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 Infrastructure Log files

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 and Controller

Collection and processing of personal data within Eurojust system log files is under the responsibility of the Controller, who is the Head of Information Management Unit and can be contacted at ICTProjects2@eurojust.europa.eu.

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) 2018/1725 of 23 October 2018 (a2) (a) as per 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 5 (1b) necessary for compliance with legal obligation incumbent on controller

To be compliant with security regulations

Purpose of the processing
The log file data is used to analyse and resolve technical issues, detect performance issues, identify failing components, detect unauthorised access and security threats to the infrastructure or persons at Eurojust. Furthermore it is used to ensure compliance with Eurojust regulations and policies.

Technical means
Your personal data are provided by the means of:
Videoconferencing systems – log files
Network monitoring systems – syslog are retrieved via the corresponding management interface
VPN – syslog are retrieved via the corresponding management interface
Access Control Server (ISE) – syslog are retrieved via the corresponding management interface
Fax – log files
WIFI – syslog are retrieved via the corresponding management interface
VDI (Transfer Solution, Storage Solution, Analysis Solution) – syslog are retrieved via corresponding management interface

For information concerning the personal data and logs collected for the users assigned an Eurojust mobile phone, please refer to the dedicated Data Protection Notice "Data Protection Notice Mobile Phones".

Types of personal data

Personal data collected and further processed concern Eurojust infrastructure log files. Information can relate to the following data:

a) Active Directory User name
b) Time and Date
c) IP address of user's device
d) Media Access Control (MAC) address
e) Uniform Resource Locator (URL)/ web address
f) Dialled number
g) Dialling number
h) Duration of the connection
i) Address of the videoconference (for Eurojust operated internal Videoconferencing systems)

For Videoconferencing systems accessed by external participants via the Cisco Meeting App (for internal and external users) the following personal data are collected:

a) Username provided by the data subject
b) IP address of user's device
c) Address of the videoconference
d) Time and Date
e) Duration of the connection.

For Videoconferencing systems accessed by internal and external participants using the WebEx Meetings, refer to the corresponding Data Protection Notice.

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

For the purpose detailed above, access to your 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:

Access restrictions apply based strictly on need to know basis.

a) User Support
b) Back Office
c) Application Managers
d) ICT Security (via Splunk)

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?

You have the right to access your personal data and to relevant information concerning how we use your personal data. You have the right to request rectification of your personal data. You have the right to ask that we delete your personal data or restrict its use. Where applicable, you have the right

to object to our processing of your personal data, on grounds relating to your particular situation. Where applicable, you the right to your data portability. 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).

To exercise your rights, please contact via the following email address: usersupport@eurojust.europa.eu.

6. How long do we keep your personal data?

The retention period for Audit log is in line with the POLICY- Audit log as approved by the AD 08/03/2018.

Videoconferencing systems – retention period is up to 1 year maximum (or less in case of installation of a Cisco patch)

Network monitoring systems – retention period is 1 year

VPN – retention period is 3 months

Access Control Server (ISE) – retention period is 5 days on ISE appliances itself. The logs however are forwarded to SPLUNK where they are kept for the duration of 1 year.

Blackberry Server – retention period is 1 year

Fax – retention period is 3 months

WIFI – retention period is 1 year

VDI (Transfer Solution, Storage Solution, Analysis Solution) – retention period is 1 year

7. Contact information

In case of queries regarding the processing of personal data you may also contact the Data Protection Officer of the Eurojust (dpo@eurojust.europa.eu).

8. Recourse

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