PRIVACY STATEMENT

PROTECTION OF YOUR PERSONAL DATA

This privacy statement provides information about the processing and the protection of your personal data.

1. Introduction

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (hereafter, 'eu-LISA') is committed to protect your personal data and to respect your privacy. eu-LISA collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council 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 (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data.

The information in relation to processing operation Email Traffic Monitoring undertaken by eu-LISA Security Unit is presented below.

2. Why and how do we process your personal data?

The main purpose of processing the personal data of the eu-LISA email account owners is to ensure the implementation of the specific security measure consisting in performing the monitoring of the emails exchange at eu-LISA in order to identify potential security risks associated with the email service provided and the exchange of the organisation data therefore ensuring the functionality of the service and avoiding security breaches.

Such processing activity includes the following specific security and traffic management operations:

- To ensure security and stability for the email system and/or network.
- To detect and analyse attacks (internal and external), including but not limited to phishing attempts, spoofing or impersonations.
- To measure loads, as well as to ensure the proper functioning of the email system.

- To troubleshoot technical problems.
- To analyse security filters' efficiency in order to verify whether the content filter is not too restrictive or too lax.
- To find traces of unauthorised activity inside the Agency's IT infrastructure.
- To verify whether email users comply with the security rules on sharing information only based on the "need-to-know" principle and in the context of fulfilling the professional's tasks and responsibilities, in line with applicable normative framework. And therefore, as a mechanism for enforcing the Acceptable Use Policy.

Log analysis is done only for security purposes and not to assess staff work productivity.

Your personal data will not be used for an automated decision-making including profiling.

Your personal data processed may be reused for the purpose of procedures before the EU Courts, national courts, or the European Court of Auditors.

3. On what legal ground(s) do we process your personal data

We process your personal data, because:

(a) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body, including because it might be necessary for the management and functioning of the Agency.

eu-LISA is tasked by its founding regulation to ensure the protection and continuous running of the systems under its responsibility, and to grant "continuity and uninterrupted service" (Regulation (EU 2018/1726, Articles 2(b) and 2(e)). This processing operation relates to one aspect of the protection of said systems and the functioning of the Agency, as eu-LISA is mandated to adopt a "security plan and a business continuity and disaster recovery plan" (Regulation EU 2018/1726, Article 19(1)(z)), and to ensure "the security and the maintenance of order within the buildings, premises and land used by it" (Regulation EU 2018/1726, Article 38(1)). The present processing is directly connected with this particular legal obligation of the Agency, and complemented by the following security framework:

- Agency General Information Security Policy.
- Decision of the Management Board No 2019-148 on the Security Rules on the Protection of Communication and Information Systems in eu-LISA.
- Decision of the Management Board No 2016-133 REV 3 on the Security Rules in eu-LISA.
- Decision of the Management Board No 2019-208 on the Security Rules for Protecting Sensitive Non-Classified Information at eu-LISA.
- Decision of the Management Board No 2019-273 on the Security Rules for Protecting EU Classified Information.
- eu-LISA Acceptable Use Policy.

- Implementation of a specific security measure consisting in performing the monitoring of the emails exchange at eu-LISA in order to identify potential security risks associated with the email service provided and the exchange of the organisation data therefore ensuring the functionality of the service and avoiding security breaches, in line with obligations stemming from Article 4 and Article 8 of the Regulation (EU) 2023/2841.

4. Which personal data do we collect and further process?

In order to carry out this processing operation the Security Unit collects the following categories of personal data:

- Email header data (Sender and recipient addresses, CC/BCC fields, Subject line, Timestamps (sent/received), Message-ID and other technical headers).
- Email body content (plain text or HTML email content, embedded links and scripts).
- Attachments (file names, extensions, file content, embedded metadata.
- User and Account Identifiers (sender username, alias, organisational unit, unique ID).
- Communication Patterns and Behaviours (Frequency and volume of emails sent/received, direction of communication (internal vs external), known vs unknown recipients).
- Technical Data (IP address, device information, geographic location).
- System Logs and Metadata (email processing logs, security event logs, timestamps).

The provision of personal data is mandatory to ensure the effective management and functioning of the Agency, in line with the public interest or in the exercise of official authority vested in eu-LISA. If you do not provide your personal data, possible consequence is non-compliance with organisational policies.

We have obtained your personal data from the Agency email infrastructure, security monitoring systems, email security filters, network traffic logs. Additional contextual information may be obtained from the eu-LISA directory services and identity management systems when necessary for security incident investigation and resolution.

5. How long do we keep your personal data?

The Security Unit only keeps your personal data for the time necessary to fulfil security purposes and requirements.

When determining the maximum retention periods, the Agency takes also into account possible legal recourses, legal, auditing, archiving and reporting obligations.

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

Access to your personal data is provided to eu-LISA staff responsible for carrying out this processing operation and to authorised staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

Data processed within this processing activity might be disclosed to investigative and supervisory bodies/authorities (internal and external), such as internal investigators and to OLAF, if an investigation is launched and if the conditions for the intervention of OLAF or the investigative bodies are met.

Data processed within this processing activity might also be shared with qualified external service providers to support the email security operations (e.g., supporting the analysis of security threats and vulnerabilities, assisting with email security reporting and quarantine), which is bound by a data processing agreement that ensures appropriate protection of your personal data. In case of major cyber incidents, logs can be shared with CERT-EU, on the basis of an SLA signed between the parties.

The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

7. What are your rights and how can you exercise them?

You have specific rights as a ‘data subject’ under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. You also have the right to object to the processing or, where applicable, the right to data portability.

~~You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a).~~

Nevertheless, you should be informed that by virtue of Article 25 of Regulation (EU) 2018/1725 and of the Internal Rules laid down under Decision No 2021-096 Rev 1 of the Management Board, one or several of these rights may be restricted for a temporary period of time inter alia on the grounds of prevention, investigation, detection and prosecution of criminal offences. Any such restriction will be limited in time, proportionate and respect the essence of the above-mentioned rights. It will be lifted as soon as the circumstances justifying the restriction are no longer applicable. You will receive a more specific data protection notice when this period has passed.

As a general rule, you will be informed on the principal reasons for a restriction, unless this information would cancel the effect of the restriction as such.

You have the right to make a complaint to the European Data Protection Supervisor about the application of the restriction.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor.

8. Contact Information

- **The Data Controller**

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments,

questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, *security-coordination@eulisa.europa.eu.*

- **The Data Protection Officer of eu-LISA**

You may contact the Data Protection Officer (dpo@eulisa.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- **The European Data Protection Supervisor (EDPS)**

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.