

Copilot im Oktober: Neue Frontier-Modelle in Cowork und eine Admin-Frist am 25. Oktober

Executive Summary

Der Oktober ist bei Microsoft traditionell der Monat, in dem die Blätter fallen – und mit ihnen die Standardeinstellungen, auf die du dich verlassen hast. Dieses Jahr bringt er zwei Dinge, die du auseinanderhalten solltest: ein Geschenk und eine Falle.

Das Geschenk: Im Modellpicker von Copilot Cowork stehen jetzt **Grok 4.7** von SpaceXAI, **GPT-6 Astra**, **GPT-6.1 Sol**, **Sonnet 5.5**, **Opus 5.5** und **Fable 5.1** zur Wahl. Gleichzeitig bekommen die Spending Policies die Fähigkeit, die Modellwahl zu steuern. Du kannst also künftig nicht nur festlegen, wie viele Copilot Credits jemand verbrennen darf, sondern auch, mit welchem Modell er das tut.

Die Falle: Am **Sonntag, dem 25. Oktober**, schaltet sich die neue Einstellung „**Advanced package uploads**“ automatisch ein. Ab dann dürfen Benutzer erweiterte Pakete hochladen – deklarative Agenten mit Actions und MCP-Server. Wer bis dahin nichts tut, hat trotzdem entschieden: für alle. Die Einstellung findest du im Copilot Control System ganz unten in der Liste, angekündigt im Message Center unter MC1472007.

Wichtig: Das Wichtigste in einem Satz

Bis Freitag, 23. Oktober, „Advanced package uploads“ bewusst auf „Keine“ oder „Bestimmte Gruppen“ setzen und eine Spending Policy mit Modellauswahl vorbereiten – denn am Sonntag liest niemand Mails, aber der Schalter kippt trotzdem.

Worum geht es im Detail?

Das Modellbuffet in Cowork

Zur Einordnung: Cowork ist seit Juni 2026 für alle Mandanten mit Microsoft 365 Copilot allgemein verfügbar. Es ist der Teil von Copilot, der nicht nur antwortet, sondern Aufgaben abarbeitet – Dateien bearbeiten, im lokalen Edge-Browser Webformulare ausfüllen, auf eingehende Mails reagieren, Präsentationen im Brand-Template bauen. Abgerechnet wird das seit dem GA-Start nutzungsbasiert über Copilot Credits.

Hintergrund des Modellzoos: Microsoft hat sich spätestens 2025 von der Monogamie mit OpenAI verabschiedet. Anthropic-Modelle laufen seither als Unterauftragsverarbeiter in Copilot, OpenAI ebenfalls – und jetzt kommt mit Grok 4.7 ein dritter Anbieter hinzu. Für Microsoft ist das Verhandlungsmacht, für dich ist es Auswahl. Und Auswahl ist in der IT bekanntlich das Gegenteil von Ruhe.

Modell	Anbieter	Wofür gedacht	Was du als Admin wissen musst
Auto	Cowork wählt	Standard für den Alltag	Wählt nur aus den Modellen, die du freigegeben hast
Sonnet 5.5	Anthropic	Schnelle Alltagsaufgaben, Entwürfe	Läuft über Anthropic als Unterauftragsverarbeiter
Opus 5.5	Anthropic	Komplexe Arbeit mit hohem Einsatz	Wie Sonnet: Anthropic-Familienschalter greift
Fable 5.1	Anthropic	Das Schwergewicht für ambitionierte Aufgaben	Hinweise zur Datenaufbewahrung beim Anbieter prüfen
GPT-6 Astra	OpenAI	Harte Probleme, tiefes Reasoning	OpenAI als Unterauftragsverarbeiter
GPT-6.1 Sol	OpenAI	Nachfolger der effizienten Sol-Linie	OpenAI als Unterauftragsverarbeiter
Grok 4.7	SpaceXAI	Neuzugang im Picker	Vertrags- und Datenschutzlage vor Freigabe klären

Dazu kommt die Reasoning-Stufe neben dem Modellpicker: **Light, Medium, High, Extra High und Max**. Medium ist Standard. Jede Stufe nach oben heißt: gründlicher, langsamer, teurer. Der Credit-Verbrauch hängt laut Microsoft von Modell, Kontextvolumen, Orchestrierung und genutzten Tools ab. Übersetzt: Wer Fable 5.1 auf Max stellt, um „Danke, passt so“ zu formulieren, bezahlt für eine Doktorarbeit.

