European Labour Authority

DATA PROTECTION OFFICER

RECORD OF PROCESSING OPERATIONS ON PERSONAL DATA

DPR-ELA-2022-0012 ELA Microsoft Office 365 environment

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

1.1 GENERAL INFORMATION

Record reference	DPR-ELA-2022-0012
Title of the processing operation	ELA Microsoft Office 365 environment
Controller entity	European Labour Authority, Resources Unit, Information and Communication Technologies and Facilities (ELA ICT Team)
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 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

Microsoft Office 365 (M365) is a cloud based package of applications (Word, Excel, PowerPoint, Outlook, OneNote or OneDrive) provided by the European Labour Authority (ELA) to all ELA staff with the aim to offer more flexibility and improve communications, collaborations and the availability of resources.

The processing of personal data is carried out under the responsibility of the Head of Resources Unit at the European Labour Authority, acting as delegated ELA data controller. However, for each specific application/service, the organizing Unit/Sector/Team will act as Controller.

The processing of personal data is carried out under the responsibility of the European Labour Authority (ELA) and Microsoft as Processor.

Due to the outbreak of the coronavirus COVID-19 virus, the Authority extended the use of Microsoft Office 365, and in particular Microsoft Teams to organise virtual meetings and teleconferences with internal staff and external stakeholders.

The services of Microsoft Office 365 available to ELA staff are the following:

Microsoft Word: MS Word is a word processor used to write any documents such as letters, reports or even posters.

Microsoft Excel: A spreadsheet and charting application used for making simple lists and quick calculations to complex reporting, data crunching, pivot tables or what-if analysis.

Microsoft PowerPoint: MS PowerPoint is mainly used for slideshows with animations but can also be used as a graphic design tool or even basic animator.

Microsoft Outlook:

Module 1 - Mail: Email tool allowing the user to organise emails and folders, flag for later, manage multiple email accounts or add signatures.
Module 2 - Calendar: Manage appointments (only the user) and meetings (user and participants). Share individual and shared calendar.
Module 3 - People (Contact): Displays all the contacts in the organisation and any individual created by the user.
Module 4 - To do (Tasks): Helps users manage tasks, or task lists, with the ability to sync it with the planner application.

Microsoft OneNote: A free form note tacking application organized by Notebooks, sections and pages.

Microsoft Delve: Delve is a personal profile in Office365 where the users can upload their profile picture, description and other information like past projects, skills, schools and more. Delve also suggests content the users might be interested in based on what they have worked on before and what people close to users, in the system, are working on.

Delve does not change any permission, so the users will only see documents that they already have access to. Other users will not see your private documents either.

Microsoft Visio: MS Visio is a diagramming and vector graphics application used for workflow design, engineering diagrams or floor plans.

Microsoft Access: A database building Application, that can be used to create and manage forms, or relational databases.

Microsoft Bookings: Appointment / reservation Tool. Can be used to allow others to book appointments with the user.

Microsoft Sway: MS Sway is a presentation program that can be seen as a friendly alternative to PowerPoint providing a more fluid and light way to present information.

Microsoft Project: Premium project application. It provides professional project management and resource planning and is usually used by project managers.

Microsoft Planner: MS Planner is a project management Application used by teams.

Microsoft Publisher: MS PowerPoint is a publishing design tool. It can be used for posters, pamphlets, newsletters or business cards.

Microsoft Lists: The Lists Application is useful for tracking and organising information whether that is inventory and assets, a big picture project overview, newcomers onboarding or event planning.

Microsoft SharePoint Online: SharePoint Online is Microsoft's intranet and Team file management portal. SharePoint is the base for Microsoft Teams and Communication sites (meant for organising and sharing information, news, links for internal teams or the whole organisation. E.g. ICT communication site)

SharePoint is also the file sharing repository for groups and teams using Office365 offering various permission options, folder setups and the ability to organise files by tags, external and internal sharing features and advance protection and security options.

A specific record covers this process of personal data at the European Labour Authority (Record DPR-ELA-2022-0032 ELA Sharepoint Spaces)

Microsoft OneDrive for Business: MS OneDrive and OneDrive for Business is the personal file storage and sharing tool in Microsoft and Office365. Each ELA user has 1TB (1'000 GB) of personal storage available.

