

PROTECTION OF YOUR PERSONAL DATA

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

Processing operation: Stakeholder Relationship Management (SRM) System

Data Controller: European Labour Authority, Operations Department, Coordination and Liaison (NLO and Brussels Office) Sector

Record reference: DPR-ELA-2024-0007

Table of Contents

1. Introduction
2. Why and how do we process your personal data?
3. On what legal ground(s) do we process your personal data?
4. Which personal data do we collect and further process?
5. How long do we keep your personal data?
6. How do we protect and safeguard your personal data?
7. Who has access to your personal data and to whom is it disclosed?
8. What are your rights and how can you exercise them?
9. Contact information
10. Where to find more detailed information?

1. Introduction

The European Labour Authority (hereafter 'ELA') is committed to protect your personal data and to respect your privacy. ELA 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. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to processing operation "**Stakeholder Relationship Management (SRM) system**", undertaken by the European Labour Authority, Operations Department, Coordination and Liaison (NLO & Brussels Officer) Sector, is presented below.

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

Purpose of the processing operation: 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.

Therefore, Stakeholders Relations 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	<ul style="list-style-type: none">- Nature of the case or issue- Status of the case (e.g., open, closed, pending)- Resolution or ongoing actions
Identification Data	<ul style="list-style-type: none">- 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)

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.

In particular, 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](#)".

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.

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.

Coordination and Liaison (NLO and Brussels Office) Sector - Coordinator:

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:

- Manage 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 (NLO and Brussels Office) Sector to address issues that they cannot solve.

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

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

We process your personal data, because, according to Article 5(1) of Regulation (EU) 2018/1725:

(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;

ELA's mission, as outlined in Article 1 of its Founding Regulation, includes promoting fair labour mobility within the EU and enhancing the effectiveness of national labour market policies. The processing of personal data is necessary to achieve these objectives, such as when ELA organises events for stakeholder engagement or training initiatives. By managing expert profiles, ELA ensures that it can connect stakeholders with the appropriate expertise needed to address labour mobility challenges effectively.

(b) processing is necessary for compliance with a legal obligation to which the controller is subject;

According to Article 6 of ELA's Founding Regulation, ELA has a legal obligation to promote cooperation between Member States and the Commission in matters related to labour mobility. This involves processing personal data as required to execute its functions under EU law, particularly in enforcing regulations such as Regulation (EU) 2016/589 on the coordination of social security systems. For example, processing personal data is essential for responding to requests for information or assistance regarding social security entitlements across borders.

(c) 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;

ELA processes personal data to fulfill its obligations under contracts with Member States regarding the coordination of labour mobility. For instance, when a Member State requests

assistance in resolving labour-related issues or in the management of inquiries regarding cross-border workers, ELA collects and processes the personal data of involved individuals to effectively facilitate this support.

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

ELA may process personal data when individuals voluntarily provide their information for specific purposes, such as participating in consultations or providing feedback on labour mobility initiatives. For instance, when users fill out forms on ELA's website to express interest in upcoming events or share their experiences, their consent is obtained to process their personal data for those purposes. This aligns with ELA's commitment to transparency and stakeholder engagement.

For further details on the specific legal basis applicable to each individual processing activity carried out through the applications, please refer to the respective privacy notices made available for each processing activity.

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

In order to carry out this processing operation, the following categories of personal data may be processed, depending on the specific processing activity 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. (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).

5. How long do we keep your personal data?

The European Labour Authority only keeps personal data for the time necessary to fulfil the purpose of collection or further processing:

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

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.](#)

6. How do we protect and safeguard your personal data?

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

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

Access to your personal data is provided to ELA staff responsible for carrying out this processing operation and, where necessary, to external recipients, strictly for the purposes of carrying out the relevant processing operations.

Such access is limited to what is necessary in accordance with the *need-to-know principle* and the principle of data minimisation. All recipients are bound by statutory obligations of confidentiality and, where applicable, by additional contractual data protection and confidentiality requirements.

General Activities:

Personal data may be accessed by the 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

Please note that pursuant to Article 3(13) of the Regulation, public authorities (e.g. Court of Auditors, EU Court of Justice) which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients. The further processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. If applicable, a specific clause about investigations, including legal requests from public authorities, should be included.

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.

8. 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, your personal data and to rectify them in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and 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) on grounds relating to your particular situation.

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. Their contact information is given under Heading 9 below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e. their Record reference(s) as specified under Heading 10 below) in your request.

9. 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: governance@ela.europa.eu

- **The Data Protection Officer (DPO) of ELA**

You may contact the Data Protection Officer (data-protection@ela.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.

10. Where to find more detailed information?

ELA Data Protection Officer (DPO) publishes the register of all processing operations on personal data by ELA, which have been documented and notified to him. You may access the register via the following link: <https://www.ela.europa.eu/en/privacy-policy>

This specific processing operation has been included in the DPO's public register with the following Record reference: **DPR-ELA-2024-0007 Stakeholder Relationship Management (SRM) system**