



Stand: Juli 2026
Version 1.0 · DE

LEITFADEN FÜR ADMINS

Microsoft 365 Copilot: sicher bereitstellen

Voraussetzungen, Governance und Monitoring – der technische Fahrplan für die Copilot-Einführung, nach den offiziellen Microsoft-Empfehlungen.

Zielgruppe: IT-Administratoren, M365-, SharePoint-, Purview- und Entra-Verantwortliche sowie Einführungsteams

Bereitgestellt von der Copilotenschule.

Die Copilotenschule ist spezialisiert auf die Einführung und Weiterqualifizierung im Umfeld des Microsoft Copiloten. Wir befähigen Wissensarbeiter, Teams und Organisationen, Microsoft Copilot produktiv, sicher und wertschöpfend im Arbeitsalltag einzusetzen – praxisnah, an echten Arbeitsprozessen.

INHALT

Inhaltsverzeichnis

Wichtiger Hinweis / Haftungsausschluss	3
Admin-Checkliste für die Copilot-Einführung	3
1 · Die Pflicht-Voraussetzungen von Microsoft	4
2 · Die eigentliche Hürde: Datengrundlage & Berechtigungen	5
3 · Der technische Rollout in vier Phasen	6
4 · Governance & Sicherheit mit Microsoft Purview	6
5 · Rollen & Zuständigkeiten	7
6 · Monitoring: aktiviert ist nicht genutzt	7
7 · Extensibility governen: Agenten & Connectoren	7
8 · Die häufigsten Fehler bei der Bereitstellung	8
So begleiten wir Ihre Einführung	8
Quellen	9

RECHTLICHER HINWEIS

Wichtiger Hinweis / Haftungsausschluss

Dieser Leitfaden fasst den Stand von Juli 2026 zusammen und stützt sich auf die offizielle Microsoft-Dokumentation (siehe Quellen). Microsoft ändert Produktverhalten, Voraussetzungen und Lizenzmodelle laufend; Menüpfade und Details können sich seit Erscheinen geändert haben. Maßgeblich ist die jeweils aktuelle Microsoft-Learn-Dokumentation.

Der Leitfaden richtet sich an IT-Administratoren und Einführungsteams. Die Datenschutz- und Grounding-Details – Oversharing, Berechtigungssanierung, Restricted Content Discovery – behandelt der begleitende Grounding-Leitfaden für Admins.

Der Kerngedanke in einem Satz

„Copilot bereitzustellen dauert Minuten – ihn sicher und wirksam bereitzustellen ist die eigentliche Admin-Aufgabe.“ Nicht die Lizenz entscheidet über Erfolg oder Risiko, sondern Voraussetzungen, Datengrundlage und Governance.

Für Admins heißt das: Die technische Freischaltung ist der kleinste Schritt. Dieser kompakte Leitfaden bündelt die Pflicht-Voraussetzungen, die Governance-Weichen und das Monitoring – nach den offiziellen Microsoft-Empfehlungen.

ZUM ABHAKEN

Admin-Checkliste für die Copilot-Einführung

- ☐ Berechtigte Basislizenz und das Microsoft-365-Copilot-Add-on beschafft und je Nutzer zugewiesen – keine Device-based-Lizenzierung.
- ☐ Primäres Postfach in Exchange Online (On-Premises- und Hybrid-Postfächer werden für das Grounding nicht unterstützt).
- ☐ Entra-ID-Konten, aktuelle Microsoft-365-Apps und OneDrive bereitgestellt; Netzwerk-Endpunkte freigegeben (Drittanbieter-Cookies für die Office-Web-Apps).
- ☐ AI-Administrator-Rolle zugewiesen (verwaltet Copilot, Agenten und Nutzungsberichte).
- ☐ Berechtigungen und Oversharing geprüft – SharePoint Advanced Management und, wo nötig, Restricted SharePoint Search.
- ☐ Microsoft Purview eingerichtet: Vertraulichkeitskennzeichnungen, Audit-Log und DLP.
- ☐ Conditional-Access-Richtlinien geprüft (Copilot unterstützt mandantenweite CA in SharePoint).
- ☐ Pilotgruppe definiert; Readiness- und Nutzungsbericht bzw. Copilot Dashboard eingerichtet.

