European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2026-0002– ESSbot (AI powered chatbot on SSC) testing phase

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

1.1 GENERAL INFORMATION

Record reference	DPR-ELA-2026-0002
Title of the processing operation	ESSbot (AI powered chatbot on SSC) testing phase
Controller entity	European Labour Authority, Cooperation Support Unit (ELA COP Unit)
Joint controllers	☒ N/A ☐ YES, fill in details below
Processor(s)	☐ N/A ☒ YES, fill in details below
Internal organisation(s)/entity(ies) Names and contact details	☒ N/A ☐ YES *Click here to enter text.*
External organisation(s)/entity(ies) Names and contact details	☐ N/A ☒ YES ***Microsoft Ireland Operations Limited*** One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521 Ireland **Accenture** Amsterdam Gustav Mahlerplein 90, Amsterdam, Netherlands, 1082 MA
Data Protection Officer Name and contact details	*Daniela Qatam Benetin* Landererova 12, 811 09 Bratislava I Slovakia Email: data-protection@ela.europa.eu
Corporate Record	☐ Yes ☒ No
DPO Notes	*During the testing phase, processing activities were performed with the support of an external contractor acting as processor.* *The processing agreement with the contractor expired on 20/11/2025. Notwithstanding this, the contractor continues to have restricted access to the system for a limited period to support transition, familiarisation with the tool, and closure of testing activities.* *No new processing activities have been initiated since the expiry of the contract, and access is being phased out.*
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 goal in this phase is the creation of an AI tool that integrates **GenAI** and **RAG** technologies to answer user-testers' questions with none or minimal risks on providing wrong information, basing its answers solely on official documents at EU level collected for this purposes into a database ('knowledge base'). These documents do not contain personal information and are of professional character, concerning interpretation and application of EU rules on social security coordination ('SSC').

A Retrieval-Augmented Generation (RAG) solution for Knowledgebase Inquiry Management integrates information retrieval with natural language generation to efficiently address user queries by leveraging a blend of unstructured and structured knowledge sources, to provide accurate, context-aware responses by leveraging both internal documents and advanced AI language models. ESSbot is designed to address queries about the general interpretation and application of EU rules in an anonymised manner, i.e. it is not intended to handle individual cases or process personal claims.

Generative AI (GenAI) integrated with Retrieval Augmented Generation (RAG) knowledge management offers a transformative solution by combining the contextual understanding of AI with precise document-based knowledge retrieval.

For testing purposes and enhancing quality, the pilot phase will include a **feedback mechanism**, that will temporarily store the following information for further processing (SQL DB):

1. Question
2. Answer
3. List of references / resources (with hyperlinks)
4. Parts of the information the answers are based on
5. Email of question creator
6. Time and date
7. Country of the tester's expertise
8. Like / dislike
9. Comment
10. LLM for user interaction
11. System prompt from selected LLM configuration (AI Assistant)

ESSbot consists of two primary components: the **admin console** and the interactive **SharePoint knowledge management** site, each with distinct roles and access controls to ensure secure and efficient operation.

Admin console: The admin console is a secure interface available exclusively to ELA staff and, temporarily, to its contractor. It allows administrators to configure and manage the chatbot's settings, including adjusting the LLM's prompt and temperature settings to influence response generation. Admins also can grant roles to other users, such as testers, and control their access to various parts of the system. This includes managing access to the chatbot itself and overseeing the feedback mechanism, where feedback from testers is gathered to refine the system. The admin console's role-based access control ensures that only authorised internal staff can perform these administrative tasks, maintaining a secure environment for system management.

SharePoint knowledge management: The SharePoint site acts as the knowledge management platform for the pilot phase, with access and editing capabilities depending on the user's role. Testers, based on their permissions, can add new sources for the chatbot's scraper mechanism to download, enhancing the system's knowledge base. Testers can also access and delete content they have been granted permission to, but all their actions, such as content modifications or deletions, require approval by a content approver. This approval process ensures that only validated and relevant data are integrated into the knowledge base. The SharePoint platform fosters collaboration by allowing testers to contribute to the chatbot's knowledge while maintaining control over content integrity and accuracy.

