



Stand: Juli 2026  
Version 1.0 · DE

LEITFADEN FÜR ENTSCHEIDER

# Microsoft 365 Copilot: Grounding verantworten

Was Geschäftsführung und Datenschutzbeauftragte über Datenzugriff, Oversharing und ihre Verantwortung wissen müssen – verständlich erklärt, ohne Technikjargon.

Zielgruppe: Geschäftsführung, Bereichs- und L&D-Leitung, Datenschutzbeauftragte und Compliance-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

|                                                                          |           |
|--------------------------------------------------------------------------|-----------|
| <b>Wichtiger Hinweis / Haftungsausschluss</b>                            | <b>3</b>  |
| <b>Entscheider-Checkliste: In Schritten zum sicheren Grounding</b>       | <b>4</b>  |
| <b>Grundlagen: Was „Grounding“ bedeutet – und warum es Chefsache ist</b> | <b>5</b>  |
| <b>So lesen Sie diesen Leitfaden</b>                                     | <b>6</b>  |
| <b>TEIL A · DIE RISIKEN VERSTEHEN</b>                                    |           |
| 1 · Copilot ist berechtigungstreu – und macht Altlasten sichtbar         | 7         |
| 2 · Freigabe-Altlasten: Gehalt, Finanzen, Verträge                       | 7         |
| 3 · Teams-Chats & Meeting-Transkripte als Dauer-Freigaben                | 8         |
| 4 · Gäste, Externe & die Tenant-Grenze                                   | 9         |
| 5 · Web-Grounding (Bing): Datenabfluss aus der EU                        | 10        |
| <b>TEIL B · DATENSCHUTZ &amp; MITBESTIMMUNG</b>                          |           |
| 6 · DSGVO-Pflichten rund um Copilot (Kompaktübersicht)                   | 11        |
| 7 · Mitbestimmung: Copilot & Betriebsrat (§ 87 BetrVG)                   | 12        |
| <b>TEIL C · VERANTWORTUNG &amp; STEUERUNG</b>                            |           |
| 8 · Wer ist verantwortlich? Rollen & Zuständigkeiten                     | 13        |
| 9 · Was Sie von der IT einfordern sollten                                | 14        |
| 10 · Copilot-Einführung als Governance-Projekt                           | 15        |
| <b>Schulung: Grounding &amp; Freigaberegeln für Ihr Team</b>             | <b>16</b> |
| <b>Quellen (offizielle Microsoft-Dokumentation)</b>                      | <b>17</b> |

## 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. Für Geschäftsführung und Datenschutz heißt das: Die Einführung ist weniger ein Technik- als ein Governance- und Compliance-Thema. Dieser Leitfaden erklärt die Risiken, Ihre Verantwortung und die richtigen Entscheidungen – die technische Umsetzung beschreibt der begleitende **Admin-Leitfaden**.

## ZUM ABHAKEN

## Entscheider-Checkliste

Die Kurzfassung dieses Leitfadens als Entscheidungs- und Governance-Liste. Die Verweise (K1–K10) führen zum jeweiligen Kapitel.

### PHASE 1 · VOR DER ENTSCHEIDUNG / VOR DEM ROLLOUT

- ☐ Verantwortlichkeiten schriftlich klären: Wer entscheidet, wer setzt um, wer prüft? (GF, IT, DSB, Betriebsrat, Fachbereiche). → K8
- ☐ Von der IT eine Bestandsaufnahme zum Oversharing einfordern, **bevor** Copilot-Lizenzen zugewiesen werden. → K9
- ☐ Sanierung der Freigabe-Altlasten als eigenes, budgetiertes Arbeitspaket einplanen. → K10
- ☐ Datenklassifizierung (Sensitivity Labels) als verbindliche Vorgabe beschließen. → K2 · K9

### PHASE 2 · DATENSCHUTZ & MITBESTIMMUNG

- ☐ Copilot-Einsatz ins Verzeichnis von Verarbeitungstätigkeiten aufnehmen; DSFA prüfen/erstellen. → K6
- ☐ Transparenz gegenüber Beschäftigten sicherstellen (Meeting-Transkription, Protokollierung im Audit-Log). → K6
- ☐ Betriebsrat frühzeitig einbinden; Betriebsvereinbarung zur Copilot-Nutzung anstreben. → K7
- ☐ Web-Grounding (Bing) bewusst freigeben oder deaktivieren lassen. → K5