OneDrive is also the name of the sync tool used to keep and access SharePoint and OneDrive files on the users's computer and mobile device including for offline use.

A secific record covers this process of personal data at the European Labour Authority (Record DPR-ELA-2022-0043 Microsoft OneDrive for Business – Personal file storage at the European Labour Authority)

Microsoft Yammer: Yammer is an online community forum and internal communications platform where users can create groups of likeminded individuals and share updates, ask questions, provide answers and keep in contact with people they otherwise may not interact with.

Yammer is a tool that is more about information sharing and community building.

Microsoft Stream: Microsoft Stream is the online video portal in Office365. It lets users upload and manage videos, transcripts and channels as well as respond to videos with reactions and comments.

Users can also use Streams for simple video editing and screen recording. Stream is the tool used for creating meeting recording in Microsoft Teams and for hosting live events on both Teams and Yammer.

MS Teams: is a cloud-based application included as part of Office 365 that is provided to users with the aim to offer more flexibility and improve communications and collaboration between stakeholders and the Authority. The core capabilities in Microsoft Teams include business messaging, calling, video meetings and file sharing. Microsoft Teams also connects to meeting rooms and devices.

Microsoft MyAnalytics: MyAnalytics is a time and productivity tracking tool that will send the users information on how much time they have spent on certain tasks as well as suggestion for being more productive. It also shows the users who they work with, how well they are focusing and guidance on overall well-being.

Microsoft Forms: Microsoft Forms is a tool to make quizzes, questionnaires and surveys. With it, users can easily create, collaborate and share forms both internally and externally.

Microsoft Whiteboard: Whiteboard is a big white canvas allowing users to draw, type, and add sticky notes for taking notes and brainstorming. Users can create individual or team Whiteboards. Every Microsoft Teams meeting comes with its own whiteboard that will be saved, allowing the participant to go back to it once the meeting ended.

Microsoft Power BI: To create actionable, dynamic, and engaging data dashboards that can be shared with others.

Viva Insights: To improve users' productivity and wellbeing.

The personal data is collected and stored in Microsoft's Cloud servers with the purpose of providing the abovementioned services.

1.2.2 Processing for further purposes

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

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

3. ☒ Any other mode, specify

Description

ELA as Controller:
The purpose(s) of processing data using Office 365 is determined by ELA that implements, configures, and uses it.
As specified by the Online Services Terms and Data Protection Addendum, Microsoft, as a data processor, processes Customer Data to provide Customer the Online Services in accordance with Customer's documented instructions.

Microsoft as Controller

As detailed in the standard Online Services Terms and Data Protection Addendum, Microsoft also uses Personal Data to support a limited set of legitimate business operations consisting of:
(1) billing and account management;
(2) compensation (for example, calculating employee commissions and partner incentives);
(3) internal reporting and modeling (for example, forecasting, revenue, capacity planning, product strategy);
(4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products;
(5) improving the core functionality of accessibility, privacy, or energy efficiency; and

(6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Customer Data outlined in the Online Service Terms).

Microsoft is controller of the processing of personal data to support these specific legitimate business operations. Generally, Microsoft aggregates Personal Data before using it for its legitimate business operations, removing Microsoft's ability to identify specific individuals, and uses personal data in the least identifiable form that will support processing necessary for legitimate business operations.

Microsoft will not use Customer Data or information derived from it for profiling or for advertising or similar commercial purposes.

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:

Search history: The personal search history in Microsoft Search isn't shared with ELA or with Microsoft. If many people in ELA search for the same thing, Microsoft Search tells the search admin that the search is popular, but not who has searched for it. The search admin can use this information to define resources that are reliable results for popular queries. This makes search better for users and ELA.

Users' search history helps them quickly get back to things they've found before. It contains their searches in Outlook, SharePoint Online, and Office.com. Users can review their search history at any time by downloading it.

<u>Licenses assigned to ELA users</u>

Below are the licenses currently assigned to ELA staff through an unique ID. If users need help accessing a product or service, this information may be helpful for ELA admin, ICT department, or Microsoft Support. The use of the service(s) is subject to the agreements ELA has with Microsoft.

