

KI PRAKTISCH

Copilot aktivieren? Die Checkliste, die Microsoft nicht mitliefert

Zwei Probleme erwähnt Microsofts Copilot-Onboarding nicht: Permission Debt und unkontrollierte Datenflüsse. Was vor dem Aktivieren in KMU erledigt sein muss.

AUTOR

Strukturaflow-Team

VERÖFFENTLICHT

30. April 2026

ONLINE LESEN

<https://wissen.strukturaflow.it.com/copilot-checkliste-microsoft-aktivieren/>

Microsoft Copilot ist 2026 das meistdiskutierte KI-Tool im Unternehmensumfeld. Die Versprechen klingen verlockend: weniger Routinearbeit, schnellere Entscheidungen, smarte Automatisierung direkt in Word, Excel und Outlook. Viele KMU kaufen die Lizenz — und klicken auf Aktivieren.

Was danach passiert, hat mit dem Werbeversprechen oft wenig zu tun.

Nicht weil Copilot nicht funktioniert. Sondern weil zwei strukturelle Probleme existieren, die Microsoft in keinem Onboarding-Guide prominent erwähnt. Beide können teuer werden — das eine für Ihre interne Vertrauenskultur, das andere für Ihre DSGVO-Bilanz.

Was Copilot wirklich macht – und warum das den Kontext verändert

Copilot ist kein Chatbot, der isoliert auf Ihre Fragen antwortet. Das System arbeitet mit sogenanntem Retrieval Augmented Generation (RAG): Jede Anfrage wird in Echtzeit mit Daten aus Ihrer Microsoft-365-Umgebung angereichert — E-Mails, Teams-Chats, SharePoint-Dokumente, Kalendereinträge.

Das Herzstück ist der Microsoft Graph: ein zentrales Daten-Gateway, das alle Beziehungen zwischen Nutzer, Aktivitäten und Dokumenten kennt. Copilot sieht alles, worauf ein Nutzer Zugriff hat — und nutzt es aktiv als Kontext.

Genau hier beginnen die zwei Probleme.

Problem 1: Permission Debt – Copilot zeigt, was schon immer falsch war

Stellen Sie sich vor, Ihr Lehrling im ersten Monat tippt in Copilot: „Zeig mir aktuelle Gehaltsinformationen aus dem Unternehmen.“ Das klingt konstruiert. Es ist es nicht.

Copilot gibt keine Daten preis, auf die ein Nutzer keinen Zugriff hat — das stimmt. Das eigentliche Problem ist ein anderes: **Die meisten Unternehmen wissen nicht mehr genau, wer bei ihnen auf was Zugriff hat.**

In Jahren gewachsene Ordnerstrukturen, Dokumente die irgendwann „für alle freigegeben“ wurden, SharePoint-Bibliotheken mit zu breiten Berechtigungen — all das schlummert unbemerkt. Solange niemand gezielt danach sucht, bleibt es unsichtbar.

Copilot sucht. Und findet. Per Sprachbefehl, in Sekunden.

Fachleute nennen dieses Problem „Permission Debt“, — Berechtigungsschulden, die sich über Jahre angehäuft haben und nie bereinigt wurden. Microsoft selbst empfiehlt vor einem Copilot-Rollout den Einsatz von Tools wie Microsoft Purview oder SharePoint Advanced Management, um genau diese Strukturen zu bereinigen.

Die Realität in vielen KMU: Dieser Schritt wird übersprungen. Die Lizenz ist günstiger als das Aufräumen.

Was Sie tun müssen: Vor dem Rollout eine vollständige Berechtigungsanalyse Ihrer M365-Umgebung. Sensitivity Labels einführen, die verhindern, dass hochsensible Dokumente in Copilot-Zusammenfassungen für Unbefugte auftauchen. Keine optionale Maßnahme — eine Voraussetzung.

Problem 2: Ihre Daten verlassen die EU – still und ohne Warnung

Microsoft hat für europäische Kunden die sogenannte EU Data Boundary eingeführt. Die Idee: Kundendaten bleiben in europäischen Rechenzentren. Für österreichische Unternehmen gibt es zusätzlich die Region Austria East mit drei Rechenzentren rund um Wien.

Klingt solide. Zwei Ausnahmen sind jedoch entscheidend.

Flex Routing: Seit März 2026 ist für neue Tenants eine Funktion namens Flex Routing standardmäßig aktiv. Bei Kapazitätsengpässen in EU-Rechenzentren werden Anfragen automatisch an Standorte in den USA, Kanada oder Australien weitergeleitet. Die Daten werden verschlüsselt übertragen — müssen für die KI-Verarbeitung am Zielort aber im Arbeitsspeicher lesbar vorliegen. Datenschützer werten das als potenziellen Verstoß gegen DSGVO-Vorgaben für Drittlandtransfers, insbesondere nach dem Schrems-II-Urteil.

