// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

KI-Workflows mit Unternehmensdaten absichern

KI-Workflows sicher mit Unternehmensdaten betreiben: Architektur, DSGVO, AVV und organisatorische Maßnahmen — konkret für DACH-KMU.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
2. Mai 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/ki-workflows-unternehmensdaten-absichern/

KI-Tools sparen Zeit — aber sobald echte Unternehmensdaten ins Spiel kommen, steigen die Risiken messbar. Kundenlisten, Verträge, interne Berichte: Was in ein Sprachmodell fließt, verlässt unter Umständen das Unternehmen, landet auf Servern im Drittland oder fließt in das Training eines externen Modells ein.

„Wir schicken keine Daten an ChatGPT" ist keine vollständige Sicherheitsstrategie. Viele KMU übertragen bereits ohne klare Absicht sensible Daten in externe Systeme — über Browser-Erweiterungen, Automatisierungstools wie Zapier oder direkte Copy-paste-Workflows in Konsumenten-Produkte. Das passiert selten böswillig, aber regelmäßig.

Dieser Artikel zeigt Ihnen einen strukturierten Handlungsrahmen: vier Absicherungsebenen, konkrete Architekturoptionen und eine Checkliste für den sofortigen Einsatz — ohne IT-Studium, ohne teure Berater als Voraussetzung.

Was bedeutet „KI-Workflow mit Unternehmensdaten" überhaupt?

Ein KI-Workflow ist jede automatisierte oder halbautomatische Verarbeitung, bei der ein Sprachmodell oder ein KI-System Unternehmensdaten entgegennimmt und darauf basierend eine Ausgabe erzeugt. Das kann ein Chatbot sein, der interne Dokumente beantwortet, eine Automatisierung, die eingehende E-Mails klassifiziert, oder ein Tool, das Verträge zusammenfasst.

Der entscheidende Unterschied liegt in der technischen Architektur:

- **Öffentliche KI-Dienste direkt im Browser** (z. B. chat.openai.com, Gemini ohne Unternehmenskonto): kein Vertrag, keine Kontrolle, ggf. Training auf Eingaben
- **API-Integration** (z. B. OpenAI API, Azure OpenAI, Google Vertex AI): datenschutzrechtlicher Vertrag möglich, konfigurierbar
- **Lokal betriebene Modelle** (z. B. Ollama, LM Studio): Daten verlassen das Unternehmen nicht

Typische Datenkategorien, die in solche Workflows fließen:

- Personenbezogene Kundendaten (Name, Kontakt, Kaufhistorie)
- Geschäftsgeheimnisse (Kalkulationen, Strategiepapiere)
- Finanzdaten (Rechnungen, Buchhaltungsexporte)
- Gesundheitsdaten (relevant für Arztpraxen, Sozialeinrichtungen, Betriebsmedizin)

Wichtig: Viele KMU merken erst im Nachhinein, dass ihre Automatisierungstools — Zapier-Workflows, Notion-KI, CRM-Integrationen — Daten automatisch in Dienste außerhalb der EU übertragen. Das ist kein Designfehler dieser Tools, sondern ein Konfigurationsthema. Und ein Dokumentationsthema.

Die vier Absicherungsebenen im Überblick

Eine isolierte Maßnahme reicht nicht. Wer nur technisch absichert, aber keine internen Regeln hat, verlässt sich darauf, dass Mitarbeitende immer richtig handeln. Wer nur einen AVV abschließt, aber das Modell auf unsicherer Architektur betreibt, hat das Papier, aber nicht den Schutz.

