

Microsoft 365 G7 enthält AI, Copilot, agent governance

Consulting Briefing · 22. September 2026 · boddenberg.de · Lesezeit rund 9 Minuten

Executive Summary

Microsoft hat am 15. September 2026 Microsoft 365 G7 angekündigt, die sogenannte Frontier Suite für US-Behörden in der Government Community Cloud. Ab dem 1. Oktober 2026 kann man sie kaufen. Drin sind Microsoft 365 G5, Microsoft Copilot, Work IQ, die Entra Suite und Agent 365, die neue Kontrollebene für KI-Agenten. Die Varianten für GCC High und DoD sollen „im Herbst“ folgen — ein in der Microsoft-Zeitrechnung erfreulich dehnbarer Begriff.

Jetzt denkst du: US-Behörden, GCC, das interessiert mich in Düsseldorf ungefähr so sehr wie die Kantinenpreise im Pentagon. Verständlich, aber falsch. G7 ist nur das Behördenderivat von Microsoft 365 E7, das seit dem 1. Mai 2026 kommerziell für 99 US-Dollar pro Benutzer und Monat zu haben ist. Die eigentliche Nachricht steckt nicht im Kürzel, sondern in der Architektur dahinter: Microsoft trennt ab sofort sauber zwischen dem, was Agenten tun, und dem, was Agenten tun dürfen. Das Zweite heißt Agent 365 und kostet extra.

Drei Dinge solltest du mitnehmen. Erstens: Agenten bekommen eine eigene Identität in Entra, werden inventarisiert, überwacht und lassen sich abschalten. Das ist genau die Governance-Schicht, die in deinem Copilot-Projekt bisher gefehlt hat — du hast sie nur noch nicht vermisst, weil niemand hingeschaut hat. Zweitens: Der Lizenzpreis deckt die Aufsicht, nicht den Betrieb. Die Rechnung für die Ausführung kommt separat aus Azure, von einem anderen Team, auf ein anderes Budget. Drittens, und das ist der Teil, der dir am ehesten um die Ohren fliegt: Sobald Claude-Modelle im Spiel sind, verlässt du die EU Data Boundary. Nicht vielleicht, sondern laut Microsofts eigener Dokumentation.

FAKTEN · Die Zahlen, die in der Vorstandsvorlage stehen müssen

Microsoft 365 E7 kostet 99 US-Dollar pro Benutzer und Monat und bündelt E5 (60), Microsoft Copilot (30), Entra Suite (12) und Agent 365 (15) — einzeln 117 US-Dollar, also rund 15 Prozent Rabatt auf Listenpreis. Für G7 hat Microsoft noch keinen Preis veröffentlicht. Agent 365 gibt es auch einzeln für 15 US-Dollar, setzt aber Microsoft 365 E5, Business Premium oder die Defender- und Purview-Suite voraus.

Worum geht es im Detail?

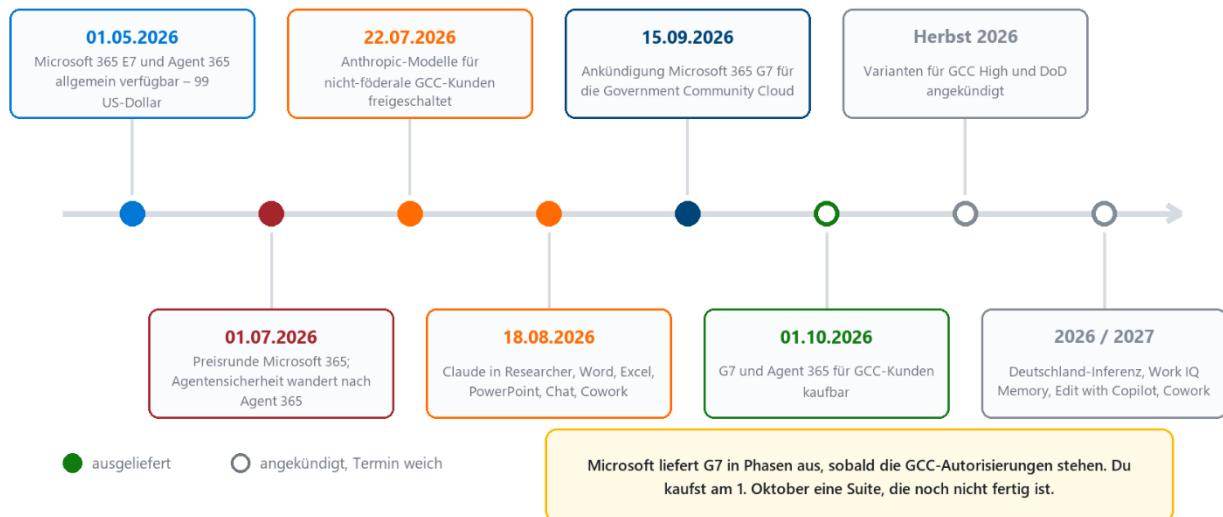
Chris Barry, bei Microsoft Präsident für den US-Public-Sector, verkauft G7 mit dem Satz, Innovation und Vertrauen müssten gemeinsam vorankommen. Das ist Marketing, aber ausnahmsweise mit Substanz dahinter. Behörden bekommen Copilot für Recherche, Analyse und Zusammenarbeit, dazu die fertigen Agenten Researcher und Analyst, den Agent Builder für eigene

