

CHECKLISTE · TOMORIS TOOLBOX

Microsoft Copilot (bisher Microsoft 365 Copilot) einführen: Checkliste

Fünf Phasen von Lizenz und Berechtigungen bis zum Pilot, nach Microsoft Learn, mit KI-Verordnung, DSGVO, DSFA-V und Mitbestimmung nach dem ArbVG

STAND

25.10.2026

UMFANG

PDF, 12 Seiten

ONLINE

tomoris.com/downloads/microsoft-365-copilot-einfuehrung

AUF EINEN BLICK

1 Lizenz

Copilot-Lizenz im Mandanten bringt SAM-Funktionen mit

EXTRACT

Recht, ohne das Copilot Verschlüsseltes nicht liefert

180 Tage

Copilot-Protokolle in Audit (Standard)

Art. 4

KI-Verordnung: KI-Kompetenz fördern, neu seit 27.7.2026

FÜR WEN

- Administration von Microsoft 365, SharePoint und Microsoft Purview
- Datenschutzbeauftragte und Datenschutzverantwortliche
- Projektleitung für die Einführung von KI-Assistenten
- Geschäftsführung, die über Lizenzen, Pilot und interne Regeln entscheidet

WURUM ES GEHT

Microsoft Copilot, früher Microsoft 365 Copilot, kann alles anzeigen, was eine Person in Microsoft 365 öffnen darf, auch zu weit Freigegebenes. Diese Checkliste führt Administration, Datenschutz und Projektleitung in fünf Phasen durch die Einführung: Voraussetzungen und Lizenzen klären, Überfreigabe mit SharePoint Advanced Management beheben, Bezeichnungen, Websuche, KI-Modelle, Protokollierung und Aufbewahrung festlegen, dann mit einer kleinen Gruppe pilotieren und schulen. Mit KI-Verordnung, DSGVO, DSFA-V, ArbVG und einer Lizenztafel nach Microsoft Learn.

Die Checkliste ist eine Empfehlung von TOMORIS und an die eigene Umgebung anzupassen; sie ersetzt keine Rechtsberatung. Maßgeblich sind die Gesetzestexte in der geltenden Fassung, insbesondere KI-Verordnung, DSGVO, DSFA-V, ArbVG und AVRAG. Microsoft ändert Bezeichnungen, Menüs, Funktionen, Standardeinstellungen und Lizenzen laufend: Maßgeblich sind die verlinkten Seiten von Microsoft Learn in der aktuellen Fassung sowie Ihr Vertrag mit Produktbedingungen und DPA.

INHALT

01	Worum es geht: Copilot Chat, Microsoft Copilot, Fahrplan	2
02	Phase 1: Voraussetzungen und Lizenzen	3
03	Datenschutz und Sicherheit: was Microsoft zusagt	5
04	Phase 2: Überfreigabe finden und beheben	6
05	Phase 3: Bezeichnungen, Websuche und Protokolle	8
06	Phase 4 und 5: Pilot, Schulung und Ausrollen	9
07	Recht: KI-Kompetenz, Folgenabschätzung, Betriebsrat	10
08	Häufige Fehler	11
09	Quellen	11

01

Worum es geht: Copilot Chat, Microsoft Copilot, Fahrplan

Neue Namen, zwei Stufen, ein Grundsatz: Copilot zeigt, was die Person öffnen darf. Dazu der Fahrplan in fünf Phasen.

Microsoft hat umbenannt: Microsoft 365 Copilot heißt jetzt Microsoft Copilot, Microsoft 365 Copilot Chat heißt Microsoft Copilot Chat; manche Lizenzen und Funktionen tragen in der Übergangszeit noch die alten Namen. Copilot verbindet Sprachmodelle mit Inhalten aus Microsoft Graph wie E-Mails, Chats und Dokumenten und zeigt nur Unternehmensdaten, für die die Person mindestens Anzeigeberechtigung hat. Laut Microsoft verstärkt generative KI aber das Problem übermäßiger Freigaben, weil sie veraltete oder zu weit freigegebene Inhalte schnell und von sich aus anzeigen kann. Deshalb steht das Aufräumen der Berechtigungen vor dem Ausrollen.