### PHASE 3 · ROLLOUT & BETRIEB

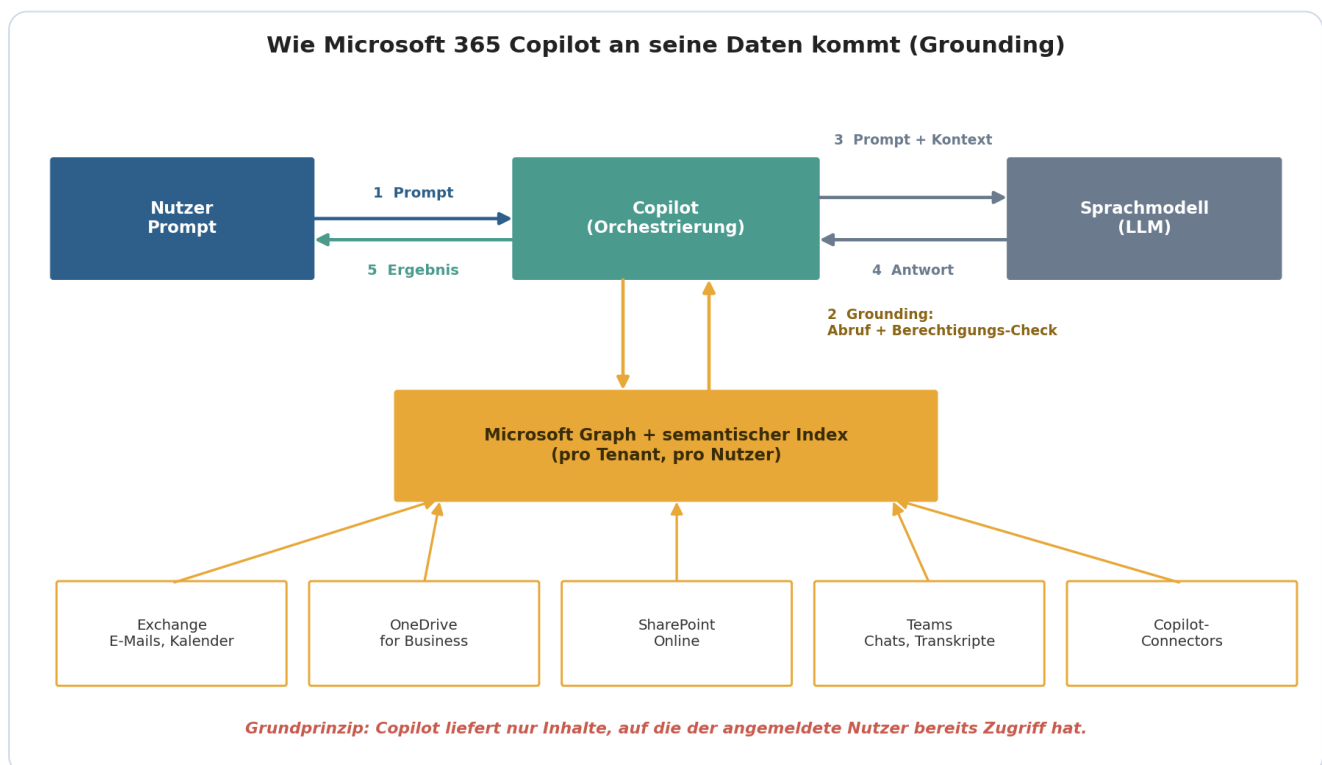
- ☐ Mit einer Pilotgruppe starten, nicht sofort für alle. → K10
- ☐ Regelmäßige Nachweise einfordern: Oversharing-Status und Audit-Routine. → K9
- ☐ Nutzungsrichtlinien kommunizieren und die Belegschaft vor dem Rollout schulen. → Schulung

## GRUNDLAGEN

## Was „Grounding“ bedeutet – und warum es Chefsache ist

In zwei Minuten verständlich: Wie Copilot an Daten kommt und warum die Verantwortung nicht allein bei der IT liegt.

