// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

KI-Tools und Datenverlust: So schützen sich KMU

Wie KMU in Deutschland und Österreich Datenverlust durch KI-Tools verhindern — mit Risiko-Check, Schritt-für-Schritt-Plan und DSGVO-Checkliste.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
13. Mai 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/ki-tools-datenverlust-verhindern-kmu-deutschland/

Eine Mitarbeiterin im Vertrieb gibt die Adress- und Auftragsdaten eines Kunden in ChatGPT ein — sie möchte schnell ein Angebot formulieren. Das funktioniert. Was sie nicht weiß: Bei der kostenlosen Variante von ChatGPT können Eingaben standardmäßig für das Modell-Training genutzt werden. Kein Angriff, kein Hacking — aber ein reales Datenschutzproblem.

Dieser Guide richtet sich an Unternehmen mit 10 bis 49 Mitarbeitern ohne eigene IT-Abteilung. Keine Enterprise-Architekturen, keine abstrakten Compliance-Frameworks. Stattdessen: eine prüfbare To-do-Liste, eine ehrliche Risikobewertung gängiger Tools — und ein realistischer Schutzplan für Betriebe, die KI-Tools bereits nutzen oder bald einführen wollen.

Der Aufbau folgt einer klaren Logik: Was sind die konkreten Risiken? Welche Tools sind sicherer — und welche nicht? Was muss organisatorisch geregelt sein? Und was gilt speziell für Österreich?

Warum KI-Tools ein Datenverlust-Risiko darstellen – konkret erklärt

Zwei Begriffe werden im Alltag oft vermischt, meinen aber unterschiedliche Probleme: „Datenverlust“ bedeutet, dass Daten unwiederbringlich weg sind — etwa weil ein Cloud-Dienst sie löscht oder ein Gerät ausfällt. „Datenweitergabe“ bedeutet, dass Daten unkontrolliert an Dritte gelangen — zum Beispiel an KI-Anbieter, Subunternehmer oder fremde Serverzentren. Beide Szenarien können DSGVO-relevant sein, beide können Bußgelder auslösen.

In KMU sind besonders folgende Datentypen gefährdet: Kundenstammdaten, Angebote und Auftragsunterlagen, Verträge, interne Kommunikation und Personalakten. Genau diese Daten landen aber häufig in KI-Tools — weil sie im Arbeitsalltag am häufigsten gebraucht werden.

Die drei häufigsten Einfallstore

Consumer-KI ohne Datenschutzvereinbarung: Wer ChatGPT Free, den kostenlosen Bard-Nachfolger Gemini oder ähnliche Tools nutzt, hat in der Regel keinen Auftragsverarbeitungsvertrag (AVV) mit dem Anbieter. Für Unternehmen, die personenbezogene Daten verarbeiten, ist das nach DSGVO Art. 28 nicht ausreichend.

KI-Browser-Plugins mit unkontrolliertem Datenzugriff: Viele Browser-Extensions lesen den gesamten Seiteninhalt mit — inklusive geöffneter CRM-Tabs, Webmail oder Buchhaltungsoberflächen. Welche Daten dabei übertragen werden, ist für den Nutzer oft nicht nachvollziehbar.

Automatisierungstools mit KI-API-Anbindung: Zapier, Make und ähnliche Plattformen leiten Daten an externe KI-APIs weiter. Wer z. B. eingehende E-Mails automatisch zusammenfassen lässt, überträgt dabei möglicherweise Kundendaten an mehrere Dienste gleichzeitig — ohne dass das jemandem bewusst ist. Wie Sie solche Workflows gezielt absichern, erläutert der Artikel KI-Workflows mit Unternehmensdaten absichern.

Was die DSGVO konkret verlangt

Der Mindeststandard ist ein gültiger AVV mit jedem Dienstleister, der in Ihrem Auftrag personenbezogene Daten verarbeitet — das gilt auch für KI-Anbieter. Fehlt dieser Vertrag, liegt bereits bei der ersten Dateneingabe ein formaler Verstoß vor. Wie Sie AVV und Rechtsgrundlagen im Detail prüfen, erklärt unser Leitfaden zur DSGVO-konformen KI-Nutzung.

