Stand: Juli 2026
Version 1.0 · DE

ADMIN-LEITFADEN

Microsoft 365 Copilot: Grounding sicher gestalten

Der technische Leitfaden für M365-Administratoren: Freigaben, Oversharing und die richtigen Steuerungen im Admin-Portal – damit Copilot nur findet, was er finden darf.

Zielgruppe: Microsoft-365-Administratorinnen und -Administratoren · SharePoint-, Purview- und Entra-Verantwortliche

---

Bereitgestellt von der Copilotenschule.

Die Copilotenschule ist spezialisiert auf die Einführung und Weiterqualifizierungen im Umfeld des Microsoft Copiloten. Im Gegensatz zu anderen Anbietern bieten wir den Teilnehmern keinen Bauchladen an Tools an, die in ihrem Umfeld nicht compliant oder wertschöpfend sind. Wir befähigen Wissensarbeiter, Teams und Organisationen, Microsoft Copilot produktiv, sicher und wertschöpfend im Arbeitsalltag einzusetzen. Unser praxisorientierter Trainingsansatz verbindet reale Arbeitsprozesse mit direkt anwendbaren Workflows.

INHALT

Inhaltsverzeichnis

RECHTLICHER HINWEIS

Wichtiger Hinweis / Haftungsausschluss

Die Recherche zu diesem Leitfaden wurde gründlich und nach bestem Wissen und Gewissen durchgeführt, und die getroffenen Aussagen wurden beim Schreiben sorgfältig gegen die zitierten Quellen geprüft (Stand der Prüfung: Juli 2026). Dennoch wird **keine Garantie für die Richtigkeit, Vollständigkeit oder Aktualität** der getroffenen Aussagen übernommen. Microsoft ändert Produktverhalten, Lizenzbedingungen und Dokumentation laufend; einzelne hier beschriebene Mechanismen können sich seit Erscheinen dieses Leitfadens geändert haben. Der Beitrag ersetzt weder Rechtsberatung noch eine tenant-spezifische Sicherheits- und Datenschutzprüfung; maßgeblich bleiben die jeweils aktuelle Herstellerdokumentation (am Ende dieses Leitfadens verlinkt) und die rechtliche Bewertung im Einzelfall.

Stand: Juli 2026. Alle zentralen Aussagen sind mit Quellen aus der offiziellen Microsoft-Dokumentation belegt; wo eine Aussage nicht wörtlich dokumentiert ist, sondern sich aus dokumentierten Einzelfakten ergibt, ist das im Text ausdrücklich gekennzeichnet.

Der Kerngedanke in einem Satz

„Wir haben kein Copilot-Problem. Wir haben ein SharePoint-Problem, das Copilot sichtbar macht.“ Microsoft 365 Copilot erzeugt keine neuen Zugriffe – er findet nur zuverlässig, was schon immer offen stand. Dieser Leitfaden zeigt Administratorinnen und Administratoren, mit welchen Einstellungen im Admin-Portal sie das Grounding von Copilot sicher gestalten: von der Prävention über die Bestandsaufnahme bis zur Sanierung und laufenden Kontrolle.

ZUM ABHAKEN

Checkliste: Grounding sicher gestalten

Die Kurzfassung des gesamten Leitfadens. Die Verweise (K1–K15) führen zum jeweiligen Kapitel mit Portal-Pfad und Einstellungsoptionen.

PHASE 1 · VOR DER ERSTEN COPILOT-LIZENZ

- [ ] DSPM-for-AI-Oversharing-Assessment in Microsoft Purview starten und die 100 meistgenutzten Sites bewerten. → K5
- [ ] Data-Access-Governance-Berichte (DAG) ziehen: EEEU-Report, Sharing-Link-Report, „Sites mit potenziellem Oversharing“. → K6
- [ ] Standard-Freigabelinktyp tenant-weit auf „Bestimmte Personen“ (oder mind. „Personen in Ihrer Organisation“) setzen. → K1
- [ ] „Jeder“-Links deaktivieren oder auf Ansicht-only mit Pflicht-Ablauf beschränken. → K2
- [ ] EEEU sowie „Everyone“- und „All Users“-Claims aus der Personenauswahl ausblenden (PowerShell). → K3
- [ ] Externe Freigabe je Site auf das nötige Maß stellen; Gastablauf und Einladungsrechte in Entra regeln. → K4

PHASE 2 · HOCHRISIKO-SITES ABSICHERN & SANIEREN

- [ ] Restricted Content Discovery (RCD) als Interimsschutz auf Hochrisiko-Sites aktivieren – hält Inhalte aus Suche & Copilot, ohne Berechtigungen zu ändern. → K7
- [ ] Site Access Reviews an die Site Owner delegieren; überzählige Nutzer, Gruppen, Links und EEEU entfernen lassen. → K9
- [ ] Sensitivity Labels (mit Verschlüsselung) verpflichtend einführen und per Auto-Labeling auf Bestandsdaten nachziehen. → K10
- [ ] DLP-Richtlinie für Microsoft 365 Copilot einrichten: gelabelte Inhalte von der Copilot-Verarbeitung ausschließen. → K11
- [ ] Inaktive Sites über Site-Lifecycle-Policies erkennen und archivieren (archivierte Inhalte fließen nicht in Copilot). → K12

