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 Eurojust Security Information and Event Management (SIEM) solution SPLUNK

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*.
Collection and processing of personal data within Security Information and Event Management (SIEM) solution SPLUNK 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 base 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 data protection and security regulations.

Purpose of the processing

The purpose of implementing a SIEM solution is to allow ICT Security to identify security threats and incidents and to carry out ICT forensics during a security investigation through manual examination and cross referencing of logs from different devices; through reports and alerts generated automatically based on pre-defined patterns; through the generation of anonymised statistics.

For the Back office the purpose of processing information in the SIEM solution is to analyse and resolve technical issues, detect performance issues, identify failing components and detect unauthorised access.

Technical means

Your personal data are provided by means of log files sent to SPLUNK from other systems including: authentication and identity management solutions, application and network firewalls, load balancers, telephony and video conference management solutions, anti malware solutions, wired and wireless network control and management solutions, Internet gateway routers, administrative applications and operational applications (including the Eurojust Transfer Solution and Eurojust Digital Storage Solution) deployed on the Eurojust on premise infrastructure.

Types of personal data

Personal data collected and further processed concern all Eurojust post-holders and contractors with access to Eurojust systems and applications. Information can relate to the following data:

a) Media access control (MAC) address
b) IP address
c) Username

d) Timestamp
e) Action
f) Other type of personal data included by the user in file properties such as personal data in file names.

3. Who has access to your 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 to duly authorised members of:

a) ICT Security
b) ICT Security consultants contracted under the Eurojust Framework contracts aligned with Regulation (EU) 2018/1725
c) Back Office
d) Back Office consultants
e) Data Protection Office

4. How do we protect and safeguard your information?

Personal data is protected through following industry best practices.

Eurojust applies relevant security measures to ensure the confidentiality, security and availability of all the data – including personal data – processed by SPLUNK. These include technical, personnel and procedural security measures based on industry best practices and security standards

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

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.

Identification data of individuals can be corrected at any time.

6. How long do we keep your personal data?

Log data is forwarded to SPLUNK from the devices and solutions mentioned in section 2 aboveincluding the Eurojust Transfer Solution, Eurojust Digital Storage Solution and is kept for the duration of 1 year after which it is automatically deleted. The retention period of 1 year was determined in order to allow sufficient time for forensic investigation.

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 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 Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data.