Copilot Chat und Microsoft Copilot im Vergleich (Microsoft Learn: Anforderungen, Übersicht über Copilot Chat)

MERKMAL	MICROSOFT COPILOT CHAT	MICROSOFT COPILOT
Lizenz	berechtigtes Microsoft-365-Abonnement, keine Copilot-Lizenz	Copilot-Lizenz und berechtigte Basislizenz (Stand Oktober 2026, Abschnitt 02)
Grundlage der Antworten	Web, eingefügte oder hochgeladene Inhalte, App-Kontext; in Outlook auch Posteingang, Kalender, Besprechungen, Chats	zusätzlich Microsoft Graph, Work IQ und semantischer Index über E-Mails, Chats, Dokumente und Websites
Word, Excel, PowerPoint, OneNote	je nach Lizenz und Mandantenkonfiguration	vollständig, mit vorrangigem Zugriff

Fahrplan (Empfehlung von TOMORIS nach der Bereitstellungsblaupause von Microsoft)



Pflicht und Empfehlung: Gesetzlich vorgegeben sind vor allem Art. 4 KI-Verordnung, die DSGVO und, wo ein Betriebsrat besteht, das ArbVG, sonst § 10 AVRAG (Abschnitt 07). Eine sichere Grundlage gegen Überfreigabe nennt Microsoft nicht erforderlich, aber dringend empfohlen. Die Checklisten sind Empfehlungen von TOMORIS nach Microsoft Learn, gelesen am 25. Oktober 2026.

02

Phase 1: Voraussetzungen und Lizenzen

Was Microsoft Learn für Lizenz, Konto, Postfach, Apps und Netzwerk voraussetzt, und welche Lizenz welche Schutzfunktion bringt.

- ☐ Lizenz: je Person eine Microsoft-Copilot-Lizenz und eine berechtigte Basislizenz, etwa Microsoft 365 Business Basic bis Premium, E3, E5 oder Office 365 E3; in Microsoft 365 E7 ist Copilot enthalten. Microsoft Copilot Business ist ein Add-On für bis zu 300 Personen mit Business-Lizenzen. Gerätebasierte Lizenzen von Microsoft 365 Apps for Enterprise reichen nicht.

- ☐ Kaufweg, Stand Oktober 2026: Laut Partner-Center-Ankündigung vom 14. Oktober 2026 gibt es Microsoft 365 Copilot und Copilot Business ab 1. Dezember 2026 auch ohne Basisabonnement; die bisherigen Angebote heißen seit 16. Oktober „(Add-On)“. Die Learn-Seiten zu Anforderungen und Lizenzen nennen das noch nicht. Die Funktionen hängen weiter von den lizenzierten Microsoft-365-Apps und -Diensten ab.
- ☐ Konten und Rollen: Geschäfts- oder Schulkonto in Microsoft Entra ID für jede Person. Rollen nach Aufgaben vergeben: KI-Administrator für Copilot- und KI-Einstellungen ohne Globalen Administrator, SharePoint-Administrator für SAM, passende Purview-Rollen für DLP.
- ☐ Postfach und OneDrive: Exchange-Online-Postfach für Funktionen mit E-Mail, Kalender und Besprechungen, nicht in Gruppenpostfächern; einige Funktionen brauchen ein OneDrive-Konto.
- ☐ Apps: Microsoft 365 Apps und unterstütztes klassisches oder neues Outlook; die Aufgabe „Office-Feature-Updates“ läuft. Wer verbundene Erfahrungen abschaltet, die Inhalte analysieren, nimmt Copilot aus Word, Excel, PowerPoint, Outlook und OneNote.
- ☐ Teams: Transkription oder Aufzeichnung konfiguriert, wenn Copilot Besprechungen nachträglich auswerten soll.
- ☐ Netzwerk und Browser: *.cloud.microsoft vollständig zugelassen, copilot.cloud.microsoft nicht blockiert, WebSockets erlaubt; private Microsoft-Konten sperrt man laut Microsoft gezielt über Mandanteneinschränkungen. Copilot in Word, Excel und PowerPoint für das Web braucht Cookies von Drittanbietern, die Linkprüfung in Chat-Antworten auch für [*.]safelinks.protection.outlook.com.
- ☐ Copilot Chat bewusst entschieden: Es steht berechtigten Personen auch ohne Copilot-Lizenz zur Verfügung. Den Unternehmensdatenschutz gibt es laut Microsoft für berechnigte Geschäftskonten, also nur bei Anmeldung mit dem Arbeitskonto.
- ☐ Bereitschaft geprüft: Diagnose „Copilot-Lizenzdetails“ je Person; vorab empfiehlt Microsoft die Copilot-Optimierungsbewertung zu Data Governance und Datensicherheit. Ziele, Anwendungsfälle und Verantwortliche festgelegt (Empfehlung von TOMORIS).

