European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2023-0010 Subscription to ELA electronic newsletters and notifications via Newsroom

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

1.1 GENERAL INFORMATION

Record reference	DPR-ELA-2023-0010
Title of the processing operation	Subscription to ELA electronic newsletters and notifications via Newsroom
Controller entity	European Labour Authority, Governance Unit, Communication Sector
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 The European Commission, Directorate-General for Communications Networks, Content and Technology, DG CONNECT Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË 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	☒ 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 Purpose

This processing of personal data aims to establish and administer a list of email addresses to manage the existing newsletters and alerts in the European Labour Authority (ELA).

Subscribers can at any time unsubscribe to the relevant newsletter and/or alert.

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

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. ☒ Subscribe and unsubscribe functionalities

2. ☒ Manual processing
    a. ☐ Word documents
    b. ☐ Excel sheet
    c. ☒ Via Newsroom tool

Description

The European Labour Authority will act as controller and the European Commission as data processor for this specific process of personal data.

The processor maintains a record of all data processing operations carried out on behalf of the controller, transfers of personal data, security breaches, responses to requests for exercising rights of people whose personal data is processed and requests for access to personal data by third parties. The controller has access to the personal data only via Newsroom tool via EU Login.

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

Description:

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the European Commission. 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.

1.2.5 Comments on the processing of the data

The data is accessible via EC Newsroom platform. This process of personal data is covered by the European Commission in the Record "DPR-EC-00841 - Corporate Newsroom".
Access to the platform is EU Login password-protected and accessible only to the assigned Editors. Editors are granted access to the tool by DG CONNECT upon request from the Controller.

1.3 DATA SUBJECTS AND DATA CATEGORIES

1.3.1 Data subjects' categories

1. Internal to organisation	ELA Staff (Communications Sector, assigned editors and internal ELA Staff subscribers to the newsletter(s) and alerts
2. External to organisation	External subscribers to the newsletter(s) and alerts

1.3.2 Data categories/fields

ELA editors
Name, Surname, EU-Login.

The EU Login is a separate process to properly identify users and grant the correct accesses. It belongs to the European Commission and is covered by Record "DPR-EC-03187 - Identity & Access Management Service (IAMS)".

Subscribers (internal or external): E-mails.

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** ☒ **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**
ELA editors' personal data	Personal data will be collected as long as the user has this role.
Email for subscriptions/alerts	All personal data collected via Newsroom is kept as follows: • the subscriber consents to the processing and until the subscriber unsubscribes himself or herself or requests the controller to delete his/her account, • or 5 years from the last interaction of the data subject with Newsroom. It is important to note that receiving a newsletter/notification is not considered an "interaction" for this purpose. "Interactions" are actions from the subscriber such as subscribing, confirming a subscription, updating a subscription, etc.

Description
The data subject can also ask for modifications of personal data or withdraw their consent at any time, by sending an email to the controller, and their data will be updated (or deleted) as soon as possible and no longer than 15 days after his/her request.

1.5 RECIPIENTS

Origin of the recipients of the data	
1. ☒ Within the EU organization	Authorised Editors assigned by the Controller at the European Labour Authority
2. ☒ Outside the EU organization	European Commission, DG CONNECT

Categories of the data recipients
1. ☒ A natural or legal person 2. ☒ Public authority 3. ☒ Agency 4. ☐ Any other third party, specify

Internal recipients have access to the list of subscribers, relevant documents, databases, uploaded batches of data, subscriptions/alerts.

External recipients have access to the personal data related to the ELA Editors, subscribers' email, topics of interest and the frequency of notifications.

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,
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
3. 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).

Description

There are no transfers of personal data to third countries or international organisations.

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 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 on data subjects' rights is available on 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:
Your rights at ELA are 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 personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

2 PART 2: INTERNAL – COMPLIANCE, RISK AND SECURITY CHECKLISTS

Part 2 is only visible to Controllers and ELA DPO

2.1 COMPLIANCE CHECKLIST

2.1.1 Lawfulness and fairness

Lawfulness for the processing of personal data under article 5.1	
☐ (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.
☐ (b)	Processing is necessary for compliance with a legal obligation to which the controller is subject.
☐ (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.
☒ (d)	The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
☐ (e)	Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
Lawfulness for the processing of personal data under article 5.2	
☐ The basis for the processing referred to in points (a) and (b) of paragraph 1 has been laid down in the following Union law: ☒ N/A	
Reason(s) supporting the lawfulness of the data processing (explanation as to why the processing is necessary) **:**	
If applicable, specific legal basis in addition to article 5.1:	

Description

The process of personal data is based on a voluntary basis.

