European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2023-0030 Microsoft365 Copilot at ELA

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

1.1 GENERAL INFORMATION

Record reference	DPR-ELA-2023-0030
Title of the processing operation	Microsoft365 Copilot at ELA
Controller entity	European Labour Authority, Resources Unit
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 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
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 Description

The European Labour Authority (ELA) aims to provide ELA staff access to M365 Copilot to support their daily tasks. In practice, Microsoft Copilot will provide real-time intelligent assistance, enabling ELA users to enhance their creativity, productivity, and skills.

Microsoft Copilot for Microsoft 365 is the Artificial Intelligence (AI) assistant from Microsoft, in Microsoft 365 apps like Word, Excel, and Teams, offered to Microsoft 365 Enterprise E5 business and enterprise subscribers as a premium add-on. In sum, Copilot is a set of generative AI tools that users can use inside of mini Microsoft applications.

Copilot for Microsoft 365 uses a combination of large language models (LLMs), a type of artificial intelligence (AI) algorithm that uses deep learning techniques and vast data sets to understand, summarize, predict, and generate content.

Copilot licenses are set up and assigned by the **ELA Resources Unit** as Microsoft Administrator for the European Labour Authority and in particular, Copilot inherits the security, compliance, and privacy policies that the European Labour Authority, Resources Unit, Informatics Sector have set up in Microsoft 365.

ELA uses Microsoft Copilot to enhance its staff's creativity, productivity, and skills with AI assistance in Microsoft 365 apps. Microsoft Copilot respects the ethical principles of AI and ensures that the personal data it processes is used in a lawful, secure, proportionate and transparent manner.

Purpose
Copilot is designed to create, summarise, and analyse user's documents, messages, and data.
It can also generate drafts, analyse spreadsheet data and create presentations using natural language request.

Copilot generally accessed user files that are stored on one of Microsoft's online storage tools and in the users SharePoint or One Drive. In some cases Copilot doesn't index files in the local hard drive, as is the case with Microsoft Excel and they are therefore not available for Copilot to process.

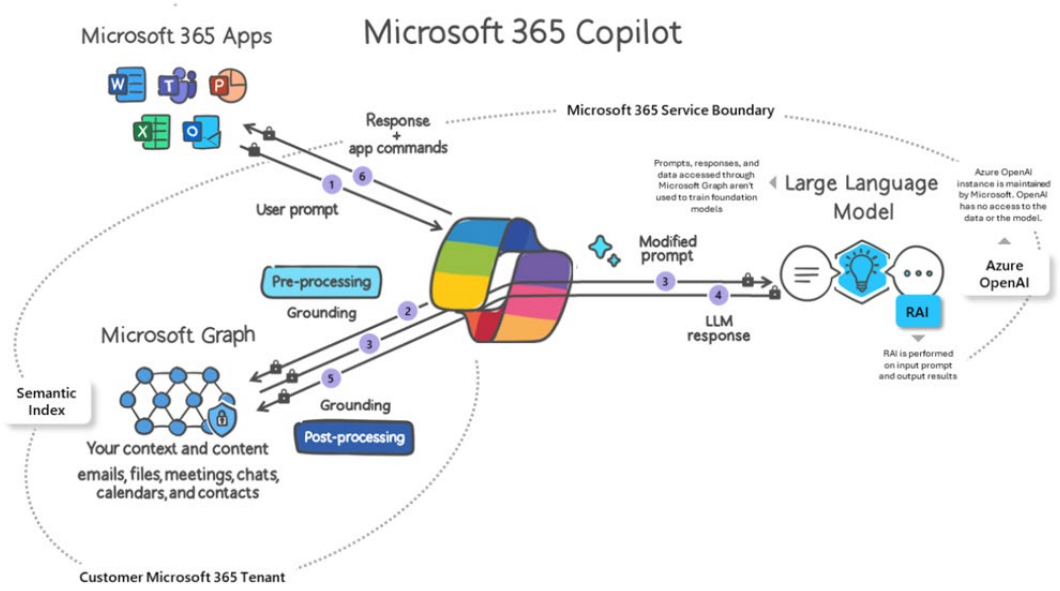
How does Copilot works?

Copilot uses a large language model that mimics natural language based on patterns from large amounts of training data. The model is optimized for conversation by using Reinforcement Learning with Human Feedback (RLHF)—a method that uses human demonstrations to guide the model toward a desired behaviour.

