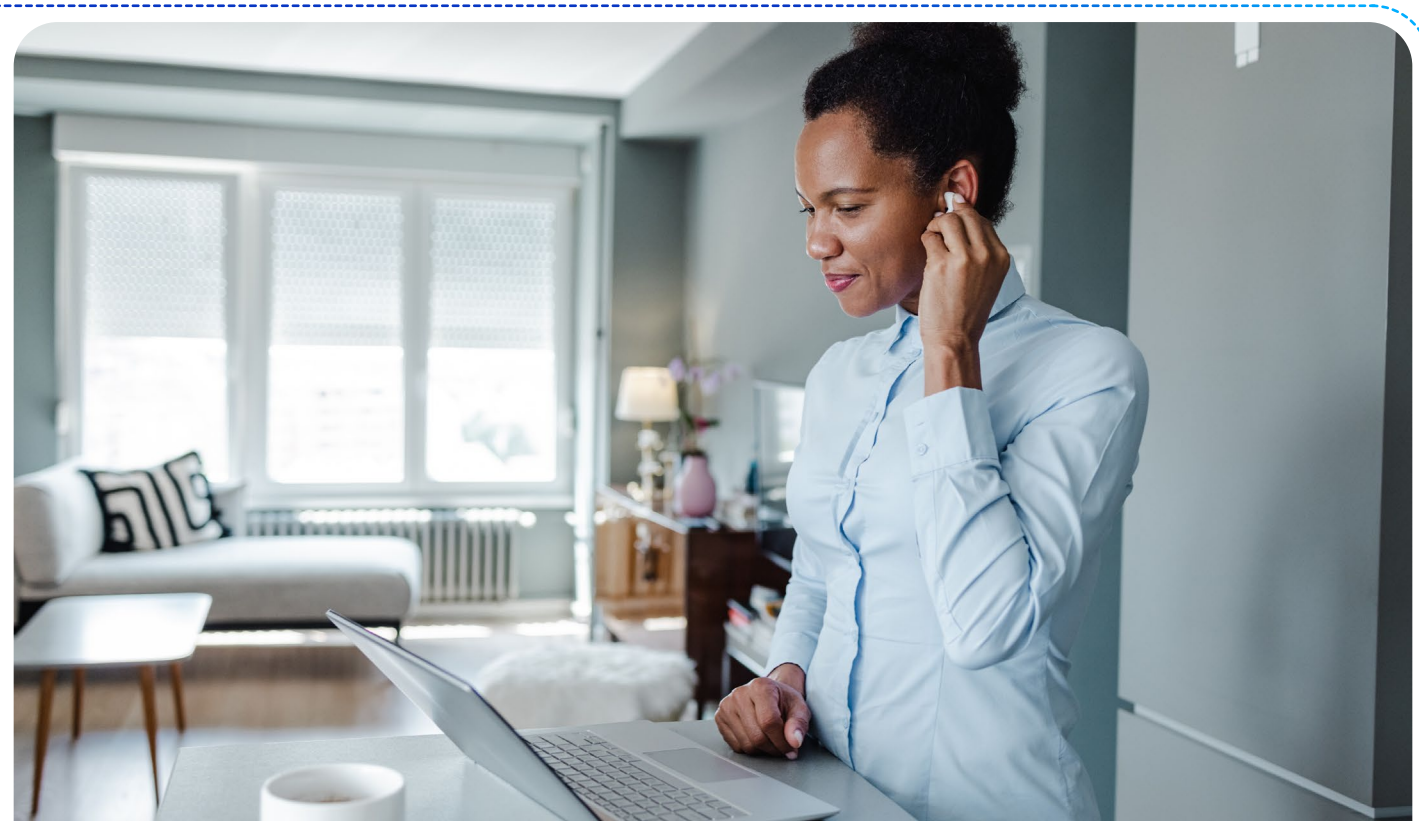
Microsoft

Transcription Management in Microsoft 365 Copilot

Discover the comprehensive access, governance, and privacy controls Microsoft offers to help you manage your transcription and recording data



Executive summary

This paper provides an overview of the various controls Microsoft provides to help you unlock the value of transcription with Microsoft 365 Copilot, a generative AI tool that provides intelligent assistance for meetings, documents, and tasks.

It explains how Copilot integrates with transcription and recording capabilities in Microsoft Teams to enhance collaboration and productivity, and outlines Microsoft's approach to managing transcription and recording data in a secure and compliant way, through application of controls for access, governance, and privacy.

Important product scope note

For this document, where "Copilot" is referenced, we are referring to Microsoft 365 Copilot. This does not include Microsoft Copilot for Sales, Microsoft Copilot for Service, Microsoft Copilot for Finance, Microsoft Copilot for Azure, Microsoft Copilot for Microsoft Security, Microsoft Copilot for Dynamics 365, or other copilots outside of Microsoft 365.

