

Copilot Chat übernimmt längere Aufgaben, fragt aber vor sensiblen Aktionen nach

Dein Chatbot bekommt Hände. Zeit, ihm zu sagen, was er anfassen darf.

Executive Summary

Copilot Chat war bisher der Kollege, der auf jede Frage eine wohlformulierte Antwort hat und dann zufrieden zurück in die Kaffeeküche schlendert. Erledigt hat er nichts. Damit ist jetzt Schluss. Mit der Message-Center-Meldung MC1479277 (veröffentlicht am 25. September, aktualisiert am 12. Oktober 2026) kündigt Microsoft an, dass Chat in der Microsoft-365-Copilot-App **mehrstufige, länger laufende Aufgaben** übernimmt: E-Mails entwerfen, Besprechungen verwalten, in Teams, OneDrive und SharePoint arbeiten, Personen suchen und Word-, Excel-, PowerPoint-, PDF- und HTML-Dateien erzeugen.

Der eingebaute Sicherheitsgurt: Bevor Copilot etwas **Sensibles** tut, also etwa eine Mail verschickt oder einen Termin umwirft, fragt er dich um Erlaubnis. Laufende Aufgaben siehst du in einer eigenen **Tasks-Ansicht** oben rechts. Ausgerollt wird zuerst im **Frontier-Programm**, Microsofts Early-Access-Spielwiese, und zwar später im Oktober. Voraussetzung ist eine **Microsoft-365-Copilot-Lizenz**. Der kostenlose Copilot Chat aus den Business-Plänen bekommt die neuen Hände also nicht automatisch.

Parallel baut Microsoft die App um: Die neue Startseite „Home“ vereint Chat und Cowork in einem Eingabefeld, dazu kommen Code, Autopilot (vormals „Scout“) und Office direkt in der Copilot-App. Mehrere dieser Bausteine laufen über **nutzungsbasierte Abrechnung** mit Copilot-Credits und brauchen eine Ausgaberichtlinie.

i FAKTEN: Das Wichtigste in 30 Sekunden

- Chat erledigt mehrstufige Aufgaben über Outlook, Teams, OneDrive, SharePoint und Office-Dateien hinweg.
- Sensible Aktionen brauchen deine ausdrückliche Zustimmung.
- Start: Frontier, später im Oktober 2026, nur mit Microsoft-365-Copilot-Lizenz.
- Cowork, Code und Autopilot: nutzungsbasiert, nur mit Ausgaberichtlinie.
- Copilot nutzt ausschließlich Inhalte, die der Nutzer ohnehin sehen darf. Genau das ist das Problem.

Die Kurzfassung für die Geschäftsleitung: Die Technik kommt, ob du willst oder nicht. Die eigentliche Frage lautet, ob dein Berechtigungskonzept den Besuch eines fleißigen, nie müden Agenten überlebt. Plane jetzt Pilotgruppe, Governance und Kostenrahmen, bevor die Funktion bei allen aufschlägt.

Worum geht es im Detail?

Vom Auskunftsschalter zum Sachbearbeiter

Um die Neuerung zu verstehen, lohnt ein Blick zurück. Microsoft hat bislang sauber getrennt: **Chat** war das Frage-Antwort-Werkzeug, **Cowork** die agentische Variante. Cowork landete im März 2026 im Frontier-Programm, zunächst nur für Kunden mit Microsoft 365 Copilot (Premium), nur auf Englisch und auf Basis von Anthropic-Modellen. Cowork baut aus einem Ziel in natürlicher Sprache einen mehrstufigen Plan, arbeitet ihn über Word, PowerPoint und Outlook hinweg ab und zeigt den Fortschritt über Checkpoints an. Schon dort galt: Vor dem Senden von E-Mails oder Teams-Nachrichten, vor dem Planen, Absagen oder Verschieben von Meetings und vor dem Bearbeiten oder Verschieben von Dateien wird gefragt.