Was ein Datenverlust ein KMU wirklich kostet – eine ehrliche Rechnung

Laut BSI-Lagebericht 2023/2024 liegt der durchschnittliche Schaden eines Sicherheitsvorfalls für kleine und mittlere Unternehmen in Deutschland im fünfstelligen Bereich — bei schwerwiegenden Fällen deutlich darüber. Diese Zahl klingt abstrakt, bis man sie aufschlüsselt.

Direkte Kosten entstehen durch DSGVO-Bußgelder (theoretisch bis 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes, in der Praxis für KMU oft im Bereich von 5.000 bis 50.000 Euro — je nach Schwere und Kooperation), durch IT-Forensik und Wiederherstellung, durch Rechts- und Beratungskosten sowie durch Meldepflichten gegenüber Behörden.

Indirekte Kosten sind schwerer zu beziffern, aber oft gravierender: Vertrauensverlust bei Kunden, kurzfristige Arbeitsunterbrechungen, erhöhte Versicherungsprämien und im schlimmsten Fall Auftragsrückgang.

Was kostet ein sicheres KI-Setup dagegen? Ein AVV ist kostenlos — er muss nur abgeschlossen werden. Eine interne Nutzungsrichtlinie kostet einen halben Tag Arbeitszeit. Eine Mitarbeiterschulung von 60 Minuten kostet im Wesentlichen die Personalstunden dieses Meetings. Der ROI ist eindeutig: Prävention ist um ein Vielfaches günstiger als Reaktion.

> **Hinweis für Österreich:** Nach österreichischem DSG § 24 und DSGVO Art. 33 besteht bei einer Datenpanne eine Meldepflicht gegenüber der Datenschutzbehörde (DSB) in Wien — in der Regel binnen 72 Stunden nach Bekanntwerden des Vorfalls. Die Meldung erfolgt über das Online-Formular der DSB. Wird die Frist versäumt, kann das selbst bei geringem Schaden als erschwerender Umstand gewertet werden.

Risiko-Check: Welche KI-Tools Sie gerade nutzen – und wie sicher sie sind

Die folgende Kategorisierung hilft einzuschätzen, wo akuter Handlungsbedarf besteht. Sie ersetzt keine individuelle Prüfung, gibt aber eine erste Orientierung.

Rot — nicht für betriebliche Daten geeignet: ChatGPT Free (ohne Business-Account), kostenlose KI-Tools ohne AVV-Angebot, KI-Browser-Plugins ohne dokumentierte Datenschutzpraktiken. Diese Tools dürfen für öffentliche, nicht-personenbezogene Inhalte genutzt werden — mehr nicht.

Gelb — nutzbar, aber mit Konfigurationsaufwand: ChatGPT Team oder Enterprise (OpenAI bietet AVV an, Trainingsoption abschaltbar), Microsoft Copilot for Microsoft 365 (Datenhaltung in EU möglich, aber Konfiguration erforderlich), Google Workspace AI (abhängig von Workspace-Einstellungen und Vertragsmodell). Bei diesen Tools gilt: Ja, aber nur mit korrekter Einrichtung und abgeschlossenem AVV.

Grün — hohe Datenschutzkonformität möglich: Selbst gehostete Open-Source-Modelle wie Ollama mit Llama 3 (Daten verlassen das eigene System nicht), EU-gehostete Alternativen wie Mistral AI mit europäischem Hosting. Wichtig: „Grün" bedeutet nicht „kein Aufwand" — auch diese Lösungen brauchen Konfiguration, Zugriffsbeschränkungen und interne Richtlinien.

Besonders bei KI-Agenten mit eigenem Datenzugriff — etwa für automatisierte Recherche, CRM-Auswertung oder E-Mail-Bearbeitung — ist ein durchdachtes Berechtigungsmodell unerlässlich. Wie Sie das konkret umsetzen, erklärt dieser Artikel.