Wenn ein Mitarbeiter Copilot etwas fragt, sucht die KI zunächst passende Informationen im Datenbestand des Unternehmens zusammen – E-Mails, Chats, Dateien, Termine, Meetings. Diesen Schritt nennt Microsoft **Grounding**. Erst mit diesem Kontext formuliert Copilot seine Antwort. Entscheidend ist die eiserne Regel dahinter: Copilot zeigt jedem Nutzer **ausschließlich Inhalte, auf die er ohnehin schon Zugriff hat** – nicht mehr, aber eben auch alles davon, und das zuverlässiger als jede Suche zuvor.



So kommt Microsoft 365 Copilot an seine Daten: Anfrage → Grounding im Unternehmens-Datenbestand → KI-Modell → Antwort. Copilot bleibt dabei streng an die bestehenden Zugriffsrechte gebunden.

Genau deshalb ist das Thema Chefsache: Nicht die KI ist das Risiko, sondern die über Jahre gewachsenen Berechtigungen. Was einmal zu großzügig freigegeben wurde – die Gehaltsliste, der Vertragsentwurf, das interne Protokoll –, war schon immer auffindbar. Nur hat vorher niemand gezielt gesucht. Copilot senkt die Hürde drastisch: Eine Frage in normaler Sprache genügt. Die Einführung von Copilot wirkt damit wie ein **überfälliges Berechtigungs-Audit** – mit einem Produktivitätswerkzeug als Anlass.

**Was gut gelöst ist – und was Ihre Aufgabe bleibt**

Microsoft sichert vieles technisch ab: Verarbeitung in der EU (EU Data Boundary), keine Nutzung Ihrer Daten zum KI-Training, Verschlüsselung und strikte Mandanten-Trennung. Diese Zusagen sind wichtig – sie beantworten aber nicht alle Fragen. **Berechtigungen aufräumen, Daten klassifizieren, Datenschutz- und Mitbestimmungspflichten erfüllen und die Belegschaft befähigen** bleibt Aufgabe Ihrer Organisation.

**LESEHILFE**

## So lesen Sie diesen Leitfaden

Jedes Kapitel ist bewusst kompakt gehalten: **Das Risiko** (verständlich erklärt) und **Unsere Empfehlung** (was zu tun bzw. zu entscheiden ist). Eine Kennzeichnung zeigt, für wen der Punkt primär relevant ist.

| Kennzeichnung             | Bedeutung                                                                      |
|---------------------------|--------------------------------------------------------------------------------|
| Management                | Primär entscheidungs- und steuerungsrelevant für Geschäftsführung und Leitung. |
| Datenschutz               | Primär relevant für Datenschutzbeauftragte und Compliance.                     |
| Management<br>Datenschutz | Für beide Rollen gleichermaßen wichtig – hier lohnt die Abstimmung.            |

Dieser Leitfaden verzichtet bewusst auf technische Pfade und Einstellungen. Die konkrete Umsetzung im Admin-Portal (SharePoint, Purview, Entra) beschreibt der begleitende **Admin-Leitfaden „Grounding sicher gestalten“**. Einen eigenen, ausführlichen Leitfaden für **Betriebsräte** stellen wir separat bereit.

## TEIL A · DIE RISIKEN VERSTEHEN

## 1 Copilot ist berechtigungstreu – und macht Altlasten sichtbar

Management

Datenschutz

### DAS RISIKO

Copilot öffnet keine Türen, die vorher verschlossen waren – aber es findet zuverlässig, was schon immer offen stand. Vor Copilot brauchte man für heikle Funde Glück, böse Absicht und gute Suchkenntnisse. Jetzt genügt eine Frage in natürlicher Sprache. Bestehende Berechtigungsfehler werden damit auf einen Schlag für die gesamte Belegschaft praktisch nutzbar – ohne dass sich an den Zugriffsrechten selbst irgendetwas geändert hätte.

### UNSERE EMPFEHLUNG

Behandeln Sie die Copilot-Einführung als das, was sie faktisch ist: ein überfälliges Berechtigungs-Audit. Machen Sie die Hausaufgaben (Bestandsaufnahme und Bereinigung) **vor** dem Rollout, nicht danach – und planen Sie dafür Zeit und Budget ein.