TEIL A · VORAUSSETZUNGEN

1 Die Pflicht-Voraussetzungen von Microsoft

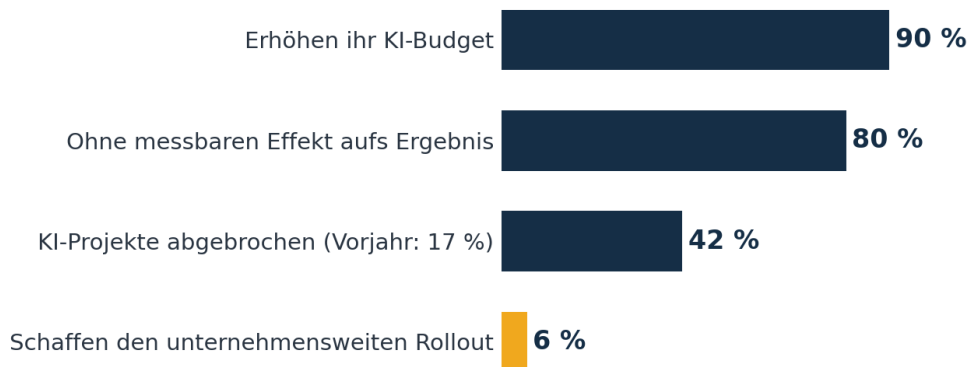
Microsoft nennt Voraussetzungen, ohne die Copilot nicht funktioniert – sie gehören vor jede Freischaltung:

- **Lizenzierung:** eine berechtigte Basislizenz (z. B. Microsoft 365 E3/E5/Business, in E7 bereits enthalten) plus das Copilot-Add-on, jedem Nutzer einzeln oder per Gruppe zugewiesen. Device-based-Lizenzierung wird nicht unterstützt.
- **Exchange Online:** Das primäre Postfach muss in Exchange Online liegen – On-Premises- oder Hybrid-Postfächer unterstützen das Mailbox-Grounding nicht.
- **Identität & Apps:** Entra-ID-Konto, aktuelle Microsoft-365-Desktop-Apps und OneDrive; für die Office-Web-Apps müssen Drittanbieter-Cookies erlaubt sein.
- **Netzwerk:** Die von Microsoft dokumentierten Endpunkte (Domains und WebSockets) dürfen nicht blockiert werden.

2 Die eigentliche Hürde: Datengrundlage & Berechtigungen

Die häufigste Ursache für Probleme ist nicht die Technik, sondern die Datengrundlage. Copilot ist berechtigungstreu – es findet nur, worauf ein Nutzer ohnehin Zugriff hat, macht damit aber jahrelang gewachsene Freigabe-Altlasten sofort sichtbar. Microsoft empfiehlt ausdrücklich, Berechtigungen vor dem Rollout zu prüfen und Oversharing zu reduzieren – mit SharePoint Advanced Management und, wo nötig, Restricted SharePoint Search.

Investition hoch – Wirkung niedrig



Quellen: Gartner (2024/25); McKinsey Global Survey on AI (2025).

