European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2023-0014 Identity & Access Management Service - EU Login

1 PART 1: PUBLIC - RECORD (ARTICLE 31[1])

1.1 GENERAL INFORMATION

Record reference	DPR-ELA-2023-0014
Title of the processing operation	Identity & Access Management Service - EU Login
Controller entity	Resources Unit
Joint controllers	☒ N/A ☐ YES, fill in details below
Processor(s)	☐ N/A ☒ YES, fill in details below
Internal organisation(s)/entity(ies) Names and contact details	☒ N/A ☐ YES
External organisation(s)/entity(ies) Names and contact details	☐ N/A ☒ YES **Service provider:** European Commission – Directorate General Informatics (DIGIT) 1049 Bruxelles/Brussel, Belgium
Data Protection Officer Name and contact details	Laura NUNEZ BAREZ European Labour Authority Landererova 12, 811 09 Bratislava I Slovakia Email: data-protection@ela.europa.eu
Corporate Record	☐ Yes ☒ No
Language of the record	English

[1] *Pursuant to **article 31** of the new data protection regulation for EU institutions and bodies (**Regulation (EU) 2018/1725**) each controller and processor have to maintain a **record of processing activities** under its responsibility that contains at least the information listed under that article.*

1.2 PURPOSE AND DESCRIPTION OF THE PROCESSING

1.2.1 Purpose

The European Labour Authority (ELA) uses the European Commission's Identity Access Management Service (IAMS), including EU-login, to provide a common way for users to register or be registered for access to a number of different ELA/Commission information systems or services.

The purpose of IAMS is to manage user populations and their rights in the context of IT systems. The main purpose is to ensure the appropriate level of security is applied in a consistent fashion across the Authority and the Commission 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.

Additional purposes for this processing operation, regarding users that have an employment relationship with ELA, are the following:

- services, allowing users contact details to be found (e.g. e-mail address book or telephone directory)
- selection of users from lists, usually based on some selection criteria
- construction of lists of users, primarily e-mail distribution lists
- customisation of user interfaces according to users' individual characteristics

1.2.2 Processing for further purposes

☒ Archiving in the public interest
☐ Scientific or historical research purposes
☐ Statistical purposes
Safeguards in place to ensure data minimisation
☐ Pseudonymisation
☐ Any other, specify

1.2.3 Modes of processing

1. ☒ Automated processing (Article 24)
    a. ☒ Computer/machine
        i. ☐ automated individual decision-making , including profiling
        ii. ☒ Online form/feedback
        iii. ☒ Any other, specify

2. ☐ Manual processing
    a. ☐ Word documents
    b. ☐ Excel sheet
    c. ☐ Any other, specify

3. ☐ Any other mode, specify

Description

For ELA staff

Collection of information about users from authoritative sources (internal HR databases, transfers from external entities such as other European Institutions, Agencies and Bodies, etc.)
Calculation of access rights based on policies defined by the Authority/Commission 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
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

For self registered individuals

Self register any user into the external domain of EU Login
Assign a role or an access right to a user
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, block or delete an user account
Create reports based on the stored data

1.2.4 **Storage medium**

1. ☐ Paper
2. ☒ Electronic
    a. ☐ Digital (MS documents (Word, excel, Powerpoint), Adobe pdf, Audiovisual/multimedia assets, Image files (.JPEG, .PNG, etc.))
    b. ☐ Databases
    c. ☒ Servers
    d. ☐ Cloud
3. ☐ External contractor premises
4. ☐ Others, specify

Description:

Electronic storage on disks of the servers and databases in the Commission's Data Centre, with backup to the Commission's Data Centre back-up systems.

1.2.5 Comments on the processing of the data

This record is linked to the record published by the European Commission Record '*DPR-EC-03187.1Identity & Access Management Service (IAMS)*', available **here**.

1.3 DATA SUBJECTS AND DATA CATEGORIES

1.3.1 Data subjects' categories

1. Internal to organisation	☒ Yes Any individual user registered in the HR records of the European Labour Authority for which by applying the defined basic entitlements policy will result in a digital identity of the user.
2. External to organisation	☒ Yes Anyone else that requires a digital identity to access any IT system of the ELA/Commission, whether self-registered users or Staff of other EU Institutions, Agencies and Bodies

1.3.2 Data categories/fields

For EU Institutions, agencies and bodies staff (EU Staff)

IAMS is processing only identification data (to identify the individuals):

Personal information:

first, middle and last name(s) as provided by the HR Systems,
date of birth
personal title
history of changes in the name
an unique number per EU Institution, Agency or Body attributed by the HR System of each entity (Personal Number)
an unique identification number in attributed by the Commission HR System (Per_ID)
Based on the above, IAMS generates an unique:

- **username or account** (based on specific rules depending on whether the user is EC Staff or not)
- **e-mail address** (based on specific rules depending on whether the user is EC Staff or not)

IAMS keeps a history of:

- name changes (not to create multiple identities for the same individual)
- password changes (to enforce regular changes (passwords are irreversibly encrypted))
- last authentication and authenticated account activity (Date and time of the most recent successful and unsuccessful authentication and number of good logins and failed attempts)

This additional information is used to diagnose and resolve problems and to deal with security incidents as well as to avoid duplicated accounts.
This information can help in following up any doubtful/malicious activity relating to the user account.