Office 365 E5		
Viva Learning Seeded	Common Data Service for Teams	Microsoft Data Investigations
Nucleus	Project for Office (Plan E5)	Microsoft Customer Key
Information Protection and Governance Analytics – Standard	Microsoft Excel Advanced Analytics	Microsoft Communications DLP
Data Classification in Microsoft 365	Microsoft 365 Defender	RETIRED - Microsoft Communications Compliance
Microsoft 365 Communication Compliance	Common Data Service	Microsoft 365 Advanced Auditing
Graph Connectors Search with Index	Microsoft Bookings	Information Barriers
Information Protection and Governance Analytics - Premium	Microsoft Records Management	Microsoft Kaizala Pro
Power Virtual Agents for Office 365	Microsoft Information Governance	Microsoft Search
Premium Encryption in Office 365	Information Protection for Office 365 - Premium	To-Do (Plan 3)

Whiteboard (Plan 3)	Information Protection for Office 365 - Standard	Microsoft Forms (Plan E5)
Insights by MyAnalytics	Office 365 Privileged Access Management	Microsoft Stream for Office 365 E5
Microsoft Defender for Office 365 (Plan 2)	Power Apps for Office 365 (Plan 3)	Office 365 Cloud App Security
Microsoft StaffHub	Microsoft Teams	Office 365 Advanced eDiscovery
Sway	Microsoft Defender for Office 365 (Plan 1)	Microsoft 365 Phone System
Power Automate for Office 365	Customer Lockbox	Microsoft MyAnalytics (Full)
Microsoft 365 Audio Conferencing	Power BI Pro	Azure Rights Management
Yammer Enterprise	Microsoft Planner	The latest desktop version of Office
Skype for Business Online (Plan 2)	Exchange Online (Plan 2)	SharePoint (Plan 2)
Office for the Web		

Enterprise Mobility + Security E5		
Exchange Foundation	Microsoft Azure Multi-Factor Authentication	Microsoft Defender for Identity
Azure Active Directory Premium P1	Microsoft Defender for Cloud Apps	Azure Information Protection Premium P1
Azure Information Protection Premium P2	Azure Rights Management	Microsoft Intune
Azure Active Directory Premium P2		

Microsoft 365 E5 Suite features		
Information Protection and Governance Analytics - Premium	Microsoft Endpoint DLP	Office 365 SafeDocs
Microsoft ML-Based Classification	Microsoft Insider Risk Management	

Windows 10/11 Enterprise E5		
PAD for Windows	Windows Update for Business Deployment Service	Universal Print
Dataverse for PAD	Exchange Foundation	

Microsoft Defender for Endpoint		
Windows 10/11 Enterprise	Microsoft Defender for Endpoint P2	MDE_SecurityManagement
Exchange Foundation	Microsoft Defender for Endpoint	

1.2.5 Comments on the processing of the data

In accordance with ELA security rules, the information will be classified on:

Public available: information that is published or ready to be published (e.g. information on Europa website, Official Journal of the EU)

ELA Use : information that is not for public use, only for internal ELA staff but is not considered sensitive (e.g. information on ELA SharePoint, other collaborative spaces, meeting agendas and minutes)

Sensitive-Non Classified Information (SNC): information that ELA must protect due to legal obligations or because of its sensitivity (e.g.information about contracts and procurement procedures, business/financial data, sensitive personal data.

Staff Matters: Double Key Encryption will be by default to all documents markes with this label.
To send encrypted email, ELA staff could choose the following options:

- Encrypt with S/MIME
- Encrypt-Only
- Do not Forward

On the other hand, Microsoft distinguishes the following data categories of personal data processed:

Customer Data: This is all data, including text, sound, video, or image files and software, that customers provide to Microsoft or that is provided on customers' behalf through their use of Microsoft online services. It includes data that customers upload for storage or processing, as well as customizations.

Examples of Customer Data processed in Office 365 include email content in Exchange Online, and documents or files stored in SharePoint Online or OneDrive for Business.

Service-generated Data (SGD): This is data that is generated or derived by Microsoft through operation of the service, such as use or performance data. Most of these data contain pseudonymous identifiers generated by Microsoft.

Diagnostic Data: This data is collected or obtained by Microsoft from software that is locally installed by Customer in connection with the Online Service and may also be referred to as telemetry. This data is commonly identified by attributes of the locally installed software or the machine that runs that software.