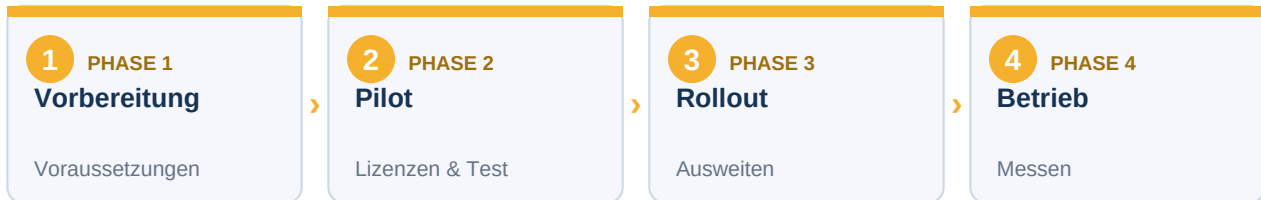
Der Zusammenhang: Ein sauberes Berechtigungs- und Governance-Fundament ist der Unterschied zwischen einem Rollout, der unter Wert bleibt, und einem, der trägt. Die Details – Freigabe-Linktypen, EEEU, Sanierungsfahrplan – behandelt der Grounding-Leitfaden für Admins.

[Zum Grounding-Detail-Leitfaden für Admins](#)

TEIL B · BEREITSTELLEN

3 Der technische Rollout in vier Phasen

Microsoft empfiehlt einen gestuften Rollout statt eines Big Bang. Bewährt hat sich dieser Ablauf:



- Phase 1 – Vorbereitung: Strategie und Use Cases definieren, Voraussetzungen schaffen, Berechtigungen und Oversharing prüfen (SharePoint Advanced Management, Purview), AI-Admin-Rolle zuweisen.
- Phase 2 – Pilot: Copilot-Lizenzen einer kleinen Gruppe zuweisen, den Readiness-Report prüfen, Feedback sammeln und die Konfiguration verfeinern.
- Phase 3 – Rollout: gruppenweise ausweiten, Conditional Access und Purview-Richtlinien greifen, Endnutzer schulen (Enablement Toolkit, Prompt Gallery).
- Phase 4 – Betrieb: Nutzung über Berichte und das Copilot Dashboard messen, inaktive Nutzer aktivieren, Agenten und Connectoren governen.

4 Governance & Sicherheit mit Microsoft Purview

Zentral eingeführt bleibt Copilot in der Microsoft-365-Compliance-Grenze (EU Data Boundary für kommerzielle Lizenzen): Daten verlassen den Tenant nicht und werden nicht für öffentliches Modelltraining genutzt. Für die Absicherung stellt Microsoft Purview die zentralen Werkzeuge bereit:

- Vertraulichkeitskennzeichnungen (Sensitivity Labels): steuern, welche Inhalte Copilot verarbeiten und ausgeben darf – Verschlüsselung und Nutzungsrechte werden respektiert.
- DLP, Audit-Log und eDiscovery: Copilot-Aktivitäten sind protokolliert und nachvollziehbar; DSPM for AI liefert Risiko-Einblick speziell für die KI-Nutzung.
- Restricted SharePoint Search und Restricted Content Discovery: begrenzen die Auffindbarkeit sensibler Inhalte, bis Berechtigungen saniert sind.

TEIL C · BETREIBEN & MESSEN

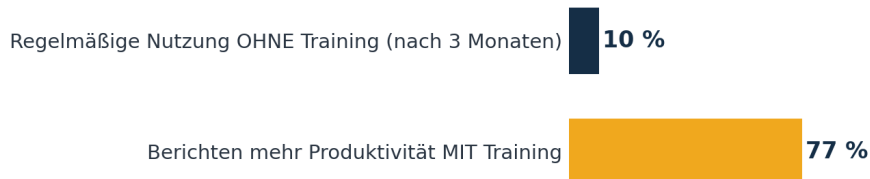
5 Rollen & Zuständigkeiten

Die zentrale Rolle ist der AI-Administrator: Er verwaltet Copilot und Agenten, gibt Line-of-Business-Agenten frei, sieht Health-Dashboards und Nutzungsberichte. Für Sicherheits- und App-Einstellungen kommen Security-Admin und Office-Apps-Admin hinzu, für Datengovernance die SharePoint- und Purview-Verantwortlichen. Eine klare Rollenzuteilung vor dem Rollout vermeidet Reibung im Betrieb.