Contents

Using Copilot in the context of meetings has a measurable impact on productivity. In a study of the Microsoft 365 Copilot Early Access Program, participants found they were able to catch up on a missed meeting nearly 4x faster with Copilot than without, 84% said Copilot made it easier to take action after a meeting, and 58% found the task of summarizing meetings to be less draining.[1]

Securing sensitive data in the AI era

Collaboration matters. It helps teams spark ideas, solve problems, and strengthen connections—but it can also be a drain on productivity. Employees spend well over half their time in meetings, chat conversations, and processing email. And they see inefficient meetings as their top productivity disruptor.[2]

At Microsoft, we've found that Microsoft 365 Copilot makes meetings more effective by combining the power of AI with your transcriptions and recordings to provide real-time intelligent assistance that supercharges collaboration, and lets you dynamically interact with the digital record after a meeting so you can catch up more quickly.

While the transformative capabilities of Copilot are immense, the adoption of such powerful technology highlights for many organizations—Microsoft included—security and governance concerns that have existed as long as there has been data. Concerns such as data oversharing, preservation and deletion of records, and compliance with regulatory requirements.

Copilot mitigates these concerns by operating within the context of the user—so it only generates responses using information currently available to that user. Further, Copilot is built on Microsoft's current commitments to data security and privacy in the enterprise, and adheres to all existing privacy, security, and compliance commitments to Microsoft 365 commercial customers. This means that:

- **You're in control of your data, prompts, responses.**
- **Data accessed through Microsoft Graph aren't used to train foundation LLMs.**
- **Your data is protected at every step by the most comprehensive compliance and security controls in the industry.**

To learn more about the built-in tools available to manage your transcription data, read on.

The tremendous power of Copilot comes from its ability to not only find information, but to provide relevant information. It's able to deliver this level of intelligence by accessing content and context through Microsoft Graph, such as documents, emails, and chats that you have permission to access. When Microsoft Teams meetings are recorded or transcribed, their data is added to your organization's Microsoft Graph for subsequent use by meeting attendees with Copilot.

Copilot can then generate responses anchored in your organizational data—such as user documents, emails, calendar, chats, meetings, and contacts—and combined with your working context, such as the meeting you're currently in, emails you've exchanged on the topic, or previous chat conversations. It's this combination of content and context that helps Copilot provide accurate, relevant, and timely responses.

Managing your transcription data

Microsoft's solution for transcription management includes built-in tools for controlling:

- **Access** over who can capture data and view, share, edit, and delete artifacts after capture.
- **Governance** over how the captured artifacts are managed throughout their lifespan.
- **Privacy** of the participants recorded in those artifacts.

Adjusting the level of restriction across these three categories of access, governance, and privacy allows you to manage your transcription data in the way that makes the most sense for your business.

To implement these controls effectively, you'll first need to define your organization's goals and policies for transcription management. At Microsoft, we've engaged stakeholders across IT, legal, corporate security, privacy, the company's data custodians, and internal users to develop policies that support empowering experiences for employees while keeping the company safe. These policies represent a mix of technical defaults, meeting options, and employee empowerment to make informed decisions about usefulness and privacy. You can learn more about our approach in the Inside Track article, "Empowering employees after the call: Enabling and securing Microsoft Teams meeting data retention at Microsoft."

Ours is just one example of how data management policy can be crafted and implemented. Every organization's situation is unique, so it's important that you consult with your relevant stakeholders to craft your own policies. Useful questions to consider include:

- When should a meeting be recorded and when should it not?
- What kind of meeting data gets stored?
- Who can initiate recording, and who can access it after the meeting?
- How do we inform attendees that a meeting may be recorded?
- How do we support attendee privacy?
- How long should we retain meeting data?
- Where does the data live while it's retained?
- What does this mean for eDiscovery?

In the following section we'll take a deep dive into the Access, Governance, and Privacy controls Microsoft offers to enact your answers to these questions.

Once you've established your policies, be sure to communicate them across the organization as part of your Copilot roll-out.

You can also customize and display a link to your organization's privacy statement in the Teams meeting join experience to ensure attendees are aware of your privacy guidelines before they join a meeting.

Access controls

Some of the most important decisions that organizations make about transcription and recording include what type of data capture to allow during meetings, who can initiate capture, as well as who can get access to, modify, or delete what was captured. Microsoft provides a rich set of controls for customers to configure their implementation to their organization's needs.

Modes of transcribing and recording meetings

Teams Meetings can be recorded or transcribed in three different modes of operation, and IT admins can enable these modes on a per user basis:

1. **Record** – records video, audio, and creates a transcript of the audio.