TOOL	HOSTING-STANDORT	AVV VERFÜGBAR	DSGVO-EIGNUNG	AUFWAND
ChatGPT Free	USA	Nein	Nicht geeignet	—
ChatGPT Team/Enterprise	USA (opt-in EU möglich)	Ja	Bedingt	Mittel
Copilot for M365	EU möglich	Ja	Bedingt	Mittel–Hoch
Google Workspace AI	EU möglich	Ja	Bedingt	Mittel
Ollama + Llama 3 (self-hosted)	Eigener Server	Intern	Hoch	Hoch
Mistral (EU-Hosting)	EU	Ja	Hoch	Mittel

Schritt-für-Schritt: KI-Tools datensicher einführen (ohne IT-Abteilung)

Schritt 1 – Bestandsaufnahme: Welche KI-Tools sind schon im Einsatz?

Bevor Sie irgendetwas einrichten, müssen Sie wissen, was bereits genutzt wird. Eine kurze Mitarbeiterbefragung — per E-Mail oder im nächsten Team-Meeting — reicht oft aus: „Welche KI-Tools nutzt ihr im Arbeitsalltag, auch privat für berufliche Aufgaben?"

Ergänzend lohnt ein Blick auf installierte Browser-Extensions und genutzte Web-Apps. Schatten-KI — also Tools, die ohne Wissen der Geschäftsführung eingesetzt werden — ist in KMU die Regel, nicht die Ausnahme. Wer sie nicht kennt, kann sie nicht absichern.

Schritt 2 – Datenkategorien definieren: Was darf in welches Tool?

Eine einfache Drei-Kategorie-Logik hilft, Klarheit zu schaffen:

- **Öffentliche Daten:** Allgemeine Texte, Marketingmaterial, Informationen, die ohnehin auf der Website stehen. Können in nahezu jedem Tool genutzt werden.
- **Interne Daten:** Prozessbeschreibungen, interne Abläufe, nicht-personenbezogene Betriebsinformationen. Nur in Tools mit AVV.
- **Vertrauliche und personenbezogene Daten:** Kundendaten, Mitarbeiterinformationen, Verträge, Finanzdaten. Ausschließlich in Tools mit AVV und nachgewiesener EU-Datenhaltung.

Diese Kategorie-Logik ist der Kern jeder internen KI-Nutzungsrichtlinie. Wer KI-Workflows mit internen Unternehmensdaten betreibt, findet in diesem Artikel eine tiefere technische Absicherung.

Schritt 3 – AVV abschließen (oder Tool wechseln)

Für die gängigsten Tools finden Sie den AVV hier:

- **Microsoft (Copilot, Azure):** Über das Microsoft Admin Center unter „Datenschutzeinstellungen" oder direkt über den Microsoft Online Subscription Agreement
- **Google (Workspace AI):** Im Google Admin Console unter den Datenverarbeitungsbedingungen
- **OpenAI (ChatGPT Team/Enterprise):** Über das OpenAI Privacy Portal, Bereich „Data Processing Agreement"

Was Sie im AVV konkret prüfen sollten: (1) Welche Unterauftragsverarbeiter werden eingesetzt — und wo sitzen diese? (2) Welche Löschfristen gelten für Ihre Daten? (3) Gibt es Datentransfers in Drittstaaten außerhalb der EU, und auf welcher Rechtsgrundlage (z. B. Standardvertragsklauseln)?

Ist kein AVV verfügbar oder nicht akzeptabel: Das Tool ist für personenbezogene Daten nicht nutzbar. Kein Kompromiss.

Wie Sie Rechtsgrundlagen und AVV-Anforderungen im Detail einordnen, zeigt unser Leitfaden zur DSGVO-konformen KI-Nutzung.