2.1.2 ☒ Purpose limitation

1. The purposes for data processing have been clearly identified and documented.
2. The details of the purposes of processing have been sufficiently referenced in the Privacy statement.
3. The processing is regularly reviewed, and where necessary the documentation and the Privacy statement is updated.
4. If personal data is intended to be used for a new purpose, it is ensured that this is compatible with the original purpose or specific consent is taken for the new purpose.

2.1.3 ☒ Data minimisation

1. Limited amount of personal data is collected for specific purposes (limited).
2. The amount of personal data collected is adequate for the processing (adequate).
3. The personal data that is held is relevant to the processing, and periodically reviewed (relevant).

2.1.4 ☒ Accuracy

1. Personal data held is kept accurate and up to date.
2. There are appropriate processes in place to check the accuracy of the data collected, record the source of that data, and to deal with data subject's requests for rectification of their data.
3. In case any personal data is incorrect or misleading, reasonable steps are taken to correct or erase it as soon as possible.

2.1.5 ☒ Storage limitation

1. Personal data held is regularly reviewed and is not kept any longer than it is needed (for the purpose it was collected). It is erased or anonymised when it's no longer needed.
2. Policy with standard retention periods are in place in case of data storage for periods exceeding their purpose.
3. There are appropriate processes in place to deal with data subjects' requests for erasure of their data (right to be forgotten).
4. Personal data is not kept for longer than for the intended purpose, except for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In such cases these personal data are clearly identified.

2.1.6 ☒ Integrity and confidentiality

1. An analysis of the risks presented by the data processing is performed, therefore assessing the appropriate level of security to be put in place.
2. When deciding which security measures to implement, the state of the art and costs of implementation are considered.
3. Appropriate technical and organizational measures are in place for security of the personal data.
4. When appropriate, measures such as pseudonymisation and encryption are used.
5. There are appropriate measures in place to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
6. A well-defined information security policy is in place and is regularly reviewed for improvements.

2.1.7 ☒ Accountability

1. Data protection policies are implemented and adopted where proportionate.
2. A 'privacy by design and default' approach is taken throughout the entire lifecycle of processing operations.
3. There are written contracts in place with organisations that process personal data on our behalf.
4. Documentation of the processing activities is maintained and kept up to date.
5. Personal data breaches are reported and recorded where necessary.
6. Data protection impact assessments are carried out and documented for personal data processing which result in high risk to data subjects' interests.
7. Adherence to relevant codes of conduct.

2.1.8 ☒ Transparency and Rights of data subjects (access to data and other rights)

1. Compliance with the conditions pertaining to the information to be provided, and the rights of data subjects mentioned in Articles 15 to 24.
2. Compliance of the data processing with the articles listed above have been stated in the Privacy statement *(see section 1.7.1 of the record)*

2.2 RISK ASSESSMENT CHECKLIST

The Controller shall carry out a risk assessment to establish if the type of processing operation at hand is likely to result in a high risk to the rights and freedoms of natural persons, which requires a further assessment of the impact on the protection of personal data.

2.2.1 Identification of high-risk processing operations and requirements for a Data Protection Impact Assessment (DPIA).

2.2.1.1 A DPIA already exists (article 39§1)

☐ A DPIA already exists that is addressing a similar set of processing operations as the one at hand. Thereby there is no need to carry out a separate DPIA as provided for in article 39,§1.

☐ Link to or attachment of the relevant DPIA:

☒ N/A

2.2.1.2 Legal requirement for DPIA (article 39.1)

Indicate if the processing operation is concerned by any of the following risky processing operations which shall in particular be subject to a DPIA (article 39.1 (a)-(c)):

☐ (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

☐ (b) processing on a large scale of special categories of data referred to in Article 10, or of personal data relating to criminal convictions and offences referred to in Article 11; or

☐ (c) a systematic monitoring of a publicly accessible area on a large scale.

