**European Labour Authority**

DATA PROTECTION OFFICER

**RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA**

DPR-ELA-2024-0007 Stakeholder Relationship Management (SRM) system

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

## 1.1 GENERAL INFORMATION

| | |
|---|---|
| **Record reference** | DPR-ELA-2024-0007 |
| **Title of the processing operation** | Stakeholder Relationship Management (SRM) system |
| *Last updated on* | *May 2026* |
| **Controller entity** | European Labour Authority, Operations Department, Coordination and Liaison (NLO and Brussels Office) Sector |
| **Joint controllers** | ☒ N/A ☐ YES, fill in details below |
| **Processor(s)** | ☐ N/A ☒ YES, fill in details below |
| Internal organisation(s)/entity(ies)<br>Names and contact details | ☒ N/A ☐ YES |
| External organisation(s)/entity(ies)<br>Names and contact details | ☐ N/A ☒ YES<br>**Microsoft Ireland Operations Limited**<br>One Microsoft Place South County Business Park<br>Leopardstown<br>Dublin 18 D18 P521<br>Ireland<br><br>**Avanade**<br>Guildensporenpark 76, Block H, 9820, Merelbeke, Belgium<br><br>**Accenture**<br>Amsterdam<br>Gustav Mahlerplein 90, Amsterdam, Netherlands, 1082 MA<br><br>*Such processors are bound by contracts defining the terms of service, including personal data protection clauses indicating their responsibilities as provided by Regulation (EU) 2018/1725.* |
| **Data Protection Officer**<br>Name and contact details | Laura NUNEZ BAREZ<br>European Labour Authority<br>Landererova 12,<br>811 09 Bratislava I<br>Slovakia<br>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) processes personal data through the Stakeholder Relationship Management system (SRM), built on Microsoft Dynamics 365, in order to support its mandate of facilitating cooperation, transparency, and efficient interaction with stakeholders.

The primary purposes of the processing are to manage and maintain stakeholder relationships, ensure structured and transparent communication with citizens and Member States, and support the effective handling of requests, complaints, and operational activities. The system enables ELA to provide improved services to citizens, reduce errors in interactions, and ensure timely and coordinated responses in line with applicable procedures and legal obligations.

In addition, the processing supports business continuity, accountability, and the coordination of stakeholder engagement activities across the organisation. The SRM system also enables data-driven decision-making by providing insights through analytics and dashboards.

Furthermore, the platform serves as the operational backbone for additional applications, including the handling of access to documents, external complaints, Member States' requests for information (NLO cases), expert management, and translation requests. These processes contribute to the consistent and effective implementation of ELA's tasks under Union law.

### 1.2.2 Description

The Stakeholder Relationship Management system (SRM), based on Microsoft Dynamics 365, is a centralized platform used by ELA to store, manage, and process stakeholder data and interactions in a structured and consistent manner. The system standardizes data management, reduces data redundancy, and facilitates the secure exchange of information across the organisation.

The SRM system supports core functionalities such as relationship management, storage of stakeholder data, workflow automation, and reporting through analytics and dashboards. It acts both as an independent system and as a foundational platform for the development of additional applications and modules.

These include:

- External complaints and access to documents processes, where citizen requests are received, tracked, and handled in accordance with defined procedures and timelines.
- Member States' requests for information (NLO Case Management), supporting cooperation and exchange of information between ELA and national authorities.
- Database of experts, enabling external experts to manage their profiles and allowing ELA staff to identify expertise based on specific needs.
- Translation requests system, supporting the registration, validation, and management of translation requests from internal and external stakeholders.

Access to the SRM system is restricted to authorised users based on their business roles and responsibilities and follows the principle of least privilege. Appropriate technical and organisational measures are implemented to protect personal data against unauthorised access, disclosure, alteration or loss. The system also supports the application of key data protection principles, including data minimisation, retention management and accountability, in accordance with applicable data protection and information security requirements.