Die vier Ebenen müssen zusammenspielen:

EBENE	THEMA	BEISPIELMASSNAHME
1 – Architektur	Wo läuft das Modell?	Azure OpenAI statt openai.com
2 – Datenzugang	Welche Daten sieht das Modell?	Anonymisierung vor dem KI-Aufruf
3 – Vertrag & Compliance	Ist die Verarbeitung rechtlich gedeckt?	AVV, DSGVO-Eintrag, EU AI Act
4 – Organisation	Wer darf was, und was passiert bei Fehlern?	Nutzungsrichtlinie, Schulung, Incident-Response

Vier aufeinanderfolgende Sicherheitsebenen für KI-Workflows mit Unternehmensdaten: Architektur (Cloud/Hybrid/On-Premise), Datenzugang (Minimale Weitergabe), Verträge & Compliance (rechtliche Absicherung), Organisation (Regeln und Bewusstsein).

Ebene 1 - Architektur: Cloud, Hybrid oder On-Premise?

Die Architekturfrage ist keine reine IT-Entscheidung — sie bestimmt, welche Datenschutzmaßnahmen überhaupt möglich sind.

Cloud-basierte KI-Dienste (z. B. Azure OpenAI, Google Vertex AI)

Cloud-KI ist schnell eingerichtet, kosteneffizient und erfordert keine eigene Infrastruktur. Für viele KMU ist das der pragmatische Einstieg.

Die Risiken: Daten werden an externe Server übertragen, oft in Drittländer außerhalb der EU. Ob und wie lange Daten gespeichert werden, hängt vom Anbieter und der gewählten Konfiguration ab. Ohne AVV ist die Cloud-Nutzung mit personenbezogenen Daten grundsätzlich rechtlich nicht haltbar.

Wann sinnvoll: Wenn die verarbeiteten Daten nicht als hochsensibel klassifiziert sind, ein belastbarer AVV mit dem Anbieter vorliegt und die Datenresidenz nachweisbar in der EU liegt.

Konkrete Maßnahme: Azure OpenAI statt openai.com. Der Unterschied ist nicht trivial: openai.com ist ein Konsumenten-Produkt ohne standardmäßigen Unternehmensvertrag. Azure OpenAI bietet EU-Datenresidenz (Rechenzentren in Deutschland und den Niederlanden stehen zur Verfügung), einen AVV nach Artikel 28 DSGVO und die Zusicherung, dass Eingabedaten standardmäßig nicht für das Training des Modells genutzt werden. Google Vertex AI und Anthropic Claude via AWS Bedrock bieten vergleichbare Unternehmensoptionen mit entsprechenden Vertragsgrundlagen.

On-Premise / Lokale Modelle (z. B. Ollama, LM Studio)

Bei lokal betriebenen Modellen verlassen die Daten das Unternehmen nicht. Das ist der maximale Datenschutz — aber er hat einen Preis.

Nachteile: Leistungsfähige Open-Source-Modelle brauchen leistungsstarke Hardware (GPU-Server, typischerweise ab ca. 5.000–15.000 € für ein funktionsfähiges Setup). Der Wartungsaufwand liegt intern, Updates müssen manuell eingespielt werden, und die Modellqualität liegt bei vielen Aufgaben noch unter den führenden Cloud-Modellen.

Wann sinnvoll: Gesundheitswesen, Steuer- und Rechtsberatung, öffentliche Verwaltung, Finanzdienstleistungen — überall wo besondere Kategorien personenbezogener Daten nach Artikel 9 DSGVO verarbeitet werden oder wo branchenspezifische Verschwiegenheitspflichten gelten.

Praxisbeispiel: Ein kleines Steuerberatungsbüro in Graz nutzt Ollama auf einem lokalen Server mit einem Llama-basierten Modell, um eingescannte Belege zusammenzufassen und Buchungstexte vorzuschlagen. Die Daten verlassen das Büro nie. Das Modell ist langsamer als GPT-4, aber für diesen Anwendungsfall ausreichend — und rechtlich unproblematisch.

RAG-Architekturen als Mittelweg

RAG steht für „Retrieval-Augmented Generation". Das Prinzip: Das Sprachmodell selbst enthält kein Unternehmenswissen. Stattdessen werden Dokumente lokal indexiert und gespeichert. Wenn eine Frage gestellt wird, sucht ein Retrieval-System die relevanten Textabschnitte und übergibt nur diese kurzen Ausschnitte an das Modell — als Kontext für die Antwort.

