KI & Copilot

Copilot Cowork: Power-Platform-Konnektoren werden über das Microsoft 365 Admin Center gesteuert

Executive Summary

Copilot Cowork, Microsofts Agent für lange, mehrstufige Aufgaben, darf jetzt auch außerhalb von Microsoft 365 zugreifen. Laut Microsoft-Ankündigung MC1542062, zuletzt geändert am 06.11.2026, nutzt Cowork **Power-Platform-Konnektoren, die als Plugins veröffentlicht sind**. Damit spricht der Agent mit CRM, Ticketsystem, Cloud-Speicher und allem anderen, wofür es einen Konnektor gibt. Gesteuert wird das nicht im Power Platform Admin Center, sondern im **Microsoft 365 Admin Center unter Agents › Tools**: Konnektor erlauben oder blockieren, fertig.

Der Haken steht in einem einzigen Satz der Meldung: **Die DLP-Richtlinien des Power Platform Admin Centers gelten für Cowork nicht.** Wer seit Jahren sauber pflegt, dass Salesforce und private Gmail-Konten nie im selben Flow landen, hat für Cowork genau null Schutz davon. Das ist keine Kleinigkeit, das ist eine Governance-Lücke mit Ansage.

Wichtig: Kein Fristsignal, aber ein Entscheidungsbedarf

Der Rollout soll weltweit bis Mitte November 2026 abgeschlossen sein. Das ist Microsofts Liefertermin, **keine Handlungsfrist für dich**. Es gibt nichts, was an einem bestimmten Tag kaputtgeht. Es gibt aber eine Frage, die du aktiv beantworten musst: Welche Drittanbieter-Konnektoren darf Cowork benutzen? Wer die Frage nicht beantwortet, hat sie trotzdem beantwortet, nur eben nicht selbst.

Worum geht es im Detail?

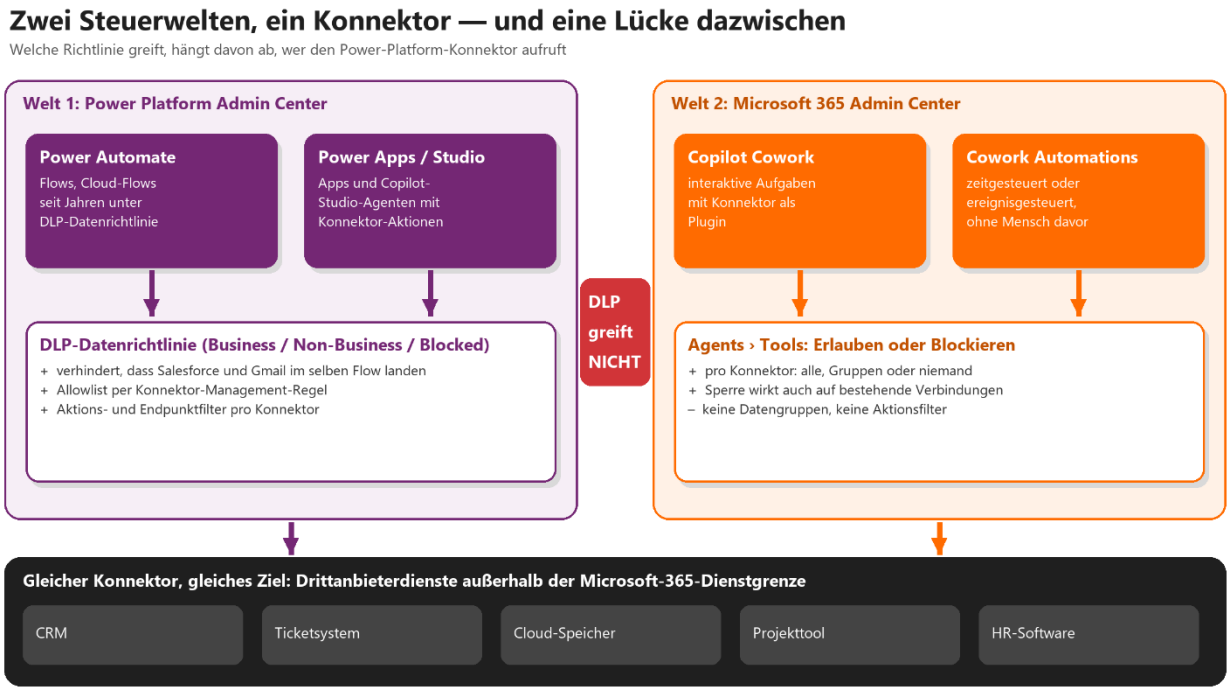
Kurzer Rückblick, damit die Einordnung stimmt. Copilot Cowork ist seit Juni 2026 allgemein verfügbar. Anders als Copilot Chat beantwortet Cowork keine Fragen, es **erledigt Aufgaben**: Es plant, ruft Werkzeuge auf, arbeitet in einer isolierten Umgebung innerhalb der Microsoft-365-Dienstgrenze und liefert am Ende ein Ergebnis ab. Zugang bekommt nur, wer eine Microsoft-365-Copilot-Lizenz hat **und** in einer Ausgabenrichtlinie für Copilot Credits steht, denn Cowork wird nutzungsbasiert abgerechnet. Jeder Werkzeug- und Konnektoraufruf kostet also mit.