PHASE 3 · ZUGANG, GRENZEN & LAUFENDER BETRIEB

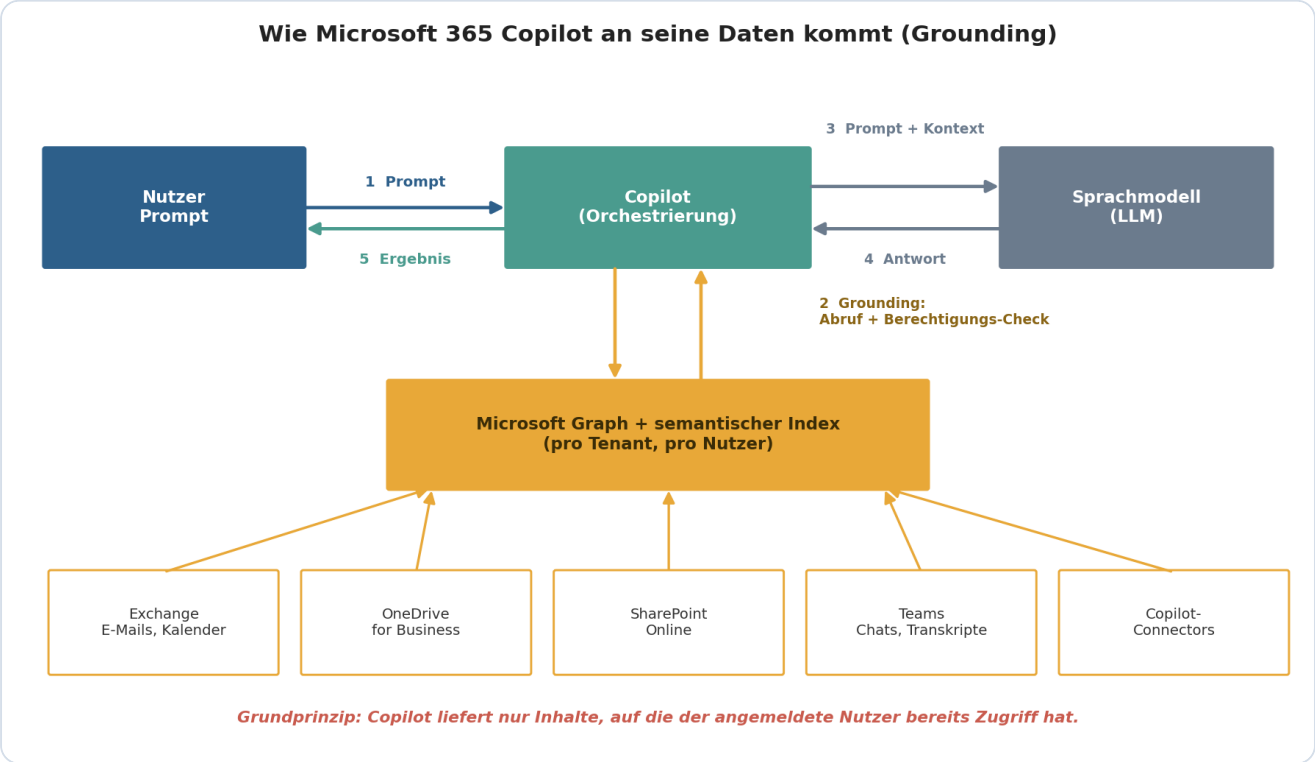
- [ ] Copilot-Lizenzen gezielt an eine Pilotgruppe zuweisen; Zugriff bei Bedarf über „Integrierte Apps“ steuern. → K15 · Zugang
- [ ] Web-Grounding (Bing) per „Allow web search in Copilot“ bewusst konfigurieren (an/aus/nur Web-Modus). → K14
- [ ] Externe-Meetings- und Transkriptionsregeln prüfen; Gäste über die Nutzung ihrer Beiträge informieren. → K13
- [ ] Audit-Routine aufsetzen: `CopilotInteraction` / „AccessedResources“ auswerten und Assessments zyklisch wiederholen. → K15
- [ ] Datenschutz-Hausaufgaben: Verzeichnis der Verarbeitungstätigkeiten, Transparenz gegenüber Beschäftigten, ggf. Betriebsvereinbarung (§ 87 BetrVG).

GRUNDLAGEN

Grounding, semantischer Index & Berechtigungen

Warum die eigentliche Arbeit nicht bei Copilot liegt, sondern bei den Berechtigungen.

Wenn ein Nutzer Copilot eine Frage stellt, passiert vor dem Sprachmodell ein entscheidender Schritt – das **Grounding**: Copilot reichert den Prompt mit Kontext aus dem Microsoft Graph des eigenen Tenants an (E-Mails, Chats, Dateien, Kalender, Meetings), bevor der angereicherte Prompt an das Modell geht. Nach der Antwort folgt ein Post-Processing, ebenfalls mit Graph-Zugriff.



So kommt Microsoft 365 Copilot an seine Daten: Prompt → Grounding über Microsoft Graph & semantischen Index → Sprachmodell → Antwort.