Schritt 4 – Interne Nutzungsrichtlinie erstellen (1 Seite reicht)

Eine Nutzungsrichtlinie für KI-Tools muss nicht umfangreich sein. Für ein KMU reicht ein einseitiges Dokument mit diesen Mindestinhalten:

- Welche Tools sind für welche Datenkategorie freigegeben?
- Was darf niemals in ein KI-Tool eingegeben werden (Negativliste)?
- Wer ist im Unternehmen Ansprechpartner bei Unsicherheiten?
- Was ist bei einem möglichen Vorfall zu tun?

Im Beratungsgespräch besprechen wir bei Strukturaflow regelmäßig, welche Formulierungen für den jeweiligen Betrieb passen — eine fertige Vorlage allein greift oft zu kurz, weil die Datentypen je nach Branche stark variieren.

Schritt 5 – Mitarbeiter kurz schulen (60 Minuten genügen)

Die häufigste Ursache für KI-bedingte Datenpannen ist kein technisches Versagen — es ist eine unbedachte Eingabe. Ein Mitarbeiter, der nicht weiß, dass Kundendaten in ChatGPT Free ein Problem sind, kann das Problem nicht vermeiden.

Ein 30-minütiges Team-Meeting zur neuen Nutzungsrichtlinie plus ein einseitiges Merkblatt zum Aufhängen oder Ausdrucken sind in den meisten Fällen ausreichend. Das Merkblatt sollte die Drei-Kategorien-Logik zeigen und drei konkrete Beispiele nennen: „Das darf rein", „Das darf nicht rein", „Hier nachfragen".

EU AI Act – was KMU jetzt wissen müssen (und was Sie noch nicht tun müssen)

Der EU AI Act ist seit Sommer 2024 in Kraft und gilt gestaffelt: Verbote für inakzeptable Risikosysteme ab Februar 2025, Pflichten für Hochrisiko-KI ab August 2026, allgemeine Transparenzpflichten schrittweise ab 2025.

Was gilt als „Hochrisiko-KI" im Sinne des AI Act? Systeme, die für Personalentscheidungen (Einstellung, Kündigung), Kreditvergabe, biometrische Identifikation oder sicherheitsrelevante Infrastruktur eingesetzt werden. Wer ein solches System einsetzt oder betreibt, braucht Dokumentation, Risikobewertungen und in manchen Fällen Konformitätsprüfungen.

Für ein 20-Personen-Dienstleistungsunternehmen, das KI für Texterstellung, E-Mail-Drafts oder Recherche nutzt, ist der unmittelbare Handlungsbedarf durch den EU AI Act noch überschaubar. Relevant ist aber die Transparenzpflicht: Wenn Kunden oder Mitarbeiter mit KI-generierten Inhalten konfrontiert werden, muss das erkennbar sein.

Die ehrliche Einschätzung: Wer jetzt eine ordentliche Datenschutzbasis aufbaut — AVV, Nutzungsrichtlinie, Datenkategorien — ist für die kommenden AI-Act-Anforderungen bereits gut positioniert. Die Grundlagen überschneiden sich erheblich. Was der EU AI Act konkret von KMU verlangt, erklärt unser Artikel EU AI Act: Was müssen KMU jetzt wirklich tun?

Besonderheiten für Österreich: DSG, DSB und KI-Tools

Das österreichische Datenschutzgesetz (DSG) ist die nationale Ausformung der DSGVO. In den meisten Bereichen sind die Anforderungen deckungsgleich — es gibt aber zwei relevante Abweichungen für den KI-Einsatz:

Meldepflicht und Behördenzuständigkeit: In Österreich ist die Datenschutzbehörde (DSB) in Wien die zuständige Aufsichtsbehörde. Datenpannen müssen dort binnen 72 Stunden gemeldet werden — gleicher Rahmen wie in Deutschland, aber abweichendes Formular und Einreichweg. Die DSB stellt ein Online-Formular bereit; die aktuelle Version finden Sie unter dsb.gv.at.

