Use of Microsoft Office 365 (M365)

The European Union Agency for Fundamental Rights (FRA or Agency) processes the personal data of a natural person in compliance with Regulation 2018/1725 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.

This privacy notice explains FRA's policies and practices regarding its collection and use of your personal data, and sets forth your privacy rights. We recognise that information privacy is an ongoing responsibility, and we will update this notice where necessary.

1. Why do we collect personal data?

The processed personal data is required for the introduction and implementation of the Microsoft Office M365 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.

Within this framework, 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 organisations and other collaborators invited to the M365 environment by the Agency staff.

2. What kind of personal data are collected and further processed?

The Agency processes your personal data to enable digital collaboration platforms in the context of the digital services and cloud transformation services for Agency staff.

The processing activity refers to the use Microsoft Office 365 (M365) services offered by the Agency to its staff or assigned external users like Management Board members, Scientific Committee members, as well as any other external persons who are granted access to use the Office 365 service as guests.

(a) General personal data:

- Personal details (name, title, address, IP address, cookies, connection data)
- Contact details (postal address, email address)

(b) Other:

The M365 platform distinguishes between the following data categories as defined in detail in section 4 of this document:

- 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 FRA 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 M365 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

Your personal data will not be used for an automated decision-making including profiling, advertising or marketing.
For cyber security and system monitoring purposes M 365 raw SGD logs are collected in the Agency's log. The Agency reserves the right to consult user activity based on raw SGD to maintain the security and integrity of the M365 environment.

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.

FRA and Microsoft **do not process special categories** of personal data in the context of Office 365. Nevertheless, the end-users and may use M365 as a means for processing special categories of personal data in the context of specific policies.

3. How is your data collected and further processed

3a. Information you provide us: This includes personal information like name, address, title provided by you to FRA.
3b. Information we collect about you: This include data that are being collected through the use of the M365 (logs, etc.) as described under section 2. This data is collected via automated or manual steps.

4. Who is responsible for processing your personal data?

The Agency is the legal entity responsible for the processing of your personal data and determines the objective of this processing activity. The Head of Corporate Services Unit is responsible for this processing operation.

For services related to the Microsoft Office 365 cloud-based collaboration platform, Microsoft acts as data processor. Contact details: Microsoft Ireland, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland.

5. Which is the legal basis for this processing operation?

All personal data connected to the use of Microsoft Office 365 are processed based on the necessity for the performance of the tasks carried out in the public interest by the Agency on the basis of its Founding Regulation,[1] including the processing of personal data that are necessary for the management and functioning of the Agency. More specifically, the objective of all processing activities related to Microsoft Office 365 is to support the management and the functioning of the Agency, by adjusting the internal mechanisms and management systems to the new technological environment and advancements, by providing to Agency Staff the necessary means and tools to perform their daily tasks and by organizing the Agency's operations according to the principles of sound financial management. (Article 33 of the Regulation 2018/1046)[2].

The digital transformation of the Agency is in line with the EC's Digital Transformation strategy. These actions are guided by policies on digital affairs (data, interoperability, eGovernment) and based on the following existing detailed strategies for specific domains:

- digital services and cloud strategies;
- IT-security and information-security policy;
- data, information and knowledge management at the Agency;

These actions also use, extend and develop the Agency's

- existing portfolio of policy and administrative information systems,
- digital services and
- current digital infrastructure.

The deployment of M365 cloud services is the implementation of the Agency's cloud strategy. Therefore, the processing is lawful under Article 5.1.(a) of the Regulation (EU) No 2018/1725.

[1] Regulation (EC) No. 168/2007 establishing the European Union Agency for Fundamental Rights

[2] Regulation 2018/1046 of the European Parliament and of the council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012.

6. Who can see your data?

Within the Agency, access to your personal data is provided to the 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 Corporate Services unit staff and if needed contractors acting under the supervision of the Digital Services and Facilities (DSF) staff. The information we collect will not be given to any third party, except to the extent and for the purpose we may be required to do so by law.

Outside the Agency, 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. Do we share your data with other organisations?