Funktion, Ort und Lizenz laut Microsoft Learn (Anforderungen, Lizenzoptionen, SAM-Voraussetzungen, Purview-Dienstbeschreibung)

FUNKTION	WO	LIZENZ LAUT LEARN
Microsoft Copilot Chat	Copilot-App, Outlook, Teams, Edge	berechtigtes Microsoft-365-Abonnement
Microsoft Copilot	Copilot-App, Word, Excel, PowerPoint, Outlook, Teams	Copilot-Lizenz plus Basislizenz (Stand Oktober 2026); in Microsoft 365 E7 enthalten
SAM: RCD, RAC, Datenzugriffsgovernance, Websitezugriffsüberprüfung	SharePoint Admin Center	mit zugewiesener Copilot-Lizenz (RCD setzt Copilot voraus); sonst SAM Plan 1

Eingeschränkte Websiteerstellung durch Apps	SharePoint Admin Center	nur SAM Plan 1, nicht in der Copilot-Lizenz
Vertraulichkeitsbezeichnungen manuell	Office-Apps, Purview-Portal	u. a. Microsoft 365 Business Premium, E3, E5
Bezeichnungen automatisch anwenden	Purview-Portal	Microsoft 365 E5, Office 365 E5, Purview Suite
DLP: Dateien und E-Mails mit Bezeichnung ausschließen	Purview-Portal > Verhinderung von Datenverlust	Microsoft 365 E5, Office 365 E5, Purview Suite; nicht Business, nicht E3
DLP für Prompts (Sperre als Vorschau)	Purview-Portal > Verhinderung von Datenverlust	alle Nutzer von Copilot und Copilot Chat
Audit (Standard), 180 Tage	Purview-Portal > Überwachung	u. a. Microsoft 365 E3, Business Basic bis Premium
Audit (Premium), Aufbewahrungsrichtlinie bis ein Jahr	Purview-Portal > Überwachung	Microsoft 365 E5, Office 365 E5, Purview Suite, Purview Suite for Business Premium
Aufbewahrung von Copilot-Interaktionen	Purview-Portal > Datenlebenszyklusverwaltung	Microsoft 365 E3 oder E5 mit Microsoft 365 Copilot (auch E3 mit Purview Suite oder E5 IPG); Business-Pläne nennt die Dienstbeschreibung nicht

Verkürzte Wiedergabe von Microsoft Learn am 25. Oktober 2026, ohne Preise. Lizenzverfügbarkeit und Produktbedingungen können sich laut Microsoft ändern; bestätigen Sie die Berechtigung vor Kauf oder Zuweisung in Produktbedingungen und Dienstbeschreibung.

03

Datenschutz und Sicherheit: was Microsoft zusagt

Berechtigungen, Training, EU-Datengrenze mit Flex-Routing, Verlauf, Websuche und KI-Modelle von Drittanbietern laut Microsoft Learn.

- **Berechtigungen:** Copilot nutzt dieselben Zugriffskontrollen wie die übrigen Microsoft-365-Dienste. Das trennt Mandanten und Personen, schützt aber nicht vor eigenen Überfreigaben: Wer zu viel öffnen darf, dem kann Copilot zu viel zeigen.
- **Kein Training:** Prompts, Antworten und über Microsoft Graph abgerufene Daten werden nicht zum Training von Basismodellen verwendet. Für Prompts und Antworten gelten Produktbedingungen und Nachtrag zum Datenschutz (DPA); Microsoft ist Auftragsverarbeiter.
- **EU-Datengrenze und Flex-Routing:** Für EU-Kunden ist Microsoft Copilot ein Dienst der EU-Datengrenze. Ist Flex-Routing erlaubt, kann die Verarbeitung durch das Sprachmodell in Spitzenlastzeiten aber in den USA, Kanada oder Australien stattfinden; für nach dem 25. März 2026 erstellte Mandanten ist es standardmäßig aktiv. Die Datenschutzseite nennt das nicht: Dort bleibt EU-Verkehr in der Grenze.

- Verlauf: Prompts und Antworten speichert Microsoft verschlüsselt bei den Inhalten des Mandanten; Administratoren verwalten sie mit Inhaltssuche und Purview, jede Person kann ihren Verlauf im Portal „Mein Konto“ löschen.
- Websuche: Copilot schickt eine kurze, aus dem Prompt abgeleitete Suchanfrage ohne Benutzer- und Mandanten-ID an Bing; in Microsoft Copilot kann sie auch Begriffe aus geöffneten oder genannten Dokumenten und aus Microsoft-365-Daten enthalten, etwa einen Namen. Für diese Anfragen gelten weder DPA noch EU-Datengrenze; Microsoft ist dafür Verantwortlicher.
- Anthropic allgemein: Die Einstellung für Anthropic als Unterauftragsverarbeiter steht in EU und EFTA standardmäßig auf „Keine Benutzer“; die Modelle sind derzeit von der EU-Datengrenze ausgenommen. „Anthropic-Modelle mit Datenaufbewahrung“ sind immer standardmäßig aus und fallen nicht unter Microsoft-Kundenvereinbarung und DPA.
- Anthropic in Word, Excel, PowerPoint: Die eigene Einstellung „Copilot in Microsoft 365-Apps mit Anthropic-Modellen“ ist für nach dem 25. März 2026 erstellte Mandanten in EU, EFTA und Vereinigtem Königreich standardmäßig aktiv; verarbeitet wird dann außerhalb der EU-Datengrenze; ältere Mandanten: Nachrichtencenter. Ihr Zusammenspiel mit der allgemeinen Einstellung beschreibt Learn widersprüchlich.
- OpenAI: Von OpenAI betriebene Modelle sind seit 24. Juli 2026 für berechtigte kommerzielle Kunden aktiv, wenn Sie nicht „Keine Benutzer“ wählen; sie liegen laut Microsoft in der EU-Datengrenze. Von Microsoft betriebene GPT-Modelle (Azure OpenAI) betrifft diese Einstellung nicht.