Erweitert wird Cowork über **Plugins**. Ein Plugin ist ein Paket im gleichen Format wie Teams-Apps und Copilot-Agenten und kann zwei Dinge enthalten: Skills, also gelernte Arbeitsabläufe, und Konnektoren zu externen Diensten. Bisher waren das vor allem Microsofts eigene Plugins für Dynamics 365 und Fabric sowie MCP-Server von Partnern. Mit MC1542062 kommt der große Fundus der Power Platform hinzu: Hunderte Konnektoren, die Power Automate seit Jahren benutzt, stehen nach und nach auch Cowork zur Verfügung. Microsoft fügt sie laufend dem Admin Center hinzu, und sobald einer dort auftaucht, ist er in Cowork nutzbar.

Was die Meldung konkret zusagt:

Regel laut MC1542062	Was das praktisch heißt
Admins erlauben oder blockieren unterstützte Konnektoren unter Agents › Tools	Steuerung pro Konnektor, für alle, für Gruppen oder für niemanden
Cowork beachtet die Einstellung beim Anlegen von Verbindungen und beim Ausführen von Aktionen	Auch Verbindungen, die vor der Sperre angelegt wurden, sind danach tot
Konnektor-Richtlinien gelten auch für Cowork Automations	Zeit- und ereignisgesteuerte Aufgaben ohne Mensch davor sind eingeschlossen
Weitere Konnektoren kommen laufend hinzu	Deine Liste ist nie fertig, sie braucht einen Prüfrhythmus
E-Mail, Kalender, Teams und Dateien bleiben unberührt	Die Microsoft-365-Grundfunktionen von Cowork ändern sich nicht
DLP-Richtlinien der Power Platform gelten nicht für Cowork	Deine bestehende Konnektor-Klassifizierung ist hier wirkungslos

Warum baut Microsoft das so? Die Antwort ist organisatorisch, nicht technisch. Cowork gehört zur Microsoft-365-Copilot-Familie, und die wird zentral im Microsoft 365 Admin Center verwaltet: Agenten, Plugins, Ausgabenrichtlinien, Modellauswahl. Die Power-Platform-DLP stammt aus der Welt der Low-Code-Entwickler und kennt Umgebungen, Datengruppen und Konnektoraktionen. Cowork lebt in keiner Power-Platform-Umgebung. Also hat Microsoft die Steuerung dorthin gelegt, wo Cowork wohnt, und dabei das feinere Werkzeug zurückgelassen. Zwei Admin Center, ein Konnektor, zwei Regelwerke. Willkommen in der Cloud.