Support Data: This is data provided to Microsoft by or on behalf of Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain technical support for Online Services.

Customer Data, System-generated Log Data, and Support Data do not include administrator and billing data, such as customer administrator contact information, subscription information, and payment data, which Microsoft collects and processes in its capacity as a data controller and which is outside the scope of this document.

Microsoft uses the data to provide users with rich, interactive experiences. In particular, they use data to:

- Provide their products, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions the users request.
- Improve and develop their products.
- Personalize their products and make recommendations.
- Advertise and market to users, which includes sending promotional communications, targeting advertising, and presenting relevant offers.
- Operate their business, which includes analyzing M365 performance, meeting their legal obligations, developing their workforce, and doing research.

In carrying out these purposes, Microsoft combines data they collect from different contexts (for example, from clients's use of two Microsoft products) or obtain from third parties to give users a more seamless, consistent, and personalized experience, to make informed business decisions, and for other legitimate purposes.

The processing of personal data for these purposes includes both automated and manual (human) methods of processing. Their automated methods often are related to and supported by their manual methods. For example, their automated methods include artificial intelligence (AI), which is a set of technologies that enable computers to perceive, learn, reason, and assist in decision-making to solve problems in ways that are similar to what people do. To build, train, and improve the accuracy of their automated methods of processing (including AI), Microsoft manually reviews some of the predictions and inferences produced by the automated methods against the underlying data from which the predictions and inferences were made. For example, they manually review short snippets of voice data that they have taken steps to de-identify to improve their speech recognition technologies. This manual review may be conducted by Microsoft employees or vendors who are working on Microsoft's behalf.

The operation of these services requires the processing of data categories by Microsoft, for the following specific purposes: **Providing the Office 365 service to ELA:** Identification data, Content data, SGD **Technical support to IT teams for issues with Office 365:** Identification data, SGD **Prevention, detection and resolution of security events (e.g. cyber-attack**): Identification data, SGD **Assistance to data subjects in exercising their rights in relation to data processed within Office 365**: Identification data, SGD

1.3 DATA SUBJECTS AND DATA CATEGORIES

1.3.1 Data subjects' categories

1. Internal to organisation	☒ Yes All ELA Staff including the Executive Director
2. External to organisation	☒ Yes Any natural person whose personal data is being processed using M365 (e.g. a participant in a Teams call; an email recipient; a participant in a survey).

1.3.2 Data categories/fields

Indicate the categories of data that will be processed:

Identification data: e.g. title, name, email address, birthday, profile photo (if applicable);
Contact details: e.g. office telephone number, mobile and home telephone number (optional);
Personal characteristics: e.g. gender, hobbies and interests, skills and expertise, school and education (all optional);
Professional data: e.g. current position and unit, line manager, current responsibilities / projects involved;
Contacts data: Third party contacts are processed in Outlook and MS Teams
Electronic communications data: e.g. IP addresses, cookies and connection data;
User patterns: e.g. media utilisation, methods of communication;
Content data: any data content generated and controlled by ELA staff members, including chat messages (one-to-one as well as group messages) and any other personal information, voluntarily posted on the platform;
Multimedia: e.g. image and sound recording;
Support/Feedback data: information related to troubleshooting tickets or feedback submission to Microsoft; and
Diagnostic and service data: diagnostic data related to service usage.

In some specific procedures special categories of personal data may be processed by ELA. A specific legal basis to lawfully collect and process those type of data will be declared through the relevant record and privacy statement covering the procession operation.

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 probhibited 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.

Description:
In some specific procedures special categories of personal data may be processed by ELA. A specific legal basis to lawfully collect and process those type of data will be declared through the relevant record and privacy statement covering the procession 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** ☐ **Yes** ☒
Description: For some specific processes of personal data, such as the process on selection and recruitment of staff, data related to criminal convictions and offences will be collected. This process is specifically covered by Record "*DPR-ELA-2022-0010 Selection and recruitment of staff, interimaires, Seconded National Experts(SNEs) National Liaison Officers (NLOs), and trainees*".	