Die Einstellungen finden Sie im Microsoft 365 Admin Center unter Copilot > Einstellungen > Alle anzeigen: „KI-Anbieter, die als Microsoft-Unterauftragsverarbeiter arbeiten“ und „Flex-Routing in Spitzenlastzeiten“, mit der Rolle KI-Administrator. Das sind Herstellerangaben; maßgeblich sind Vertrag, Produktbedingungen und DPA.

04 —

Phase 2: Überfreigabe finden und beheben

Mit SharePoint Advanced Management: bewerten, Berichte auswerten, riskante Websites vorläufig aus der Copilot-Suche nehmen, Rechte bereinigen.

SharePoint Advanced Management (SAM, auf Microsoft Learn „Erweiterte SharePoint-Verwaltung“) ist in der Copilot-Lizenz enthalten: Sobald mindestens einer Person eine Microsoft-Copilot-Lizenz zugewiesen ist, erhalten die SharePoint-Administratoren die SAM-Funktionen für die Copilot-Bereitstellung, darunter RCD, RAC, Datenzugriffsgovernance-Berichte und Websitezugriffsüberprüfung. Die eingeschränkte Websiteerstellung durch Apps braucht das Add-On „SharePoint Advanced Management Plan 1“, das es auch ohne Copilot gibt (für SharePoint K, Plan 1 oder 2). Als Basisabonnement nennen die SAM-Voraussetzungen u. a. Office 365 E3/E5 und Microsoft 365 E1/E3/E5, die Featureliste spricht dagegen auch von Geschäftskunden: für Business-Pläne vor einer Zusage prüfen. SharePoint setzt die Freigabeeinstellungen standardmäßig auf die freizügigste Option (SharePoint Admin Center > Richtlinien > Freigabe).

1

Bewerten

SharePoint Admin Center > Erweiterte Verwaltung > Bewertung starten. Die Inhaltsverwaltungsbewertung findet Websites mit zu großem Publikum, Freigaben an „Jeder außer externen Benutzern“ (EEEU), unterbrochener Vererbung sowie inaktive und besitzerlose Websites; laut Microsoft alle 30 Tage wiederholen.

2

Berichte auswerten

Berichte > Datenzugriffsgovernance: Momentaufnahme der Websiteberechtigungen als Ausgangslage, Aktivitätsberichte zu Freigabelinks und EEEU-Freigaben der letzten 28 Tage für laufende Freigaben.

3

Vorläufig schützen

Risikante Websites per eingeschränkter Inhaltsermittlung aus der organisationsweiten Suche und der Copilot-Ermittlung nehmen: Aktive Websites > Website > Einstellungen > „Inhalt von Microsoft Copilot einschränken“ oder per PowerShell `Set-SPOSite -Identity <site-url> -RestrictContentOrgWideSearch $true` und danach die Wirkung mit der Purview-Überwachung prüfen.

4

Bereinigen lassen

Für Hochrisikowebsites SAM-Zugriffsüberprüfungen starten: Die Websitebesitzer entfernen überzählige Personen, Gruppen und organisationsweite Links bis auf Dateiebene und korrigieren unterbrochene Vererbung.

5

Dauerhaft absichern

Eingeschränkte Zugriffssteuerung für geschäftskritische Websites, „Jeder“-Links und organisationsweite Freigabegruppen im Mandanten einschränken, Besitz und inaktive Websites über Richtlinien steuern. Erst dann die vorläufige Sperre aufheben.

Kurz gesagt: Die eingeschränkte Inhaltsermittlung (RCD) verbirgt eine SharePoint-Website vor organisationsweiter Suche und Copilot-Ermittlung, nicht aber vor Copilot in bereits geöffneten Dokumenten; Berechtigungen und Suchen im Websitekontext bleiben unberührt, OneDrive ist nicht erfasst. Bei mehr als 500.000 Elementen kann die Wirkung über eine Woche dauern. Die eingeschränkte Zugriffssteuerung (RAC) sperrt: Zugang hat nur, wer berechtigt und Mitglied einer von bis zu 10 Gruppen ist; Websites freigegebener und privater Kanäle brauchen eine eigene Einstellung. RCD laut Microsoft selektiv und vorübergehend einsetzen.

