European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2023-0022 ELA ICT security investigations

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

1.1 GENERAL INFORMATION

Record reference	DPR-ELA-2023-0022
Title of the processing operation	ELA ICT security investigations
Controller entity	The European Labour Authority, Resources Unit, ICT and Facilities Sector (ELA ICT 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 **CERT EU** Rue de la Loi 107, 1000 Brussels, Belgium. **Microsoft Ireland** South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.
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
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) aims to protect its ICT infrastructure against any type of threats, vulnerabilities or incidents. To this purpose, the ELA has concluded and agreement with the European Commission, DG DIGIT, CERT-EU[1].

The purpose of this processing of personal data is to contribute to the security of the ICT infrastructure of the Authority and to enable CERT-EU to carry out its mission, which is to contribute to the security of the ICT infrastructure of all Union institutions, bodies and agencies by helping to prevent, detect and mitigate and respond to cyber-attacks, and by acting as their cyber-security information exchange and incident response coordination hub.

CERT-EU collects, manages, analyses and shares information with the Union institutions, bodies and agencies (the constituents) on threats, vulnerabilities and incidents on unclassified ICT infrastructure. It coordinates responses to incidents at interinstitutional and constituent level, including by providing or coordinating the provision of specialised operational assistance.

This process of personal data is linked to the record prepared by the CERT-EU, Record "DPR-EC-07167 – CERT-EU activities".

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

2. ☒ Manual processing
   a. ☒ Word documents
   b. ☒ Excel sheet

3. ☒ Any other mode, specify
   Automated processing may involve any personal data flowing or stored on ELA's electronic networks and firewalls, namely logs and intrusion detection sensors.

1.2.4 Storage medium

1. ☐ Paper
2. ☒ Electronic

[1] The Computer Emergency Response Team for the EU institutions, bodies and agencies, the CERT-EU is an inter-institutional service provider working as the Computer Security Incident Response Team of all the EU institutions, bodies and agencies. Their missions is to contribute to the security of EU institutions and agencies' ICT infrastructure by helping them to prevent, detect, mitigate and respond to cyber attacks. The CERT-EU is administratively hosted within the Directorate-General for Informatics of the European Commission.

a. ☒ Digital (MS documents (e.g. Word, Excel, Powerpoint), Adobe pdf, Audiovisual/multimedia assets, Image files (.JPEG, .PNG, etc.)) and video conference calls and other video recordings.
b. ☒ Databases
c. ☒ Servers
d. ☒ Cloud

3. ☐ External contractor premises

1.3 DATA SUBJECTS AND DATA CATEGORIES

1.3.1 Data subjects' categories

1. Internal to organisation	ELA Staff, in particular ICT Sector staff
2. External to organisation	CERT-EU staff Any citizen

1.3.2 Data categories/fields

In general the following personal data will be collected:

- Any file (with user-id included) stored in, transmitted from / to a host involved in an incident (such as victim, relay or perpetrator);
- Email addresses, phone number, role, name, organisation;
- Name of the owner of assets involved in an incident, user account name (for email, operating system, applications or centralised authentication services); and
- Technical protocol data (IP address, MAC address) to which an individual may be associated or the device connection at the time of the incident.

In particular, for Cyber Threat Management (first response, analysts and vulnerability assessment teams): IP addresses will be checked. *Please note that IP addresses may be related with threat actor groups (suspected malicious cyber activity groups), and, therefore will not be considered as personal data.*

For Incident response management: IP addresses, connection information, files and logs, including network traffic.

For automated cybersecurity procedures: online media sources (including name/surnames of authors, journalists, etc.), cybersecurity information sharing partnership (such as metadata or IP addresses).

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**
Personal data that might be processed for automated cybersecurity procedures	Data will be kept for up to 3 years
Personal data processed for Cyber Threat Management:	For reports: 5 years and an additional 5 year period for archiving. For all other data: up to 10 years and an additional 10 year period for archiving.
For Personal data processed for Incident response management:	Data is kept for up to 2 years. For network traffic up to few days.

Time limits according to the information declared in record "DPR-EC-07167 – CERT-EU activities".

Where data has not been collected for cyber incident investigation purposes, then the retention period for standard operational processing will apply. i.e. it will be retained for significantly shorter periods than advised above.

1.5 RECIPIENTS

Origin of the recipients of the data	
1. ☒ Within the EU organization	ELA ICT Sector Resources HoU Executive Director
2. ☒ Outside the EU organization	CERT-EU authorised staff working in the specific incident CERT EU Steering Board European Court of Justice

Categories of the data recipients
1. ☒ A natural or legal person 2. ☒ Public authority 3. ☒ Agency

4.	☐ Any other third party, specify

Description

CERT-EU will have access to all data categories in case of an incident. It will be after an internal decision taken by The Executive Director, following the assessment of the ICT Manager, Head f Resources Unit and the Data Protection Officer.

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

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: https://eulabourauthority.sharepoint.com/sites/PersonalDataProtection)
- 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.

Guidance on data subjects' rights on ELA main website.

1.8 SECURITY MEASURES

Short summary of overall Technical and Organizational Measures implemented to ensure Information Security:

Description:

In ELA:
All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored in the Microsoft Azure Cloud environment.
Microsoft are bound by a specific contractual clause for any processing operations of personal data on behalf of European Labour Authority, and by the confidentiality obligations deriving from the General Data Protection Regulation in the EU Member States ('GDPR' Regulation (EU) 2016/679).

In order to protect personal data, 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.

In the CERT-EU:
All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of CERT-EU, or the respective EU institutions, agencies and bodies. Administrative documents may also be stored in paper form. CERT EU has implemented security measures to protect server hardware, software and the network from accidental or malicious manipulations and loss of data. Data is stored on servers managed by CERT-EU in line with the technical security provisions laid down in the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, its subsequent versions, its implementing rules (as adapted from time to time) and the corresponding security standards and guidelines, as well as the Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on the security in the Commission, its implementing rules and the corresponding security notices or on servers managed by the respective EU institutions, bodies and agencies. These documents (as adapted from time to time) are available for consultation at the following address: https://ec.europa.eu/info/publications/security-standards- applying-all-european-commission-information-systems_en

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures in place. 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.

Access to data is restricted by several means, such as user's credentials (username and password), specific IP access lists, Multi-Factor Authentication.