Eurojust Digital Storage.</p> <p>A yearly review takes place to confirm the need for accounts and remove the unnecessary ones.</p> <p>Logs are sent to <a href="#">Splunk</a>, where they are kept for three years to allow ICT Security to monitor the use of the system and carry out their tasks (e.g. detect possible intrusion).</p>

Nr.	Item	Description
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>Authorised staff of the ICT Security (via Splunk) – for administrative personal data; in cases of suspicious/malicious contributions received and saved in the Digital Storage Solution and for monitoring the system for possible security threats.</p> <p>No external contractors will have access to the data stored in the Eurojust Digital Storage Solution, nor to the system in the Production Environment.</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>	No.
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>	All the data are stored in Eurojust premises and secured following the Eurojust Security requirements.
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>	Data subjects can exercise their rights as is be described in the <a href="#">Data protection Notice</a> .