Fakten: Der Anthropic-Schalter ist ein Hauptschalter

Die Anthropic-Modellfamilie lässt sich im Microsoft 365 Admin Center unter den Copilot-Einstellungen abschalten – aber nur mandantenweit. Einzelne Gruppen kannst du damit nicht freigeben. Für feinere Steuerung sind die neuen Spending Policies mit Modellauswahl das richtige Werkzeug.

Warum die Spending Policies plötzlich so wichtig werden: Bisher konntest du dort vor allem Budgets und Limits pro Benutzer oder Gruppe setzen. Jetzt kommt die Modellwahl dazu, und im vierten Quartal soll die nutzungsbasierte Abrechnung vollständig dort landen. Damit wird aus einer Finanzeinstellung ein Governance-Werkzeug. Die Rechtsabteilung bekommt das datenschutzrechtlich geprüfte Modell, die Entwicklung das starke Reasoning-Modell, und der Rest des Hauses arbeitet mit „Auto“ – ohne dass du dafür den Anthropic-Hauptschalter für alle umlegen musst.

Der Schalter ganz unten in der Liste

Jetzt zum unangenehmen Teil. „Advanced package uploads“ regelt, ob Benutzer erweiterte Pakete selbst hochladen dürfen. Gemeint sind zwei Dinge: **deklarative Agenten mit Actions**, also Agenten, die nicht nur lesen, sondern über API-Aufrufe in anderen Systemen handeln, und **MCP-Server**.

Kurz zum Hintergrund: Das Model Context Protocol wurde Ende 2024 von Anthropic als offener Standard veröffentlicht und ist inzwischen so etwas wie USB-C für KI-Agenten. Ein MCP-Server stellt einem Modell Werkzeuge und Daten zur Verfügung – Ticketsystem abfragen, Datei konvertieren, Bestellung auslösen. Das ist genial, wenn der Server von deiner IT kommt. Und es ist ein hervorragender Datenabfluss mit eingebautem Firmenlogo, wenn ihn jemand aus einem GitHub-Repo mit drei Sternen gezogen hat.

Die Optionen sind übersichtlich: alle Benutzer, keine Benutzer oder bestimmte Gruppen. Microsoft setzt den Standard am 25. Oktober auf „alle“. Das Datum ist ein Sonntag. Ob das Zufall ist, überlassen wir deiner Paranoia.

Oktober 2026: Was wann in deinem Mandanten landet



Abbildung 1: Der Oktober im Überblick – der rote Sonntag ist der einzige Termin, der dein Eingreifen verlangt.

Was sonst noch im Oktober kommt

Damit die Frist nicht allein ist, liefert Microsoft drumherum eine ganze Menge: Copilot in **SharePoint und OneDrive** ist allgemein verfügbar. Fortgeschrittene Funktionen wie Bildgenerierung, Site-Analytics-Berichte und Metadaten-Autofill in Echtzeit verbrauchen allerdings Copilot Credits. In der neuen **Plugin-Registry** im Admin Center siehst du Microsoft-, Partner- und selbst gebaute Plugins an einem Ort und kannst sie pro Gruppe steuern – in einem Beispielmandanten tauchten dort 288 Werkzeuge auf: 40 Plugins, 244 MCP-Server, drei Connectors. Mit **Authoritative Content** markierst du bis zu 100 SharePoint-Sites als verbindliche Quellen für Copilot und die Suche.