Das Modell „lernt" dabei nichts. Es speichert nichts dauerhaft. Es sieht immer nur den Ausschnitt, der für die aktuelle Anfrage relevant ist.

Beispiel-Setup: Interne Richtlinien und Handbücher werden lokal in einer Vektordatenbank gespeichert. Ein Mitarbeiter fragt „Wie ist unsere Urlaubsregelung bei Teilzeit?". Das System findet den relevanten Absatz im Handbuch und gibt diesen — plus die Frage — an das Cloud-Modell weiter. Das Modell formuliert eine klare Antwort. Personenbezogene Daten fließen dabei nicht ins Modell.

Ehrliche Einschätzung: RAG ist kein Allheilmittel. Auch hier muss definiert sein, welche Dokumente in die Vektordatenbank geladen werden und welche Textausschnitte das Modell maximal zu sehen bekommt. Wenn das Retrieval-System unkontrolliert auf alle Unternehmensdaten zugreift, ist der Datenschutzgewinn begrenzt.

Ebene 2 - Datenzugang: Das Prinzip der minimalen Datenweitergabe

Das „Least Privilege"-Prinzip aus der klassischen IT-Sicherheit gilt auch für KI-Workflows: Das Modell bekommt nur die Daten zu sehen, die es für die jeweilige Aufgabe tatsächlich braucht.

In der Praxis bedeutet das: Bevor ein Workflow gebaut wird, wird schriftlich festgelegt, welche Datenfelder das Modell sehen darf — und welche nicht.

Datenklassifizierung als Grundlage:

- **Öffentlich:** Marketingtexte, veröffentlichte Preislisten
- **Intern:** Prozessbeschreibungen, allgemeine Leitfäden
- **Vertraulich:** Kundendaten, Verträge, Finanzdaten
- **Streng vertraulich:** Gesundheitsdaten, besondere Kategorien nach Art. 9 DSGVO, Geschäftsgeheimnisse mit hohem Schadenpotenzial

KI-Workflows sollten grundsätzlich nur mit öffentlichen und internen Daten ohne Weiteres operieren. Für vertrauliche Daten braucht es technische und organisatorische Absicherung. Streng vertrauliche Daten sollten nur in vollständig kontrollierten Architekturen verarbeitet werden.

Technische Maßnahmen:

- Anonymisierung oder Pseudonymisierung vor dem KI-Aufruf: Klarnamen, Kundennummern, E-Mail-Adressen werden durch Platzhalter ersetzt, bevor die Daten an das Modell gehen
- Keine vollständigen Datenbankexporte an Sprachmodelle — nur die Felder, die für die Aufgabe notwendig sind
- Logging: Welche Daten wurden wann an welches Modell übermittelt?

Praxisbeispiel: Ein österreichisches Beratungsunternehmen nutzt einen KI-Workflow, um Kundenanfragen zu kategorisieren. Vor dem API-Aufruf werden Name und E-Mail-Adresse durch die interne Kundennummer ersetzt. Das Modell sieht nur den Anfragetext — ausreichend für die Kategorisierung, ohne personenbezogene Daten preiszugeben.

Leitfrage vor jedem Workflow-Aufbau: „Welche Daten braucht der KI-Workflow wirklich — und welche kommen nur versehentlich mit?"

Ebene 3 - Verträge & Compliance: Was rechtlich abgesichert sein muss

Auftragsverarbeitungsvertrag (AVV)

Wer personenbezogene Daten an einen externen Dienstleister — auch einen KI-Anbieter — übermittelt, braucht nach Art. 28 DSGVO einen AVV. Dieser muss festlegen, welche Daten zu welchem Zweck verarbeitet werden, welche Sicherheitsmaßnahmen der Anbieter garantiert und dass Daten nicht für eigene Zwecke des Anbieters genutzt werden.

