// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

KI-Agenten Berechtigungen einschränken: KMU-Leitfaden

Least-Privilege für KI-Agenten: Berechtigungen in Copilot, Make und Zapier richtig einschränken — mit Berechtigungsmatrix und DSGVO-Bezug für KMU.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
19. Mai 2026

ONLINE LESEN
https://wissen.strukturaflow.it.com/ki-agenten-berechtigungen-einschraenken-kmu/

KI-Agenten Berechtigungen einschränken: Der KMU-Leitfaden für sichere Automatisierung

Ein Automatisierungs-Agent in einem Steuerberatungsbüro bekommt bei der Einrichtung Lesezugriff auf das gesamte E-Mail-Postfach — weil jemand auf „Alles erlauben" geklickt hat, ohne die Konsequenzen zu überdenken. Wenige Wochen später enthält das Automatisierungsprotokoll vertrauliche Mandantenkommunikation, auf die der Agent nie hätte zugreifen sollen. Kein Angriff von außen, kein bösartiger Akteur — nur eine zu weit gefasste Berechtigung.

KI-Agenten sind kein Sicherheitsrisiko per se. Zu weit gefasste Berechtigungen sind es. Und das ist ein besonderes KMU-Problem: Wer keine IT-Abteilung hat, die Fehlkonfigurationen erkennt und korrigiert, sitzt auf einem stillen Risiko.

Dieser Leitfaden zeigt, wie Sie Berechtigungen nach dem Least-Privilege-Prinzip einrichten — ohne IT-Studium, mit konkreten Schritten für die Tools, die KMU tatsächlich verwenden.

Was KI-Agenten überhaupt „dürfen" – ein Überblick für Nicht-Techniker

Ein KI-Agent ist Software, die selbstständig Aufgaben ausführt. Er liest E-Mails, verschiebt Dateien, erstellt Entwürfe, bucht Kalendertermine oder überträgt Daten zwischen Systemen — ohne dass jemand jedes Mal auf einen Knopf drückt. Der entscheidende Unterschied zu klassischen Tools: Ein Agent handelt, er schaut nicht nur.

Damit ein Agent handeln kann, braucht er Berechtigungen. Diese lassen sich in vier Grundtypen unterteilen:

- **Lesen:** Der Agent kann Daten einsehen — E-Mails, Dokumente, Kalendereinträge. Er verändert nichts.
- **Schreiben:** Der Agent kann Inhalte erstellen oder ändern — z. B. einen Angebotsentwurf in ein Dokument schreiben.
- **Ausführen:** Der Agent kann Prozesse starten — z. B. eine Automatisierung auslösen oder eine API aufrufen.
- **Weiterleiten:** Der Agent kann Daten an andere Systeme oder Personen schicken — z. B. eine E-Mail versenden oder Daten in ein externes CRM übertragen.

Wie Sie den Datenzugriff von KI-Agenten grundsätzlich modellieren, zeigen wir im verwandten Artikel KI-Agenten Datenzugriff kontrollieren: KMU-Guide.

Warum Berechtigungen bei KI-Agenten kritischer sind als bei normalen Apps

Klassische Software wartet auf Ihre Eingabe. Ein KI-Agent agiert autonom — und skaliert Fehler in einem Tempo, das kein Mensch manuell erreichen würde. Ein falsch konfigurierter Zapier-Zap kann in einer Stunde hunderte Aktionen ausführen, die Sie einzeln nie genehmigt hätten.

Das konkrete Risiko: Ein Agent, der Rechnungen versendet, sollte nicht gleichzeitig Zahlungen auslösen können. Diese Trennung ist keine technische Spitzfindigkeit, sondern ein Grundprinzip sicherer Automatisierung.

Das Least-Privilege-Prinzip – was steckt dahinter?

Jeder Agent bekommt nur die Rechte, die er für seine konkrete Aufgabe braucht — nicht mehr. Das ist Least Privilege, auf einen Satz gebracht.

Für KMU ist dieses Prinzip besonders relevant: Kein Sicherheitsteam fängt Fehlkonfigurationen auf. Was zu weit geht, bleibt zu weit — solange es niemand überprüft. Eine einfache Merkhilfe für den Arbeitsalltag: „Putzkraft braucht den Kellerschlüssel nicht."

Kurze Abgrenzung zu Zero-Trust, weil der Begriff manchmal fällt: Zero-Trust geht weiter und setzt grundsätzlich kein Vertrauen in Netzwerk-Ebenen voraus. Least Privilege ist ein Teilaspekt davon — und der für KMU ohne eigene Infrastruktur relevantere Einstieg. Zero-Trust ist ein eigenes Thema; hier bleibt der Fokus auf dem, was heute umsetzbar ist.

