

Copilot Premium bietet jetzt GPT 6.1 und Claude Opus 5.5

Executive Summary

Microsoft hat nachgelegt: Copilot bindet jetzt OpenAIs GPT 6.1 und Anthropics Claude Opus 5.5 ein, dazu Claude Sonnet 5.5 als flinkeren Bruder. Freigeschaltet wird das Ganze für Kunden mit Copilot-Premium-Abo. In der Chat-Oberfläche taucht dafür ein Modellwähler auf, und damit landet eine Frage auf deinem Tisch, die bisher bequem Microsoft für dich beantwortet hat: Welches Gehirn darf eigentlich welche Daten sehen?

Die kurze Antwort: Das ist kein Feature-Thema, sondern ein Governance-Thema. GPT 6.1 läuft bei Microsoft in Azure und bleibt in der EU Data Boundary. Die Claude-Modelle laufen bei Anthropic, das zwar inzwischen offizieller Microsoft-Subprozessor ist, aber ausdrücklich außerhalb der EU Data Boundary arbeitet. Für Tenants in EU, EFTA und Großbritannien ist Anthropic deshalb standardmäßig ausgeschaltet. Wer es einschaltet, trifft eine bewusste Datenschutzentscheidung, und die sollte nicht ein genervter Admin um 23 Uhr treffen, weil der Vertrieb drängelt.

Fakten: Das Wichtigste in drei Sätzen

GPT 6.1, Claude Opus 5.5 und Claude Sonnet 5.5 stehen in Copilot zur Wahl, Voraussetzung ist ein Premium-Abo. Anthropic-Modelle unterliegen bei normalem Betrieb den Microsoft Product Terms und dem DPA, liegen aber außerhalb der EU Data Boundary. Freischalten können nur AI-Administratoren oder globale Administratoren, und zwar gezielt für Benutzer oder Entra-ID-Sicherheitsgruppen.

Worum geht es im Detail?

Erst mal zur Begriffsverwirrung, denn Microsoft hat wieder fleißig umbenannt: Aus „Microsoft 365 Copilot“ ist „Microsoft Copilot“ geworden, aus „Copilot Chat“ wurde „Microsoft Copilot Chat“. An Sicherheit, Compliance und Datenschutz ändert die Umbenennung laut Microsoft nichts. Das kennen wir: Der Name wechselt häufiger als die Kaffeemaschine in der Teeküche, das Lizenzblatt wird trotzdem nicht kürzer. Auch bei den Modellnamen geht es in der Berichterstattung munter durcheinander, mal ist von „Claude 5.5“ die Rede, mal von GPT-6-Varianten mit Zusatznamen. Verlass dich deshalb auf das, was im Admin Center deines Tenants tatsächlich angezeigt wird.

Inhaltlich passiert Folgendes: Copilot ist nicht mehr ein Modell mit Office-Anschluss, sondern eine Orchestrierungsschicht. Sie sammelt deine Daten aus Microsoft Graph ein, prüft Berechtigungen und reicht den angereicherten Prompt an ein Sprachmodell weiter. Welches Modell das ist, kannst du jetzt wählen. In der Copilot-App zeigen UI-Hinweise an, wenn Claude im Spiel ist. In Copilot Studio wählen Agentenbauer das Modell beim Anlegen des Agenten. In Funktionen wie „Edit with Copilot“ in Word, Excel und PowerPoint oder im Researcher-Agenten können Anwender gezielt „Claude“ auswählen.

Neben den Modellen kommen frische Funktionen in den Apps: PowerPoint baut interaktive Dashboards, Timelines und Vergleichsfolien mit Schieberegler und kann wiederkehrende Formatierungsschritte als „Skill“ aufzeichnen. Excel erzeugt interaktive HTML-Dashboards und kennt Arbeitsmappenregeln für einheitliche Formatierung. Outlook bekommt eigene Anweisungen für Priorisierung und Entwürfe, und die Copilot-Einstellungen gelten künftig einheitlich für Desktop, Web und Mobil. SharePoint kann Abschnitte aus PDFs in neue Dateien extrahieren, OneDrive vereinfacht die Wiederherstellung gelöschter Dateien.