2. **Transcribe** – uses speech-to-text processing to create a text version of what was said in the meeting. There is no temporary or permanent recording of the audio.

3. **"Copilot only during the meeting"** – provides Copilot during the meeting, but doesn't keep a transcript or a recording, and doesn't keep a record of prompts and responses from users' interactions with Copilot. For more on using Copilot only during the meeting, please refer to the Microsoft Support article, "Use Copilot without recording a Teams meeting".

Microsoft 365 Copilot is compatible with all three modes, but there is one important difference. Unlike with the first two modes, the last mode doesn't create a persistent recording or transcript. In this mode, there is no transcript available to the users and administrators at any point, and there is no transcript available for retention or eDiscovery.

At Microsoft we use all these modes, and we believe that they all have appropriate usage scenarios for our customers. Administrators can make all, some, or none of these available in their tenant through the admin console. To learn more about how administrators can manage transcription for Copilot, please refer to the Microsoft Learn article "Manage Copilot for Microsoft Teams meetings and events".

Initiating transcription or recording

Many organizers give everyone in the meeting a presenter role, which allows those users to start (or stop) transcription or recording. However, in sensitive and regulated scenarios such broad access to capture data on record is not appropriate. Microsoft provides multiple options to give you control over this important decision.

Brief guide to roles in Teams Meetings:

Teams meetings include the following roles:

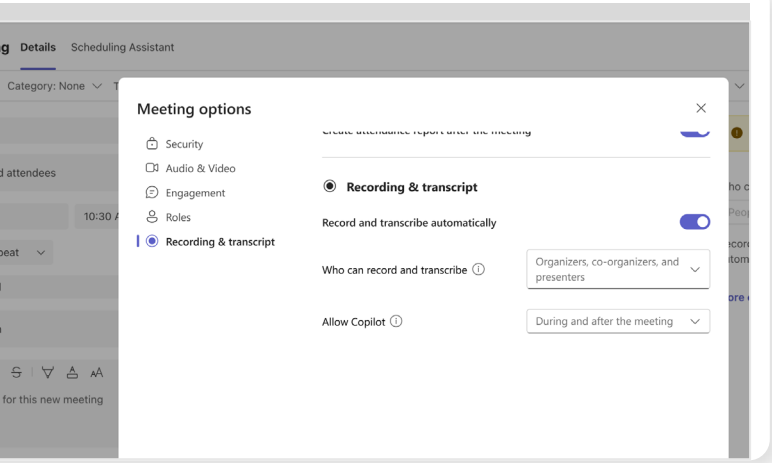
1. **Organizer/Co-Organizer – schedules the meeting, controls the settings of the meeting, can start / stop recording and transcription, and much more.**
2. **Presenter – shares many of the same rights as Organizer / Co-Organizer, but can't change meeting settings and manage breakout rooms.**
3. **Attendee – can speak, share video, and participate in meeting chat, but they can't start / stop recording or transcription.**

To learn more about differences between the roles, see "Roles in Microsoft Teams meetings".

Limit presenter access to actual presenters
Assign the attendee role to anyone who doesn't need recording rights. Meeting organizers can set participants' roles while scheduling the meeting and can also change their roles during the meeting. For more on who can record, please refer to the Microsoft Support article "Record a meeting in Microsoft Teams".

Meeting organizers can control who can record and transcribe*
As of June 2024, meeting organizers with a Teams Premium license or Copilot can select from three options for both record and transcribe while setting up the meeting:

1) Organizers and co-organizers
2) Organizers, co-organizers, and presenters (default option)
3) No one†



Controlling who can record and transcribe in a Teams meeting

In the default option, any tenant users in the presenter role will also be able to record or transcribe. While they set up the meeting, organizers can also decide whether to **record automatically** and whether to **allow Copilot only during the meeting**.

Meeting templates
Meeting templates provide a convenient way to manage multiple settings including all three recording options mentioned above: which roles can record, whether to record automatically, and whether to use Copilot with or without transcription. Templates are set up by administrators and are selected by meeting organizers to enforce a set of standards for all meetings attendees. For more information about meeting templates, please refer to the Microsoft Learn article, "Overview of custom meeting templates in Microsoft Teams."

For organizations that use Purview to protect and govern their data in Microsoft 365, **sensitivity labels** (assigned to a meeting invitation in Outlook or Teams) can also provide control over who can record. Sensitivity labels will override templates in case of a discrepancy in who can record. For more information about sensitivity labels, please refer to the Microsoft Learn article, "Use sensitivity labels to protect calendar items, Teams meetings, and chat."

Viewing, sharing, and downloading

As with the ability to capture data, Microsoft offers multiple controls over viewing, sharing, and downloading of meeting records.