In practice, when users submit a text prompt to Copilot, the model generates a response by making suggestions about what text should come next in a string of words. The model is based on a domain-specific language (DSL) that allows users to specify what kind of information they want to search and synthesize from their Microsoft 365 data.

It is important to note however that Copilot does not learn from the prompts that the users submits.

The following diagram provides a visual representation of how Microsoft Copilot for Microsoft 365 works.



Below an explanation of how Microsoft Copilot for Microsoft 365 works: **STEPS FOLLOWED**

1. User introduce a prompt in one of the M365 Apps, such as Word or Excel and send it to Copilot (**input prompt)**.
2. Copilot receives the prompt and accesses **Microsoft Graph** (user's context and content such as emails, files, meetings, chats, calendars and contacts). Copilot only accesses data that an individual user has existing access to, based on, for example, existing Microsoft 365 role-based access controls.
3. Copilot **sends this prompt to the LLM for processing**.
4. Copilot receives LLM response.
5. Copilot takes the response from the LLM and post-processes it. This **post-processing** includes other grounding calls to Microsoft Graph, responsible AI checks, security, compliance and privacy reviews, and command generation.
6. Copilot **returns the response** to the app, where the user can review and assess the response.

For which applications Copilot will be available?

Here below a summary of the applications where Copilot may be available, the actions allowed and description of the possible tasks to be developed.

Microsoft 365 App	**Feature**	**Description**
Microsoft Word	Draft with Copilot	*Generate text with and without formatting in a new or existing document. Words files can be also used for grounding data.*
	Chat	*Create content, summarize, ask questions about your document and do light commanding via Chat.*
Microsoft PowerPoint	Draft with Copilot	*Create a new presentation from a prompt or Word file, leveraging enterprise templates. PowerPoint files can be also used for grounding data.*
	Chat	*Summary and Q&A*
	Light commanding	*Add slides, pictures, or make check-wide formatting changes.*
Microsoft Loop	Collaborative content creation	*Create content that can be collaboratively improved through direct editing or refinement by Copilot.*
Microsoft Outlook	Coaching tips	*Get coaching tips and suggestions on clarity, sentiment and tone along with an overall message assessment and suggestions for improvement.*

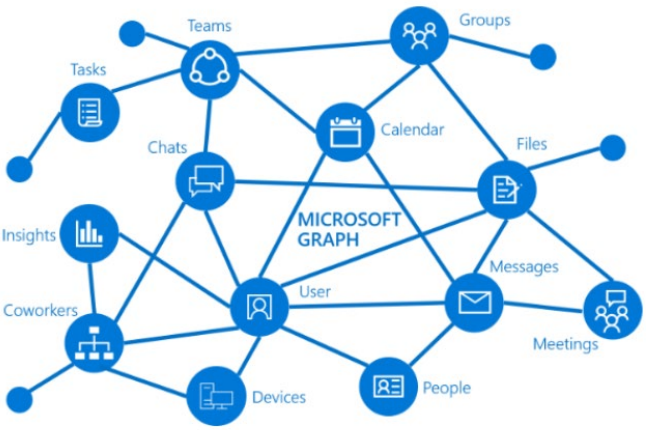
	Summarize	*Summarize an email thread to help the user quickly understand the discussion.*
	Draft	*Pull from other emails or content across Microsoft 365 that the user already has access to.*
Teams	Chat	*Users can invoke Copilot in any chat. Copilot can summarize up to 30 days of the chat content prior to the last message in a given chat. Copilot uses only the single chat thread as source content for responses and can't reference other chats or data types (for example, meeting transcripts, emails, and files). Users can interact with Copilot by selecting pre-written prompts or writing their own questions. Responses include clickable citations that direct users to the relevant source content that was used. Conversations with Copilot take place in a side panel that allows users to copy and paste. Copilot conversations will disappear after the side panel is closed.*
	Meeting	*Users can invoke Copilot in meetings or calls within the same tenant. Copilot will use the transcript in real-time to answer questions from the user. It only uses the transcript and knows the name of the user typing the question. The user can type any question or use pre-determined prompts; however, Copilot will only answer questions related to the meeting conversation from the transcript. The user can copy/paste an answer and access Copilot after the meeting ends on the Recap page.*
	Copilot	*Allows users to access data across their Microsoft 365 Graph and leverage LLM functionality. Copilot can be accessed in Teams and when signed-in to Bing with an active directory account.*
	Whiteboard	*Makes meetings and brainstorm sessions more creative and effective. Use natural language to ask Copilot to generate ideas, organize ideas into themes, create designs that bring ideas to life and summarize whiteboard content.*
OneNote	Draft with Copilot	*Use prompts to draft plans, generate ideas, create lists, and organize information to help you easily find what you need.*
Microsoft Excel	Copilot only works on tables	*Analyse data and get insights: Copilot can perform OLAP operations, analyse data from a given table or worksheet, provide insights, create charts and pivot tables based on the data, summarize, aggregate, and answer questions about the data. You can ask for specific insights or a general request for analysis.* *Edit the document: Copilot can perform Excel commands, including operations related to formatting, conditional formatting, sorting, filtering, clearing formatting or content, finding and replacing, and modifying table structure such as inserting or deleting rows or columns, and adding or removing headers or total rows.* *Add formula columns: Copilot can perform calculations using formulas to create new columns in a table. These calculations can involve data, string, or number processing, as well as conditional logic or lookups. This feature can be used to process data in a table, produce information based on the table columns, or add new columns.*