Der eigentliche Knackpunkt ist aber die Vertragslage, und die erklärt sich am besten über die Vorgeschichte. Anfangs liefen Claude-Modelle in Copilot unter Anthrups eigenen Geschäftsbedingungen und eigenem Auftragsverarbeitungsvertrag. Das war für europäische Datenschützer ungefähr so beruhigend wie ein Fallschirm mit der Aufschrift „Beta“. Inzwischen ist Anthropic offiziell Microsoft-Subprozessor. Damit gelten die Microsoft Product Terms, das Microsoft DPA, Enterprise Data Protection und sogar die Customer Copyright Commitment. Was bleibt: Die Verarbeitung findet außerhalb der EU Data Boundary statt, Zusagen zur In-Country-Verarbeitung greifen nicht.

Warum macht Microsoft das überhaupt, wo man doch Milliarden in OpenAI gesteckt hat? Weil der Konzern gelernt hat, dass eine Einbahnstraße zum Modellanbieter ein strategisches Risiko ist. Wenn ein einziger Lieferant Preis, Tempo und Qualität bestimmt, sitzt du als Plattformbetreiber am kürzeren Hebel. Mit Anthropic im Boot kann Microsoft verhandeln, vergleichen und im Zweifel umschalten. Für dich als Kunde ist das eine gute Nachricht, solange du die Weiche selbst stellst und nicht zusiehst, wie sie für dich gestellt wird. Außerhalb Europas hat Microsoft die Anthropic-Modelle übrigens schon im Januar 2026 standardmäßig eingeschaltet. In Europa hat die EU-Datengrenze das verhindert, und das ist ausnahmsweise mal ein Fall, in dem Regulierung dir Bedenkzeit schenkt statt Arbeit.