Before we review the controls, it's important to note that, starting in June 2024, **recordings and transcripts are stored in the meeting organizer's OneDrive folder**, but are accessible in the Teams app, as well as in Stream. Previously, the recordings and transcripts were stored in the OneDrive folder of the participant who initiates the recording.

*Generally available for both record and transcribe as of June 2024, †New as of June 2024

View access to transcripts and recordings is managed through the following controls:

- **Meeting invitation or join is required.** Users must be members of the meeting invite list or have joined the meeting otherwise (e.g. forwarded invite or nudged into the meeting).
- **No access for external and anonymous users.** External and anonymous users don't get access to the transcript and recording.

Share access to transcripts and recordings is managed through the following control:

- **Organizer approval required** to share access to transcript or recording with internal users. There is no option to share with external users. Organizers can grant access in Stream or OneDrive.

Download access to transcripts and recordings is managed through the following controls:

- The recording owner is the only user who can download the recording. Recording owner can also grant download (and view, edit) access to specified internal users via Stream. As of June 2024, the recording owner defaults to the meeting organizer. *Note: prior to June, the recording owner defaulted to the person who initiated the recording.*
- As of June 2024, we have updated the default settings for transcripts to match that of recordings so that only the transcript file owner (meeting organizer) can download or delete the transcript in Teams client. *Note: Prior to June, all internal meeting participants/invitees could download the transcript from Teams.*
- SharePoint Advanced Management also provides an admin policy to block users from downloading recordings and meeting transcripts*. Admins can exempt people who are members of specified security groups from the policy, this allows admins to specify which users or groups should still have download access. Learn more in the Microsoft Learn article, "Block the download of Teams meeting recording files from SharePoint or OneDrive". When this policy is enabled by an admin, it cannot be overridden by meeting organizer's permissions in Stream.

Editing and deleting

Edit access to transcripts and recordings is managed through the following controls. *Note: Prior to June 2024, video ownership defaulted to the person who started the recording or transcription, but as of June 2024 defaults to the meeting organizer.*

- Only the video owner can edit the transcript in Stream.
- Only the video owner can trim the recording in Stream, which creates a customized video view with a dedicated link but preserves the original. Learn more about video trimming and hard editing in the Microsoft Support article, "How to trim videos in Stream."
- Video owners with edit permissions can grant edit access to other users.

Delete access to transcripts and recordings is managed through the following controls:

- Deletion access is limited to organizer/co-organizer and IT admin.
- Only the video owner (meeting organizer) can delete the transcript from Stream.

*New as of June 2024 for transcripts

Note: Automatic deletion policies, retention policies, and legal holds also govern deletion. Refer to the Governance Controls section of this paper for additional details.

*Note: **Channel meetings** have different access controls than non-channel meetings. The main difference is that every member of the channel gets access to view, edit, and download the recording and transcript of a channel meeting.*

Managing participant use of Copilot

Copilot provides read/view access to the information in the transcript/recording via prompts entered by meeting participants and via Intelligent Meeting Recap.

Copilot is available only to the internal tenant users licensed for Copilot. In addition, Copilot responses consider the user's permissions. In this case, users must have access to the transcript in order for contents of that transcript to be surfaced in a Copilot response.

Advanced scenario: How to limit access to meeting artifacts to specific people?

Some meetings involve a lot of participants, but require restricted access to recording, transcription, and Copilot. Scenarios include large meetings and long meetings (such as executive leadership business reviews), with multiple topics and audiences.

Under normal circumstances every internal meeting participant gets access to the transcript, recording, as well as Copilot (license required).

In June 2024, we introduced a new meeting option to provide more granular **meeting artifact access management**. This control gives Copilot and Teams Premium customers* the flexibility to manage which attendees have access to meeting artifacts such as transcript, recording, AI-generated recap, and Copilot. Meeting organizers can select from three options:

1) Everyone: Anyone with the meeting link or nudged into the meeting has access,

2) Organizer and Co-organizers: Only the people who organized the meeting have access,

3) Specific People: Besides the organizers, you can choose specific individuals to have access.

Turning the dials on access

Here are some ways organizations can use the above controls to manage access:

1) **Limit recording and transcription rights to organizers/co-organizers through meeting options.**
2) **Set up sensitivity labels that allow recording only for organizers/co-organizers.**
3) **If you don't use recording or transcription for privacy/sensitivity reasons, consider using "Copilot only during the meeting" mode to benefit from Copilot during the meeting and generate action items and summaries without leaving behind a transcript.**

*Starting June 2024 for Copilot, July 2024 for Teams Premium

Governance controls

After meeting data is captured in the form of a recording or a transcript, organizations must decide how to manage the artifacts throughout their lifecycle. This includes important decisions about where to store, how long to store, and when to delete. Since the recording and transcript are stored in OneDrive for Business, customers can take advantage of the extensive capabilities Microsoft offers to support information governance, a familiar set of controls, as well as advanced governance features of Microsoft Purview.