What about Microsoft Graphs?

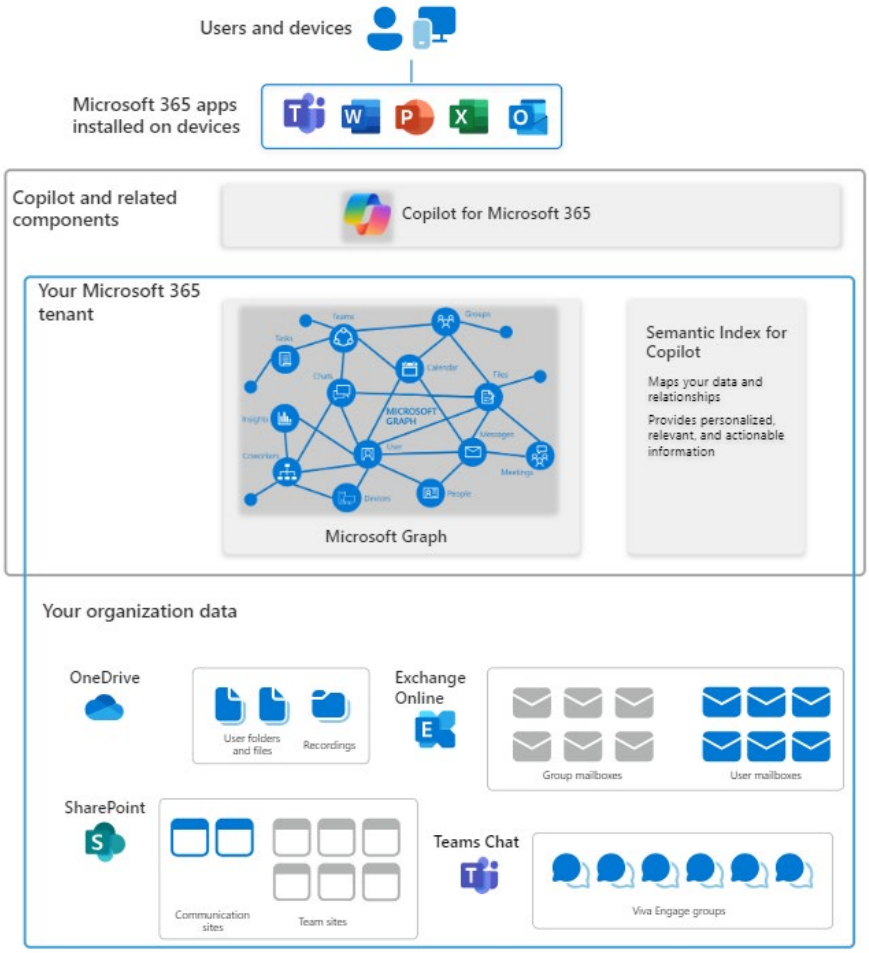
Copilot uses language models which are capable of parsing text to translate user own words about what they're looking for. And it is connected with the **Microsoft Graph**, so Copilot can use data in user calendar, emails, chats, documents, and more to give personalised responses.

Microsoft Graph is the gateway to data and intelligence in Microsoft 365. It provides a unified programmability model that users can use to access the tremendous amount of data in Microsoft 365, Windows, and Enterprise Mobility + Security.