Die wichtigsten Anbieter stellen AVVs bereit: - Microsoft (Azure OpenAI): über das Microsoft Admin Center abrufbar - Google (Vertex AI): über die Google Cloud Console - OpenAI API: Data Processing Addendum auf openai.com

Wichtig: Wer chat.openai.com direkt im Browser nutzt, schließt keinen Unternehmensvertrag ab — das ist ein Konsumentendienst. Für den DSGVO-konformen Einsatz mit Unternehmensdaten ist die API-Route oder eine Unternehmenslizenz (ChatGPT Enterprise) mit entsprechendem Vertrag notwendig. Eine ausführlichere Darstellung der Rechtsgrundlagen und der Vertragsdokumentation finden Sie im Artikel KI DSGVO-konform einsetzen: Leitfaden für KMU.

EU AI Act

Der EU AI Act ist seit August 2024 in Kraft und wird stufenweise anwendbar. Für die meisten KMU-Workflows — Textzusammenfassung, interne FAQ-Bots, Dokumentenklassifizierung — fällt die Einstufung in die Kategorie „minimales Risiko“. Das bedeutet: keine besonderen gesetzlichen Pflichten, aber empfohlene Transparenz gegenüber Nutzenden.

Hochrisiko-Einstufungen (Anhang III des EU AI Acts) betreffen unter anderem: KI-Systeme in der Personalentscheidung, in der Kreditvergabe, im Bereich kritischer Infrastruktur oder im Gesundheitswesen. Wenn Ihr KI-Workflow in einem dieser Bereiche operiert, gelten ab 2026 erweiterte Anforderungen (Dokumentation, Risikobewertung, menschliche Aufsicht). Eine aktuelle Einschätzung dazu bietet der Artikel EU AI Act: Was müssen KMU jetzt wirklich tun?.

NIS2 / NISG 2026

Wenn KI in unternehmenskritischen Prozessen eingesetzt wird — etwa in der Auftragssteuerung, Finanzbuchhaltung oder im Kundensupport mit Systemzugang — können je nach Unternehmensgröße und Sektor erhöhte Anforderungen aus dem NISG 2026 relevant werden. Auch Unternehmen, die nicht direkt unter das Gesetz fallen, sind oft über Lieferketten betroffen. Was das konkret bedeutet, erläutert der Artikel NIS2 und was das für Ihren KI-Einsatz bedeuten kann.

Verzeichnis der Verarbeitungstätigkeiten

KI-Workflows mit personenbezogenen Daten gehören ins Verzeichnis der Verarbeitungstätigkeiten (VVT) nach Art. 30 DSGVO. Einzutragen sind: Zweck der Verarbeitung, Datenkategorien, Empfänger (also der KI-Anbieter), Speicherort und -dauer sowie die Rechtsgrundlage.

Ehrliche Einschätzung: Für die meisten KMU-Anwendungen — Textzusammenfassung interner Dokumente, einfache Chatbots — ist der Compliance-Aufwand überschaubar, wenn die Architektur stimmt. Ein AVV, ein Eintrag im VVT, eine klare Rechtsgrundlage: das ist in der Mehrzahl der Fälle das Wesentliche.

Ebene 4 - Organisation: Regeln, Rollen und Bewusstsein

Technische Maßnahmen allein schützen nicht. Der größte Risikofaktor bleibt menschliches Fehlverhalten aus Unwissenheit — nicht aus Böswilligkeit.

Interne KI-Nutzungsrichtlinie

Eine KI-Nutzungsrichtlinie muss nicht umfangreich sein, aber sie muss existieren. Folgende Punkte sollten geregelt sein:

- Welche KI-Tools sind im Unternehmen genehmigt?
- Welche Datenkategorien dürfen in welche Tools eingegeben werden?
- Was ist explizit verboten (z. B. Kundendaten in chat.openai.com)?
- Wer genehmigt den Einsatz neuer KI-Tools?
- Wie werden KI-generierte Ausgaben geprüft, bevor sie weiterverwendet werden?

