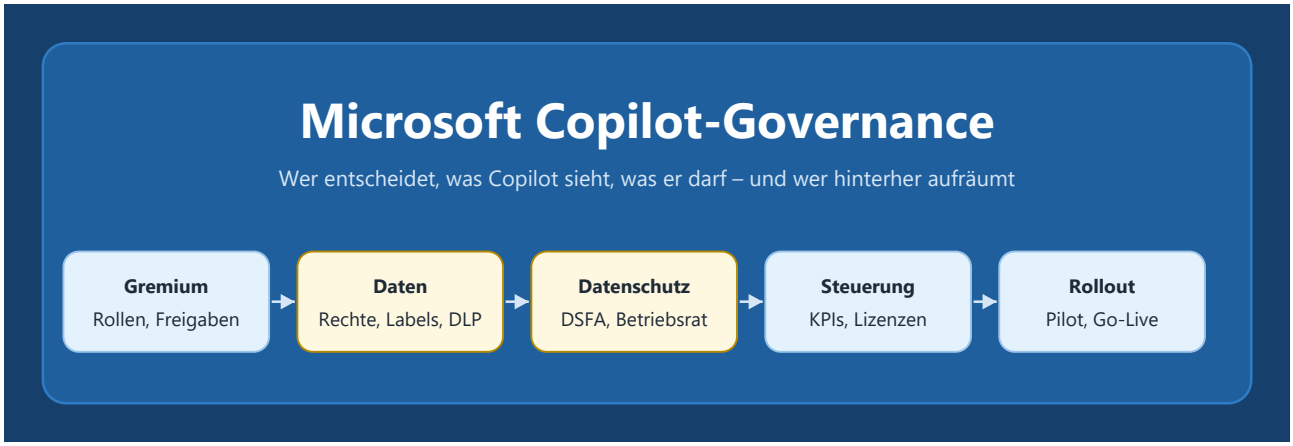
Microsoft Copilot-Governance – Grundlagen, Umsetzung, Praxis



Wissen	Beratung	Schulung
Was sich bei Copilot gerade bewegt und welche Regeln du deshalb nachschärfen musst: › Erwartete Neuerungen in Microsoft Copilot in 2026	Rechte bereinigen, Gremium aufsetzen, Pilot mit Leitplanken fahren – so sieht ein begleitetes Einführungsprojekt aus: › Copilot-Einführung bei der Harry Hase AG	Prompting, Fehlererkennung und KI-Kompetenz nach AI Act für Anwender, Admins und Führungskräfte: › KI im Unternehmen erfolgreich einführen – Praxisleitfaden

Dienstagmorgen, Pilotgruppe in einem Maschinenbau-Unternehmen, Tag zwei mit Microsoft 365 Copilot. Eine Sachbearbeiterin aus dem Einkauf will wissen, wie die Weihnachtsfeier organisiert wird, und fragt Copilot nach „allem zur Feier im Dezember“. Copilot liefert brav: Location, Budget, Shuttle-Plan – und eine Zusammenfassung der Tischordnung, in der praktischerweise auch steht, welche zwei Abteilungsleiter „wegen der laufenden Trennungsgespräche“ nicht nebeneinander sitzen sollen. Die Datei lag in einer Team-Site, die vor vier Jahren für ein Sommerfest angelegt und für die ganze Firma geöffnet worden war. Niemand hatte sie je wiedergefunden. Copilot schon, am zweiten Tag.

Genau darum geht es bei **Microsoft Copilot-Governance**: um den Ordnungsrahmen, der festlegt, wer über den Einsatz von Microsoft 365 Copilot entscheidet, auf welche Daten der Assistent zugreifen kann, wie Ergebnisse geprüft werden, was protokolliert wird, wie der Betriebsrat eingebunden ist und woran du merkst, ob sich das Ganze lohnt. Copilot ist kein Sicherheitsrisiko, das aus dem Nichts kommt. Er ist ein extrem fleißiger Suchhund, der jede Berechtigung nutzt, die in deinem Tenant existiert – auch die, die du längst vergessen hast.

Dieser Beitrag richtet sich an Verantwortliche aus IT, Security, Datenschutz und Fachbereichen. Du erfährst, wie du ein Gremium mit klaren Zuständigkeiten aufsetzt, warum Berechtigungsbereinigung vor dem Rollout kommt, was Sensitivitätslabels und DLP realistisch leisten, wie du Datenschutz und Mitbestimmung sauber löst, was Purview Audit wirklich aufzeichnet, welche Kennzahlen taugen und wie ein stufenweiser Rollout mit harten Go-Live-Kriterien aussieht. Den Gesamtüberblick über Funktionen, Varianten und Einsatzgebiete findest du auf der Seite Microsoft Copilot.

Fakten: Copilot-Governance in einem Satz

Copilot-Governance ist das Zusammenspiel aus **Zuständigkeiten** (wer entscheidet), **technischen Leitplanken** (was Copilot sehen und tun darf), **Regeln für Menschen** (was Nutzer eingeben und ungeprüft weitergeben dürfen) und **Messung** (ob Nutzen und Risiko im Rahmen bleiben).

Sie ersetzt weder IT-Governance noch Datenschutzmanagement, sondern konkretisiert beide für einen Assistenten, der auf nahezu alle Inhalte zugreifen kann, auf die seine Nutzer zugreifen können.

Grundlagen: Was Copilot-Governance regelt und wer entscheidet

Wer Copilot einführt, ohne vorher zu klären, wer was entscheidet, erlebt ein bekanntes Muster: Die IT schaltet frei, weil der Vorstand es will. Der Datenschutzbeauftragte erfährt es aus dem Intranet. Der Betriebsrat erfährt es aus der Kantine und schickt eine Unterlassungsaufforderung. Drei Wochen später sitzen alle in einem Meeting, das „Copilot-Taskforce“ heißt und eigentlich eine Schadensbegrenzung ist. Das lässt sich vermeiden, und zwar billiger, als man denkt.

Abgrenzung zu IT-Governance, Data Governance, Security und Compliance

Copilot-Governance ist eine Querschnittsdisziplin. Sie erfindet keine neuen Prinzipien, sondern übersetzt bestehende Regeln in die Welt eines KI-Assistenten. Die Tabelle zeigt, wo die Grenzen verlaufen und was Copilot jeweils konkret hinzufügt.

Disziplin	Regelt allgemein	Was Copilot-Governance ergänzt
IT-Governance	Strategie, Investitionen, Rollen, Change-Management	Wer Copilot bekommt, wer Funktionen freischaltet, wie neue Copilot-Features bewertet werden
Data Governance	Klassifizierung, Datenqualität, Lebenszyklus, Eigentümer	Welche Inhalte Copilot finden darf, Bereinigung veralteter Daten, Label-Pflicht für sensible Bereiche
Informationssicherheit	Vertraulichkeit, Integrität, Verfügbarkeit, ISMS	Berechtigungsbereinigung, DLP für Prompts und Antworten, Agent- und Plugin-Freigabe, Vorfallprozess
Datenschutz	DSGVO, Verzeichnis, DSFA, Betroffenenrechte	DSFA für Copilot, Löschkonzept für Verläufe, Websuche, Protokolldaten von Beschäftigten
Compliance und Recht	Gesetze, Aufbewahrung, Haftung, interne Kontrollen	Prüfpflichten für KI-Ausgaben, Aufbewahrung von Copilot-Interaktionen, KI-Kompetenz nach AI Act

Daraus folgt eine einfache Regel: Copilot-Governance gehört als Anhang oder Kapitel in dein bestehendes Regelwerk, nicht als frei schwebendes Dokument daneben. Bei Widersprüchen gilt die strengere Vorgabe. Und kläre früh den Geltungsbereich: Meinst du nur Microsoft 365 Copilot, oder auch Copilot Chat ohne Lizenz, Agents aus Copilot Studio und Copilot-Funktionen in der Power Platform? Meine Empfehlung: alles, was im Tenant generative KI anbietet, unter ein Dach. Sonst führst du in einem Jahr die gleiche Diskussion für jedes neue Produkt neu.

Das Gremium: Rollen und Zuständigkeiten

Copilot-Entscheidungen berühren zu viele Interessen, um sie einer Person zu überlassen. Bewährt hat sich ein kleiner Lenkungskreis, der monatlich tagt und in der Einführungsphase alle zwei Wochen. Größer als sieben Personen sollte er nicht werden, sonst wird aus dem Gremium ein Publikum.

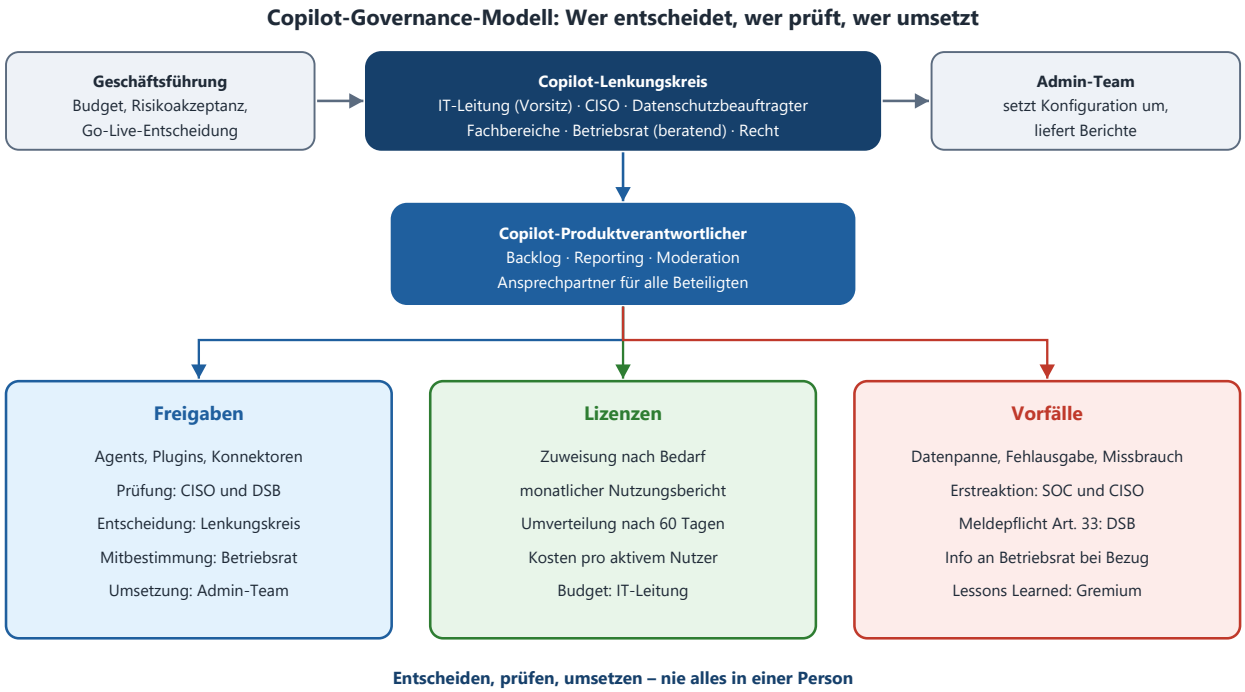


Abbildung 1: Ein schlankes Governance-Modell trennt Entscheidung, Prüfung und Umsetzung und ordnet Freigaben, Lizenzen und Vorfälle klaren Wegen zu.

