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 IMSecretariat@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 the means of log files sent to SPLUNK from other systems. These systems are Active Directory, Firewalls, Cisco ISE, F5, Jumper Servers, Cisco Firepower, Symantec, Peter Connect, Secure Network/CMS Gateway, Wireless LAN controller, Internet Gateway router, eHR system and Network Management tool/Cisco Prime 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) 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.

a) ICT Security staff
b) ICT Security consultants
c) Back Office staff
d) Back Office consultants

4. How do we protect and safeguard your information?

Personal data is protected through following industry best practices.

Security Controls

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

In case you wish to verify which personal data is stored on your behalf by the Controller, have it modified, corrected, or deleted, or restrict the processing, or object to it or to exercise the right to data portability, please make use of the following email address: usersupport@eurojust.europa.eu , by explicitly describing your request. Any correction of your personal data will be taken into consideration from the data protection point of view.

Identification data of individuals can be corrected at any time.

6. How long do we keep your personal data?

The retention period of 1 year was determined in order to allow sufficient time for forensic investigations. After the 1 year period the data is automatically deleted.

7. Contact information

You have the right to access, rectify or erase or restrict the processing of your personal data or, where applicable, the right to object to processing or the right to data portability in line with Regulation (EU) 2018/1725.

Any such request should be directed to the Controller, by using the following email address: usersupport@eurojust.europa.eu , and by explicitly specifying your request.

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 (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.