The following applications have been developed using the SRM system as a foundational platform (Horizon 1):

- **External complaints and Access to documents**
  The ELA Compliance team coordinates responses to complaints received from citizens. This involves a coordinated and consolidated action with the relevant sectors, ensuring that responses are provided within the defined timelines. Requests for public access to documents and complaints must be handled within specific timeframes. The handling of these inquiries is currently managed through standard operating procedures and an Excel tracking tool. To automate the process, a Power Automate flow has been developed, enabling members of the public to submit requests via a form on the ELA website, receive an automatic acknowledgement of receipt by email, and have their requests recorded in a SharePoint list for further processing.
  These processes are covered by:
  Record '**DPR-ELA-2022-0002 Handling request for access to documents lodged under Decision No 8/2020 of 24 April 2020 of the Management Board laying down the rules for applying Regulation (EC) 1049/2001 with regard to European Labour Authority documents**'
  Record '**DPR-ELA-2022-0006 External complaints in the field of European labour mobility**'.

- **Member States's request for information system (NLO cases)**

  ELA facilitates cooperation and the cross-border exchange of information between Member State authorities, in order to support the consistent, efficient, and effective application and enforcement of relevant Union law.

  In this context, ELA supports National Liaison Officers (NLOs) in identifying relevant national contact points, coordinating and following up on requests for the exchange of information and administrative data, and facilitating cooperation in individual cases related to cross-border labour mobility, including cases involving potential cross-border fraud.

  This process is currently covered by Record **"DPR-ELA-2022-0015 National Liaison Officers (NLOs) activities on cooperation and exchange of information with Member States".**

- **Database of experts**
  The solution enables external experts to upload, update, and manage their CV information through a secure online portal. It also allows ELA staff to search for and identify suitable experts based on their experience, skills, and areas of expertise, for example in the context of organising events or identifying speakers for specific activities.
  Access to the system is restricted to authenticated users, and experts are required to log in to access and manage their profiles.
  A specific record covers this specific process, in particular, Record "**DPR-ELA-2023-0008 ELA independent expert management".**

- **Translation requests system**
  The Information Sector is responsible for handling translation requests. Such requests may originate either from Member States or from internal ELA services.
  In all cases, translation requests are registered in a centralised registry, where their eligibility is verified, relevant pre-processing information (ex-ante data) is recorded, and the necessary approvals are documented.
  This process is covered by Record "**DPR-ELA-2025-0007 Management of ELA Translation Facility for Information activities and ELA Translation application".**

Therefore, **Stakeholders Relationship Management System (**SRM) serves as the foundational platform for other systems while also operating independently, and refers, in general terms, to the following categories of personal data:

| Data Category | Type of data |
|---|---|
| **Case or Issue Tracking** | - Nature of the case or issue - Status of the case (e.g., open, closed, pending) - Resolution or ongoing actions |
| **Identification Data** | - Full name of stakeholders - Position/role within the organization - Affiliation (e.g., department, organization) |
| **Contact Information** | - Email address - Phone number (work/personal) - Physical address (office or mailing address) |
| **Relationship Data** | - Key interests or areas of collaboration with ELA - History of interactions (e.g., meetings, Teams calls) - Collaboration context (e.g., past/current projects, joint initiatives) |
| **Demographic Information** | - Nationality or country of residence (if relevant) - Professional background (e.g., expertise areas, previous roles) |
| **Access and Permissions** | - User roles and permissions in SRM system (data and feature access) |

#### 1.2.3 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
- Encryption
- User access control
- Security Groups (permissions)
- Collecting minimum set of personal data

#### 1.2.4 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
      Manual input of data
3. ☒ Any other mode, specify
   Email Integration
   Aggregation of non-personal and anonymised data for analytics and reporting

**Description**

The system is designed to gather data through two main methods: manual submission and automated integration with other software tools (e.g., Outlook).

- Manually submitted data refers to information input directly by users, such as contact details, meeting notes, or stakeholder interactions.

- Automated integration allows the system to collect data seamlessly from other applications, like synchronising emails and meeting schedules from Outlook, to enhance data accuracy and streamline processes.

