

Copilot for Microsoft 365

Record of ESMA activities processing personal data, based on Article 31 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Nr.	Item	Record Information
Copilot for Microsoft 365		
1	Last update of the record	03/02/2026
2	Reference number	ESMA65-955014868-13139
3	Name and contact details of controller	Controller: European Securities and Markets Authority (ESMA) Address of the controller: European Securities and Markets Authority (ESMA) 201-203 Rue de Bercy 75012 Paris France

4	ESMA area entrusted with processing	ESMA/DIT/Data & Content Systems (DCS)
5	Processors (if any)	Microsoft NV/SA
6	Name and contact details of DPO	Data Protection Officer (ESMA) dpo@esma.europa.eu
7	Name and contact details of processor (where applicable)	Microsoft NV/SA, Da Vincilaan 3 Corporate Village, 1935 Zaventem (Belgium)
8	Purpose of the processing	Microsoft Copilot for Microsoft 365 is like having a helpful assistant right inside computer apps, like Word, Excel, or Outlook. Copilot is able to support users with writing reports, creating presentations, analyzing data, or writing emails from scratch. Overall, Copilot is able to assist users in the following ways: Writing and Editing: When working on a document, Copilot can suggest ways to make the writing clearer and more professional. It can even help users find the right wording and phrasing. Data Analysis: In Excel, it can help users make sense of numbers by creating charts and summaries automatically. In other words, it is like having a data expert who can explain what the data means. Emails and Scheduling: In Outlook, Copilot can help users manage their emails by suggesting replies or organizing their schedule. It makes sure users don't miss important messages or appointments.

	Presentations: When users are putting together a PowerPoint presentation, Copilot can help them design slides and suggest content to make their presentation more engaging and effective. Copilot for Microsoft 365 accesses Microsoft 365 (personal) data stored on ESMA tenant through Microsoft Graph (which is essentially managing accesses to documents, making sure that the right users have access to the right data). The answers generated by Copilot for Microsoft 365 are produced thanks to ESMA data present in Microsoft 365 apps (please refer to question related to the categories of personal data that will be processed). Copilot for Microsoft 365 combines this content with the user's working context, such as the meeting a user is in now, the email exchanges the user had on a topic, or the chat conversations the user had last week. Copilot for Microsoft 365 uses this combination of content and context to help provide accurate, relevant, and contextual responses. Copilot for Microsoft 365 only accesses organizational data to which individual users have at least view permissions, and only the data relevant for a specific search. By using the access policies available in Microsoft 365 services, it's possible to ensure the right users or groups have the right access to the right content within ESMA. Like this, the personal data already being present in ESMA tenant of Microsoft 365, will be used by Copilot for Microsoft 365 to provide to the usage of Microsoft 365 productivity apps (such as Word, Excel, PowerPoint, Outlook, through the large language models (LLMs). This provides an intelligent assistance to the day-to-day work of ESMA users, increasing their productivity in fulfilling the mandate set out in Article 1(5) of Regulation (EU) No 1095/2010. The overall goal is to enhance the capabilities of Microsoft 365 applications by leveraging (generative) AI to provide more efficient, effective, and personalized user experiences. As such, the specific purpose of Copilot for Microsoft 365 processing of personal data is enhanced
--	---

		productivity and burden reduction – at the same time, for such purpose the use of personal data is more incidental/secondary, rather than primary purpose.
9	Description of categories of persons whose data ESMA processes and list of data categories	Categories of persons Copilot for Microsoft 365 accesses data from the same data subjects as in the case of Microsoft 365. Such categories of persons include ESMA Staff, external stakeholders, vendors, service providers and EU Citizens. Categories of data - Enablement Data: functional personal data required to use the service - Identity contact data (e.g., name, user ID, telephone numbers, encrypted passwords, authentication tokens etc.) mainly managed in Azure Active Directory, and - Content data: handled in O365 applications: Teams, SharePoint. Content data is data the user of Copilot enters him/herself (e.g., when drafting a Word file) or that are within ESMA tenant to which he/she has access to (e.g.,) emails, Teams chats, SharePoint files). This category also comprises user's prompt, which is the text that the user types or speaks to request a response from M365 Copilot and the user's response, which is the text that M365 Copilot generates or suggests based on the user's prompt or optional user feedback. Accordingly, the categories of personal data covered are any personal data (if any) reflected in the Content data and may be basic contact details (such as email addresses in Outlook) or other types of data reflected in the content data (be in the form of Word file, Teams chat etc.).
10	Time limit for keeping the data	User Context