## 2 Freigabe-Altlasten: Gehalt, Finanzen, Verträge

Management

Datenschutz

### DAS RISIKO

Die typischen Funde in gewachsenen Umgebungen: die HR-Tabelle mit Gehaltsdaten, die 2019 „kurz mit der Buchhaltung“ organisationsweit geteilt wurde; das Due-Diligence-Verzeichnis mit der Berechtigung „Jeder außer externen Benutzern“; Kündigungsentwürfe, die per Chat verschickt wurden. Besonders brisant: Es handelt sich oft um **besondere Kategorien personenbezogener Daten** (Art. 9 DSGVO) oder um Geschäftsgeheimnisse – ein Fund kann direkt einen meldepflichtigen Datenschutzvorfall bedeuten.

### UNSERE EMPFEHLUNG

Lassen Sie von der IT einen Oversharing-Bericht über die meistgenutzten Bereiche erstellen und priorisieren Sie die Hochrisiko-Bereiche (HR, Finanzen, Recht, Geschäftsführung) für die Bereinigung. Beschließen Sie Datenklassifizierung als verbindliche Vorgabe – klassifizierte, verschlüsselte Inhalte bleiben auch dann geschützt, wenn Berechtigungen einmal falsch stehen.

### 3 Teams-Chats & Meeting-Transkripte als Dauer-Freigaben

Management

Datenschutz

#### ■ DAS RISIKO

Eine im Teams-Chat verschickte Datei ist keine flüchtige Nachricht, sondern eine **dauerhafte Freigabe** aus dem Speicher des Absenders – sie bleibt bestehen, bis jemand sie aktiv entzieht, auch wenn der Empfänger längst die Abteilung gewechselt hat. Noch heikler sind Meeting-Aufzeichnungen: Das Transkript liegt beim Organisator, ist an alle internen Eingeladenen freigegeben und macht offen Gesprochenes durchsuchbar. Bei öffentlichen Teams kann zudem jede Person im Unternehmen jederzeit beitreten.

#### ■ UNSERE EMPFEHLUNG

Schaffen Sie Bewusstsein in der Belegschaft (Anwenderschulung) und legen Sie klare Regeln fest: Was wird aufgezeichnet und transkribiert, wie lange wird es aufbewahrt, wer hat Zugriff? Das gehört in Nutzungsrichtlinie und – wo Beschäftigte betroffen sind – in die Abstimmung mit Datenschutz und Betriebsrat.



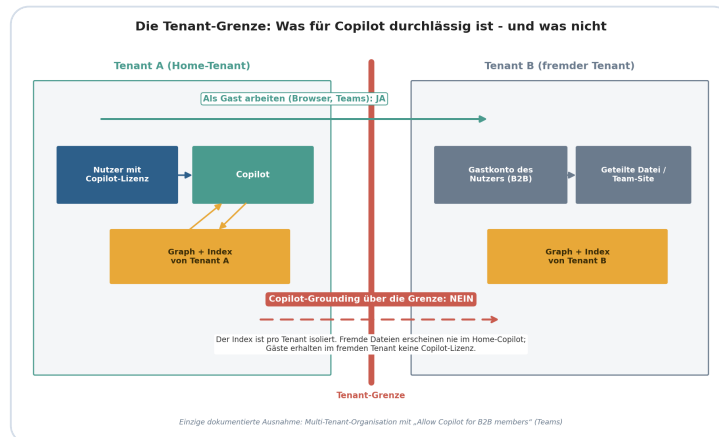
## 4 Gäste, Externe & die Tenant-Grenze

Management

Datenschutz

### ■ DAS RISIKO

Die gute Nachricht zuerst: Der Datenbestand von Copilot endet an der Grenze Ihres Mandanten (Tenant). Ein Gast kann in Ihrem Tenant keinen Copilot nutzen und Ihre Daten nicht per KI durchsuchen. Die unbequeme Kehrseite: **Alles, was ein Gast in Ihren Teams einstellt, und alles, was ein externer Teilnehmer in einem aufgezeichneten Meeting sagt, wird zu Copilot-Material Ihrer eigenen, lizenzierten Mitarbeitenden** – der Externe „füttert“ Ihr Grounding, ohne selbst eine KI-Sicht darauf zu bekommen.