Szenarien und Copilot Studio für die größeren Missionsagenten. Work IQ liefert den Organisationskontext, also das Wissen darüber, wer mit wem woran arbeitet und wer was sehen darf.

Der Haken ist die Lieferform. Microsoft liefert G7 in Phasen aus, sobald die jeweiligen GCC-Autorisierungsmeilensteine erreicht sind. Aktuelle GPT-Modelle, Work IQ Memory und Personalisierung, „Edit with Copilot“ in Word, Excel und PowerPoint sowie Copilot Cowork für mehrstufige Abläufe kommen erst später. Du kaufst am 1. Oktober also eine Suite, die zu diesem Zeitpunkt noch nicht fertig ist. Analysten haben das bereits angemerkt: ob die Anfangskosten durch das gerechtfertigt sind, was am Starttag tatsächlich funktioniert, ist eine offene Frage. Übersetzt: Du zahlst ab Tag eins für eine Roadmap.

Das Agenten-Jahr 2026

Von der Ankündigung bis zur Rechnung – und was noch aussteht



boddenberg.de · Consulting Briefing · 21.09.2026

Abbildung 1: Das Agentenjahr 2026 – was ausgeliefert ist und was noch aussteht.

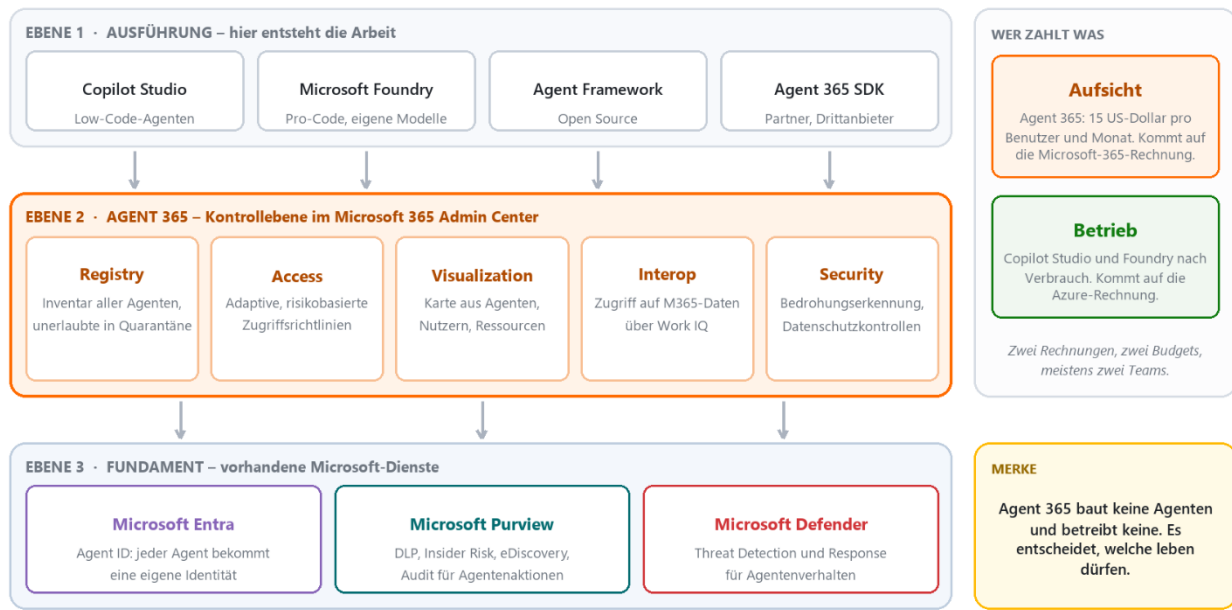
Agent 365 ist kein Produkt, sondern eine Aufsichtsbehörde