Terms of use

Testers are authenticated via EU Login, the European Commission's central Identity and Access Management service, which provides Single Sign-On (SSO) and multi-factor authentication. The authentication process is handled entirely by the EU Login service, operated by the European Commission (DIGIT), which verifies user identity and manages user credentials and authentication events. The system itself does not process authentication credentials or maintain identity provider logs. Only the user identification data received (e.g. user identifier or email address) and application-level access events are processed locally by ELA for the purposes of access control, security, and audit logging. DPR-ELA-2023-0014 Identity & Access Management Service - EU Login

Once authenticated, access to the ESSbot's functionalities is governed by Role-Based Access Control (RBAC), which restricts available features and permissions according to the user's assigned role.

Express consent	- Testers must provide consent before their personal data are used in specific applications.	All testers, whether internal or external staff, are required to provide consent prior to being granted access to the tool and its functionalities.
Data minimisation	- Personal data collection is limited to what is strictly necessary for operational and testing purposes. - Retention policies ensure data are not stored longer than required. - All data remaining after the retention period will be anonymised.	-The tool collects only the personal data necessary for its operation, e.g., • Comments from feedback. • Email of external experts. • Member State the externals have expertise in. • Audit logs

1.2.2 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
Click here to enter text.

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
   Click here to enter text.

Description

As part of the personal data processing framework, a logging mechanism was implemented to ensure traceability and accountability throughout the user's account lifecycle. When a user account is created, key personal data — such as the user's email address and identifying credentials — are collected and securely stored. These data are automatically integrated into the Audit Logs, which capture login events, access patterns, and administrative interactions involving that account. The logs record personal data such as user identifiers, email addresses, IP addresses, and timestamps, making it possible to monitor system usage and detect anomalous or unauthorised behavior. These records are essential for safeguarding user data and investigating incidents involving personal data breaches. Access to audit logs is strictly limited to authorised personnel through predefined Access Management protocols, ensuring that sensitive information, including email addresses and login metadata, remains protected against unauthorised access or tampering. Logged data are stored securely, subject to retention limits and encryption where appropriate, in line with data protection obligations.

Access to the platform's functionalities shall not be granted immediately upon user registration. Prior to obtaining access, each user must be formally approved by ELA's internal team for integration into the network environment. As a prerequisite, the user account must be registered as an external user within the ELA's designated tenant.

Following approval and account registration, users shall be required to authenticate their identity using Multi-Factor Authentication (MFA) as a mandatory condition for accessing the tool. This measure ensures compliance with ELA's security standards and mitigates the risk of unauthorised access.

Notwithstanding the granting of network access, access to specific functionalities shall remain subject to Role-Based Access Control (RBAC) protocols. These protocols enforce a secondary layer of security by defining and restricting user permissions based on pre-assigned roles, thereby determining which functionalities each user may access.

The main channel for submitting and temporarily storing personal data directly by the testers during the pilot phase, other than the previously mentioned above, is through the integrated feedback mechanism. Test users may engage with this feature via the chatbot's user interface by indicating whether a response was helpful (like/dislike) and by providing written comments. These interactions are temporarily stored on SharePoint for the purpose of improving the tool's performance and any personal data will be deleted or anonymised upon completion of the testing phase.

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

   Email Integration
   Aggregating of non-personal data

Description:

Audit logs are securely stored in centralised or cloud-based systems, encrypted at rest and in transit, access-restricted, and maintained under retention and deletion policies. These logs contain personal data (e.g., user email addresses and login timestamps), making their secure and compliant storage a legal requirement under the EUDPR (European Data Protection Regulation).