*Gastzugriff auf einzelne Dateien funktioniert über die Tenant-Grenze – der KI-Datenbestand von Copilot bleibt pro Unternehmen strikt getrennt.*

### ■ UNSERE EMPFEHLUNG

Informieren Sie externe Teilnehmer transparent, wenn Meetings transkribiert werden. Befristen Sie Gastzugriffe automatisch und regeln Sie, wer überhaupt Externe oder Gäste einladen darf. Das ist zugleich eine Datenschutz- und eine Vertraulichkeitsfrage.

## 5 Web-Grounding (Bing): Datenabfluss aus der EU

[Datenschutz](#)[Management](#)

### ■ DAS RISIKO

Copilot kann Antworten optional mit aktuellen Web-Inhalten anreichern. Dazu sendet er kurze Suchanfragen an den Bing-Dienst. Diese Anfragen **können die EU-Datengrenze verlassen** und unterliegen eigenen Datenschutzregeln: Microsoft agiert hier als eigenständig Verantwortlicher, nicht als Auftragsverarbeiter. Für viele interne Anwendungsfälle wird die Web-Suche gar nicht benötigt.

### ■ UNSERE EMPFEHLUNG

Entscheiden Sie bewusst, ob Web-Grounding in Ihrem Umfeld gebraucht wird. Im Zweifel lassen Sie es deaktivieren oder auf einen getrennten „Web-Modus“ begrenzen. Nehmen Sie die Entscheidung in Ihre Datenschutz-Folgenabschätzung auf.

## TEIL B · DATENSCHUTZ &amp; MITBESTIMMUNG

## 6 DSGVO-Pflichten rund um Copilot (Kompaktübersicht)

### Datenschutz

#### ■ WORUM ES GEHT

Microsofts technische Zusagen (EU Data Boundary, kein Training mit Kundendaten, Verschlüsselung, Mandanten-Isolation) sind eine gute Grundlage – ersetzen aber nicht die organisatorischen Pflichten, die bei Ihnen als Verantwortlichem bleiben. Die wichtigsten im Überblick:

| DSGVO-Baustein                                 | Was zu tun ist                                                                                                                               |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Verzeichnis von Verarbeitungstätigkeiten (VVT) | Copilot-Einsatz als Verarbeitung aufnehmen: Zwecke, Datenkategorien, Empfänger, Löschfristen.                                                |
| Datenschutz-Folgenabschätzung (DSFA)           | Prüfen bzw. erstellen. Microsoft bietet seit Nov. 2025 ein M365-Kit mit DSFA-Vorlagen, das mit deutschen Aufsichtsbehörden abgestimmt wurde. |
| Rechtsgrundlage                                | Art. 6 DSGVO (i. d. R. berechtigtes Interesse/Vertragserfüllung); bei Beschäftigtendaten § 26 BDSG bzw. Betriebsvereinbarung beachten.       |
| Transparenz & Information                      | Beschäftigte über Copilot, Meeting-Transkription und die Protokollierung von Interaktionen informieren.                                      |
| Aufbewahrung & Löschung                        | Konzepte für Transkripte, Aufzeichnungen und Audit-Daten festlegen.                                                                          |
| Betroffenenrechte                              | Auskunft und Löschung auch für Copilot-Interaktionen berücksichtigen.                                                                        |

#### ■ UNSERE EMPFEHLUNG

Binden Sie die/den Datenschutzbeauftragte:n früh ein. Dokumentieren Sie die technischen Zusagen von Microsoft und arbeiten Sie die eigenen Pflichten strukturiert ab. In unseren Compliance-Workshops bereiten wir genau diese Punkte auf – auch zur Kommunikation gegenüber einer skeptischen DSB.

## 7 Mitbestimmung: Copilot & Betriebsrat (§ 87 BetrVG)

Management

Datenschutz

### ■ DAS RISIKO

Copilot protokolliert Nutzungs- und Interaktionsdaten und kann damit als technische Einrichtung gelten, die geeignet ist, Verhalten oder Leistung von Beschäftigten zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG). Die Einführung ist deshalb in vielen Unternehmen **mitbestimmungspflichtig**. Wird der Betriebsrat spät oder schlecht informiert, drohen Verzögerungen und Blockaden – häufig nicht aus Unwillen, sondern aus fehlender Information.