Der interessante Teil an G7 heißt Agent 365 und ist seit dem 1. Mai 2026 allgemein verfügbar, direkt im Microsoft 365 Admin Center. Es baut keine Agenten und betreibt keine. Es beantwortet die fünf Fragen, die jeder Vorstand stellt, sobald das Wort Agent fällt: Welche gibt es? Wem gehören sie? Worauf greifen sie zu? Verhalten sie sich wie gedacht? Und wie werde ich sie wieder los?

Technisch stehen dafür fünf Bausteine bereit. Die Registry inventarisiert alle Agenten in Entra, egal ob sie aus Copilot Studio, aus Microsoft Foundry, aus einem Open-Source-Framework oder von einem Drittanbieter stammen; nicht genehmigte Agenten landen in Quarantäne. Der Zugriffsbaustein vergibt jedem Agenten eine eigene Entra Agent ID und wendet adaptive, risikobasierte Richtlinien an – Least Privilege, diesmal auch für Software, die keine Mittagspause macht. Die Visualisierung zeichnet eine Karte aus Agenten, Nutzern und Ressourcen. Die Interoperabilität regelt den Datenzugriff über Work IQ. Und die Sicherheitsschicht hängt an Microsoft Defender für die Bedrohungserkennung und an Microsoft Purview für DLP, Insider Risk und eDiscovery.

Agent 365: die Kontrollebene

Microsoft trennt das Tun der Agenten vom Dürfen der Agenten



Kernaussage: Ohne Ebene 2 hast du Ebene 1 bereits im Haus – nur eben unsichtbar.

boddenberg.de · Consulting Briefing · 21.09.2026

Abbildung 2: Agent 365 sitzt als Kontrollebene zwischen Ausführung und Fundament.

WICHTIG · Seit dem 1. Juli 2026 ist das keine Option mehr

Die Sicherheitsfunktionen für Agenten aus Microsoft Foundry und Copilot Studio sind zum 1. Juli 2026 von Defender nach Agent 365 gewandert. Wer diese Plattformen nutzt und die Schutzfunktionen behalten will, braucht die Lizenz. Das ist die eleganteste Art, einen Zusatzverkauf zu bauen: Man verschiebt eine Funktion, die schon bezahlt war, in ein neues SKU.

Was der Preis nicht enthält

Hier wird es für die Budgetplanung unangenehm. Agent 365 ist eine Governance-Gebühr, keine Betriebskostenpauschale. Die Lizenz wird pro Person gekauft und deckt alle Agenten ab, die diese Person besitzt, verwaltet oder mit denen sie arbeitet; die Agenten selbst brauchen keine eigene Lizenz. Was sie aber sehr wohl brauchen, ist Rechenzeit, und die läuft über Copilot Studio oder Microsoft Foundry und landet auf der Azure-Rechnung.

Kostenblock	Modell	Listenpreis	Landet auf
Agent 365	pro Benutzer und Monat	15 US-Dollar	Microsoft-365-Rechnung
Microsoft 365 E7 (Bündel)	pro Benutzer und Monat	99 US-Dollar	Microsoft-365-Rechnung
Copilot Studio Capacity Pack	Miete, 25.000 Credits	200 US-Dollar pro Monat	Microsoft-365-Rechnung

Kostenblock	Modell	Listenpreis	Landet auf
Copilot Studio Pay-as-you-go	Verbrauch	0,01 US-Dollar pro Credit	Azure-Rechnung
Microsoft Foundry	Verbrauch	variabel, kein TCO-Modell	Azure-Rechnung

Tabelle 1: Aufsicht und Betrieb werden getrennt abgerechnet — und meist von getrennten Teams verantwortet.