Once the data is collected, it is processed and organized within the system to generate reports and dashboards. These reports provide analyses, including trends, metrics, and insights relevant to stakeholder engagements and operational activities. Dashboards offer a visual representation of the data, providing users with at-a-glance summaries of key performance indicators, stakeholder relationships, and progress metrics. This functionality supports decision-making, strategic planning, and efficient monitoring of activities, ensuring that users have a clear, up-to-date overview of their operations.

### 1.2.5 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:**

The Stakeholder Relationship Management (SRM) system is based on Microsoft Dynamics 365 and uses associated Microsoft cloud services to support stakeholder relationship management, operational workflows, case handling and document management activities.

Personal data are stored electronically in structured databases and document repositories.

### 1.2.6 Comments on the processing of the data

The SRM processes data in structured phases designed to protect, manage, and operationalize personal data through a series of well-defined stages and controls to ensure compliance with data protection regulations, especially since it serves multiple functions across ELA. Here's a breakdown of how data flows through each phase:

– Data Ingestion: Users manually/automatically input data

– Data Validation: Ensures mandatory fields are completed and formats match expectations (e.g., email addresses).

– Case Assignment and Tracking: Cases are routed to the appropriate operational team for follow-up, with tracking capabilities for updates, escalations, or case closures.

<u>The Coordination and Liaison (NLO and Brussels Office) Sector:</u>

Responsible for overall coordination, ensuring alignment with ELA's strategic goals, and decision-making processes.

- Establishing Governance Policies: Develop policies that govern the usage, security, compliance, and overall management of the platform.
- Ensuring Compliance: Work with the ELA Data Protection Officer (ELA DPO) to ensure the platform adheres to data protection regulations (EUDPR, GDPR).
- Monitoring Platform Usage: Monitor how the platform is being used, identifying patterns, inefficiencies, or underutilized features.
- Improvement and Optimization: Continuously assess the platform for potential improvements, whether in performance, user experience, or new features.
- Maintain Master Data Tables: Ensure the accuracy and consistency of master data tables, making updates and changes in alignment with business needs and operational requirements.

The ICT and Digitalisation Support Sector:

- Manages the technical infrastructure, security, and integration with other systems.
- Manage user access and permissions, ensuring appropriate levels of access for different users.
- Coordinate with technical teams for system updates, maintenance, and troubleshooting.
- Oversee the overall operation and performance of the platform.

Coordination and Liaison (NLO and Brussels Office) Sector, Information Sector, Cooperation and Capacity Building Sectors and Compliance team:

- Execute stakeholder engagement strategies within their respective module.
- Record and report stakeholder interactions in the designated system (e.g., NLO cases).
- Collaborate with the Coordination and Liaison Team to address issues that they cannot solve.

Access Control and Security Measures:

Access to personal data is restricted to authorised users who require access for the performance of their duties and is granted on a need-to-know basis. Access rights are assigned according to business roles and responsibilities and are reviewed periodically.

Appropriate technical and organisational measures are implemented to ensure the confidentiality, integrity and availability of personal data. These measures include access management controls, secure authentication mechanisms, monitoring of system activities and other safeguards designed to prevent unauthorised access, disclosure, alteration or loss of information.

Activities performed within the system may be logged for security, operational and accountability purposes in accordance with applicable policies and legal requirements.

| Category | Boundaries | Developed Systems on Dynamics 365 |
|---|---|---|
| **Online survey and feedback tool** | Utilised as an alternative to EU Survey, as the data collected will be stored in Dataverse. This eliminates the requirement for integration with EU Survey and facilitates easier data transfer. | Dynamics 365 Dataverse |
| **Data Minimisation** | - Data collection is limited to what is limited to what is necessary and proportionate to the purposes of processing.<br>- Retention policies ensure data is not stored longer than required. | -Each system collects only the necessary personal data for its operation (e.g., Complaint details for public inquiries, Contact data for stakeholders, Skills and knowledge profiles for the expert database). |
| **Express Consent** | - Users must provide explicit consent before their personal data is used in specific applications. | - For **External Complaints**, members of the public must provide explicit consent before their personal data is processed for complaint handling.<br>- For **NLO Cases**, National Liaison Officers must provide explicit consent before their personal data is processed as part of information exchange and cooperation activities.<br>- For the **Database of Experts**, experts must give explicit consent before their CV data is stored, accessed, or used by ELA staff. |