Rolle	Entscheidet	Prüft und berät	Typische Aufgaben
Geschäftsführung	Budget, Go-Live, Risikoakzeptanz	–	Sponsor, löst Zielkonflikte, unterschreibt Betriebsvereinbarung
IT-Leitung	Vorsitz Lenkungskreis, Lizenzbudget, Prioritäten	Machbarkeit	Ressourcen, Abstimmung mit Betrieb und Fachbereichen
CISO	Sicherheitsvorgaben, Notabschaltung bei Vorfall	Agents, Plugins, Konnektoren	Berechtigungsbereinigung, DLP, Monitoring, Incident Response
Datenschutzbeauftragter	– (berät, kontrolliert)	DSFA, Löschkonzept, Websuche, Protokolle	Beratung nach Art. 39 DSGVO, Prüfung von Datenflüssen, Meldewege
Fachbereiche	Einsatzfälle und Prüfpflichten im eigenen Bereich	Nutzen, Praxistauglichkeit	Use Cases, Champions, fachliche Qualitätssicherung
Betriebsrat	Mitbestimmung nach § 87 BetrVG	Nutzungsregeln, Auswertungen	Betriebsvereinbarung, Vertretung der Belegschaft
Copilot-Produktverantwortlicher	operative Freigaben im Rahmen der Policies	alles, koordiniert	Backlog, Reporting, Schulungskonzept, Ansprechpartner
Admin-Team	Sofortmaßnahmen im Notfall	technische Umsetzbarkeit	Konfiguration, Lizenzzuweisung, Berichte,

Rolle	Entscheidet	Prüft und berät	Typische Aufgaben
			Support

Zwei Punkte werden in der Praxis gern übersehen. Erstens: Der Datenschutzbeauftragte entscheidet nicht, er berät und kontrolliert. Wer ihn zum Freigabeorgan macht, schiebt ihm eine Verantwortung zu, die rechtlich beim Unternehmen liegt – und wundert sich dann, warum alles so lange dauert. Zweitens: Der Betriebsrat ist kein Gast, der informiert wird, sondern hat bei Copilot ein echtes Mitbestimmungsrecht. Dazu mehr in Kapitel 3.

Warum ein Produktverantwortlicher für Copilot den Unterschied macht

In fast jedem Projekt, das ich ins Stocken geraten sehe, fehlt eine Person, die Copilot als Produkt verantwortet. Ohne sie gehört Copilot allen und damit niemandem: Die Lizenzen verwaltet der Einkauf, die Konfiguration ein Admin, der nebenbei noch Exchange betreut, die Schulung das HR-Team, das von Labels noch nie gehört hat. Neue Funktionen landen per Release-Welle im Tenant, und keiner prüft, ob sie zur Policy passen.

Der Produktverantwortliche hält diese Fäden zusammen. Er pflegt den Backlog mit Anfragen der Fachbereiche, bereitet die Entscheidungen des Lenkungskreises vor, liest die Microsoft-Ankündigungen mit Blick auf Governance-Folgen, verantwortet Reporting und Schulungskonzept und ist erste Anlaufstelle, wenn etwas schiefgeht. In Organisationen mit mehr als einigen Hundert Lizenzen ist das eine halbe bis ganze Stelle. Klingt teuer? Rechne gegen, was zehn Prozent ungenutzte Lizenzen pro Jahr kosten – dann ist die Stelle meist schon bezahlt.

> **Tipp: Freigabewege schriftlich festlegen**
>
> Halte in einer Seite fest, wer was freigibt: neue Agents, Plugins und Konnektoren, neue Copilot-Funktionen, Lizenzzuweisungen, Policy-Änderungen, Ausnahmen. Ein einfaches Raster mit „entscheidet / prüft / wird informiert“ spart dir mehr Meetings als jedes Tool.

Reifegrade: Wo du stehst und wohin du willst

Governance entsteht nicht auf einen Schlag. Ein Reifegradmodell hilft, ehrlich einzuordnen, wo du stehst, und dem Management zu zeigen, was der nächste Schritt kostet.

Stufe	Merkmal	Typisches Symptom	Nächster Schritt
1 – Ad hoc	Copilot läuft ohne Regeln	„Wir testen erst mal mit ein paar Interessierten“	Gremium und Basis-Policy, Websuche und Dritt-Agents aus
2 – Reaktiv	Einzelmaßnahmen nach Vorfällen	DLP-Regel nach dem ersten Leak	Risikoanalyse, Berechtigungsbereinigung, DSFA
3 – Definiert	Policies, Rollen, Schulung vorhanden	Regeln existieren, Messung fehlt	KPIs und KRIs mit Schwellwerten, Freigabeprozess
4 – Gesteuert	Kennzahlen, Gremium, Rezertifizierung	Entscheidungen auf Datenbasis	Automatisierte Alarme, Agent-Lebenszyklus
5 – Optimiert	Governance ermöglicht schnelle Einführung neuer KI-Funktionen	neue Features in Wochen statt Monaten	Benchmarks, Red-Teaming, Ausbau auf Agenten

Realistisches Ziel für den breiten Rollout ist Stufe 3, für das Ende des ersten Betriebsjahres Stufe 4. Stufe 5 ist kein Selbstzweck, wird aber relevant, sobald autonome Agenten ins Spiel kommen – dann wird die Governance-Frage nicht kleiner, sondern größer. Wie das im Agenten-Kontext aussieht, beschreibe ich in Copilot-Agenten in der Praxis und in Agent 365 – KI-Agenten als Steuerzentrale für Microsoft 365, Sicherheit und Automatisierung.

Daten und Berechtigungen: Grounding, Oversharing, Labels und Erweiterungen

Wenn du aus diesem Beitrag nur ein Kapitel mitnimmst, dann dieses. Neun von zehn Copilot-Vorfällen, die mir in Projekten begegnen, sind keine KI-Probleme, sondern Berechtigungsprobleme, die Copilot sichtbar macht.

Grounding über Microsoft Graph: Copilot sieht, was du sehen darfst

Microsoft 365 Copilot beantwortet Fragen nicht aus dem Gedächtnis des Sprachmodells, sondern reichert jeden Prompt mit Inhalten aus deinem Tenant an. Dieser Schritt heißt Grounding. Die Copilot-Orchestrierung sucht über Microsoft Graph und den semantischen Index nach passenden Mails, Chats, Besprechungen, Dateien und Inhalten aus angebundenen Systemen, übergibt die Fundstellen zusammen mit dem Prompt an das Sprachmodell und prüft die Antwort anschließend, bevor sie mit Quellenverweisen beim Nutzer ankommt.

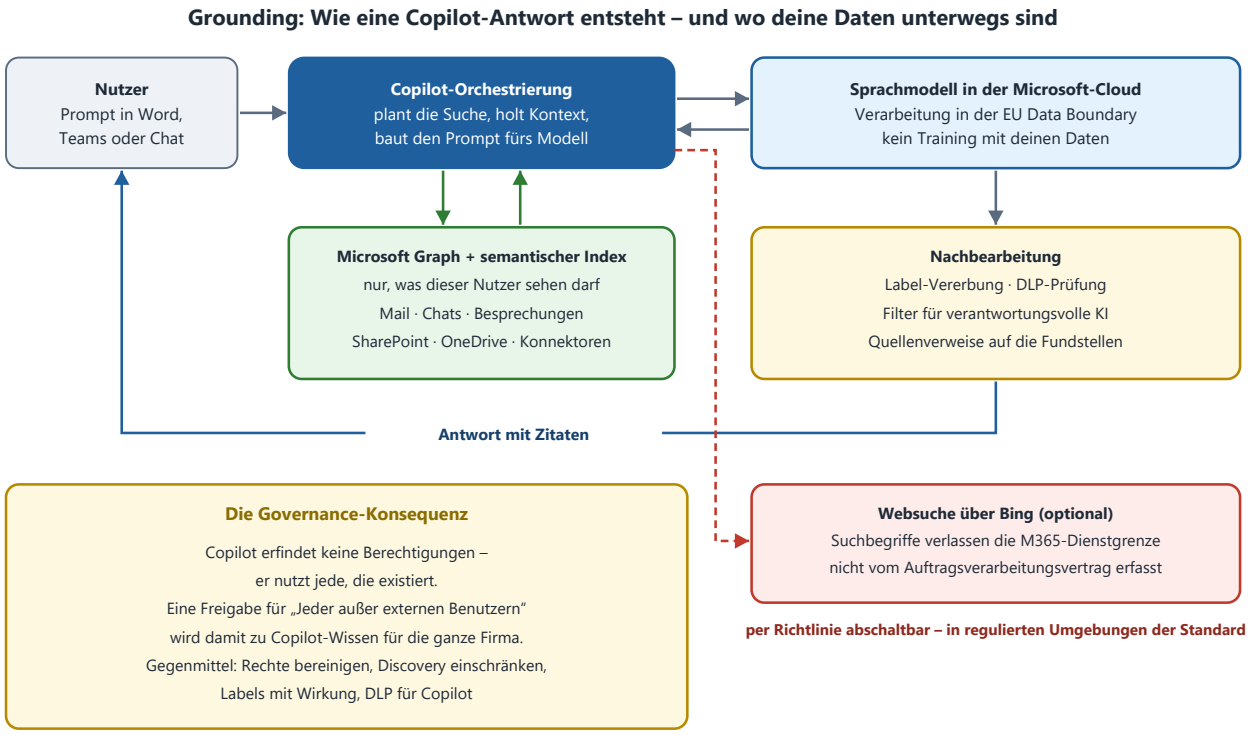


Abbildung 2: Copilot findet über Microsoft Graph nur Inhalte, auf die der fragende Nutzer Zugriff hat. Die optionale Websuche ist der einzige Weg, auf dem Suchbegriffe die Microsoft-365-Dienstgrenze verlassen.