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:

ELA as Controller:

In ordert to be able to perform its activities, ELA collects, process and manages personal data. All processing activities performed by ELA are publicly available and described in the Register of the European Labour Authority at ELA main website (https://www.ela.europa.eu/en/privacy-policy)

For each process, a specific record describes the operations performed and contains specific information, according to Article 31 of Regulation (EU)2018/1725:

- name and contact details of the controller in ELA, the data protection officer and, where applicable, the processor and the joint controller;
- purpose(s) of the processing;
- a description of the data categories of data subjects and of the categories of personal data;
- the categories of recipients to whom personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organisation and the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures referred to in Article 33 of Regulation (EU)20181725.

Therefore, the specific record covering a particular process of personal data in ELA applies.

Microsoft as processor:

Data category	**Retention period**
Customer 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 90 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.
User patterns:	Up to five years
Content data:	Up to 180 days upon expiration/termination of the subscription
Multimedia:	Up to 180 days upon expiration/termination of the subscription
Support/Feedback data:	Up to 180 days upon expiration/termination of the subscription

Diagnostic and service data	Up to 180 days upon expiration/termination of the subscription
Log files	Up to six months

Description

Customer Data:

As set out in the Data Protection Terms in the Online Services Terms, Microsoft will retain Customer Data for the duration of the customer's right to use the service and until all Customer Data is deleted or returned in accordance with the customer's instructions or the terms of the Online Services Terms.

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, subject in some cases to specific product functionality intended to mitigate the risk of inadvertent deletion (for example, Exchange recovered items folder), as further described in product documentation.

Except for free trials and LinkedIn services, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of the customer's subscription so that the customer may extract the data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the Customer Data.

Service-generated Data:

This data is retained for a default period of up to 180 days from collection, subject to longer retention periods where required for security of the services or to meet legal or regulatory obligations.

For further information about service capability that enables the customer to delete personal data maintained in the service at any time, see the Office 365 Data Subject Requests Guide.

Microsoft remains a processor for Online Services data upon expiration or termination of the subscription, i.e., during the 90-day retention period and subsequent period, up to an additional 90 days, to delete Content Data and Personal Data and during any Extended Term. Microsoft will at the choice of the user, delete or return all the Personal Data to the user after the end of the provision of services relating to the processing. It will delete existing copies unless Union or Member State law requires storage of the Personal Data. To the extent Microsoft engages in any processing of Personal Data during the Extended Term, Microsoft will remain a processor.

1.5 RECIPIENTS

Origin of the recipients of the data	
1. ☒ Within the EU organization	ELA staff in a need to know basis
2. ☒ Outside the EU organization	External processors Other European Union Institutions and bodies Citizens

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

ELA as Controller:

For each specific process of personal data, the responsible Unit/Sector/Team will act as Controller and describe the process in a specific record where the data recipients will be explained in detail.

All recipients may have access to all parts of the data, on a need-to-know basis, to the extent that the data are adequate, relevant and limited to what is necessary in relation to the purpose of management and execution of the particular processing operation performed by ELA in collaboration/supported by external entities. The specific data may be disclosed to recipients to the extent that such disclosure is necessary for the performance by ELA of a task in the public interest or in the exercise of official activity vested in ELA, or it is necessary for compliance with a legal obligation.

Microsoft as processor:
In principle the majority of the service operations are automated in order to reduce the need for human access. Microsoft engineers and support staff do not have access to customer data by default, and are only granted access in case it is required for maintenance purposes.

That said, information may be stored in the US. In addition, information may be made available to subcontractors in other countries, depending on the requirements for maintenance or support and the availability of this expertise.
Nevertheless, if access is granted, it is always temporarily and only to the information required for the specific maintenance or support procedure being carried out.
The following safeguards are implemented:

- In all transfers, Microsoft uses EU Standard contract clauses for the transfer.
- In the specific case of transfers to the US, Microsoft is certified to the EU-US Privacy Shield Framework.
- Microsoft requires subprocessors to join the Microsoft Supplier Security and Privacy Assurance Program. This program is designed to standardize and strengthen data handling practices, and to ensure supplier business processes and systems are consistent with those of Microsoft.

It is also possible to use the logs in the privacy console to verify when information has been shared with Microsoft staff or subprocessors.