Es gibt übrigens eine kostenlose Stufe: Agentenidentität, Basisinventar und grundlegende Nutzungseinblicke bekommt jeder Microsoft-Cloud-Kunde ohne Aufpreis. Die bezahlten 15 US-Dollar liefern die erweiterten Governance-Richtlinien, die Bedrohungserkennung und die Datensicherheitskontrollen. Wo genau die Grenze zwischen „noch kostenlos“ und „schon lizenzpflichtig“ verläuft, ist erstaunlich unscharf beschrieben. Plane also Puffer ein, und zwar nicht nur zeitlich.

Und was hat Claude damit zu tun?

Eine ganze Menge. Anthropic ist seit Januar 2026 offiziell Microsoft-Subprozessor. Das bedeutet: Für die regulären Claude-Modelle gelten die Microsoft Product Terms und das Data Protection Addendum, die Enterprise Data Protection greift, und das Microsoft Customer Copyright Commitment deckt Copilot und Copilot Studio mit ab. Seit dem 18. August 2026 stehen Claude-Modelle in Researcher, Copilot Studio, Word, Excel, PowerPoint, Copilot Chat, Power Platform und Copilot Cowork zur Auswahl. Claude Opus 4.7 ist über das Frontier-Programm und die Early-Release-Ringe von Copilot Studio erreichbar und rollt in Excel aus.

Im kommerziellen Cloud-Angebot sind Anthropic-Modelle für die meisten Kunden standardmäßig eingeschaltet — mit einer großen Ausnahme: EU, EFTA und Großbritannien. Dort stehen sie auf „No users“, und zwar aus einem sehr konkreten Grund. Genau diese Zuordnung entscheidet, was du in deinem Tenant überhaupt anschalten darfst.

Umgebung	Anthropic-Modelle	Standard	Was du tun musst
Commercial, ohne EU/EFTA/UK	verfügbar	eingeschaltet	prüfen, ob du das willst; sonst deaktivieren
EU, EFTA, Großbritannien	verfügbar	ausgeschaltet	bewusstes Opt-in durch AI Administrator
GCC, nicht-föderal	seit 22.07.2026	ausgeschaltet	Opt-in im Admin Center
GCC, föderale Kunden	nicht verfügbar	—	Option erscheint gar nicht erst
GCC High und DoD	nicht verfügbar	—	Planung ohne Claude
Andere Sovereign Clouds	nicht verfügbar	—	betrifft auch souveräne Plattformen wie Delos

Tabelle 2: Wo du Claude-Modelle in Microsoft 365 Copilot einschalten darfst — und wo die Frage sich gar nicht stellt.

Das ist die eigentliche Pointe für G7: Ausgerechnet in der Behördensuite, die mit Modellvielfalt und Governance wirbt, gibt es für föderale GCC-Kunden, GCC High und DoD keine Claude-Modelle.

Wer also eine Agentenarchitektur baut, die auf ein bestimmtes Modell optimiert ist, baut sich damit eine Migrationsaufgabe in die Zukunft ein.

Was sind Chancen? Was sind Risiken?

Fangen wir mit dem Positiven an, das geht schneller. Zum ersten Mal gibt es eine Kontrollebene für Agenten, die nicht aus drei Nischenwerkzeugen und einer Excel-Tabelle besteht. Agenten werden zu verwalteten Identitäten und laufen damit durch dieselben Prozesse wie Benutzerkonten: Beantragung, Freigabe, Rezertifizierung, Abschaltung. Das ist kein neues Konzept, es ist nur endlich auf die richtige Objektklasse angewendet.

