




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
Extranet		
1.	Last update of this record	18/03/2023
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 Information Management Unit ICTProjects2@eurojust.europa.eu The entities listed below will be a separate controller for their individual processing of personal data activity using Restricted Area on Extranet: Head of the JITs Network Secretariat: jitsnetworksecretariat@eurojust.europa.eu Head of the Genocide Network Secretariat: GenocideNetworkSecretariat@eurojust.europa.eu
4.	Name and contact details of DPO	dpo@eurojust.europa.eu
5.	Name and contact details of joint controller (where applicable)	

Nr.	Item	Description
	<p>[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.]</p>	
6.	<p>Name and contact details of processor (where applicable)</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>European Commission Directorate-General for Informatics (DIGIT) B-1049 Brussels Email: DIGIT-MOU@ec.europa.eu</p>
7.	<p>Purpose of the processing</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"> • Authorising and validating of accounts <ul style="list-style-type: none"> ○ For Extranet RA owners to set up, maintain, and update their respective Extranet RA. ○ For Eurojust authorised external partners (e.g. contact points) to facilitate exchange of non-confidential and non-operational information. • Monitor and detect external security threats to the infrastructure
8.	<p>Description of categories of persons whose data are processed and list of data categories</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"> 1) Eurojust post holders, managing the Extranet accounts, from JITs and GEN, : Name, surname, rank/position, business contact details (email address, telephone number), IP address (processed only in the backend). 2) External partners e.g. National Experts and contact points: Name, surname, rank/position, business contact details (email address, telephone number, national authority/organisation, and address of the national authority), account email address (as inserted in the EU login) and IP will be processed in the backend. 3) Administrator (security screened contractor working in the Information Management Unit), webmaster and editor from

Nr.	Item	Description
		<p>the respective Extranet (JITs, GEN):</p> <p>Email (as inserted in the EU login), and IP address will be processed in the backend.</p> <p>The authentication to the Extranet is done via EU Login where the accounts are created. After completing the authentication, the EU Login ID will be recorded in the backend of the Extranet. The EU Login ID is composed of a random string of numbers and letters. For the processing of the data please consult the EC's data protection notice on the EU login.</p>
9.	<p>Time limit for keeping the data</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 administrative personal data published on the Extranet of the Eurojust post holders/secretariats from JITs, GEN are kept until they have a valid account with access to the Extranet.</p> <p>The administrative personal data published on the Extranet of the external partners are kept until the account is terminated either based on user's request, or based on information provided by the National Authority, i.e., the practitioner/expert left the position/office/national authority.</p> <p>The account data visible only to the administrator and webmaster are kept until the account is valid.</p> <p>The log data are deleted after the first 1000 logs.</p> <p>The data submitted in the submission form on the Extranet to request access to the Extranet and for validation of the accounts is kept until the account validation process is completed.</p>
10.	<p>Recipients of the data</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>	<ol style="list-style-type: none"> 1) Data described in point 1) under Section 8, Eurojust post holders, managing the Extranet accounts, from JITs, GEN: <ol style="list-style-type: none"> a. Name, surname, rank/position, business contact details (email address, telephone number) will be made available upon the post-holder's consent in their Extranet b. Email address as inserted in the EU Login account will be visible in the backend of the Extranet accessible by Extranet administrator, Editor and Webmaster c. IP address is only visible to the Extranet Administrator (Security screened contractor working in the Information Management Unit), in case there is a need for e.g. blocking a specific IP address. 2) Data described in point 2) under Section 8, External partners e.g. National Experts and contact points: <ol style="list-style-type: none"> a. Name, surname, rank/position, business contact details (email address, telephone number) will be made available on the Extranet site upon the external

Nr.	Item	Description
		<p>partners written consent;</p> <ul style="list-style-type: none"> b. Email address as inserted in the EU Login account will be visible in the backend of the Extranet accessible by Extranet administrator, Editor and Webmaster; c. IP address is only visible to the Extranet Administrator (Security screened contractor working in the Information Management Unit), in case there is a need for e.g. blocking a specific IP address. <p>3) Data described in point 3) under Section 8, Administrator, Webmaster, Editor:</p> <ul style="list-style-type: none"> a) Email address is visible in the backend for Administrator, Webmaster, and Editor b) IP address is only visible to the Extranet Administrator (Security screened contractor working in the Information Management Unit), in case there is a need for e.g. blocking a specific IP address. <p>Outside Eurojust:</p> <p>- DIGIT and subcontractor AWS have access to the backend/account data for hosting of the Extranet. The Cloud II Framework Contract (FwC ref. 2020-1742) between DIGIT and AWS applies here for third party hosting services. DIGIT will access the data only after obtaining permission from Eurojust and only in case of a security risk. For example if the administrator account is blocked, DIGIT then needs to unblock this.</p>
11.	<p>Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?</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. DIGIT does make use of Amazon for the cloud hosting, however, all data will reside within the EU, Ireland region as per contract between DIGIT-AWS (Cloud II FwC, REF. 2020-1742), as reported by DIGIT.</p>
12.	<p>General description of security measures, where possible.</p> <p>[Include a general description of your security measures that you could also provide to the</p>	<p>The data are hosted via EC's DIGIT project and stored in an encrypted form in DIGIT's cloud, hosted in Amazon AWS EU regions, specifically in Ireland, the Dublin AWS region.</p> <p>The external Drupal developer with access to the data has a</p>

Nr.	Item	Description
	public.]	security clearance and is bound by the specific contract to comply with EJ rules and regulations and NDA with Eurojust.
13.	<p>For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the data protection notice:</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 Data protection Notice.</p> <ul style="list-style-type: none"> • Data protection notice for processing of personal data in the context of functioning and administration of JITs Restricted Area website. • Data protection notice for processing of personal data in the context of the Genocide Network Secretariat.