EUROJUST
The European Union's Judicial Cooperation Unit
P.O. Box 16183 – 2500 BD The Hague • The Netherlands

DATA PROTECTION NOTICE
For processing of personal data in the context of Core International Crime Evidence Database (CICED) - Eurojust Analysis Solution (analysis tool(s))

As Eurojust collects and further processes personal data, it is subject to *Regulation (EU) 2018/1725 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* ('the Regulation').

The following information is provided as per Article 15 of the Regulation.

1. Context of the processing activity and Controller

Regulation (EU) 2022/838 stipulates an obligation for Eurojust to facilitate the preservation, analysis and storage of evidence in the field of Core International Crimes. To comply with this, Eurojust collects operational personal data from competent national authorities and stores this into the Digital Storage Solution. In order to comply with its extended mandate introduced by Regulation 2022/838, Eurojust has implemented analysis tools behind a dedicated environment to allow analysis of operational data received in the context of the new mandate.

Collection and processing of the administrative personal data required for the functioning of the tools is under the responsibility of the Controller, who is the Head of Information Management Unit and can be contacted at ICTProjects2@eurojust.europa.eu.

The operational personal data stored in the analysis tools remain under the responsibility of the College of Eurojust. The relevant Data Protection Notice on the processing of operational data by Eurojust is available on the Eurojust website.

2. What personal information do we collect, for what purpose, under which legal bases and through which technical means?

Purpose of the processing

The administrative personal data are processed to create and manage the accounts and folders to be used to access the analysis tools via the dedicated environment, to analyse and detect technical and performance issues, and to detect external security threats to the Eurojust infrastructure and/or identify unauthorised attemps to access the system.

The operational personal data are processed for the purposes to support Member States' action in combating genocide, crimes against humanity, war crimes and related criminal offences, including by preserving, analysing and storing evidence related to those crimes and related criminal offences and enabling the exchange of such evidence with, or otherwise making it directly available to, competent national authorities and international judicial authorities, in particular the International Criminal Court.

Types of personal data

The following **categories of personal data** are processed in the context of the above mentioned processing activity:

Administrative personal data:

1) Eurojust post-holders from the Digital Infrastructure Sector, Data Protection, Members for the National Desks, Liaison Prosecutors, Representative of Denmark, and Casework Unit

   - Name
   - Surname
   - Email

2) Technical logs for troubleshooting purposes.

3) Access logs available to ICT Security via Splunk for monitoring the use of the system and carry out tasks (e.g. detect possible intrusion).

Operational personal data: the data categories processed will be in accordance with Article 27 of and Annex II of the Eurojust Regulation. To know more on how Eurojust processes operational personal data, please consult our Data Protection notice regarding the processing of operational personal data.

Legal basis

The legal basis for processing of personal data are:

Regulation (EU) 2022/838 of 30 May 2022 Article 4(1)(j) of the Eurojust Regulation: to support Member States' action in combating genocide, crimes against humanity, war crimes and related criminal offences, including by preserving, analysing and storing evidence related to those crimes and related criminal offences and enabling the exchange of such evidence with, or otherwise making it directly available to, competent national authorities and international judicial authorities, in particular the International Criminal Court;

Regulation (EU) 2018/1725 of 23 October 2018 Article 5 (1)(b): to comply with the extended mandate of Eurojust by Regulation (EU) 2022/838 (Art. 4(1)(j));

Regulation (EU) 2018/1725 of 23 October 2018 recital 22, second sentence: to be able to maintain and support IT systems needed for the operation of Eurojust.

Regulation (EU) 2018/1725 of 23 October 2018 Article 88(1): to be able to maintain the logs needed for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the operational personal data, and for criminal proceedings.

Technical means

Your administrative personal data are managed in Active Directory, the system used for the accounts creation and access management for the analysis tools.

The analysis tools are fully hosted on Eurojust premises and maintained by authorised Eurojust staff members.

3. Who has access to personal data and to whom is it disclosed?

For the purpose detailed above, access to the personal data is given to the following persons, without prejudice to a possible transmission to the bodies in charge of a monitoring or inspection task in accordance with European Union law:

For administrative personal data: duly authorised members of the Digital Infrastructure Sector and application managers team under the Information Management Unit for granting permissions to the analysis tools. User Support team for the creation of the accounts in Active Directory. No external contractors nor consultants will have access to the data stored in the analysis tools.

The administrative data are also sent to Splunk, where dedicated staff members from ICT Security and Data Protection will have access to. These logs are used to detect or investigate possible attempts to gain access to the Eurojust infrastructure by unauthorised actors.

For operational personal data, only duly authorised staff members from the Operations Department(Casework Unit), National Members/Liaison Prosecutors/Representative of Denmark and authorised staff from the National Desks/Liaison Prosecutors posted in Eurojust, Representative of Denmark will have access to the data in accordance with Article 34 of Eurojust Regulation. The system administrator from the Digital Infrastructure Sector will have access to the analysis tools' database for technical support. No other staff members nor external consultants or contractors will have access to these data.

4. How do we protect and safeguard information?

Personal data is protected through following industry best practices.

All data are stored on Eurojust premises in physically secure data centres. Eurojust's data centres are protected with security controls and accessible only by verified and authorised people. Eurojust has also several layers of protection in place and dedicated systems to detect and block unauthorised and/or malicious traffic.

5. How can you verify, modify or delete your information?

For administrative personal data: you have the right of access to your personal data and to relevant information concerning how we use it. You have the right to rectify your personal data. Under certain conditions, you have the right to ask that we delete your personal data or restrict their use, where applicable, you also have the right to data portability and the right to object to the processing of your personal data, on grounds relating to your particular situation. We will consider your request, take a decision and communicate it to you. For more information, please see Articles 14 to 21, 23 and 24 of Regulation (EU) 2018/1725. Please note that in some cases restrictions under Article 25 of Regulation (EU) 2018/1725 may apply (see College Decision 2020-04 of 15 July 2020 on internal rules concerning restrictions of certain data subjects rights in relation to the processing of personal data in the framework of activities carried out by Eurojust, available in the Eurojust website here).
If you wish to exercise your data subject rights, please make use of the following email address: usersupport@eurojust.europa.eu, by explicitly describing your request.

For operational personal data and the exercise of your rights, please consult Articles 31, 32, 33 of Eurojust Regulation, Articles 80, 81 and 82 of the Regulation 2018/1725 and our Rules of procedures on the processing and protection of personal data at Eurojust. Any request regarding your rights should be directed to Eurojust (via email dpo@eurojust.europa.eu) 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.

6. How long do we keep your personal data?

Administrative Personal Data:

Administrative personal data are kept in the analysis tools until the users need access to the system, with a yearly review of the accounts to ensure only those who need access to the system have an account.

Access logs are also sent to Splunk 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). Logs kept in the analysis audit tool are kept for three years to allow sufficient time to DPO for auditing.

Operational Personal Data:

The operational personal data 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. The regular reviews on the need to store the data shall be carried out every three years after they were entered in the Eurojust Digital Storage.

7. Contact information

In case of queries regarding the processing of personal data, Eurojust Data Protection Officer can be contacted via email address: dpo@eurojust.europa.eu .

8. Recourse

You have the right to lodge a complaint to the European Data Protection Supervisor via email: edps@edps.europa.eu or following the link: https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en if you consider that your rights under the Eurojust Regulation or Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data.