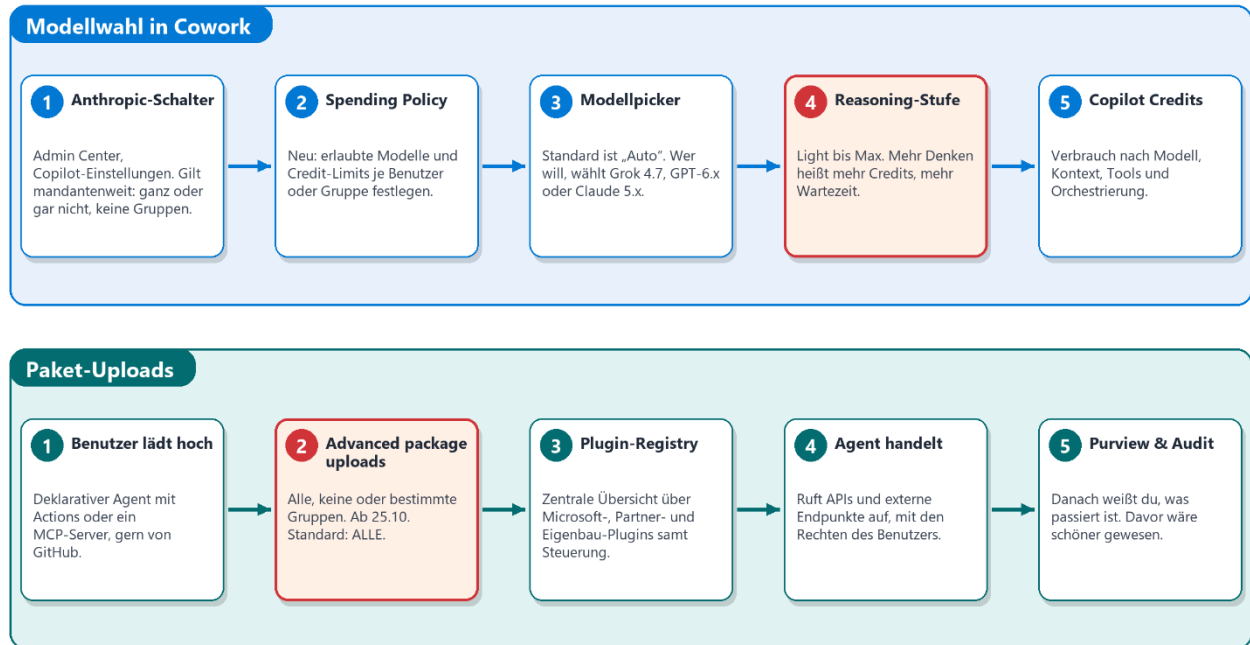
Für die Anwender ändert sich sichtbar: Der Copilot-Eintrag verschwindet Mitte bis Ende Oktober aus der Teams-Chatliste, Copilot lebt dann zentral in der linken Navigation – mit Umschalter zwischen Chat und Cowork. PowerPoint bekommt Hintergrundaufgaben und Brand-Kit-Skills, Teams Phone eine KI-Telefonzentrale. Und im vierten Quartal landet die nutzungsbasierte Abrechnung vollständig in den Spending Policies.

Was sind Chancen? Was sind Risiken?

Fangen wir freundlich an. Die Modellauswahl ist ein echter Fortschritt, weil verschiedene Aufgaben verschiedene Modelle brauchen. Ein Vertragsvergleich über 80 Seiten profitiert von Opus 5.5 oder

GPT-6 Astra auf hoher Stufe; die Zusammenfassung des Wochenmeetings braucht das nicht. Wer das steuert, bekommt bessere Ergebnisse und spart Geld. Wer es nicht steuert, bekommt eine Rechnung, deren Höhe nur noch von der Kreativität der Belegschaft begrenzt wird.

Die Türsteher: Wo du Modellwahl und Uploads kontrollierst



Rot umrandet: die Stellen, an denen ohne dein Zutun Geld oder Kontrolle abfließt.

Abbildung 2: Zwei Kontrollstrecken – oben die Modellwahl, unten die Paket-Uploads. Rot markiert, wo ohne Zutun Geld oder Kontrolle abfließt.

Chancen	Risiken
Passendes Modell pro Aufgabe statt Einheitsbrei	Credits explodieren, weil jeder „das Beste“ wählt – auf Max
Spending Policies steuern endlich auch die Modellwahl	Anthropic-Schalter nur mandantenweit, also grob wie ein Vorschlaghammer
MCP-Server und Agenten mit Actions automatisieren echte Prozesse	Ungeprüfte Pakete mit Benutzerrechten greifen auf externe Endpunkte zu
Plugin-Registry schafft erstmals zentrale Übersicht	Übersicht ohne Prozess ist nur eine schönere Liste des Chaos
Authoritative Content verbessert Antwortqualität	Falsch gepflegte „verbindliche“ Sites machen Fehler verbindlich
Mehrere Anbieter senken Abhängigkeit	Mehr Unterauftragsverarbeiter heißt mehr Dokumentationspflicht im Datenschutz

Bleibt der Neuzugang Grok 4.7. Technisch ist ein weiteres Modell im Picker nur eine Zeile mehr. Organisatorisch ist es ein weiterer Anbieter, der Prompts und Antworten deiner Belegschaft verarbeitet. Bevor du ihn freigibst, gehören Vertragslage, Datenstandort und Aufbewahrung auf

den Tisch des Datenschutzbeauftragten. Gleiches gilt für Fable 5.1, bei dem Microsoft ausdrücklich auf die Datenaufbewahrung beim Anbieter hinweist. Das ist kein Grund zur Panik, aber ein guter Grund, das Verzeichnis der Verarbeitungstätigkeiten nicht erst nach dem nächsten Audit zu aktualisieren.