Databases created in MySQL

- **System database** - MySQL managed. Feedback is stored centrally in the System database (MySQL managed) to enable unified access via Power BI.
- **Core database** - managed by team, database for whole core structure (except chatbot application), there is only one instance of core database, since Admin tool and Copy functionality is shared across all chatbot applications.
- **AI Chatbot database** (per each instance) - managed by team, this is chatbot specific database, meaning that each new instance of chatbot application will contain its own database. Naming convention is based on the metadata (from UI part of Copy functionality in Admin – each chatbot database will have its unique suffix/prefix). The documents and sources of information utilised by ESSbot do not contain any personal data.

1.2.5 Comments on the processing of the data

The processing of the data serves as a core element of the project's development, playing a crucial role in improving the chatbot's performance. It will be used to refine the retrieval-augmented generation (RAG) framework, improving the tool's ability to accurately fetch relevant information from external sources. Both positive and negative feedback from testers is essential for evaluating and improving the system, facilitating iterative adjustments that influence the LLM-generated responses.

Virtual Network (VNet) Protection

All data are stored within a secure, private network called a Virtual Network (VNet). This network acts like a secure area where only authorised users can access the data.

Role-Based Access Control (RBAC)

Access to data is controlled through specific roles assigned to users. These roles determine what actions users can perform, ensuring that only those with the appropriate permissions can access or manage the data.

VPN Access for Data Management

To manage the data, users must connect to the secure network through a Virtual Private Network (VPN). This connection ensures that the data remain protected while being accessed or managed.

Personal data from testers to be processed:

Identification data – First name and surname of stakeholders.
Contact information, access and credentials - Email address.
Expertise information - Expertise of the tester – related to an EU Member State.
Access and permissions - Tester's roles and permissions in admin console and database (data and feature access).
Logs - Tester's interactions – Exclusively on adding new sources and deletion of sources.
Consent records - Documentation of tester consent for data processing, and communication preferences.
Feedback interaction - Tester's comments on ESSbot's response and context of the conversation.
Audit logs configuration - Access-related events but also logs generated by firewalls and security systems events

In the context of strengthening system oversight and security accountability, ELA undertook a structured configuration of audit logs to ensure comprehensive traceability of activities across both application and network layers. This involved enabling detailed logging mechanisms not only for user access and administrative actions, but also for firewall events and security system outputs, thereby

creating a robust dataset for behaviour tracking, anomaly detection, and incident investigation. Access to these audit logs was tightly controlled through dedicated access management protocols, limiting visibility and modification rights to authorised personnel only, thus preserving the integrity and confidentiality of sensitive information, including security events and firewall-related activity. Furthermore, ELA ensured the systematic logging of administrative actions — such as configuration changes, system-level updates, and security rule modifications — to establish a verifiable trail of accountability. These logs serve as a foundational element for post-incident review and reinforce governance over both user management and infrastructure-level operations.

Accenture:
In the context of the tool's risk assessment, Accenture acts as a data processor under the provisions outlined in Article 14.2 of the agreement (DIGIT/A3/PR/2018/035 – CLOUD II, DPS2 MC11 SOFIA – FWC DI-7980). The Contractor must comply with strict conditions regarding data access, retention, and international transfers, as well as support the Controller in case of data breaches or necessary audits. The processing activities are defined in the contract and are subject to prior approval by the Controller, ensuring alignment with GDPR and Regulation (EU) 2018/1725 requirements.

1.3 DATA SUBJECTS AND DATA CATEGORIES

1.3.1 Data subjects' categories

1. Internal to organisation	☐ N/A	
	☒ Yes	**Data element** / **Location(s)** / **Who has access** Full name / SharePoint / KM Admin Email address / Admin console/ SharePoint / Admin (AC), Power Admin (AC), KM Admin Expertise information / SharePoint (feedback) / KM Admin Roles and permissions / Admin console/SharePoint / Power Admin (AC), KM Admin Interaction logs / SharePoint / KM Admin Consent records / System level / ICT Admin Feedback interaction / SharePoint / KM Admin Access credentials / System level / ICT Admin Audit log configuration / System-level (ICT logs) / ICT Admin
2. External to organisation	☐ N/A	
	☒ Yes	Full name / SharePoint / Content approver Email address / SharePoint / Content approver

