KI & COPILOT

Copilot Managed Runtime wird allgemein verfügbar; App-Erstellung in Copilot Cowork wird geöffnet

Consulting Briefing · 19.11.2026 · boddenberg.de

Executive Summary

Kurz und schmerzhaft: Du hast 29 Tage. Laut Microsoft-Ankündigung MC1558033 wird Copilot Managed Runtime allgemein verfügbar. Der Rollout hat Mitte November begonnen und soll bis Mitte Dezember abgeschlossen sein, die Meldung läuft am 17.12.2026 aus. Ab dann darf jeder mit Microsoft-365-Copilot-Lizenz in Copilot Cowork per Chat eigene Apps bauen, nicht mehr nur der kleine Kreis im Frontier-Programm. Die Apps greifen über Konnektoren auf SharePoint, Outlook, Teams, Excel und Dataverse zu und lassen sich standardmäßig per Link an die ganze Organisation verteilen.

Was du verstehen musst: Microsoft hat Cowork-App-Bau und Copilot-Studio-App-Bau standardmäßig für alle eingeschaltet, die Umgebungsweiterleitung für Copilot Managed Runtime ist in jedem Tenant aktiv und lässt sich nicht abschalten. Die gute Nachricht: Die Voreinstellungen sind überraschend vernünftig, und jede Tür hat einen Schalter. Die schlechte: Ein paar Türen stehen offen, und eine davon heißt „organisationsweites Teilen“. Wer jetzt nichts tut, bekommt ab Weihnachten eine Schatten-IT mit Microsoft-Gütesiegel.

Für deutsche Organisationen kommt die Mitbestimmung obendrauf. Microsoft protokolliert jeden App-Start mit Benutzername und IP-Adresse im Purview-Audit, und die gebauten Apps selbst werten oft Kalender, Aufgaben und Anwesenheiten aus. Damit ist § 87 Abs. 1 Nr. 6 BetrVG im Spiel, in Behörden das Personalvertretungsrecht. Unsere Empfehlung: App-Bau sofort auf eine Pilotgruppe beschränken, Governance prüfen, Credits bewusst konfigurieren, dann mit dem Betriebs- oder Personalrat einen Rahmen vereinbaren.

Fakten: Das Wichtigste auf einen Blick

Quelle: Microsoft-Ankündigung MC1558033, zuletzt geändert am 18.11.2026. Vorgänger war die Preview-Meldung MC1469329 aus dem September 2026.

Rollout: allgemeine Verfügbarkeit weltweit von Mitte November bis Mitte Dezember 2026, Meldungsende 17.12.2026.

Werkzeuge: Copilot Cowork, Copilot Studio, Copilot Code und die Copilot Managed Runtime CLI. Alle Apps laufen auf derselben verwalteten Plattform.

Kosten: Bau und Ausführung laufen über Copilot Credits. 0,1 Credit pro API-Aufruf, 100 Credits entsprechen 1 US-Dollar.

Worum geht es im Detail?

Erinnerst du dich an Access-Datenbanken auf dem Abteilungslaufwerk? An das Excel-Makro „Urlaubsplanung_final_NEU_v3.xlsm“, das ein Kollege 2009 geschrieben hat, bevor er in Rente

ging, und das seitdem niemand anzufassen wagt? Genau dieses Problem will Microsoft lösen, nur mit dem Unterschied, dass heute keiner mehr VBA lernen muss. Man tippt in Copilot Cowork „Bau mir eine App für unser Daily Scrum“, und eine KI liefert eine fertige Web-App mit angebundenen Daten.

Copilot Managed Runtime ist die Plattform darunter. Microsoft beschreibt sie als IT-gesteuerte Umgebung, die Code innerhalb der Tenant-Grenze ausführt. Technisch läuft jede App in einem abgeschotteten iframe auf einem von Microsoft betriebenen Host. Die Anmeldung erfolgt über Entra ID, Conditional Access greift, und der Host hält die Authentifizierungstokens vom App-Code fern. Datenzugriffe laufen nicht direkt aus dem Browser, sondern über Konnektoren, die der Host gegen die hinterlegten Richtlinien prüft. Den Quellcode legt die Plattform in verwalteten Git-Repositorys ab, gebaut wird in einer Sandbox ohne freien Netzwerkzugang. Das ist, ehrlich gesagt, mehr Governance, als die meisten Eigenentwicklungen im Mittelstand je gesehen haben.