Das Fundament ist der **semantische Index**: eine vektorisierte Aufbereitung der Tenant-Inhalte, die inhaltliche Ähnlichkeit versteht statt nur Stichworte zu matchen. Ihn gibt es auf Tenant-Ebene (organisationsweit aus textbasierten SharePoint-Inhalten) und auf Nutzer-Ebene (personalisiert, für Nutzer mit bezahlter Copilot-Lizenz). Wichtig für die Steuerung: Die semantische Indexierung lässt sich **nicht abschalten** – sie respektiert aber ausnahmslos die Zugriffsgrenze.

Die eine Regel, aus der alles folgt

Laut Microsoft präsentiert Copilot „only data that each individual can access using the same underlying controls for data access used in other Microsoft 365 services“. Copilot ist also **berechtigungstreu**. Das Problem sind nicht die KI, sondern die über Jahre gewachsenen Berechtigungen. Ziel ist Microsofts Zero-Trust-Leitbild „just enough access“: jeder Nutzer genau so viel Zugriff wie nötig – und keinen Deut mehr. Prompts, Antworten und indizierte Daten werden nicht zum Training der Sprachmodelle verwendet; Zweckbindung, Transparenz, Aufbewahrung und Protokollierung bleiben aber Aufgabe der eigenen Organisation.

LESEHILFE

So lesen Sie die Kapitel

Jedes Kapitel folgt derselben Struktur: **Warum wichtig** (Auswirkung), **Wo im Admin-Portal** und **Einstellungsoptionen & Wirkung**. Zusätzlich zeigt eine Kennzeichnung, welche Lizenz eine Steuerung voraussetzt.

Kennzeichnung	Bedeutung
Bordmittel	Verfügbar ohne kostenpflichtiges Copilot-Add-on – in Standard-SharePoint, Entra bzw. per PowerShell/Cloud Policy.
Premium	Setzt Zusatzlizenzen voraus – meist SharePoint Advanced Management (in der Regel enthalten, sobald mindestens eine Microsoft-365-Copilot-Lizenz zugewiesen ist) oder Microsoft Purview/E5. Einzelne Funktionen (z. B. der Sensitivity-Label-Bericht) haben zusätzliche Anforderungen.
Portal	Nennt das Admin-Portal, in dem die Einstellung liegt (SharePoint, Purview, Entra, Microsoft 365 Admin Center, Teams, PowerShell).

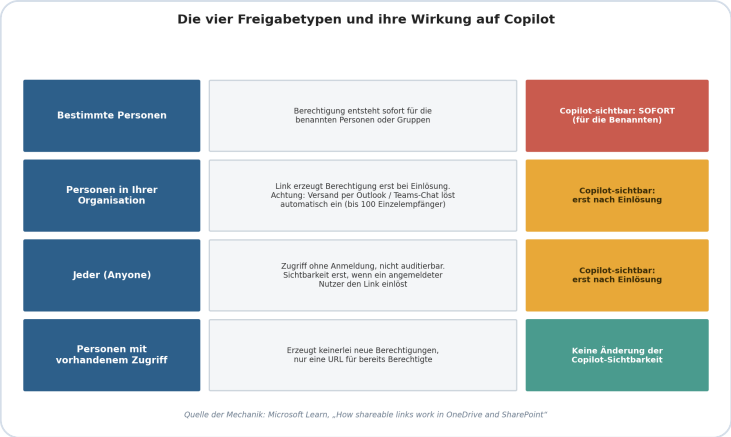
Hinweis zur Lizenzierung: Lizenzumfänge gehören zu den beweglichsten Teilen des Microsoft-Ökosystems. Prüfen Sie die konkreten Voraussetzungen vor Projektstart gegen die aktuelle Herstellerdokumentation (siehe Quellen).

TEIL A · LEITPLANKEN SETZEN (PRÄVENTION)

1 Standard-Freigabelinktyp festlegen

Bordmittel | SharePoint Admin Center · PowerShell

Der Teilen-Dialog bietet bis zu vier Linktypen – und der voreingestellte Typ entscheidet still darüber, wie viel in Suche und Copilot auffindbar wird. Der wirksamste einzelne Hebel ist deshalb der **Default-Linktyp**.



Die vier Freigabetypen und wann sie Inhalte für Copilot sichtbar machen.

WARUM WICHTIG (AUSWIRKUNG)

„Bestimmte Personen" macht eine Datei sofort für die benannten Empfänger such- und Copilot-relevant – bei einer Sicherheitsgruppe für *alle* Mitglieder. „Personen in Ihrer Organisation" (Firmenlink) wird dagegen erst durch Einlösung wirksam – aber Achtung: Beim Versand über SharePoint/OneDrive-UI, Outlook oder Teams-Chat gilt der Link für Einzelempfänger **automatisch als eingelöst (bis zu 100 Personen)**. „Personen mit vorhandenem Zugriff" vergibt keine neuen Rechte und ist der sicherste Typ für internen Versand.

WO IM ADMIN-PORTAL

SharePoint Admin Center → **Richtlinien** → **Freigabe** → Abschnitt „Standardlink für die Freigabe / Dateien- und Ordnerlinks". Per PowerShell: `Set-SPOTenant -DefaultSharingLinkType SpecificPeople` und `-DefaultLinkPermission View`.

