Data, Privacy, and Security for Microsoft 365 Copilot

Article • 01/15/2025

Microsoft 365 Copilot is a sophisticated processing and orchestration engine that provides AI-powered productivity capabilities by coordinating the following components:

- Large language models (LLMs)
- Content in Microsoft Graph, such as emails, chats, and documents that you have permission to access.
- The Microsoft 365 productivity apps that you use every day, such as Word and PowerPoint.

For an overview of how these three components work together, see Microsoft 365 Copilot overview. For links to other content related to Microsoft 365 Copilot, see Microsoft 365 Copilot documentation.

> **Important**
>
> - Microsoft 365 Copilot is compliant with our existing privacy, security, and compliance commitments to Microsoft 365 commercial customers, including the General Data Protection Regulation (GDPR) and European Union (EU) Data Boundary.
> - Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs, including those used by Microsoft 365 Copilot.
> - Microsoft 365 Copilot operates with multiple protections, which include, but aren't limited to, blocking harmful content, detecting protected material, and blocking prompt injections (jailbreak attacks).

The information in this article is intended to help provide answers to the following questions:

- How does Microsoft 365 Copilot use your proprietary organizational data?
- How does Microsoft 365 Copilot protect organizational information and data?
- What data is stored about user interactions with Microsoft 365 Copilot?
- What data residency commitments does Microsoft 365 Copilot make?
- What extensibility options are available for Microsoft 365 Copilot
- How does Microsoft 365 Copilot meet regulatory compliance requirements?

- Do privacy controls for connected experiences in Microsoft 365 Apps apply to Microsoft 365 Copilot?
- Can I trust the content that Microsoft 365 Copilot creates? Who owns that content?
- What are Microsoft's commitments to using AI responsibly?

> **Note**
>
> Microsoft 365 Copilot will continue to evolve over time with new capabilities. To keep up to date on Microsoft 365 Copilot or ask questions, visit the **Microsoft 365 Copilot community** on the Microsoft Tech Community.

How does Microsoft 365 Copilot use your proprietary organizational data?

Microsoft 365 Copilot provides value by connecting LLMs to your organizational data. Microsoft 365 Copilot accesses content and context through Microsoft Graph. It can generate responses anchored in your organizational data, such as user documents, emails, calendar, chats, meetings, and contacts. Microsoft 365 Copilot 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. Microsoft 365 Copilot uses this combination of content and context to help provide accurate, relevant, and contextual responses.

> **Important**
>
> Prompts, responses, and data accessed through Microsoft Graph aren't used to train foundation LLMs, including those used by Microsoft 365 Copilot.

Microsoft 365 Copilot only surfaces organizational data to which individual users have at least view permissions. It's important that you're using the permission models available in Microsoft 365 services, such as SharePoint, to help ensure the right users or groups have the right access to the right content within your organization. This includes permissions you give to users outside your organization through inter-tenant collaboration solutions, such as shared channels in Microsoft Teams.

When you enter prompts using Microsoft 365 Copilot, the information contained within your prompts, the data they retrieve, and the generated responses remain within the Microsoft 365 service boundary, in keeping with our current privacy, security, and

compliance commitments. Microsoft 365 Copilot uses Azure OpenAI services for processing, not OpenAI's publicly available services. Azure OpenAI doesn't cache customer content and Copilot modified prompts for Microsoft 365 Copilot. For more information, see the Data stored about user interactions with Microsoft 365 Copilot section later in this article.

> **Note**
>
> - When you're using plugins to help Microsoft 365 Copilot to provide more relevant information, check the privacy statement and terms of use of the plugin to determine how it will handle your organization's data. For more information, see **Extensibility of Microsoft 365 Copilot**.
> - When you're using the web content plugin, Microsoft 365 Copilot parses the user's prompt and identifies terms where web search would improve the quality of the response. Based on these terms, Copilot generates a search query that it sends to the Bing Search service. For more information, **Data, privacy, and security for web queries in Microsoft 365 Copilot and Microsoft 365 Copilot Chat**.

