MICROSOFT 365 AT EDPS

DATA PROTECTION NOTICE

This data protection notice provides information regarding processing of personal data related to the use by the European Data Protection Supervisor (EDPS), in view of its mandate and tasks, of the Microsoft 365 cloud-based service ('M365') that includes applications and online services such as email and collaboration tools.

Personal data is processed in accordance with Regulation (EU) 2018/1725 (hereinafter 'the Regulation').

We provide you with the information that follows based on Articles 15 and 16 of the Regulation.

Who is the controller?
European Data Protection Supervisor (EDPS)
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels
Telephone: +32 2 283 19 00
Email: edps@edps.europa.eu

Delegated controller:
Secretary-General
EDPS-Secretary-General@edps.europa.eu

Contact form for enquiries on processing of personal data to be preferably used: https://www.edps.europa.eu/about-edps/contact_en.

For more information: https://www.edps.europa.eu/about/data-protection-within-edps/data-protection-officer-edps_en.

The EDPS is controller for the personal data it processes in the exercise of its tasks within the M365 platform.

Particular processing activities, under the remit of EDPS units and services, are covered by specific records, available in the EDPS register.

The EDPS is also controller with regard to instructions given to its staff on the use of the available applications and the use of certain of their features (to the extent possible, given the customisation done at ITEC level), as defined in the EDPS Acceptable Use Policy.

The EDPS is also controller regarding business processing operations related to its usage of M365, such as meetings recording or documents processing (containing personal data) and processing of personal data in such contexts.

The **European Parliament (EP)** acts as a separate controller regarding M365 as it determines the technical standard configuration of the platform (i.e. operational decisions regarding platform's setup and management, including controlling data protection-related settings).

The Directorate-General for Innovation and Technological Support (DG ITEC) operates the EP's M365 platform.

DG ITEC > Directorate for Infrastructure and Equipment
ITEC-OPERATIONS-personal-data-protection@europarl.europa.eu

Given the specificities of the responsibilities of the EP and the EDPS, respectively, as outlined above, the information included in this document draws, where applicable, on the EP documentation, namely the EP record and data protection notice, while emphasising the particularities of the EDPS' processing of personal data.

Microsoft Corporation processes personal data as a controller for other purposes as a consequence of the EP's and EDPS' use of its services (https://www.microsoft.com/en-us/privacy/privacystatement).

Are any processors engaged in the processing of personal data?
Microsoft Ireland South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland
https://www.microsoft.com/en-ie/microsoft-365

What personal data is processed and who has access it?

Categories of personal data processed
M365 distinguishes between the following data categories:

Identification Data (ID) used to recognise and authenticate a user and the corresponding account and includes:
- user name, email address and account status
- user personal data (title, last name, first name)
- function related data (organisation (i.e. EDPS), office address, telephone number)

In order to establish accounts for its staff, the EDPS provides DG ITEC with following categories of personal data of its staff: professional contact details (such as name, surname, function, office number), statutory link, starting and end date of contract,

permissions to be granted and any other personal data processed in the context of service provision, as specific for each particular service.

Identification on the EP M365 environment is done with the email address only.

Content Data (CD): includes material created and stored in M365 such as documents, emails, chat messages.

Such data are stored by the user in M365 but not otherwise processed by the service.

All EDPS units and services process personal data within M365 in order to perform their tasks in view of the EDPS' mandate. As such, CD (such as those related to complaints management, personal data breach management, audit, investigations) will be processed by EDPS staff within M365, as defined in the specific EDPS processing activities (see EDPS register).

Diagnostic Data (DD) or '**telemetry data**': is data related to the data subjects' usage of M365. It is collected to monitor performance and detect issues and includes technical information such as error reports and device configuration details. DG ITEC has applied technical measures to disable sharing of diagnostic data with external parties, including Microsoft. Nevertheless, DG ITEC collects Office Diagnostic Data about the client software for its own support purposes in a database hosted in the EP's data centers.

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. These data are generated by events that are related to user activity in EP M365 environment.

Any of these categories may contain personal data.

The EDPS applies safeguards in order to limit personal data processing within M365 and for information security purposes. For these purposes, the EDPS has established organisational measures defining use cases and acceptable tools to be used by its staff.

For example:

- for processing Office documents, LibreOffice, locally installed, is available to EDPS users

- in case of collaborative Office documents editing/viewing amongst staff, it uses SharePoint on premise and its Case Management System, amongst other non Microsoft tools

- for one-to-one communications amongst EDPS staff, and one to one communications with EU staff outside of EDPS, other available tools than Teams shall be used

- for internal meetings, other available tools than Teams shall be used

- when organising meetings with external participants, other available tools than Teams shall be used

Specifically to the email corporate system (also provided by the EP to the EDPS), the following categories of personal data are processed by DG ITEC: user account details (including first name, last name, encrypted password), email address, email folders, emails content (including header information [on the sender, the recipient(s), the subject, date and time of sending], body information and attachment(s)), emails metadata (including the network traffic data, such as the IP addresses), automatic reply, membership of distribution lists, contacts, tasks and calendars.

