



European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2023-0020 ELA Business Continuity Plan activities

1 PART 1: PUBLIC - RECORD (ARTICLE 31¹)

1.1 GENERAL INFORMATION

Record reference	DPR-ELA-2023-0020
Title of the processing operation	ELA Business Continuity Plan activities
Controller entity	European Labour Authority, Governance and Coordination Unit
Joint controllers	<input checked="" type="checkbox"/> N/A <input type="checkbox"/> YES, fill in details below
Names and contact details of respective joint controllers	
Description of the main responsibilities of each of the controllers, and the essence of the Joint controllership arrangements.	
Joint controllership arrangement (Article 28(1))	<input type="checkbox"/> Link: <input type="checkbox"/> Attachment
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 type="checkbox"/> N/A <input checked="" 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. 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.
Data Protection Officer Name and contact details	Laura NUNEZ BAREZ 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
Record Model	<input checked="" type="checkbox"/> N/A

¹ Pursuant to **article 31** of the new data protection regulation for EU institutions and bodies (**Regulation (EU) 2018/1725**) each controller and processor have to maintain a **record of processing activities** under its responsibility that contains at least the information listed under that article.

1.2 PURPOSE AND DESCRIPTION OF THE PROCESSING

1.2.1 Purpose

The European Labour Authority (ELA) aims to set up and establish a Business Continuity Plan to:

- increase the resilience of the Authority,
- minimise the impact of any disruption and
- facilitate the identification and recovery of key business processes and systems within agreed time frames.

The Business Continuity Policy was officially approved by the Executive Director through Decision 10/2023 in September 2023. This policy outlines procedures related to business continuity, including:

- an Incident Management Procedure
- Recovery Strategies and a
- Simulation Plan to test possible disaster scenarios.

This plan foresees different types of risks a different strategies to face them.

Under this record, contact details of the ELA's workforce shall be processed exclusively by the **Business Continuity Manager/ Steering Committee** for the following purposes:

1. to manage contact lists;
2. to notify about an incident that may constitute a threat to business continuity;
3. to manage a crisis/incident and send crisis/incident related information to, and to request any
4. For training purposes and business continuity exercises follow-up action to ensure business continuity;
5. to enable critical and essential staff to perform their tasks by giving them prioritised access to resources, including offices, equipment and IT, financial and logistical support, when necessary;
6. to maintain a logbook of actions taken in relation to a business continuity incident.

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
- Anonymisation when possible.

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
2. Manual processing
 - a. Word documents
 - b. Excel sheet
 - c. Any other, specify
3. Any other mode, specify

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 **Business Continuity Steering Committee** is the governance body comprised of senior management representatives from ELA that provides leadership, oversight and direction to ELA’s business continuity management. It is comprised by the Executive Director and the Head of Units in the Authority.

This process will include the following actions:

- Creation of a back-up Plan for critical tasks,
- Set up of a Register of incidents
- Relevant FMB created for follow-up actions
- Creation of a specific group to communicate with all staff
- Specific training to be provided

The **Business Continuity Manager (BCM)** of ELA is the Head of Unit (HoU), Governance and Coordination Unit. The BCM is responsible for overseeing the BCM programme. The Business Continuity Manager oversees, reports on, and oversees daily activities related to the business continuity programme.

The **Business Continuity Plan Owner** is the Head of the Resources Unit. The Business Continuity Plan Owner reports to the BCM and oversees creating, implementing, and testing the Business Continuity Plan.

The **Business Continuity Policy Owner** is an employee in the Governance and Coordination Unit. The Business Continuity Policy Owner reports to the BCM and works with the Business Continuity Team to ensure the smooth day-to-day operation of the Business Continuity Management System.

In the event of an emergency, also the following teams can meet:

The **Crisis Management Team** consists of key executives/stakeholders/business unit leaders with critical functions responsible for ensuring that ELA can respond effectively and efficiently to a crisis while protecting the safety and well-being of personnel and assets and minimising the negative impact on the Agency’s operations and reputation. Is composed by the Executive Director, Head of Units, ICT Manager, Logistic Manager and the Spokesperson/Communication Officer.

The **Crisis Communication Team** is responsible for managing and disseminating information in crisis or emergency situations. It is composed by the Executive Director, Head of Governance and Coordination Unit, ICT Manager, Logistics Manager, Spokesperson and Communication Officer.