Der entscheidende Satz für deine Governance: Copilot arbeitet immer mit den Rechten des Nutzers, der fragt. Er umgeht keine Berechtigung und erfindet keine neue. Er nutzt aber jede, die existiert – und zwar mit einer Gründlichkeit, die kein Mensch je aufbringen würde. Früher schützte dich, dass niemand wusste, wo die Gehaltsliste lag. Das nennt man in der Security-Szene „Security by Obscurity", und Copilot beendet diese Ära zuverlässig. Wer vor Copilot nichts gefunden hat, findet jetzt alles, worauf er formal Zugriff hat.

Typische Fundgruben sind Team-Sites mit der Freigabe „Jeder außer externen Benutzern“, Freigabelinks für „Personen in deiner Organisation“, die einmal per Mail verschickt und nie wieder entzogen wurden, OneDrive-Ordner ehemaliger Kolleginnen und Kollegen, öffentliche Microsoft-365-Gruppen mit sensiblen Dateien und Projekt-Sites, deren Mitgliedschaft seit Jahren niemand gepflegt hat.

Warnung: Oversharing ist kein Copilot-Fehler

Wenn Copilot einem Nutzer vertrauliche Inhalte zeigt, war dieser Nutzer vorher schon berechtigt, sie zu öffnen. Abschalten von Copilot behebt das Problem nicht, es versteckt es nur wieder. Die Ursache sitzt in den Berechtigungen – und die musst du bereinigen, mit oder ohne KI.

Berechtigungsbereinigung als Voraussetzung für den Rollout

Die gute Nachricht: Microsoft liefert inzwischen brauchbare Werkzeuge, und einige davon sind mit der Copilot-Lizenz bereits abgedeckt. SharePoint Advanced Management ist für Tenants mit Microsoft 365 Copilot enthalten; ohne Copilot gibt es es als Zusatzlizenz, und Microsoft 365 E5 allein bringt nur einen Teil der Berichte mit. Die wichtigsten Werkzeuge im Überblick:

Werkzeug	Was es leistet	Grenzen und Hinweise
Berichte zur Datenzugriffs-Governance (SharePoint Advanced Management)	Sites mit Freigaben an „Jeder außer externen Benutzern“, viele Freigabelinks, sensible Labels; Snapshot-Berichte zu Site-Berechtigungen und Oversharing-Basisbericht	Zeigt Muster, nicht jede einzelne Datei; Aktivitätsberichte decken die letzten 28 Tage ab
Site-Zugriffsüberprüfung und Restricted Access Control	Site-Besitzer prüfen Zugriffe; Zugriff auf eine Site auf eine Gruppe begrenzen, unabhängig von Freigaben einzelner Dateien	Braucht Site-Besitzer, die ihre Aufgabe ernst nehmen
Restricted Content Discovery (RCD)	Nimmt einzelne Sites aus der organisationsweiten Suche und dem Copilot-Grounding heraus, ohne Rechte zu ändern; seit Herbst 2026 auch für zuletzt geöffnete Dateien	Notpflaster: Berechtigte erreichen die Inhalte weiter direkt; keine Lösung für falsche Rechte
Restricted SharePoint Search (RSS)	Begrenzte Suche und Copilot auf eine Liste von bis zu 100 Sites	Auslaufmodell: Seit 31. Juli 2026 keine Neueinrichtung mehr, Umstieg auf RCD erforderlich
Microsoft Purview DSPM für KI	Oversharing-Bewertungen, Übersicht über Copilot-Nutzung mit sensiblen Daten, Empfehlungen für Labels und DLP	Volle Funktion je nach Purview-Lizenzstufe; Bewertungen sind Einstieg, kein Abschluss
Sensitivitätslabels für Container	Steuern Privatsphäre, Gastzugriff und Freigaben ganzer Teams und Sites	Schützen den Container, nicht automatisch jede Datei darin

Das Vorgehen, das sich in Projekten bewährt hat, hat vier Schritte. Zuerst ziehst du die Berichte und sortierst die Sites nach Risiko: Personal, Finanzen, Recht, Geschäftsführung, Forschung und alles mit auffällig breiten Freigaben. Zweitens nimmst du die kritischsten Bereiche per Restricted Content Discovery aus dem Copilot-Grounding, damit du Zeit gewinnst. Drittens bereinigst du die Rechte an der Wurzel: „Jeder“-Freigaben entfernen, Freigabelinks kassieren, verwaiste Sites

archivieren, Besitzer benennen. Viertens nimmst du das Notpflaster wieder ab, sobald die Rechte stimmen. Wer Schritt vier vergisst, hat in zwei Jahren eine Site-Liste, die niemand mehr versteht.

Tipp: Der Testnutzer-Trick

Lege vor dem Pilot ein Testkonto an, das die Gruppenmitgliedschaften eines durchschnittlichen Sachbearbeiters hat, und frage Copilot gezielt nach Gehältern, Kündigungen, Übernahmen, Passwörtern, Vorstandsprotokollen und Personalakten. Was dabei auftaucht, ist deine Bereinigungsliste. Das dauert einen Nachmittag und ist die überzeugendste Präsentation, die du je für den Vorstand vorbereitet hast.

Zur Bereinigung gehört auch das Ausmisten. Veraltete, doppelte und triviale Dokumente sind nicht nur ein Risiko, sondern verschlechtern die Antwortqualität: Wenn drei Fassungen der Reisekostenrichtlinie herumliegen, zitiert Copilot mit schöner Regelmäßigkeit die von 2019. Aufbewahrungsrichtlinien mit automatischer Löschung und ein Archivierungskonzept für inaktive Sites zahlen deshalb doppelt auf Copilot ein.

Sensitivitätslabels und DLP im Zusammenspiel mit Copilot

Labels aus Microsoft Purview Information Protection sind das wichtigste Werkzeug, um Copilot über die Berechtigungen hinaus zu steuern. Drei Mechanismen musst du kennen.

Label-Vererbung: Erstellt Copilot neue Inhalte auf Basis gelabelter Dateien, etwa einen Entwurf in Word oder eine Zusammenfassung, übernimmt das Ergebnis das Label mit der höchsten Priorität aus den verwendeten Quellen. In Copilot Chat wird das Label der Quellen bei den Verweisen angezeigt, und die Antwort erbt die Einstufung. Wer also aus einem „Streng vertraulich“-Dokument eine Zusammenfassung erzeugt, bekommt eine „Streng vertraulich“-Zusammenfassung – inklusive Verschlüsselung, falls das Label sie vorsieht.

Nutzungsrechte bei Verschlüsselung: Verschlüsselt ein Label Inhalte, kann Copilot sie nur verwenden, wenn der Nutzer neben dem Anzeigerecht auch das Nutzungsrecht EXTRACT besitzt, also Inhalte kopieren darf. Wer nur lesen darf, bekommt von Copilot auch nur Ablehnungen. Das ist ein eleganter Hebel: Ein Label für „nur ansehen“ hält Copilot zuverlässig fern, ohne dass du an den Berechtigungen etwas änderst.

DLP für Microsoft 365 Copilot: In Purview DLP gibt es einen eigenen Speicherort für Microsoft 365 Copilot und Copilot Chat. Damit kannst du festlegen, dass Dateien und Mails mit bestimmten Labels nicht in Antworten zusammengefasst werden, obwohl der Nutzer sie öffnen darf. Neuere Richtlinientypen prüfen zusätzlich den Prompt selbst auf sensible Informationstypen wie Kreditkarten- oder Ausweisnummern und verhindern, dass Copilot damit weiterarbeitet. Beim Weiterversand greifen wie gewohnt deine DLP-Regeln für Exchange, Teams und Endgeräte.