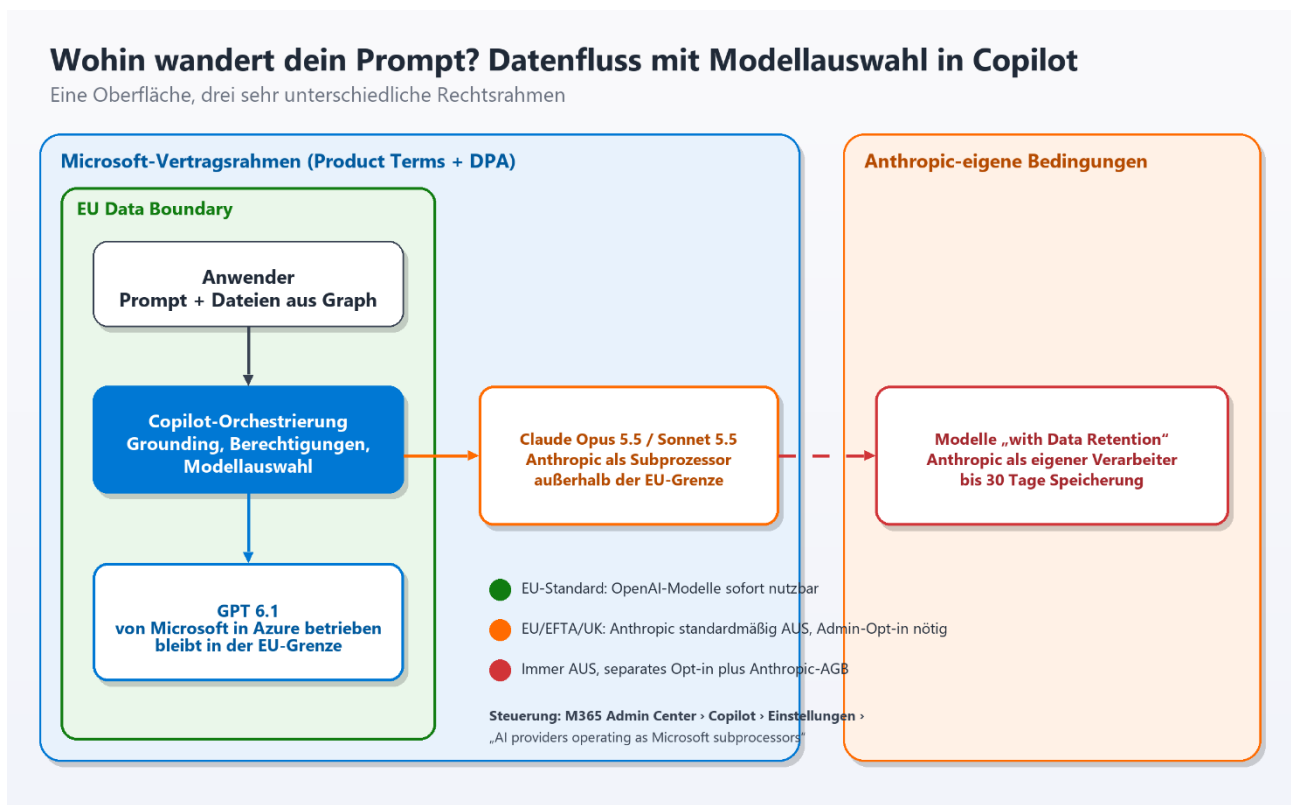


Abbildung 1: Ein Klick im Modellwähler entscheidet, in welchem Rechtsrahmen dein Prompt landet.

Und dann gibt es noch eine dritte Schublade, die du kennen musst: „Anthropic models with Data Retention“. Das sind besonders leistungsfähige Modelle, bei denen Anthropic Daten selbst speichert. Hier agiert Anthropic als eigenständiger Verarbeiter, es gelten Anthropics Bedingungen, nicht dein Microsoft-Vertrag. Eingaben und Ausgaben werden bis zu 30 Tage gespeichert, bei Verdacht auf Richtlinienverstöße Inhalte bis zu zwei Jahre und Klassifizierungswerte bis zu sieben Jahre. Diese Modelle sind überall standardmäßig aus und brauchen ein separates Opt-in.

Kriterium	GPT 6.1	Claude Opus 5.5 / Sonnet 5.5	Modelle mit Data Retention
Betrieb	Microsoft (Azure)	Anthropic als Microsoft-Subprozessor	Anthropic als eigenständiger Verarbeiter
Vertragsrahmen	Product Terms + DPA	Product Terms + DPA	Anthropic-AGB + Anthropic-DPA
EU Data Boundary	Ja	Nein	Nein
Standard in EU/EFTA/UK	An	Aus („No users“)	Aus, überall
Datenspeicherung beim Anbieter	Nach Microsoft-Regeln	Nach Microsoft-Regeln	Bis 30 Tage, Sonderfälle länger
Steuerbar per Gruppe	Über Copilot-Lizenz	Ja, Benutzer oder Entra-ID-Gruppen	Ja, separat