## 1.3 DATA SUBJECTS AND DATA CATEGORIES

### 1.3.1 Data subjects' categories

| | |
|---|---|
| 1. Internal to organisation | **ELA Staff:** Staff members (TA, CA, SNE, NLO, and trainees) who may use the SRM for managing their tasks, accessing personal information, and participating in internal processes. |
| 2. External to organisation | **Stakeholders:** Individuals or organizations that interact with ELA, including partners, agencies, consultants, or social partners.<br><br>The categories of stakeholders vary depending on the specific processing activity within the SRM system. |

### 1.3.2 Data categories/fields

**The categories of personal data processed vary depending on the specific processing operations performed within the SRM system:**

**Data categories:**

- **Identification data:** name, user ID, organisational affiliation
- **Access and permissions data:** User roles and permissions within the SRM system (data and feature access).
- **Activity data (captured via system logs):** Records of user interactions within the system (access to records, updates, case handling actions)
- **Relationship data:** History of interactions (meetings, Teams calls), Collaboration context (past and ongoing projects, joint initiatives), Position/role within the organisation, Affiliation (department, organisation), Synergies between different stakeholder records, Key interests or areas of collaboration with ELA
- **User experience data:** Feedback collected through surveys. Where applicable, a dedicated Privacy Statement is provided for specific survey activities.

**Technical management of the platform (ICT Sector):**

- **Technical data:** IP address, connection data, device and system information (e.g. browser type, operating system)
- **Log data:** System logs, access logs, security logs, and audit trails
- **Backup data:** Copies of system data stored for business continuity and disaster recovery purposes

**Additional related processing:**

- ICT support requests are covered by Record "**DPR-ELA-2022-0042: ELA ICT Ticket system**"
- Security incidents are covered by Record **"DPR-ELA-2023-0022 ELA ICT security investigations**"

**Specific Databases:**

**I) External complaints:**

*This database is not linked to other specific databases, and therefore only accessible for the case handler, Head of Compliance Sector and designated ELA staff assisting on each particular case.*

**Data categories:**

-Identification data of the case handler and of the complainant

-Content of the query/complaint submitted to ELA Compliance Team received by e-mail:

Name and Surname, Address, ID number, copy of ID or passport, Social security number, Nationality-Dates: date of initial request, acknowledge of receipt, deadline and date of closure.

-Case or inquiry related data: nature of the case, status of the case, workflow, and resolution or ongoing actions.

-Complaint/request concerning a specific situation that can possibly include: social security entitlements such as insurance periods, employers, medical data or family status.

-In some cases, we may receive special categories of data: health data or trade union membership.

**II) Access to documents**
*This database is not linked to other specific databases, and therefore only accessible for the case handler, Head of Compliance Sector and* designated ELA *staff assisting on each particular case.*

**Data categories:**
-Identification data of the legal officer handling the case and the requester.
-Personal data, which the applicant provided in his/her application, submitted in another electronic or paper format
-Personal data contained in the documents requested.
-Contact information: Email address, mailing address.
-Case related data: nature of the case, status of the case and resolution or ongoing actions.
-Dates: date of initial request, acknowledge of receipt, deadline and date of closure.
-ELA staff on a need-to-know basis will be requested to provide information related to each particular request. Personal data in the documents subject of the request will be removed before sending a final reply.

For further details on the categories of personal data processed and the handling procedures, please refer to the relevant record '**DPR-ELA-2022-0002 Handling requests for access to documents lodged under Decision No 8/2020 of 24 April 2020 of the Management Board, laying down the rules for applying Regulation (EC) No 1049/2001 with regard to European Labour Authority documents**'.