Subprocessors:

Microsoft's GDPR Terms reflect the commitments required of processors in Article 28. Article 28 requires that processors commit to:

- Only use subprocessors with the consent of the controller and remain liable for subprocessors.
- Process personal data only on instructions from the controller, including with regard to transfers.
- Ensure that persons who process personal data are committed to confidentiality.
- Implement appropriate technical and organizational measures to ensure a level of personal data security appropriate to the risk.
- Assist controllers in their obligations to respond to data subjects' requests to exercise their GDPR rights.
- Meet the breach notification and assistance requirements.
- Assist controllers with data protection impact assessments and consultation with supervisory authorities.
- Delete or return personal data at the end of provision of services.
- Support the controller with evidence of compliance with the GDPR.

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,

Country(ies) to which the data is transferred	EU Data Boundary. Subporcessors in several countries as specified in relevant contractual information.

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).

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

ELA as Controller:

Third countries/International Organisations with which ELA collaborates related with ELA activities.

If personal data are published on a publicly available Internet website, this means that they are accessible worldwide.

For each specific process of personal data, the responsible Unit/Sector/Team will act as Controller and describe the process in a specific record where the data recipients will be ex¡plained in detail

Microsoft as Processor:

Microsoft has long used the Standard Contractual Clauses (also known as the Model Clauses) as a basis for transfer of data for its enterprise online services. The Standard Contractual Clauses are standard terms provided by the European Commission that can be used to transfer data outside the European Economic Area in a compliant manner. Microsoft has incorporated the Standard Contractual Clauses into all of our Volume Licensing agreements via the Online Services Terms. For personal data from the European Economic Area, Switzerland, and the United Kingdom, Microsoft will ensure that transfers of personal data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses for processors and other model contracts, Microsoft continues to abide by the terms of the Privacy Shield framework but will no longer rely on it as a basis for the transfer of personal data from the EU/EEA to the United States.

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

Privacy Statement for Microsoft Office, Word and Power Point

Privacy Statement for Teams

Privacy Statement for VivaSight

Privacy Statement on the use fo Microsoft 365

☒ 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:

ELA as Controller

A guidance on data subjects' rights is available at ELA main website.
Privacy Statements for specific applications will be prepared in order to increase transparency and clarity to the process.

Microsoft as processor:
The Data Protection Addendum, Microsoft commits to respond to requests for the management of personal data, including data access, modification, deletion, etc.

When operating as a processor, Microsoft makes available to customers (data controllers) the personal data of its data subjects and the ability to fulfill data subject requests when they exercise their rights under the GDPR. We do so in a manner consistent with the functionality of the product and our role as a processor. If we receive a request from the customer's data subjects to exercise one or more of its rights under the GDPR, we redirect the data subject to make its request directly to the data controller. The Office 365 Data Subject Requests Guide provides a description to the data controller on how to support data subject rights using the capabilities in Office 365.

Requests from a data subject to exercise rights under the GDPR for personal data processed to support the legitimate business processes should be directed to Microsoft, as clarified in the Microsoft Privacy Statement.

Microsoft generally aggregates personal before using it for our legitimate business operations and is not in a position to identify personal data for a specific individual in the aggregate. This significantly reduces the privacy risk to the individual. Where Microsoft is not in a position to identify the individual, it cannot support data subject rights for access, erasure, portability, or the restriction or objection of processing.

1.8 SECURITY MEASURES

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

Description:

ELA as Controller
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.

Microsoft as processor
The key risks to the rights and freedoms of data subjects from the use of Office 365 will be a function of how and in what context the data controller implements, configures, and uses it.

Microsoft takes measures such as the anonymization or aggregation of personal data used by Microsoft to support legitimate business operations to support provision of the services, minimizing the risk of such processing to data subjects that use the service.

However, as with any service, personal data held in the service may be at risk of unauthorized access or inadvertent disclosure. Measures Microsoft takes to address such risks are the following:
Microsoft is committed to helping protect the security of Customer's information. In compliance with the provisions of Article 32 of the GDPR, Microsoft has implemented and will maintain and follow

appropriate technical and organizational measures intended to protect Customer Data and Support Data against accidental, unauthorized, or unlawful access, disclosure, alteration, loss, or destruction.

Further, Microsoft complies with all other GDPR obligations that apply to data processors, including but not limited to, data protection impact assessments and record keeping.

Where Microsoft processes personal data for its legitimate business operations, it complies with GDPR obligations that apply to data controllers.