Roles and accesses:

ICT administrator – System/Azure resources
Power administrator – Admin console (AC)/SharePoint (SP)
Knowledge management (KM) administrator – SharePoint (SP)

Administrator – Admin console (AC)
Content approver – SharePoint (SP)

1.3.2 Data categories/fields

Indicate the categories of data that will be processed

Description:

Data category	Type of data
Identification data	- First name and surname of stakeholders
Contact Information, access and credentials	- Email address
Expertise information	- Expertise of the tester – related to an EU Member State
Access and permissions	- Tester's roles and permissions in admin console and database (data and feature access)
Logs	- Tester's interactions – Exclusively on adding new sources and deletion of sources
Consent records	Documentation of tester consent for data processing, and communication preferences
Feedback interaction	- Tester's comments – on the ESSbot's response and context of the conversation
Audit logs configuration	Access-related events but also logs generated by firewalls and security systems events

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**

Description:
Click here to enter text.

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 […].

Additional information
Click here to enter text.

1.3.2.2 Data related to 'criminal convictions and offences'

The data being processed contain sensitive data which fall(s) under Article 11 'criminal convictions and offences'	**N/A** ☒ **Yes** ☐
Description: *Click here to enter text.*	

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
Identification data	Until the end of the pilot phase (and not beyond 28/02/2027)
Contact information	Until the end of the pilot phase (and not beyond 28/02/2027)
Expertise information	Until the end of the pilot phase (and not beyond 28/02/2027)
Access and permissions	Until the end of the pilot phase (and not beyond 28/02/2027)
System logs and metadata	Until the end of the pilot phase (and not beyond 28/02/2027)
Feedback interactions	Until the end of the pilot phase (and not beyond 28/02/2027)

Description

All personal data will be stored exclusively for testing purposes during the pilot phase of the project. These data serve as a core element of the project's development, playing a crucial role in improving the chatbot's performance. It will be used to refine the retrieval-augmented generation (RAG) framework, improving the tool's ability to accurately fetch relevant legal information from external sources. Both positive and negative feedback from users is essential for evaluating and improving the system, facilitating iterative adjustments that influence the LLM-generated responses.

The feedback will directly inform the optimisation of the ESSbot by adjusting its ability to understand and process complex social security coordination queries. Feedback is used to refine the retrieval-augmented generation (RAG) framework through prompt updates, retrieval optimisation and configuration adjustments ensuring that the retrieval mechanism effectively matches queries with the most accurate legal sources. This will optimise the system's capacity to provide precise, contextually relevant, and user-satisfactory responses. The continuous integration of feedback will help improve the model's robustness, ensuring that the chatbot can handle increasingly sophisticated queries and deliver more reliable answers.

Anonymisation:

User queries submitted to ESSbot are automatically processed to remove any personal data before storage or further use. An anonymisation step replaces identifiable information (e.g. names, contact details, IDs) with neutral placeholders and generates a generalised version of the query for search purposes. The original input is not stored.

Only anonymised and rewritten queries are retained to support system improvement and monitoring. Where necessary, authorised administrators may review stored records and apply additional corrections or deletions to ensure effective anonymisation.

The same approach applies to user feedback, which is anonymised prior to storage and subject to review.

Data minimisation and storage limitation principles are ensured, as only non-identifiable data are retained for improving the service.

All personal data collected, as mentioned in section 1.3.2, will be safely stored, anonymised or deleted by the end of the pilot phase (and not beyond 28/02/2027).