Warum KI-Modelle selbst für ihre Entwickler zunehmend undurchsichtig werden — und was das für die Kontrolle bedeutet — erklärt dieser Artikel: Superposition: Warum KI-Modelle besser werden — und schwerer zu kontrollieren.

DSGVO-Pflichten bei KI-Agenten-Berechtigungen – was DE, AT und CH verlangt

Berechtigungsminimierung ist keine freiwillige Best Practice. Sie ist nach aktueller Rechtslage für Unternehmen, die personenbezogene Daten verarbeiten, rechtlich verankert.

Artikel 25 DSGVO — Privacy by Design und by Default: Systeme müssen so konfiguriert sein, dass standardmäßig nur die notwendigen Daten verarbeitet werden. Ein KI-Agent, der Zugriff auf mehr Daten hat als er für seine Aufgabe benötigt, verletzt diesen Grundsatz — unabhängig davon, ob er diesen Zugriff tatsächlich nutzt.

Artikel 32 DSGVO — Technische und organisatorische Maßnahmen: Unternehmen müssen geeignete Maßnahmen ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Berechtigungskonzepte für automatisierte Systeme gehören explizit dazu.

Besonderheit Österreich: Die österreichische Datenschutzbehörde hat in mehreren Bescheiden klargestellt, dass automatisierte Verarbeitungsprozesse nachvollziehbar dokumentiert und auf das Notwendige beschränkt sein müssen. Fehlende Dokumentation wird als eigenständiges Problem gewertet — nicht nur das Datenleck selbst.

Besonderheit Schweiz: Das neue Datenschutzgesetz (nDSG), seit September 2023 in Kraft, übernimmt die Privacy-by-Design-Logik der DSGVO und verlangt ebenfalls, dass Bearbeitungssysteme so ausgestaltet werden, dass nur erforderliche Daten verarbeitet werden. Für Schweizer KMU gilt damit sinngemäß dasselbe.

Die praktische Konsequenz: Wer im Audit nicht nachweisen kann, welche Berechtigungen seine KI-Agenten haben — und warum — hat ein Compliance-Problem. Nicht „könnte haben". Hat.

Was droht bei Verstößen – realistische Einschätzung für KMU

Keine Panikmache, aber eine ehrliche Einordnung: Bußgelder für KMU sind nach DSGVO verhältnismäßig zum Umsatz — das bedeutet, kleinere Beträge als bei Konzernen, aber keine Null. Schwerer wiegt für die meisten KMU der Reputationsschaden. Ein Steuerberatungsbüro oder eine Arztpraxis, die in einem Datenschutzvorfall auftaucht, verliert Mandanten. Das lässt sich schwer mit einem Versicherungsanspruch kompensieren.

Typische Fehler – und was dabei konkret schiefgeht

Szenario 1 – Handwerksbetrieb

Ein Zapier-Agent soll automatisch Angebote auf Basis von Kundenanfragen erstellen. Bei der Verbindung zu Google Drive wurde der gesamte Drive freigegeben — weil das die einfachste Option war. Ergebnis: Im Zapier-Protokoll tauchen Dateinamen und Inhalte aus Ordnern auf, die für den Prozess irrelevant sind — inklusive Personalunterlagen. Lernpunkt: Scope der Google Drive-Verbindung auf den spezifischen Angebots-Ordner begrenzen.

Szenario 2 – Einzelhandel

Ein Microsoft Copilot-Agent wertet Lagerbestände aus und gibt Empfehlungen für Nachbestellungen. Da der Account des Agenten auch Schreibrechte im ERP-System hat, löst ein fehlerhafter Prompt eine tatsächliche Bestellung aus — bei einem Lieferanten, zu einem Preis, den niemand freigegeben hat. Lernpunkt: Auswertungs-Agenten erhalten ausschließlich Lesezugriff. Bestellvorgänge erfordern immer einen menschlichen Schritt.

Szenario 3 – Steuerberatung

Ein Make-Szenario verarbeitet Mandantendaten für automatische Fristenerinnerungen. Das Szenario läuft unter dem persönlichen Account des Inhabers — keine Trennung von privaten und geschäftlichen Verbindungen, kein nachvollziehbares Audit-Log, keine klare Zuordnung bei einem Ausscheiden. Lernpunkt: Automatisierungen laufen immer unter dedizierten Accounts mit klar definiertem Zweck.

Was passiert, wenn Daten durch KI-Tools abfließen — und wie KMU gegensteuern, lesen Sie in KI-Tools und Datenverlust: So schützen sich KMU.