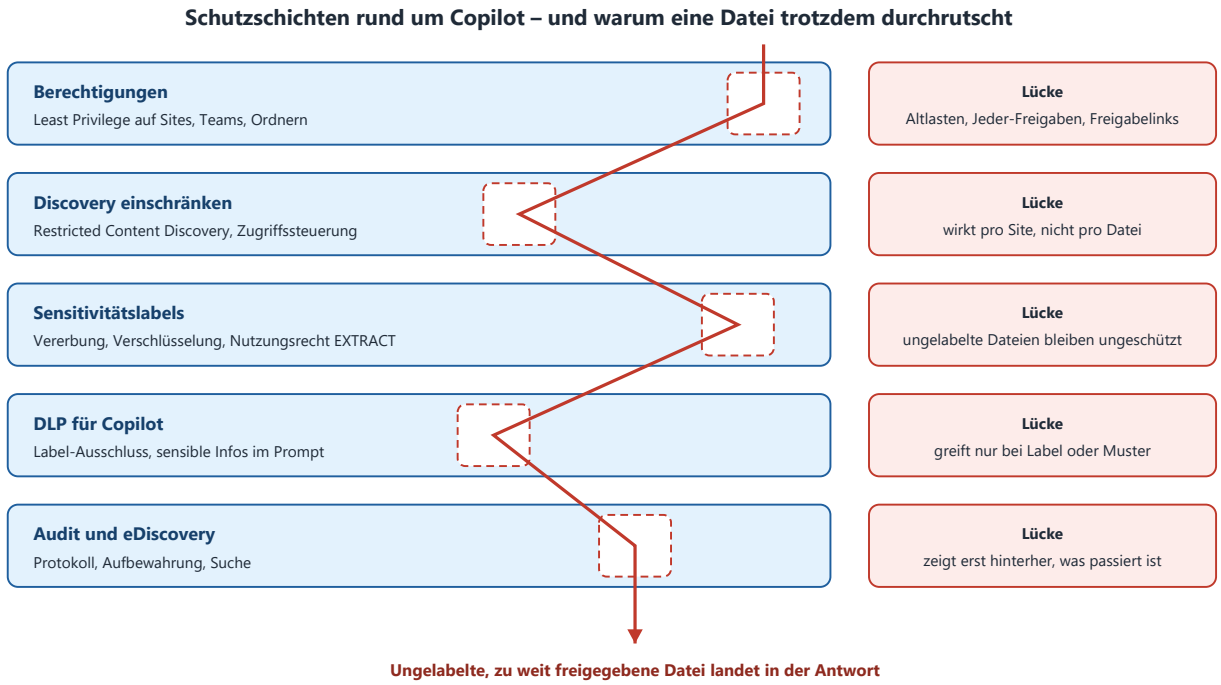


Abbildung 3: Jede Schutzschicht hat Lücken. Gefährlich wird es, wenn sie übereinander liegen – typischerweise bei einer ungelabelten, zu weit freigegebenen Datei.

Und jetzt die realistische Erwartung, die in keiner Marketingfolie steht: All das wirkt nur auf gelabelte oder per Muster erkannte Inhalte. In den meisten Tenants, die ich sehe, tragen zehn bis dreißig Prozent der Dateien überhaupt ein Label, und die wirklich heiklen Altbestände gehören selten dazu. Die Gehaltsliste von 2021 ohne Label, ohne Kreditkartennummer und mit „Jeder“-Freigabe rutscht durch alle Schichten. Automatisches Labeling hilft, ist aber kein Zauberstab: Clientseitig greift es nur beim Bearbeiten, dienstseitig arbeitet es mengenbegrenzt und braucht saubere Erkennungsregeln.

Maßnahme	Schützt zuverlässig vor	Schützt nicht vor
Berechtigungen bereinigen	Zugriff durch Unbefugte, auch über Copilot	Missbrauch durch Berechtigte
Restricted Content Discovery	zufälligem Auftauchen ganzer Sites in Antworten	gezieltem Zugriff Berechtigter, Einzeldateien in anderen Sites
Label mit Verschlüsselung ohne EXTRACT	Verarbeitung durch Copilot	Abschreiben vom Bildschirm
Label-Vererbung	Verlust der Einstufung in abgeleiteten Inhalten	ungelabelten Quellen
DLP für Copilot	Zusammenfassung gelabelter Inhalte, sensiblen Mustern im Prompt	inhaltlich heiklen Texten ohne Label oder Muster
DLP für Mail, Teams, Endgerät	Weitergabe nach außen	interner Weitergabe an falsche Kollegen

Wichtig: Labels zuerst für die Top-Bereiche

Versuche nicht, vor dem Pilot den ganzen Tenant zu labeln. Beginne mit Standardlabels für die Bibliotheken von Personal, Finanzen, Recht und Geschäftsführung, setze Pflichtlabels für neue Dokumente und hänge eine DLP-Regel für Copilot an das höchste Label. Das deckt mit wenig Aufwand den größten Teil des Schadenspotenzials ab.

Agents, Plugins und Konnektoren: Freigabe statt Wildwuchs

Copilot lässt sich erweitern, und jede Erweiterung öffnet neue Datenwege. Die Begriffe haben sich in den letzten Jahren mehrfach verschoben; was früher Plugin hieß, läuft heute meist als Agent oder Aktion, und die Graph Connectors heißen inzwischen Copilot-Konnektoren. Für die Governance zählt nicht der Name, sondern die Frage: Welche Daten fließen wohin, mit wessen Rechten?

Erweiterung	Datenfluss	Hauptrisiko	Freigabe durch
Copilot-Konnektoren (früher Graph Connectors)	Inhalte aus Drittsystemen werden in den Microsoft-Index übernommen	Rechte des Quellsystems falsch oder pauschal abgebildet	Datenverantwortlicher, CISO
Agents von Microsoft	innerhalb der Microsoft-365-Dienstgrenze	Funktionsumfang, neue Datenquellen	Produktverantwortlicher nach Policy
Selbst gebaute Agents (Agent Builder, Copilot Studio)	Wissensquellen und Aktionen nach Konfiguration, teils mit Ersteller-Rechten	Agent nutzt Rechte seines Erstellers für alle Fragenden	Lenkungskreis bei Schreibaktionen
Agents und Aktionen von Drittanbietern	Prompts und Kontext gehen an fremde Dienste	Datenabfluss, eigene Vertragsbedingungen des Anbieters	CISO, DSB, Lenkungskreis
Websuche über Bing	Suchbegriffe verlassen die Dienstgrenze	Interna in Suchanfragen	Grundsatzentscheidung Lenkungskreis

Ein tragfähiger Freigabeprozess hat fünf Stationen: Antrag mit fachlicher Begründung, Prüfung von Berechtigungen und Datenflüssen durch Security und Datenschutz, ein befristeter Test mit wenigen Nutzern, eine dokumentierte Entscheidung mit Auflagen und eine jährliche Rezertifizierung. In der Agent-Verwaltung des Microsoft 365 Admin Centers legst du fest, welche Agents für wen verfügbar sind; Agents von Drittanbietern und von Nutzern geteilte Agents sollten standardmäßig blockiert sein, bis sie den Prozess durchlaufen haben. Für Copilot Studio gehören eigene Umgebungen und Power-Platform-Datenrichtlinien dazu, damit nicht jeder Agent mit jedem Konnektor sprechen kann.

Bei Agents mit Schreibrechten kommt ein Risiko hinzu, das viele unterschätzen: indirekte Prompt-Injection. Eine präparierte Mail oder ein Dokument kann Anweisungen enthalten, die der Agent beim Lesen für bare Münze nimmt. Microsoft filtert solche Angriffe, aber kein Filter ist vollständig. Deshalb gilt: Aktionen mit Außenwirkung nur mit Bestätigung durch einen Menschen, und regelmäßige Red-Teaming-Tests mit typischen Angriffsmustern.

Warnung: Websuche in regulierten Umgebungen standardmäßig aus

Ist die Websuche aktiv, erzeugt Copilot aus dem Prompt Suchbegriffe und schickt sie an Bing. Diese Anfragen verlassen die Microsoft-365-Dienstgrenze und fallen nicht unter den Auftragsverarbeitungsvertrag für Microsoft 365, sondern unter die Bedingungen von Bing. Ein Prompt wie „Due-Diligence-Risiken bei der Übernahme von Firma X“ ist dann auch ein Suchbegriff.

Über die Richtlinie „Websuche in Copilot zulassen“ im Cloud-Richtliniendienst für Microsoft 365 schaltest du die Websuche ab oder erlaubst sie nur im Web-Modus. In Banken, Versicherungen, Gesundheitswesen, Behörden und überall mit Insiderinformationen ist „aus“ der richtige Standard. Ausnahmen gibt es per Gruppe und mit Begründung.

Datenschutz, Mitbestimmung und Nachvollziehbarkeit

Copilot verarbeitet personenbezogene Daten in einer Menge, die jede Datenschutzbeauftragte nervös machen darf: Mails, Chats, Besprechungstranskripte, Dokumente mit Kunden- und Beschäftigtendaten. Das ist beherrschbar, aber nicht nebenbei.

Auftragsverarbeitung und EU Data Boundary

Microsoft 365 Copilot ist Teil der Microsoft-365-Dienste und fällt unter das Data Protection Addendum, den Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Prompts, Antworten und die über Graph abgerufenen Daten werden nicht zum Training der Basismodelle verwendet. Seit Abschluss der dritten Phase der EU Data Boundary im Februar 2025 bleiben Kundendaten und pseudonymisierte personenbezogene Daten für Kunden in der EU und EFTA grundsätzlich innerhalb der EU-Datengrenze gespeichert und verarbeitet; Copilot gehört zu den abgedeckten Diensten. Ausnahmen beschreibt Microsoft in seiner Dokumentation, die wichtigste für Copilot ist die Websuche über Bing.

Für deine Dokumentation heißt das: Microsoft ist Auftragsverarbeiter, du bleibst Verantwortlicher. Trage Copilot ins Verzeichnis der Verarbeitungstätigkeiten ein, benenne Zwecke und Rechtsgrundlagen, prüfe die Unterauftragsverarbeiter-Liste und halte fest, welche optionalen Dienste du nutzt. Denn bei Drittanbieter-Agents und Websuche bist du schnell außerhalb des Vertragsrahmens, den du mit Microsoft hast.

Datenschutz-Folgenabschätzung für den Copilot-Einsatz

Ob eine DSFA nach Art. 35 DSGVO zwingend ist, hängt vom konkreten Einsatz ab. In der Praxis komme ich fast immer zum gleichen Ergebnis: Neue Technologie, umfangreiche Verarbeitung von Beschäftigtendaten und die objektive Eignung zur Verhaltens- und Leistungskontrolle sprechen deutlich dafür. Die Orientierungshilfe der Datenschutzkonferenz zu KI und Datenschutz liefert brauchbare Leitfragen, und Microsoft stellt eigene Unterlagen zur DSFA bereit, die du als Baustein, nicht als fertige Lösung verwenden kannst.