1.5 RECIPIENTS

Origin of the recipients of the data

1. ☒ Within the EU organisation

1. Internal to organisation	☐ N/A			
	☒ Yes	**Data Element**	**Location(s)**	**Who Has Access**
		Full Name	SharePoint	KM Admin (SP)
		Email Address	Admin Console/ SharePoint	Admin (AC), Power Admin (AC), KM Admin (SP)
		Expertise Information	SharePoint (feedback)	KM Admin (SP)
		Roles & Permissions	Admin Console/SharePoint	Power Admin (AC), KM Admin (SP)
		Interaction Logs	SharePoint	KM Admin (SP)
		Consent Records	System level	ICT Admin
		Feedback Interaction	SharePoint	KM Admin (SP)
		Access Credentials	System level	ICT Admin
		Audit Log Configuration	System-level (ICT logs)	ICT Admin
2. External to organisation	☐ N/A			
	☒ Yes	Full Name	SharePoint	Content Approver (SP)
		Email Address	SharePoint	Content Approver

ELA staff on a need-to-know basis

2. ☒ Outside the EU organisation

External contractors' staff on a need-to-know basis

The contractor will have access to all personal data elements until the end of their contract, except for access credentials, audit logs, and consent records, which will remain under the exclusive control of the organisation's internal ICT administrators.

Categories of the data recipients

1. ☒ A natural or legal person
2. ☒ Public authority
3. ☒ Agency
4. ☒ Any other third party, specify
   Microsoft (Cloud service provider)
   Accenture

Specify who has access to which parts of the data:

Data category	**Type of data**
Identification data	- Full name of stakeholders

Contact information, access and credentials	- Email address
Expertise information	- Expertise of the tester – related to an EU Member State
Access and permissions	- Tester's roles and permissions in admin console and database (data and feature access)
Logs	- Tester's interactions – Exclusively on adding new sources and deletion of sources
Consent records (1)*	Documentation of tester consent for data processing, and communication preferences
Feedback interaction	- Tester's comments –on the ESSbot responses and context of the conversation
Audit logs configuration (1)*	Access-related events but also logs generated by firewalls and security systems events

ELA Resources Unit – ICT sector.
ELA Cooperation support Unit – Information and Services sector.

External contractor (Accenture) - Access until the contract expires.

(1)* Exclusive to internal ELA's ICT sector.

1.6 INTERNATIONAL DATA TRANSFERS

Transfer to third countries or international organisations of personal data	
1. Transfer outside of the EU or EEA ☒ N/A, transfers do not occur and are not planned to occur ☐ YES,	
Country(ies) to which the data is transferred	*Click here to enter text.*
2. Transfer to international organisation(s) ☒ N/A, transfers do not occur and are not planned to occur ☐ Yes, specify further details about the transfer below	
Names of the international organisations to which the data are transferred	
3. Legal base for the data transfer ☐ Transfer on the basis of the European Commission's **adequacy decision** *(Article 47)* ☐ Transfer subject to **appropriate safeguards** *(Article 48.2 and .3),* specify: 2. (a) ☐ A legally binding and enforceable instrument between public authorities or bodies. Standard data protection clauses, adopted by (b) ☐ the Commission, or	

(c) ☐ the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2).

(d) ☐ Binding corporate rules, ☐ Codes of conduct, ☐ Certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.

3. Subject to the authorisation from the European Data Protection Supervisor:

☐ Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.

☐ Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

☐ Transfer based on an i**nternational agreement** *(Article 49),* specify
Click here to enter text.

4. Derogations for specific situations (Article 50.1 (a) –(g))

☒ N /A

☐ Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply (ies).

In the absence of an adequacy decision, or of appropriate safeguards, transfer of personal data to a third country or an international organisation is based on the following condition(s):

(a) ☐ The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards

(b) ☐ The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request

(c) ☐ The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person

(d) ☐ The transfer is necessary for important reasons of public interest

(e) ☐ The transfer is necessary for the establishment, exercise or defence of legal claims

(f) ☐ The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

(g) ☐ The transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case

Description

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: *Click here to enter text.*)
- External website ☐(URL: *Click here to enter text.*)

☐ Other form of publication, specify
Click here to enter text.

☒ 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:
Click here to enter text.

1.8 SECURITY MEASURES

Short summary of overall technical and organisational measures implemented to ensure information security:

All data in electronic format (emails, 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.
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.