Genau dieses Prinzip wandert jetzt in den normalen Chat. Auf der neuen Home-Seite tippst du in ein einziges Eingabefeld und schaltest zwischen Chat und Cowork um. Die bisherigen Einstiege „Agents“ und „Customize“ weichen einem Bereich namens „Plugins“, die Cowork-Automations ziehen in die Home-Navigation um. Researcher und Analyst sind nicht mehr standardmäßig angeheftet, Admins können sie aber über das Microsoft 365 Admin Center wieder festpinnen. Wer seine Anwender gerade mühsam auf die alte Oberfläche geschult hat, darf an dieser Stelle kurz und leise weinen.

Was „mehrstufig“ konkret bedeutet

Stell dir vor, du schreibst: „Bereite das Quartalsgespräch mit dem Vertrieb Süd vor.“ Früher bekamst du eine hübsche Checkliste, was du alles tun solltest. Jetzt sucht Copilot die beteiligten Personen, prüft Kalender, sammelt die letzten Mails und Teams-Threads zum Thema, zieht die Umsatzdatei aus SharePoint, baut daraus eine Agenda als Word-Dokument und eine kleine PowerPoint, entwirft die Einladung und schlägt einen Termin vor. Bis hierhin läuft alles im Hintergrund. In dem Moment, in dem die Einladung tatsächlich an zwölf Leute rausgehen soll, hält Copilot an und fragt dich.

Damit du nicht im Blindflug unterwegs bist, zeigt Copilot bei der Antwort an, welche **Skills** er gerade nutzt. Dieses Feature rollt laut Microsoft im Oktober weltweit aus, ebenfalls nur mit Copilot-Lizenz. Für Administratoren ist das Gold wert, denn endlich lässt sich nachvollziehen, warum der Agent plötzlich in einer Excel-Datei herumrechnet, nach der niemand gefragt hat.

Anatomie einer Copilot-Chat-Aufgabe

Vom Auftrag bis zur Freigabe

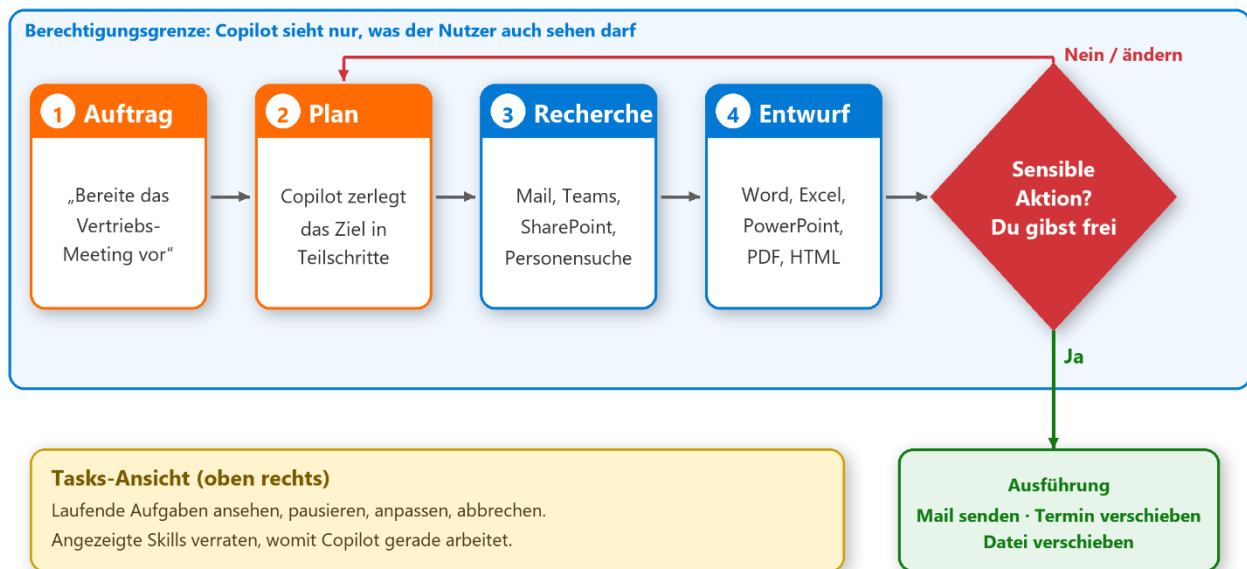


Abbildung 1: Ablauf einer mehrstufigen Aufgabe. Alles innerhalb der Berechtigungsgrenze läuft autonom, an der roten Schleuse entscheidest du.