05 —

Phase 3: Bezeichnungen, Websuche und Protokolle

Was Bezeichnungen, DLP und Websuche-Richtlinie bei Copilot bewirken und wie Sie protokollieren.

Verschlüsselt eine Vertraulichkeitsbezeichnung aus Microsoft Purview Information Protection, gibt Copilot die Daten nur zurück, wenn die Person die Nutzungsrechte VIEW und EXTRACT hat. Erstellt Copilot in Word, PowerPoint oder Outlook neue Inhalte aus bezeichneten Dateien, erbt das Ergebnis die Bezeichnung mit der höchsten Priorität samt Schutz. Mit S/MIME geschützte E-Mails gibt Copilot nicht zurück.

- ☐ Vertraulichkeitsbezeichnungen für Office-Dateien in SharePoint und OneDrive aktiviert; sonst nutzt Copilot verschlüsselte Dateien nur, wenn sie in Office-Apps unter Windows geöffnet sind.
- ☐ EXTRACT für streng vertrauliche Bezeichnungen nur dem engsten Personenkreis gewährt (Empfehlung von TOMORIS).
- ☐ DLP-Richtlinie für den Speicherort „Microsoft 365 Copilot und Copilot Chat“ geprüft: Dateien und E-Mails mit gewählten Bezeichnungen von der Verarbeitung ausschließen (sie erscheinen weiter als Zitat), Prompts mit vertraulichen Informationstypen sperren (Vorschau, Rollout prüfen) oder bei solchen Prompts nur die Websuche sperren (Lizenzen: Abschnitt 02).
- ☐ Websuche entschieden: Richtlinie „Websuche in Copilot zulassen“ im Clouddrichtliniendienst für Microsoft 365 setzen, mit drei Optionen: aktiviert, deaktiviert oder nur im Arbeitsmodus von Copilot deaktiviert. Ohne diese Richtlinie bleibt die Websuche verfügbar, außer optionale verbundene Erfahrungen sind abgeschaltet.
- ☐ Flex-Routing und Anthropic-Einstellungen bewusst entschieden und dokumentiert (Abschnitt 03); bei Mandanten von vor dem 25. März 2026 den aktuellen Stand im Admin Center ablesen.

Microsoft Purview protokolliert Copilot-Interaktionen automatisch im Rahmen von Audit (Standard), das für Organisationen mit passendem Abonnement standardmäßig aktiviert ist. Ein Datensatz zeigt, wer wann wo mit Copilot gearbeitet hat, verweist auf genutzte Dateien und Websites samt Bezeichnung, vermerkt erkannte Jailbreak- und Prompt-Injection-Versuche und nennt meist das Modell. Hat Copilot das Web genutzt, steht in **AISystemPlugin.Id** der Wert **BingWebSearch**. Audit (Standard) bewahrt Datensätze 180 Tage auf. Mit Audit (Premium) lassen sie sich über eine Aufbewahrungsrichtlinie für Überwachungsprotokolle bis zu einem Jahr, mit Zusatzlizenz zehn Jahre aufbewahren; ein Jahr ab Werk gilt dort nur für Entra-ID-, Exchange-, OneDrive- und SharePoint-Datensätze.

- ☐ Überwachung im Microsoft Purview-Portal geprüft und eine Testsuche nach Copilot-Aktivitäten durchgeführt; Aufbewahrungsdauer der Protokolle nach gesetzlichen und internen Anforderungen festgelegt, länger als 180 Tage per Aufbewahrungsrichtlinie (Audit Premium).

- ☐ Aufbewahrungsrichtlinie für Prompts und Antworten am Speicherort „Microsoft Copilot-Erfahrungen“ angelegt, der inzwischen von den Teams-Chats getrennt ist. Auch eine Löschung nach einem Tag kann laut Microsoft rund 16 Tage dauern, bis eDiscovery die Nachricht nicht mehr findet; Holds und andere Aufbewahrungsrichtlinien schieben sie weiter auf.
- ☐ Einsicht in Prompts und Antworten geregelt: Im Aktivitäts-Explorer zeigt Purview sie nur Mitgliedern der Rollengruppe „Content Explorer Content Viewer“; zusätzlich finden Berechtigte mit Inhaltssuche und eDiscovery sie im Postfach der Person. Beide Kreise klein halten, Einsicht nur mit dokumentiertem Zweck (Empfehlung von TOMORIS).