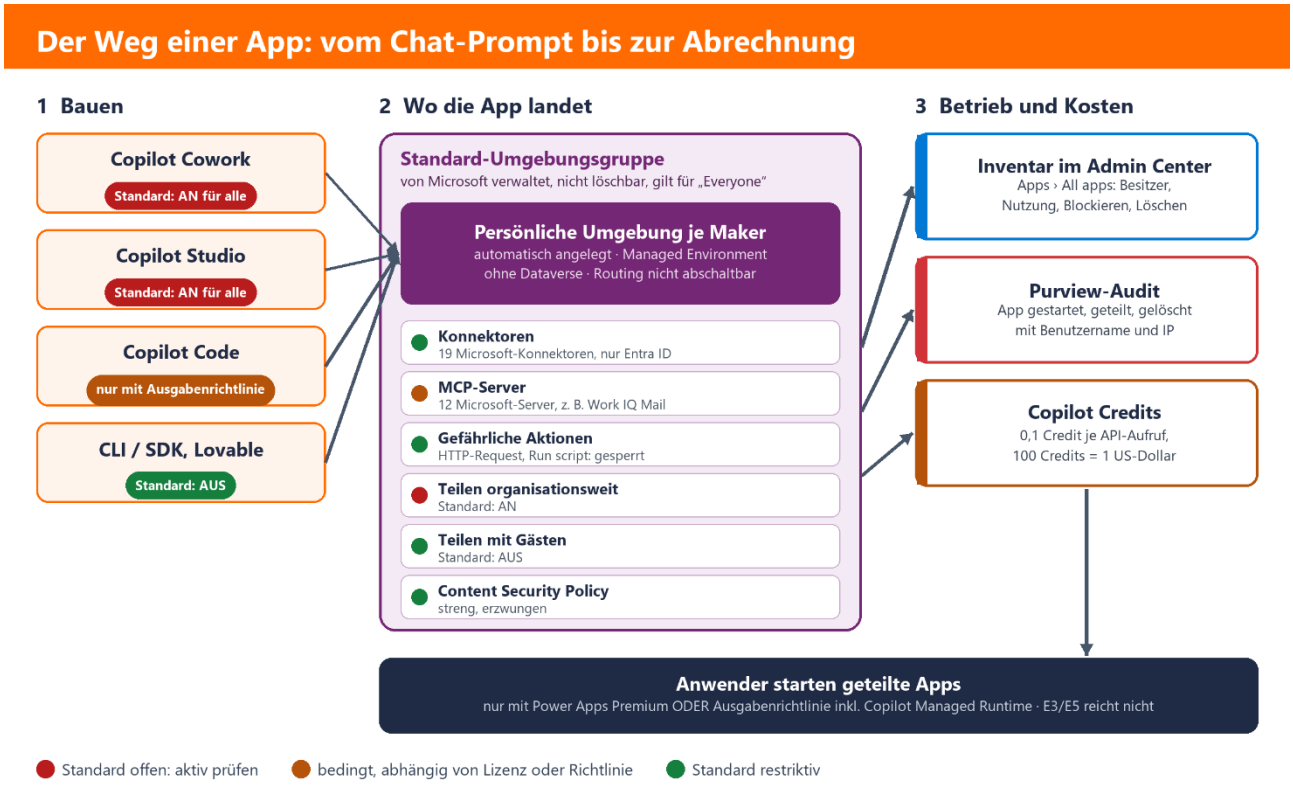


Abbildung 1: Egal mit welchem Werkzeug gebaut wird, jede App landet in einer persönlichen Umgebung, erbt die Regeln der Umgebungsgruppe und kostet bei der Ausführung Credits. Rot markiert, was standardmäßig offen ist.

Die Umgebungsweiterleitung ist der Teil, der Power-Platform-Admins kalt erwischt. Jeder Maker bekommt beim ersten App-Bau automatisch eine persönliche Umgebung. Laut Microsoft Learn ist das Routing für Copilot Managed Runtime in allen Tenants aktiviert und nicht änderbar. Gibt es noch keine Routing-Regeln, legt der Dienst eine Regel für „Everyone“ und eine neue Standard-Umgebungsgruppe an. Ist diese Governance einmal initialisiert, lässt sich die Everyone-Regel weder löschen noch ändern. Die Tenant-Einstellung, die das Anlegen von Entwicklerumgebungen verbietet, hilft hier übrigens nicht: Sie gilt nur für manuell erstellte Umgebungen. Hast du dagegen schon Routing-Regeln mit Sicherheitsgruppen ohne Auffangregel, bleiben alle anderen draußen, bis du sie aufnimmst.