Die Freigabe-Schleuse und warum es sie gibt

Ein Agent handelt mit deiner Identität. Wenn Copilot eine Mail verschickt, kommt sie von dir, nicht von „der KI“. Der Empfänger wird sich im Zweifel nicht über ein Sprachmodell beschweren, sondern über dich. Hinzu kommt ein technisches Grundproblem aller Agenten: Sie lesen Inhalte, die andere geschrieben haben, und können durch geschickt platzierte Anweisungen in Dokumenten oder Mails (Prompt Injection) zu Dingen verleitet werden, die du nie wolltest. Die Freigabe vor Aktionen mit Außenwirkung ist deshalb das klassische Prinzip „Human in the Loop“: Lesen und vorbereiten darf die Maschine, abdrücken darfst nur du.

Wichtig: Microsoft nennt in der Meldung zum Chat keine abschließende Liste, was als sensibel gilt. Die Cowork-Liste (Mails und Teams-Nachrichten senden, Termine planen, absagen, verschieben, Dateien bearbeiten oder verschieben) ist ein guter Anhaltspunkt, aber keine Garantie. Teste es in deinem Pilot selbst.

Lizenzen und Abrechnung: das Kleingedruckte

Hier wird es, wie immer bei Microsoft, sportlich. Der Basis-Copilot-Chat steckt in den meisten Microsoft-365-Business-Plänen. Die neuen Aufgaben-Funktionen in Chat gibt es aber nur mit einer Microsoft-365-Copilot-Lizenz. Und einige Bausteine kosten zusätzlich nach Verbrauch.

Baustein	Was er tut	Voraussetzung	Abrechnung
Chat (Aufgaben)	Mehrstufige Wissensarbeit, Freigabe vor sensiblen Aktionen	M365-Copilot-Lizenz, zuerst Frontier	Im Abo enthalten
Cowork	Plant und koordiniert Aufgaben über mehrere Apps	M365-Copilot-Lizenz, Ausgaberichtlinie	Nutzungsbasiert

Baustein	Was er tut	Voraussetzung	Abrechnung
Code	Tracker, Dashboards und Apps per Sprache	M365-Copilot-Lizenz, Ausgaberichtlinie, Beta-Kanal	Nutzungsbasiert
Autopilot (vormals Scout)	Dauerhaft aktiver persönlicher Agent mit Gedächtnis	M365-Copilot-Lizenz, Ausgaberichtlinie	Nutzungsbasiert
Office in der Copilot-App	Word, Excel, PowerPoint direkt neben Copilot	M365-Copilot-Lizenz	Über Chat im Abo, über Cowork nach Verbrauch
Copilot in SharePoint/OneDrive	Alltagsfunktionen plus neue agentische Funktionen	M365-Copilot-Lizenz, GA ab Ende Oktober	Alltag im Abo, Agentik über Credits

⚠ **WARNUNG: Die alte Einstellung verschwindet**

Die bisherige Admin-Option „Allow users to discover and use AI experiences enabled by usage-based billing“ wird entfernt. An ihre Stelle tritt eine neue Einstellung: Du legst fest, ob Nutzer ohne Ausgaberichtlinie „Zugriff anfordern“ oder nur „Mehr erfahren“ sehen, ob sie Copilot-Credits anfordern dürfen oder ob Anfragen komplett blockiert werden. Rollout: Standardkunden im Oktober, verzögerte Kunden im November. Wer sich auf den alten Schalter verlassen hat, verlässt sich gerade auf nichts.

Was sind Chancen? Was sind Risiken?

Fangen wir mit dem Positiven an, bevor die Stimmung kippt. Der größte Hebel ist nicht die einzelne Mail, sondern die **Kleinarbeit zwischen den Werkzeugen**: Informationen aus drei Postfächern, zwei Teams-Kanälen und einer SharePoint-Bibliothek zusammensuchen, daraus etwas Brauchbares bauen und an die richtigen Leute verteilen. Genau das frisst in vielen Unternehmen die halbe Woche, und genau dafür ist der neue Chat gebaut.