Eine gute Copilot-DSFA beschreibt die Datenflüsse, also Grounding, Modell, Nachbearbeitung, Speicherung und optionale Dienste. Sie bewertet die Risiken: Offenlegung durch Oversharing, falsche Aussagen über Personen, Profilbildung über Protokolldaten, Datenabfluss über Erweiterungen. Und sie ordnet jedem Risiko konkrete Maßnahmen zu, die du in diesem Beitrag findest. Ohne Berechtigungsbereinigung wird die DSFA übrigens kaum zu einem vertretbaren Restrisiko kommen – ein gutes Argument, wenn das Budget für die Bereinigung wackelt.

Löschkonzept für Copilot-Verläufe

Copilot-Interaktionen, also Prompt und Antwort, speichert Microsoft in einem versteckten Ordner im Postfach des Nutzers. Dort unterliegen sie Aufbewahrungsrichtlinien aus Microsoft Purview. Seit 2025 sind diese Richtlinien von denen für Teams-Chats getrennt, und inzwischen lassen sich Copilot und weitere KI-Apps getrennt voneinander steuern. Das ist die Grundlage für ein Löschkonzept mit eigenen Fristen.

Ein praxistauglicher Ansatz: Copilot-Interaktionen werden nach einer kurzen Frist automatisch gelöscht, typischerweise 30 bis 180 Tage, es sei denn, eine Aufbewahrungspflicht oder ein Legal Hold greift. In regulierten Bereichen wie Anlageberatung gelten längere Fristen nur für die betroffenen Gruppen. Geschäftsrelevante Ergebnisse speichert der Nutzer ohnehin als Dokument oder Mail, und die unterliegen den normalen Fristen. Nutzer können ihren Copilot-Aktivitätsverlauf zusätzlich selbst über das Portal „Mein Konto“ löschen; eine aktive Aufbewahrungsrichtlinie hält die Inhalte für Compliance-Zwecke trotzdem vor. Das musst du in der Mitarbeiterinformation offen sagen, sonst fühlen sich die Leute zu Recht getäuscht.

Fakten: Aufbewahrung wirkt nicht rückwirkend

Eine Aufbewahrungsrichtlinie erfasst nur Interaktionen ab ihrer Wirksamkeit. Wer erst nach dem Pilot Fristen definiert, hat für die Pilotphase entweder alles oder nichts – je nachdem, ob vorher eine Richtlinie für Teams-Chats oder Copilot existierte. Lege die Richtlinie deshalb vor dem ersten Prompt fest.

Mitbestimmung: Betriebsvereinbarung statt Unterlassungsklage

Nach der Rechtsprechung des Bundesarbeitsgerichts genügt für die Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG die objektive Eignung einer technischen Einrichtung zur Verhaltens- und Leistungskontrolle. Ob du die Daten auswerten willst, spielt keine Rolle. Copilot erzeugt Nutzungsdaten pro Person, Audit-Protokolle mit Zeitstempel und gespeicherte Prompts – die Eignung ist offensichtlich. Dazu kommen die Unterrichtungspflicht nach § 90 BetrVG bei der Planung und regelmäßig § 87 Abs. 1 Nr. 1 für die Verhaltensregeln im Umgang mit Copilot. Der Betriebsrat kann nach § 80 Abs. 3 BetrVG einen Sachverständigen hinzuziehen, und bei KI-Themen gilt die Erforderlichkeit kraft Gesetzes als gegeben. Plane das ein.

Eine Betriebsvereinbarung zu Copilot regelt typischerweise:

- **Zweck und Einsatzbereiche:** Unterstützung der Arbeit, keine automatisierten Personalentscheidungen.
- **Auswertungsverbot:** Keine Leistungs- oder Verhaltenskontrolle aus Copilot-Nutzungsdaten, Auswertungen nur aggregiert ab einer Mindestgruppengröße, zum Beispiel zehn Personen.
- **Anlassbezogene Prüfung:** Zugriff auf Prompts und Protokolle einzelner Personen nur bei konkretem Verdacht, im Vier-Augen-Prinzip und unter Beteiligung des Betriebsrats.
- **Berichte im Admin Center:** Die Einstellung, Benutzernamen in Berichten verborgen anzuzeigen, bleibt aktiv; Ausnahmen nur mit Zustimmung.
- **Speicher- und Löschfristen** für Interaktionen und Protokolle.
- **Schulung** vor Freischaltung, Freiwilligkeit oder Verpflichtung zur Nutzung, Umgang mit Fehlern.
- **Erweiterungen:** Information oder Zustimmung bei neuen Agents und wesentlichen neuen Funktionen.

Nach dem Urteil des Europäischen Gerichtshofs zu § 23 HDSIG aus dem Jahr 2023 ist die Betriebsvereinbarung als eigenständige Rechtsgrundlage für Beschäftigtendaten nur tragfähig, wenn sie die Anforderungen von Art. 88 DSGVO erfüllt. Lass den Entwurf deshalb nicht nur vom Personalbereich, sondern auch vom Datenschutz prüfen.

Tipp: Den Betriebsrat in den Pilot holen

Die schnellsten Einführungen, die ich begleitet habe, hatten eines gemeinsam: Zwei Mitglieder des Betriebsrats waren Teil der Pilotgruppe. Wer selbst gesehen hat, was Copilot kann und was die Berichte wirklich zeigen, verhandelt sachlich. Wer nur Folien kennt, verhandelt mit der Angst im Nacken. Eine Rahmenvereinbarung für den Pilot und eine endgültige Vereinbarung danach ist ein bewährter Weg.

Audit und Nachvollziehbarkeit: Was Purview protokolliert

Microsoft Purview Audit erfasst Copilot-Interaktionen automatisch, ohne dass du etwas einschalten musst, sofern das Überwachungsprotokoll im Tenant aktiv ist. Der Datensatz vom Typ CopilotInteraction enthält, wer wann in welcher Anwendung mit Copilot gearbeitet hat, auf welche Ressourcen die Antwort zugegriffen hat – Dateien, Sites, Mails – und welche Sensitivitätslabels

diese Ressourcen tragen. Für Agents und Aktionen kommen entsprechende Angaben zum verwendeten Agent hinzu.

Was viele überrascht: Den Text von Prompt und Antwort findest du nicht im Audit-Datensatz. Der steckt im erwähnten versteckten Postfachordner und ist über eDiscovery durchsuchbar, exportierbar und mit Legal Hold sicherbar. DSPM für KI in Purview zeigt zusätzlich Interaktionen mit sensiblen Informationen in einem Aktivitäts-Explorer an. Die Tabelle fasst zusammen, welches Werkzeug welche Frage beantwortet.

Frage	Werkzeug	Aufbewahrung
Wer hat wann Copilot genutzt, mit welchen Dateien?	Purview Audit (CopilotInteraction)	180 Tage mit Audit Standard, ein Jahr mit Audit Premium, länger per Zusatzlizenz
Was genau wurde gefragt und geantwortet?	eDiscovery, Inhaltssuche	nach deiner Aufbewahrungsrichtlinie für Copilot
Wo tauchen sensible Daten in Prompts auf?	DSPM für KI, DLP-Berichte	nach Purview-Konfiguration
Wie viele Nutzer sind aktiv, in welchen Apps?	Copilot-Nutzungsbericht im Admin Center	Zeiträume von 7 bis 180 Tagen
Wie entwickelt sich die Nutzung je Bereich?	Copilot Dashboard in Viva Insights	aggregiert, mit Mindestgruppengrößen

Die Grenzen dieser Protokolle solltest du kennen, bevor ein Prüfer sie dir erklärt. Audit zeigt, welche Dateien eine Antwort herangezogen hat, aber nicht, ob der Nutzer die Antwort weitergegeben hat. Was jemand aus dem Copilot-Fenster kopiert und in eine private Mail tippt, sieht kein Protokoll – dafür brauchst du Endpoint-DLP. Inhalte, die vor Wirksamkeit einer Aufbewahrungsrichtlinie gelöscht wurden, sind weg. Außerdem lässt sich aus Protokollen nicht ablesen, ob eine Antwort inhaltlich stimmte; dafür sind Prüfprozesse da, nicht die Technik. Und vergiss nicht: Jede Protokollauswertung über Personen ist mitbestimmungs- und datenschutzrelevant.

Für Aufbewahrungspflichten aus Handels- und Steuerrecht, für Finanzaufsicht oder Records Management gilt: Maßgeblich ist das Ergebnis, nicht der Weg. Ein mit Copilot formuliertes Angebot ist ein Handelsbrief und wird wie jeder andere archiviert. Ob zusätzlich die Interaktion selbst aufzubewahren ist, entscheidest du nach Branche – in der Anlageberatung meist ja, im Marketing meist nein.

Steuerung im Betrieb: Kennzahlen, Lizenzen und Haftung

Ein Dashboard mit zwanzig Kacheln ist keine Steuerung. Steuerung heißt: Für jede Kennzahl gibt es einen Zielwert, eine Schwelle, ab der jemand handelt, einen Verantwortlichen und einen festen Termin, an dem sie angeschaut wird.

KPIs und KRIs mit Schwellwerten und Rhythmus

Leistungskennzahlen (KPIs) zeigen, ob Copilot Nutzen stiftet. Risikokennzahlen (KRIs) warnen, bevor aus einer Entwicklung ein Vorfall wird. Acht bis zehn Werte reichen völlig. Mehr misst du am Anfang ohnehin nicht sauber.