While abuse monitoring, which includes human review of content, is available in Azure OpenAI, Microsoft 365 Copilot services have opted out of it. For information about content filtering, see the How does Copilot block harmful content? section later in this article.

> **Note**
>
> We may use customer feedback, which is optional, to improve Microsoft 365 Copilot, just like we use customer feedback to improve other Microsoft 365 services and Microsoft 365 productivity apps. We don't use this feedback to train the foundation LLMs used by Microsoft 365 Copilot. Customers can manage feedback through admin controls. For more information, see **Manage Microsoft feedback for your organization** and **Providing feedback about Microsoft Copilot with Microsoft 365 apps** .

Data stored about user interactions with Microsoft 365 Copilot

When a user interacts with Microsoft 365 Copilot (using apps such as Word, PowerPoint, Excel, OneNote, Loop, or Whiteboard), we store data about these interactions. The stored data includes the user's prompt and Copilot's response, including citations to any information used to ground Copilot's response. We refer to the user's prompt and Copilot's response to that prompt as the "content of interactions" and the record of those interactions is the user's Copilot activity history. For example, this stored data provides users with Copilot activity history in Microsoft 365 Copilot Chat (previously named Business Chat) and meetings in Microsoft Teams. This data is processed and stored in alignment with contractual commitments with your organization's other content in Microsoft 365. The data is encrypted while it's stored and isn't used to train foundation LLMs, including those used by Microsoft 365 Copilot.

To view and manage this stored data, admins can use Content search or Microsoft Purview. Admins can also use Microsoft Purview to set retention policies for the data related to chat interactions with Copilot. For more information, see the following articles:

- Overview of Content search
- Microsoft Purview data security and compliance protections for generative AI apps
- Learn about retention for Copilot

For Microsoft Teams chats with Copilot, admins can also use Microsoft Teams Export APIs to view the stored data.

Deleting the history of user interactions with Microsoft 365 Copilot

Your users can delete their Copilot activity history, which includes their prompts and the responses Copilot returns, by going to the My Account portal. For more information, see Delete your Microsoft 365 Copilot activity history.

Microsoft 365 Copilot and the EU Data Boundary

Microsoft 365 Copilot calls to the LLM are routed to the closest data centers in the region, but also can call into other regions where capacity is available during high utilization periods.

For European Union (EU) users, we have additional safeguards to comply with the EU Data Boundary. EU traffic stays within the EU Data Boundary while worldwide traffic can be sent to the EU and other countries or regions for LLM processing.

Microsoft 365 Copilot and data residency

Microsoft 365 Copilot is upholding data residency commitments as outlined in the Microsoft Product Terms and Data Protection Addendum. Microsoft 365 Copilot was added as a covered workload in the data residency commitments in Microsoft Product Terms on March 1, 2024.

Microsoft Advanced Data Residency (ADR) and Multi-Geo Capabilities offerings include data residency commitments for Microsoft 365 Copilot customers as of March 1, 2024. For EU customers, Microsoft 365 Copilot is an EU Data Boundary service. Customers outside the EU may have their queries processed in the US, EU, or other regions.

Extensibility of Microsoft 365 Copilot

While Microsoft 365 Copilot is already able to use the apps and data within the Microsoft 365 ecosystem, many organizations still depend on various external tools and services for work management and collaboration. Microsoft 365 Copilot experiences can reference third-party tools and services when responding to a user's request by using Microsoft Graph connectors or plugins. Data from Graph connectors can be returned in Microsoft 365 Copilot responses if the user has permission to access that information.

When plugins are enabled, Microsoft 365 Copilot determines whether it needs to use a specific plugin to help provide a relevant response to the user. If a plugin is needed, Microsoft 365 Copilot generates a search query to send to the plugin on the user's behalf. The query is based on the user's prompt, Copilot activity history, and data the user has access to in Microsoft 365.