Chancen	Risiken
Spürbare Entlastung bei Routine: Meeting-Vorbereitung, Statusberichte, Protokolle	Oversharing wird sichtbar: Copilot findet zuverlässig, was falsch berechtigt ist
Ein Eingabefeld statt fünf Apps senkt die Einstiegshürde	Freigabe-Müdigkeit : Nach dem zwanzigsten Dialog wird geklickt wie beim Cookie-Banner
Freigabe vor Außenwirkung macht Fehler korrigierbar, bevor sie peinlich werden	Kosten : Nutzungsbasierte Bausteine ohne Budget werden zur Überraschung im Monatsabschluss
Skills-Anzeige und Tasks-Ansicht schaffen Nachvollziehbarkeit	Schnelle Oberflächenwechsel entwerten Schulungen und Dokumentation
Bessere Rendite auf bereits gekaufte Copilot-Lizenzen	Datenschutz : Bei Cowork ist Anthropic Subprozessor, für EU-Mandanten standardmäßig deaktiviert

Risiko Nummer eins: dein eigenes Berechtigungschaos

Copilot respektiert die vorhandenen Microsoft-365-Berechtigungen und nutzt nur, was der jeweilige Nutzer sehen darf. Klingt beruhigend, ist es aber nur, wenn deine Berechtigungen stimmen. Jeder Berater kennt den Klassiker: Die Gehaltsliste liegt seit 2019 in einer Teams-Site, die irgendwann für „Jeder außer externen Benutzern“ freigegeben wurde, weil der Projektleiter es eilig hatte. Bisher war das eine Zeitbombe ohne Zünder, weil niemand gesucht hat. Ein Agent, der für die Vorbereitung eines Personalgesprächs „relevante Unterlagen“ zusammenträgt, sucht. Gründlich. Und findet. Die Datei war schon immer offen, nur hat es bisher keiner gemerkt.

Risiko Nummer zwei: der Daumen auf „Genehmigen“

Die Freigabe-Schleuse schützt genau so gut, wie der Mensch davor aufpasst. Wir haben alle schon Sicherheitsdialoge weggeklickt, deren Text wir nie gelesen haben. Das Szenario ist absehbar: Freitag, 16:45 Uhr, Copilot fragt zum vierten Mal, ob er die Mail senden darf, und der Daumen ist schneller als das Gehirn. Dass die Mail die interne Kalkulation im Anhang hat und an den Kunden geht, merkt man dann am Montag. Im Gespräch mit dem Kunden. Und wahrscheinlich auch mit dem Anwalt.

! WICHTIG: Freigabe ist kein Sicherheitskonzept

Die Rückfrage vor sensiblen Aktionen ist ein Komfort- und Kontrollmerkmal, keine Data-Loss-Prevention. Vertrauliche Inhalte schützt du mit Sensitivity Labels, DLP-Richtlinien und sauberen Berechtigungen. Der Freigabe-Dialog ist die letzte Verteidigungslinie, nicht die einzige.

Risiko Nummer drei: das Budget

Microsoft verschiebt Copilot sichtbar Richtung Verbrauchsabrechnung. Cowork, Code und Autopilot laufen über Copilot-Credits, ebenso die neuen agentischen Funktionen in SharePoint und OneDrive. Ohne Ausgaberichtlinie geht nichts, mit zu großzügiger Ausgaberichtlinie geht dagegen sehr viel, vor allem Geld. Ein dauerhaft aktiver Autopilot, der für jeden Mitarbeiter im Hintergrund werkelt, ist ein Agent mit eigenem Gedächtnis und eigener Kostenstelle. Nur dass die Kostenstelle deine ist.

Was müssen wir jetzt schon vorbereiten?

Die gute Nachricht: Du hast ein kurzes Zeitfenster. Frontier bekommt die Funktion zuerst, der breite Rollout folgt in den Wochen danach. Nutze die Zeit, statt im November von den eigenen Anwendern überrascht zu werden, die „das neue Ding“ schon längst ausprobieren.