Administrative data (to identify the relationship with the organization):

the entity where the individual is assigned
the job title
the job status
information related to the start and end of the contract
office address and phone number
mobile phone number (for two-factor authentication, when available into the HR System)

Based on the above and on the HR "basic entitlements policy", IAMS generates **access rights - information about group membership** (for granting access to the intended systems)

For self registered individuals

Personal information (as provided by the individual during self-registration):

first, middle and last name(s)
e-mail address
username
mobile number, when provided for two-factor authentication
Social-media/eID identifier (in case of using a social media account or the eID for authentication).

For the two-factor authentication using the EU Login mobile app, the Operating System software of the mobile device is stored as well.

Log files for both users

Each time the user logs in to a site protected by EU Login, the identifier, the site and the time will be recorded in a log file. The exact time of log-out will also be recorded for security purposes.

1.3.2.1 Special categories of personal data

Indicate if the processing operation concerns any 'special categories of data' which fall(s) under Article 10(1), which shall be prohibited unless any of the reasons under article 10(2) applies:

☐ **Yes , the processing concerns the following special category(ies):**

Data revealing

☐ racial or ethnic origin,
☐ political opinions,
☐ religious or philosophical beliefs,
☐ trade union membership,

Or/and,

☐ Genetic data, biometric data for the purpose of uniquely identifying a natural person,
☐ Data concerning health,
☐ Data concerning a natural person's sex life or sexual orientation.

☒ **N/A**

1.3.2.2 Data related to 'criminal convictions and offences'

The data being processed contain sensitive data which fall(s) under Article 11 'criminal convictions and offences'	**N/A** ☒ **Yes** ☐

1.4 RETENTION PERIOD

Indicate the administrative time limit(s) for keeping the personal data per data category, and if known, specify the start/end date, or describe the specific start/end moment of each time limit:

Data category	**Retention period**
Data related to ELA staff and history of identity changes	As long as the individual has any relationship with the European Labour Authority. This information should be kept to avoid duplication of identities (First/Last Name, UserID)
Data related to self-registered users	Until the individual himself/herself requests the deletion or delete the account himself/herself
Log files	6 months

Description
Data created by the system in respect of an individual user is maintained as long as the user is active.
For ELA Staff and other EU Institutions, Agencies and Bodies, the above-mentioned data, will be limited to the information provided by each one of them.
Since it is possible for users to change their identifiers, a history of changes must also remain accessible.
Data that is obtained by IAMS from external systems can only be modified by changing the data in the source system.
Any modification will be reflected automatically in IAMS.
Self registered individuals have full control on their data.
Data that is maintained by IAMS itself can be corrected by the individual participating system.

1.5 RECIPIENTS

Origin of the recipients of the data	
1. ☒ Within the EU organization	System Administrators of European Labour Authority Information Systems (e.g.help desk, authorised support Staff)
2. ☒ Outside the EU organization	European Commission, DG DIGIT Other EU Institutions, Agencies and Bodies, information about the consolidated Address Book

Categories of the data recipients
1. ☒ A natural or legal person 2. ☐ Public authority 3. ☐ Agency 4. ☐ Any other third party, specify

Description

System Administrators of the Information Systems consuming IAMS data can potentially access all data provided via IAMS.

1.6 INTERNATIONAL DATA TRANSFERS

Transfer to third countries or international organisations of personal data	
1. Transfer outside of the EU or EEA ☒ N/A, transfers do not occur and are not planned to occur ☐ YES,	
Country(ies) to which the data is transferred	
2. Transfer to international organisation(s) ☒ N/A, transfers do not occur and are not planned to occur ☐ Yes, specify further details about the transfer below	
Names of the international organisations to which the data is transferred	

1.7 INFORMATION TO DATA SUBJECTS ON THEIR RIGHTS

Rights of the data subjects
Article 17 – Right of access by the data subject *Article 18 – Right to rectification* *Article 19 – Right to erasure (right to be forgotten)* *Article 20 – Right to restriction of processing*

Article 21 – Notification obligation regarding rectification or erasure of personal data or restriction of processing

Article 22 – Right to data portability

Article 23 – Right to object

Article 24 – Rights related to Automated individual decision-making, including profiling

1.7.1 Privacy statement

☒ The data subjects are informed about their rights and how to exercise them in the form of the a privacy statement attached to this record.

Publication of the privacy statement

☒ Published on website

Web location:

- ELA internal website ☒ (URL: **SharePoint on Personal Data**)
- External website ☒(URL: https://www.ela.europa.eu/en/privacy-policy)

☒ Other form of publication, specify

☒ Guidance for Data subjects which explains how and where to consult the privacy statement is available and will be provided at the beginning of the processing operation.

Description:
Any user of the IAMS can access the above mentioned link to find the privacy statement. For self-registered users consent is given only after reading, understanding and agreeing on the Privacy Statement by clicking the relevant box.

1.8 SECURITY MEASURES

Short summary of overall Technical and Organizational Measures implemented to ensure Information Security:

Description:
The European Labour Authority relies in the European Commission, DG DIGIT, to implement the appropriate organizational and technical security measures.

IAMS has put in place all necessary measures in accordance to Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

IAMS takes all reasonable measures to protect the Confidentiality, Integrity and Availability of information stored in IAMS, whether provided by other IT systems or by the individual directly.

The measures include the use of physically separate machines to hold strong user passwords, located in computer rooms (EC DIGIT data centres) that are protected against unauthorised physical access. Passwords are furthermore stored in irreversible hashes, with the only purpose to authenticate an individual.

Other personal information is protected in line with its declared level of privacy: thus, whereas private group memberships of users will only be revealed to the owning application and designated administrators, public group membership may be available to any application using IAMS in the context of calculated access rights.