EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

RECORD OF PROCESSING ACTIVITY ACCORDING TO ARTICLE 31 REGULATION 2018/1725[1] NOTIFICATION TO THE DATA PROTECTION OFFICER

NAME OF PROCESSING OPERATION[2]: Use of Microsoft Office 365 (M365)

Reference number: DPR-2020-108
Creation date of this record: 07/07/2020
Last update of this record: 25/03/2022
Version:2

Part 1 (Publicly available)

1) Controller(s)[3] of data processing operation (Article 31.1(a))
Controller: European Union Agency for Fundamental Rights (FRA) Schwarzenbergplatz 11, A-1040 Vienna, Austria Telephone: +43 1 580 30 – 0 Email: contact@fra.europa.eu Organisational unit **responsible**[4] for the processing activity: Corporate Services Contact details: it.helpdesk@fra.europa.eu Data Protection Officer (DPO): dpo@fra.europa.eu

2) Who is actually conducting the processing? (Article 31.1(a))[5]	
The data is processed by the FRA itself	☒
The data is processed also by a third party For services related to the Microsoft Office 365 cloud-based collaboration platform, Microsoft acts as data processor.	☒

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

2 **Personal data** is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.
Processing means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3 In case of more than one controller (e.g. joint FRA research), all controllers need to be listed here

4 This is the unit that decides that the processing takes place and why.

5 Is the FRA itself conducting the processing? Or has a provider been contracted?

Contact details: Microsoft Ireland, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.

NOTE: Contacts with Microsoft take place only via the Agency and the Commission. The above information is provided for internal use only.

3) Purpose of the processing (Article 31.1(b))

Why are the personal data being processed? Please provide a very concise description of what you intend to achieve with the processing operation. Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing. If you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).

The processed personal data is required for the introduction and implementation of the Microsoft Office 365 to the Agency's staff. This is aligned with the Agency's Digital Services strategy as well as the cloud strategy which follow the corresponding Commission's Digital and Cloud Strategies.

The Agency's Digital Workplace Program is an essential part of the Agency's digital strategy. The Agency's Digital Workplace Program allows secure collaboration and sharing of information between Agency staff and third parties, including other EU institutions and agencies, public administrations, international organizations and other collaborators invited to the M365 environment by the Agency staff.

Modes of processing

- Automatic processing (Article 24): Computer machine
- Manual processing: In addition to automatic processing FRA or Microsoft may process personal data manually. This is part of service operations and most importantly to investigate security alerts. For cyber security and system monitoring purposes M365 raw SGD logs are collected. FRA and CERT-EU Commission services reserve the right to consult user activity on raw SGD to maintain security and integrity of the M365 environment.

4) Description of the categories of data subjects (Article 31.1(c))

Whose personal data are being processed?

FRA staff (incl. SNEs, trainees) ☒

Non-FRA staff ☒

Non- staff is any external person who is using the Agency's cloud services for example MB and Scientific Committee members, as well as any other external persons who are granted access to use the Office 365 service as guests.

5) Categories of personal data processed (Article 31.1(c))

Please tick all that apply and give details where appropriate

(a) General personal data (add or delete as appropriate – the data in the brackets are only examples)

Personal details (name, title, address, IP address, cookies, connection data)	☒
Contact details (postal address, email address)	☒
Education & Training details	☐
Employment details (e.g. work experience, languages, name and type of the employer/organisation, address of the employer/ organisation)	☐
Financial details (e.g. financial identification form, bank account information)	☐
Family, lifestyle and social circumstances	☐
Goods or services provided	☐
Other (please give details):	☒

The Office365 platform distinguishes between the following data categories:

- Identification data
- Content data
- Service generated data (SGD)
- Diagnostic data

Any of these categories may contain personal data. The operation of this platform requires the processing of data categories by Microsoft, for the following specific purposes:

1. Providing the Office 365 service to the Commission:
    a. Identification data, Content data, SGD
2. Technical support to IT teams for issues with Office365
    a. Identification data, SGD
3. Prevention, detection and resolution of security events (e.g. cyber-attack)
    a. Identification data, SGD
4. Assistance to data subjects in exercising their rights in relation to data processed within Office 365
    a. Identification data, SGD

The operation of this platform requires the processing of data categories by DIGIT C6, for the following specific purposes:

1. Set-up, configuration and maintenance of Office365 capabilities
    a. Identification data, SGD
2. Administration of the rights allocated to a user account
    a. Identification data

3. End-user support for issues with Office365
    a. Identification data, SGD, Diagnostic data
4. Prevention, detection and resolution of security events (e.g. cyber-attack)
    a. Identification data, SGD
5. Assistance to data subjects in exercising their rights in relation to data processed within Office 365
    a. Identification data, SGD

The above-mentioned processing of personal data by the Agency and/or Microsoft is done to provide the cloud component of the Digital Workplace services.

