**European Labour Authority**

DATA PROTECTION OFFICER

**RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA**

**DPR-ELA-2026-0006 Staff Claims App**

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

## 1.1 GENERAL INFORMATION

| | |
|---|---|
| **Record reference** | DPR-ELA-2026-0006 |
| **Title of the processing operation** | Staff Claims App |
| **Controller entity** | European Labour Authority, Resources Unit, Finance, Budget & Procurement Sector (Finance Team) |
| **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<br>Microsoft Ireland South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.<br><br>Insight Technology Solutions Belgium Inc., Romeinsesteenweg 468, 1853 Grimbergen, Belgium.<br><br>Avanade, Guildensporenpark 76, Block H, 9820, Merelbeke, Belgium<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** Name and contact details | Daniela QATAM BENETIN<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 Description

The Staff Claims Application is an internal business application developed on Microsoft Dynamics and used within the European Labour Authority (ELA) to support the administration of staff claims.

The tool enables authorised ELA staff to update/upload relevant personal and employment information, submit claims, upload supporting documentats, and where required, complete mandatory declarations.

The application centralises the handling of these requests and provides a structured workflow through which Finance Sector can verify eligibility, review supporting documents, validate the completeness of submissions, and approve or reject claims in accordance with the applicable financial, administrative, and audit rules.

Access to the Staff Claims App is strictly role-based and enforced through ELA Entra ID Security Groups, ensuring that users can only access data necessary for the performance of their duties.

Within the application, staff initiate claims or update their profile by entering the required personal, employment, or family-related information. The system then routes these submissions through predefined steps, allowing designated HR to confirm healthcare enrollment and Finance staff to verify eligibility of costs, review supporting documentation, apply financial ceilings or pro-rata calculations, and finalise reimbursement decisions. Throughout the lifecycle of each claim, the application maintains a record of status changes and logs all actions performed by authorised users, ensuring full traceability and accountability. The system operates in a secure environment with role-based access controls, audit trails, and controlled data input mechanisms to support accurate processing and internal control.

### 1.2.2 Purpose

The Staff Claims Application is designed to ensure the efficient, transparent, and compliant administration of staff claims. Its purpose is to provide a central, reliable platform through which staff can manage and have an overview of their claims, while HR can upload some personal data and carry out enrollment in healthcare. The Finance Sector can carry out the necessary verification, and reimbursement tasks in line with applicable ELA rules..

The Application processes personal data to:

- Manage staff claims based on applicable ELA decisions
- Enable staff to submit and track claims
- Verify claims and supporting documents
- Apply financial ceilings, pro rata rules and administrative checks
- Manage declarations and healthcare enrolment
- Ensure accurate processing, auditability and internal control.

### 1.2.3 Processing for further purposes

☒ Archiving in the public interest
☐ Scientific or historical research purposes
☒Statistical purposes
☐ N/A

Safeguards in place to ensure data minimisation
☒ Pseudonymisation
☒ Any other, specify
Anonymization
Encryption
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
        PDF documents, Email communication, Other Microsoft Applications.

#### 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

*Microsoft Dataverse is a cloud-based relational database platform that powers data storage and management across the Microsoft Power Platform and Dynamics 365.*

#### 1.2.6 Comments on the processing of the data

Users enter the place of residency and claim- related financial information and submit supporting documentation through the application. User profile and master data are maintained within the application by authorised staff within HR Sector.

Infrastructure:
Implemented as a controlled and access-restricted module within Dynamics, but with restricted access layers.
Safeguards:
Strict role-based access control (RBAC), Encryption at rest and in transit, Periodic access reviews and full audit logging, Mandatory multi-factor authentication (MFA), Continuous logging, monitoring, and auditing of administrative activities, Access limited to ELA staff within ELA-controlled environments (no external devices or systems permitted).

Overall data processing approach:
The application follows a minimal-data, high-security processing model, ensuring that only essential personal data is collected and processed. Strong security controls, including encryption, RBAC, MFA, and structured logging are consistently applied across the application.

### 1.3 DATA SUBJECTS AND DATA CATEGORIES

#### 1.3.1 Data subjects' categories

| | |
|---|---|
| 1. Internal to organisation | ☒Yes<br><br>Data subjects<br><br>*Temporary Agents (TAs)*<br><br>*Contract Agents (CAs)*<br><br>*Trainees*<br><br>*Seconded National Experts (SNEs)*<br><br>*Authorised ELA staff involved in the administration of the application (ELA Staff of the Finance, Budget & Procurement Sector and HR Sector)* |
| 2. External to organisation | ☒ N/A |

**1.3.2 Data categories/fields**

Indicate the categories of data that will be processed
Description:
**Identification and contact data:** Full name, ELA email address, Staff category (TA/CA/Trainee/SNE).

