RECORD OF PERSONAL DATA PROCESSING ACTIVITY

According to Article 31 of Regulation (EU) 2018/1725[1]

IT-11 Videoconferencing, Communication and Collaboration with Microsoft 365

EIOPA-DPO-22-01

I. GENERAL INFORMATION

1) Introduction
EIOPA, as a European Authority, is committed to protect individuals with regard to the processing of their personal data in accordance with Regulation (EU) No 2018/1725 (further referred as the Regulation)[2].

2) Contact Details of Data Controller(s)
Name: Fausto Parente, Executive Director
Email Address: fausto.parente@eiopa.europa.eu
Address: Westhafenplatz 1, 60327 Frankfurt am Main, Germany

3) Contact Details of the Data Protection Officer
Name: Eleni Karatza
Email Address: dpo@eiopa.europa.eu
Address: Westhafenplatz 1, 60327 Frankfurt am Main, Germany
Date of Consultation: 29 July 2022

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

4) Contact Details of Processor

Who is actually conducting the processing?

EIOPA's Team/Unit responsible for the processing:

IT Unit

Contact: IT-DPC@eiopa.europa.eu

4.bis Contact Details of External Processor(s) / Joint Controller(s)

☒ External processor(s):

- Microsoft Ireland Operations Limited
  Microsoft EU Data Protection Officer
  One Microsoft Place
  South County Business Park
  Leopardstown
  Dublin 18 D18 P521 Ireland
  Telephone: +353 (1) 706-3117
  https://aka.ms/privacyresponse

- A list of Microsoft's current sub-processors is available at https://aka.ms/servicesapprovedsuppliers

☐ Joint controller(s)

☐ N/A

II. DESCRIPTION AND PURPOSE OF THE PROCESSING

5) Description of Processing

This record of personal data processing relates to audio, video and chat communication, collaborative sharing and drafting of documents through Microsoft 365.

Microsoft 365 includes a set of cloud-based services that are provided to users with the aim to offer more flexibility and facilitate communication and collaboration with internal and external stakeholders:

- Communication and collaboration using Microsoft Teams: business messaging, chat, calling, video meetings and file sharing;
- Communication and collaboration using the Microsoft 365 email service;
- Collaboration on documents using Microsoft SharePoint Online;
- Use of integrated Microsoft 365 functionality within these tools.

To manage access to these services, user accounts are processed in Microsoft Azure Active Directory.

EIOPA provides you with the information that follows based on Article 31 of the EUDPR.

Personal data will not be used for any purposes other than the performance of the activities specified above. Otherwise you will be informed accordingly.

6) Purpose (s) of the processing

Why are the personal data being processed?

☒ Staff administration

☒ Relations with external parties

☒ Procurement and accounting

☒ Administration of membership records

☒ Auditing

☒ Information administration

☒ Other:

EIOPA processes your personal data for:

- organising virtual meetings, trainings and presentations (internal and external);
- enabling communication by email;
- allowing drafting, sharing and collaboration on documents.

Personal data will not be used for any purposes other than the performance of the activities specified above. Otherwise you will be informed accordingly.

7) Lawfulness of processing

Article 5 of Regulation (EU) 2018/1725

A. Legal basis justifying the processing:

- EIOPA Regulation;
- Policy and Working Instructions on the Acceptable Use of EIOPA's Information and Communications Technology Resources (soon to be adopted).

B. Processing is necessary:

☒ for the performance of a task carried out in the public interest

☐ for compliance with a legal obligation to which the Controller is subject

☐ for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

☐ in order to protect the vital interests of the data subject or of another natural person

Or

☐ Data subject has given his/her unambiguous, free, specific and informed consent

III. THE DATA SUBJECT'S RIGHTS

8) Information on how to exercise data subject's rights

Data subjects may exercise their data privacy rights provided in Articles 17 to 24 of the Regulation (EU) 1725/2018.

To exercise these rights, please contact: IT-DPC@eiopa.europa.eu or DPO@eiopa.europa.eu.

1. Data subjects have the right to:

- access their personal data, receive a copy of them in a structured and machine-readable format or have them directly transmitted to another controller, as well as request their rectification or update in case they are not accurate;
- request the erasure of their personal data, as well as object to or obtain the restriction of their processing.

Without prejudice to the above, rights might be restricted in accordance with EIOPA's decision on the restriction of data subject's rights (EIOPA-MB-19-056).