Die Standard-Umgebungsgruppe bringt eine kuratierte Positivliste mit: 19 Microsoft-Konnektoren, die ausschließlich über Entra ID authentifizieren, darunter SharePoint, OneDrive, Outlook, Teams, Planner, Excel, Power BI und Dataverse. Dazu kommen 12 Microsoft-MCP-Server, etwa für

Outlook-Mail, Kalender, Teams und Benutzerprofile. Riskante Aktionen wie „Send an HTTP request“ oder „Run script“ in Excel sind gesperrt, Drittanbieter- und Custom-Konnektoren ebenfalls. Ein Haken: Microsoft nimmt künftige Konnektoren, die die Kriterien erfüllen, automatisch in die Liste auf. Wer das nicht will, übernimmt die Richtlinie per „Edit this policy“ selbst und verzichtet damit auf alle weiteren Updates.

Werkzeug	Standard	So steuerst du es
Copilot Cowork	AN für alle Nutzer	Admin Center: Copilot › Cowork › Settings › Build apps in Copilot. Optionen: All users, No users, Specific users and groups.
Copilot Studio	AN für alle Nutzer	Power Platform CLI: pac admin update-tenant-settings mit der Einstellung enableManagedAppsMcsPreview auf off oder enabledGroupsManagedAppsMcsPreview mit Gruppen-IDs.
Copilot Code	nur mit Ausgabenrichtlinie	Kein eigener Schalter. Wer in keiner Ausgabenrichtlinie für Copilot Code steht, baut nichts.
CLI und SDK	AUS	Power Platform Admin Center: Copilot › Settings › Managed apps, pro Umgebung oder Umgebungsgruppe.
Externe Artefakte	AUS	Gleicher Pfad, Einstellung „External artifacts in managed apps“. Bitte so lassen.

Was sind Chancen? Was sind Risiken?

Die Chance ist real. Fachabteilungen bauen sich ihre kleinen Werkzeuge ohnehin, nur heute eben in Excel, in privaten Trello-Boards oder mit dem Freemium-Formular-Tool, dessen Server irgendwo stehen, wo du nie hinwolltest. Copilot Managed Runtime holt diese Fantasie in eine Umgebung, die du siehst: Jede App erscheint im Admin Center unter Apps › All apps, mit Besitzer, Konnektoren, Nutzung und Freigaben. Du kannst sie blockieren, ohne sie zu löschen, und du siehst Gesundheitswerte. Microsoft formuliert es selbst treffend: Man kann nur regieren, was man sieht.

Aspekt	Chance	Risiko
Produktivität	Fachbereiche bauen Tracker, Formulare und Dashboards in Stunden statt Monaten	Hunderte Kleinst-Apps ohne Pflegeverantwortung, wenn der Maker das Haus verlässt
Sicherheit	Strenge Content Security Policy, gesperrte HTTP-Aktionen, Build in der Sandbox	Geteilte Verbindungen nutzen die Rechte des Makers statt die des Anwenders
Datenschutz	Daten bleiben in Microsoft-Diensten des Tenants	Apps verknüpfen Kalender, Mail und Aufgaben zu neuen Profilen

Aspekt	Chance	Risiko
Mitbestimmung	Zentrales Inventar erleichtert Transparenz	Jede App kann eine technische Einrichtung im Sinne des § 87 BetrVG sein
Kosten	Laufzeit ist billig: 100 Credits decken rund 1.000 Aufrufe	Bauen ist der teure Teil, ohne Limits wird Cowork zum Spendierhosen-Modus

Jetzt zu den Risiken, und die haben Humor, wenn auch einen schwarzen. Stell dir folgendes Szenario vor, es ist leider kein weit hergeholtes: Ein Teamleiter in der Logistik baut sich in Cowork einen „Verfügbarkeits-Tracker“. Die App liest Outlook-Kalender, Teams-Status und Planner-Aufgaben seines Teams und zeigt in Ampelfarben, wer gerade „produktiv“ ist. Gebaut in 20 Minuten, per Organisations-Link an alle Schichtleiter verteilt, die ihn wiederum weitergeleitet haben. Technisch einwandfrei, alle Konnektoren auf der Positivliste. Rechtlich eine Leistungs- und Verhaltenskontrolle ohne Betriebsvereinbarung. Und wer findet die App als Erster? Natürlich der Betriebsrat.

