

## **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 "Identity & Access Management Service (IAMS)" undertaken by the Corporate Services Department of eu-LISA (CSD) is presented below.

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

Corporate Services Department collects and uses your personal information to ensure the appropriate level of security is applied in a consistent fashion across eu-LISA IT services with the ability to identify the user of the service, authenticate that user, and / or determine his or her authorisations and roles within the context of their service.

Your personal data can be processed in the following cases:

- Collection of information about users from authoritative sources (internal HR databases, transfers from external entities such as other European Institutions, Agencies and Bodies, Intranet, Extranet, SECABC, VPN, training, Planview, ProjectPlace, Knomnavigator, Condeco, Internet email services, iLearn etc.)
- Calculation of access rights based on policies defined by the HR services and on the attributes of users.
- Assignment of access rights on request by users or service providers.
- Input and storage of user information in a common repository or set of repositories
- Authentication of users "on behalf of" and transmission of authorization data to the registered information systems that needs it
- Validate and execute a user's request to reset their password if they are unable to do it themselves: validation of the request may involve checking personal details supplied by the user against the database
- Activate or deactivate a user account or an access right
- Check user information against the data sources for diagnostic purposes and security reasons

## PUBLIC

- Correct (and amend if necessary) user details in order to resolve conflicts that are preventing automatic processes from working
- Create reports based on the stored data

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 contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(b) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

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

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

- Name, contact details, email and affiliation
- Contract details (Starting date, contract end date)
- Personal identification numbers & pictures (uploaded by the user)
- Sign-In Logs
- Azure audit logs

The provision of personal data is mandatory to meet a contractual requirement resulting from the onboarding process after signing an employment contract or an external support contract with Intramuros. ~~If you do not provide your personal data, possible consequences are inability to onboard the user and denial of access to eu-LISA systems.~~

We have obtained your personal data from the respective responsible entities (File Manager in eu-LISA or contractors for Intramuros).

### **5. How long do we keep your personal data?**

Corporate Services Unit only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely:

- Name, contact details and affiliation, Personal identification numbers & pictures - As long as the individual has any relationship with the Agency;
- Sign-in Logs– 30 days
- Azure audit logs – 30 days
- On-premises disabled users – 365 days
- On-premises audit logs (Splunk) – 365 days
- On-premises sign-in logs (Splunk) – 365 days
- Users in Azure Entra ID are permanently deleted automatically 30 days after they are moved to the deleted users list.
- Disabled users in on-premises Active Directory are deleted after one year.
- ~~History of identity changes – As long as the individual is active. This information should be kept for avoiding duplication of identities~~

- ~~Log Files – 6 months After that period the file may be transferred to the Historical Archives.~~

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.

The following data recipients will have access to your personal information within the context of this processing activity:

- Both eu-LISA staff and external staff with eu-LISA accounts: all user accounts in the eu-LISA domain have read access to other user accounts in the domain. This means that end-user information Corporate Services Department registers is visible to both eu-LISA staff and external staff with eu-LISA accounts. Any eu-LISA user account can see the phone number and organisational details of other users (e.g., in Outlook application) thanks to this.
- Support Team, Administrators Teams and Security Operations Teams of the systems and platforms: have read/write access to all accounts data and derived activity logs.
- European Commission and other Agencies: for these categories limited information is released for the purpose of update of their address book, namely: first name, last name, telephone and organisation.

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. Where applicable, you also have the right to object to the processing or 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).

You have consented to provide your personal data to Corporate Services Unit for the publication of photos in the Internal Active Directory. You can withdraw your consent at any time by notifying the Data Controller (i.e., Corporate Services Unit). The withdrawal will not affect the lawfulness of the processing carried out before you have withdrawn the 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.

## **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

“HoCSU@eulisa.europa.eu”

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

You may contact the Data Protection Officer ([dpo@eulisa.europa.eu](mailto: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](mailto: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.