Ein Fall, wie er uns so oder so ähnlich immer wieder begegnet: In einem Maschinenbauunternehmen mit rund 900 Beschäftigten hatte ein ambitionierter Werkstudent einen MCP-Server gebaut, der „mal eben“ das Ticketsystem mit Copilot verband. Funktionierte prächtig. Leider authenticizierte sich der Server mit einem Token, das er in seinem privaten Repository liegen ließ. Die IT fand es nicht durch Monitoring, sondern weil ein Dienstleister freundlich nachfragte, warum ihre Kundentickets öffentlich durchsuchbar seien. Der Werkstudent hat inzwischen seinen Abschluss. Der CISO hat inzwischen Bluthochdruck.

Warnung: Wer am 25. Oktober nichts tut, hat auch entschieden

Standard-on heißt: Jeder Benutzer darf ab dem 25. Oktober Agenten mit Actions und MCP-Server hochladen. Die Plugin-Registry zeigt dir das hinterher brav an – wie ein Rauchmelder, der erst nach dem Brand piept.

Fun Fact: Der 25. Oktober ist auch der Tag der Zeitumstellung. Du bekommst also eine Stunde extra Schlaf, bevor du merkst, dass du die Frist verpasst hast.

Zweiter Fall, diesmal aus der Abteilung Finanzen: Ein Vertriebsleiter entdeckte, dass Cowork auf Fable 5.1 mit Reasoning-Stufe Max wirklich hervorragende Angebotsentwürfe schreibt. Er erzählte es begeistert im Teamchat. Drei Wochen später erzählte der Controller etwas weniger begeistert, wie hoch der Credit-Verbrauch der Vertriebsgruppe war. Niemand hatte etwas falsch gemacht – es gab nur keine Spending Policy, die irgendetwas verhindert hätte.

Was müssen wir jetzt schon vorbereiten?

Die gute Nachricht: Das meiste ist in einer Stunde erledigt, wenn du weißt, was du willst. Die schlechte: Die Entscheidung, was du willst, dauert erfahrungsgemäß drei Meetings und einen Betriebsrat.

Nr.	Aufgabe	Wer	Bis wann
1	MC1472007 lesen, „Advanced package uploads“ im Copilot Control System suchen (ganz unten)	M365-Admin	diese Woche
2	Entscheidung treffen: Keine oder bestimmte Gruppen – und die Einstellung aktiv speichern	IT-Leitung, Security	23.10.
3	Pilotgruppe für Agenten mit Actions und MCP-Server definieren, inklusive Freigabeprozess	Security, Fachbereich	23.10.
4	Plugin-Registry sichten: Welche MCP-Server und Plugins sind schon da, wer hat sie installiert?	M365-Admin	Ende Oktober
5	Spending Policies anlegen: erlaubte Modelle und Credit-Limits je Gruppe	IT, Controlling	vor Q4-Abrechnung
6	Grok 4.7 und Fable 5.1 datenschutzrechtlich bewerten, bevor sie breit freigegeben werden	Datenschutz	vor Freigabe

Nr.	Aufgabe	Wer	Bis wann
7	Authoritative Content: bis zu 100 gepflegte SharePoint-Sites benennen	Wissensmanagement	November
8	Anwender informieren: Copilot zieht in Teams in die linke Navigation um	Change, Helpdesk	Mitte Oktober

