




## 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 Service Portal</b>		
1.	<b>Last update of this record</b>	29/02/2024
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.]	Marc Chanfreau 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 process personal data on your behalf, please indicate so (e.g. 360° evaluations, outsourced IT services or	N/A

Nr.	Item	Description
	pre-employment medical checks).]	
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 Eurojust Service Portal is a technical upgrade of the existing on premises Remedy.</p> <p>Remedy is used for two purposes:</p> <ul style="list-style-type: none"> <li>- Manage the assets allocation in Eurojust;</li> <li>- Collect, track, and monitor incidents, permissions request.</li> </ul> <p>The system allows:</p> <ul style="list-style-type: none"> <li>- User support to record the allocation of assets to Eurojust post-holders;</li> <li>- Eurojust post-holders to report incidents, submit requests, and ask for new/updated permissions in the systems used by Eurojust, following the relevant system policy for authorisation of access, for themselves or on behalf of other post-holders;</li> <li>- Eurojust Digital Infrastructure Sector, ICT Project, Application Management, User Support, Data Management, Security, Events and Logistics teams to assess the requests submitted by the users, and track the work performed until the closure of the request.</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>	<ul style="list-style-type: none"> <li>- All Eurojust post-holders</li> </ul> <p>From all Eurojust post-holders the following data categories will be collected to enable access:</p> <ul style="list-style-type: none"> <li>- First name;</li> <li>- Last name;</li> <li>- Work email;</li> <li>- Work phone number;</li> <li>- Usernames.</li> </ul> <p>These data come directly from Eurojust Active Directory (AD) and are synchronised daily with it.</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 data retention is linked to the different functions of the system:</p> <p><b>For asset management:</b></p> <p>The Service portal is used for asset management, and therefore the retention period is bound to the asset management data retention period:</p> <ul style="list-style-type: none"> <li>- The data retention period for asset management in accordance with the <a href="#">Eurojust financial regulations</a> is 5+2 years. This is also in line with the <a href="#">data protection notice for the AD</a>, page 3 section 6 where the data is vetted from. The personal data will be kept available in the application as long as the post-holder is active at Eurojust. After the post-holder leaves Eurojust, the data will be archived from the system and</li> </ul>

Nr.	Item	Description
		<p>will only remain available in the system's database, accessible only to Administrators from the Information Management Unit. The data will remain available in the database for budgetary auditing, control, and for security investigations, if needed.</p> <p><b>For incident management:</b></p> <p>All the personal data related to incident management will be anonymised on a yearly basis after the post-holder is not active anymore at Eurojust.</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>	<ul style="list-style-type: none"> <li>- The people mentioned under section 8 will have access to their own data and to the data (name, mail address, ticket progress) of other post-holders on whose behalf they are submitting a request;</li> <li>- User Support, Application Management, Back Office, ICT Projects and DMU dedicated post-holders have access to the data under section 8 for the incidents and requests assigned to them;</li> <li>- Back Office also has admin access to the portal for setting up and troubleshooting the system, and therefore access to the data listed under section 8 for all post-holders, and to the database where the assets related data are archived after the post-holders departure.</li> </ul>
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 personal data are transferred to third countries or organisations</p>
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 electronic and hard copies of documents including personal data are stored securely in a secure infrastructure, at Eurojust premises, with limited access to duly authorised Eurojust post-holders only.</p> <p>The system is fully on premises, and it has been upgraded following the best security practices for its technical infrastructure.</p>

Nr.	Item	Description
		 <p>CIS_Red_Hat_Enterprise_Linux_8_Benchmark</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>The Data Protection notice will be made available on the portal itself.</p>