Fahrplan 2026: Microsoft liefert, du bereitest vor

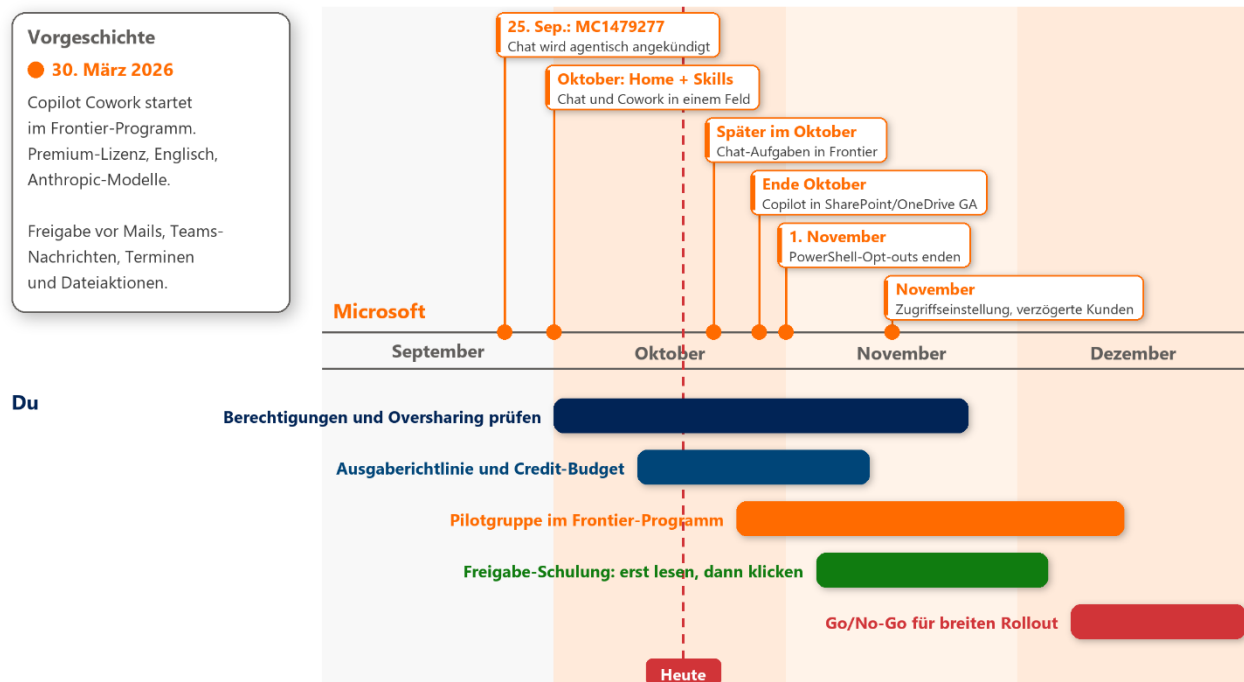


Abbildung 2: Microsoft-Meilensteine 2026 (oben) und ein realistischer Vorbereitungsplan (unten). Die rote Linie markiert den 18. Oktober.

Maßnahme	Warum	Wer
Oversharing-Check auf SharePoint- und Teams-Sites, Freigaben für „Jeder“ aufräumen	Der Agent findet alles, was falsch berechtigt ist	IT, Datenschutz, Site-Owner
Ausgaberrichtlinie unter Copilot > Cost Management anlegen, Budget pro Gruppe	Ohne Richtlinie kein Cowork, Code oder Autopilot, ohne Limit keine Kostenkontrolle	IT, Controlling
Neue Zugriffseinstellung festlegen: anfordern, informieren oder blockieren	Die alte Einstellung entfällt, der Standard passt selten	M365-Admin
Pilotgruppe im Frontier-Programm definieren	Echte Erfahrungen statt Marketingfolien	IT, Fachbereiche
Freigabe-Schulung: lesen, prüfen, erst dann genehmigen	Gegen Klick-Reflexe hilft nur Gewohnheit	IT, Personalentwicklung
Anthropic-Subprozessor für Cowork bewerten	EU-Mandanten müssen bewusst aktivieren	Datenschutz, Betriebsrat
PowerShell-Opt-outs für SharePoint-Copilot prüfen	Sie gelten nur bis zum 1. November, danach über die KI-Einstellungen der Site	SharePoint-Admin