Woran Sie erkennen, dass Ihre Agenten zu viel dürfen

Fünf Warnsignale, auf die Sie sofort reagieren sollten:

1. Der Agent läuft unter einem Admin-Account oder unter dem persönlichen Account der Inhaberin.
2. Sie haben keine Möglichkeit, das Aktivitätsprotokoll des Agenten einzusehen.
3. Die Berechtigungen wurden seit der Ersteinrichtung nie überprüft.
4. Der Agent hat Zugriff auf Ordner, Postfächer oder Systeme, die für seine Aufgabe nicht benötigt werden.
5. Sie können nicht benennen, welche Daten der Agent verarbeitet — und an welche Dienste er diese weitergibt.

Schritt-für-Schritt: Berechtigungen einschränken in den drei häufigsten KMU-Tools

Microsoft 365 Copilot

Berechtigungen für Copilot werden im **Microsoft 365 Admin Center** und in **Microsoft Entra ID** (früher Azure Active Directory) verwaltet.

Konkrete Schritte:

1. Legen Sie für Copilot-gestützte Automatisierungen einen eigenen Service-Account an — keinen regulären Benutzeraccount, schon gar keinen Admin-Account.
2. Schränken Sie SharePoint-Freigaben gezielt ein: Copilot kann nur auf Bibliotheken und Ordner zugreifen, die explizit freigegeben wurden. Prüfen Sie im SharePoint Admin Center, welche Bereiche aktuell zugänglich sind.
3. Nutzen Sie **Sensitivity Labels** (Vertraulichkeitsbezeichnungen) für Dokumente mit sensiblen Daten. Dokumente mit dem Label „Vertraulich" oder „Streng vertraulich" können Sie so konfigurieren, dass Copilot sie nicht indiziert.
4. Im Admin Center unter „Copilot"-Richtlinien lässt sich steuern, welche Nutzergruppen Copilot-Funktionen überhaupt nutzen dürfen — nutzen Sie das für eine schrittweise Einführung.

Eine hilfreiche Grundlage bietet auch die Copilot-Checkliste, die Microsoft nicht mitliefert.

Make (ehemals Integromat)

Eigene Verbindungen je Agent anlegen: Verwenden Sie für jedes Make-Szenario eine eigene „Connection" — nie den Hauptaccount des Unternehmens oder die persönlichen Zugangsdaten der Inhaberin. So lässt sich jede Verbindung bei Bedarf isoliert deaktivieren, ohne andere Prozesse zu stören.

Teams und Rollen in Make: Make erlaubt es, Teammitglieder mit unterschiedlichen Rechten zu versehen. Unterscheiden Sie zwischen Personen, die Szenarien erstellen und bearbeiten dürfen, und solchen, die sie nur ausführen können.

Protokollierung minimieren: Unter den Szenario-Einstellungen lässt sich die Protokollierungstiefe steuern. Sensible Daten — Kundennamen, Auftragsnummern, E-Mail-Inhalte — sollten nicht im vollständigen Ausführungsprotokoll landen. Aktivieren Sie „Execution history: errors only" für Szenarien, die personenbezogene Daten verarbeiten.

Zapier

Zapier **Teams und Abteilungsstruktur:** Zapier-Workspaces lassen sich in Teams aufteilen. Trennen Sie Zaps nach Abteilungen oder Prozessbereichen — so hat die Buchhaltungs-Automatisierung keinen Bezug zur Kundenkommunikations-Automatisierung.

Scoped OAuth-Verbindungen: Wenn Sie eine App-Verbindung in Zapier einrichten, fragt OAuth in der Regel nach einer Reihe von Berechtigungen. Wählen Sie bei jeder neuen Verbindung bewusst aus, welche Scopes Sie tatsächlich benötigen. Bei Google-Diensten etwa: Nur der Zugriff auf spezifische Google Sheets-Tabellen statt auf den gesamten Drive.

Zapier stellt eigene Compliance-Dokumentation bereit, die Auskunft über Datenspeicherung und Sicherheitszertifizierungen gibt — relevant für die DSGVO-Dokumentation.

Hinweis für andere Tools: Wer mit n8n oder Power Automate arbeitet, findet dasselbe Grundprinzip — die Benutzeroberfläche variiert, die Logik nicht. Einen direkten Vergleich zwischen n8n und Zapier bietet dieser Artikel: n8n vs. Zapier 2026: Welches Tool passt zu Ihrem KMU?