EINSTELLUNGSOPTIONEN & WIRKUNG

Option	Wirkung auf Copilot-Sichtbarkeit
Standardtyp „Bestimmte Personen"	Empfohlen. Reduziert die automatische Auffindbarkeit in Enterprise Search und Copilot am stärksten.
Standardtyp „Personen in Ihrer Organisation"	Mindestniveau. Wirkt erst nach Einlösung – Vorsicht wegen Auto-Einlösung beim Versand.
Standard-Berechtigung „Ansicht" statt „Bearbeiten"	Verringert Schaden bei Fehlfreigaben; Empfehlung, wo möglich.
Default je Vertraulichkeit (via Sensitivity Label)	Erlaubt strengere Defaults für vertrauliche Inhalte (siehe K10).

2 „Jeder“-Links (Anyone-Links) einschränken

Bordmittel | SharePoint Admin Center · PowerShell

WARUM WICHTIG (AUSWIRKUNG)

Anyone-Links sind aus Governance-Sicht der problematischste Typ: Empfänger müssen sich **nicht authentifizieren**, und ihr Zugriff kann **nicht auditiert** werden. Zwar wird ein Anyone-Link erst durch Anklicken suchbar – löst ihn aber ein angemeldeter interner Nutzer ein, wird der Inhalt Teil seines Grounding-Horizonts. Zudem fehlen Anyone-Links ausgerechnet im Selbstauskunfts-Freigabebericht der Nutzer.

WO IM ADMIN-PORTAL

SharePoint Admin Center → **Richtlinien** → **Freigabe** → „Externe Freigabe“ und „Dateien- und Ordnerlinks → Jeder“. Ablauf/Berechtigung ebenda; per Site überschreibbar. PowerShell: `-RequireAnonymousLinksExpireInDays`, `-FileAnonymousLinkType`, `-FolderAnonymousLinkType`.

EINSTELLUNGSOPTIONEN & WIRKUNG

Option	Wirkung
Anyone-Links tenant-/site-weit deaktivieren	Bestehende anonyme Links werden sofort ungültig – stärkste Maßnahme.
Pflicht-Ablauffrist verkürzen	Setzt auch bestehende Links auf die neue, kürzere Frist – begrenzt Altlasten automatisch.
Berechtigung auf „Nur Ansicht“ beschränken	Verhindert anonyme Bearbeitung; reduziert Missbrauchsrisiko.

3 EEEU & „Everyone“-Claims deaktivieren

Bordmittel | PowerShell (SharePoint Online Management Shell)

WARUM WICHTIG (AUSWIRKUNG)

„Everyone except external users“ (EEEU) ist kein Link, sondern eine echte Berechtigung – und deshalb riskanter als jeder Sharing-Link: Es gibt **keinen Einlöse-Schritt**, alle internen Nutzer haben sofort Zugriff. Microsoft: „EEEU makes content public … the entire content of the site becomes public and more prone to oversharing.“ EEEU-Inhalt ist damit grundsätzlich organisationsweit in Suche und Copilot auffindbar – der Klassiker in historisch gewachsenen Tenants.

WO IM ADMIN-PORTAL

Ausblenden künftiger Vergaben per PowerShell: `Set-SPOTenant -ShowEveryoneExceptExternalUsersClaim $false`, analog `-ShowEveryoneClaim $false` und `-ShowAllUsersClaim $false`. **Bestehende** EEEU-Berechtigungen werden damit nicht entfernt – sie müssen über DAG-Berichte (K6) gefunden und via Site Access Review (K9) entfernt werden.

Wichtig: Das Ausblenden verhindert nur *neue* Vergaben. Ohne aktive Bereinigung der Altbestände bleibt EEEU wirksam.

4 Externe Freigabe & Gastzugriff steuern

Bordmittel | SharePoint Admin Center · Microsoft Entra Admin Center

WARUM WICHTIG (AUSWIRKUNG)

Externe Freigabe und Gastkonten bestimmen, wer von außen Inhalte in Ihren Tenant bringt oder aus ihm sieht. Gäste können in Ihrem Tenant zwar keinen Copilot nutzen – aber alles, was ein Gast in Ihren Teams einstellt, liegt in Ihrem Tenant und ist für Ihre lizenzierten internen Nutzer ganz normales Copilot-Material.

WO IM ADMIN-PORTAL

SharePoint Admin Center → **Richtlinien** → **Freigabe** (externe Freigabestufe je Organisation und je Site). Microsoft Entra Admin Center → **Externe Identitäten** → **Einstellungen für die externe Zusammenarbeit** (wer darf Gäste einladen) sowie Gastablauf. Die Entra-Einstellungen übersteuern die SharePoint-Einstellungen, wenn sie restriktiver sind.

EINSTELLUNGSOPTIONEN & WIRKUNG

Option	Wirkung
Externe Freigabestufe je Site (von „Jeder“ bis „nur Organisation“)	Passt das Risiko pro Site an; sensible Sites strenger stellen.
Gastzugriff mit automatischem Ablauf (in Tagen)	Verhindert dauerhaft „vergessene“ Gastkonten.
Einladungsrechte einschränken (Entra)	Nur berechtigte Rollen dürfen Gäste einladen – weniger Wildwuchs.