The EDPS staff can, in some situations, extract copies of emails related to certain processing activities under the EDPS controllership (e.g. complaints, personal data breaches, human resources). They could be subject of further processing related to the processing activities under the EDPS controllership such as saving into the EDPS Case Management System.

Access to personal data processed

The EP
Access to personal data is provided to EP 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.

DG ITEC, including EP M365 environment ICT administrators, processes personal data and transmits it (ID, DD, SGD) as required within the EP units.

Decentralised ICT administration/security/incident/crisis management (Business continuity): EP M365 environment ICT administrators of other DGs and ICT security analysts may have access to ID, CD, DD and SGD respectively for decentralised ICT service administration and ICT security incident management and/or incident/crisis management (Business continuity). For the most part, they access aggregated data.

Users support: The operational managers within EP DES or ESIO Directorate and ICT helpdesk staff may have access to ID, DD and SGD during users' issues resolutions or users' requests process. Access to these data help to establish the issues' characteristics and origin (e.g. the correct access rights) to solve them and to provide requested support

to users. If necessary, EP M365 environment ICT administrators may also have access to the CD to support strictly the same purposes.

Technical support to official investigations: In case of official investigations, the EP Operations Unit of the ESIO Directorate may provide technical support to, and as requested by the EDPS competent authorities. In this respect, these competent authorities may instruct the Operations Unit (within the scope of the mandate defined by the relevant legal basis) to obtain the necessary information to achieve their own purposes. None of the information from EP M365 environment extracted and transmitted is kept at Operations Unit level. Such personal data processing operations (in this context) are of the responsibility of these competent authorities, constituting different processing activities from the one described in this personal data protection statement. Such processing activities are not the subject of this personal data protection statement. For more information on the specific EDPS processing activities in scope, you can refer to the EDPS register.

Microsoft
As processor, Microsoft's staff (e.g. managing the databases on Microsoft cloud servers) and, where applicable, its sub-processors' staff could have access to certain personal data on a need-to-know basis. A list of sub-processors was agreed upon by the EC when signing the ILA. Microsoft commits to have in place written agreements with all its sub-processors that are at least as restrictive in terms of data protection and security as their data processing agreement with the EC.

Other possible recipients

- Bodies charged with a monitoring or inspection task under EU law, where required for official investigations or for audit purposes (e.g. European Ombudsman, the EDPS, as data protection supervisory authority)

- The Court of Justice of the European Union, where applicable

- Where applicable, citizens in the context of requests for access to documents, in accordance with the Regulation (EC) 1049/2001

- Any other party with whom the EDPS decides to exchange a document containing personal data in the context of its tasks as defined in EDPS specific processing activities.

Where did we get your personal data?
Some personal data (e.g. identification data) originates directly from the EDPS staff member (i.e. provided when taking up the service).

Personal data (related to ID, CD, DG, SGD) are collected directly from the users' activities when using the EP M365 environment services.

Where strictly necessary to obtain technical support from Microsoft on EP M365 environment services, users may be asked to provide some data (which may include personal data) that will be forwarded to Microsoft to obtain technical support (as part of the professional services delivered by Microsoft). Such data should be considered as support data. In order to limit this process to what it is strictly necessary, strong safeguards are applied (see section on transfers).

Personal data related to ID are collected indirectly from the users as it is retrieved from the on-premises EP Active Directory (corporate ICT account directory), such as first name, last name, email address, office phone, office address, profile picture (if it exists), organisational entity.

Why is personal data processed and under what legal basis?

Purpose of processing
M365 is a cloud-based set of work and collaboration tools that includes apps like Word, Excel, PowerPoint, Outlook, SharePoint and Teams.

It enables EDPS staff to perform their tasks in view of the EDPS mandate and tasks. M365 allows EDPS staff to work on any (corporate) device and facilitates collaboration with internal and external stakeholders.

As mentioned, M365 distinguishes between the following data categories:
* Identification Data (ID)
* Content Data (CD)
* Service Generated Data (SGD)
* Diagnostic Data (DD)

The operation of this platform requires processing of personal data (per category) by **the EP**, for the following specific purposes:

1. Set-up, configuration and maintenance of M365 capabilities: ID, SGD
2. Administration of the rights allocated to a user account: ID
3. End-user support for issues with M365: ID, SGD, DD
4. Prevention, detection and resolution of security events (e.g. cyber-attack): ID, SGD
5. Assistance to data subjects in exercising their rights in relation to data processed within M365: ID, SGD

The operation of this platform requires processing of personal data (per category) by **Microsoft**, for the following specific purposes:

1. Providing the M365 service to the EP: ID, CD, SGD
2. Technical support to IT teams for issues with M365: ID, SGD
3. Prevention, detection and resolution of security events (e.g. cyber-attack): ID, SGD
4. Assistance to data subjects in exercising their rights in relation to data processed within M365: ID, SGD

In addition to this, **Microsoft** has been granted permission by the EP to process personal information for internal business functions in the context of providing the M365 services (exhaustive list):
1. Billing and Account Management: ID, SGD
2. Compensation: SGD
3. Internal Reporting and Business Modelling: SGD
4. Combatting fraud, Cybercrime, and Cyberattacks: ID, SGD
5. Improving Core Functionality of Accessibility, Privacy and Energy Efficiency: SGD
6. Mandatory Financial Reporting and Compliance with Legal Obligations: ID, SGD

For the purpose of reporting related to the M365 use within the EP, EP M365 environment services usage (not specific to individuals) is analysed by the EP using SGD, such as the number of video meetings, number of team sites, etc.

Further processing might be used for statistical purposes. Such processing will use pseudonymisation as safeguards to ensure data minimisation.

System activity data are collected in a database to support the adoption process of M365 in the organisation.

Reporting and analytics on usage and user activity available in the Microsoft Admin center are pseudonymised by default.

The (raw) SGD generated in the logs on M365 servers in the data centres may contain personal data. As a next step, the SGD are pseudonymised so that logs contain pseudonymous identifiers. The aggregation process starts from the pseudonymised SGD. SGD are mainly pseudonymised and aggregated for Microsoft's six internal business functions stated above, with the following exceptions: Combatting fraud, Cybercrime, Cyberattacks, Compliance with Legal Obligations.

Processing of personal data for profiling, advertising or marketing is explicitly prohibited according to the contract signed by the European Commission (EC), as the lead contracting authority for the Inter-institutional Licence Agreement (ILA), on behalf of participating EU institutions (including the EP), bodies and agencies.

In addition to automated processing that happens when users make use of the EP M365 environment, DG ITEC services or Microsoft may process personal data manually in the

framework of service operations, most importantly to investigate ICT security alerts and incidents.

The EDPS services process personal data (i.e. CD) within the M365 platform in order to fulfil EDPS tasks as described in the EDPS specific records of processing activities.

The EDPS can also request certain information from the EP (ID, CD, SGD and DD, depending on the circumstances) in order to investigate security incidents as well as to conduct administrative enquiries and disciplinary proceedings (see specific processing activity in the EDPS register).

Legal basis
The legal basis for the processing is Article 5(1)(a) of the Regulation interpreted in the light of the Recital 22, since it is necessary for the performance of tasks carried out in the public interest by the EDPS.

How long do we keep your personal data?
The data are kept as follows:
1. **ID**: kept as long as the EP user account is active, after which they will be deleted from Microsoft's servers within 90 days. Accounts deactivation occurs for EDPS internal users based on the date of their departure from the EDPS, and for external users (guests) after 6 months of inactivity.

2. **CD**: kept until the retention periods defined and implemented by the EDPS for its specific processing activities (see EDPS register) expires. Specific applicable retention periods:
- In 1:1 chats and group chats, individual messages (in the chats) can be deleted by the message author and on a message-by-message basis (not per conversation). The remaining chat history is automatically deleted after 18 months.
- Audio and video calls/meetings are processed 'real time' (on the fly). Meeting recordings are deleted from Teams by default after 60 days. Meeting transcript retention is defined by, and under the responsibility of, the team meeting organisers. In addition, each user can enable closed captions (processed 'real time' and not stored).
- CD actively deleted are retained in a limited access mode for up to 93 days.
- CD will be kept up to 180 days upon expiration/termination of the subscription by the EP for the M365 Service.

3. **DD**: kept up to 5 years from their creation.

4. **SGD**: kept for a default period of up to 180 days from collection.
- **SGD** and **ID** used for support: deleted after the fulfilment of Microsoft business purposes or upon request.

In case of emails, specific retention periods are applicable (according to the EP specific record and data protection notice):

Electronic mailboxes (current and intermediary archives) are kept for as long as the email accounts are active. As regard the emails themselves, there is a deletion and archiving mechanism for messages and folders in electronic mailboxes, as follows:

[CURRENT ARCHIVE]
- All email messages and folders located in “Inbox”, “Sent Items” and “Drafts” are kept for a maximum of 90 days from their creation.
- All email messages and folders located in "Junk Email" are kept for a maximum of 14 days from their creation.
- All email messages and folders located in "Deleted Items" are kept for a maximum of 7 days from their creation.

After these respective periods, those email messages and folders are deleted from the current archive.

All email messages and folders located in any custom folder created outside the above-mentioned folders are kept up to 90 days from their creation, then they are moved to the correspondent “Archive” mailboxes.