Kennzahl	Typ	Messung	Ziel	Eingreifen ab	Rhythmus, Owner
Aktive Nutzer	KPI	Nutzungsbericht: aktiv in 28 Tagen / lizenziert	≥ 80 %	< 60 %	monatlich, Produktverantwortlicher

Kennzahl	Typ	Messung	Ziel	Eingreifen ab	Rhythmus, Owner
Nutzungstiefe	KPI	Anteil Nutzer mit Copilot in mindestens drei Apps	≥ 50 %	< 30 %	monatlich, Produktverantwortlicher
Zeitersparnis	KPI	Stichprobenmessung je Use Case plus Befragung	nach Business Case	< 50 % des Plans	quartalsweise, Fachbereich
Fehlerquote	KRI	Anteil geprüfter Ausgaben mit wesentlichem Fehler	< 5 %	> 10 %	quartalsweise, Qualitätsverantwortliche
DLP-Treffer mit Copilot-Bezug	KRI	DLP-Berichte, Copilot-Speicherort	stabil, sinkend	Anstieg > 50 % zum Vormonat	monatlich, CISO
Oversharing-Fundstellen	KRI	Datenzugriffs-Governance-Berichte	sinkend	neue kritische Site	monatlich, CISO
Datenschutzvorfälle	KRI	Meldungen an den DSB mit Copilot-Bezug	0	≥ 1	laufend, DSB
Kosten pro aktivem Nutzer	KPI	Lizenzkosten / aktive Nutzer	≤ 1,25 × Listenpreis	> 1,5 × Listenpreis	monatlich, IT-Controlling
Schulungsquote	KPI	Abschluss Pflichtmodul vor Freischaltung	100 %	< 95 %	laufend, Produktverantwortlicher

Wichtig ist die zweite Spalte von rechts. „Eingreifen ab“ heißt: Wird die Schwelle gerissen, steht das Thema automatisch auf der nächsten Tagesordnung des Lenkungskreises, mit einer Analyse und einem Vorschlag. Ohne diese Verknüpfung produziert dein Reporting schöne Kurven, die niemand liest. Weitere Kennzahlen, gerade für Agenten, beschreibe ich ausführlich in Metriken zur Messung des Erfolgs der Microsoft 365 Copilot KI-Agenten.

Zeitersparnis: Telemetrie gegen Selbstauskunft

Die Frage nach der eingesparten Zeit ist die Lieblingsfrage jedes Vorstands und die unzuverlässigste Zahl im ganzen Projekt. Es gibt drei Quellen, und alle drei sind auf ihre Weise verzerrt.

Quelle	Was sie liefert	Typische Verzerrung
Telemetrie (Nutzungsbericht, Copilot Dashboard)	Anzahl Aktionen, Zusammenfassungen, Entwürfe; im Dashboard geschätzte unterstützte Stunden	Die Stunden sind Hochrechnungen mit Faktoren aus Studien, keine Messung; Aktivität ist nicht Nutzen
Selbstauskunft (Umfragen)	Gefühlte Ersparnis pro Woche, Zufriedenheit	Neuheitseffekt, soziale Erwünschtheit, Begeisterte antworten häufiger; meist deutlich zu hoch
Prozessmessung (Stichproben)	Durchlaufzeiten vorher und nachher für definierte Aufgaben	Aufwendig, kleine Stichproben, Effekte durch andere Änderungen im Prozess

Mein Rat: Nutze die Telemetrie für Adoption, die Befragung für Akzeptanz und die Prozessmessung für die Euro-Zahl. Miss vor dem Pilot eine Baseline für drei bis fünf konkrete Aufgaben, etwa Protokollerstellung, Angebotsentwurf und Recherche für Kundenanfragen, und wiederhole die Messung nach acht Wochen. In einem Projekt gaben die Pilotnutzer im Schnitt vier

gesparte Stunden pro Woche an; die Stichprobenmessung kam auf anderthalb. Beides ist ein Erfolg. Aber nur die anderthalb Stunden halten der Nachfrage des Controllings stand.

Lizenzsteuerung und ROI ehrlich rechnen

Microsoft 365 Copilot kostet als Zusatzlizenz rund 30 US-Dollar pro Nutzer und Monat bei Jahresbindung; Details, Varianten für kleinere Unternehmen und die Abgrenzung zum kostenlosen Copilot Chat findest du in Microsoft 365 Copilot Lizenzierung. Weil die Lizenz pro Kopf und nicht pro Nutzung bezahlt wird, ist der größte Kostenhebel nicht der Preis, sondern die Zuweisung.

Der Copilot-Nutzungsbericht im Microsoft 365 Admin Center zeigt pro Nutzer das letzte Aktivitätsdatum je Anwendung. Daraus lässt sich ein einfacher Prozess bauen: Wer 30 Tage nicht aktiv war, bekommt eine freundliche Mail mit Schulungsangebot. Wer nach 60 Tagen immer noch nicht aktiv ist, gibt die Lizenz an die Warteliste ab, nach Rücksprache mit der Führungskraft. Klingt hart, ist aber fairer als die übliche Praxis, bei der der Bereichsleiter eine Lizenz hat, weil er Bereichsleiter ist, und die Assistenz, die den ganzen Tag Protokolle schreibt, keine. Beachte bei der Auswertung die Betriebsvereinbarung – die Lizenzsteuerung auf Basis der Aktivität sollte dort ausdrücklich geregelt sein.

Fakten: Rechenbeispiel: Kosten pro aktivem Nutzer

Angenommen: 200 Lizenzen zu je 30 Euro pro Monat, also 6.000 Euro. Aktiv in den letzten 28 Tagen sind 120 Nutzer. Die Kosten pro aktivem Nutzer liegen damit bei **50 Euro**, nicht bei 30.

Gemessen werden im Schnitt 1,5 gesparte Stunden pro aktivem Nutzer und Woche, also rund 6 Stunden im Monat. Bei einem internen Stundensatz von 60 Euro sind das 360 Euro pro aktivem Nutzer, zusammen 43.200 Euro. Abzüglich Lizenzen und anteiliger Betriebskosten von geschätzt 4.000 Euro bleibt ein rechnerischer Nutzen von gut 33.000 Euro im Monat.

Ehrlich bleiben: Gesparte Zeit ist nur dann Geld, wenn sie in andere wertschöpfende Arbeit fließt. Sag dem Management, wofür die Zeit genutzt wird, statt sie als Kostensenkung zu verkaufen.

Belastbar wird die Darstellung gegenüber dem Management durch drei Dinge: eine dokumentierte Baseline, konservative Annahmen, die du offenlegst, und qualitative Belege aus den Fachbereichen. Ein Satz wie „Die Angebotsabteilung bearbeitet 18 Prozent mehr Anfragen mit gleicher Besetzung“ wirkt stärker als jede ROI-Formel. Und wenn ein Bereich nach drei Monaten keinen Nutzen zeigt, ist das kein Scheitern, sondern eine Information: Lizenzen umverteilen, Use Cases schärfen oder nachschulen.

Halluzinationen, Prüfpflichten und Haftung

Copilot erzeugt Text nach Wahrscheinlichkeiten. Grounding senkt die Fehlerquote deutlich, schaltet sie aber nicht ab. Die gefährlichsten Fehler sind nicht die offensichtlich absurden, sondern die plausiblen: eine falsche Kündigungsfrist, ein vertauschter Betrag, eine Zusage aus einem veralteten Dokument, eine Besprechungszusammenfassung, die einer Person eine Aussage zuschreibt, die sie nie gemacht hat.

Ausgabe	Prüfpflicht	Wer prüft
Kundenkommunikation, Angebote, Zusagen	immer vor Versand, inhaltlich und tonal	Absender
Rechtliche Aussagen, Vertragsklauseln	immer, Verwendung nur nach Fachprüfung	Rechtsabteilung
Finanzzahlen, Kennzahlen, Berichte ans	immer gegen die Quelldaten	Ersteller plus Vier

Ausgabe	Prüfpflicht	Wer prüft
Management		Augen
Aussagen über Personen, Personalthemen	immer; keine Entscheidungen auf KI-Basis	Führungskraft, HR
Besprechungszusammenfassungen als Protokoll	vor Verteilung durch Leitung der Besprechung	Besprechungsleitung
Interne Entwürfe, Ideensammlungen, Gliederungen	Plausibilitätsprüfung	Nutzer
Zusammenfassungen für den Eigenbedarf	bei Weiterverwendung prüfen	Nutzer

Quellenprüfung im Alltag funktioniert nur, wenn sie schnell geht. Copilot verweist in seinen Antworten auf die Fundstellen; die Regel lautet: Bei jeder Zahl, jedem Datum, jeder Zusage und jeder Aussage über eine Person einmal auf den Verweis klicken. Fehlt ein Verweis bei einer Faktenaussage, ist das ein Warnsignal. Und beim Zusammenfassen von Mails und Chats gilt: Was nicht im Original steht, steht auch nicht in der Zusammenfassung – wenn doch, ist es erfunden.

Zur Haftung: Gegenüber Kunden und Geschäftspartnern haftet das Unternehmen für das, was es versendet, völlig unabhängig davon, ob ein Mensch oder Copilot den Text geschrieben hat. „Das hat die KI formuliert“ ist rechtlich so wertvoll wie „das hat der Praktikant formuliert“. Im Innenverhältnis gelten für Beschäftigte die Grundsätze des innerbetrieblichen Schadensausgleichs: Bei leichter Fahrlässigkeit keine Haftung, bei mittlerer anteilig, bei grober Fahrlässigkeit und Vorsatz in der Regel voll. Wer eine klare Prüfpflicht kennt und ignoriert, rutscht schnell in die grobe Fahrlässigkeit – auch das ist ein Grund, Prüfpflichten schriftlich festzuhalten und zu schulen. Für Urheberrechtsansprüche Dritter aus Copilot-Ausgaben bietet Microsoft mit dem Customer Copyright Commitment eine Freistellung, sofern du die vorgesehenen Schutzmechanismen nicht umgehst.

Warnung: Hochrisiko-Einsatz nach AI Act vermeiden

Copilot als Schreib- und Rechercheassistent ist nach dem AI Act kein Hochrisiko-System. Das ändert sich, wenn du ihn für Entscheidungen über Bewerbungen, Beförderungen, Leistungsbewertung oder Kündigungen einsetzt – solche Anwendungen fallen in Anhang III. Schreib in die Policy, dass Copilot dort höchstens Material zusammenträgt und nie entscheidet. Mehr zur Regulierung in Der EU AI-Act – Regulierung der Künstlichen Intelligenz. Viel Schaden, wenig Nutzen..

Umsetzung: Stufenweiser Rollout mit Guardrails

Der häufigste Fehler beim Rollout ist nicht zu viel Vorsicht, sondern ein Big Bang auf Druck von oben. Die zweithäufigste ist das Gegenteil: ein Pilot, der nie endet, weil niemand festgelegt hat, wann er erfolgreich ist. Beides vermeidest du mit Phasen und Gates.