**III) NLO cases** (Member States' requests for information)
*This processing activity is linked to other EU information system, in particular the Internal Market Information System (IMI), and the Electronic Exchange System on Social Security (EESSI) owned by ELA.*
*These systems are used to facilitate the secure exchange of information between Member States. ELA does not have direct access to all underlying data within these systems and, where applicable, only limited or pseudonymised data (e.g. reference numbers) are processed.*

**Data categories:**
Identification the relevant contact points:
Name, surname, organization, Member State, email, telephone and job position.
Follow up request for cooperation and accelerating information exchanges between national authorities (NLO requests):
Date case received, requesting Member State, requested Member State, national institutions, type of request (e.g. exchange of information, follow up, cases status, contact point), subject of request (abstract of the case), area of cooperation, case status (e.g. date of initial request, acknowledge of receipt, deadline, case closed positive (data and result), in progress etc.), date case closed, result, response time. In some specific cases, individual cases referred by national authorities to ELA/NLOs may contain personal data which can also be of a sensitive nature. This is necessary for ELA's NLOs to follow up the particular case with the NLO of another Member State with a view to sort out the cooperation dispute or to speed up the exchange of information on the individual's particular case. In these cases, a reference to the IMI reference number, trade union membership data, social security affiliation/number, private companies TVA number, registration and/or fiscal data could be exchanged. This should be considered pseudonymized data, as neither ELA nor the NLOs has access to this system.
Provide information to support Member States in the effective application of the Union Law:
Name, surname, organization, Member State represented, email, telephone, job position, request/enquiry.

**IV) Database of experts**
*This database is not directly linked to other specific databases or systems. Access is restricted to authorised ELA staff of Cooperation Support Unit on a need-to-know basis for the management of expert profiles and related activities.*

Data categories (registration and profile management):

- Identification data
- Contact details (email address, mobile number)
- Education
- Areas of expertise (e.g. social security, posting, free movement, mediation, cross-border inspections, road transport, etc.)
- Motivation

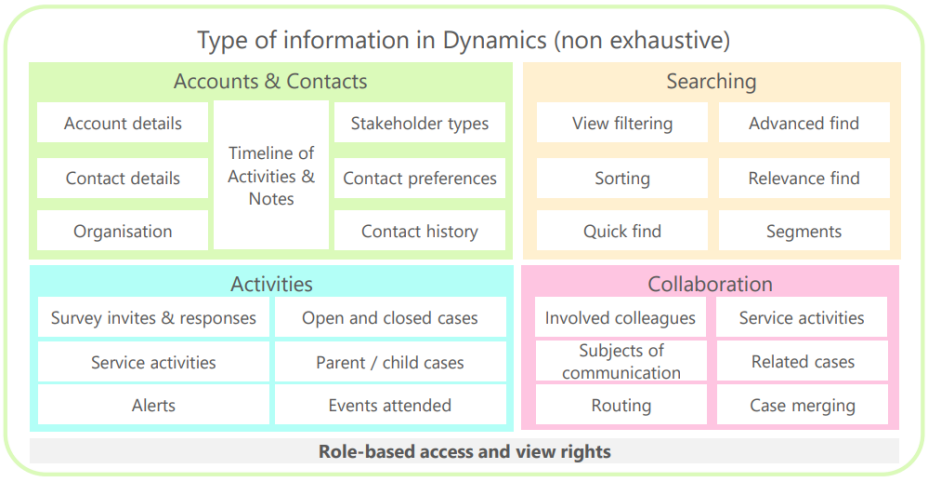
- Languages
- Employment history / work experience
- Publications
- Additional information provided in free-text fields

If selected, the processing of personal data is further expanded in accordance with the relevant record '**DPR-ELA-2023-0008 ELA independent expert management'**, where additional categories of personal data may be collected and processed for the purposes of expert engagement and management.

**V) Translation activities**

*This processing activity is linked to other systems used for the management of translation requests, in particular the ELA Translation App, and the eCdT Client Portal 2.0 managed by the Translation Centre for the Bodies of the European Union (CdT). Personal data may also be processed through SharePoint and Ares for the storage of related lists, records, and clarification exchanges. Access is limited to authorised users on a need-to-know basis.*

Data categories:
First name, last name, administrative phone number (not requested, but may be voluntarily offered), administrative address (not requested, but may be voluntarily offered) and e-mail address of the principal return address, the contact person, the person responsible of a request, the institution they are representing and their role in the institution. There are situations in which the National Translation Coordinator provides contact details, such as name, surname, email of a colleague or a functional mailbox for the translated files delivery in case of their unavailability The same fields are kept for data subjects who play the role of preparator, approver and administrator of a request (ELA staff).