Entscheidungsbaum für den 25. Oktober

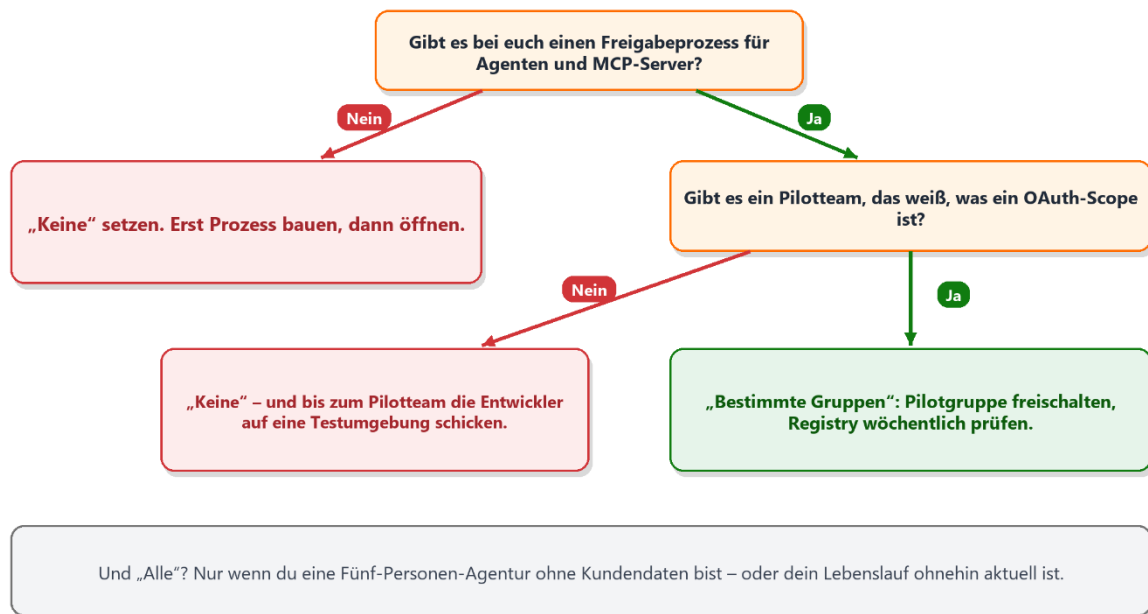


Abbildung 3: Die ehrliche Entscheidungshilfe für den 25. Oktober.

Tipp: Gruppen statt Glaubensfragen

Leg für „Advanced package uploads“ eine eigene Sicherheitsgruppe an, zum Beispiel „Copilot-Agentenbau-Pilot“, statt eine bestehende Abteilungsgruppe zu verwenden. Dann kannst du später erweitern, ohne versehentlich die ganze Entwicklung samt Praktikanten freizuschalten.

Tipp: Kosten sichtbar machen, bevor sie sichtbar werden

Stell im Pilot bewusst „Auto“ als empfohlene Einstellung ein und kommuniziere: Modell und Stufe nur hochdrehen, wenn das Ergebnis es wirklich braucht. Ein Monatsbericht über den Credit-Verbrauch je Gruppe wirkt Wunder – niemand will der Name ganz oben auf der Liste sein.

Und ein letzter Rat: Plane die Teams-Änderung nicht als Nebensache. Wenn der Copilot-Eintrag aus der Chatliste verschwindet, ruft garantiert jemand beim Helpdesk an und meldet, Copilot sei „weg“. Eine kurze Mail vorab spart zwanzig Tickets und mindestens ein Gerücht, die Geschäftsführung habe KI verboten.

Häufig gestellte Fragen

Was passiert, wenn ich „Advanced package uploads“ bis zum 25. Oktober 2026 nicht ändere?

Dann ist die Einstellung ab dem 25. Oktober automatisch für alle Benutzer aktiv. Jeder darf in Microsoft 365 Copilot deklarative Agenten mit Actions und MCP-Server hochladen, bis ein Admin die Einstellung auf „Keine“ oder bestimmte Gruppen beschränkt.

Wo finde ich die Einstellung „Advanced package uploads“ im Microsoft 365 Admin Center?

Sie liegt im Copilot Control System des Microsoft 365 Admin Centers, ganz unten in der Liste der Copilot-Einstellungen. Microsoft kündigt die Änderung im Message Center unter MC1472007 an.

Kann ich die Anthropic-Modelle in Copilot Cowork nur für bestimmte Gruppen freigeben?

Der Schalter für die Anthropic-Modellfamilie im Admin Center wirkt nur mandantenweit, also für alle oder niemanden. Für eine gruppenbezogene Steuerung der Modellwahl sind die Spending Policies gedacht, die seit Oktober 2026 auch erlaubte Modelle festlegen können.

Kostet die Nutzung von Opus 5.5, Fable 5.1 oder GPT-6 Astra in Copilot Cowork extra?

Cowork wird nutzungsbasiert über Copilot Credits abgerechnet. Der Verbrauch steigt mit leistungsfähigeren Modellen, höherer Reasoning-Stufe, größerem Kontext und mehr eingesetzten Tools, deshalb lohnt sich eine Spending Policy mit Limits je Gruppe.

Ist ein selbst hochgeladener MCP-Server in Copilot ein Sicherheitsrisiko?

Er kann eines sein, weil ein MCP-Server dem Agenten Zugriff auf Werkzeuge und Daten gibt und dabei externe Endpunkte ansprechen kann. Ohne Prüfung von Herkunft, Berechtigungen und Datenflüssen sollte ein MCP-Server deshalb nicht produktiv freigegeben werden.