



European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2025-0009 Database related to the coordination and support of concerted and joint inspections - Inspections App

1 PART 1: PUBLIC - RECORD (ARTICLE 31¹)**1.1 GENERAL INFORMATION**

Record reference	DPR-ELA-2025-0009
Title of the processing operation	Database related to the coordination and support of concerted and joint inspections - Inspections App
Controller entity	European Labour Authority, Enforcement and Analysis Unit, Concerted and Joint Inspection Sector
Joint controllers	<input checked="" type="checkbox"/> N/A <input type="checkbox"/> YES, fill in details below
Processor(s)	<input type="checkbox"/> N/A <input checked="" type="checkbox"/> YES, fill in details below
Internal organisation(s)/entity(ies) Names and contact details	<input checked="" type="checkbox"/> N/A <input type="checkbox"/> YES
External organisation(s)/entity(ies) Names and contact details	<input type="checkbox"/> N/A <input checked="" type="checkbox"/> YES Microsoft Ireland South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland. Insight Technology Solutions Belgium Inc., Romeinsesteenweg 468, 1853 Grimbergen, Belgium. Avanade, Guildensporenpark 76, Block H, 9820, Merelbeke, Belgium 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 Name and contact details	Daniela QATAM BENETIN European Labour Authority Landererova 12, 811 09 Bratislava I Slovakia Email: data-protection@ela.europa.eu
Corporate Record	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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 Description

The Inspections application is a case management system created in order to facilitate the process of planning, carrying out and reporting on concerted and joint inspections.

The Inspections application will contain:

(a) A database of individuals that work at national institutions and coordinate ELA supported concerted and joint inspections; the database will only be used to assign individuals from this database to particular inspection cases, in which their institutions are involved.

(b) Agenda of the concerted and joint inspection, which contains a list of main organisers and their contacts, describes the program of the event and ELA financial and other support provided.

(c) Participants list of concerted and joint inspections the purpose of which is to confirm the presence of those inspectors and other participants to whom ELA financial and other support were provided.

Role-Based Access Control (RBAC) is a security mechanism that ensures users are granted access only to the data and functionalities necessary for their specific roles, adhering to the principle of least privilege. To maintain its effectiveness, roles and permissions are periodically reviewed. This approach not only ensures the segregation of duties but also minimizes the risks of unauthorized access.

Role-specific access is applied as follows:

- Role definition

Roles correspond to functional responsibilities (e.g., ELA staff, National Coordinators, National Liaison Officers, ELA case handlers involved in coordination).

Each role has a specific set of permissions.

- Granular access

Role, Permissions

ELA Staff: Full access (view, upload, edit, manage)

National Liaison Officers (NLOs): Full access (view, upload, edit)

ELA case handlers: Full access (view, upload, edit, manage)

Purpose

The initiative forms part of ELA's operational mandate to support fair labour mobility and the enforcement of Union labour law. Its purpose is to enable the effective planning, execution, coordination and reporting of concerted and joint inspections, thereby strengthening cooperation among Member States and improving the implementation of labour mobility rules across the Union.

The objective of the European Labour Authority (ELA), as established in Article 2 of Regulation (EU) 2019/1149, is to contribute to ensuring fair labour mobility across the Union and to facilitate cooperation between Member States in the enforcement of relevant Union law, including in the context of concerted and joint inspections. In line with Recital (18), which highlights the Authority's responsibility to support national authorities through strategic, logistical and technical assistance for such inspections, the Inspections application functions as a digital tool to enable their organisation, coordination and follow-up.

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
- Encryption

- Role-Based Access Control (RBAC): Access is granted solely to staff of the Concerted and Joint Inspections Sector, staff performing operational analysis in the Analysis and Risk Assessment Sector, and National Liaison Officers.
- Logging and Access Monitoring

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
Click here to enter text.
2. Manual processing
 - a. Word documents
 - b. Excel sheet
 - c. Any other, specify
Manual input of data
3. Any other mode, specify

Description

National coordinators name and contact information is gathered through case descriptions submitted by national authorities.