### ■ UNSERE EMPFEHLUNG

Binden Sie den Betriebsrat früh als Partner ein und legen Sie in einer Betriebsvereinbarung fest, welche Nutzungs- und Audit-Daten erhoben werden, wer sie auswerten darf und welche Auswertungsgrenzen gelten. **Hinweis:** Einen ausführlichen, eigenen Leitfaden speziell für Betriebsräte stellen wir separat bereit.

## TEIL C · VERANTWORTUNG &amp; STEUERUNG

## 8 Wer ist verantwortlich? Rollen & Zuständigkeiten

**Management**

### DAS RISIKO

Grounding-Sicherheit fällt zwischen die Stühle, wenn Verantwortung unklar ist: Die IT kann Dateiinhalte oft gar nicht bewerten (und darf sie teils nicht einmal sehen), die Fachbereiche kennen die Technik nicht, und der Datenschutz erfährt zu spät davon. Ohne klare Rollen bleibt die Bereinigung liegen.

| Rolle                         | Verantwortung                                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Geschäftsführung / Leitung    | Entscheidet über Rollout und Budget, benennt Verantwortliche und verankert Datenklassifizierung als Pflicht.                |
| IT / M365-Administration      | Setzt die technischen Leitplanken, liefert Oversharing-Berichte und betreibt die Audit-Routine (Details → Admin-Leitfaden). |
| Datenschutzbeauftragte:r      | Verantwortet VVT, DSFA, Transparenz und Aufbewahrung; berät zu Rechtsgrundlagen.                                            |
| Betriebsrat                   | Mitbestimmung; Aushandlung der Betriebsvereinbarung.                                                                        |
| Fachbereiche / Bereichs-Owner | Entscheiden, wer auf ihre Inhalte zugreifen darf, und bereinigen Freigaben – sie kennen die Inhalte am besten.              |

### UNSERE EMPFEHLUNG

Legen Sie diese Verantwortlichkeiten **vor** dem Rollout schriftlich fest. Delegieren Sie die inhaltliche Bereinigung an die Fachbereiche – die IT kann und darf diese Entscheidungen nicht allein treffen.

## 9 Was Sie von der IT einfordern sollten

### Management

#### ■ WURUM ES GEHT

„Ist alles sicher“ bleibt eine Behauptung, solange keine Nachweise vorliegen. Mit diesen sechs Fragen behalten Sie als Entscheider die Kontrolle – ohne selbst tief in die Technik einsteigen zu müssen.

| Frage an die IT                                       | Nachzuweisen durch                                                                           |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Wie stark ist unser Umfeld von Oversharing betroffen? | Oversharing-Bericht (DSPM for AI / Data-Access-Governance) über die meistgenutzten Bereiche. |
| Sind Hochrisiko-Bereiche vor dem Rollout geschützt?   | Nachweis eines Interimsschutzes für HR, Finanzen, Recht, Geschäftsführung.                   |
| Sind vertrauliche Inhalte klassifiziert?              | Konzept für Sensitivity Labels / Auto-Labeling und Ausschluss sensibler Inhalte aus Copilot. |
| Wer kann eigentlich auf was zugreifen?                | Bericht über weitreichende Berechtigungen und „Jeder/Everyone“-Freigaben.                    |
| Was fasst Copilot tatsächlich an?                     | Regelmäßige Audit-Auswertung der von Copilot genutzten Inhalte.                              |
| Ist die Web-Suche (Bing) geregelt?                    | Nachweis der bewussten Richtlinien-Entscheidung zum Web-Grounding.                           |

#### ■ UNSERE EMPFEHLUNG

Fordern Sie diese Nachweise vor der ersten Lizenzzuweisung – und danach in festen Zyklen – ein. Die technischen Details dazu liefert der begleitende Admin-Leitfaden.