[INTERMEDIARY ARCHIVES]

TECHNICAL INTERMEDIARY ARCHIVE
Once the email messages and folders are deleted from the current archive, they are moved to another space with limited access (intermediary technical archive) and kept:

- For 30 days, after erasure by the users (if they were deleted actively by the users in the current archive), then they are totally erased from the intermediary technical archive.

- For 60 days (if they were moved automatically to this intermediary archive), then they are totally erased from the intermediary technical archive.

Users have the possibility to recover the above deleted email messages (i.e. recovering them from the intermediary technical archive to the current archive) before their total deletion from the intermediary technical archive.

BUSINESS INTERMEDIARY ARCHIVE
All email messages and folders located in the “Archive” mailboxes are kept until the retention periods defined and implemented by the business owners of the related email messages and folders, and maximum until the email accounts are deactivated.

Is personal data transferred outside of the EU/European Economic Area or international organisations?
Personal data (emails, documents, etc.) are stored either on the servers of the EP's data centre or in Microsoft data centres in the EU (linked to the EP M365 environment).

More specifically, the data are stored as follows:
- ID: stored in the EP data centers in Belgium/Luxembourg synchronised with Microsoft data centers within the EU.
- CD: stored in Microsoft data centers within the EU ("data at rest").
- SGD: stored in the EP data centers in Belgium/Luxembourg and, mainly in pseudonymised and aggregated form, in Microsoft data centers within and outside of the EU.
- DD: stored in the EP data centers in Belgium/Luxembourg.

EP DG ITEC and EDPS do not limit the regions from which users may access EP's IT services (e.g. users travelling outside the EU/European Economic Area (EEA) and using those services) or to which users may send data (e.g. emails/information sent to recipients outside of the EEA).

EP DG ITEC does not transfer personal data to third countries directly. The data exporter for the transfers which take place under the ILA is the processor (Microsoft Ireland Operations Ltd.) and the data importer the sub-processor (Microsoft Corp.). Limited personal data might be transferred to the United States (US) to Microsoft as data processor and/or its sub-processors.

Microsoft Corporation is certified under the EU-US Data Privacy Framework (DPF) and, as such, can rely on the DPF for transfers to the US.

The EC signed with Microsoft standard data protection clauses in accordance with Article 48(2) of the Regulation.

To protect personal data, several strong contractual safeguards have been put in place, complemented by technical and organisational measures. In particular, in addition to the general policy of Microsoft to secure personal data by means of pseudonymisation and encryption, 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 measured. Contractual provisions address the way Microsoft responds to access requests, limiting risks to personal data. 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.

Transfers are effectively taking place in four transfer scenarios, according to the EP data protection notice:
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). SGD are processed outside of the EU. In most cases, SGD are pseudonymised before being transferred SGD. Microsoft as a controller will transfer pseudonymised SGD data to Microsoft Corp., located in the US, and the network of sub-processors. This type of data contains information on the usage of the service.
2. Worldwide access to EP M365 environment: Identification on the EP M365 environment is done with the email address only.
3. Support case: Only designated 2nd-level support teams (system administrators) can open support cases with Microsoft. Most support cases do not need access to 'Customer Data' at all. 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.

Transfer could also occur due to the nature of the email (i.e. emails exchanged by EDPS staff with recipients that are outside of the EEA).

What are your rights regarding your personal data?
You have the right to request access to your personal data and to relevant information concerning how we use it. You have the right to request rectification of your personal data. You have the right to ask for the erasure of your personal data or to restrict its processing. You have the right to object to the processing of your personal data, on grounds relating to your particular situation, at any time.

We will consider your request, take a decision and communicate it to you. The time limit for treating your request is one (1) month. This period may be extended by two (2) further months where necessary, taking into account the complexity and the number of the requests. In those cases, the EDPS will inform you of the extension within one (1) month of receipt of your request and will provide reasons for the delay.

You can send your request to the EDPS electronically or by post (see section on contact details below).

Automated decision-making
Personal data is not subject to automated decision-making.

You have the right to lodge a complaint
If you have any remarks or complaints regarding the processing of your personal data, you can lodge a complaint with the EDPS as a supervisory authority: https://edps.europa.eu/data-protection/our-role-supervisor/complaints_en.

Contact details for enquiries regarding your personal data
We encourage you to contact us using the EDPS contact form, selecting 'My personal data' as the relevant subject: https://www.edps.europa.eu/about-edps/contact_en.

If you wish to contact the EDPS DPO personally, you can send an e-mail to DPO@edps.europa.eu or a letter to the EDPS postal address marked for the attention of the EDPS DPO.

EDPS postal address: European Data Protection Supervisor, Rue Wiertz 60, B-1047 Brussels, Belgium

You can also find contact information on the EDPS website: https://edps.europa.eu/about-edps/contact_en.