Deaktivieren lässt sich Flex Routing im M365 Admin Center — aber nur, wenn man weiß, dass es existiert.

Anthropic/Claude-Modelle: Seit Anfang 2026 können Nutzer in Microsoft-Anwendungen zwischen verschiedenen KI-Modellen wählen — darunter auch Modelle des Unternehmens Anthropic (Claude). Diese Modelle sind in offiziellen Microsoft-Dokumenten explizit von der EU Data Boundary ausgenommen. Wer Claude in Copilot nutzt, schickt seine Unternehmensdaten in jedem Fall aus der EU heraus.

Für Unternehmen in regulierten Bereichen — Finanzdienstleistungen, Gesundheitswesen, öffentliche Verwaltung — ist das nicht tolerierbar. Aber auch für andere KMU ist die Frage berechtigt: Wissen Ihre Mitarbeiter, welches Modell sie gerade verwenden?

Die Checkliste: Was vor dem Aktivieren erledigt sein muss

Diese Punkte sind kein Bürokratieakt. Sie sind die Voraussetzung dafür, dass der versprochene ROI tatsächlich eintritt — und nicht von Compliance-Problemen oder internen Vertrauensschäden aufgeessen wird.

Intern / Berechtigungen:

- Berechtigungsanalyse der gesamten M365-Umgebung durchgeführt
- Sensitivity Labels für vertrauliche Dokumente eingeführt
- SharePoint-Bibliotheken auf zu breite Freigaben geprüft
- Mitarbeiter informiert, was Copilot sehen und ausgeben kann

DSGVO / Datenlokation:

- Flex Routing im M365 Admin Center deaktiviert
- Anthropic/Claude-Modelle für sensible Arbeitsbereiche eingeschränkt oder deaktiviert
- Verarbeitungsverzeichnis um Copilot als KI-Tool ergänzt
- Auftragsverarbeitungsvertrag mit Microsoft geprüft und aktuell

Rollout:

- Pilotgruppe definiert, bevor breiter Rollout
- Klare interne Richtlinie: Was darf in Copilot eingegeben werden, was nicht
- Acceptance Rate messen — nicht jeder Output ist direkt verwendbar

Prozessdiagramm mit fünf sequenziellen Schritten zur sicheren Aktivierung von Microsoft Copilot in Unternehmen: von der Permission-Analyse über Datenschutzmaßnahmen bis zur finalen Rollenverteilung.

Was Copilot dann wirklich leistet

Wenn diese Basis stimmt, sind die Effizienzgewinne real. Microsoft Research dokumentiert durchschnittlich 7 Minuten Zeitersparnis pro akzeptiertem Output. Die tatsächliche Netto-Ersparnis hängt stark von der Acceptance Rate ab — liegt sie bei 20 bis 30 Prozent, was in der Praxis häufig vorkommt, reduziert sich der Gewinn auf 1,5 bis 2 Minuten pro Prompt.

Das klingt wenig. Skaliert auf eine Wissensarbeiterin mit 30 Copilot-Interaktionen täglich ergibt sich trotzdem eine substantielle Entlastung — wenn die Qualität der Eingaben stimmt und die Ergebnisse kritisch geprüft werden.

Der höchste ROI entsteht nicht durch schnellere E-Mails. Er entsteht, wenn ganze Prozesse neu gedacht werden: automatisierte Rechnungsverarbeitung, KI-gestütztes Onboarding, strukturierte Vertragsanalyse. Das erfordert Vorbereitung — und oft eine Begleitung, die über die Microsoft-Dokumentation hinausgeht.

Was das für Ihr Unternehmen bedeutet

Copilot ist ein mächtiges Werkzeug. Aber es ist kein Werkzeug, das man einfach auspackt und loslaufen lässt.

Die zwei Risiken in diesem Artikel — Permission Debt und unkontrollierte Datenweitergabe — sind keine Randthemen für Konzerne. Sie treffen KMU im DACH-Raum unmittelbar, weil dort die IT-Governance-Strukturen oft gewachsen und selten dokumentiert sind.

Das Strukturaflow-Team begleitet KMU bei genau dieser Vorbereitung: Berechtigungsanalyse, DSGVO-konforme Konfiguration, und die Frage, ob Copilot überhaupt das richtige Werkzeug für Ihre Prozesse ist — oder ob eine andere KI-Architektur mehr Sinn ergibt.

Lassen Sie Ihr KI-Potenzial analysieren — kostenlos und unverbindlich.

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

<https://wissen.strukturaflow.it.com>