It includes information about the relationships between users, activities, and ELA's data. The Microsoft Graph API brings more context from customer signals into the prompt, such as information from emails, chats, documents, and meetings.

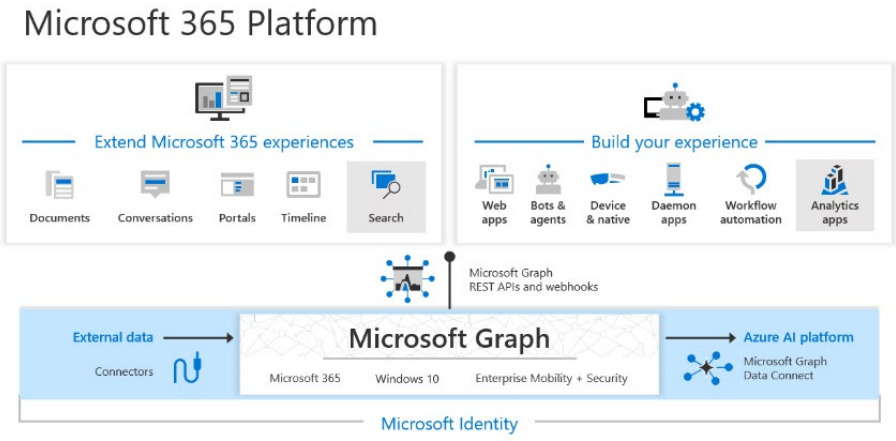


Copilot logical architecture



Explanation:

- User devices in the ELA have Microsoft 365 apps installed from which users can initiate Copilot prompts
- Copilot components include:
  - The **Copilot service**, which orchestrates the responses to user prompts
  - A **Semantic Index** for the data in your Microsoft 365 tenant
  - An instance of the **Microsoft Graph** for the data of user's Microsoft 365 tenant
- Microsoft 365 tenant that contains your organisation's data



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
Contractual clauses related to personal data protection in place.

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

      Automatic processing of the personal data to monitor the operations of the system (in order to comply with the ELA security policy, and the terms of use of the several LLM models), and the personal data that users chose to input to be processed by the LLM models.

2. ☒ Manual processing
   a. ☒ Word documents
   b. ☒ Excel sheet
   c. ☒ Any other, specify

      Other Microsoft Applications, such as PowerPoint, OneNote etc and other applications such as Adobe Acrobat

Description

Information detailed above under 'How Copilot works?'

1.2.4 Storage medium

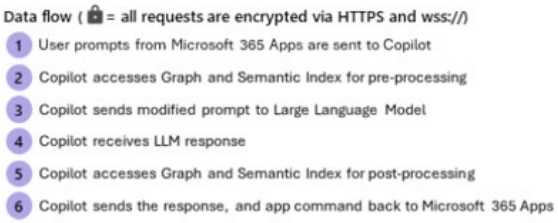
1. ☒ Paper
2. ☒ Electronic
   a. ☒ Digital (MS documents (Word, excel, Powerpoint), Adobe pdf, Audiovisual/multimedia assets, Image files (.JPEG, .PNG, etc.))
   b. ☒ Databases
   c. ☐ Servers
   d. ☒ Cloud

3. ☒ External contractor premises
4. ☐ Others, specify

1.2.5 Comments on the processing of the data

The processing of personal data depends on the app used. Explained in detail above under the description.

Summary:



1.3 DATA SUBJECTS AND DATA CATEGORIES

1.3.1 Data subjects' categories

1. Internal to organisation	ELA Staff
2. External to organisation	Partner contacts from EU Institutions and bodies External contractors Citizens

1.3.2 Data categories/fields

Indicate the categories of data that will be processed

ELA Staff:

- Entra ID: username and password used to authenticate the user and validate the license eligibility.
- Personal data contained in the Microsoft Graph (user's context and content such as emails, files, meetings, chats, calendars and contacts). Only data that each user has existing access to, based on, access controls.
  The information saved in the users' computer is outside the scope of Microsoft Copilot.

- User interactions with Copilot, including prompt and responses, for monitoring purposes to comply with the terms of use of the several LLM models;
- Optionally, feedback sent by users related to the way they use the system for their work and their experience with it including success cases, failures, hallucinations or biases, etc.).