**Employment related data:** Contract start date, Contract end date, place of employment, place of residence (for eligibility in some measures).

**Household / Family data:** Yes/No spouse or registered partner, number of dependent children, residence status of spouse/partner (declared in the app).

**Claim related data:** Subject of claim, expense date, claim amount, prorata ceiling (based on employment dates), eligible amount, status (submitted, under review, ready for payment, rejected, rejected for correction, under payment, paid), confirmation form HR, notes or comments from Finance (if applicable).

**Financial Supporting Documentation:** Invoice, tickets, receipts, bank statements submitted as proof of payment, declarations on Honour.

Financial reference identifiers associated with claims (e.g. LEF and BAF codes), displayed for reference purposes only and not used to create, modify, or execute payments.

**Healthcare enrollment data (administrative only):** Enrollment status (enrolled, unenrolled), enrollment/unenrollment date.

**Access and activity data:** Membership in Entra ID Security Groups for Staff Claims App, login timestamps, user action logs (submissions, declarations), role assignment (staff, HR, Finance).

**Data relating to authorised users of the application:** Identification and professional contact data of authorised ELA staff members accessing or managing the application (e.g. name, professional email address, user identifier), as well as role and access related information and system generated logs recording user actions for security, audit, and accountability 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** ☒<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:

| **Data category** | **Retention period** |
|---|---|
| All data categories | Files relating to financial transactions are to be retained in the archives for a period of 5 years following the discharge of the financial exercise.<br><br>The discharge of the financial exercise generally takes place 2 years after the financial year (personal data is thus retained as a rule for a total of 7 years);<br><br>→ Until the end of a possible audit if it started before the end of the above-mentioned period. |
| IT system and user access data | 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. |

Personal data processed in the Staff Claims application are retained in accordance with the ELA filing plan and applicable Union financial and accounting rules.

### 1.5 RECIPIENTS

| **Origin of the recipients of the data** | |
|---|---|
| 1. ☒ Within the EU organization | Recipients<br><br>-ELA Staff within the HR Sector on a "need-to-know basis"<br><br>-Authorised staff of ELA Finance, Budget and Procurement Sector on a "need-to-know basis"<br><br>-Authorised staff of ICT Team providing technical or administrative support |
| 2. ☒ Outside the EU organization | Recipients<br><br>Personal data may also be made available to EU oversight bodies upon request (e.g., IDOC, IAS, Court of Auditors, OLAF) in line with their mandates. |
| **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>Specify who has access to which parts of the data:<br><br>Access to personal data processed through the Staff Claims Application is restricted to authorised ELA staff members, in accordance with a role- based access control (RBAC) model and the need- to- know principle. | |

| |
|---|
| Depending on their assigned role and responsibilities, this may include:<br>-authorised staff of the HR Sector, limited to the verification and updating of staff- related administrative data (such as contract details, family- status information, number of dependent children, and administrative healthcare enrolment), strictly within predefined workflows and on a need- to- know basis. HR staff do not assess costs, approve or reject claims, or authorise payments.<br><br>-authorised staff of the Finance Sector responsible for the verification, assessment, and approval of claims.<br><br>-authorised staff providing technical or administrative support to the application, where strictly necessary.<br><br>Access is granted and managed through ELA Entra ID security groups. |

### 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). |

### 1.7 INFORMATION TO DATA SUBJECTS ON THEIR RIGHTS

| **Rights of the data subjects** |
|---|
| *Article 17 – Right of access by the data subject*<br>*Article 18 – Right to rectification*<br>*Article 19 – Right to erasure (right to be forgotten)*<br>*Article 20 – Right to restriction of processing*<br>*Article 21 – Notification obligation regarding rectification or erasure of personal data or restriction of processing*<br>*Article 22 – Right to data portability*<br>*Article 23 – Right to object*<br>*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 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.

**Description:**
Guidance on data subjects' rights available on ELA website.

## 1.8 SECURITY MEASURES

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

**Description:**
All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the European Labour Authority or of its contractors. All processing operations are carried out pursuant to the **Commission Decision (EU, Euratom) 2017/46** of 10 January 2017 on the security of communication and information systems in the European Commission.

ELA's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of ELA, and by the confidentiality obligations deriving directly from the General Data Protection Regulation in the EU Member States ('GDPR' **Regulation (EU) 2016/679).**

In order to protect your personal data, ELA has put in place a number of technical and organisational measures in place. 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.