



European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2022-0011 Email system at the European Labour Authority

1 PART 1: PUBLIC - RECORD (ARTICLE 31¹)**1.1 GENERAL INFORMATION**

Record reference	DPR-ELA-2022-0011
Title of the processing operation	Email system at the European Labour Authority
Controller entity	European Labour Authority, Resources Unit, ICT and facilities (ELA ICT Team)
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
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 GlobalSign certificates for encrypted email provided by GMO GlobalSign NV, Diestsevest 14, 3000 Leuven, Belgium
Data Protection Officer Name and contact details	Laura NUNEZ BAREZ Landererova 12, 811 09 Bratislava I Slovakia Email: data-protection@ela.europa.eu
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 main purpose of the Email Service of the European Labour Authority (ELA) is to enable electronic communication, in particular the exchange of electronic messages and attachments, amongst ELA staff, with external partners of the European Labour Authority and with the general public (EU citizens etc.).

This operations aims at:

- 1) Providing users of the email system what they expect from a modern electronic communication tool: consolidated data storage, an address book to ease the addressing of internal correspondents and main external partners (other EU institutions and bodies), the possibility to recover items recently deleted by mistake etc.;
- 2) Managing the email system regarding its availability, its capacity, its security etc.;
- 3) Reducing the risks associated with external communications, for instance by removing or blocking incoming malware before it damages users' or EC assets;
- 4) Enforcing compliancy to rules defined at EU level, such as the "eDOME" rules on document management;
- 5) Supporting ELA investigation authorities in their duties.

Only non-classified information may be communicated on the ELA email systems; **confidential information must be encrypted.**

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. Any other, specify

Mail processing rules as defined by individuals in their personal mailboxes, for Functional Mailboxes or globally in the Cloud Tenant.

For encrypted email, the European Labour Authority staff use GlobalSign certificates.

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

Description

Management of data containers

Clean-up and routing of email traffic

Provision of an email address book - Generation and management of a global address book (which includes some personal data), exchanged with counterpart services of other EU institutions.

Other general operations

Monitoring of system usage and collection of usage statistics;

Operators' interventions while managing the supporting systems (e.g. client access servers, transport servers, storage disk arrays...).

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:

The data processed by the Email Service as part of the management of the data containers and the address book is stored outside ELA premises.

1.2.5 Comments on the processing of the data**1.3 DATA SUBJECTS AND DATA CATEGORIES****1.3.1 Data subjects' categories**

1. Internal to organisation	<input checked="" type="checkbox"/> Yes "Users" are the actual users of the ELA email system, owning a personal mailbox on that system.
2. External to organisation	<input checked="" type="checkbox"/> Yes "Partner contacts" are all staff of European institutions and bodies (themselves called "partners" hereafter). This category specifically applies to the management of the email address book. "Anyone else" means anybody whose email address appears in the "To", "From", "CC" or "BCC" traffic fields of an email message, as soon as these messages have been processed by the email system of the European Commission.

1.3.2 Data categories/fields

— **Identification data:** Professional email address, First name, last name, Office location (building, floor, room), Office phone number, Affectation (Directorate General, Service, Department...), Mobile phone number (for "users" who have provided this information in their M365 User Account on a voluntary basis); Picture (for "users" who decided to make one available) (managed by each "user" for themselves); Responsibility on functional (shared) mailboxes; Membership of distribution groups (usually related to the affectation, the business roles and/or the rights on IT systems).

— **Email messages information:** header, subject, body and attachments, Calendar items and tasks (including their header, body and attachments), Any other types of documents with their own specific characteristics, Name of the mailbox folder in which the document is stored, Meta-data about those email messages, calendar items and other documents, as automatically generated by the email systems (e.g. the date when the document was stored in the system, a status such as “read” or “recently deleted”...), Invitations, which is actually just a specific type of email message, Sender (source: meta-data of the message transmission), Recipients towards which the ELA email systems are asked to route the message (source: meta-data of the message transmission), Date and time of handling by ELA email servers (source: the email system).

Log files: Information logged regarding user access to the email system and activity:

— Details about each access: date/time, username, source IP address, protocol and/or used software (depending on the type of access) and who performed certain types of actions (esp. items deletion) and when.

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:

Although e-mail messages may contain special categories of data, ELA staff is encouraged to use encrypted email to communicate this type of information. Special categories of data are not used for this processing operation.

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 [...].

Additional information

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: Although e-mail messages may contain references to criminal records and/or offences, ELA staff is encouraged to use encrypted email to communicate this type of information. Special categories of data are not aimed by this processing operation.	