## 10 Copilot-Einführung als Governance-Projekt

### Management

#### ■ DAS RISIKO

Wer Copilot einfach „anschaltet“, macht bestehende Berechtigungsfehler produktiv nutzbar. Die Sanierung der Altlasten ist ein eigenes Arbeitspaket mit Beteiligung der Fachbereiche – kein Nebenprodukt der IT und nicht an einem Nachmittag erledigt.

#### ■ UNSERE EMPFEHLUNG – DIE REIHENFOLGE

**1.** Bestandsaufnahme (Oversharing-Bericht). **2.** Hochrisiko-Bereiche interimweise schützen. **3.** Fachbereiche die Freigaben bereinigen lassen. **4.** Datenklassifizierung und Leitplanken verankern. **5.** Mit einer Pilotgruppe starten und schrittweise ausrollen. **6.** Anwenderschulung und Audit-Routine etablieren. Budgetieren Sie Sanierung und Schulung von Anfang an mit ein.

## Schulen Sie Ihr Team auf Grounding & Freigaberegeln

Die beste Governance 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 Trainings 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 Governance.

Für Entscheider und Datenschutz bieten wir zusätzlich **Compliance-Workshops** (Datenschutz, Betriebsrat, Verantwortlichkeiten) sowie die Begleitung des gesamten Rollouts – ohne Bauchladen, mit Fokus auf das, was in Ihrem Umfeld compliant und wertschöpfend ist.

### 15-Minuten-Erstgespräch buchen

[outlook.office.com](mailto:outlook.office.com) · direkter Terminkalender

### Kontaktformular: Team-Enablement anfragen

[copilotenschule.de/#contact](https://copilotenschule.de/#contact)

### Weitere Details: Grounding-Fachartikel lesen

[copilotenschule.de/wissen/welche-daten-sieht-microsoft-365-copilot](https://copilotenschule.de/wissen/welche-daten-sieht-microsoft-365-copilot)

### E-MAIL

[info@copilotenschule.de](mailto:info@copilotenschule.de)

### TELEFON

+49 221 950 187 74

### TEAMS-CHAT

Direkt im Teams-Chat schreiben

### WEB

[copilotenschule.de](https://copilotenschule.de) · Köln (DACH & Remote)

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

- Data, privacy, and security for Microsoft 365 Copilot — [learn.microsoft.com/.../microsoft-365-copilot-privacy](https://learn.microsoft.com/.../microsoft-365-copilot-privacy)
- Enterprise data protection (EU Data Boundary, Web-Queries) — [.../copilot/enterprise-data-protection](https://.../copilot/enterprise-data-protection)
- Manage public web access (Allow web search in Copilot) — [.../copilot/manage-public-web-access](https://.../copilot/manage-public-web-access)
- Microsoft 365 Copilot architecture — [.../copilot/microsoft-365-copilot-architecture](https://.../copilot/microsoft-365-copilot-architecture)

### Oversharing, Governance & Audit

- Secure and govern Microsoft 365 Copilot (Foundational deployment) — [.../copilot/secure-govern-copilot-foundational-deployment-guidance](https://.../copilot/secure-govern-copilot-foundational-deployment-guidance)
- DSPM for AI / oversharing (Microsoft Purview) — [.../purview/data-security-posture-management-oversharing](https://.../purview/data-security-posture-management-oversharing)
- Data access governance reports — [.../sharepoint/data-access-governance-reports](https://.../sharepoint/data-access-governance-reports)
- Audit Copilot interactions — [.../purview/audit-copilot](https://.../purview/audit-copilot)
- Considerations for Microsoft 365 Copilot (Purview) — [.../purview/ai-m365-copilot-considerations](https://.../purview/ai-m365-copilot-considerations)

### Sharing, Teams-Dateien & Tenant-Grenze

- How shareable links work in OneDrive and SharePoint — [.../sharepoint/shareable-links-...](https://.../sharepoint/shareable-links-...)
- File storage in Microsoft Teams — [support.microsoft.com/.../file-storage-in-microsoft-teams](https://support.microsoft.com/.../file-storage-in-microsoft-teams)
- Microsoft 365 Copilot requirements (Gäste/Cross-Tenant) — [.../copilot/microsoft-365-copilot-requirements](https://.../copilot/microsoft-365-copilot-requirements)