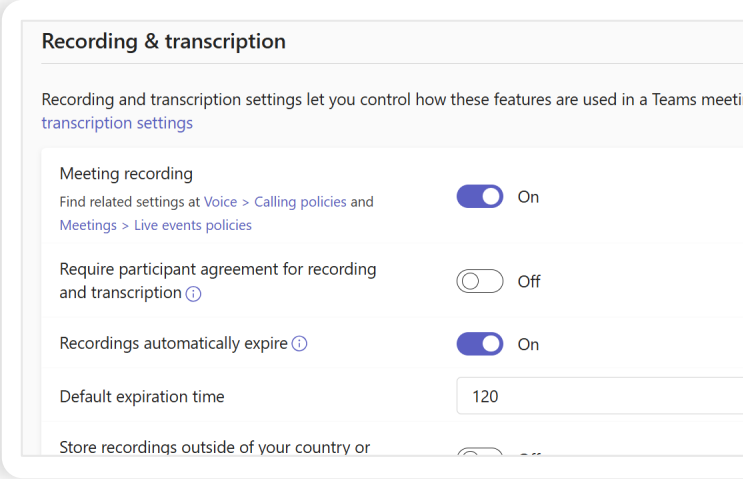
Microsoft Digital, our IT organization, created an AI Center of Excellence (CoE) bringing together experts from across the company working in several disciplines—from data science and machine learning to product development and experience design—to provide the guidance and governance we need to ensure our employees and organization are set up for success. To learn more about our approach, read the Inside Track article, "Getting the Most Out of Generative AI at Microsoft with Good Governance."

Note: None of the controls in this section apply to "Copilot only during the meeting" because the transcript isn't retained in this mode.

Retention and deletion

Retention and deletion of Teams meeting recordings and transcripts is managed through the following controls:

- **Auto-expiration of recordings**. Teams provides a default policy to retain meeting recordings for 120 days and customers are free to change this period to suit their needs. After this period ends, the records are automatically deleted. This control is designed to help manage the overall volume of stored data, which can increase quickly with multiple recordings as each hour takes up approximately 400 MB. **However, this control is not intended for compliance purposes**. Meetings organizers and co-organizers can delete a meeting prior to the expiration period. *Note: Starting in June 2024, auto-expiration will also apply to transcripts stored in OneDrive*.



Teams meeting auto-expiration settings

- **Retention and expiration compliance controls**. Customers who use Microsoft Purview can use auto-apply retention label policies (requires one of the E5/A5/G5 SKUs) to set explicit retention and expiration controls on Teams recordings and transcripts alone. To learn more about auto-applying retention labels, please refer to the Microsoft Learn article, "Automatically apply a retention label to Microsoft 365 items".

Alternatively, customers who use Microsoft Purview can use Retention policies (requires one of the SharePoint Plan 2/Microsoft 365 E5/A5/G5/E3/A3/G3, Business Premium, Microsoft 365 E5/A5/G5/F5 Compliance and F5 Security & Compliance, Microsoft 365 E5/A5/F5/G5 Information Protection and Governance, Office 365 E5/A5/G5/E3/A3/G3 SKUs) to set general file-based retention and expiration controls, which would also implicitly cover recordings and transcripts as well as regular files.

Either of the above is the recommended approach for meeting organization's compliance requirements for record retention. Configured policies supersede auto-expiration settings and user's attempts to delete files manually.

Note: The user's view of files doesn't always match the organization's. For example, if a user deletes a recording before the retention policy ends, the user won't see the file, but the file will persist in the Preservation Hold through the end of the retention period.

eDiscovery and legal holds

Legal holds are an important component of a defensible discovery process. The following controls support eDiscovery and legal holds for recordings and transcripts stored in OneDrive:

- Recordings and transcripts are available for eDiscovery using Microsoft Purview.
- Recordings and transcripts can be preserved via legal hold using Microsoft Purview.

In case of conflict, legal holds will supersede other retention and deletion policies.

For customers using third-party eDiscovery tools, Microsoft offers APIs, including Graph APIs for eDiscovery and Graph APIs to get Teams meetings recordings and transcripts.

Note: Prior to June 2024, the storage location was determined by the Preferred Data Location of the person who initiated the recording or transcription of the meeting. As of June 2024, the storage location is determined by the Preferred Data Location of the meeting organizer.