Fakten: Was Microsoft auf Learn zur Plugin-Steuerung dokumentiert

Plugins verwalten darf, wer Mandanten-Admin ist oder die Rolle Copilot-Administrator hat. Nutzer brauchen eine Microsoft-365-Copilot-Lizenz. Eine länder- oder regionsbasierte Freigabe gibt es nicht, dafür sind Sicherheitsgruppen vorgesehen. Konnektoren mit Anmeldung lassen sich **nicht stellvertretend autorisieren**: Jeder Nutzer muss die Anmeldung beim Drittanbieter selbst durchlaufen, Cowork merkt sich die Zustimmung danach, bis sie widerrufen wird. Plugin-Aktivitäten erscheinen im Microsoft-Purview-Überwachungsprotokoll unter Copilot-Aktivitäten, mit Audit Standard ohne Zusatzkosten.

Die vollständige Admin-Anleitung beschreibt Microsoft unter Manage plugins for Copilot Cowork, die Zugriffssteuerung über Ausgabenrichtlinien unter Manage Copilot Cowork for your organization.

Was sind Chancen? Was sind Risiken?

Die Chance ist real. Stell dir den Vertriebsinnendienst eines Mittelständlers vor, der Freitag für Freitag dieselbe Übung macht: offene Angebote aus dem CRM ziehen, mit den Ticketständen aus dem Servicesystem abgleichen, eine Zusammenfassung für die Geschäftsführung bauen. Zwei Stunden Copy-and-paste, jede Woche, seit 2019. Mit einem freigegebenen Konnektor erledigt Cowork das als Automation am Freitagmorgen, und der Kollege kann sich wieder dem widmen, wofür er eingestellt wurde. Oder der Kaffeemaschine.

Zweiter Vorteil: Die Steuerung ist simpel. Ein Schalter pro Konnektor, gruppenweise Freigabe, und eine Sperre wirkt sofort auch auf bestehende Verbindungen. Das ist ehrlicher als manches Governance-Konstrukt, das nur auf dem Papier existiert.

Chance	Risiko
Cowork erreicht endlich die Fachanwendungen, in denen die Arbeit wirklich passiert	Daten fließen per KI-Agent zu Drittanbietern, ohne dass die Power-Platform-DLP mitredet
Einfache Steuerung: erlauben, für Gruppen freigeben, blockieren	Keine Datengruppen, keine Aktionsfilter: entweder ganz oder gar nicht
Sperre wirkt auch auf bereits angelegte Verbindungen	Neue Konnektoren erscheinen laufend, die Freigabeliste veraltet still
Automations sparen wiederkehrende Routinearbeit	Automations handeln ohne Mensch davor, mit den Rechten des Erstellers
Purview-Audit protokolliert Plugin-Aktivitäten	Protokolle über Arbeitsverhalten sind ein Fall für die Mitbestimmung

Jetzt zum unangenehmen Teil. Die Power-Platform-DLP kann heute deutlich mehr als ein Ein-Aus-Schalter: Sie trennt Business- von Non-Business-Konnektoren, damit Firmendaten nicht in private Dienste wandern, sie sperrt einzelne Aktionen wie „Datei löschen“ und filtert Endpunkte. Nichts davon gilt für Cowork. Der Agent darf mit einem freigegebenen Konnektor alles, was der Konnektor kann, und er darf zwei freigegebene Konnektoren beliebig kombinieren. Wenn du einen Konnektor zu einem privaten Cloud-Speicher freigibst und einen zum CRM, kann eine Cowork-Aufgabe theoretisch die Kundenliste vom einen in den anderen tragen. Die DLP hätte das verhindert. Hier hindert sie niemand.