Branchenspezifische Regelungen: Österreichische Gesundheitsdienstleister unterliegen zusätzlich dem Gesundheitstelematikgesetz (GTelG). Rechtsanwaltskanzleien müssen die Standesregeln der Rechtsanwaltskammer beachten, die den Einsatz externer Datenverarbeitungsdienste für mandantenbezogene Daten einschränken können. Wer in diesen Branchen tätig ist, sollte den KI-Einsatz nicht allein anhand der DSGVO bewerten.

Kostenloser Rat für österreichische KMU: Die Wirtschaftskammer Österreich (WKO) bietet eine kostenlose Datenschutz-Hotline an. Diese ist unter wko.at/datenschutz erreichbar und kann bei grundlegenden Fragen zur AVV-Pflicht oder Meldepflicht erste Orientierung geben — bevor teure Rechtsberatung notwendig wird.

Deutschland vs. Österreich — zwei konkrete Unterschiede: 1. In Deutschland sind die Landesdatenschutzbehörden zuständig (je nach Bundesland unterschiedlich); in Österreich gibt es mit der DSB nur eine einzige zuständige Behörde. 2. Das österreichische DSG enthält in § 24 explizite Regelungen zur Datenschutzbeauftragten-Pflicht, die in einigen Punkten von den deutschen Regelungen abweichen — relevant vor allem für KMU, die unsicher sind, ob sie einen DSB benennen müssen.

Checkliste – KI-Datenschutz für KMU (zum Abhaken)

Tools & Verträge

- [ ] Alle im Betrieb genutzten KI-Tools sind bekannt und dokumentiert (inkl. Browser-Extensions)
- [ ] Für jedes Tool mit Zugang zu personenbezogenen Daten liegt ein gültiger AVV vor
- [ ] Der Hosting-Standort jedes Tools ist bekannt; Drittstaatentransfers sind geprüft
- [ ] Hochrisiko-KI-Systeme (Personalentscheidungen, biometrische Daten) sind identifiziert und separat bewertet

Organisation & Richtlinien

- [ ] Interne KI-Nutzungsrichtlinie ist erstellt und schriftlich dokumentiert
- [ ] Drei-Kategorien-Logik für Daten (öffentlich / intern / vertraulich) ist definiert
- [ ] Negativliste verbotener Eingaben ist für Mitarbeiter klar kommuniziert
- [ ] Zuständigkeit bei Datenpannen ist intern geregelt (wer meldet, wann, an wen?)

Mitarbeiter

- [ ] Team wurde über die Nutzungsrichtlinie informiert (Meeting-Protokoll vorhanden)
- [ ] Merkblatt „Was darf in KI-Tools — was nicht?“ ist verfügbar (ausgedruckt oder digital)

Monitoring

- [ ] Es gibt einen regelmäßigen Check (z. B. quartalsweise): Welche neuen Tools sind hinzugekommen?
- [ ] Datenpannen oder Verdachtsfälle werden intern dokumentiert

> Sie möchten diese Checkliste auf Ihr Unternehmen anpassen? Im Beratungsgespräch gehen wir Ihre Situation Schritt für Schritt durch.

Häufige Fehler – und wie Sie sie vermeiden

Fehler 1: Auf den Anbieter vertrauen, ohne selbst zu prüfen „Die sind doch DSGVO-konform“ ist keine ausreichende Grundlage. DSGVO-konform bedeutet nur, dass ein Anbieter die Rahmenbedingungen für einen datenschutzkonformen Einsatz bieten kann — nicht, dass Ihr konkreter Einsatz automatisch rechtmäßig ist. Sie tragen als Verantwortlicher die Pflicht zur eigenen Prüfung.

Fehler 2: AVV unterschreiben, aber nicht lesen Viele AVVs enthalten Klauseln zu Unterauftragsverarbeitern in Drittstaaten oder zu Löschfristen, die nicht den eigenen Vorstellungen entsprechen. Drei Punkte müssen Sie verstehen, bevor Sie unterschreiben: Wer verarbeitet die Daten außer dem Anbieter selbst? Wann werden meine Daten gelöscht? Gibt es Datentransfers außerhalb der EU?