6 Monitoring: aktiviert ist nicht genutzt

Microsoft stellt vier Reporting-Quellen bereit: den Readiness- und den Nutzungsbericht im Microsoft-365-Admin-Center, das Copilot Dashboard in Viva Insights (Readiness, Adoption, Impact, Sentiment) sowie die Purview-Audit-Logs. Die Kernfrage lautet: „Wir haben Lizenzen zugewiesen – wird Copilot auch genutzt?“ Der Nutzungsbericht zeigt inaktive Nutzer (etwa keine Nutzung in 28 Tagen) und kann sie über Organizational Messages gezielt anstoßen.

Der Unterschied ist die Begleitung



Quellen: Microsoft Work Trend Index; Forrester TEI (M365 Copilot).

Genau hier liegt der Wert der Investition: Aktivierte, aber ungenutzte Lizenzen kosten Geld ohne Wirkung. Messen Sie Nutzung statt Zuweisung – und steuern Sie mit Schulung und Kommunikation nach.

7 Extensibility governen: Agenten & Connectoren

Copilot lässt sich über Agenten (Copilot Studio) und Copilot-Connectoren erweitern. Das schafft Mehrwert, aber auch Governance-Bedarf: Line-of-Business-Agenten sollten über die AI-Admin-Freigabe laufen, Connectoren nur kuratiert und mit passenden Berechtigungen eingebunden werden. Microsoft rät bei autonomen Agenten in sensiblen Bereichen ausdrücklich zur Vorsicht. Behalten Sie Agenten-Metriken (Copilot Studio Analytics) im Blick.

8 Die häufigsten Fehler bei der Bereitstellung

- Rollout ohne Berechtigungs-Cleanup – Copilot macht Oversharing sofort sichtbar.
- Device-based-Lizenzierung oder On-Premises-/Hybrid-Postfächer – Copilot funktioniert dann nicht wie erwartet.
- Netzwerk-Endpunkte blockiert oder Drittanbieter-Cookies gesperrt – die Web-Apps liefern kein Copilot.
- Kein Monitoring – ohne Readiness- und Nutzungsbericht bleibt die Adoptionslücke unsichtbar.
- Purview und Conditional Access erst nach dem Rollout – Governance gehört vor die breite Freischaltung, nicht danach.

SO BEGLEITEN WIR IHRE EINFÜHRUNG

So begleiten wir Ihre Einführung

Die Copilotenschule begleitet Rollouts von der Strategie über die Governance bis zur breiten Adoption – und schult Admins wie Fachbereiche praxisnah. Passende Formate:

Change-Programm – Rollout-Begleitung inkl. Governance und Use-Case-Definition

Praxis-Training „Microsoft 365 Copilot“ – Befähigung der Fachbereiche

Grounding-Leitfaden für Admins (kostenloses PDF)

QUELLEN

Quellen

- Microsoft Learn: „Minimum requirements to deploy Microsoft 365 Copilot“ – Lizenzierung, Exchange Online, Entra ID, Netzwerk.
- Microsoft Learn: „Microsoft 365 app and network requirements for Microsoft 365 Copilot“ – Apps, OneDrive, Cookies, Endpunkte.
- Microsoft Learn: „Set up Microsoft 365 Copilot and assign licenses“ und „Rollout Microsoft 365 Copilot to your organization“ – phased rollout, Conditional Access, SharePoint Advanced Management, Purview.
- Microsoft Learn: „Get ready for Microsoft 365 Copilot with SharePoint Advanced Management“ und „Secure & governed data foundation for Microsoft 365 Copilot“.
- Microsoft Learn: „Microsoft 365 Copilot reporting options for admins“ – Readiness-/Nutzungsbericht und Copilot Dashboard (Viva Insights).
- Copilotenschule: die Grounding-Leitfäden sowie „Copilot im Unternehmen einführen: Rollout-Leitfaden“.