DATA PROTECTION STATEMENT

M365

Organisational part of the Agency entrusted with the processing of personal data
Head of CPU (information(at)osha.europa.eu)

Purpose

M365 is a cloud based package of Microsoft applications (Word, Excel, PowerPoint, Outlook, MS Teams, SharePoint, OneNote, OneDrive…) which EU-OSHA provides to staff members with the aim of facilitating their daily work and improving communications, collaborations, and the availability of resources. The services provided via the applications cover a wide range of activities and enable EU-OSHA staff to deliver on its mission. The services provided via MS Teams include business messaging, calling, video meetings and file sharing.

The provision of services by Microsoft is based on an Agreement between the EU Institutions and Microsoft Ireland Operations Ltd. which was negotiated by the DIGIT on behalf of the EU Institutions. In coordination with the EDPS, the DIGIT has negotiated a so-called custom Data Protection Addendum (DPA) which is part of the Agreement. This DPA introduces comprehensive data protection terms for the most important online Services and software products of Microsoft, providing significantly improved levels of transparency, clarity and protection compared to the use of such services as a private user. Most staff members’ personal data which is processed by M365 is stored in each member's email account. E.g., this is the case for MS Teams chats, calendar information, content of emails, data processed for MS Viva services, data contained in the personal One-Drive.

Legal basis

- Commission Decision No 46/2017 of 10 January 2017 concerning the security of communication and information systems in the EU.
- Licensing Agreement between the European Union Institutions and Microsoft Ireland Operations Limited dated 1 June 2018 including the Custom Data Protection Addendum

Type of data processed

The categories/types of personal data processed are the following:
- Personally identifying information: username, name, surname, unit, email, work telephone number, and current function.

- Electronic identifying information: Connection data and access time. - Certain types of metadata (e.g., email address, organization) used for the maintenance of the services provided. The main part of metadata is not personal data but anonymized service data.

- Any data potentially processed in the content shared with the MS applications for professional activities (e.g., emails, messages, images, files, voicemail, calendar meetings, contacts...). - Any picture, video and sound, for example those that are displayed and exchanged during MS Teams calls.

**Lawfulness of processing**

The processing is based on Article 5.1 of 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 (hereinafter the Regulation).

**Data recipients**

ICT Administrators can access the email accounts management information only for the purpose of ICT system administration. Emails can only be accessed in line with the ‘EU-OSHA E-mail accounts’ activation and deactivation Policy’. External provider Microsoft can only access data in line with the service agreement for maintenance purposes. For M365, the majority of 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 or on its own and are only granted access in case it is required for maintenance purposes (when EU-OSHA is submitting a specific support request). In 2021, Microsoft has committed itself to storing all data of European users in storage centers located in the EU. In accordance with the DPA, personal data that Microsoft processes on EU-OSHA’s behalf may not be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its subprocessors operate, except in accordance with the safeguards provided in the DPA (e.g., any such transfer shall be governed by Chapter 5 of the EUDPR and be subject to an adequacy decision in line with article 47 of the EUDPR).

**The data subject’s rights**

You have specific rights as a ‘data subject’ under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, your personal data and to rectify them in case your personal data are inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data, to object to the processing, and the right to data portability. You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a) and 5(1)(b) on grounds relating to your particular situation. You can exercise your rights by contacting the Data Controller (organisational part of the Agency entrusted with the processing of personal data), or in case of conflict the Data Protection
Officer. If necessary, you can also address the European Data Protection Supervisor. The contact information of the Data Protection Officer and the European Data Protection Supervisor is given below.

Information on the conservation period of data

Data will be retained for as long as the Agreement between the EU-Institutions (including EU-OSHA) and Microsoft is in force. Once the Agreement expires, any data is retained for 90 days for the purposes of collection by the Agency or possible renewal of the Agreement. Any personal data that is stored in the user’s email account, is deleted in line with the EU-OSHA E-mail accounts’ activation and deactivation Policy. I.e., the email account is deleted three months after the deactivation of the account.

Security measures

Microsoft Datacentres are certified in several security standards, most notable ISO 27001, SOC 1 and SOC 2, NIST Cybersecurity Framework (CSF), ISO 27017 and ISO 27018 Code of Practice for Protecting Personal Data in the Cloud. Microsoft has implemented several controls to ensure the availability of the information. As a minimum, data is replicated between two datacenters within the same region, has redundancy controls and implements backups that are encrypted before being transmitted and stored. Datacenters have physical and logical security monitoring measures, such as:

- Video surveillance of the perimeter
- Seismic and environmental monitoring at the buildings
- Monitoring of security threats, such as worms, denial of service attacks, unauthorized access, or any type of unlawful activity.

Request for information

For any further information regarding the handling of their personal data, data subjects can address their request to EU-OSHA Data Protection Officer at: dpo(at)osha.europa.eu.

Recourse to the EDPS

Data subjects are entitled to make recourse to the European Data Protection Supervisor: http://www.edps.europa.eu, should they consider that the processing operations do not comply with the Regulation.

Date when processing starts

Whenever data is entered into the system.

Privacy statement last updated: 1/16/2023 12:25:05 PM