PROTECTION OF YOUR PERSONAL DATA

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

1. Introduction

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (hereafter, 'eu-LISA') is committed to protecting your personal data and to respecting your privacy. eu-LISA collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council dated 23 October 2018 on the protection of natural persons with regard to the processing of personal data by 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.

Information related to the processing operation for Access to eu-LISA premises, undertaken by the Security Unit, is presented below.

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

The Security Unit collects and uses your personal information to prevent, to deter, to impede or to detect actions/events that might affect the security of the Agency, its premises, personnel or assets.

In order to allow access to eu-LISA premises (Tallinn and Strasbourg) security staff collects data to be processed for the preparation of access badges. Badges are printed and registered in the access control system. For each individual, specific access rights are assigned, depending on the business need to access specific areas, according to the tasks and responsibilities they have to perform inside eu-LISA premises. Fingerprint templates persons, are locally recorded in the badge's memory, with no storage in the central database.

Your personal data will not be used for any automated decision-making, including profiling.
3. On what legal ground(s) do we process your personal data

- Commission Decision 46/2017 on security of information and communication systems
- Decision of the Management Board 2016-133 Rev 3 on Security rules in eu-LISA
- Commission Decision 2015/444 on the security rules for EUCI
- Access Rules in eu-LISA

What personal data do we collect and further process?

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

- Name, surname, photo, type of contract – for staff, interns, SNEs and intramuros
- Name, surname, ID number – for visitors
- Fingerprint of the person who has been given an access token (only for access to the eu-LISA Strasbourg premises and Tallinn site dependent on business needs)

The provision of personal data is mandatory to meet a Decision of the Management Board 2016-133 Rev 3 on Security rules and Access Rules in eu-LISA. If you do not provide your personal data, the possible consequences could result in a non-compliance with the Security rules.

4. How long do we keep your personal data?

The Security Unit only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing.

Name, surname, photo and ID number for badges are stored for 2 years after the validity expiration time or after return. The electronic format is kept in the Security Unit, partially in a shared folder that is restricted to only controller personnel and partially on 1 out of domain laptop for technical use.

Fingerprints are destroyed with the badge immediately after it has been returned to the Security Unit and no longer needed.

5. 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.

Access to the data is restricted based on access rights. The Security Unit keeps the data in dedicated folders on a Tallinn drive. Access to said data is limited to Security Unit personnel and security guards.

The information collected will not be given to any third party, except to the extent and for the purposes eu-LISA may be required to do so by law.
6. 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. Where applicable, you also have the right to object to the processing or the right to data portability.

You have consented to provide your personal data to the Security Unit for the present processing operation. You can withdraw your consent at any time by notifying the Data Controller. The withdrawal will not affect the lawfulness of the processing carried out before you withdrew consent.

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.

7. 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 Unit, eulisa-SECURITY[at]eulisa.europa.eu

- The Data Protection Officer of eu-LISA

You may contact the Data Protection Officer (dpo[at]eulisa.europa.eu) regarding 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[at]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.