This information is necessary to facilitate effective communication and coordination among all stakeholders involved in the planning and execution of supported, concerted, and joint inspections.

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

1.2.5 Comments on the processing of the data

The technical solution consists of an integrated online platform designed to support ELA’s process of planning, carrying out and reporting on concerted and joint inspections. Only minimal personal data is processed, strictly for authentication, access control, and user management purposes.

1.3 DATA SUBJECTS AND DATA CATEGORIES

1.3.1 Data subjects' categories

1. Internal to organisation	<input type="checkbox"/> N/A	
	<input checked="" type="checkbox"/> Yes	<u>Data subjects</u> -ELA Staff authorised to manage the inspections application

Data category	Retention period
All data categories	5 years

Description

According to the ELA filing plan and specific retention list: ELA.4.2 > Enforcement and analysis > Files related to inspections, carried out in accordance with Articles 8-9 of Regulation 2019/1149 will be kept for a maximum of 5 years. After that period of time, the personal data will be anonymized and kept for statistical purposes.

1.5 RECIPIENTS

Origin of the recipients of the data

- 1. Within the EU organization
 - Recipients
 - Staff members of the Concerted and Joint Inspections Sector and the Analysis and Risk Assessment Sector.
 - National Liaison Officers (NLOs)

Categories of the data recipients	
1.	<input checked="" type="checkbox"/> A natural or legal person
2.	<input type="checkbox"/> Public authority
3.	<input checked="" type="checkbox"/> Agency
4.	<input type="checkbox"/> Any other third party, specify
Specify who has access to which parts of the data:	

Description

Access to the database is restricted to authorised staff members from the Concerted and Joint Inspection Sector, who manage and coordinate supported, concerted, and joint inspections. The Analysis and Risk assessment Sector will have access only to aggregated data, specifically the final analytical report, not the raw database.

NLOs will have access, view and edit rights, but only for data related to the Member State they represent (not all Member States).

IT administrators may access the system solely for maintenance and security purposes.

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 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.

The information collected by ELA 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.

1.6 INTERNATIONAL DATA TRANSFERS

Transfer to third countries or international organisations of personal data	
1. Transfer outside of the EU or EEA	
<input checked="" type="checkbox"/> N/A, transfers do not occur and are not planned to occur	
<input type="checkbox"/> YES,	
Country(ies) to which the data is transferred	<i>Click here to enter text.</i>
2. Transfer to international organisation(s)	
<input checked="" type="checkbox"/> N/A, transfers do not occur and are not planned to occur	
<input type="checkbox"/> Yes, specify further details about the transfer below	
Names of the international organisations to which the data is transferred	<i>Click here to enter text.</i>
3. Derogations for specific situations (Article 50.1 (a) –(g))	
<input checked="" type="checkbox"/> N /A	
<input type="checkbox"/> Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply (ies).	

1.7 INFORMATION TO DATA SUBJECTS ON THEIR RIGHTS

Rights of the data subjects
<i>Article 17 – Right of access by the data subject</i>
<i>Article 18 – Right to rectification</i>
<i>Article 19 – Right to erasure (right to be forgotten)</i>
<i>Article 20 – Right to restriction of processing</i>
<i>Article 21 – Notification obligation regarding rectification or erasure of personal data or restriction of processing</i>
<i>Article 22 – Right to data portability</i>
<i>Article 23 – Right to object</i>
<i>Article 24 – Rights related to Automated individual decision-making, including profiling</i>

1.7.1 Privacy statement

The data subjects are informed about their rights and how to exercise them in the form of the 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>)

Other form of publication, specify

A specific Privacy Statement will be published on the ELA main website.

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:

Guide on data subject's rights is available on ELA main website

1.8 SECURITY MEASURES

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

Description

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.