### 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.

**Description:**
SRM handles professional information, so it generally doesn't include special categories. However, ELA's social partners provide ELA with protected characteristics (trade union membership).
The representatives of trade unions, as part of the Stakeholder Group of the ELA are acting in an official capacity (e.g. as a union leader in a public forum and the SRM system handles their personal data within this specific purpose.).

**If applicable, indicate the reasons under article 10(2) allowing the processing of the special categories of data:**

(a) ☐ The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, […].
(b) ☐ Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security[…].
(c) ☐ Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.
(d) ☐ Processing is carried out in the course of its legitimate activities with appropriate safeguards by a non-profit-seeking body which constitutes an entity integrated in a Union institution or body and with a political, philosophical, religious or trade-union aim […].
(e) ☐ Processing relates to personal data which are manifestly made public by the data subject.
(f) ☐ Processing is necessary for the establishment, exercise or defence of legal claims or whenever the Court of Justice of the European Union is acting in its judicial capacity.
(g) ☒ Processing is necessary for reasons of substantial public interest, […]
(h) ☐ Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services […].
(i) ☐ Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices […].
(j) ☐ Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes […].

#### 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 ☒**<br>**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:

| Processing Activity | Data category | Retention period |
|---|---|---|
| External complaints | All data categories received in a particular query | 3 (three) years. After this period, the data will be anonymised and kept for statistical purposes. |
| Access to documents | All personal data belonging to the case file of a request for access to documents | No longer than 5 (five) years after the closure of a case-file. |

| | | |
|---|---|---|
| NLO cases | Contact points' personal data | As long as the as person collaborates with ELA in his/her position based on the relevant appointment or contract |
| | Data related to requests on cooperation/exchange of information | 5 years after the case is closed. |
| | Data related to information regarding EU Law | Personal data will be deleted 1 year later the case was closed. After this year, personal data will be anonymised and data will be kept for statistical/historical purposes. |
| Database of experts | Data related to the registration of the database | Unsuccessful candidates will be kept for a period of 3 months after the end of the screening |
| | Data concerning the selection and management | Successful candidates will be kept until the end of the nomination period (2 years), or longer should such data be necessary for other ongoing purposes (e.g. reimbursement of expenses). |
| Translation Activities | All data categories | 5 years |
| | Identification data | Retained for the duration of the user's active relationship with the system. Once a contract expires, information is retained for 90 days for the purposes of collection or possible renewal. After this period, information is deleted. |
| | Consent Form | Consent is stored and remains valid until it is withdrawn by the data subject. Data subjects may withdraw their consent at any time. Such withdrawal shall take effect immediately upon receipt and will be implemented without undue delay |
| | Activity Data / System Logs | Data are retained for a period of one (1) year from the last recorded user activity, unless further retention is required for security investigations or audit purposes. |
| | User Experience Data (Support/Feedback data) | Up to 180 days upon expiration/termination of the subscription |
| | Diagnostic and service data | Up to 180 days upon expiration/termination of the subscription |

**Description**

Further processing for archiving purposes in the public interest may take place in relation to the specific processing activities within the SRM system.

Personal data selected for retention as part of the historical archives may be kept for long-term or permanent preservation, where this is justified by its historical value and in accordance with applicable legal and organisational requirements.

During the appraisal process, ELA will, by default and where feasible, sanitise or minimise personal data, retaining only the information strictly necessary to preserve the historical integrity and purpose of the records. Where possible, personal data is removed or anonymised prior to the transfer of records to the historical archives. Log files are not archived.