Wie Claude in Copilot einzog – in fünf Etappen

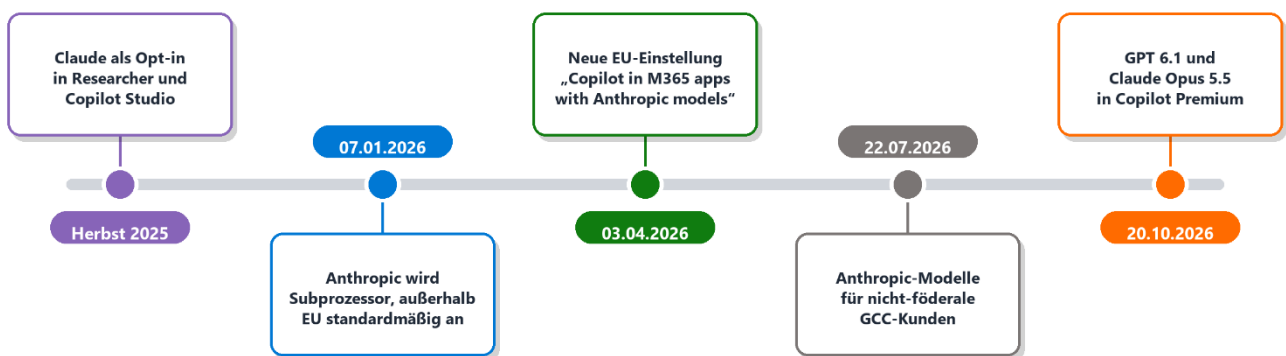


Abbildung 2: Vom vorsichtigen Opt-in zum Modellwähler im Premium-Abo.

Was sind Chancen? Was sind Risiken?

Fangen wir mit dem Positiven an, bevor die Stimmung kippt. Modellvielfalt ist echter Mehrwert. Unterschiedliche Modelle haben unterschiedliche Stärken: Das eine schreibt sauberere Excel-Formeln, das andere argumentiert in langen Analysen schlüssiger, das dritte ist schneller und billiger in der Rechenzeit. Wer Researcher-Berichte, Vertragsentwürfe oder komplexe Tabellenmodelle baut, kann künftig das passende Werkzeug wählen, statt mit dem Einheitsmodell

zu leben. Dazu kommt ein strategischer Vorteil: Du bist weniger abhängig von einem einzigen KI-Anbieter. Wenn OpenAI morgen strauchelt, hat Copilot noch ein zweites Bein.

Tipp: Lass die Modelle gegeneinander antreten

Nimm fünf echte Aufgaben aus deinem Alltag, etwa eine Vertragszusammenfassung, eine Pivot-Analyse und eine Kundenmail, und lass beide Modellfamilien ran. Das Ergebnis taugt mehr als jeder Benchmark aus dem Marketing, und du hast gleich Argumente für die Freigabe-Entscheidung.

Jetzt die Risiken, und die sind handfest. Erstens Datenschutz: Für EU-Unternehmen bedeutet Claude, dass Daten die EU Data Boundary verlassen. Das ist mit dem Microsoft DPA vertraglich abgesichert, muss aber in deinem Verzeichnis der Verarbeitungstätigkeiten auftauchen, unter Umständen eine Datenschutz-Folgenabschätzung auslösen und deinem Betriebsrat erklärt werden. Zweitens Schatten-Governance: Wenn der Modellwähler einmal da ist, wählen Anwender nach Bauchgefühl. Und Bauchgefühl hat noch nie eine DSGVO-Prüfung bestanden.

Drittens Fragmentierung: Wenn manche Abteilungen Claude dürfen und andere nicht, entstehen Ergebnisse, die sich nicht mehr vergleichen lassen. Viertens Kosten und Lizenzwirrwarr: Premium-Funktionen gibt es nur mit Premium-Lizenz, und wer Copilot Business, Copilot Enterprise und Consumer-Abos nebeneinander betreibt, verliert schnell den Überblick, wer eigentlich was darf.

Fünftens, und das wird gern übersehen: Abschalten ist nicht folgenlos. Microsoft weist selbst darauf hin, dass manche Funktionen nur verfügbar sind, wenn Anthropic aktiviert ist. Wer Anthropic später wieder deaktiviert, nimmt den Anwendern also womöglich Features weg, an die sie sich gewöhnt haben. Das ist ungefähr so beliebt wie die Ankündigung, dass die Kantine ab Montag nur noch Graubrot serviert. Plane deshalb von Anfang an mit Pilotgruppen, damit ein Rückzieher wenige trifft und nicht die ganze Firma.