In addition to this, Microsoft has been granted permission to process personal information for internal business functions in the context of providing the Office365 service (exhaustive list):

1. Billing and Account Management
    a. Identification data, SGD
2. Compensation
    a. SGD
3. Internal Reporting and Business Modelling
    a. SGD
4. Combatting fraud, Cybercrime, and Cyberattacks
    a. Identification data, SGD
5. Improving Core Functionality of Accessibility, Privacy and Energy Efficiency
    a. SGD
6. Mandatory Financial Reporting and Compliance with Legal Obligations
    a. Identification data, SGD

Personal data will not be used for an automated decision-making including profiling, advertising or marketing.

For cyber security and system monitoring purposes Office 365 raw SGD logs are collected in the Agency's log correlation service. The Agency's responsible staff reserves the right to consult user activity based on raw SGD to maintain the security and integrity of the M365 environment. All such access activity is also logged by the system.

Related to the provision of the service, the Agency or Microsoft process four different categories of data, all of which may include personal data. These categories are:

1. Identification data contains personal data necessary for the proper identification of the user and the corresponding user account, including exhaustively
    - Agency's username, email address and account status
    - User personal data (title, last name, first name)
    - Function-related data (unit, office address and telephone number, city and country). Logging into the FRA M365 environment is done with the email address only. Microsoft's servers process the domain name @fra.europa.eu of the Agency redirecting to the FRA M365 environment. Finally, authentication is happening using the Microsoft authentication services. Note that identification data (see who is who) is visible to everyone having

access to the M365 environment.

2. Content data includes any content uploaded to the Office 365 platform by its users, such as documents, and multimedia (e.g. video recordings). Such data is stored by the user in Office 365 but not otherwise processed by the service.
3. Diagnostic data (also known as telemetry data) is related to the data subjects' usage of office client software. FRA has applied technical measures to disable sharing of diagnostic data with external parties, including Microsoft. Nevertheless, FRA collects Office Diagnostic Data about the client software for its own support purposes in a database hosted in the Agency's data centre.
4. Service generated data (SGD) contains information related to the data subjects' usage of online services, most notably the user IP address, creation time, site URL and user email address. This data is generated by events that are related to user activity in Office 365. Event data will allow to monitor all activity in the cloud environment of each user. To learn which events trigger the creation of SGD, consult the annex. SGD are mainly pseudonomysed and aggregated for Microsoft's six internal business functions stated above, with the following exceptions:
   a. Combatting fraud, Cybercrime, and Cyberattacks
   b. Compliance with Legal Obligations

For international data transfers refer below (Section 7).

There might be personal information being processed, in particular personal information contained within the Content Data of individual users or groups of users in addition to the personal data processed by all Office 365 tools that are covered by this record and privacy statement. This refers for example to documents or messages exchanged between members of a specific group or team.
Microsoft does NOT process special categories of personal data in the context of Office 365. Nevertheless, end-users may use Office 365 as a means for processing special categories of personal data in the context of specific policies and other processing operations which entail specific security measures.

(b) Sensitive personal data (Article 10)
The personal data collected reveal:

Racial or ethnic origin ☐

Political opinions ☐

Religious or philosophical beliefs ☐

Trade union membership ☐

Genetic, biometric or data concerning health ☐

Information regarding an individual's sex life or sexual orientation ☐

N/A ☒

6) Recipient(s) of the data (Article 31.1 (d))

*Recipients are all parties who have access to the personal data. Who will have access to the data **within** FRA? Who will have access to the data **outside** FRA? No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).*

Designated **FRA** staff members ☒
This includes staff members of the CS DSF sector.
Access to your personal data is provided to Agency Staff responsible for carrying out this processing operation and to authorised staff according to the "need-to-know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements. Those members of staff include appointed staff and service providers under officials' supervision. The information collected will not be given to any third party, except to the extent and for the purpose required by law.

Recipients **outside** FRA:
(please provide a generic/functional mailbox) ☒
Personal data is processed by the Agency and its contractor Microsoft. Recipients can include Microsoft's personnel managing the databases on Microsoft cloud servers and their sub-processors' personnel on a need-to-know basis.

In case that we need to share your data with third parties, you will be notified with whom your personal data has been shared.

7) Transfers to third countries or international organisations (Article 31.1 (e))[6]

If the personal data are transferred outside the European Economic Area or to international organisations, this needs to be specifically mentioned, since it increases the risks of the processing operation.

Transfer outside of the EU or EEA

[6] **Processo**r in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult your DPO for more information on how to ensure safeguards.

Yes ☒

No ☐

Transfers of personal data outside the European Union are not foreseen.
However, diagnostic data covered by contractual rules may be sent to Microsoft in the United States.