Warnung: „Teilen gibt keinen Datenzugriff“ stimmt nur halb

Microsoft betont, dass eine geteilte App keinen Zugriff auf die zugrunde liegenden Daten gewährt, weil jeder Anwender seine eigene Verbindung nutzt. Das gilt aber nicht, wenn der Maker bewusst eine geteilte Verbindung konfiguriert. Dann arbeitet die App mit seinen Berechtigungen. Die Cowork-Dokumentation sagt es deutlich: Wer den Link hat, kann die App samt ihren Daten nutzen. Ein Organisations-Link darf außerdem weitergeleitet werden. Herzlichen Glückwunsch, du hast gerade die Gehaltsliste der Personalabteilung demokratisiert.

Datenschutz und Mitbestimmung, nüchtern eingeordnet. Nach ständiger Rechtsprechung des Bundesarbeitsgerichts reicht für § 87 Abs. 1 Nr. 6 BetrVG, dass eine technische Einrichtung objektiv geeignet ist, Verhalten oder Leistung zu überwachen. Das trifft hier auf zwei Ebenen zu. Erstens die Plattform: Das Purview-Audit erfasst unter dem Datensatztyp CopilotManagedRuntime unter anderem jeden App-Start mit Benutzerprinzipal, IP-Adresse und User-Agent, das Inventar zeigt Nutzung pro App. Zweitens die Apps selbst: Jede App, die Kalender, Mails oder Aufgaben von Kollegen auswertet, ist potenziell eine eigene technische Einrichtung. Einzeln mitbestimmen lassen ist bei hundert Apps unrealistisch. Deshalb braucht es eine Rahmenvereinbarung mit klaren Verbotszonen und einem Freigabeprozess für Apps mit Personenbezug. In Bundesbehörden gilt § 80 Abs. 1 Nr. 21 BPersVG, in Ländern und Kommunen das jeweilige Landespersonalvertretungsgesetz.

Datenschutzrechtlich gilt: Die Plattform ist Teil deines bestehenden Microsoft-365-Vertrags, aber jede App ist eine neue Verarbeitung. Für Apps mit Personenbezug gehört ein Eintrag ins Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO, bei systematischer Auswertung von Beschäftigtendaten auch eine Prüfung auf Datenschutz-Folgenabschätzung. Und weil die Maker mit KI bauen, hilft ein Hinweis auf die Pflicht zur KI-Kompetenz nach Art. 4 KI-Verordnung, die seit Februar 2025 gilt. Wer Apps baut, sollte wissen, was ein Konnektor darf.

Wichtig: E3 und E5 reichen nicht zum Ausführen

Die Power-Apps-Nutzungsrechte aus Microsoft 365 E3 oder E5 decken Apps auf Copilot Managed Runtime nicht ab, und eine Copilot-Lizenz allein auch nicht. Wer eine geteilte App starten will, braucht Power Apps Premium oder muss in einer Ausgabenrichtlinie stehen, die Copilot Managed Runtime einschließt. Sonst steht da: „You do not have enough credits to use this app." Die Helpdesk-Tickets schreiben sich von selbst.

Was müssen wir jetzt schon vorbereiten?

Die Reihenfolge ist entscheidend: erst Schalter, dann Governance, dann Credits, dann Kommunikation. Wer mit den Credits anfängt, öffnet die Tür, bevor die Hausordnung steht. Der folgende Fahrplan ist auf die 29 Tage bis zum Meldungsende zugeschnitten.