2. Data subjects have the right to withdraw their consent to the processing of their personal data at any time, in case such processing is based solely on their consent.

3. For the protection of the data subjects' privacy and security, every reasonable step shall be taken to ensure that their identity is verified before granting access, or rectification, or deletion.

4. Should data subjects wish to access/rectify/delete their personal data, or receive a copy of them/have it transmitted to another controller, or object to/restrict their processing, please contact IT-DPC@eiopa.europa.eu or dpo@eiopa.europa.eu.

5. Any complaint concerning the processing of the data subjects' personal data can be addressed to EIOPA's Data Protection Officer (DPO@eiopa.europa.eu). Alternatively, data subjects can also have at any time recourse to the European Data Protection Supervisor (www.edps.europa.eu).

IV. CATEGORIES OF DATA SUBJECTS & PERSONAL DATA

9) Categories of Data Subjects

☒ EIOPA permanent staff, Temporary or Contract Agents

☒ SNEs or trainees

☒ Visitors to EIOPA:

e.g. members of Board of Supervisors, Management Board, EIOPA Working Group / seminar or event participants having access to EIOPA's Sharepoint environment, being invited to EIOPA virtual meetings, etc.

☒ Providers of good or services

☒ Complainants, correspondents and enquirers

☒ Relatives and associates of data subjects

☒ Other / in particular:

- Every natural person EIOPA staff members might collaborate with or EIOPA might have information on. In particular, in addition to the above:
    - External collaborators, National Competent Authorities (NCAs), EU bodies and authorities communicating with EIOPA staff members;
    - Participants in EIOPA's online meetings, conferences and events;
    - Any person provided with access to shared documents and Microsoft 365 applications enabled by EIOPA;
    - Any person mentioned in a stored and shared document.

10) Categories of personal data

(a) General personal data:

The personal data contains:

Any personal data included in the content uploaded to the Microsoft 365 platform by users / data subjects, such as documents (e.g. Word, Excel documents), multimedia (e.g. video recordings should a meeting be recorded), meeting and conversation chats and voicemail. Such data is stored in Microsoft 365 but not otherwise processed by the service provider. More precisely, the following categories of personal data are being processed:

☒ Personal details

Identification data such as the user's name, email address, phone number, profile picture, profile settings and chosen user name. For better security, EIOPA enforces the use of Azure Multi-Factor Authentication (MFA) using Microsoft Azure services. A valid phone number provided by the user is required by this service in particular.

☒ Education & Training details

☒ Employment details

☒ Financial details

☒ Family, lifestyle and social circumstances

☒ Other:

- So-called "service-generated data" contains information related to the usage of the online services, which are the user IP address, creation time, site URL and user email address. This data is generated by events that are related to user activities in Microsoft 365;

- Call history: a detailed history of the phone calls made, which allows each user to go back and review their own call records;
- Call quality data: details of meetings and call data are available to EIOPA system administrators. This allows the Authority's administrators to diagnose issues related to poor call quality and service usage;
- Support/feedback data: information related to troubleshooting tickets or feedback submission to Microsoft;
- Diagnostic and service data: diagnostic data related to service usage. This personal data allows Microsoft to deliver the service (troubleshoot, secure and update the product and monitor security and performance) as well as perform some internal business operations, such as: determine revenue; develop metrics; determine service usage; and conduct product and capacity planning.

In the context of certain meetings, EIOPA may organise live web streaming and video or audio recording. In such cases, a recording alert is visible and available to all participants. EIOPA will arrange for an opt-out facility for meeting participants who prefer their images are not recorded. Consent from all participants for recording a meeting is required before starting recording.

(b) Special categories of personal data

The personal data reveals:

☒ Racial or ethnic origin, in case of virtual meetings where participants are using their camera.

☐ Political opinions

☐ Religious or philosophical beliefs

☐ Trade union membership

☐ Genetic or Biometric data

☐ Data concerning health, sex life or sexual orientation

Please note that neither EIOPA nor Microsoft can control what participants share during meetings and in conversation chats. EIOPA highly advises that users refrain from using Microsoft Teams and other Microsoft 365 services to disseminate sensitive data, e.g. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data (mental & physical), data concerning a natural person's sex life or sexual orientation, as well as data regarding criminal convictions and offences or related security measures – which either concern themselves or another natural person.