Die zweite Chance liegt im Timing. Deine Belegschaft baut bereits Agenten — mit Agent Builder, in Copilot Studio, über Power Platform. Das ist nicht böartig, das ist genau das Verhalten, das jede Adoption-Kampagne der letzten zwei Jahre gefordert hat. Wenn du jetzt eine Registry einführest, inventarisierst du einen überschaubaren Bestand. Wenn du zwei Jahre wartest, machst du Archäologie.

Thema	Chance	Risiko
Governance	Agenten werden inventarisiert, bekommen Besitzer und lassen sich gezielt abschalten.	Ohne saubere Berechtigungen inventarisierst du nur, wer wo überall zu viel sieht.
Kosten	Bündelpreis spart rund 15 Prozent gegenüber Einzelkauf, Rabatte bis 31.12.2026.	Der Verbrauch für Ausführung ist nicht gedeckelt und steht auf einer anderen Rechnung.
Modellvielfalt	Claude neben GPT verfügbar, Auswahl pro Nutzer und pro Agent möglich.	Anthropic-Modelle liegen außerhalb der EU Data Boundary und der In-Country-Zusagen.
Souveränität	Deutschland-Inferenz für Copilot ist für 2026 angekündigt.	Flex Routing kann Inferenz bei Lastspitzen in die USA, nach Kanada oder Australien verlagern.
Zeitplan	Früher Einstieg sichert Rabatte und Erfahrungsvorsprung.	Halbfertige Suite: Kernfunktionen kommen erst nach Autorisierungsmeilensteinen.

Tabelle 3: Fünf Themen, bei denen Chance und Risiko dieselbe Ursache haben.

Jetzt das Unangenehme. Microsofts eigene Dokumentation sagt es unmissverständlich: Anthropic-Modelle in Copilot, Researcher, Copilot Studio, Power Platform und in den Microsoft-365-Apps sind derzeit von der EU Data Boundary ausgenommen und, wo einschlägig, auch von den In-Country-Processing-Zusagen. Wer in Deutschland den Schalter umlegt, exportiert Verarbeitung. Dazu kommt das Flex Routing: Bei Kapazitätsspitzen darf Copilot-Inferenz die EU Data Boundary verlassen und in den USA, in Kanada oder in Australien landen — und für Tenants, die nach dem 25. März 2026 angelegt wurden, ist das standardmäßig aktiv.

Das dritte Risiko ist hausgemacht und hat mit Microsoft wenig zu tun: Oversharing. Ein Agent mit delegierten Rechten sieht exakt das, was sein Auftraggeber sehen darf — inklusive der SharePoint-Bibliothek, die seit 2019 auf „Jeder in der Organisation“ steht. Der Unterschied zu früher: Früher hat niemand danach gesucht. Jetzt fasst ein Sprachmodell den Inhalt höflich zusammen und schickt ihn per Teams weiter.

WARNUNG · Modelle mit Data Retention sind eine andere Rechtslage

Bestimmte fortgeschrittene Anthropic-Modelle werden als „Anthropic models with Data Retention“ angeboten. Hier gelten nicht die Microsoft Product Terms, sondern Anthropic's eigene Commercial Terms und das Anthropic-DPA. Anthropic speichert die meisten Ein- und Ausgaben bis zu 30 Tage; schlägt ein Trust-und-Safety-Klassifikator an, können Inhalte bis zu zwei Jahre und Klassifikationswerte bis zu sieben Jahre aufbewahrt werden. Diese Modelle sind überall ausgeschaltet und brauchen ein ausdrückliches Opt-in. Ein Training mit deinen Daten findet ohne deine Erlaubnis nicht statt — das ist aber auch der einzige Teil, den du ungeprüft weitergeben kannst.

Wohin läuft dein Prompt wirklich?