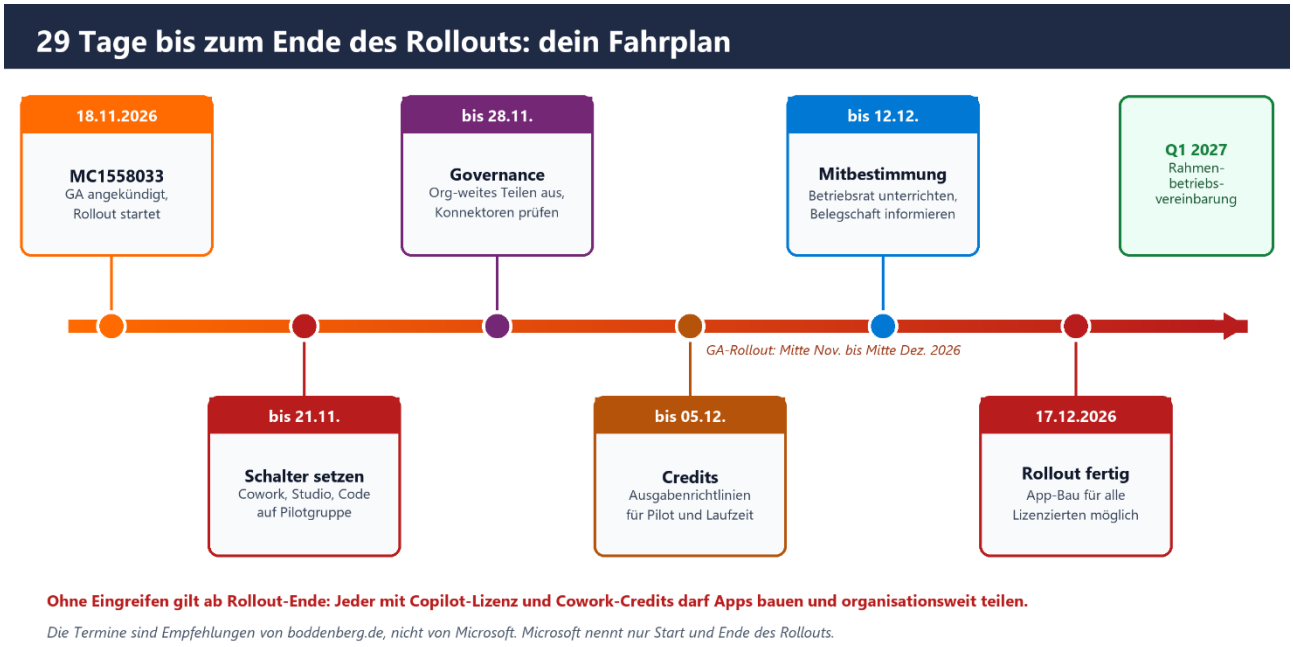


Abbildung 2: Microsoft liefert Start und Ende, den Rest musst du füllen. Die Rahmenvereinbarung mit Betriebs- oder Personalrat ist der langsamste Baustein.

Wann	Wer	Was konkret
Bis 21.11.2026	Copilot-Admin	Im Microsoft 365 Admin Center unter Copilot › Cowork › Settings › Build apps in Copilot von All users auf Specific users and groups umstellen und eine Pilotgruppe eintragen. Ohne Zustimmung der Interessenvertretung: No users. Copilot Studio per pac-CLI abschalten oder auf eine Sicherheitsgruppe beschränken. Bestehende Ausgabenrichtlinien auf den Dienst Copilot Code prüfen.

Wann	Wer	Was konkret
Bis 28.11.2026	Power-Platform-Admin	Vorhandene Routing-Regeln prüfen, bevor die Governance initialisiert wird. Unter Apps › Settings › Environment groups die Standardgruppe öffnen: Allow organization-wide sharing ausschalten, Gäste aus lassen, Konnektor-Positivliste und MCP-Server gegen eigene Vorgaben halten, besonders Work IQ für Mail und Kalender.
Bis 05.12.2026	Lizenz- und Kostenverantwortliche	Unter Copilot › Cost management die nutzungsbasierte Abrechnung prüfen. Eine Laufzeit-Richtlinie mit Copilot Managed Runtime für die Pilotgruppe mit 100 Credits pro Person und Monat, eine eigene Bau-Richtlinie für Cowork mit engem Limit. Alarme an einen echten Menschen schicken.
Bis 12.12.2026	IT-Sicherheit	Im Inventar unter Apps › All apps alle Preview-Apps sichten, Besitzer und Freigaben prüfen, Fragwürdiges blockieren. Purview-Audit für den Datensatztyp CopilotManagedRuntime testen und die Leserechte dafür eng vergeben.
Bis 12.12.2026	HR, Datenschutz, Interessenvertretung	Betriebs- oder Personalrat rechtzeitig nach § 90 BetrVG unterrichten. Eckpunkte vorlegen: keine Leistungs- und Verhaltenskontrolle, Freigabeprozess für Apps mit Beschäftigtendaten, Zweckbindung der Audit-Daten.
Bis 17.12.2026	Kommunikation	Belegschaft und Maker informieren: wer bauen darf, wie man Credits beantragt, was nicht gebaut werden darf, wer bei Fragen hilft.
Q1 2027	Entscheider	Rahmenbetriebsvereinbarung oder Dienstvereinbarung abschließen, Pilot auswerten, dann gruppenweise ausrollen.