Microsoft Exchange and its role in storing artifacts

Within Copilot's architecture, Microsoft Exchange plays an important role as the place where the user's prompts and responses are stored. Exchange is also the place where the automatically generated meeting summaries and action items are stored after they are created by Copilot. A few things to know about these summaries:

- Access to the summary is limited to internal meeting participants with a Teams Premium or Copilot license.
- Summaries can't be modified.
- The retention and deletion of these automatically generated summaries is tied to the transcript/recording file for the same meeting. This associates summary retention policies and deletion with the transcript/recording's retention and deletion.

Historically Exchange also played a role in storage of recordings and transcripts. Until June 2024, recording and transcription were stored in two locations: Microsoft Exchange and OneDrive for Business, which has since become the designated storage location. This section covers controls related to the dual storage locations:

- OneDrive was previously intended as the primary storage location for information governance purposes and as of June 2024 has become the exclusive storage location.

  When a meeting organizer deletes the transcript from the Teams apps, both the Exchange copy and the OneDrive copy will be deleted. Note that manual deletions by meeting organizer are not intended to meet information governance scenarios, which are supported by Microsoft Purview.

- Customers can bulk delete Exchange copies with a bulk script provided by Microsoft. For more information and the relevant code sample, please refer to the Microsoft Learn article, "Teams meeting recording and transcript storage and permissions in OneDrive and SharePoint".

For customers who haven't already done so, Microsoft recommends using the aforementioned deletion script to remove Exchange copies of meeting and transcripts.

Advanced scenario: Compliance archives

Customers in Financial Services and other heavily regulated industries often use specialized archiving solutions that create a centralized content archive from multiple communications platforms. For such scenarios, Microsoft Teams provides an Export API (currently in Beta) function for recordings and transcripts. For more information about the Export API, please refer to the Microsoft Learn article, "Export content with the Microsoft Teams Export APIs."

Advanced scenario: Communication compliance

Many organizations need to monitor regulatory compliance (for example, SEC or FINRA) and business conduct violations such as sensitive or confidential information, harassing or threatening language, and sharing of restricted content. Microsoft Purview Communication Compliance is designed to help you detect, capture, and act on potentially inappropriate messages in your organization. For Teams, it provides these capabilities for meeting transcripts (Preview) and Microsoft 365 Copilot prompts. For more information, please refer to the Microsoft Learn article, "Learn about communication compliance."

Turning the dials on governance

Here are a couple of ways organizations can use the above controls:

1) **Set auto expiration of Teams recordings to support your organization's needs. In most cases, meetings aren't viewed after 60 days and only a tiny portion of meetings are viewed more than 120 days after capture. Organizations looking to minimize data storage and potential exposure can set a shorter expiration schedule.**
2) **Use Microsoft Purview to set appropriate retention policies for different types of content. Purview provides the recommended set of lifecycle management controls and allows you to adjust them to the circumstances (vs. single auto-expiration period).**

Privacy controls

Whenever we discuss capture of meeting content, we also have to consider privacy of the participants. Organizations need to consider whether to simply inform the participants that recording is taking place or to request explicit consent. In some circumstances, attendees may want to participate but may not want their contributions directly attributed. Data residency is another consideration for many organizations as they evaluate privacy implications of a new technology service.

Notification

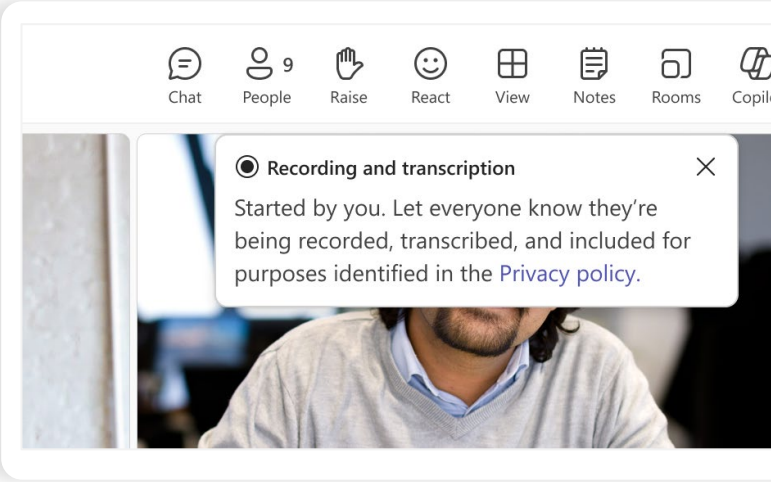
The following automated notifications help inform attendees that data recording or transcription is taking place:

- Notification prompt that recording or transcription has been initiated. This prompt is presented automatically to all meeting participants, as soon as recording or transcription starts.
- Notification prompt that Copilot "Only during the meeting" has been initiated. This prompt shows automatically to meeting participants.