TEIL B · OVERSHARING SICHTBAR MACHEN (ASSESSMENT)

5 DSPM for AI – Oversharing-Assessment

Premium (Microsoft Purview / E5-Teile) | Microsoft Purview Portal

WARUM WICHTIG (AUSWIRKUNG)

Data Security Posture Management for AI (DSPM for AI) liefert die Bestandsaufnahme: Ein Standard-Datenrisiko-Assessment läuft **automatisch wöchentlich** über die 100 meistgenutzten SharePoint-Sites und zeigt pro Site, welcher Anteil der Inhalte mit „jedem“, „allen in der Organisation“, „bestimmten Personen“ oder extern geteilt ist. Ohne diese Sicht sanieren Sie blind.

WO IM ADMIN-PORTAL

Microsoft Purview Portal (`purview.microsoft.com`) → **DSPM für KI** → Empfehlungen & Assessments. Vertiefte Auswertung von Copilot-Aktivitäten über den **Activity Explorer** in DSPM for AI.

EINSTELLUNGSOPTIONEN & WIRKUNG

Funktion	Wirkung
Oversharing-Assessment (wöchentlich)	Priorisiert Sites nach Freigabe-Risiko; Grundlage der Sanierungsliste.
Empfehlungen umsetzen	Führt direkt zu passenden Kontrollen (Labels, DLP, RCD).
Activity Explorer	Zeigt, welche sensiblen Inhalte Copilot tatsächlich berührt.

6 Data-Access-Governance-Berichte (DAG)

Premium (SharePoint Advanced Management) | SharePoint Admin Center

WARUM WICHTIG (AUSWIRKUNG)

DAG-Berichte aus SharePoint Advanced Management (SAM) liefern die technische Detailsicht: Berechtigungs-Snapshots über alle Sites, Sharing-Link-Aktivität der letzten 28 Tage (getrennt nach Anyone-, Organisations- und Specific-People-Links), **EEEU-Auswertungen** und einen Bericht, welche Sites ein bestimmter Nutzer erreichen kann. Das Content Management Assessment bündelt die Befunde zu einer Copilot-Readiness-Einschätzung.

WO IM ADMIN-PORTAL

SharePoint Admin Center → **Berichte** → **Datenzugriffs-Governance**. Microsoft empfiehlt, das Content Management Assessment alle 30 Tage zu wiederholen.

Lizenz: SAM ist in der Regel enthalten, sobald mindestens eine Microsoft-365-Copilot-Lizenz zugewiesen ist; einzelne Randfunktionen und der Sensitivity-Label-Bericht (E5) haben Zusatzanforderungen.

TEIL C · OVERSHARING EINDÄMMEN & SANIEREN

7 Restricted Content Discovery (RCD)

Premium (SAM · Copilot-Lizenz) | SharePoint Admin Center

WARUM WICHTIG (AUSWIRKUNG)

RCD ist das Mittel der Wahl, um „die Blutung zu stoppen“, bevor einzelne Berechtigungen angefasst werden: Eine Site-Einstellung hält deren Inhalte aus der organisationsweiten Suche und aus Copilot heraus – **ohne eine einzige Berechtigung zu ändern**. Wer kürzlich mit einem Inhalt gearbeitet hat, sieht ihn weiterhin.

WO IM ADMIN-PORTAL

SharePoint Admin Center → **Aktive Websites** (Spalte/Einstellung „Restricted Content Discovery“) bzw. über die entsprechende Richtlinie; steuerbar je Site und tenant-weit.

EINSTELLUNGSOPTIONEN & WIRKUNG

Aspekt	Wirkung
RCD auf Hochrisiko-Site aktivieren	Nimmt Auffindbarkeit & Copilot-Verwertbarkeit heraus – als Interimsschutz.
Grenze OneDrive	RCD wirkt nur für SharePoint-Sites, **nicht** für OneDrive.
Große Sites (> 500.000 Elemente)	Umsetzung kann länger als eine Woche dauern – Zeit einplanen.
Nach Sanierung	RCD wieder entfernen, damit Copilot dort Nutzen stiftet.

8 Restricted SharePoint Search & Restricted Access Control

Bordmittel (RSS) | Premium (RAC · SAM) | SharePoint Admin Center

WARUM WICHTIG (AUSWIRKUNG)

Restricted SharePoint Search (RSS) war die schnelle Notbremse: Es beschränkte die organisationsweite Suche auf eine Positivliste von maximal 100 Sites. Microsoft hat RSS aber stets als Kurzzeitlösung deklariert – ab dem **31. Juli 2026** ist eine Neuaktivierung blockiert. Planen Sie neue Vorhaben mit RCD (K7), nicht mit RSS. Für den Extremfall existiert **Restricted Access Control (RAC)**: Es beschränkt den Zugriff auf eine Site hart auf eine definierte Gruppe – auch für Nutzer, die vorher Berechtigungen oder Links hatten.

WO IM ADMIN-PORTAL

SharePoint Admin Center → Sucheinstellungen (RSS, Auslauf) bzw. Site-Richtlinien / SAM (RAC).

EINSTELLUNGSOPTIONEN & WIRKUNG

Werkzeug	Wirkung / Status
RSS (Positivliste ≤ 100 Sites)	Auslaufend – ab 31.07.2026 keine Neuaktivierung. Nicht mehr einplanen.
RAC (harte Zugriffsbeschränkung)	Beschränkt Site-Zugriff auf eine definierte Gruppe – auch entgegen bestehender Rechte.