Tipp: Gruppen statt Einzelpersonen, und zwar überall dieselben

Lege eine Entra-Sicherheitsgruppe „CMR-Maker-Pilot“ an und verwende sie konsequent: im Cowork-Schalter, in der Copilot-Studio-Einstellung und in der Ausgabenrichtlinie. Dann ist die Erweiterung später ein Gruppenmitglied mehr und kein Konfigurationsmarathon durch drei Admin Center. Beachte bei überlappenden Ausgabenrichtlinien: Es gilt die Richtlinie mit dem höchsten Limit pro Person, die Limits setzen sich zum Monatsersten zurück.

Zu den Kosten noch ein Wort aus der Praxis. Microsofts eigene Beispielrechnung kommt für eine Abteilungs-App mit 300 Anwendern, einem Start pro Tag und acht Datenaufrufen auf rund 60 bis 120 US-Dollar im Monat. Das ist nicht die Rechnung, vor der du Angst haben musst. Teuer wird das Bauen: Cowork verbraucht beim Generieren und Nachbessern deutlich mehr Credits als die spätere Ausführung. Ein Maker, der seine App 40-mal „noch ein bisschen hübscher“ machen lässt, finanziert dir keinen Mehrwert, sondern eine Rechenzentrumsheizung. Deshalb Bau-Limits getrennt von Laufzeit-Limits planen.

Und dann die Kommunikation, die meistens vergessen wird. Sag der Belegschaft offen, dass App-Bau ab sofort möglich ist, wo die Grenzen liegen und warum. Ein guter Satz für das Intranet: „Bau dir Werkzeuge für deine Arbeit, nicht für die Arbeit deiner Kollegen." Wer Apps über Personen baut, braucht vorher die Freigabe. Klingt streng, erspart aber die Einigungsstelle, die erfahrungsgemäß länger dauert als jeder Microsoft-Rollout.

Die Administratorenübersicht mit allen Schaltern beschreibt Microsoft im Artikel Übersicht über Microsoft Copilot Managed Runtime für Administratoren auf Microsoft Learn.

Häufig gestellte Fragen

Wie schalte ich die App-Erstellung in Copilot Cowork ab?

Im Microsoft 365 Admin Center unter Copilot › Cowork › Settings › Build apps in Copilot wählst du No users oder Specific users and groups. Bereits gebaute Apps können ihre Besitzer danach weiterhin öffnen, teilen und löschen, aber nicht mehr bearbeiten.

Kann man die Umgebungsweiterleitung für Copilot Managed Runtime deaktivieren?

Nein, laut Microsoft ist das Routing für Copilot Managed Runtime in allen Tenants aktiv und nicht abschaltbar. Steuern lässt sich aber, wer überhaupt Apps bauen darf, und damit, ob persönliche Umgebungen entstehen.

Welche Lizenz brauchen Anwender, um eine geteilte Copilot-App zu starten?

Sie brauchen eine Power-Apps-Premium-Lizenz oder müssen in einer Ausgabenrichtlinie für Copilot Credits stehen, die den Dienst Copilot Managed Runtime einschließt. Die Nutzungsrechte aus Microsoft 365 E3 oder E5 und eine Copilot-Lizenz allein reichen dafür nicht.

Ist der Betriebsrat bei Copilot Managed Runtime mitbestimmungspflichtig?

In aller Regel ja, weil die Plattform App-Starts personenbezogen protokolliert und selbstgebaute Apps Verhaltens- und Leistungsdaten auswerten können, was unter § 87 Abs. 1 Nr. 6 BetrVG fällt. Praktikabel ist eine Rahmenvereinbarung mit Freigabeprozess für Apps, die Beschäftigtendaten verarbeiten; in Behörden gilt das Personalvertretungsrecht entsprechend.

Was kostet der Betrieb einer App auf Copilot Managed Runtime?

Microsoft berechnet 0,1 Copilot Credit pro API-Aufruf, 100 Credits kosten 1 US-Dollar und decken rund 1.000 Aufrufe. Eine Abteilungs-App mit 300 täglichen Anwendern liegt laut Microsofts Beispielrechnung bei etwa 60 bis 120 US-Dollar im Monat, das Bauen der App wird zusätzlich abgerechnet.