✓ **TIPP: So setzt du die Pilotgruppe zusammen**

Nimm nicht die fünf Technikbegeisterten aus der IT, die ohnehin alles toll finden. Du brauchst eine Assistenz der Geschäftsführung mit vollem Kalender, einen Vertriebler mit chaotischem Postfach, jemanden aus dem Einkauf mit vielen Excel-Dateien und einen notorischen Skeptiker. Wenn der nach vier Wochen sagt „Na ja, ganz brauchbar“, hast du gewonnen.

Vergiss den **Betriebsrat** nicht. Ein Agent, der Kalender, Mails und Teams-Chats durchsucht und mit Gedächtnis arbeitet, berührt die Frage der Leistungs- und Verhaltenskontrolle. Wer die Mitbestimmung erst einbindet, wenn das Feature schon läuft, bekommt keinen Pilot, sondern ein Einigungsstellenverfahren. Das dauert länger als jeder Rollout.

⚠ **WARNUNG: Warte nicht auf die perfekte Doku**

Microsoft ändert Namen, Menüs und Lizenzmodelle derzeit schneller, als dein Intranet-Team Screenshots machen kann. Aus Scout wurde Autopilot, aus Agents wurde Plugins. Schreib deine Leitlinien deshalb prinzipienbasiert („Wer genehmigt, verantwortet“) und nicht klickbasiert. Klickanleitung sind bei Veröffentlichung bereits historische Dokumente.

Häufig gestellte Fragen

Brauche ich für die neuen Aufgaben in Copilot Chat eine eigene Lizenz?

Ja. Der Basis-Copilot-Chat ist in den meisten Microsoft-365-Business-Plänen enthalten, die mehrstufigen Aufgaben in Chat setzen aber eine Microsoft-365-Copilot-Lizenz voraus. Für Cowork, Code und Autopilot fällt zusätzlich nutzungsbasierte Abrechnung über Copilot-Credits an, die eine Ausgaberichtlinie erfordert.

Welche Aktionen gelten bei Copilot als sensibel und brauchen eine Freigabe?

Microsoft nennt für Chat keine abschließende Liste. Bei Cowork fragt Copilot vor dem Senden von E-Mails und Teams-Nachrichten, vor dem Planen, Absagen oder Verschieben von Meetings sowie vor dem Bearbeiten oder Verschieben von Dateien nach, was ein guter Anhaltspunkt für das Verhalten im Chat ist.

Kann Copilot Chat auf Dateien zugreifen, für die ich keine Berechtigung habe?

Nein. Copilot verwendet ausschließlich Inhalte, die der jeweilige Nutzer bereits sehen darf. Ist eine Datei aber versehentlich zu weit freigegeben, findet Copilot sie, weshalb sich vor dem Rollout eine Prüfung der SharePoint- und Teams-Berechtigungen lohnt.

Wie kann ich als Administrator steuern, ob Nutzer die kostenpflichtigen Copilot-Funktionen verwenden?

Über eine Ausgaberichtlinie unter Copilot > Cost Management im Microsoft 365 Admin Center und eine neue Einstellung, die festlegt, ob Nutzer Zugriff anfordern, nur Informationen sehen oder blockiert werden. Die alte Einstellung zu nutzungsbasierten KI-Erlebnissen entfällt dabei.

Wann ist die neue Aufgabenfunktion in Copilot Chat für alle verfügbar?

Microsoft startet später im Oktober 2026 im Frontier-Programm, dem Early-Access-Kanal für Microsoft 365 Copilot. Die breite Verfügbarkeit soll in den Wochen danach folgen, ein festes Datum für alle Mandanten hat Microsoft noch nicht genannt.