9 Site Access Reviews – Sanierung delegieren

Premium (SharePoint Advanced Management) SharePoint Admin Center

WARUM WICHTIG (AUSWIRKUNG)

Die eigentliche Sanierung kann kein Admin allein leisten – die Entscheidung, wer auf eine Fachbereichs-Site gehört, treffen die Site Owner am besten (IT-Admins dürfen die Inhalte oft gar nicht sehen). Site Access Reviews schicken die DAG-Befunde direkt an die Site Owner zur Bereinigung.

WO IM ADMIN-PORTAL

SharePoint Admin Center → aus dem **DAG-Bericht** heraus „Websitezugriffsüberprüfung anfordern“. Der Site Owner erhält die Befunde und arbeitet sie ab.

EINSTELLUNGSOPTIONEN & WIRKUNG

Schritt des Site Owners	Wirkung
Überzählige Nutzer, Gruppen & unternehmensweite Links inkl. EEEU entfernen	Beendet konkretes Oversharing an der Wurzel.
Gebrochene Berechtigungsvererbung reparieren	Stellt nachvollziehbare Rechte wieder her.
Ownership bestätigen	Sichert dauerhafte Verantwortlich-keit.

Vorsicht bei Massenbereinigung: Ein Cmdlet `Remove-SPOSiteSharingLinks` existiert in der dokumentierten SharePoint-PowerShell *nicht*. Massenbereinigung läuft über die Graph-Permissions-API oder Community-Werkzeuge (z. B. PnP-PowerShell) – stets zuerst gegen einen isolierten Test-Satz von Sites prüfen.

TEIL D · INHALTE SELBST SCHÜTZEN

10 Sensitivity Labels & Auto-Labeling

Premium (Purview / E5 für Auto-Labeling & Verschlüsselung) | Microsoft Purview Portal

WARUM WICHTIG (AUSWIRKUNG)

Sensitivity Labels mit Verschlüsselung sind die **einzige Kontrolle, die am Inhalt selbst klebt** – sie greift auch dann noch, wenn Berechtigungen falsch stehen. Entscheidend für Copilot: Verschlüsselte Inhalte darf Copilot nur verwenden, wenn der Nutzer neben dem Recht VIEW auch das Nutzungsrecht **EXTRACT** besitzt.

WO IM ADMIN-PORTAL

Microsoft Purview Portal → **Information Protection** → **Bezeichnungen (Labels)** und **Richtlinien zur automatischen Bezeichnung (Auto-Labeling)**. Auto-Labeling zieht Labels auf Bestandsdaten nach.

EINSTELLUNGSOPTIONEN & WIRKUNG

Option	Wirkung
Label mit Verschlüsselung + EXTRACT-Steuerung	Copilot verwendet Inhalt nur bei ausreichendem Nutzungsrecht.
Auto-Labeling auf Bestandsdaten	Klassifiziert Altbestände automatisch – Basis für DLP (K11) und Default-Links (K1).
Label-gebundene Freigabe-Defaults	Erzwingt strengere Freigaberegeln je Vertraulichkeitsstufe.

11 DLP-Richtlinie für Microsoft 365 Copilot

Premium (Microsoft Purview DLP) | Microsoft Purview Portal

WARUM WICHTIG (AUSWIRKUNG)

Eine DLP-Richtlinie für den Speicherort „Microsoft 365 Copilot“ schließt Dateien und E-Mails mit bestimmten Sensitivity Labels von der **Copilot-Verarbeitung** aus – die Inhalte fließen dann nicht mehr in Antworten ein. So schützen Sie besonders sensible Klassen gezielt, auch wenn Berechtigungen noch nicht vollständig saniert sind.

WO IM ADMIN-PORTAL

Microsoft Purview Portal → **Data Loss Prevention** → **Richtlinien** → Speicherort **„Microsoft 365 Copilot“** → Bedingung auf Sensitivity Label.

> Kombination empfohlen: Auto-Labeling (K10) klassifiziert, die DLP-Richtlinie schließt die klassifizierten Inhalte aus Copilot aus.

12 Site-Lifecycle & Archivierung

Premium (SharePoint Advanced Management) | SharePoint Admin Center

WARUM WICHTIG (AUSWIRKUNG)

Verwaiste, inaktive Sites sind ein stiller Oversharing-Herd. Site-Lifecycle-Policies erkennen inaktive Sites und führen sie über eine Read-only-Phase in die Archivierung – **archivierte Inhalte fließen nicht in Copilot ein**.

WO IM ADMIN-PORTAL

SharePoint Admin Center → **Richtlinien** → **Websitelebenszyklusverwaltung** (inaktive Sites erkennen, Archivierung steuern).

EINSTELLUNGSOPTIONEN & WIRKUNG

Option	Wirkung
Inaktivitäts-Erkennung	Findet Sites ohne Nutzung – Kandidaten fürs Archiv.
Read-only- und Archiv-Phase	Reduziert Angriffsfläche; entfernt Inhalte aus dem Copilot-Grounding.