Einschätzung von TOMORIS: Eine Bezeichnung ohne Verschlüsselung verbirgt nichts vor Copilot; ausschließen lassen sich Inhalte über Berechtigungen, Verschlüsselung ohne EXTRACT oder DLP. „DSPM für KI“ führt Microsoft nur noch als „DSPM für KI (klassisch)“; neue Funktionen erhält das aktuelle Datensicherheitsstatus-Management (DSPM) in Purview.

06

Phase 4 und 5: Pilot, Schulung und Ausrollen

Klein anfangen, schulen, nachsteuern, dann in Wellen erweitern. Mit Mustertext für die Pilotgruppe.

- ☐ Pilotgruppe bestimmt: wenige Personen aus mehreren Bereichen mit bereinigten Websites (Empfehlung von TOMORIS); die eingeschränkte Inhaltsermittlung nennt Microsoft auch für stufenweise Rollouts.
- ☐ Lizenzen mit dem Installationshandbuch (Setup guide) im Microsoft 365 Admin Center zugewiesen, Begrüßungs-E-Mail gesendet; im Onboarding sieht Microsoft einen Link zur KI-Nutzungsrichtlinie vor.
- ☐ Geschult: Grenzen von KI, Ergebnisse prüfen, erlaubte Daten, Arbeitskonto, Bezeichnungen, Websuche; je Person dokumentiert, als Nachweis zu Art. 4 KI-Verordnung.
- ☐ Feedback-Richtlinien bewusst gesetzt: „Nicht konfiguriert“ wirkt wie „Aktiviert“, und Feedback kann Protokolle mit Prompts und Antworten, Screenshots und Anlagen an Microsoft senden. Gemeldete Überfreigaben sofort behoben, personenbezogene Auswertungen vorher mit Datenschutz und Betriebsrat geklärt.
- ☐ In Wellen erweitert: nächste Abteilung erst nach Bereinigung ihrer Websites, dann vorläufige Sperren aufheben.

Mustertext zum Anpassen (Empfehlung von TOMORIS): „Ab [Datum] steht Ihnen Microsoft Copilot zur Verfügung. Melden Sie sich immer mit Ihrem Arbeitskonto an. Copilot kann alles finden, was Sie in Microsoft 365 öffnen dürfen. Inhalte, die Sie nicht sehen sollten, geben Sie nicht weiter und melden sie sofort an [Name, Funktion, Kontakt]. Prüfen Sie jedes Ergebnis, bevor Sie es verwenden. Welche Daten Sie verwenden dürfen, regelt unsere KI-Nutzungsrichtlinie: [Link]. Ihre Schulung findet am [Datum] statt.“

07 —

Recht: KI-Kompetenz, Folgenabschätzung, Betriebsrat

Art. 4 und 50 KI-Verordnung, Art. 35 DSGVO mit der DSFA-V und Mitbestimmung nach ArbVG und AVRAG.

- Art. 4 KI-Verordnung: Wer ein KI-System in eigener Verantwortung beruflich nutzt, ist Betreiber (Art. 3 Z 4). Seit 27. Juli 2026 gilt Art. 4 in der Fassung der VO (EU) 2026/1744: Betreiber „ergreifen Maßnahmen, um die Entwicklung der KI-Kompetenz ihres Personals ... zu unterstützen“, ohne ein bestimmtes Niveau zu garantieren. Früher galt: nach besten Kräften ein ausreichendes Maß sicherstellen.
- Art. 50 Abs. 4 KI-Verordnung (seit 2. August 2026): Betreiber legen offen, dass Deepfakes und veröffentlichte Texte zu Angelegenheiten von öffentlichem Interesse künstlich erzeugt sind; bei solchen Texten nicht, wenn sie menschlich überprüft oder redaktionell kontrolliert werden und jemand die redaktionelle Verantwortung trägt.
- Art. 35 und 30 DSGVO: Bei voraussichtlich hohem Risiko, insbesondere mit neuen Technologien, ist vorab eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 Abs. 1). Copilot gehört als Verarbeitungstätigkeit ins Verzeichnis nach Art. 30.
- DSFA-V (BGBl. II Nr. 278/2018): Nach § 2 Abs. 2 ist eine DSFA durchzuführen, wenn ein Kriterium der Z 1 bis 6 erfüllt ist; Z 4 erfasst neue Technologien, welche die Abschätzung der Auswirkungen erschweren, „insbesondere durch den Einsatz von künstlicher Intelligenz“.
- Schlussteil von § 2 Abs. 2 DSFA-V: „Im Zusammenhang mit Beschäftigungsverhältnissen gilt dies nicht, wenn eine Betriebsvereinbarung oder Zustimmung der Personalvertretung vorliegt.“
- § 96 Abs. 1 Z 3 ArbVG: Die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer bedarf der Zustimmung des Betriebsrates, sofern diese die Menschenwürde berühren.
- § 96a Abs. 1 Z 1 ArbVG: Ebenso Systeme zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung personenbezogener Daten der Arbeitnehmer über allgemeine Angaben zur Person und fachliche Voraussetzungen hinaus, außer die Verwendung geht nicht über Pflichten aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag hinaus; ersetzbar durch die Schlichtungsstelle (Abs. 2).
- § 10 AVRAG: Ohne Betriebsrat sind Kontrollmaßnahmen und technische Systeme, welche die Menschenwürde berühren, nur mit Zustimmung des Arbeitnehmers zulässig.