External (Partner contacts, External contractors and citizens)
'Partner contacts' are all staff of European institutions and bodies, members of the ELA Management Board and Stakeholder Groups and Working Groups.
'External contractors'
'Citizens'

Categories of data (mainly related to e-mails, events or procurement):
Partner contacts: Name, Surname, Role/Position, Institution, Unit, Email messages (subject, date, documents attached and recipients). In particular, this process is covered by the Records:

- '**DPR-ELA-2022-0011 Email system at the European Labour Authority (ELA)**'
- 'DPR-ELA-2022-0051 ELA Organisation and management of ELA Management Board meetings',
- 'DPR-ELA-2022-0052 ELA Organisation, management and activities of ELA Stakeholder Group'.

External contractors: in addition to the ones mentioned in the previous categories, financial data and information for the evaluation of selection criteria or eligibility criteria. In particular, this process is

covered by Record "***DPR-ELA- 2022-0003 Managing award procedures for procurement and the execution of contracts***".
Citizens: Name, Surname, Contact details (address, email, telephone), company/organisation, role/position. In particular, this process is covered by the Records:

- '**DPR-ELA-2022-0023 ELA live, hybrid and digital events, seminars, workshops, conferences, meetings, open/celebration/information days and visits**',
- '**DPR-ELA-2022-0024 ELA Contact lists & network partners databases'**
- '**DPR-ELA-2022-0006 External complaints in the field of European labour mobility'**
- '**DPR-ELA-2022-004: Monitoring, investigative, auditing and consultative activities of ELA Data Protection Officer'**.

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:
According to ED Decision/Staff guidelines on the use of AI, documents labelled with "SENSITIVE NON CLASSIFIED (DKE)" will not be subject of Artificial Intelligence.

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** ☐
Description: According to ED Decision/Staff guidelines on the use of AI, documents labelled with "SENSITIVE NON CLASSIFIED (DKE)" will not be subject of Artificial Intelligence.	

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 Staff data	*Identification data is stored for as long as the user account is active. For Office 365, data will be retained for as long as there is a contractual relation with M365 Office. Once a contract expires, information is retained for 30 days for the purposes of collection or possible renewal. After this period, information is deleted. At all times during the term of the customer's subscription, the customer will have the ability to access, extract, and delete Customer Data stored in the service.*
Content data	*Up to 180 days upon expiration/termination of the subscription*
Data related to partner contacts	*As referred in the concerned records, 30 days after the deletion of the user or 30 days after the departure of the user (e-mail system),*
Data related to external contractors	*As declared in the concerned record, 5 years for unsuccessful tenderers, unsuccessful candidates, candidates to a Call for Expressions of Interest or 10 years for successful tenderer.*
Data related to citizens	*As declared in the concerned records, 3 years (external complaints), 5 years (activities related to the Data Protection Officer) as long as the data subject collaborates with ELA in his/her position based on the relevant appointment or contract (contact lists) or as long as ELA continues to work in support of labour mobility and social security systems, or until the data subject requests to be deleted from the list (contact list).*

Description
The specific retention period is defined in the relevant record. Records could be found under the ELA Register of personal data processing activities: **here**.

1.5 RECIPIENTS

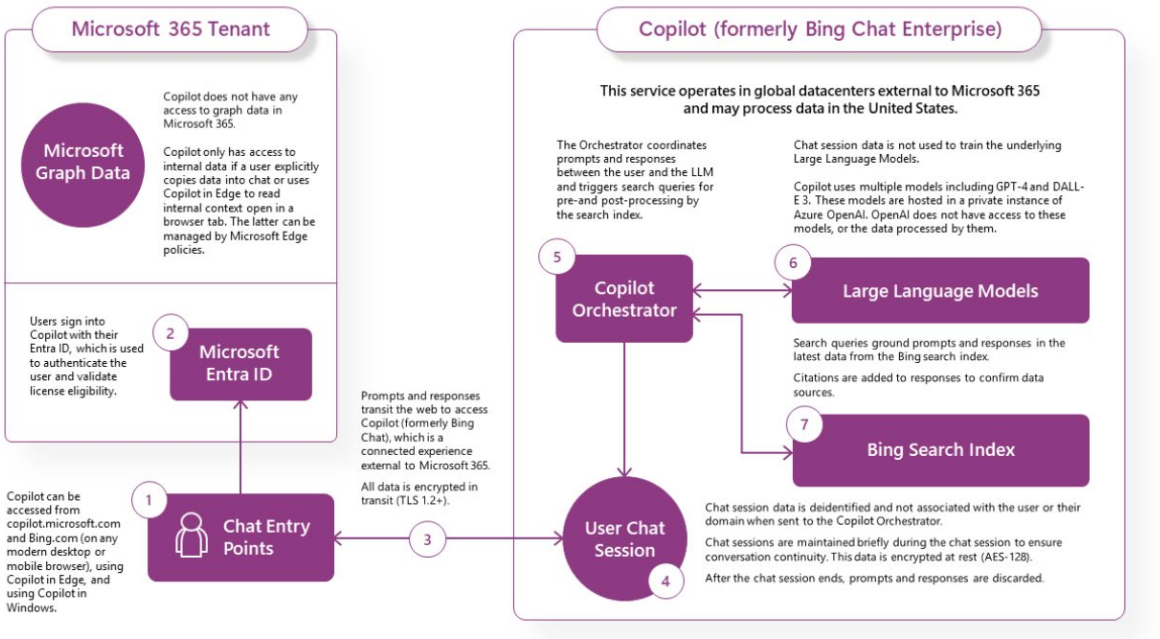
Origin of the recipients of the data	
1. ☒ Within the EU organization	ELA Staff
2. ☒ Outside the EU organization	According to Microsoft 365 Copilot terms and services and privacy setting, the information will not be used outside the organisation.