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	Optional	
		Start date/moment	End date/moment
Identification data - Address book entry	Kept for 6 months after the deletion of their owner's user account.		
Messages and documents stored in mailboxes	These data are stored centrally for 6 weeks after the departure of the user and deleted after this period.		
Message or document deleted from a mailbox	These data are stored centrally for 6 weeks after the departure of the user and deleted after this period		
Traffic logs, clean-up logs, system usage logs, system access logs	Maximum of 6 months		

Description

Address book

The email service only provides the address books to its users. As a general rule, a "user" is known in the address book for as long as he has a contractual position with ELA, while a "partner contact" is

known in the address book for as long as it is mentioned in the information periodically received from the partner organisation.

A message or document deleted from a mailbox is permanently deleted.

Traffic logs, clean-up logs, system usage logs, system access logs:

- These information sources are essential in the context of the operations of the email systems and the management of the email service, especially for incidents, problems, capacity and security management.

- The retention period for traffic logs is 6 months.

- The retention period for the clean-up, system usage and system access logs produced is maximum 6 months.

Would logs data that may convey personal information, have to be kept for longer than 6 months, it would then be either anonymised or aggregated in such a way that there is no possibility to link the data back to data subjects.

No historical or statistics usage of personal data is planned after the retention period. Any data that needs to be kept longer is either anonymised or aggregated in such a way that there is no possibility to link the data back to data subjects.

1.5 RECIPIENTS

Origin of the recipients of the data	
1. <input checked="" type="checkbox"/> Within the EU organization	ELA users ELA ICT Team, responsible for the email system and IT security
2. <input checked="" type="checkbox"/> Outside the EU organization	CERT-EU Staff European Commission and other EU Institutions and bodies Any other email recipient Software providers, hardware providers, computer emergency response teams, external parties providing anti-malware services, i.e. M365, GlobalSign.

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
Specify who has access to which parts of the data: All the users have access to the information mentioned under Identification data Email messages information will be received by specific recipients. In case of an incident, access to log files is provided to ELA ICT Team and the CERT-EU staff responsible for carrying out this processing operation and any other authorised staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements. GlobalSign have access to Common name (Name and Surname), Organization, Organizational Unit, Locality, State of Province, Country, Email Address. European Commission will receive Name, Surname, Organization, E-mail, Telephone number, Office and Department. Actually manager or Job title are not predefined field

The information collected will not be given to any third party, except to the extent and for the purpose the controller may be required to do so by law.

Description

European Commission will receive periodically an update on ELA staff in order to be integrated on the Global Address Book. This processing of personal data is covered by the European Commission Record: DPR-EC-03610 Email system of the European Commission, under DG Informatics (DG DIGIT).

1.6 INTERNATIONAL DATA TRANSFERS

Transfer to third countries or international organisations of personal data	
1. Transfer outside of the EU or EEA	
<input type="checkbox"/> N/A, transfers do not occur and are not planned to occur <input checked="" type="checkbox"/> YES,	
Country(ies) to which the data is transferred	Email messages and attachments could be sent out to and received from anybody around the world.
2. Transfer to international organisation(s)	
<input type="checkbox"/> N/A, transfers do not occur and are not planned to occur <input checked="" type="checkbox"/> Yes, specify further details about the transfer below	
Names of the international organisations to which the data is transferred	
3. Legal base for the data transfer	
<input checked="" type="checkbox"/> Transfer on the basis of the European Commission's adequacy decision (<i>Article 47</i>) <input checked="" type="checkbox"/> Transfer subject to appropriate safeguards (<i>Article 48.2 and .3</i>), specify:	
2. (a) <input type="checkbox"/> A legally binding and enforceable instrument between public authorities or bodies. Standard data protection clauses, adopted by (b) <input type="checkbox"/> the Commission, or (c) <input type="checkbox"/> the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2) . (d) <input type="checkbox"/> Binding corporate rules, <input type="checkbox"/> Codes of conduct , <input type="checkbox"/> 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:	
<input checked="" type="checkbox"/> 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. <input checked="" type="checkbox"/> Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	
<input checked="" type="checkbox"/> Transfer based on an international agreement (<i>Article 49</i>), specify	
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 defense 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

By definition of an e-mail system, e-mail messages and attachments could be sent out to and received from anybody around the world. This includes ELA email system users willingly or unknowingly sharing personal data of other ELA email system users (for example, by having the email address of other ELA email system users in copy of an email sent to a third party)

Security measures in place

Authentication and authorization of the users.

Authentication and authorization at server level, no anonymous access allowed.

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: ELA 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:

Available under Data protection Policy in ELA main website.

What regards incorrectly encoded data in the global address book, data subjects are instructed to take contact with the ELA IT Helpdesk who will guide them to initiate the corresponding change procedures.

Received e-mail messages in a data subject mailbox are under the full control of the user, thus having ALL the rights on these messages (like accessing, storing and deleting). Those rights do not apply to other copies of the same messages stored in somebody else's mailbox.

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.