Drei Pfade, drei völlig verschiedene Antworten für den Datenschutzbeauftragten

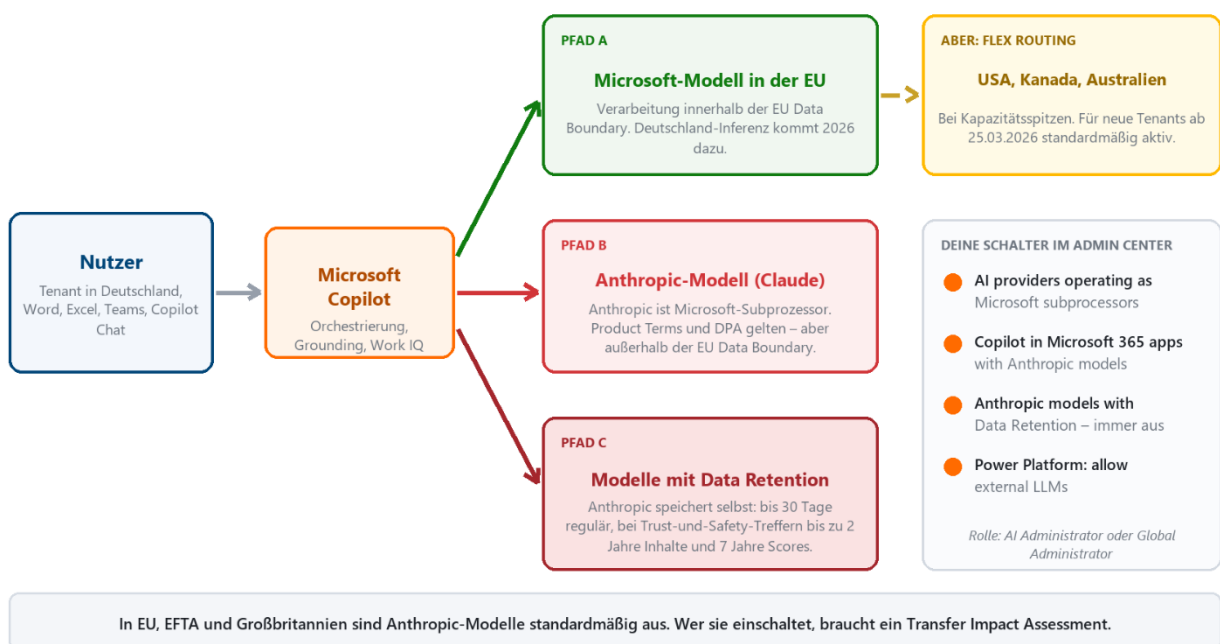


Abbildung 3: Drei Pfade für denselben Prompt — mit sehr verschiedenen Antworten für die Datenschutzprüfung.

Was müssen wir jetzt schon vorbereiten?

G7 kannst du in Deutschland nicht kaufen, und das musst du auch nicht. Die Architektur dahinter kommt aber genauso in dein kommerzielles Tenant. Diese sechs Punkte kosten dich wenige Wochen und ersparen dir später ein Projekt.

- **Inventur zuerst:** Zieh dir die Liste aller vorhandenen Agenten aus Copilot Studio, Power Platform und den Agent-Builder-Erstellungen. Die kostenlose Stufe von Agent 365 liefert Identität und Basisinventar ohne Zusatzlizenz — nutze das als Bestandsaufnahme, bevor du über Budget redest.
- **Besitzerschaft klären:** Jeder Agent braucht eine Person, keine Abteilung. Ohne benannten Besitzer ist die schönste Registry nur ein Friedhof mit Namensschildern.
- **Berechtigungen aufräumen:** Sensitivity Labels setzen, SharePoint-Suche einschränken, „Jeder“-Freigaben jagen. Das ist die unsexy Vorarbeit, ohne die jede Agentenstrategie an Tag drei in der Rechtsabteilung landet.

- Modellpolitik festlegen: Entscheide bewusst, ob Anthropic-Modelle an sind. Der Schalter heißt „AI providers operating as Microsoft subprocessors“ und sitzt im Microsoft 365 Admin Center unter Copilot und Einstellungen. Zuständig sind die Rollen AI Administrator oder Global Administrator. Wer in EU, EFTA oder Großbritannien früher unter Anthropic's eigenen Bedingungen zugestimmt hat, muss erneut zustimmen — der Schalter steht wieder auf aus.
- Datenschutz sauber dokumentieren: Transfer Impact Assessment für die US-Verarbeitung, Flex-Routing-Status im Tenant prüfen, Auditprotokollierung für Agentenaktionen aktivieren. Und ja, CLOUD Act und FISA 702 stehen weiter im Raum, unabhängig davon, wo die Festplatte steht.
- Budget zweigleisig planen: Seat-Kosten für die Governance, Verbrauchsbudget für die Ausführung. Wenn diese beiden Posten bei euch von verschiedenen Kostenstellen getragen werden, klär das vor dem ersten produktiven Agenten und nicht beim Quartalsabschluss.