In the **Integrated apps** section of the Microsoft 365 admin center, admins can view the permissions and data access required by a plugin as well as the plugin's terms of use and privacy statement. Admins have full control to select which plugins are allowed in their organization. A user can only access the plugins that their admin allows and that the user installed or is assigned. Microsoft 365 Copilot only uses plugins that are turned on by the user.

For more information, see the following articles:

- Manage Plugins for Copilot in Integrated Apps
- Extend Microsoft 365 Copilot
- How Microsoft 365 Copilot can work with your external data

How does Microsoft 365 Copilot protect organizational data?

The permissions model within your Microsoft 365 tenant can help ensure that data won't unintentionally leak between users, groups, and tenants. Microsoft 365 Copilot presents only data that each individual can access using the same underlying controls for data access used in other Microsoft 365 services. Semantic Index honors the user identity-based access boundary so that the grounding process only accesses content that the current user is authorized to access. For more information, see Microsoft's privacy policy and service documentation .

When you have data that's encrypted by Microsoft Purview Information Protection, Microsoft 365 Copilot honors the usage rights granted to the user. This encryption can be applied by sensitivity labels or by restricted permissions in apps in Microsoft 365 by using Information Rights Management (IRM). For more information about using Microsoft Purview with Microsoft 365 Copilot, see Microsoft Purview data security and compliance protections for generative AI apps.

We already implement multiple forms of protection to help prevent customers from compromising Microsoft 365 services and applications or gaining unauthorized access to other tenants or the Microsoft 365 system itself. Here are some examples of those forms of protection:

- Logical isolation of customer content within each tenant for Microsoft 365 services is achieved through Microsoft Entra authorization and role-based access control. For more information, see Microsoft 365 isolation controls.
- Microsoft uses rigorous physical security, background screening, and a multi-layered encryption strategy to protect the confidentiality and integrity of customer content.
- Microsoft 365 uses service-side technologies that encrypt customer content at rest and in transit, including BitLocker, per-file encryption, Transport Layer Security (TLS), and Internet Protocol Security (IPsec). For specific details about encryption in Microsoft 365, see Encryption in the Microsoft Cloud.
- Your control over your data is reinforced by Microsoft's commitment to comply with broadly applicable privacy laws, such as the GDPR, and privacy standards, such as ISO/IEC 27018, the world's first international code of practice for cloud privacy.
- For content accessed through Microsoft 365 Copilot plugins, encryption can exclude programmatic access, thus limiting the plugin from accessing the content.

For more information, see Configure usage rights for Azure Information Protection.

Meeting regulatory compliance requirements

As regulation in the AI space evolves, Microsoft will continue to adapt and respond to fulfill future regulatory requirements.

Microsoft 365 Copilot is built on top of Microsoft's current commitments to data security and privacy in the enterprise. There's no change to these commitments. Microsoft 365 Copilot is integrated into Microsoft 365 and adheres to all existing privacy, security, and compliance commitments to Microsoft 365 commercial customers. For more information, see Microsoft Compliance.

Beyond adhering to regulations, we prioritize an open dialogue with our customers, partners, and regulatory authorities to better understand and address concerns, thereby fostering an environment of trust and cooperation. We acknowledge that privacy, security, and transparency aren't just features, but prerequisites in the AI-driven landscape at Microsoft.

Additional information

Microsoft 365 Copilot and privacy controls for connected experiences

Some privacy controls for connected experiences in Microsoft 365 Apps can affect the availability of Microsoft 365 Copilot features. This includes the privacy controls for connected experiences that analyze your content and the privacy control for optional connected experiences. For more information about these privacy controls, see Overview of privacy controls for Microsoft 365 Apps for enterprise.

Privacy control for connected experiences that analyze your content

If you turn off connected experiences that analyze your content on devices in your organization, Microsoft 365 Copilot features won't be available to your users in the following apps:

- Excel
- OneNote
- Outlook

- PowerPoint
- Word

This applies to when you're running the most current version of these apps on Windows, Mac, iOS, or Android devices.

There's also a privacy control that turns off all connected experiences, including connected experiences that analyze your content. If you use that privacy control, Microsoft 365 Copilot features won't be available in the apps and on the devices described above.