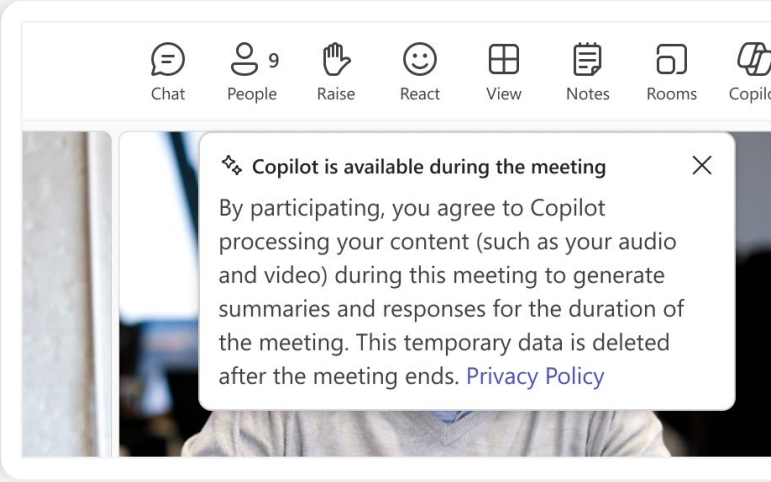
Administrators can also make use of the following optional control:

- Optional control enabling administrators to include a privacy policy link inside the notification prompt. Once set up, this control will apply to all recorded or transcribed meetings in the tenant.

Collectively, these notifications enable organizations to inform their users that meeting discussion is being captured either in a persistent manner (recording/transcription) or temporarily for the duration of the meeting (Copilot only during the meeting).



Notification that recording and transcription have started, with privacy policy link



Notification that Copilot only during the meeting has been initiated, with privacy policy link

Best practice: recommend that meeting organizers "tell and confirm" before initiating a recording.

Consent

In certain cases, an organization may need to go beyond notification for recording and transcription of their meeting participants. In such scenarios, starting in June 2024, we offer an additional administrator control to capture participants' **explicit consent** to process their audio, video and screen sharing content. The consent control covers all three modes of operation:

- Explicit consent to be recorded.
- Explicit consent to be transcribed.
- Explicit consent for Copilot only during the meeting.

Explicit consent is first configured by the administrator by assigning the consent policy to the relevant users in their tenant.

On the participant side, explicit consent works the same way across all modes. Each meeting participant, assigned to the consent policy, is presented with a prompt requesting their explicit consent for their participation in the meeting to be recorded or transcribed. If the participant consents, they will be able to participate in the meeting according to their permissions. If they decline, their participation will be limited to muted observation—their microphone will be muted and their video will not display to other participants. For more information on managing explicit consent, please refer to the Microsoft Learn article, "Require participant agreement for recording and transcription".

Attribution

In some circumstances, meeting participants may want to participate in a meeting while maintaining some degree of anonymity in the transcript about what they said, when they joined, and when they departed the meeting.

Teams meetings have **no join/leave timestamps in transcripts**, providing a degree of anonymity from other meeting participants. This is built into Teams and requires no action for administrators and meeting organizers. *Note: Meeting organizers have access to attendance reports that show join and leave times.*

Transcript attribution opt-out allows users to remove their name from the transcript. This control applies to all meetings in which the user participates. *Note: There are some inherent limitations to the degree of anonymity provided by this control in meetings that are recorded—for example, a participant's identity can be deduced from the attendance reports, which are available to the meeting organizer during and after the meeting. Meeting organizers can allow participants to opt out of sharing their attendance information, however this applies only to the post-meeting report. For more information on meeting policies, please refer to the Microsoft Learn article, "Teams settings and policies reference".*

Data residency

Many organizations consider data location as a part of privacy considerations. The storage location of recording and transcript is automatically determined based on the meeting organizer's Preferred Data Location.

Organizations with the **Microsoft 365 Multi-Geo Capabilities add-on** can manage data-at-rest locations at a granular level for their users, SharePoint sites, Microsoft 365 Groups, and Microsoft Teams team level to satisfy their data residency requirements.

Without Multi-Geo Capabilities, the Preferred Data Location is determined by the country/region selected during tenant creation and cannot be changed.

Turning the dials on privacy

Here are some ways organizations can use the above controls to manage privacy:

1) **Turn on notification prompts any time recording, transcription, or Copilot transcription is initiated.**
2) **Include a link to your organization's privacy policy in the notification prompt.**
3) **If appropriate, require consent from meeting participants. This control involves more change management than the rest and may result in missing participation of some users as they learn to respond to consent requests.**

Get started

Generative AI is already being woven into the workplace at an unexpected scale. Three out of four knowledge workers are already using AI at work today, and report that it helps them save time (90%), focus on their most important work (85%), be more creative (84%), and enjoy their work more (83%). [3]

Microsoft 365 Copilot combines the power of generative AI with your organization's data to enhance efficiency, foster innovation, and boost productivity across your entire organization. With meeting transcription enabled, the intelligence of Copilot is unlocked to deliver contextual information both during and about your meetings.