TIPP · Der Rabatt hat ein Verfallsdatum

Microsoft gewährt auf Microsoft 365 E7 noch bis zum 31. Dezember 2026 Einführungsrabatte: 10 Prozent bei jährlicher Zahlung ab 10 Plätzen, 15 Prozent bei jährlicher Zahlung ab 100 Plätzen und 15 Prozent bei dreijähriger Bindung ab 300 Plätzen. Gleichzeitig sind zum 1. Juli 2026 die regulären Listenpreise gestiegen, E5 um 5 bis 8 Prozent, Frontline-Pläne teilweise um bis zu 43 Prozent. Rechne beide Effekte gegeneinander, bevor du dich dreijährig bindest.

TIPP · Für die öffentliche Verwaltung in Deutschland

Wenn du im souveränen Umfeld unterwegs bist: Die Delos Cloud hat Anfang 2026 ihr zweites Operations Center im Raum Leipzig in Betrieb genommen, nach dem ersten im Raum Gütersloh. Microsoft 365 Local erlaubt zusätzlich den Betrieb von SharePoint Server und Exchange Server auf Azure Local, inklusive einer Variante ohne Internetverbindung. In diesen Umgebungen stehen Anthropic-Modelle nicht zur Verfügung — plan deine Agentenszenarien entsprechend modellneutral.

Häufig gestellte Fragen

Brauchen wir Microsoft 365 G7, wenn wir gar keine US-Behörde sind?

Nein. G7 ist ausschließlich für die US Government Community Cloud gedacht und in Europa nicht bestellbar. Das kommerzielle Gegenstück heißt Microsoft 365 E7 und enthält dieselben Bausteine; Agent 365 lässt sich zusätzlich einzeln lizenzieren, wenn du nur die Governance-Schicht brauchst.

Kostet jeder KI-Agent jetzt eine eigene Lizenz?

Nein, Agent 365 wird pro Person lizenziert. Eine Lizenz deckt alle Agenten ab, die dieser Benutzer besitzt, verwaltet oder mit denen er arbeitet, unabhängig davon, ob der Agent mit delegiertem oder mit eigenem Zugriff läuft. Die Ausführung der Agenten wird davon getrennt nach Verbrauch abgerechnet.

Dürfen wir Claude-Modelle in Microsoft 365 Copilot in Deutschland nutzen?

Technisch ja, standardmäßig sind sie in EU, EFTA und Großbritannien aber ausgeschaltet und müssen von einem AI Administrator oder Global Administrator freigeschaltet werden. Rechtlich

musst du beachten, dass Anthropic-Modelle derzeit von der EU Data Boundary und den In-Country-Processing-Zusagen ausgenommen sind — ein Transfer Impact Assessment ist damit Pflicht, keine Kür.

Was passiert mit unseren Daten bei Modellen mit Data Retention?

Bei diesen Modellen tritt Anthropic nicht als Microsoft-Subprozessor auf, sondern unter eigenen Bedingungen. Anthropic speichert die meisten Ein- und Ausgaben bis zu 30 Tage, bei Treffern der Trust-und-Safety-Klassifikatoren Inhalte bis zu zwei Jahre und Klassifikationswerte bis zu sieben Jahre. Ein Training mit diesen Daten erfolgt nur mit ausdrücklicher Erlaubnis.

Reicht Agent 365 als Governance, oder brauchen wir noch etwas?

Agent 365 liefert Identität, Inventar, Zugriffsrichtlinien, Bedrohungserkennung und Compliance-Anbindung an Purview — also die Werkzeuge. Es beantwortet nicht, welcher Agent fachlich zulässig ist, und es räumt auch keine falsch gesetzten Berechtigungen auf. Diese beiden Aufgaben bleiben bei dir und sind erfahrungsgemäß der aufwendigere Teil.