Warnung: Die Governance, die nur in Welt 1 wohnt

Ein Logistikunternehmen hat 2023 nach einem Vorfall die Power-Platform-DLP penibel aufgebaut: 40 Konnektoren in Business, alles mit Consumer-Bezug geblockt, der Betriebsrat hat unterschrieben, der Datenschutzbeauftragte hat geweint vor Glück. Im Dezember 2026 fragt der Vertriebsleiter, warum Cowork seine Dropbox nicht findet. Ein freundlicher Admin gibt den Konnektor unter Agents › Tools frei, weil er ja „in der Power Platform ohnehin geregelt" ist. Ist er. Dort. **Für Cowork existiert die Regel nicht.** Drei Jahre Governance, ausgehebelt durch einen Klick im falschen Admin Center. Kein Hacker nötig, nur gute Absichten.

Sicherheit und Priorität: Das ist keine Sicherheitslücke im klassischen Sinn, niemand Unbefugtes kommt herein. Es ist eine **Abflusslücke**: Befugte Nutzer bekommen einen Agenten, der Daten effizienter bewegt, als es ihnen je selbst gelungen wäre. Hinzu kommt: Information Barriers aus Microsoft Purview unterstützt die Plugin-Verwaltung laut Microsoft-Dokumentation derzeit nicht. Wer Ethikmauern zwischen Abteilungen braucht, etwa in Kanzleien oder Banken, sollte Konnektoren besonders zurückhaltend freigeben. Priorität: hoch, Dringlichkeit: mittel. Ein Nachmittag Arbeit jetzt erspart dir einen Vorfallbericht im Frühjahr.

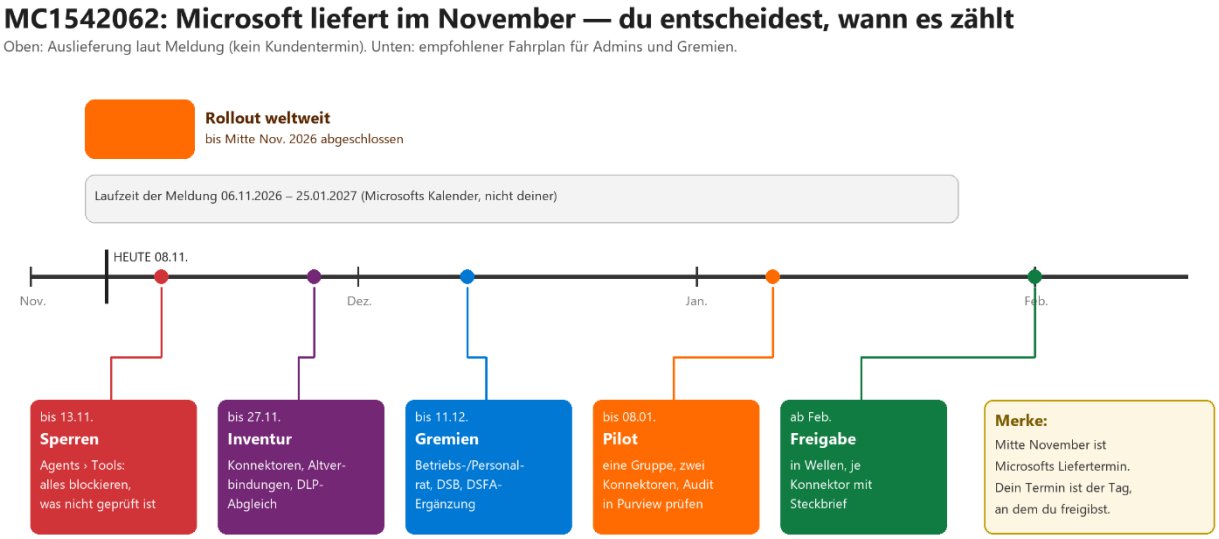
Datenschutz: Ein Konnektor zu einem Drittanbieter bedeutet, dass Daten die Microsoft-365-Dienstgrenze verlassen. Microsofts Zusagen zur EU-Datengrenze enden genau dort. Für jeden freigegebenen Konnektor gilt deshalb: Gibt es einen Auftragsverarbeitungsvertrag mit dem Zielanbieter, wo verarbeitet er, gibt es Drittlandtransfer? Die Datenschutz-Folgenabschätzung für Copilot, die du hoffentlich hast, deckt Drittanbieter-Konnektoren mit an Sicherheit grenzender Wahrscheinlichkeit nicht ab. Ergänzen.