Built on the foundation of Microsoft's comprehensive approach to security, compliance, privacy and responsible AI, Copilot is the only enterprise-ready generative AI that inherits your security, compliance and privacy controls. Its robust management tools empower you to customize controls to protect sensitive data and govern usage to meet the unique needs of your organization.

With a firm grasp of the technology and close collaboration with the right stakeholders, you can guide your own policy decisions and unlock the value of generative AI for your business.

Further reading

Here are some additional resources to help you on your AI journey:

- Microsoft 365 Copilot overview
- Getting the most out of generative AI at Microsoft with good governance
- Enabling and Securing Microsoft Teams Meeting Data Retention at Microsoft
- Data, Privacy, and Security for Microsoft 365 Copilot
- Empowering responsible AI practices

Microsoft's privacy commitments apply to AI

- **We keep your organization's data private.** Your data remains private when using Microsoft 365 Copilot and is governed by our applicable privacy and contractual commitments, including the commitments we make in the Microsoft's Data Protection Addendum, Microsoft's Product Terms, and the Microsoft Privacy Statement.
- **You are in control of your organization's data.** Your data is not used in undisclosed ways or without your permission.
- **Your organization's data is not shared.** Microsoft does not share your data with third parties without your permission. Your data, including the data generated through your organization's use of Microsoft 365 Copilot – such as prompts and responses – are kept private and are not disclosed to third parties.
- **Your organization's data privacy and security are protected by design.** Security and privacy are incorporated through all phases of design and implementation of Microsoft 365 Copilot. As with all our products, we provide a strong privacy and security baseline and make available additional protections that you can choose to enable. As external threats evolve, we will continue to advance our solutions and offerings to ensure world-class privacy and security in Microsoft 365 Copilot, and we will continue to be transparent about our approach.
- **Your organization's data is not used to train foundation models.** Microsoft's generative AI solutions, including Microsoft 365 Copilot services and capabilities, do not use your organization's data to train foundation models without your permission. Your data is not available to OpenAI or used to train OpenAI models.
- **Our products and solutions continue to comply with global data protection regulations.** The Microsoft AI products and solutions you deploy continue to be compliant with today's global data protection and privacy regulations. As we continue to navigate the future of AI together, organizations can be certain that Microsoft will be transparent about our privacy, safety, and security practices. We will comply with laws globally that govern AI, and back up our promises with clear contractual commitments.
- **Your access control and enterprise policies are maintained.** To protect privacy within your organization when using enterprise products with generative AI capabilities, your existing permissions and access controls will continue to apply to ensure that your organization's data is displayed only to those users to whom you have given appropriate permissions.

The power of Copilot with transcription

Copilot with transcription unlocks	Copilot only during the meeting
Enhanced Productivity: Transcriptions allow users to quickly recap information, remember key points from discussions, and identify action items.	Users can only access specific details or decisions made during the meeting. Content is not available after the meeting.
Searchability: Stored transcripts make it easier to search for specific information discussed in meetings.	Users can only access specific details or decisions made during the meeting. Content is not available after the meeting.
Knowledge Management: Transcription turns conversations into searchable, manageable data, boosting knowledge retention and accessibility.	Conversations no longer become searchable data for recall on given topics, losing valuable knowledge across the organization.
Collaboration and Inclusivity: Transcription fosters inclusivity and better collaboration, especially in a global workforce with diverse language needs.	Global colleagues have a limited ability to access meeting details and interact with their peers.
Data-Driven Insights: Transcripts serve as a source for AI to understand meeting content, enabling it to provide more accurate and relevant assistance.	Copilot is unable to provide the most up to date and accurate information based on meetings and conversations.
Compliance and Record-Keeping: Having a transcript can be beneficial for compliance purposes, as it provides a verifiable record of the discussions that took place.	Organizations may face challenges in keeping track of important decisions and discussions, potentially leading to compliance risks.
Training and Onboarding: Transcriptions can be valuable resources for onboarding new employees or training team members.	New hires may have to rely on secondhand information or miss out on valuable insights shared during meetings.

Microsoft

[1]What Can Copilot's Earliest Users Teach Us About Generative AI at Work? Work Trend Index Special Report by Microsoft, November 2023

[2]Microsoft 2023 Work Trend Index: Annual Report by Edelman Data x Intelligence, May 2023

[3]2024 Work Trend Index Annual Report from Microsoft and LinkedIn by Edelman Data x Intelligence and LinkedIn Economic Graph Research Institute, May 2024