European Economic and Social Committee

European Committee of the Regions

Data Protection Notice
M365 Copilot

1. Introduction

The European Economic and Social Committee (EESC) and The European Committee of the Regions (CoR) are committed to respecting and protecting your personal data in accordance with Regulation (EU) 2018/1725 (EUDPR), which applies to the processing of personal data by M365 Copilot.

The Directorate for Innovation and Information Technology of the Joint Services of the CoR and the EESC aims to provide staff access to M365 Copilot to support their daily tasks.
Copilot only accesses data that the user can already access within Microsoft 365 applications. It cannot grant new permissions or read data from systems such as Sysper, Mima, or EVA. Responsibility for access rights lies with the data owners, while users remain accountable for responsible use of Copilot within those rights.

2. Who is responsible for the processing of personal data?

The EESC and the CoR are responsible (as joint controllers) for the processing of personal data.
The responsible directorate is DIIT, helpdesk@cor.europa.eu.

Microsoft processes data on behalf of the EESC and the CoR and thus acts as processor.

3. What is the purpose of the processing?

Microsoft 365 Copilot is an AI-powered productivity tool designed to create, summarise, and analyse user's documents, messages, and data. It can also generate drafts, analyse spreadsheet data and create presentations using natural language request.
The purpose of the use of Microsoft 365 Copilot is to enable EESC/CoR staff to perform their official duties, namely, administrative and drafting tasks more efficiently. From a business impact perspective, users receive outputs relevant to their daily work tasks, like drafting, summarizing, and answering questions; all in the context of their work within their Microsoft 365 application.

This processing is carried out in accordance with the updated Data Protection Terms introduced by the Interinstitutional Licensing Agreement (ILA 2025), implementing the corrective measures identified by the EDPS in its March 2024 Decision.

4. What is the legal basis for the processing?

The legal basis for the processing of personal data is Article 5.1.a of the EUDPR, according to which "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".

5. What personal data are processed?

Copilot processes content from Microsoft 365 applications to which the user has legitimate access, namely Outlook, Teams, SharePoint Online, OneDrive for Business, Word, Excel, PowerPoint, Loop and Viva Insights (in anonymised form). Copilot cannot access business applications such as Sysper, Mima, EVA or other administrative systems.

Owners of data in files and folders that are stored in SharePoint Online and Onedrive should always set permissions on these files and folders so that only authorised people can access them. If someone has access to a file, Copilot can also use that data to provide answers and suggestions. The owner of the data must review and adjust permissions regularly to prevent accidental sharing and keep sensitive information secure.
Broad sharing or inherited group permissions (e.g., large groups or “anyone with the link”) increases the audience able to see Copilot-derived output from those items; therefore Data Owners should apply least-privilege or need to know settings.

M365 Copilot has access to data in files and folders in SharePoint Online and OneDrive for Business. However, it does not have access to data from other business applications such as Sysper, Mima, EVA, nor to data stored in the shared folders on-premise that are typically mapped to drive letters. While certain personal data may incidentally appear in the processed materials, the objective of Copilot is to assist users in their professional tasks rather than to process personal data.
Highly sensitive files and repositories (e.g. Directorate E HR or Finance) have been excluded from SharePoint Online migration and therefore from Copilot indexing. Additional information-protection labelling will be rolled out to further limit processing of classified or confidential content.
In principle, no special categories of data, other than those used by CoR Directorate E and EESC Directorate E, being one of their shared drives that could contain personal data, will be in scope of Copilot.
In the new Information protection and governance setup, Copilot cannot access data that is labelled as "Sensitive Non Classified" or Personal.

In July of 2025, an amendment to the Interinstitutional Licensing Agreement (or ILA 2025) was signed. The purpose of this amendment is to replace the Data Protection Terms (DPTs) in light of the EDPS' Decision of 8 March 2024 on the Commission's use of M365.

This amendment clarifies that Microsoft acts as a processor for service provision and each party (both Committees) is a controller for contract management. Standard Contractual Clauses and additional obligations are included to ensure compliance with EU data protection standards. Additional details on processed data are now specified in Annex VI to the Standard Contractual Clauses (SCCs). Changes to data types require prior notification and may be objected to within 5 days, otherwise tacit approval applies.