Mitbestimmung: Nach § 87 Abs. 1 Nr. 6 BetrVG bestimmt der Betriebsrat bei technischen Einrichtungen mit, die **geeignet** sind, Verhalten oder Leistung zu überwachen. Cowork protokolliert Plugin-Aktivitäten im Überwachungsprotokoll, Automations laufen unter der Identität ihres Erstellers, und Drittsysteme führen eigene Protokolle über jeden Aufruf. Das ist geeignet, ganz ohne böse Absicht. Hast du eine Rahmenvereinbarung zu Microsoft 365 oder Copilot, prüfe, ob neue Konnektoren als „neue Funktion" vorlagepflichtig sind. Viele Vereinbarungen enthalten dafür eine Anlage mit freigegebenen Komponenten, die sich elegant um eine Konnektor-Positivliste erweitern lässt. In Behörden gilt das Personalvertretungsrecht, im Bund § 80 Abs. 1 Nr. 21 BPersVG, in den Ländern die jeweiligen Landespersonalvertretungsgesetze.

Lizenzen und Kosten: Cowork-Konnektoraufrufe laufen über Copilot Credits, nicht über Power-Automate-Lizenzen. Jede Automation, die jeden Morgen um sieben drei Systeme abfragt, verbraucht Credits, auch an den Tagen, an denen niemand das Ergebnis liest. Ausgabenrichtlinien pro Gruppe sind dein Werkzeug gegen die Überraschung beim Monatsabschluss.

Was müssen wir jetzt schon vorbereiten?

Was passiert, wenn du nichts tust? Konnektoren tauchen in deinem Admin Center auf, und je nach Freigabezustand nutzt Cowork sie oder eben nicht. Microsoft sagt in der Meldung nicht ausdrücklich, ob neu hinzukommende Konnektoren standardmäßig erlaubt oder gesperrt sind. Genau deshalb solltest du nicht raten, sondern nachsehen. Die Verantwortung für die Liste liegt ab sofort bei dir, nicht bei der Power-Platform-DLP.



So gehst du vor: Melde dich als Mandanten-Admin oder Copilot-Administrator im Microsoft 365 Admin Center an, öffne **Agents › Tools** und filtere auf Power-Platform-Konnektoren. Prüfe für jeden Eintrag den Reiter Benutzer: verfügbar für alle, für bestimmte Gruppen oder blockiert. Alles, was du nicht bewusst freigeben willst, setzt du auf **Blockieren**. Danach vergleichst du deine Liste mit der DLP-Klassifizierung im Power Platform Admin Center: Was dort in Non-Business oder Blocked steht, darf hier nicht frei sein.

Wann	Was	Wer
bis 13.11.2026	Agents › Tools sichten; alle ungeprüften Power-Platform-Konnektoren blockieren	M365-Administration
bis 27.11.2026	Abgleich mit Power-Platform-DLP; Liste möglicher Freigaben mit Zweck, Datenart, Zielanbieter	M365- und Power-Platform-Administration
bis 11.12.2026	Betriebs- oder Personalrat und Datenschutzbeauftragten einbinden; DSFA um Drittanbieter-Konnektoren ergänzen	IT-Leitung, Datenschutz
bis 08.01.2027	Pilot mit einer Sicherheitsgruppe und zwei Konnektoren; Purview-Audit und Credit-Verbrauch prüfen	M365-Administration, Fachbereich
ab Februar 2027	Freigabe in Wellen; monatlicher Blick auf neu hinzugekommene Konnektoren	M365-Administration