1.3 DATA SUBJECTS AND DATA CATEGORIES

1.3.1 Data subjects' categories

1. Internal to organisation	ELA Staff appointed as back up and the person in charge of each process.
2. External to organisation	<input checked="" type="checkbox"/> N/A

1.3.2 Data categories/fields

ELA critical and essential staff

Unit, key position, critical task, person in charge

ELA business continuity staff

Back-up person's personal data: Name, surname, professional and personal contact details (phone number, address and e-mail).

All other ELA workforce

Name, surname and private phone number.

In the event of an emergency (operational/cybersecurity/security or data privacy incident) , the following personal data will be collected and processed in the Incident Register by the Business Continuity Policy Owner: the name of the person who reported the incident, date and time of the report, his/her contact's information, accurate description of the incident (date and time of the incident, type of incident, location of the incident, measures taken (if any) and an estimate of the extend of the impact).

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.

In case of an incident, it has to be reported and encoded in the Incident Register about any injured or fatalities and if there is a significant actual or potential damage/threat to life. In these specific cases, personal data will be collected in order to inform the relevant national authorities and/or emergency services.

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 defense of legal claims or whenever the Court of Justice of the European Union is acting in its judicial capacity.
- (g) Processing is necessary for reasons of substantial public interest, [...]

- (h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services [...].
- (i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices [...].
- (j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes [...].

1.3.2.2 Data related to 'criminal convictions and offences'

The data being processed contain sensitive data which fall(s) under Article 11 'criminal convictions and offences'	N/A <input checked="" type="checkbox"/> Yes <input type="checkbox"/>
Description:	

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	Personal data is kept for as long as the person works or provides a service in the ELA plus three months for smooth service operation.

Description

The list of contact persons is replaced by an updated version whenever there is a change in workforce.

1.5 RECIPIENTS

Origin of the recipients of the data	
1. <input checked="" type="checkbox"/> Within the EU organization	ELA Business Continuity Steering Committee ELA Business Continuity Manager ELA Business Continuity Policy Owner ELA Business Continuity Plan Owner ELA Crisis Communication Team ELA Crisis Management Team ELA Data Protection Officer ELA Staff on a need to know basis
2. <input checked="" type="checkbox"/> Outside the EU organization	CERT-EU External Security services of the building Building Management Relevant national authorities (police, fire brigade, care service providers)

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

Specify who has access to which parts of the data:

Description

The Business Continuity Manager, Business Continuity Steering Committee and the Business Continuity Policy Owner have access to all data categories.

In case of an incident, the Crisis Management Team will have access to the information contained in the Incident Register and the Crisis Communication Team will be informed accordingly depending on the need, assessed case-by case by the Steering Committee.

In case of a **personal data breach**, the ELA Data Protection Officer will be involved and informed accordingly to the European Data Protection Supervisor when required. This process is covered by the Record “DPR-ELA-2022-0001 Register of personal data breaches in the European Labour Authority”.

In case of a **security or cybersecurity incident**, the CERT-EU may be involved accordingly to the Record “DPR-ELA-2023-0022 ELA ICT security investigations”.

In case of a **security incident**, the External Security services of the building, the Landererova 12 Building Management and/or the relevant national authorities (police, fire brigade, care service providers) may need to be informed to implement an effective solution to the incident, according to the Record “DPR-ELA-2022- 0008 ELA access control, CCTV system and parking cards”.

ELA Staff will have access to partial information on a need to know basis.

1.6 INTERNATIONAL DATA TRANSFERS

Transfer to third countries or international organisations of personal data
<p>1. Transfer outside of the EU or EEA</p> <p><input checked="" type="checkbox"/> N/A, transfers do not occur and are not planned to occur</p> <p><input type="checkbox"/> YES,</p>
<p>2. Transfer to international organisation(s)</p> <p><input checked="" type="checkbox"/> N/A, transfers do not occur and are not planned to occur</p> <p><input type="checkbox"/> Yes, specify further details about the transfer below</p>

1.7 INFORMATION TO DATA SUBJECTS ON THEIR RIGHTS

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

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>)

Other form of publication, specify

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:

Your data protection rights available at ELA main website: [here](#).

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.