Berechtigungsmatrix-Vorlage – direkt einsatzbereit für Ihr KMU

Eine Berechtigungsmatrix ist eine strukturierte Übersicht aller aktiven KI-Agenten und Automatisierungen — mit den Rechten, die sie haben, der Person, die dafür verantwortlich ist, und dem Datum der letzten Überprüfung. Sie ist kein IT-Dokument, sondern ein Managementwerkzeug.

Der Nutzen ist doppelt: Sie behalten den Überblick, und Sie können im Audit oder bei einem Datenschutzvorfall nachweisen, dass Sie sich aktiv um Berechtigungen gekümmert haben.

Agent-Name	Aufgabe	Benötigte Berechtigungen	Platt-form	Verant-wortliche Person	Letztes Re-view
Copilot-Auswer-tungsagent	Umsatzberichte aus SharePoint zusammenfas-sen	Lesen (SharePoint: /Be-richte/Umsatz)	Microsoft 365 Co-pilot	Maria Hu-ber (GF)	2025-03-01
Zapier-Rechnungs-agent	Rechnungen aus Lexware nach SharePoint ex-portieren	Lesen (Lexware), Schreiben (Share-Point: /Buchhaltung/ Ausgangsrechnungen)	Zapier	Thomas Kern (Buchhal-tung)	2025-02-15
Make-Kor-respon-denz-Agent	Kundenanfragen kategorisieren und in CRM ein-tragen	Lesen (E-Mail: Postfach anfragen@), Schreiben (CRM: Kontakte)	Make	Maria Hu-ber (GF)	2025-01-20

Diese Vorlage können Sie direkt in Excel übertragen und um Ihre eigenen Agenten ergänzen. Das Formular zum Download der vollständigen Excel-Version steht im Beratungsgespräch zur Verfügung — gemeinsam mit einem Review der Einträge.

Wie oft sollten Sie Berechtigungen reviewen?

Empfehlung: **quartalsweise**, plus unmittelbar nach jeder größeren Änderung an einem Tool — neues Feature-Update, neue Integration, Mitarbeiterwechsel.

Wer macht das Review, wenn keine IT-Abteilung vorhanden ist? Benennen Sie eine verantwortliche Person — auch wenn es die Inhaberin selbst ist. Entscheidend ist nicht, ob ein IT-Experte prüft, sondern dass jemand mit der Matrix in der Hand die Fragen stellt: Braucht dieser Agent noch diese Rechte? Hat sich die Aufgabe verändert?

Rollenkonzept für KMU – wer darf was konfigurieren?

Auch ein Betrieb mit zehn Mitarbeitenden profitiert von einem klaren Rollenkonzept — nicht aus bürokratischen Gründen, sondern weil es im Ernstfall (Vorfall, Mitarbeiteraustritt, Audit) sofort klare Verantwortlichkeiten gibt.

Drei Rollen reichen für den Anfang:

- **KI-Admin:** Richtet Agenten ein, vergibt Berechtigungen, pflegt die Berechtigungsmatrix.
- **KI-Nutzer:** Verwendet Agenten im Tagesgeschäft, kann keine Berechtigungen ändern.
- **KI-Reviewer:** Prüft in regelmäßigen Abständen die Protokolle und die Berechtigungsmatrix — ob alles noch stimmt.

Diese Rollen müssen nicht an verschiedene Personen vergeben werden. In einem kleinen Betrieb kann die Inhaberin alle drei Rollen übernehmen. Wichtig ist nur: Sie sind dokumentiert. Und die Dokumentation landet im DSGVO-Verarbeitungsverzeichnis — KI-Agenten-Berechtigungen gehören dort als technische und organisatorische Maßnahme explizit hinein.

Praxis-Tipp: So starten Sie diese Woche (ohne IT-Dienstleister)

Drei Sofortmaßnahmen, die Sie heute umsetzen können:

1. Alle aktiven KI-Agenten und Automatisierungen auflisten. Eine einfache Excel-Tabelle reicht. Fragen Sie sich: Welche Prozesse laufen bei uns automatisch, ohne dass jemand aktiv auf „Start“ drückt? Das ist Ihr Ausgangspunkt.

2. Prüfen: Läuft ein Agent unter persönlichem Account oder Admin-Account? Wenn ja: Das ist die dringendste Korrektur. Erstellen Sie einen dedizierten Account für die Automatisierung — oder zumindest eine separate Verbindung mit eingeschränktem Scope.

3. Berechtigungen eines Agenten exemplarisch nachschauen. Nehmen Sie einen einzigen Agenten, öffnen Sie dessen Verbindungseinstellungen, und dokumentieren Sie, welche Rechte er tatsächlich hat — im Vergleich zu dem, was er für seine Aufgabe braucht. Das ist der erste Eintrag in Ihrer Berechtigungsmatrix.

