

DATA PROTECTION NOTICE

For processing of personal data in the context of the Eurojust Digital Transfer Solution

1. Context and Controller

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 and Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA.*

In order to comply with its extended mandate introduced by Regulation 2022/838, Eurojust has implemented a tool (Eurojust Digital Transfer Solution) to allow the exchange for large files. The system is fully hosted on premises and managed by Eurojust.

Collection and processing of the administrative personal data required for the functioning of the Eurojust Digital Transfer Solution 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 data transmitted to Eurojust via the Eurojust Digital Transfer Solution 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?

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.

Purpose of the processing

The administrative personal data are processed to create and manage the accounts and folders to be used to transfer large files to Eurojust, to analyse and detect technical and performance issues, and

to detect external security threats to the Eurojust infrastructure and/or identify unauthorised attempts 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

Technical means

Your administrative personal data are managed in [Active Directory](#), the system used for the accounts creation and management for the Eurojust Digital Transfer Solution.

The Eurojust Digital Transfer Solution is a large file transfer platform, which allows external users to share large files with Eurojust. The Eurojust Digital Transfer Solution is fully hosted on Eurojust premises and maintained by authorised Eurojust staff members.

Your administrative personal data are saved also in the Eurojust Digital Transfer Solution as logs for 7 days, after which they are sent automatically to Splunk. All these systems are fully hosted on Eurojust premises, with access restricted to authorised Eurojust staff members. provided by the means of logs files fully stored in Eurojust premises.

Mobile Pass is a on premises solution that is used for multi factor authentication. No personal data is shared by Mobile pass outside Eurojust, as defined by the application [Privacy Policy](#). The authentication takes place on premises.

Types of personal data

Administrative Personal data collected and further processed:

1) Eurojust post-holders from Back Office and Casework Unit

- Name
- Surname
- Email
- Mobile phone number

If the user decides to use the SMS as 2 factor authentication method, mobile phone number is used.

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:

- User ID
- Device ID

Note that User ID and Device ID are collected when the initial registration takes place, by the app itself.

These data are only used to aid in case of troubleshooting.

2) External users authorized to transfer large files to Eurojust

- Name
- Surname
- Email
- Mobile phone number

If the user decides to use the SMS as 2 factor authentication method, mobile phone number is used.

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:

- User ID
- Device ID

Note that User ID and Device ID are collected when the initial registration takes place, by the app itself.

These data are only used to aid in case of troubleshooting.

- Technical logs for troubleshooting purposes.

Operational personal data: the data categories transferred will be in accordance with Article 27 of and Annex 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](#).*

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 Back Office and User Support under the Information Management Unit. No external contractors nor consultants will have access to the data stored in the Eurojust Digital Transfer Solution. In case of need for consultants to support the troubleshooting of the system, they will only have access to the testing environment, where no real data are stored.

The administrative data are also sent to [Splunk](#), the Security Information and Event Management, 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 and authorised staff from the National Desks in Eurojust will have access to these data. 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 have the right to object to our processing of your personal data, on grounds relating to your particular situation, at any time. 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 our [Rules of procedures on the processing and protection of personal data at Eurojust](#).

6. How long do we keep your personal data?

Administrative Personal Data:

Administrative personal data are kept in the Eurojust Digital Transfer Solution 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.

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).

Operational Personal Data:

Operational data uploaded in the Eurojust Digital Transfer Solution will be deleted within 7 days from upload. The operational personal data will be then 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.

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.