Personal data is processed by the Agency and its contractor Microsoft. In case that we need to share your data with third parties, you will be notified with whom your personal data has been shared.

8. Do we intend to transfer your personal data to Third Countries/International Organizations

Only diagnostic data (see under 2) covered by contractual rules may be sent to Microsoft in the United States. More specifically, 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

9. When we will start the processing operation?

We will start the processing operation once your account profile is created on Microsoft's platform.

10. How long do we keep your data?

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 are the following:

- 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.

11. How can you control your data?

Under Regulation 2018/1725, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information. You are not required to pay any charges for exercising your rights except in cases were the requests are manifestly unfounded or excessive, in particular because of their repetitive character.

We will reply to your request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

You can exercise your rights described below by sending an email request to it.helpdesk@fra.europa.eu which will forward your request to the data controller.

11.1. How valuable is your consent for us?

Since the participation in the use of Microsoft office 365 is mandatory in accordance with the Agency abovementioned cloud startegy, in accordance with the applicable legal framework (please refer to Section 5 above) you are not required to provide your consent.

11.2. Your data protection rights

a. Can you access your data?

You have the right to receive information on whether we process your personal data or not, the purposes of the processing, the categories of personal data concerned, any recipients to whom the personal data have been disclosed and their storage period. Furthermore, you can have access to such data, as well as obtain copies of your data undergoing processing.

b. Can you modify your data?

You have the right to ask us to rectify your data you think is inaccurate or incomplete at any time.

c. Can you restrict us from processing your data?

You have the right to block the processing of your personal data when you contest the accuracy of your personal data or when the Agency no longer needs the data for completing its tasks. You can also block the processing activity when the operation is unlawful, and you oppose to the erasure of the data under specific legitimate grounds.

d. Can you delete your data?

You have the right to ask us to delete your data when the personal data are no longer necessary for the purposes for which they were collected, when you have withdrawn your consent or when the processing activity is unlawful. In certain occasions we will have to erase your data in order to comply with a legal obligation to which we are subject.

We will notify to each recipient to whom your personal data have been disclosed of any rectification or erasure of personal data or restriction of processing carried out in accordance with the above rights unless this proves impossible or involves disproportionate effort from our side.

e. Are you entitled to data portability?

Data portability is a right guaranteed under Regulation 1725/2018 and consists in the right to have your personal data transmitted to you or directly to another controller of your choice.

In this case, this does not apply for two reasons: I) in order for this right to be guaranteed, the processing should be based on automated means, however we do not base our

processing on any automated means; II) this processing operation is carried out in the public interest, which is an exception to the right to data portability in the Regulation.

f. Do you have the right to object?

When the legal base of the processing is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body" which is the case in most of our processing operations, you have the right to object to the processing. In case you object, we have to stop the processing of your personal data, unless we demonstrate a compelling reason that can override your objection.

g. Do we do automated decision making, including profiling?

Not applicable

12. What security measures are taken to safeguard your personal data?

All personal data in electronic format (emails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the European Commission's data centre or in Microsoft datacentres in the EU (linked to the EC M365 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.

To protect your personal data, the Commission, who represented the Agency in the negotiation with Microsoft, has put in place several strong contractual safeguards, complemented by technical and organisational measures.

In addition to the general policy of Microsoft to secure personal data by means of pseudonymisation and encryption (at rest and in transit), the risk of disclosure of personal data to third country authorities by Microsoft Ireland and its affiliates is mitigated by customised contractual provisions and technical and organisational measures. Contractual provisions address the way Microsoft responds to access requests, limiting risks to personal data of the customer.

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.

13. What can you do in the event of a problem?

a) The first step is to notify the Agency by sending an email to it.helpdesk@fra.europa.eu and ask us to take action. This request will be provided to the data controller for further actions.

b) The second step, if you obtain no reply from us or if you are not satisfied with it, contact our Data Protection Officer (DPO) at dpo@fra.europa.eu.

c) At any time you can lodge a complaint with the EDPS at http://www.edps.europa.eu, who will examine your request and adopt the necessary measures.

14. How do we update our data protection notice?

We keep our privacy notice under regular review to make sure it is up to date and accurate.

END OF DOCUMENT