For certain limited categories of personal data which are detailed in the below scenarios, Microsoft IRELAND may transfer personal data to the USA or any other country in which Microsoft or its sub- processors operate. These data flows take place from Microsoft IRELAND to Microsoft Corp. in the USA and to Microsoft's sub-processors.

Microsoft Ireland has signed with Microsoft Corp. the new Standard Contractual Clauses ("SCCs") adopted by Commission Implementing Decision (EU) 2021/914 (module three: processor-to- processor). The new Standard Contractual Clauses cover all transfer scenarios indicated below.

SGD is processed outside of the EU. In most cases, SGD is pseudonymised before being transferred.
International data transfers are effectively taking place in four transfer scenarios:
1. SGD transfers
SGD transfers for Combatting fraud, Cybercrime, and Cyberattacks and Compliance with Legal Obligations are protected by encryption (ensuring their confidentiality in transit).
2. Worldwide access to EC M365 environment
Logging into the M365 environment is done with the email address only. Microsoft's servers process the domain name @fra.europa.eu of the Agency redirecting to the EC M365 environment. Finally, the authentication service is also provided by Microsoft services.
3. Support case
Only designated second-level support teams (system administrators) can open support cases with Microsoft. Most support cases do not need access to 'Customer Data'. In exceptional cases where such access is needed, mitigation is achieved by activating the 'Customer Lockbox' feature. This feature enforces customer approval for giving time-bound access to any 'Customer Data' by Microsoft engineers.
4. Microsoft 365 Apps licensing and activation data
In the context of combatting software piracy, Microsoft needs to verify a user's right to use Office products and manage product keys. This process is essential for the provision of the service and cannot be avoided. The standard technical measures for securing transfers, notably robust protection against interception, apply.
Considering the specific circumstances of the transfers, the use of appropriate safeguards and the above analysed supplementary measures, the transfer of personal data concerned to the United States is effectively subject to appropriate safeguards.

Transfer to international organisation(s)

Yes ☐

No ☒

If yes specify to which organisation:

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:

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.

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 international agreement (Article 49), specify:

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
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

ADDITIONAL INFORMATION:

The EC represented by DIGIT, who is the leader of the related framework contract with Microsoft, negotiated additional terms regarding the use of the M365 products. These were further examined by EDPS who recommended a number of enhancements. These were then included in the revised framework contract. All details of the measures as well the DPIA are annexed to this request.

8) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Please indicate the starting point and differentiate between categories of persons or data where needed (e.g. in selection procedures candidates who made it onto the reserve list vs. those who didn`t). Are the data limited according to the adage "as long as necessary, as short as possible"?

The Agency only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing. The Agency maintains data for as long as the user account is activated or if users have not decided to remove or delete personal data from their account. Log data will be kept for up to 6 months.

The administrative time limit(s) for keeping the personal data per data category

- Identification data
  - for as long as the user account is active
- Content data
  - up to 180 days upon expiration/termination of the subscription
- SGD
  - up to six months
- Diagnostic data
  - up to five years

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.

9) Technical and organisational security measures (Article 31.1(g))

Please specify where/how the data are stored during and after the processing; please describe the security measures taken by FRA or by the contractor

How is the data stored?

Document Management System (DMS)	☐
FRA network	☒
Outlook Folder(s)	☐

CRM	☐
Hardcopy file	☐
Cloud (give details, e.g. cloud provider)	☒
Servers of external provider	☐

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the Agency's Data Centre or in Microsoft datacentres in the EU (linked to the Agency's and Commission's Office 365 environment). All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.
In order to protect your personal data, the Commission (who represented the Agency in the negotiations with Microsoft) has put in place several strong contractual safeguards, complemented by 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.

The Agency is actively configuring customer data location (at rest) of its Office 365 services. The online services the Agency will use are offered from data centres in EU Member States, respectively Ireland, the Netherlands, Austria or Finland. No content data will be stored outside the EU territory.

Any log files generated by using Microsoft Office 365 Online services can be analysed in the US, and while the Commission (and hence the Agency) cannot technically avoid this, strong contractual safeguards apply to this data. Any data in transit is protected by strong encryption.

The Commission (who represented the Agency in the negotiations with Microsoft) has taken legal and technical measures to protect personal data that are transferred outside the EU/EEA according to Chapter V of Regulation 2018/1725.

NOTE:
The Agency based on the DPIA undertaken by the Commission services adopted the same practices. The related report and DPIA are annexed to this record.

10) Exercising the rights of the data subject (Article 14 (2))

How can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? How will you react?

See further details in the privacy notice: e-mail to it.heldesk@fra.europa.eu

Data subject rights

☒ Right of access

☒ Right to rectification

☒ Right to erasure (right to be forgotten)

☒ Right to restriction of processing

☐ Right to data portability

☒ Right to object

☒ Notification obligation regarding rectification or erasure of personal data or restriction of processing

☒ Right to have recourse

☐ Right to withdraw consent at any time