Backups: Backup copies of data are managed under the separate processing record **DPR-ELA-2025-0008 Management of backups of data contained in ELA systems.**

## 1.5 RECIPIENTS

| Origin of the recipients of the data | |
|---|---|
| 1. ☒ Within the EU organization | ELA Staff on a need-to-know basis |
| 2. ☒ Outside the EU organization | Social Partners<br>Member States National Authorities<br>ELA Contact Points in Member States<br>EU Institutions and Bodies<br>Citizens<br>System external provider on a need-to-know basis |

| Categories of the data recipients |
|---|
| 1. ☒ A natural or legal person<br>2. ☒ Public authority<br>3. ☒ Agency<br>4. ☒ Any other third party, specify<br>Microsoft (Cloud Service Provider)<br>Specify who has access to which parts of the data: |

**Description**

**General Activities:**

Personal data may be accessed by the Operations Department, Coordination and Liaison (NLO and Brussels Office) Sector for the purposes of monitoring, maintenance, and continuous improvement of the platform. Such access is limited to what is strictly necessary for governance, reporting, and performance analysis, in accordance with the *need-to-know principle* and data minimisation requirements.

**Manage the platform from a technical point of view - ICT Team (IT Support)**

-Personal data may be accessed by the ICT team strictly for the purpose of providing technical support and managing the platform through the IT ticketing system. Access is granted on a *need-to-know basis* and in line with the data minimisation principle.

-Where necessary, authorised external contractors (Microsoft) may have limited access to personal data to assist users with technical issues. Such access is strictly limited to what is necessary (*need-to-know basis*) and governed by contractual data protection and confidentiality obligations.

-In the event of an ICT or cybersecurity incident, relevant personal data may be shared with CERT-EU (Computer Emergency Response Team for the EU institutions, bodies, offices and agencies) for the purposes of detection, analysis, and incident response.

**Specific databases:**

**External complaints:**
**-Within the EU organisation:** ELA Compliance team
**-Outside the EU organisation:** National authorities for further information related to the actual complaint.

**Access to documents**
**-Within the EU organisation:** ELA Staff dealing with access to documents requests (need-to-know basis).
**-Outside the EU organisation:** Personal data submitted by the applicants are not disclosed outside the European Labour Authority, except to the extent necessary for dispatching a letter by registered mail or if required by law.

**NLO cases**
**-Within the EU organisation:** Cooperation and NLO's Office Team
**-Outside the EU organisation:** IMI Coordinators/ELA Contact Points in Member States IMI users

**Database of experts**
**-Within the EU organisation:** ELA Capacity Building Sector, ELA Finance team on a need-to-know basis, Head of Unit(s) and Head of Sector(s) of the different Units in ELA

**Translation activities**
**-Within the EU organisation:** ELA staff that requested the translation, ELA staff with super user role in the Translation Centre app have access to download all translated documents and to all users contact data (ELA staff and external users of ELA services)
**-Outside the EU organisation:**
Translation Centre for the Bodies of the European Union (CdT)
ELA may disclose the contact details of the National Translation Coordinator to the national authorities interested in the translation support

### 1.6 INTERNATIONAL DATA TRANSFERS

| **Transfer to third countries or international organisations of personal data** |
|---|
| **1. Transfer outside of the EU or EEA**<br>☒ N/A, transfers do not occur and are not planned to occur<br>☐ YES, |
| **2. Transfer to international organisation(s)**<br>☒ N/A, transfers do not occur and are not planned to occur<br>☐ Yes, specify further details about the transfer below |
| **3. Derogations for specific situations** (Article 50.1 (a) –(g))<br>☒ N /A<br>☐ Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply (ies). |

**Description**
Personal data processed within the SRM system and its associated applications is not transferred to any third country or international organisation.

## 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 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 Protection)
- External website ☒(URL: https://www.ela.europa.eu/en/privacy-policy

☒ 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.
Specific guidance for citizens available on ELA website: Your data protection rights at ELA.

## 1.8 SECURITY MEASURES

All data in electronic format (e-mails, documents, uploaded batches of data etc.) are stored either on the servers of the European Labour Authority or of its contractors.

The European Labour Authority's contractors are bound by a specific contractual clause for any processing operations of personal data on behalf of the European Labour Authority, and by the confidentiality obligations deriving from the General Data Protection Regulation.

In order to protect personal data, the European Labour Authority has put in place a number of technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation