

AI Explainability Statement for Copilot in Microsoft 365

The contents of this statement are a summary provided for information purposes only and are subject to change. This statement is not intended to be formally relied on in contractual documentation.

Why and how do we use Copilot?

Like many global businesses, Kantar uses Microsoft business applications in the Microsoft 365 suite. This suite has an embedded AI called Copilot.

There are three types of Copilot in Microsoft 365:

- Microsoft Copilot Chat: Primarily designed for phone/chat-based interactions, enabling users to leverage AI for various tasks directly within a Teams chat interface.
- Copilot for Microsoft 365: Provides AI-powered assistance for tasks such as drafting emails, creating documents, analyzing data, and generating presentations. This is embedded in Windows OS and Excel, PowerPoint, Word, Outlook and other applications.
- Copilot in Edge Browser: Search queries are generated from the prompt into a few words. They are transmitted to Bing via a secure connection with user and tenant identifiers removed.

More information can be found here [What Is a Copilot and How Does It Work? | Microsoft Copilot](#)

Where does the data processed by Copilot sit?

Copilot is a feature of the Microsoft 365 and Microsoft 365 is operated in Kantar's separate, encrypted environment that is not visible to or reachable by other third parties without permissions granted by Kantar. Although hosted in the Microsoft cloud, Microsoft does not ordinarily have access to Kantar's data, except where essential for support or maintaining the security and compliance of the cloud service.

Employees of Kantar might use Copilot for assistance with Microsoft tools (Excel, PowerPoint, Word, Outlook and others) and, as such, data that is historically used for the provision of the services by Kantar might be used in conjunction with Copilot. However, this data remains in an encrypted environment to which only Kantar employees will have logical access to. The data is not used for any AI training purposes nor accessible to any third parties.

Is the Copilot open (publicly available) or closed?

Copilot and Microsoft 365 is operated in a closed separate, encrypted environment that is not visible to or

reachable by other third parties. The environment is not public.

In the case of Copilot in the Edge browser, search queries are generated from the prompt into a few words and transmitted to Bing via a secure connection with user and tenant identifiers removed. Microsoft states that the queries / prompts are not shared with advertisers and are not used to train Microsoft's foundation large language models (LLMs).

What role do humans play with Copilot

Kantar uses Copilot to augment the expertise of the Kantars teams and helps them be more productive. It is not a replacement for the expertise of the people at Kantar but helps with the more administrative tasks. In terms of minimising potential negative results, this capability is a partner to, and not a replacement for human intelligence. It reduces effort but doesn't replace a human analyst's role. Kantar teams check any outputs supported by Copilot.

How is Copilot trained?

Kantar has played no part in the development of Copilot and buys it as is incorporated into Microsoft 365. Microsoft 365 Copilot uses pretrained LLM models hosted by Microsoft; it doesn't use Kantar's or customer's data to train these models. In addition, prompt data isn't used to train Copilot and is never shared with Microsoft/OpenAI or other third parties. Copilot uses a combination of Office 365 apps, Microsoft Graph and Azure Open AI to deliver the outputs.

Azure OpenAI Service is trained on OpenAI's powerful language models including o3-mini, o1, o1-mini, GPT-4o, GPT-4o mini, GPT-4 Turbo with Vision, GPT-4, GPT-3.5-Turbo, and Embeddings model series. Information by Microsoft can be found here:

[AI security for Microsoft 365 Copilot | Microsoft Learn](#)
[What is Azure OpenAI Service? - Azure AI services | Microsoft Learn](#)

Is client data used to train the Copilot?

We don't train any AI models in this product. And as stated earlier, we restrict access to data and outputs. Microsoft customers can't see our clients' data, and that data cannot be used by Microsoft or OpenAI or any other AI provider to train or improve their models.

data loss prevention (DLP), identity modernization, and security operations.

How do we ensure the integrity of data?

Kantar has a range of global IT policies covering accessibility, accuracy, security and safety of data.

Microsoft Enterprise Data Protection (EDP) is active. This includes encryption at rest and in transit, rigorous physical security controls, and data isolation between tenants.

Data is private and not used to train foundation models.

Copilot respects Kantar's identity model and permissions, inherits Kantar's sensitivity labels, applies Kantar's retention policies, supports audit of interactions, and follows Kantar's administrative settings.

Microsoft's in-built functionality is included to mitigate and manage AI Security and Copyright Risks. It helps safeguard against AI-focused risks such as harmful content and prompt injections, and provides protected material detection. More information can be found here:

[AI security for Microsoft 365 Copilot | Microsoft Learn](#)

Does Copilot make automated decisions?

Copilot at Kantar does not make automated decisions. Nevertheless, Kantar's teams are advised that they shouldn't rely solely on Copilot's responses to make decisions. We use human-in-the-loop collaborative approach to ensure consistency and accuracy of data in making decisions. More information on the training data can be found here:

[AI security for Microsoft 365 Copilot | Microsoft Learn](#)

How will we protect against threats to our systems?

The security controls for Copilot are part of a planned comprehensive security framework designed to ensure secure access, collaboration, and protection against emerging threats. This framework is divided into several key areas:

1. **AI Security Cockpit:** focuses on threat modelling, cloud security, information protection, identity modernization, and security operations
2. **Kantar Initiatives:** Kantar is working with Microsoft to cover the entire AI pipeline, from business understanding and solution design to infrastructure setup, data acquisition, analysis, AI pipeline development, evaluation, and deployment.
3. **Security Streams:** Work is ongoing focusing on cloud security, information protection and

4. **Defendable architecture:** this principle involves creating systems that can be defended against attacks, survive compromises, and adapt to changes. It includes the integration of CIS Controls, ISO Controls, NIST Controls, and NIST Special Publication 800-171 into a zero-trust architecture
5. **Logging and monitoring:** Enhanced logging and monitoring capabilities are implemented for Azure OpenAI models to ensure responsible use and compliance
6. **Microsoft Defender for APIs:** This is a security product that enhances API visibility and security

These controls will collectively help ensure that Copilot operates securely, protecting data and systems from unauthorized access and emerging threats.

How do we ensure compliance with laws?

In regard to the development of Copilot itself, compliance with laws are intrinsically connected with Microsoft Copilot's policies and commitments, which can be found here: [Data, Privacy, and Security for Microsoft 365 Copilot | Microsoft Learn](#) [Introducing the Microsoft Copilot Copyright Commitment | Microsoft Community Hub](#)

Kantar has played no part in the development of Copilot. However, Copilot went through different assessments, including:

- Privacy risk assessment
- EU AI Act risk assessment
- Security assessment

We conduct IP assessments to ensure that we can provide the results the tool produces while respecting intellectual property rights.

Otherwise, Kantar respects the provisions of any IP rights agreed in any agreements we have with clients and vendors.

Has training been provided to individuals?

Training is provided to all employees at Kantar that have the Copilot feature. Live user briefings have also been run with key audiences which are recorded and made available to reuse. Kantar also has also implemented an AI Responsible Use Policy and various guidelines.

Who can I speak to?

Please contact your local client representative at Kantar and they will help resolve queries