



European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2023-0019 ELA network services (internal and E-Guest WiFi)

1 PART 1: PUBLIC - RECORD (ARTICLE 31¹)

1.1 GENERAL INFORMATION

Record reference	DPR-ELA-2023-0019
Title of the processing operation	ELA network services (internal and E-Guest WiFi)
Controller entity	European Labour Authority, Resources Unit, ICT Sector (ELA ICT 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 Vodafone Belgium Rue Archimede 25, 1000, Bruxelles
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

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) makes available for the benefit of persons who visit, work or are otherwise present in ELA premises in professional, educational or private grounds ('users') a direct and free or charge internet access service based on a Wi-Fi hotspot, and specifically the wireless network **E-Guest**.

The European Labour Authority is responsible for the provision of Wi-Fi services for its premises.

By connecting to the ELA's guest Wi-Fi network, the user has to accept the terms and conditions and the relevant privacy statement (here attached under point 1.7) prior to their connection.

1.2.2 Processing for further purposes

- Archiving in the public interest
- Scientific or historical research purposes
- Statistical purposes

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
2. Manual processing
 - a. Word documents
 - b. Excel sheet
 - c. Any other, specify O365 tools

Description

Automatic process without any manual intervention.

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

1.2.5 Comments on the processing of the data

By nature, the infrastructure devices should store the data for the period of time the user is connected; this goes from extremely short periods of some milliseconds to several hours (the time of a remote connection for teleworking, for example).

Beside this functional usage, Statistics about the user (and associated parameters) are collected for troubleshooting and the detection of technical problems

1.3 DATA SUBJECTS AND DATA CATEGORIES

1.3.1 Data subjects' categories

1. Internal to organisation	<input checked="" type="checkbox"/> Yes ELA Staff
2. External to organisation	<input checked="" type="checkbox"/> Yes Persons who visit, work or are otherwise present in ELA premises in professional, educational or private grounds

1.3.2 Data categories/fields

Indicate the categories of data that will be processed:

- Userid
- User IP address
- Required service IP address
- Required Application type
- Start time
- Connection duration
- Logs

Some of those data categories are obtained by the end-user directly (typically the userid on remote connections).

The provision of this personal data is mandatory to start the service with a well-identified user in order to associate the right authentication and authorization parameters to the connection. As a result , **no anonymous access is allowed.**

The remaining personal data are collected from the technical infrastructure , which allows the establishment of the connection or the duration of the connection based on the user’s activity .

1.3.2.1 Special categories of personal data

<p>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:</p> <p><input type="checkbox"/> Yes , the processing concerns the following special category(ies):</p> <p style="margin-left: 20px;">Data revealing</p> <p style="margin-left: 40px;"><input type="checkbox"/> racial or ethnic origin,</p> <p style="margin-left: 40px;"><input type="checkbox"/> political opinions,</p> <p style="margin-left: 40px;"><input type="checkbox"/> religious or philosophical beliefs,</p> <p style="margin-left: 40px;"><input type="checkbox"/> trade union membership,</p> <p style="margin-left: 20px;">Or/and,</p> <p style="margin-left: 40px;"><input type="checkbox"/> Genetic data, biometric data for the purpose of uniquely identifying a natural person,</p> <p style="margin-left: 40px;"><input type="checkbox"/> Data concerning health,</p> <p style="margin-left: 40px;"><input type="checkbox"/> Data concerning a natural person’s sex life or sexual orientation.</p> <p><input checked="" type="checkbox"/> N/A</p>

1.3.2.2 Data related to 'criminal convictions and offences'

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

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	Maximum 6 months after leaving ELA or for guests 12 months after dormant account.

1.5 RECIPIENTS

Origin of the recipients of the data	
1. <input checked="" type="checkbox"/> Within the EU organization	ELA Staff responsible for the service and the intramural contractors associated with the service
2. <input checked="" type="checkbox"/> Outside the EU organization	External contractor staff individually identified in charge of the technical and/or organisational support CERT-EU staff

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

Description

ELA Staff responsible for the service and the intramural contractors associated with the service.
 External contractor staff individually identified in charge of the technical and/or organisational support.
 CERT-EU staff in case of a security incident or breach. The processing of personal data will be covered by Record “DPR-ELA-2023-0022 ELA security investigations”.

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>	
<p>3. Derogations for specific situations (Article 50.1 (a) –(g))</p> <p><input checked="" type="checkbox"/> N /A</p> <p><input type="checkbox"/> Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply (ies).</p>	

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 a privacy statement attached to this record.

Publication of the privacy statement

Published on website

Web location:

- ELA internal website (URL: <https://eulabourauthority.sharepoint.com/sites/PersonalDataProtection>)
- External website (URL: <https://www.ela.europa.eu/en/privacy-policy>)

Other form of publication, specify

QR available for ELA Guests.

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 here: <https://www.ela.europa.eu/sites/default/files/2023-04/Your-data-protection-rights-at-ELA.pdf>

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.