




### 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 Transfer Solution for transferring large files to Eurojust.</b>		
1.	<b>Last update of this record</b>	13/02/2024
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 their queries.]	N/A
6.	<b>Name and contact details of processor (where applicable)</b> [If you use a processor (contractor) to	Duly authorised staff members of the Back Office and User Support– accounts and folders creation and technical troubleshooting

Nr.	Item	Description
	process personal data on your behalf, please indicate so (e.g. 360° evaluations, outsourced IT services or pre-employment medical checks).]	Duly authorised staff members from the CWU – for downloading the files from the Eurojust Digital Transfer Solution.
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 data is:</p> <ul style="list-style-type: none"> <li>• Create and manage the accounts and folders to be used to transfer large files to 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>
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> <p><b>1) Eurojust post-holders from Back Office and Casework Unit</b></p> <ul style="list-style-type: none"> <li>- Name</li> <li>- Surname</li> <li>- Email</li> <li>- Mobile phone number</li> </ul> <p>If the user decides to use the SMS as 2 factor authentication method, mobile phone number is used.</p> <p>If the user decides to use <a href="#">Mobile Pass</a> as 2 factor authentication method, email is used to receive the activation link of the application. In this case, two additional data are processed:</p> <ul style="list-style-type: none"> <li>- User ID</li> <li>- Device ID</li> </ul> <p>Note that User ID and Device ID are collected when the initial registration takes place, by the app itself.</p> <p>These data are only used to aid in case of troubleshooting.</p> <p><b>External users authorized to transfer large files to Eurojust</b></p> <ul style="list-style-type: none"> <li>- Name</li> <li>- Surname</li> <li>- Email</li> </ul>

Nr.	Item	Description
		<ul style="list-style-type: none"> <li>- Mobile phone number</li> </ul> <p>If the user decides to use the SMS as 2 factor authentication method, mobile phone number is used.</p> <p>If the user decides to use Mobile Pass as 2 factor authentication method, email is used to receive the activation link of the application. In this case, two additional data are processed:</p> <ul style="list-style-type: none"> <li>- User ID</li> <li>- Device ID</li> </ul> <p>Note that User ID and Device ID are collected when the initial registration takes place, by the app itself.</p> <p>These data are only used to aid in case of troubleshooting.</p> <p>- Technical logs for troubleshooting purposes available for dedicated staff members of the Back Office team.</p> <p>No external contractors will have access to the data stored in the Eurojust Digital Transfer Solution, nor to the system in the Production Environment.</p> <p><i>Regarding the <u>operational personal data</u> - the data transferred will be in accordance with Article 27 of Eurojust Regulation and Annex II point 1(n) and point 2(f) of the revised Eurojust Regulation.</i></p> <p><i>Find below the changes in Annex II:</i></p> <ul style="list-style-type: none"> <li>(a) point 1(n) is replaced by the following: <ul style="list-style-type: none"> <li>'(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.';</li> </ul> </li> <li>(b) point 2(f) is replaced by the following: <ul style="list-style-type: none"> <li>'(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.';</li> </ul> </li> </ul>

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>The files uploaded in the Eurojust Digital Transfer Solution are kept for maximum 7 days, after which they are manually downloaded in a digital storage and deleted from the Eurojust Digital Transfer Solution .</p> <p>The data listed in section 8 are kept in the system until the users no longer need access to the Eurojust Digital Transfer Solution.</p> <p>A yearly review takes place to confirm the need for accounts and remove the unnecessary ones.</p> <p>For external users, while the account is kept until the above mentioned review, users are only allowed to upload documents for 7 days at time.</p> <p>Logs are sent to <a href="#">Splunk</a>, where they are kept for one year to allow ICT Security and Data Protection to monitor the use of the system and carry out their tasks (e.g. detect possible intrusion).</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>Authorised staff of the National Desks – for operational personal data;</p> <p>Authorised staff of the Back Office – for administrative personal data only;</p> <p>Authorised staff of the ICT Security (via Splunk) – for administrative personal data; in cases of suspicious/malicious contributions received via the Eurojust Digital Transfer Solution – access to the Eurojust Digital Transfer Solution and to the operational personal data (on case by case basis only) for the purpose of investigating whether the contribution is actually malicious.</p> <p>Only authorised Eurojust staff members will have access to the data in the Eurojust Digital Transfer Solution, not external contractors. In case contractors need to be involved for technical support, they will not be granted access to the real data but only to the Test environment or to anonymised data.</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.

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. The system has been successfully pen tested and it is protected with a two factor authentication.</p> <p>Additionally, accounts of external users are only activated on demand and for a limited period of time (7 days).</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 be described in the <a href="#">Data Protection Notice</a></p>