Only in case the data subjects include in the meeting, meeting chat or documents the above-mentioned sensitive information will such data be processed.

Remark:

Personal information may be processed, in particular personal information contained within the content created by individual users or groups of users, in addition to the personal data processed by all Microsoft 365 tools that are covered by this record. For example, this refers to documents, messages or meeting chats exchanged between members of a specific group or team. The decision on which data will be shared using Microsoft 365 remains fully with the respective user. To this extent, special categories of data might be processed.

V. CATEGORIES OF RECIPIENTS & DATA TRANSFERS

11) Recipient(s) of the data
To whom is the data disclosed?

☐ Managers of data subjects

☒ EIOPA staff members

☐ Relatives or others associated with data subjects

☐ Current, past or prospective employers

☐ Healthcare practitioners

☐ Education/training establishments

☐ Financial organisations

☒ External contractors

In particular:

Personal data are accessible on a strict need-to-know basis to:

- EIOPA staff members and external users (see point 9 above) included in Microsoft 365 used for the exchange of information, or who are granted access to the Microsoft 365 service;
- EIOPA meeting organisers and internal and/or external participants. Meeting organisers and participants are recipients of all the contents exchanged during a session;

- Designated EIOPA support and security personnel who have access to host and usage information;
- EIOPA's processors, including Microsoft and Microsoft's processors mentioned above, who are involved in the data processing necessary to provide the service.

12) Data transfer(s)

Is the data transferred outside EIOPA?

☒ Within EIOPA or to other EU Institutions/Agencies/Bodies

- Potentially any EU institution/body with which EIOPA conducts business.

☒ To other recipients within the EU (e.g. NCAs):

- Any organisation or external person conducting business with EIOPA, and to whom EIOPA grants access to its applications or documents, which may contain personal data;
- Microsoft cloud data centres located within the EU.

☒ To third countries

If yes, please specify:

a) the country:

- The data exporter for the transfers is the processor (Microsoft Ireland Operations Ltd) and the data importer Microsoft and other sub-processors that might be located in several third countries. Limited personal data might be transferred to the United States (US) to Microsoft Corp as sub-processor and/or its further sub-processors (see https://aka.ms/servicesapprovedsuppliers);
- In case an organisation or person conducting business with EIOPA is located outside the European Economic Area and is granted access to documents containing personal data, personal data will be transferred to the respective third country;
- In addition, real time audio/video/chat processing might occur in third countries based on host or attendee location.

b) whether suitable safeguards have been adopted:

Adequacy Decision of the European Commission[3] ☐

Standard Contractual Clauses (SCC) ☒

The data exporter has put in place SCCs with the various sub-contractors located in third countries.

Binding Corporate Rules (BCR) ☐

Administrative Arrangements between public Authorities (AA) ☐

☒ To international organisations

Personal data might be sent out to other international organisations with which EIOPA conducts business and to which EIOPA grants access to documents containing personal data.

VI. AUTOMATED DECISION MAKING

13) Automated Decision Making, including profiling

A decision is taken in the context of this processing operation solely on the basis of automated means or profiling:

☐ Yes

☒ No

VII. RETENTION PERIOD & SECURITY MEASURES

14) Retention period

A. How long will the data be retained?

a) Identification data, e.g. guest user email addresses
   - for as long as the user account is active, and
   - for 90 days after deletion of the user account.

b) Content data
   - up to 90 days upon expiration/termination of the subscription by EIOPA

[3] Third countries for which the European Commission has issued adequacy decisions are the following: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

c) Service generated data
   - until the business purposes for which the data was collected or transferred have been fulfilled

B. For further processing envisaged beyond the original retention period for historical, statistical or scientific purposes, please specify whether the personal data will be anonymised:

☒ No

☐ Yes

15) Technical & organisational security measures taken

EIOPA implements several technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

Microsoft 365, including Teams, has been configured to preserve the confidentiality of the information exchanged by implementing encryption during all communications and when in storage, while anonymous access is not authorised.

Processing of identity and access data in Microsoft 365 and Azure Active Directory is necessary for the management of the internal and external user population and their access rights, in order to ensure that the appropriate level of security and access to resources is applied. As mentioned above, to reduce the occurence of online identity theft and other online fraud, EIOPA implements Azure Multi-Factor Authentication (MFA), a process in which users are prompted during the sign-in process for an additional form of identification, such as using the Microsoft Authenticator app or a voice call.