Warnung: Der Klassiker aus dem Projektalltag

Ein Maschinenbauer aus Ostwestfalen, 800 Leute, hatte Copilot sauber in der EU-Grenze eingeführt. Dann schaltete ein Admin Anthropic „mal eben für alle“ frei, weil der Vertriebsleiter auf einer Messe gehört hatte, Claude schreibe die schöneren Angebote. Drei Wochen später fragte der Datenschutzbeauftragte, warum Konstruktionsdaten mit Exportkontroll-Vermerk durch ein Modell außerhalb der EU-Grenze gelaufen waren. Die Antwort „Die Angebote sind aber wirklich schöner geworden“ hat ihn nicht überzeugt. Der Admin übrigens auch nicht mehr lange.

Chance	Risiko
Bestes Modell pro Aufgabe	Anwender wählen nach Bauchgefühl statt nach Datenklasse
Weniger Abhängigkeit von einem KI-Anbieter	Datenverarbeitung außerhalb der EU Data Boundary
Bessere Researcher-Berichte und Office-Ergebnisse	Mehr Aufwand für VVT, DSFA und Betriebsrat
Copyright-Zusage gilt auch für Anthropic	Data-Retention-Modelle hebeln den Microsoft-Vertrag aus
Gezielte Freigabe per Entra-ID-Gruppe	Uneinheitliche Ergebnisse zwischen Abteilungen

Was müssen wir jetzt schon vorbereiten?

Die gute Nachricht: In EU-Tenants passiert erst einmal nichts von allein, Anthropic steht auf „No users“. Die schlechte: Irgendjemand wird bald fragen, warum die Konkurrenz Claude hat und ihr nicht. Bereite dich so vor, dass du dann eine Antwort hast und keine Ausrede. Der Hintergrund: Die Entscheidung für oder gegen Claude ist keine Technikfrage, die IT allein beantworten kann. Sie berührt Datenschutz, Exportkontrolle, Mitbestimmung und Einkauf. Wer das als reines Admin-Häkchen behandelt, hat in drei Monaten ein Meeting mit fünf Abteilungen, die alle gleichzeitig beleidigt sind.

- **Ist-Zustand prüfen:** Schau im Microsoft 365 Admin Center unter Copilot › Einstellungen › „AI providers operating as Microsoft subprocessors“ nach, was aktuell gilt. Prüfe separat die Einstellung „Copilot in Microsoft 365 apps with Anthropic models“, die es seit April 2026 für EU, EFTA und UK gibt.
- **Altlasten aufräumen:** Wer früher schon Claude unter Anthropics eigenen Bedingungen genutzt hat, muss in EU, EFTA und UK neu zustimmen. Der Schalter steht dort wieder auf „Aus“.
- **Modell-Matrix definieren:** Lege fest, welche Datenklassen mit welchem Modell verarbeitet werden dürfen. Ohne saubere Vertraulichkeitsbezeichnungen in Purview ist das Wunschdenken.
- **Gruppen statt Gießkanne:** Lege Entra-ID-Sicherheitsgruppen wie „KI-Anthropic-Pilot“ an und weise den Zugriff nur diesen Gruppen zu. Die Zuweisung wirkt auf Anbieter-Ebene in Copilot und Copilot Studio.
- **Datenschutz und Mitbestimmung:** Ergänze das Verzeichnis der Verarbeitungstätigkeiten, prüfe die Notwendigkeit einer DSFA und hole den Betriebsrat früh ins Boot. Ein Betriebsrat, der es aus der Zeitung erfährt, ist teurer als jede Lizenz.
- **Copilot Studio mitdenken:** Nach der Freischaltung im M365 Admin Center gibt es im Power Platform Admin Center eigene Schalter für externe Modelle. Die gehören in dasselbe Konzept.

Governance-Matrix: Welches Modell darf welche Daten sehen?

Vorschlag für einen EU-Mittelständler – als Diskussionsgrundlage, nicht als Rechtsberatung

	GPT 6.1	Claude Sonnet 5.5	Claude Opus 5.5	Modelle mit Data Retention
Öffentlich	erlaubt	erlaubt	erlaubt	Pilot
Intern	erlaubt	erlaubt	erlaubt	nein
Vertraulich	erlaubt	Freigabe-gruppe	Freigabe-gruppe	nein
Streng vertraulich	nur mit Label-Schutz	nein	nein	nein
Personenbezogen (Art. 9 DSGVO)	nur nach DSFA	nein	nein	Finger weg

Abbildung 3: So kann eine Freigabematrix aussehen. Grün heißt nicht „egal“, sondern „bewusst entschieden“.