6. Who are the recipients or categories of recipients of your personal data?

Microsoft acts as processor under the ILA 2025 and may access limited data solely to provide technical support or maintenance under strict contractual safeguards.
Within the Committees, only authorised IT administrators may access relevant data in very exceptional cases, such as incident investigations or security troubleshooting, and always under confidentiality obligations.
Copilot cannot access systems such as Sysper, Mima, or EVA, nor any other business applications outside Microsoft 365.

7. Are your personal data transferred to a third country (non-EU Member State) or international organisation?

Your personal data are stored and processed within the European Data Boundary (EDB), meaning within the EU / European Economic Area (EEA) by default.
Transfers outside the EEA are strictly limited to specific countries, relying on adequacy decisions or derogations for important reasons of public interest. Binding instructions have been issued to Microsoft and sub-processors regarding transfers. Transfer Impact Assessments (TIAs) are now required for each destination, with a clearer tiering system and reporting mechanisms. Transfers are exceptional and non-systematic; log processing is limited to exclude transfers.

8. How can you exercise your rights?

You have the right to access your personal data, to rectify any inaccurate or incomplete personal data, to restrict (under certain conditions) the processing of your personal data, to request the deletion of your personal data (if processed unlawfully) and, where applicable, the right to data portability. You have the right to object to the processing of your data on grounds relating to your particular situation, at any time.
You can direct your queries to helpdesk@cor.europa.eu (of the delegated controller). Your query will be dealt without undue delay and in any event within one month of receipt of the request.
Certain records may become temporarily inaccessible after a user leaves the institution because their mailbox is inactive. Such data remain subject to the retention policy and are deleted once the retention period expires.
That period may be extended by two further months where necessary.

You have the right of recourse to the European Data Protection Supervisor through its contact form at any time if you consider that your rights under the EUDPR have been infringed because of the processing of your personal data by the EESC or the CoR.

9. How long are your personal data kept for?

Appropriate retention policies will be defined in consultation with the user community, as one of the outcomes of the pilot project.

At present, one retention policy applies: individual (meaning one to one) chats are preserved for two years and then deleted. These chats are stored in the user's mailbox. This duration is under review and may be shortened (e.g. to six months) to align with other EU institutions and limit storage costs. When a user leaves the Committees and his mailbox contains one to one chats, these chats together with their Copilot and AI app data remain in an inactive mailbox subject to the same retention period until expiry, after which the content is permanently deleted.

10. Are personal data collected used for automated decision-making, including profiling?

The EESC and the CoR will not use your personal data to make automated decisions about you. "Automated decisions" are defined as decisions made without human intervention.

Copilot provides suggestions that always require human oversight. Outputs are advisory and cannot by themselves produce decisions affecting staff. Users are instructed to verify Copilot responses before use.

11. Will your personal data be further processed for a purpose other than that for which the data were obtained?

Your personal data will not be further processed for a different purpose.

12. Who can you contact if you have queries or complaints?

If you have any further questions about the processing of your personal data, please contact first of all the data controller, helpdesk@cor.europa.eu.

You may also contact the EESC data protection officer by using the contact form and/or contact the CoR data protection officer (data.protection@cor.europa.eu) and/or the European Data Protection Supervisor by using the relevant contact form at any time.

13. Training and Awareness

All users of M365 Copilot will receive mandatory training on responsible use of AI, data protection principles, and sensitive-data handling. This training is integrated into the Committees' broader AI Act and information-security awareness programme.

As part of the Copilot Rollout project, the Committees will offer both generic and targeted training events to all M365 Copilot users. These sessions are designed to ensure that staff understand how to use Copilot effectively and responsibly, with a focus on data protection, information security, and AI guidelines. Generic training will provide an overview of Copilot's features and best practices for everyday use, while targeted training will address specific needs and scenarios relevant to different tasks such as Content Creation, Data Insights, (Re)Search and Meetings.[i]

[i] This notice will be reviewed following the pilot phase to reflect updated retention policies, deployment of information-protection labels, and any EDPS recommendations