☒ N/A
☐ One or more boxes ticked = DPIA is required

2.2.1.3 EDPS list of processing operations requiring a DPIA (article 39.4)

Indicate if the processing operation corresponds to one or more of the types of 'risky' processing operations on the **EDPS 'positive' list** for which a DPIA is required, pursuant to article 39.4:

☒ N/A = Proceed with the EDPS threshold assessment
☐ Yes = DPIA is required

2.2.1.4 EDPS threshold assessment for 'High risk' criteria

Indicate if the processing operation corresponds to one or more of the following of the EDPS' threshold criteria for a DPIA :

1. ☐ Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting

2. ☐ Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects
3. ☐ Systematic monitoring: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces
4. ☐ Sensitive data: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for identification purposes, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or otherwise considered sensitive

5. ☐ Data processed on a large scale, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage
6. ☐ Datasets matched or combined from different data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject
7. ☐ Data concerning vulnerable data subjects: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified
8. ☐ Innovative use or applying technological or organizational solutions that can involve novel forms of data collection and usage
9. ☐ Preventing data subjects from exercising a right or using a service or a contract

Result of threshold assessment

Are two or more boxes on the list of high-risk criteria ticked?:

☒ No = The processing is unlikely to result in a high risk to the rights and freedoms of natural persons and a DPIA is **not** required

☐ Yes = The processing is likely to result in a high risk to the rights and freedoms of natural persons, therefore a DPIA shall be required.

2.2.2 Overall result of the risk level assessment

☐ **DPIA is required**

☒ DPIA is **not** required, based on one of the following criterion:

☒ The processing operation does not involve high-level risks.

☐ The processing operation is on the EDPS 'negative list' of types of processing for which a DPIA is not required (article 39.5).

☐ Pursuant to the conditions under article 39.10, a DPIA has already been carried out as part of a general impact assessment preceding the adoption of a legal act.

☐ Although, the processing operation corresponds to one or more of the criteria for DPIA requirement listed in this section, it is considered unlikely to result in a high risks to the rights and freedoms of affected persons.

☒ **Opinion of the DPO obtained** (March 2023) The processing operation does not involve high-level risks.

2.2.3 Outcome of DPIA

1. The processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk result in a high risk to the rights and freedoms of natural persons and the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation:

   ☒ N/A
   ☐ Yes, there are residual risks

2. ☐ Completed DPIA is attached

   Indicate the reference to any additional documentation related to the DPIA, if applicable:
   Click here to enter text.

2.2.4 EDPS prior consultation

1. Based on the outcome of a DPIA and after consultation with the DPO, it is considered that an EDPS prior consultation is required:

   ☒ N/A

☐ Yes

The date of DPO consultation (optional):

2. The type of processing operation is listed in a ELA implementing act pursuant to Article 40(4) of the regulation for which an EDPS prior consultation is required:

☒ N/A
☐ Yes

2.3 SECURITY MEASURES CHECKLIST

Security measures put in place for securing the processing operations on personal data and any data system used.

> ***"Article 33 Security of processing"***
>
> *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate:…"*

2.3.1 Detailed description of information security measures in place

Explanation of the security measures described in detail in the Record "*DPR-ELA-2022- 0008 ELA access control, CCTV system and parking cards*"

2.3.2 Supporting documentation

If applicable, indicate the relevant supporting documentation for the security measures applied:
☐ Attached
☐ Link:

2.3.3 Measures adopted

Indicate the type of measures in place by selecting what's applicable from the following list, or by adding measures as appropriate to the relevant processing operation:

1. ☒ Organisational measures

☒ Risk Assessment and Risk management underly the relevant security measures.

- An analysis of the risks presented by the processing has been undertaken, and it has been used to assess the appropriate level of security required to be put in place.
- When deciding what measures to implement, the state of the art and costs of implementation has been taken into account.
- An information security policy (or equivalent) or an associated set of policies are in place in specific areas and steps to make sure the policy is implemented are taken (e.g. controls to enforce them).
- The information security policies and measures are reviewed regularly and, where necessary, improved.

Description

☒ Personal data breach handling mechanism is in place

SOP 6/2022 on personal data breaches

☒ Any other, specify

Description
SOP 7/2022 for handling data subjects' requests

2. ☒ Technical measures

☒ Physical security

☒ Cybersecurity
Description
Microsoft Defender

SLA with CERT-EU

☒ Encryption and/or pseudonymisation of personal data
Description
SOP on encryption policy
☐ Any other, specify

☒ The data will be hosted on infrastructure that is either owned by DG DIGIT (and hence meets DG DIGIT's security standards) or on 3rd party infrastructure that has been approved by DG DIGIT and that meets their security requirements.

Thereby, measures are in place to
- aim for using privacy-enhancing technologies (PETs);
- ensure confidentiality, integrity availability and resilience of processing systems and services;
- to restore availability and access to personal data in a timely manner in the event of physical or technical incident.

☒ Any data processor used also has appropriate technical and organisational measures in place.