Wichtig: Nur zwei Rollen dürfen den Schalter umlegen

Opt-in und Opt-out für Anthropic erfordern die Rolle AI-Administrator oder globaler Administrator. Prüfe, wer diese Rollen heute hat. Wenn die Antwort „ziemlich viele“ lautet, hast du ein Problem, das größer ist als Claude.

Maßnahme	Verantwortlich	Zeitraumen
Ist-Zustand der Subprozessor-Einstellungen dokumentieren	M365-Admin	Diese Woche
Datenklassen und Modell-Matrix abstimmen	CISO + Datenschutz	4 Wochen
Entra-ID-Gruppen für Pilot anlegen	Identity-Team	2 Wochen
VVT ergänzen, DSFA prüfen	Datenschutzbeauftragter	6 Wochen
Betriebsvereinbarung um Modellwahl erweitern	HR + Betriebsrat	8 Wochen
Pilot mit Vergleichsaufgaben auswerten	Fachbereiche + IT	nach 6 Wochen Pilot

Tipp: Schulung in zwei Minuten

Mach aus der Matrix eine Ampelkarte fürs Intranet: Welche Daten, welches Modell, wen fragen. Wer Anwendern ein 40-seitiges KI-Rahmenwerk schickt, bekommt genau eins zurück: eine Lesebestätigung von niemandem.

Häufig gestellte Fragen

Verlassen meine Daten die EU, wenn ich Claude in Microsoft Copilot nutze?

Ja. Anthropic-Modelle sind in Microsoft Copilot, Researcher, Copilot Studio und den Office-Apps derzeit von der EU Data Boundary ausgenommen. Die Verarbeitung ist zwar über Microsofts Product Terms und Datenschutz-Addendum abgesichert, findet aber außerhalb der EU-Grenze statt.

Wie schalte ich Claude-Modelle in einem europäischen Microsoft-365-Tenant frei?

Ein AI-Administrator oder globaler Administrator öffnet im Microsoft 365 Admin Center Copilot > Einstellungen > „AI providers operating as Microsoft subprocessors“, wählt Anthropic aus und speichert. Danach legt er fest, welche Benutzer oder Entra-ID-Sicherheitsgruppen Zugriff erhalten.

Kann ich festlegen, dass nur bestimmte Abteilungen Claude Opus 5.5 verwenden dürfen?

Ja, der Zugriff auf einen KI-Anbieter lässt sich auf einzelne Benutzer oder Entra-ID-Sicherheitsgruppen beschränken. Die Zuweisung gilt auf Anbieter-Ebene und wird in Microsoft Copilot und Copilot Studio durchgesetzt.

Was ist der Unterschied zwischen normalen Claude-Modellen und Modellen mit Data Retention?

Bei normalen Claude-Modellen ist Anthropic Microsoft-Subprozessor, und es gelten Microsofts Product Terms und Datenschutz-Addendum. Bei Modellen mit Data Retention ist Anthropic eigenständiger Verarbeiter, es gelten Anthropics Bedingungen, und Eingaben sowie Ausgaben werden in der Regel bis zu 30 Tage bei Anthropic gespeichert.

Wird GPT 6.1 in Copilot genauso behandelt wie Claude Opus 5.5?

Nein. OpenAI-Modelle wie GPT 6.1 betreibt Microsoft selbst in Azure innerhalb der EU Data Boundary, sie stehen ohne gesondertes Opt-in zur Verfügung. Claude-Modelle laufen bei Anthropic und müssen in EU-, EFTA- und UK-Tenants vom Admin ausdrücklich eingeschaltet werden.