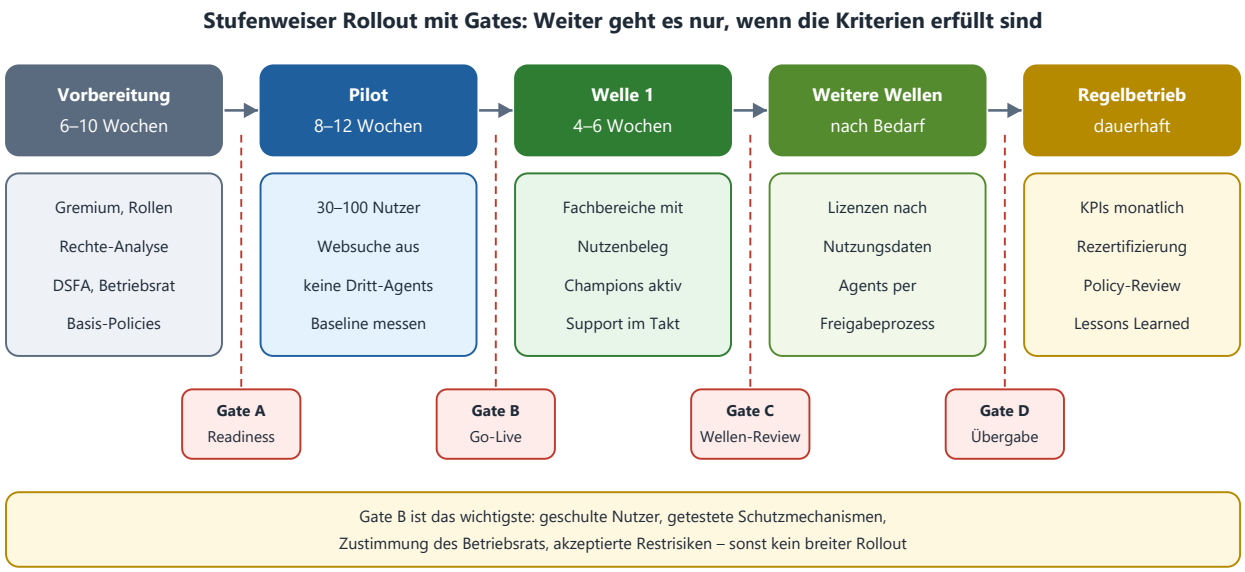


Abbildung 4: Vier Gates trennen die Phasen. Jedes Gate hat vorher festgelegte Kriterien; wer sie nicht erfüllt, verlängert die Phase, statt sie zu überspringen.

Vorbereitung und Pilot mit Guardrails

In der Vorbereitung stehen Gremium, Rollen, Risikoanalyse, Berechtigungsanalyse, DSFA, Rahmenvereinbarung mit dem Betriebsrat und eine Basis-Policy. Gleichzeitig konfiguriert das Admin-Team die technischen Grundlagen: Mehrstufige Authentifizierung und Richtlinien für bedingten Zugriff für alle Copilot-Nutzer, Überwachungsprotokoll aktiv, Aufbewahrungsrichtlinie für Copilot-Interaktionen, Labels für die kritischen Bereiche, DLP für Copilot, Restricted Content Discovery für die Sites, die bis zur Bereinigung nicht auftauchen dürfen.

Der Pilot umfasst 30 bis 100 Nutzer aus drei bis fünf Bereichen, gemischt aus Begeisterten und Skeptikern. Nur Begeisterte zu nehmen, ist bequem und liefert Ergebnisse, die nach dem Rollout keiner wiedererkennt. Die Guardrails im Pilot sind bewusst eng:

- Websuche aus, Agents von Drittanbietern und von Nutzern geteilte Agents blockiert.
- Keine Gastkonten und keine externen Nutzer mit Copilot-Zugriff.
- Sensible Bereiche per Restricted Content Discovery ausgeblendet, bis die Bereinigung durch ist.
- DLP für Copilot eher streng – lieber einige Fehlalarme als ein echter Abfluss.
- Wöchentliche Feedbackrunde, ein Teams-Kanal für Fragen und Fundstücke, ein klarer Meldeweg für Vorfälle.
- Baseline-Messung für die ausgewählten Aufgaben vor dem ersten Prompt.

Ein Wort zur externen Zusammenarbeit, weil diese Frage in jedem Pilot kommt: Gastkonten erhalten im Tenant des Gastgebers kein Copilot über dessen Lizenzen, und Copilot im Namen eines internen Nutzers findet nur, was dieser sehen darf. Das eigentliche Risiko liegt woanders: Interne Nutzer erzeugen in Besprechungen und Chats mit externen Teilnehmern Zusammenfassungen und posten sie dort, oder geben Antworten mit internem Wissen weiter. Deshalb gehören Kollaborationsbereiche mit Externen strikt getrennt von internen Ablagen, und die Policy regelt, ob Transkription und Copilot in Besprechungen mit Externen erlaubt sind.

Konkrete Go-Live-Kriterien

Gate B entscheidet über den breiten Rollout. Die Kriterien legst du vor dem Pilot fest und lässt sie vom Lenkungskreis beschließen, damit hinterher niemand die Torpfosten verschiebt.

Kriterium	Messbar als	Verantwortlich

Kriterium	Messbar als	Verantwortlich
Nutzer geschult	100 % der Welle-1-Nutzer haben Pflichtmodul und Quiz bestanden	Produktverantwortlicher
Schutzmechanismen getestet	DLP-, Label- und RCD-Testfälle dokumentiert erfolgreich; Testnutzer findet keine kritischen Inhalte mehr	CISO
Betriebsrat zugestimmt	Betriebsvereinbarung unterschrieben oder Pilotvereinbarung verlängert	Geschäftsführung, Personal
Datenschutz abgeschlossen	DSFA mit vertretbarem Restrisiko, Verzeichnis aktualisiert, Information der Beschäftigten erfolgt	DSB berät, Verantwortlicher entscheidet
Pilotziele erreicht	Aktive Nutzer ≥ 70 %, Zufriedenheit ≥ 70 %, keine offenen kritischen Vorfälle	Lenkungskreis
Betrieb bereit	Support-Wissensbasis, Eskalationswege, Notfallprozedur zur Deaktivierung getestet	Admin-Team
Restrisiken akzeptiert	Risikoregister ohne rote Einträge, gelbe mit Owner und Termin	Geschäftsführung

Wichtig: Ein Nein ist ein Ergebnis

Wenn ein Kriterium nicht erfüllt ist, verlängerst du die Phase oder reduzierst den Umfang. Copilot für Bereiche mit sauberen Rechten auszurollen und Personal, Recht und Geschäftsführung später nachzuziehen, ist eine völlig legitime Entscheidung – und viel besser als ein Rollout, der nach dem ersten Vorfall wieder einkassiert wird.

Nach Gate B folgen die Wellen. Zwischen zwei Wellen liegen mindestens zwei Wochen, in denen Support-Aufkommen, KPIs und Rückmeldungen ausgewertet werden. Lizenzen bekommen zuerst die Bereiche, in denen der Pilot den größten Nutzen gezeigt hat. Am Ende steht Gate D: die Übergabe in den Regelbetrieb mit Servicebeschreibung, Betriebshandbuch und festen Terminen für Policy-Review und Rezertifizierung. Wie so ein Projekt in der Realität verläuft, mit allen Umwegen, zeigt die Fallstudie Copilot-Einführung bei der Harry Hase AG.

Schulung: verantwortungsvolles Prompting und Fehler erkennen

Seit dem 2. Februar 2025 verpflichtet Art. 4 AI Act Betreiber von KI-Systemen, für ausreichende KI-Kompetenz ihres Personals zu sorgen. Für Copilot heißt das: Eine Schulung ist nicht nur sinnvoll, sondern gefordert, und du solltest sie dokumentieren. Bewährt hat sich ein Stufenmodell.

Zielgruppe	Inhalt	Format, Umfang
Alle Nutzer (Pflicht)	Was Copilot kann und nicht kann, Grounding und Berechtigungen, Do und Don't, Prüfpflichten, Fehler erkennen, Meldeweg	E-Learning 30–45 Minuten plus Quiz vor Freischaltung
Alle Nutzer (Praxis)	Gute Prompts mit Ziel, Kontext, Quelle und Format; Nachfragen; Prompt-Bibliothek	Live-Session 60–90 Minuten je Bereich
Champions	Vertiefung, typische Fehler, Unterstützung im Team, Rückmeldung an Governance	Workshop halber Tag, monatlicher Austausch
Führungskräfte	Prüfpflichten im Team, Umgang mit Nutzungsdaten, Erwartungsmanagement	Briefing 60 Minuten
Admins und Security	Copilot-Einstellungen, Purview, SharePoint Advanced	Workshop ein bis zwei Tage

Zielgruppe	Inhalt	Format, Umfang
	Management, Agent-Verwaltung, Vorfallbehandlung	

Der wichtigste Inhalt ist das Erkennen von Fehlern. Zeig echte Beispiele aus dem Pilot: die erfundene Zahl, die falsch zugeordnete Aussage, die Antwort aus dem veralteten Dokument. Eine Prompt-Bibliothek mit geprüften Vorlagen für die häufigsten Aufgaben hilft enorm, braucht aber einen Eigentümer und einen Pflegerhythmus. Eine veraltete Vorlagensammlung ist schlimmer als keine, weil sie Fehler vervielfältigt.