Categories of the data recipients
1. ☒ A natural or legal person 2. ☐ Public authority 3. ☐ Agency 4. ☐ Any other third party, specify Specify who has access to which parts of the data:

Description
According to the Copilot commercial data protection, user and business data is protected and will not leak outside the organization. M365 guarantees:

- that chat data is not saved,
- Microsoft has no eyes-on access to it, and
- it is not used to train the models.

Copilot is designed to protect this information, as illustrated here:



This is how commercial data protection works in Copilot:

Copilot uses **Microsoft Entra ID** (formerly known as Azure Active Directory) for authentication and only allows users to access Copilot with commercial data protection using their work account.

An Entra ID user's tenant and user information is removed from chat data at the start of a chat session.
This information is only used to determine if the user is eligible for commercial data protection. Search queries triggered by prompts from an Entra ID user aren't linked to users or organizations by Bing.

- Microsoft doesn't retain prompts or responses from Entra ID users when using Copilot.
- Prompts and responses are maintained for a short caching period for runtime purposes.
- After the browser is closed, the chat topic is reset, or the session times out, Microsoft discards prompts and responses.
- Chat data sent to and from Copilot with commercial data protection is encrypted in transit and at rest during the chat session.
- Microsoft has no 'eyes-on' access to it.
- Because Microsoft doesn't retain prompts and responses, they can't be used as part of a training set for the underlying large language model.

Advertising shown to Entra ID users isn't targeted based on workplace identity or chat history.
As commercial data protection is enabled, Copilot doesn't support the chat history feature. It doesn't retain chat prompts or responses.

It also offers no usage reporting or auditing capabilities to organizations. Copilot users may be subject to other methods of monitoring available to IT admins in their organization such as internal logging, device or network logs, etc., on their company network or devices.

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. Legal base for the data transfer

☒ Transfer on the basis of the European Commission's **adequacy decision** *(Article 47)*

☐ Transfer subject to **appropriate safeguards** *(Article 48.2 and .3),* specify:

2. (a) ☐ A legally binding and enforceable instrument between public authorities or bodies.

Standard data protection clauses, adopted by
(b) ☐ the Commission, or
(c) ☐ the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2).

(d) ☐ Binding corporate rules, ☐ Codes of conduct , ☐ 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:

☐ 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.

☐ Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

☐ Transfer based on an i**nternational agreement** *(Article 49),* 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).

Description
EU Data boundary – EU data residency (*EU data residency refers to the legal requirement and practice of storing and processing digital data within the boundaries of the European Union*).

Copilot for Microsoft 365 is upholding data residency commitments as outlined in the Microsoft Product Terms and Data Protection Addendum.

Encryption at rest and in transit. Only encrypted/pseudonymised data will be transferred, if any transfer is made.
Main Subprocessors are located in the EU/EEA area.

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 ☒ (SharePoint on personal data protection)
- External website ☒(URL: https://www.ela.europa.eu/en/privacy-policy)

☒ Other form of publication, specify
The specific Privacy Statement of the processing of personal data concerned will apply.

☒ 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 at the European Labour Authority.

1.8 SECURITY MEASURES

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

Description:
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.