Die DSFA-V nennt Fälle, in denen jedenfalls eine DSFA nötig ist (§ 2 Abs. 1); Maßstab bleibt das hohe Risiko nach Art. 35 Abs. 1 DSGVO. Ob DSFA und Mitbestimmung greifen, hängt von der Ausgestaltung ab, etwa ob Protokolle, Nutzungsberichte oder Prompt-Inhalte personenbezogen ausgewertet werden. TOMORIS empfiehlt, Datenschutz und Betriebsrat vor dem Pilot einzubinden und eine Betriebsvereinbarung zu prüfen. Diese Übersicht ersetzt keine Rechtsberatung.

08

Häufige Fehler

Was die Einführung riskant macht und wie Sie es vermeiden.

- Copilot ausrollen, bevor die Berechtigungen aufgeräumt sind: Copilot kann alles anzeigen, was eine Person öffnen darf, auch zu weit Freigegebenes.
- Copilot Chat übersehen: Es steht berechtigten Personen auch ohne Copilot-Lizenz zur Verfügung.
- Eingeschränkte Inhaltsermittlung als Dauerlösung: Sie verbirgt nur, die Berechtigungen bleiben falsch.
- EXTRACT großzügig vergeben: Ohne dieses Recht gibt Copilot verschlüsselte Inhalte nicht zurück.
- Standards ungeprüft lassen: Ohne Richtlinie ist die Websuche verfügbar; in Mandanten ab dem 25. März 2026 sind Flex-Routing und Anthropic in Word, Excel und PowerPoint standardmäßig an, mit Verarbeitung außerhalb der EU-Datengrenze; OpenAI-betriebene Modelle sind seit 24. Juli 2026 aktiv, wenn niemand widerspricht.
- Datenschutz-Folgenabschätzung und Betriebsrat erst nach dem Rollout einbinden.
- Schulung als einmaligen Termin sehen: Neue Personen und Funktionen brauchen neue Schulung.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

09

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- | | |
|---|---|
| <p>1 Learn: Datenschutz und Sicherheit für Microsoft Copilot
Umbenennung, Organisationsdaten, Verlauf, EU-Datengrenze, Schutz
learn.microsoft.com/de-de/microsoft-365/copilot/microsoft-365-c...</p> | <p>2 Learn: Anforderungen für Microsoft Copilot
Überblick, Lizenz, Identität, Rollen, Postfach, Apps, Browser, Netzwerk
learn.microsoft.com/de-de/microsoft-365/copilot/microsoft-copil...</p> |
| <p>3 Learn: Lizenzoptionen für Microsoft Copilot
Berechtigte Pläne, Copilot Business, Hinweis zu Produktbedingungen
learn.microsoft.com/de-de/microsoft-365/copilot/copilot-license...</p> | <p>4 Partner Center: Ankündigungen Oktober 2026
Copilot-Angebote ohne Basisabonnement ab 1.12.2026, „(Add-On)“ ab 16.10.2026
learn.microsoft.com/de-de/partner-center/announcements/2026-oct...</p> |
| <p>5 Learn: Übersicht über Microsoft Copilot Chat
Grounding, Vergleich, Unternehmensdatenschutz für Arbeitskonten
learn.microsoft.com/de-de/copilot/overview</p> | <p>6 Learn: Einführungshandbuch für IT-Administratoren
Optimierungsbewertung, Installationshandbuch, Onboarding, Feedback
learn.microsoft.com/de-de/microsoft-365/copilot/enablement-reso...</p> |
| <p>7 Learn: Sichere Grundlage für Copilot konfigurieren
Blaupausen-Schritte 1 bis 3, SAM in Copilot-Lizenzen, vorläufiger Schutz
learn.microsoft.com/de-de/microsoft-365/copilot/configure-secur...</p> | <p>8 Learn: Mit SAM auf Copilot vorbereiten
Bewertung, Freigabeeinstellungen, Datenzugriffsgovernance-Berichte
learn.microsoft.com/de-de/microsoft-365/copilot/get-ready-copil...</p> |