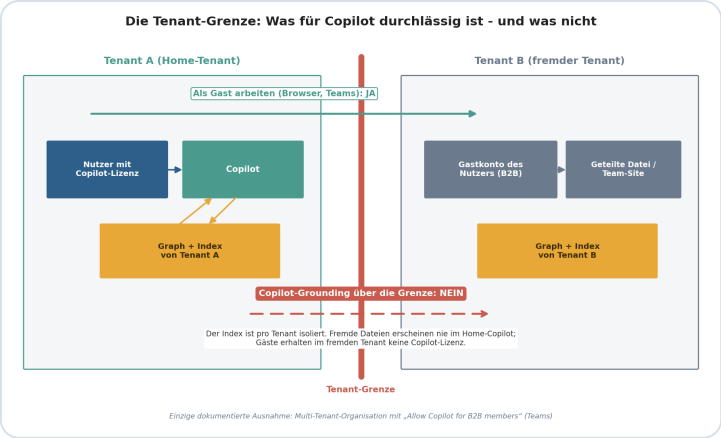
TEIL E · GRENZEN, BETRIEB & KONTROLLE

13 Tenant-Grenze, Gäste & externe Meetings

Bordmittel (Wissen & Entra/Teams-Einstellungen) | Entra · Teams Admin Center

WARUM WICHTIG (AUSWIRKUNG)

Grounding endet an der Tenant-Grenze: Der semantische Index ist pro Tenant isoliert, Copilot groundet über „Microsoft Graph in the user's tenant". Ein Gast kann in Ihrem Tenant keinen Copilot nutzen und Ihre Daten damit nicht per KI durchsuchen. Umgekehrt gilt die unbequeme Kehrseite: **Beiträge von Gästen und Gesprochenes externer Meeting-Teilnehmer werden zu Copilot-Material Ihrer internen Nutzer.**



Gastzugriff auf Dateien funktioniert über die Tenant-Grenze – Copilot-Grounding nicht. Der semantische Index bleibt pro Tenant isoliert.

WO IM ADMIN-PORTAL

Microsoft Entra Admin Center → Einstellungen für externe Zusammenarbeit / Cross-Tenant-Access. Teams Admin Center → Meeting- & Aufzeichnungs-/Transkriptionsrichtlinien; für Multi-Tenant-Organisationen die Einstellung **„Allow Copilot for B2B members"** (nur B2B-*Member*, nicht Gäste/föderierte Nutzer).

Transparenzpflicht: Wer als Externer in einem aufgezeichneten Meeting spricht, produziert durchsuchbares Grounding-Material für die Gastgeber-Seite. Informieren Sie externe Teilnehmer entsprechend und regeln Sie Transkription/Aufbewahrung.

14 Web-Grounding (Bing) & Copilot-Zugang steuern

Bordmittel | Microsoft 365 Admin Center · Cloud Policy

WARUM WICHTIG (AUSWIRKUNG)

Bei aktivem Web-Grounding kann Copilot Web-Anfragen an den Bing-Dienst senden; diese Anfragen können die EU-Datengrenze verlassen und unterliegen eigenen Datenverarbeitungsregeln (Microsoft als eigenständiger Verantwortlicher). Für rein interne Use-Cases ist Web-Grounding oft entbehrlich – eine bewusste Entscheidung gehört ins Konzept.

WO IM ADMIN-PORTAL

Steuerung über die Richtlinie **„Allow web search in Copilot“** – verfügbar im **Cloud Policy Service für Microsoft 365** sowie im Einstellungsbereich der **Copilot-Control-System-Seite im Microsoft 365 Admin Center**. Copilot-Zugang generell steuern: Microsoft 365 Admin Center → **Einstellungen** → **Integrierte Apps** → Copilot blockieren oder auf bestimmte Gruppen begrenzen.

EINSTELLUNGSOPTIONEN & WIRKUNG

Option der Richtlinie	Wirkung
Aktiviert (Copilot + Copilot Chat)	Web-Grounding verfügbar; Nutzer sehen zusätzlich den „Web content“-Schalter.
Deaktiviert (Copilot + Copilot Chat)	Keine Bing-Anfragen; Antworten nur aus Tenant-Daten und Modell.
Aus im Work-Modus / an im Web-Modus & Chat	Trennt interne Arbeit vom Web; beeinflusst auch Researcher/Analyst.

15 Audit & Kontrolle: CopilotInteraction / AccessedResources

Bordmittel (Basis-Audit) | Premium (erweiterte Aufbewahrung · eDiscovery) | Microsoft Purview Portal

WARUM WICHTIG (AUSWIRKUNG)

Jede Copilot-Interaktion erzeugt im Unified Audit Log einen Eintrag (Operation `CopilotInteraction`). Das Feld **„AccessedResources“** listet alle Dateien, Dokumente und E-Mails, die Copilot für die Antwort herangezogen hat – samt Dateiname, Site-URL und Sensitivity-Label-ID. Damit lässt sich konkret prüfen, ob eine als geschützt geglaubte Datei noch in Copilot-Antworten einfließt.

WO IM ADMIN-PORTAL

Microsoft Purview Portal → **Audit** (Suche nach `CopilotInteraction`). Wortlaut von Prompt und Antwort nicht im Audit-Log, sondern über **Content Search / eDiscovery** (Inhaltstyp „Copilot interactions“) bzw. den **Activity Explorer** in DSPM for AI.