		User context (prompt) generated by Copilot for Microsoft 365 will be cached for up to 30 questions or till the termination of the session. Content generated Where the response to a user prompt (user context) is then reflected/stored in a Microsoft 365 application (Word file, Outlook item, PowerPoint presentation, etc.) the relevant retention policies defined by ESMA for Microsoft 365 will be applicable to Copilot for Microsoft 365 generated content.
11	Recipients of the data	ESMA By using Copilot for Microsoft 365, ESMA staff (statutory and non-statutory) with a valid access to Microsoft 365 will have access to the personal data in line with their access permissions (at least read access). Microsoft There is no data storage happening in Copilot for Microsoft 365, hence Microsoft cannot access ESMA personal data via Copilot for Microsoft 365. Regarding the delivery of Microsoft 365 service as it is already the case, Microsoft can have access to ESMA personal data stored in ESMA M365 tenant, according to the authorization

		provided by ESMA via Customer Lockbox or in line with the contractual clauses. Microsoft's sub-processors could also access ESMA data as part of the service delivery for Microsoft 365. The list of Microsoft sub-processors can be found in the following link: https://api.servicetrust.microsoft.com/api/v2/downloadDocuments/6471c92a-d274-4188-914a-033aa3efb296?trk=public_post_comment-text
12	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	Copilot for Microsoft 365 follows the same principles as validated for Microsoft 365 as long as the web content plugin/ web services are not enabled. Following EU Data Residency covering Microsoft relationship with ESMA, Microsoft is committed to store and process data within EU boundaries following, so it is excluding data transfers outside the EU. According to Microsoft, this commitment includes the obligation for Microsoft to avoid remote access from a third country out of EU to ESMA data stored and processed within the EU boundaries. There is no international data transfer identified originating specifically from the use of Copilot for Microsoft 365. As mentioned above, there is no data storage happening in Copilot for Microsoft 365. Regarding the data stored in Microsoft 365 tenant, Microsoft can have access to the data in the tenant, according to the authorization provided by ESMA via Customer Lockbox or in line with the contractual clauses already in place between ESMA and Microsoft for the use of Microsoft 365.

		The data being processed in Copilot for Microsoft 365 originates from ESMA Microsoft 365 tenant (in line with the user access rights).
13	General description of security measures, where possible.	These security measures are provided by Copilot for Microsoft 365: - Data collected and stored and related to interactions with Copilot for Microsoft 365 are not used to train Large Language Models Users can access data of which they have at least view permissions (access restrictions should be defined by ESMA) - Real time abuse monitoring/Responsible AI¹ Admin can block access to web content in Copilot for Microsoft 365 - Logical isolation of customer content Physical security, background screening and multi-layered encryption strategy - BitLocker, per-file encryption, Transport Layer Security (TLS) and Internet Protocol Security (IPsec) - Implementation of ISO/IEC 27018 standard

¹ This system works by running both the input prompt and the response through pre-trained classification models that are designed to identify and block the output of harmful content without storing the content. The request/prompt will be blocked if the content is deemed inappropriate.

Please find below the description of each indicated category:

Hate and fairness-related harms refer to any content that uses pejorative or discriminatory language based on attributes like race, ethnicity, nationality, gender identity and expression, sexual orientation, religion, immigration status, ability status, personal appearance, and body size.

Fairness is concerned with making sure that AI systems treat all groups of people equitably without contributing to existing societal inequities.

Sexual content involves discussions about human reproductive organs, romantic relationships, acts portrayed in erotic or affectionate terms, pregnancy, physical sexual acts, including those portrayed as an assault or a forced act of sexual violence, prostitution, pornography, and abuse.

Violence describes language related to physical actions that are intended to harm or kill, including actions, weapons, and related entities.

Self-harm language refers to deliberate actions that are intended to injure or kill oneself.

		To consider risks related to AI, Microsoft also relies on below measures to block harmful content at LLM level: 1. Content filtering system for the Hate & Fairness, Sexual, Violence, and Self-harm categories 2. Detection for protected materials, which includes text subject to copyright and code subject to licensing restrictions Protection against jailbreak attacks
14	Information on how to exercise your rights to access, rectification, object and data portability (where applicable), including recourse right.	To exercise your Data Privacy Rights you can address your requests to the Controller at (itdpo@esma.europa.eu). a) You are entitled to access your information relating to your personal data processed by ESMA, verify its accuracy and, if necessary, correct it in case the data is inaccurate or incomplete. b) You have the right to request the erasure of your personal data, if your personal data is no longer needed for the purposes of the processing, if you withdraw your consent or if the processing operation is unlawful. c) You can ask the Data Controller to restrict the personal data processing, under certain circumstances, such as if you contest the accuracy of the processed personal data or if you are not sure if your personal data is lawfully processed. d) You may also object, on compelling legitimate grounds, to the processing of your personal data.

	e) Additionally, you may have the right to data portability which allows you to make a request to obtain the personal data that the Data Controller holds on you and to transfer it from one Data Controller to another, where technically possible. In some cases, your rights might be restricted in accordance with Article 25 of the Regulation (EU) 2018/1725. In each case, ESMA will assess whether the restriction is appropriate. The restriction should be necessary and provided by law and will continue only for as long as the reason for the restriction continues to exist. You have the right to lodge a complaint with the European Data Protection Supervisor (supervision@edps.europa.eu), if you consider that your rights under the Regulation (EU) 2018/1725 have been infringed because of the processing of your personal data by ESMA. Further information regarding your Data Privacy Rights can be found at: https://www.esma.europa.eu/about-esma/data-protection If you have additional questions or concerns, you can also contact: DPO@esma.europa.eu
--	---