- 9 **Learn: Voraussetzungen für SAM**
Basisabonnements, Copilot-Lizenz oder SAM Plan 1, Rollen
learn.microsoft.com/de-de/sharepoint/sharepoint-advanced-manage...
- 11 **Learn: Eingeschränkte Inhaltsermittlung (RCD)**
Funktionsweise, Grenzen, Admin Center, PowerShell, FAQ
learn.microsoft.com/de-de/sharepoint/restricted-content-discove...
- 13 **Learn: DSPM, Datenrisikobewertungen gegen Überfreigabe**
Aktuelle Version, DSPM für KI (klassisch), Überfreigabe durch generative KI
learn.microsoft.com/de-de/purview/data-security-posture-managem...
- 15 **Learn: DLP für Microsoft 365 Copilot und Copilot Chat**
Bezeichnungen, Prompts (Vorschau), Websuche, Rollen
learn.microsoft.com/de-de/purview/dlp-microsoft365-copilot-loca...
- 17 **Learn: Anthropic-Modelle in Microsoft Online Services**
EU und EFTA „Keine Benutzer“, Datenaufbewahrung, Einstellung
learn.microsoft.com/de-de/microsoft-365/copilot/connect-to-ai-s...
- 19 **Learn: Flexibles Routing (EU und EFTA)**
Standard ab 25.3.2026, USA, Kanada, Australien, Einstellung
learn.microsoft.com/de-de/microsoft-365/copilot/copilot-flex-ro...
- 21 **Learn: Microsoft-Feedback für Ihre Organisation verwalten**
Richtlinien, „Nicht konfiguriert“, Prompts und Screenshots im Feedback
learn.microsoft.com/de-de/privacy/microsoft-365/feedback/feedba...
- 23 **Learn: Überwachungslösungen in Microsoft Purview**
180 Tage, Audit (Premium), Aufbewahrungsrichtlinien
learn.microsoft.com/de-de/purview/audit-solutions-overview
- 25 **Learn: Microsoft-Purview-Dienstbeschreibung**
Lizenzen für Audit, Aufbewahrung, DLP, Bezeichnungen
learn.microsoft.com/de-de/office365/servicedescriptions/microso...
- 27 **DSGVO, Verordnung (EU) 2016/679, EUR-Lex**
Art. 30, Art. 35 Abs. 1 und 4
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- 29 **Arbeitsverfassungsgesetz (ArbVG), RIS**
§ 96 Abs. 1 Z 3, § 96a Abs. 1 Z 1 und Abs. 2
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 10 **Learn: SAM-Features in Microsoft-Copilot-Lizenzen**
Feature-Tabelle für Unternehmens- und Geschäftskunden, Plan-1-Ausnahme
learn.microsoft.com/de-de/sharepoint/sharepoint-advanced-manage...
- 12 **Learn: Eingeschränkte Zugriffssteuerung (RAC)**
Aktivierung, bis zu 10 Gruppen, Kanalwebsites, Suche und Copilot
learn.microsoft.com/de-de/sharepoint/restricted-access-control
- 14 **Learn: Microsoft Purview für Copilot und Copilot Chat**
Bezeichnungen, VIEW und EXTRACT, Vererbung, Audit, Aktivitäts-Explorer
learn.microsoft.com/de-de/purview/ai-m365-copilot
- 16 **Learn: Websuche in Microsoft Copilot**
Suchanfragen, DPA und EU-Datengrenze, Richtlinie
learn.microsoft.com/de-de/microsoft-365/copilot/manage-public-w...
- 18 **Learn: Copilot in Microsoft 365-Apps mit Anthropic-Modellen**
Standard ab 25.3.2026, Verarbeitung außerhalb der EU-Datengrenze
learn.microsoft.com/de-de/microsoft-365/copilot/copilot-anthrop...
- 20 **Learn: OpenAI als Unterauftragsverarbeiter**
Aktiv seit 24.7.2026, EU-Datengrenze, Azure OpenAI unberührt
learn.microsoft.com/de-de/microsoft-365/copilot/openai-subproce...
- 22 **Learn: Überwachungsprotokolle für Copilot**
Audit (Standard), Eigenschaften, BingWebSearch
learn.microsoft.com/de-de/purview/audit-copilot
- 24 **Learn: Aufbewahrung für Copilot und KI-Apps**
Speicherort, Postfachordner, Löschdauer, Holds
learn.microsoft.com/de-de/purview/retention-policies-copilot
- 26 **KI-Verordnung (EU) 2024/1689, konsolidiert 27.07.2026**
Art. 3 Z 4, Art. 4 in der Fassung der VO (EU) 2026/1744, Art. 50 Abs. 4, Art. 113
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02024R1689-20...
- 28 **DSFA-V, BGBl. II Nr. 278/2018, RIS**
§ 2 Abs. 1, Abs. 2 Z 4 und Schlussteil
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 30 **AVRAG § 10, RIS**
§ 10 Abs. 1
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...