Ehrliche Einschätzung: Diese drei Schritte lösen die einfachsten und häufigsten Probleme. Für komplexere Setups — mehrere Abteilungen, viele Agenten, sensible Branchen wie Gesundheit, Recht oder Steuerberatung — lohnt ein externer Blick. Nicht weil die Aufgabe unlösbar ist, sondern weil ein strukturiertes Review in zwei Stunden mehr bringt als ein Jahr sporadischer Eigenversuche.

FAQ

Muss ich für jeden KI-Agenten einen eigenen Benutzeraccount anlegen?

Nicht zwingend einen eigenen User-Account im Sinne einer E-Mail-Adresse mit Lizenz. Aber eine eigene „Verbindung" mit minimalen Scopes — ja. In Make, Zapier und den meisten anderen Tools lassen sich Verbindungen anlegen, die unabhängig vom persönlichen Login sind. Das ist der entscheidende Schritt: Trennung der Identitäten, nicht unbedingt Trennung der Verträge.

Was passiert, wenn mein Agent zu viele Berechtigungen hatte — muss ich das der Datenschutzbehörde melden?

Das hängt davon ab, ob personenbezogene Daten tatsächlich betroffen waren und ob ein Risiko für die betroffenen Personen bestand. Wenn ein Agent Zugriff auf Kundendaten hatte, diesen aber nicht genutzt hat und keine Daten nach außen geflossen sind, ist die Meldepflicht nach aktueller Rechtslage weniger eindeutig als bei einem klassischen Datenleck. Im Zweifel: Datenschutzbeauftragten konsultieren, nicht selbst entscheiden.

Gilt das Least-Privilege-Prinzip auch für Cloud-KI wie ChatGPT oder Claude?

Ja, aber der Ansatzpunkt ist ein anderer: Bei ChatGPT oder Claude geht es nicht um Systemberechtigungen, sondern darum, welche Daten Sie in den Prompt einspeisen. Unternehmensdaten — Kundenlisten, Verträge, Finanzdaten — dürfen nur dann in ein Cloud-KI-System eingebracht werden, wenn eine geprüfte Datenschutzvereinbarung (Data Processing Agreement, DPA) mit dem Anbieter besteht. Was DSGVO-konform möglich ist, erklärt dieser Artikel: DSGVO & ChatGPT im Unternehmen: Was gilt 2025?

Wie aufwendig ist ein Berechtigungsreview wirklich für einen 10-Personen-Betrieb?

Für ein Setup mit drei bis fünf Agenten: zwei bis vier Stunden für das erste strukturierte Review, danach 30 bis 60 Minuten pro Quartal. Der Aufwand ist überschaubar — der Unterschied liegt darin, es einmal systematisch anzugehen statt ad hoc zu reagieren.

Nächste Schritte – Ihr Fahrplan zur sicheren KI-Agentennutzung

Der praktische Einstieg lässt sich in fünf Schritte zusammenfassen:

1. **Inventar erstellen:** Alle aktiven Agenten und Automatisierungen auflisten.
2. **Berechtigungsmatrix anlegen:** Für jeden Agenten dokumentieren, welche Rechte er hat — und welche er braucht.
3. **Rollenkonzept definieren:** Wer konfiguriert, wer nutzt, wer prüft?
4. **DSGVO-Dokumentation ergänzen:** Agenten-Berechtigungen ins Verarbeitungsverzeichnis aufnehmen.
5. **Review-Rhythmus festlegen:** Quartalsweise + nach Tool-Änderungen.

KI-Sicherheit ist kein Projekt mit Enddatum. Wer einmal ein funktionierendes System aus Berechtigungsmatrix, Rollenkonzept und Review-Rhythmus eingerichtet hat, hat 80 % der laufenden Arbeit bereits erledigt — der Rest ist konsequentes Dranbleiben.

Wenn Sie nicht sicher sind, wo Sie bei Ihrem konkreten Setup ansetzen sollen — ob Copilot, Make, Zapier oder eine Kombination davon —, dann ist das genau der Ausgangspunkt für ein strukturiertes Beratungsgespräch. Das kostenlose 30-Minuten-Gespräch von Strukturaflow ist darauf ausgerichtet, Ihnen nicht eine Standardempfehlung zu geben, sondern Ihr spezifisches Setup zu analysieren: Welche Agenten laufen, welche Berechtigungen sie haben, und wo die dringendsten Anpassungen liegen. Kein IT-Vorwissen erforderlich — nur die Liste Ihrer aktiven Tools.

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