Die Nutzungsregeln auf einer Seite

Deine Policy kann zehn Seiten haben. Was die Leute lesen, passt auf eine. Diese Kurzfassung hat sich bewährt:

Das tust du	Das lässt du
Copilot für Entwürfe, Zusammenfassungen, Recherche und Struktur nutzen	Ausgaben ungeprüft an Kunden, Behörden oder Geschäftspartner schicken
Ziel, Kontext und Quelle im Prompt angeben	Personaldaten, Gesundheitsdaten oder Passwörter in den Prompt kopieren, wenn es nicht nötig ist
Bei Zahlen, Daten und Zusagen den Quellenverweis öffnen	Copilot nach Inhalten fragen, die dich dienstlich nichts angehen – auch wenn er sie finden könnte
Ergebnisse auf sensiblen Quellen intern halten und Label prüfen	Nicht freigegebene Agents oder Erweiterungen nutzen oder Inhalte in fremde KI-Dienste kopieren
Zu weit freigegebene Fundstücke sofort melden	Copilot für Entscheidungen über Personen verwenden
Fehlerhafte Antworten per Feedback und im Teams-Kanal melden	Sicherheitsfilter mit Tricks umgehen

Tipp: Fundstücke belohnen statt bestrafen

Wer Copilot eine Datei entlockt, die er nicht hätte sehen dürfen, hat dir gerade einen Gefallen getan. Mach das Melden einfach und sag ausdrücklich Danke. Wer Angst vor Ärger hat, schweigt – und dann findet die Datei der Nächste, der weniger freundlich ist.

Fazit

Microsoft Copilot-Governance ist weniger Raketenwissenschaft als konsequente Hausaufgabenerledigung. Copilot bringt kein neues Berechtigungsproblem mit, er macht das vorhandene sichtbar – in Sekunden und mit Quellenangabe. Wer vor dem Rollout die Rechte bereinigt, die kritischen Bereiche labelt, DLP für Copilot einrichtet, Websuche und fremde Erweiterungen bis zur Prüfung abschaltet, Datenschutz und Betriebsrat von Anfang an einbindet und die Protokollierung kennt, hat neunzig Prozent der Risiken im Griff.

Die restlichen zehn Prozent sind Menschen: Nutzer, die Antworten prüfen und Fehler erkennen, Führungskräfte, die Prüfpflichten ernst nehmen, und ein Produktverantwortlicher, der Kennzahlen mit Schwellwerten verknüpft und Lizenzen dorthin lenkt, wo sie wirken. Fang klein an, miss ehrlich, entscheide an Gates – und behandle jeden Fund, den Copilot zutage fördert, als Geschenk. Er hätte auch jemand anderem auffallen können.

Weiterlesen: Mehr zum Thema

› Copilot-Agenten in der Praxis
› Agent 365 – KI-Agenten als Steuerzentrale für Microsoft 365, Sicherheit und Automatisierung
› Microsoft 365 Copilot Lizenzierung
› Metriken zur Messung des Erfolgs der Microsoft 365 Copilot KI-Agenten
› Neuerungen in Microsoft Copilot in Q4/2025

Häufige Fragen zur Microsoft Copilot-Governance

Was unterscheidet Copilot-Governance von allgemeiner IT-Governance?

IT-Governance setzt den Rahmen für alle IT-Aktivitäten. Copilot-Governance konkretisiert ihn für einen KI-Assistenten, der auf nahezu alle Inhalte seiner Nutzer zugreift: Datenzugriff über Grounding, Prüfpflichten für KI-Ausgaben, Freigabe von Agents, Protokollierung von Prompts und Mitbestimmung. Sie gehört ins bestehende Regelwerk, nicht daneben.

Kann Copilot Daten sehen, auf die ein Nutzer keinen Zugriff hat?

Nein. Copilot arbeitet mit den Rechten des Nutzers, der fragt. Das Problem sind Inhalte, auf die der Nutzer formal Zugriff hat, ohne es zu wissen – über breite Freigaben, alte Links oder ungepflegte Gruppenmitgliedschaften. Vorsicht bei selbst gebauten Agents: Sie können mit den Rechten ihres Erstellers arbeiten.

Welche Mindestvoraussetzungen im Tenant sind vor dem Rollout Pflicht?

Mehrstufige Authentifizierung und bedingter Zugriff für alle Copilot-Nutzer, aktives Überwachungsprotokoll, eine Aufbewahrungsrichtlinie für Copilot-Interaktionen, Labels für die kritischen Bereiche, DLP für Copilot, eine Grundsatzentscheidung zur Websuche, blockierte Drittanbieter-Agents und eine erste Berechtigungsbereinigung der riskantesten Sites.

Brauche ich Restricted SharePoint Search noch?

Für neue Projekte nicht mehr: Seit dem 31. Juli 2026 lässt sich Restricted SharePoint Search nicht mehr neu einrichten. Das Nachfolgewerkzeug ist Restricted Content Discovery in SharePoint Advanced Management, das einzelne Sites aus Suche und Copilot-Grounding nimmt. Beides ist ein Übergangsmittel, kein Ersatz für saubere Berechtigungen.

Wie verhindere ich Datenabfluss über Prompts und Antworten?

Mit Schichten: Rechte bereinigen, Discovery für kritische Sites einschränken, Labels mit Verschlüsselung und ohne EXTRACT für Hochsensibles, DLP für Copilot und für den Weiterversand, Websuche und ungeprüfte Erweiterungen aus, Schulung und Protokollierung. Keine Schicht ist dicht, zusammen reduzieren sie das Risiko stark.

Muss ich den Betriebsrat beteiligen?

Ja. Copilot ist objektiv geeignet, Verhalten und Leistung zu überwachen, damit greift § 87 Abs. 1 Nr. 6 BetrVG. Eine Betriebsvereinbarung regelt Zweck, Auswertungsverbote, anlassbezogene Prüfungen, Fristen, Schulung und den Umgang mit neuen Funktionen. Am besten holst du den Betriebsrat schon in den Pilot.

Ist eine Datenschutz-Folgenabschätzung für Copilot erforderlich?

In den meisten Unternehmen ja, weil eine neue Technologie umfangreich Beschäftigten- und Kundendaten verarbeitet und zur Leistungskontrolle geeignet ist. Selbst wo sie nicht zwingend ist, ist sie das beste Werkzeug, um Risiken und Maßnahmen strukturiert zu dokumentieren.

Wie lange werden Copilot-Verläufe gespeichert?

So lange, wie deine Purview-Aufbewahrungsrichtlinie es vorsieht. Copilot-Interaktionen liegen in einem versteckten Postfachordner und lassen sich getrennt von Teams-Chats steuern. Üblich sind kurze Fristen von 30 bis 180 Tagen, längere nur in regulierten Bereichen. Nutzer können ihren Verlauf selbst löschen, eine aktive Aufbewahrung hält die Inhalte trotzdem vor.

Was protokolliert Purview Audit und was nicht?

Audit erfasst, wer wann in welcher App Copilot genutzt hat und welche Dateien und Labels beteiligt waren. Prompt- und Antworttext stehen nicht im Audit-Datensatz, sondern sind über eDiscovery auffindbar. Nicht erfasst wird, was ein Nutzer mit der Antwort danach macht, und ob sie inhaltlich stimmte.

Sollte die Websuche in Copilot aktiviert sein?

In regulierten Umgebungen standardmäßig nicht. Suchbegriffe gehen an Bing, verlassen die Microsoft-365-Dienstgrenze und fallen nicht unter den Auftragsverarbeitungsvertrag. Wo die Websuche fachlich nötig ist, erlaube sie per Richtlinie für bestimmte Gruppen und schule, was nicht in einen Prompt gehört.

Wie wähle ich Agents, Plugins und Konnektoren aus?

Über einen festen Prozess: Antrag mit Begründung, Prüfung von Rechten und Datenflüssen durch Security und Datenschutz, befristeter Test, dokumentierte Entscheidung mit Auflagen, jährliche Rezertifizierung. Drittanbieter-Agents bleiben blockiert, bis sie diesen Weg gegangen sind. Schreibende Aktionen nur mit menschlicher Bestätigung.

Wie gehe ich mit externen Partnern und Gastkonten um?

Gäste nutzen Copilot nicht über die Lizenzen deines Tenants. Trenne Kollaborationsbereiche mit Externen konsequent von internen Ablagen und regle, ob Copilot und Transkription in Besprechungen mit Externen erlaubt sind. Das Risiko sind interne Nutzer, die Zusammenfassungen mit internem Wissen in gemeinsame Kanäle posten.

Welche Kennzahlen sind wirklich praxistauglich?

Aktive Nutzer, Nutzungstiefe, gemessene Zeitersparnis je Use Case, Fehlerquote aus Stichproben, DLP-Treffer mit Copilot-Bezug, Oversharing-Fundstellen, Datenschutzvorfälle, Kosten pro aktivem Nutzer und Schulungsquote. Jede mit Zielwert, Eingreifschwelle, Owner und festem Termin.

Wie berechne ich den ROI von Copilot belastbar?

Kosten pro aktivem Nutzer statt pro Lizenz, Zeitersparnis aus Prozessmessung statt aus Umfragen, konservative Stundensätze und offengelegte Annahmen. Ergänze qualitative Belege aus den Fachbereichen und sag, wofür die gewonnene Zeit genutzt wird.

Wie gehe ich mit Halluzinationen um?

Mit Prüfpflichten nach Ausgabeart, Quellenprüfung bei Zahlen, Daten, Zusagen und Personen, sauberer Datenbasis ohne veraltete Dubletten und geprüften Prompt-Vorlagen. Kundenkommunikation, Rechts- und Finanzaussagen gehen nie ungeprüft raus. Gefundene Fehler werden gemeldet und fließen in Schulung und Vorlagen ein.

Wer haftet, wenn ungeprüfte KI-Inhalte Schaden verursachen?

Nach außen das Unternehmen, genau wie bei jedem anderen Text. Intern gelten die Regeln des innerbetrieblichen Schadensausgleichs; wer eine bekannte Prüfpflicht ignoriert, handelt schnell grob fahrlässig. Für Urheberrechtsansprüche aus Copilot-Ausgaben bietet Microsoft das Customer Copyright Commitment.

Wie sieht ein sinnvoller Review-Zyklus für die Policies aus?

Ein kurzer Check im Lenkungskreis jedes Quartal, ein vollständiges Review einmal im Jahr mit Security, Datenschutz, Betriebsrat und Champions, und ein außerordentliches Review bei Vorfällen, neuen Copilot-Funktionen mit Governance-Folgen oder neuen gesetzlichen Pflichten.