Privacy control for optional connected experiences

If you turn off optional connected experiences in your organization, Microsoft 365 Copilot features that are optional connected experiences won't be available to your users. For example, turning off optional connected experiences could affect the availability of web search.

There's also a privacy control that turns off all connected experiences, including optional connected experiences. If you use that privacy control, Microsoft 365 Copilot features that are optional connected experiences won't be available.

About the content that Microsoft 365 Copilot creates

The responses that generative AI produces aren't guaranteed to be 100% factual. While we continue to improve responses, users should still use their judgment when reviewing the output before sending them to others. Our Microsoft 365 Copilot capabilities provide useful drafts and summaries to help you achieve more while giving you a chance to review the generated AI rather than fully automating these tasks.

We continue to improve algorithms to proactively address issues, such as misinformation and disinformation, content blocking, data safety, and preventing the promotion of harmful or discriminatory content in line with our responsible AI principles .

Microsoft doesn't claim ownership of the output of the service. That said, we don't make a determination on whether a customer's output is copyright protected or enforceable against other users. This is because generative AI systems may produce similar responses to similar prompts or queries from multiple customers. Consequently, multiple customers may have or claim rights in content that is the same or substantially similar.

If a third party sues a commercial customer for copyright infringement for using Microsoft's Copilots or the output they generate, we'll defend the customer and pay the amount of any adverse judgments or settlements that result from the lawsuit, as long as the customer used the guardrails and content filters we have built into our products. For more information, see Microsoft announces new Copilot Copyright Commitment for customers .

How does Copilot block harmful content?

Azure OpenAI Service includes a content filtering system that works alongside core models. The content filtering models for the Hate & Fairness, Sexual, Violence, and Self-harm categories have been specifically trained and tested in various languages. This system works by running both the input prompt and the response through classification models that are designed to identify and block the output of harmful content.

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.

Learn more about Azure OpenAI content filtering.

Does Copilot provide protected material detection?

Yes, Microsoft 365 Copilot provides detection for protected materials, which includes text subject to copyright and code subject to licensing restrictions. Not all of these mitigations are relevant for all Microsoft 365 Copilot scenarios.

Does Copilot block prompt injections (jailbreak attacks)?

Jailbreak attacks are user prompts that are designed to provoke the generative AI model into behaving in ways it was trained not to or breaking the rules it's been told to follow.

Microsoft 365 Copilot is designed to protect against prompt injection attacks. Learn more about jailbreak attacks and how to use Azure AI Content Safety to detect them.

Committed to responsible AI

As AI is poised to transform our lives, we must collectively define new rules, norms, and practices for the use and impact of this technology. Microsoft has been on a Responsible AI journey since 2017, when we defined our principles and approach to ensuring this technology is used in a way that is driven by ethical principles that put people first.

At Microsoft, we're guided by our AI principles , our Responsible AI Standard , and decades of research on AI, grounding, and privacy-preserving machine learning. A multidisciplinary team of researchers, engineers, and policy experts reviews our AI systems for potential harms and mitigations — refining training data, filtering to limit harmful content, query- and result-blocking sensitive topics, and applying Microsoft technologies like InterpretML and Fairlearn to help detect and correct data bias. We make it clear how the system makes decisions by noting limitations, linking to sources, and prompting users to review, fact-check, and adjust content based on subject-matter expertise. For more information, see Governing AI: A Blueprint for the Future .

We aim to help our customers use our AI products responsibly, sharing our learnings, and building trust-based partnerships. For these new services, we want to provide our customers with information about the intended uses, capabilities, and limitations of our AI platform service, so they have the knowledge necessary to make responsible deployment choices. We also share resources and templates with developers inside organizations and with independent software vendors (ISVs), to help them build effective, safe, and transparent AI solutions.

Related articles

- Microsoft 365 Copilot requirements
- Get started with Microsoft 365 Copilot
- Microsoft 365 Copilot adoption site

Feedback