Tipp: Ein Steckbrief pro Konnektor

Lege für jeden freigegebenen Konnektor eine halbe Seite an: Zweck, Zielanbieter, Datenkategorien, Auftragsverarbeitungsvertrag ja oder nein, berechtigte Gruppe, Verantwortlicher im Fachbereich. Dieselbe Seite dient dem Betriebsrat als Anlage, dem Datenschutzbeauftragten als Nachweis und dir als Gedächtnis, wenn in einem Jahr jemand fragt, wer eigentlich Trello freigegeben hat. Spoiler: Du warst es.

Warnung: Sperren wirkt rückwirkend, Abschalten nicht ganz sofort

Laut MC1542062 respektiert Cowork eine Sperre auch bei bereits angelegten Verbindungen. Microsofts Plugin-Dokumentation ergänzt, dass eine Plugin-Sperre für **neue Unterhaltungen** greift und laufende bis zu ihrem Ende weiterlaufen. Wenn du also im Ernstfall einen Konnektor blockierst, rechne mit einem kurzen Nachlauf, bevor wirklich Ruhe ist.

Wichtig: Kommunikation an die Belegschaft

Drei Sätze genügen: Cowork kann ab sofort mit ausgewählten externen Systemen arbeiten, welche das sind, steht auf der Intranetseite. Wer beim ersten Aufruf eine Anmeldung bei einem Drittanbieter sieht, meldet sich nur bei freigegebenen Diensten an. Wer einen weiteren Konnektor braucht, stellt einen Antrag, statt den Kollegen in der IT freundlich anzulächeln. Der letzte Satz ist der wichtigste.

Häufig gestellte Fragen

Gelten Power-Platform-DLP-Richtlinien für Copilot Cowork?

Nein. Laut Microsoft-Ankündigung MC1542062 greifen die Datenrichtlinien des Power Platform Admin Centers nicht für Cowork. Welche Power-Platform-Konnektoren Cowork nutzen darf, steuerst du ausschließlich im Microsoft 365 Admin Center unter Agents › Tools.

Wo blockiere ich einen Power-Platform-Konnektor für Copilot Cowork?

Im Microsoft 365 Admin Center unter Agents › Tools: Konnektor auswählen, im Reiter Benutzer die Verfügbarkeit auf bestimmte Gruppen einschränken oder Blockieren wählen. Die Sperre gilt laut Microsoft auch für Verbindungen, die vorher angelegt wurden, und für Cowork Automations.

Brauche ich für Cowork-Konnektoren eine Power-Automate-Lizenz?

Cowork setzt eine Microsoft-365-Copilot-Lizenz voraus und wird nutzungsbasiert über Copilot Credits abgerechnet, die über eine Ausgabenrichtlinie zugewiesen werden. Konnektor- und Werkzeugaufrufe zählen dabei zum Verbrauch, eine separate Power-Automate-Lizenz nennt Microsoft für Cowork nicht.

Muss der Betriebsrat Cowork-Konnektoren zustimmen?

In aller Regel ja, weil Cowork Plugin-Aktivitäten im Purview-Überwachungsprotokoll erfasst und Automations unter der Identität des Erstellers laufen, was zur Verhaltens- und Leistungskontrolle geeignet ist und damit unter § 87 Abs. 1 Nr. 6 BetrVG fällt. In Behörden gilt Entsprechendes nach dem Personalvertretungsrecht des Bundes oder der Länder.

Bleiben Daten bei Cowork-Konnektoren in der EU-Datengrenze?

Nur solange sie innerhalb von Microsoft 365 verarbeitet werden. Sobald ein Konnektor Daten an einen Drittanbieter übergibt, gelten dessen Verarbeitungsorte und Verträge, weshalb jeder Konnektor vor der Freigabe datenschutzrechtlich geprüft werden sollte.