ZUGANG & PILOTSTEUERUNG (FLANKIEREND)

Copilot-Lizenzen gezielt an eine Pilotgruppe zuweisen (Microsoft 365 Admin Center → Abrechnung/Benutzer). Über **Einstellungen** → **Integrierte Apps** lässt sich Copilot tenant-weit blockieren oder auf bestimmte Nutzer/Gruppen begrenzen – ideal für einen kontrollierten, schrittweisen Rollout.

Offene Frage laut Microsoft-Doku: Für native SharePoint-/OneDrive-Inhalte nennt Microsoft *keine* garantierte Latenz, wie schnell ein Berechtigungsentzug in Copilot wirkt. Konservative Praxis: sensible Vorfälle zusätzlich mit RCD (K7) oder RAC (K8) absichern, nicht nur einzelne Rechte entfernen.

Schulen Sie Ihr Team auf Grounding & Freigaberegeln

Die stärkste technische Absicherung nützt wenig, wenn im Arbeitsalltag täglich neue Altlasten entstehen – durch den falschen Freigabelink, die im Chat verschickte Datei, den unbedachten „Jeder“-Link. Genau hier setzen die Anwendertrainings der Copilotenschule an: Auf Wunsch schulen wir Ihre gesamte Belegschaft praxisnah auf **Grounding, Freigabemechanik und sichere Freigaberegeln** – abgestimmt auf Ihre reale Microsoft-365-Umgebung und Ihre Governance.

Vom Admin-Enablement über Compliance-Workshops für Datenschutz & Betriebsrat bis zur breitenwirksamen Anwenderschulung: Wir befähigen Wissensarbeiter, Teams und Organisationen, Copilot produktiv, sicher und wertschöpfend einzusetzen – ohne Bauchladen, mit Fokus auf das, was in Ihrem Umfeld compliant und wertschöpfend ist.

15-Minuten-Erstgespräch buchen
outlook.office.com · direkter Terminkalender

Kontaktformular: Team-Enablement anfragen
copilotenschule.de/#contact

Weitere Details: Grounding-Fachartikel lesen
copilotenschule.de/wissen/welche-daten-sieht-microsoft-365-copilot

E-MAIL
info@copilotenschule.de

TELEFON
+49 221 950 187 74

TEAMS-CHAT
Direkt im Teams-Chat schreiben

WEB
copilotenschule.de · Köln (DACH & Remote)

Herausgeber: copilotenschule.de – eine Marke der Yellow-Boat Consulting (gegründet 2011), Köln. Verantwortlich: Martin Lang. Kontakt: info@copilotenschule.de · +49 221 950 187 74. Vollständiges Impressum: copilotenschule.de/impressum · Datenschutz: copilotenschule.de/datenschutz.

BELEGE

Quellen (offizielle Microsoft-Dokumentation)

Grundlage dieses Leitfadens ist der Fachartikel „Welche Daten sieht Microsoft 365 Copilot? Grounding, Zugriffsberechtigungen und Freigabe-Altlasten“ (copilotenschule.de, Stand Juli 2026) sowie die folgenden offiziellen Microsoft-Dokumente (abgerufen im Juli 2026).

Grounding, Architektur, Datenschutz, Web-Suche

- Microsoft 365 Copilot architecture — learn.microsoft.com/…/microsoft-365-copilot-architecture
- Data, privacy, and security for Microsoft 365 Copilot — …/microsoft-365-copilot-privacy
- Semantic index for Copilot — …/microsoftsearch/semantic-index-for-copilot
- Manage public web access (Allow web search in Copilot) — …/copilot/manage-public-web-access
- Zero Trust for Microsoft 365 Copilot — …/zero-trust/copilots/zero-trust-microsoft-365-copilot
- Enterprise data protection — …/copilot/enterprise-data-protection

Sharing-Links, EEEU, Teams-Dateien

- Shareable links (Anyone/Specific people/Organization) — …/sharepoint/shareable-links-…
- Secure by default (Purview deployment) — …/purview/…/depmod-secure-by-default-step1
- PowerShell for Data Access Governance — …/sharepoint/powershell-for-data-access-governance
- Microsoft 365 Copilot setup — …/copilot/microsoft-365-copilot-setup
- File storage in Microsoft Teams — support.microsoft.com/…/file-storage-in-microsoft-teams
- Limit sharing in Microsoft 365 — …/solutions/microsoft-365-limit-sharing

Sanierung, Admin-Werkzeuge, Audit

- Secure and govern Microsoft 365 Copilot (Foundational deployment) — …/copilot/secure-govern-copilot-foundational-deployment-guidance
- SharePoint Advanced Management & Copilot license — …/sharepoint/sharepoint-advanced-management-features-copilot-license
- Data access governance reports — …/sharepoint/data-access-governance-reports
- Site access review — …/sharepoint/site-access-review
- Restricted Content Discovery — …/sharepoint/restricted-content-discovery
- Restricted SharePoint Search — …/sharepoint/restricted-sharepoint-search
- Restricted Access Control — …/sharepoint/restricted-access-control
- DSPM for AI / oversharing — …/purview/data-security-posture-management-oversharing
- DLP for Microsoft 365 Copilot — …/purview/dlp-microsoft365-copilot-location-learn-about
- Audit Copilot interactions — …/purview/audit-copilot
- Cross-tenant / requirements & guests — …/copilot/microsoft-365-copilot-requirements
- Entra external collaboration settings — …/entra/external-id/external-collaboration-settings-configure