



DATA PROTECTION NOTICE

on the processing of personal data in the context of M365

1. Introduction

The European Union Agency for Asylum (hereinafter “the EUAA” or “the Agency”) is committed to protecting your privacy. The EUAA collects and further processes personal data pursuant to [Regulation \(EU\) 2018/1725](#)¹ (hereinafter “the EUDPR”).

This privacy statement explains *inter alia* the reasons for the processing of your personal data, the way we collect, handle and ensure protection of your personal data and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, as well as of the Data Protection Officer (DPO) and the European Data Protection Supervisor (EDPS) to which you may have recourse as well to exercise the said rights.

2. Why and how do we process your personal data?

The purpose of processing the below personal data is to allow the EUAA to conduct IT service management activities in the context of providing the Microsoft Office365 cloud environment for all EUAA users. As the M365 cloud environment relies on the Software-as-a-Service cloud model, the EUAA has a limited responsibility with regard to the maintenance and management of the service. The following purposes of processing will be considered in context of this processing activity:

- To provide and maintain M365 cloud services to EUAA users;
- To ensure adequate quality of M365 cloud services to EUAA users;
- To ensure the confidentiality, integrity and availability of M365 cloud services to EUAA users;
- To manage the vendor relationship with Microsoft as Cloud Service Provider;

3. On what legal ground(s) do we process your personal data?

We process your personal data on the basis of Article 5(1)(a) of the EUDPR, because 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. To the extent that processing is based on the (opt-in) consent of the data subject, the processing is lawful under Article 5(1)(d) of the EUDPR.

4. Which personal data do we collect and further process?

The following categories of personal data may be processed:

- User attributes synchronized to Azure AD for authentication purposes;

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, OJ L 295, 21.11.2018, p. 39-98.





- Name, title, address (private and professional), previous addresses, phone number (private and professional), identifier; (an identifier has been created by Microsoft and is tied to the user of a Microsoft service);
- Current function: employer, title and description of the function;
- Guest accounts name and surname, for purposes of accessing EUAA's resources;
- User diagnostic data (telemetry data) from OneDrive and Teams;
- Electronic Identifying Information: IP address, cookies, connection data;
- Security: password, security codes and level of authorization;
- Personal identifiable information contained in email, office documents, SharePoint and Teams sites and in recordings made via Microsoft teams conferences (stream).

5. How long do we keep your personal data?

In line with Article 4(1)(e) of the EUDPR, personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. In determining the maximum retention periods, the Agency has taken into account the nature of the sanction, possible legal recourses, legal, auditing, archiving and reporting obligations.

The retention periods for specific types of documents used within the EUAA working environment are established in accordance with the EUAA Records Retention and Disposal Policy Documents.

6. Who has access to your personal data and to whom is it disclosed?

The data collected for the correct functioning of M365, to provide and maintain M365 cloud services, to ensure adequate quality and the confidentiality, integrity and availability of M365 cloud services is shared only with the EUAA staff members responsible for the day-to-day management of the system – the EUAA ICT Unit.

The user diagnostic data (telemetry data) and the electronic identifying information (IP address, cookies, connection data) is shared with Microsoft as a data processor. This processing of personal data consists of the monitoring and analysis of the usage of the cloud-based services made by EUAA users. These processing operations of personal data of users would be for the purposes of: 1. Billing and account management; 2. Compensation (e.g. calculating employee commissions and partner incentives); 3. Internal reporting and business modelling (e.g. forecasting, revenue, capacity planning, product strategy); 4. Combatting fraud, cybercrime or cyberattacks that may affect Microsoft or Microsoft Products; 5. Improving the core functionality of accessibility, privacy or energy-efficiency; 6. Financial reporting and compliance with legal obligations (subject to the limitations outlined by contractual means).

The control over the disclosure of personal data contained in emails, office documents, SharePoint and Teams sites and in recordings made via Microsoft teams conferences (stream) is at the discretion of



individual EUAA users. This disclosure and sharing of information must comply with the applicable rules related to each processing operation.

7. How do we protect and safeguard your personal data?

In order to protect your personal data, the EUAA has put in place several technical and organisational measures in place.

Technical measures include appropriate actions to address online security, information protection, alteration of data or unauthorised access, limitation of telemetry data, conditional access, encryption of data in transit and at rest, taking into consideration the risk presented by the processing and the nature of the personal data being processed, as well as the latest technological means available.

Organisational measures include safeguarding access to data, auditing, removal of unilateral amendments of contractual provisions, strict purpose limitation, compliance with processor agreements, strict limitation of sub-processors, control of location(s), reporting on any eventual breaches via contractual means and restricting access to the personal data on a need to access and for the purposes of this processing operation.

8. What are your rights and how can you exercise them?

According to the EUDPR, you are entitled to access your personal data and to rectify it in case the data is inaccurate or incomplete. If your personal data is no longer needed by the EUAA or if the processing operation is unlawful, you have the right to erase your data. Under certain circumstances, such as if you contest the accuracy of the processed data or if you are not sure if your data is lawfully processed, you may ask the Data Controller to restrict the data processing. You may also object, on compelling legitimate grounds, to the processing of data relating to you. Additionally, under certain circumstances you have the right to data portability which allows you to obtain the data that the Data Controller holds on you and to transfer it from one Data Controller to another. Where relevant and technically feasible, the EUAA will do this work for you.

Should you require further information regarding the processing of your personal data, or should you wish to exercise any of the above-mentioned rights, you may contact the Data Controller by sending an e-mail to ictu.datacontroller@euaa.europa.eu.

You may always submit queries, remarks or complaints relating to the processing of your personal data to the Data Protection Officer (DPO) of the EUAA by using the following e-mail address: dpo@euaa.europa.eu.

In case of conflict, complaints can be addressed to the European Data Protection Supervisor (EDPS) using the following e-mail address: edps@edps.europa.eu.