Rollenkonzept

Nicht jede Mitarbeiterin und jeder Mitarbeiter braucht Zugang zu allen KI-Workflows. Definieren Sie, wer welche Tools mit welchen Daten nutzen darf — und dokumentieren Sie das. Das schützt nicht nur vor Datenschutzverstößen, sondern auch vor versehentlichen Fehlern in automatisierten Prozessen.

Mitarbeitende schulen

Eine kurze Schulung — 30 bis 60 Minuten — reicht, um die wichtigsten Do's und Don'ts zu vermitteln:

- **Erlaubt:** Öffentlich verfügbare Informationen in genehmigte Tools eingeben, interne Prozessdokumentation über abgesicherte Unternehmenstools nutzen
- **Nicht erlaubt:** Kundendaten, Verträge, Passwörter oder Finanzdaten in nicht genehmigte externe Tools eingeben
- **Im Zweifelsfall:** Vorher fragen, nicht ausprobieren

Incident-Response

Was passiert, wenn doch versehentlich sensible Daten übermittelt wurden? Das sollte vor dem ersten Vorfall geregelt sein — nicht danach.

Mindest-Setup: Wer ist zu informieren (intern, ggf. Datenschutzbehörde bei meldepflichtigem Vorfall)? Was sind die ersten Sofortmaßnahmen (Zugang sperren, Anbieter kontaktieren, Protokoll sichern)? Wo wird der Vorfall dokumentiert?

Wer seinen Umgang mit IT-Sicherheitsvorfällen grundsätzlich verbessern möchte, findet im Artikel Schwachstellen frühzeitig erkennen weiterführenden Kontext zur allgemeinen IT-Sicherheitslage für KMU.

Praxis-Checkliste: KI-Workflow absichern in 10 Schritten

Die folgende Checkliste deckt alle vier Absicherungsebenen ab. Sie können sie direkt als Vorlage für Ihr nächstes KI-Projekt verwenden.

#	MASSNAHME	EBENE	AUFWAND
1	Architekturentscheidung treffen: Cloud-API, On-Premise oder RAG? Begründung dokumentieren.	Architektur	mittel
2	Anbieter identifizieren und prüfen, ob ein AVV verfügbar und abgeschlossen ist.	Compliance	gering
3	EU-Datenresidenz bestätigen lassen (Rechenzentrum in EU/EWR).	Architektur	gering
4	Daten klassifizieren: Welche Kategorien verarbeitet der Workflow?	Datenzugang	mittel
5	Minimal-Datenprinzip umsetzen: Nur notwendige Felder ans Modell übergeben, Anonymisierung prüfen.	Datenzugang	mittel–hoch
6	Eintrag im Verzeichnis der Verarbeitungstätigkeiten vornehmen.	Compliance	gering
7	EU AI Act Risikoklasse prüfen: Handelt es sich um einen Hochrisiko-Anwendungsfall?	Compliance	gering
8	Interne KI-Nutzungsrichtlinie erstellen oder bestehende Richtlinie erweitern.	Organisation	mittel
9	Mitarbeitende schulen: Welche Tools sind erlaubt, was ist verboten, was tun bei Fehlern?	Organisation	gering
10	Incident-Response-Prozess definieren: Wer informiert wen, was wird dokumentiert?	Organisation	gering

FAQ: Häufige Fragen zur Datensicherheit in KI-Workflows

Darf ich Kundendaten an ChatGPT oder andere KI-Tools schicken?

Grundsätzlich nur dann, wenn ein AVV mit dem Anbieter besteht, die Rechtsgrundlage nach DSGVO geklärt ist (z. B. berechtigtes Interesse oder Einwilligung) und der Anbieter vertraglich zusichert, dass die Daten nicht für Trainingszwecke genutzt werden. Bei chat.openai.com ohne API und ohne Unternehmensvertrag gilt das in der Regel nicht. Die API und Enterprise-Pläne bieten andere Bedingungen — aber auch dort muss der AVV aktiv abgeschlossen werden.

Was ist der Unterschied zwischen der ChatGPT-Website und der OpenAI API bzw. Azure OpenAI?

chat.openai.com ist ein Konsumenten-Produkt. Es gibt standardmäßig keinen Unternehmensvertrag, keinen AVV nach Art. 28 DSGVO, und Eingaben können je nach Einstellung für das Modell-Training genutzt werden. Die OpenAI API und Azure OpenAI sind Unternehmensdienste mit Datenschutzvereinbarungen. Azure OpenAI bietet zusätzlich EU-Datenresidenz und ist in vielen Fällen die datenschutzrechtlich klarere Wahl für DACH-KMU.

Muss ich für einen internen KI-Chatbot mit Unternehmensdaten eine Datenschutz-Folgenabschätzung (DSFA) durchführen?

Das hängt von der Datenkategorie und der Verarbeitungstiefe ab. Bei einem FAQ-Bot mit allgemeinen internen Richtlinien in der Regel nein. Wenn personenbezogene Daten in großem Umfang verarbeitet werden, wenn besondere Kategorien nach Art. 9 DSGVO betroffen sind (Gesundheit, Religion, politische Überzeugungen) oder wenn das System automatisierte Entscheidungen trifft, die Personen erheblich beeinflussen — dann ja, nach Art. 35 DSGVO.

Was kostet ein sicheres KI-Setup für ein KMU realistisch?

Die Bandbreite ist groß. Ein Cloud-Setup mit Azure OpenAI, AVV und organisatorischen Maßnahmen ist nahezu ohne zusätzliche Infrastrukturkosten realisierbar — die Hauptarbeit liegt in Konfiguration, Dokumentation und Schulung. Ein On-Premise-Setup mit leistungsfähiger GPU-Hardware und lokalem Modell liegt typischerweise bei 5.000–15.000 € für Hardware plus Setup-Aufwand. Der richtige Ansatz hängt vom Schutzbedarf der Daten ab, nicht vom Budget allein.

Was ist ein RAG-System und warum gilt es als datenschutzfreundlicher?

Bei RAG (Retrieval-Augmented Generation) werden eigene Dokumente in einer lokalen Datenbank gespeichert und indexiert. Wenn eine Anfrage kommt, sucht das System den relevanten Textausschnitt und gibt nur diesen — nicht das gesamte Dokument — an das Sprachmodell weiter. Das Modell speichert nichts dauerhaft und „lernt“ nicht aus den Dokumenten. Verglichen mit einem Ansatz, bei dem Dokumente direkt ins Modell hochgeladen werden, ist die Datenweitergabe deutlich gezielter und kontrollierbarer.

Nächste Schritte

Die Absicherung von KI-Workflows ist kein Einmalprojekt. Anforderungen ändern sich, neue Tools kommen dazu, Mitarbeitende wechseln. Aber der Start muss nicht komplex sein.

Viele KMU können mit zwei bis drei gezielten Maßnahmen bereits 80 % der relevanten Risiken adressieren: die richtige Architektur wählen, einen AVV abschließen, eine klare interne Nutzungsregel definieren. Das ist in den meisten Fällen binnen eines Tages umsetzbar — wenn klar ist, welche Maßnahmen für den eigenen Kontext tatsächlich prioritär sind.

Genau das ist der Ausgangspunkt für ein unverbindliches 30-Minuten-Gespräch mit dem Strukturaflow-Team. Keine Vorbereitung notwendig, kein Agenda-Zwang: Sie schildern Ihren aktuellen KI-Einsatz oder Ihr Vorhaben, wir geben Ihnen eine konkrete Einschätzung, welche Schritte aus der Checkliste für Ihre Situation am wichtigsten sind — und welche Sie sich sparen können.

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