Fehler 3: Freigabe für alle Daten, weil ein Use-Case funktioniert hat Das Tool taugt für Marketingtexte — also wird es auch für Kundenangebote genutzt. Diese Logik ist nachvollziehbar, aber falsch. Die Freigabe eines Tools für eine Datenkategorie gilt nicht automatisch für alle anderen.

Fehler 4: Kein Monitoring, wer welches Tool wofür nutzt Es geht nicht um Überwachung der Mitarbeiter. Es geht darum, zu wissen, ob neue Tools stillschweigend eingeführt wurden — oder ob sich Nutzungsgewohnheiten so verändert haben, dass die ursprüngliche Risikoeinschätzung nicht mehr passt. Ein quartalsweiser Kurzcheck reicht.

Fehler 5: Datenschutz als einmalige Aufgabe Wer im Januar eine Nutzungsrichtlinie erstellt und im Dezember noch dieselbe Version hat, hat wahrscheinlich etwas verpasst. KI-Tools entwickeln sich schnell, Anbieter ändern ihre Datenschutzbedingungen, neue Mitarbeiter kommen hinzu. Datenschutz ist kein Projekt — es ist ein laufender Prozess.

Häufige Fragen

Darf ich Kundendaten in ChatGPT eingeben?

Nur wenn ein gültiger AVV mit OpenAI besteht und das Unternehmen die Datenverarbeitung in den Account-Einstellungen entsprechend konfiguriert hat (Trainingsoption deaktiviert, Business-Account). ChatGPT Free ist für personenbezogene Kundendaten grundsätzlich nicht geeignet — unabhängig davon, wie bequem das Tool im Alltag ist.

Was ist der Unterschied zwischen Datenverlust und Datenpanne im DSGVO-Sinne?

Der Begriff „Datenpanne“ nach Art. 4 Nr. 12 DSGVO ist breiter als „Datenverlust“: Er umfasst Vernichtung, Verlust und Veränderung von Daten — aber auch unbefugten Zugang oder unbefugte Offenlegung. Wer Kundendaten unbeabsichtigt an einen KI-Anbieter ohne AVV übermittelt, kann damit gleichzeitig eine meldepflichtige Datenpanne ausgelöst haben, auch wenn die Daten inhaltlich nicht „verloren“ sind.

Muss ich als KMU den EU AI Act bereits umsetzen?

Die meisten Pflichten gelten gestaffelt ab 2025 und 2026. Für KMU, die KI nur für einfache Anwendungsfälle wie Texterstellung, Übersetzung oder E-Mail-Drafts nutzen, ist der unmittelbare Handlungsbedarf durch den AI Act aktuell noch überschaubar. Wer allerdings KI für Personalent-

scheidungen oder kundenrelevante Bewertungen einsetzt, sollte sich jetzt mit den Hochrisiko-Kategorien auseinandersetzen. Der Artikel EU AI Act: Was müssen KMU jetzt wirklich tun? gibt einen strukturierten Überblick.

Nächste Schritte

Viele der Maßnahmen in diesem Artikel lassen sich mit etwas Zeit und den richtigen Vorlagen selbst umsetzen: AVV abschließen, eine Nutzungsrichtlinie schreiben, das Team kurz schulen. Das sind keine technischen Herausforderungen.

Die größten Fehler entstehen aber erfahrungsgemäß an zwei Stellen: bei der Einschätzung, welche Daten im eigenen Betrieb wirklich schutzwürdig sind — und bei der Wahl des richtigen Tool-Stacks für die eigene Branche und Betriebsgröße. Was für eine Steuerkanzlei gilt, ist für einen Handwerksbetrieb mit 15 Mitarbeitern anders zu bewerten.

Bei Strukturaflow bieten wir ein unverbindliches 30-minütiges Beratungsgespräch an. Kein Technik-Jargon, keine Verkaufspräsentation — sondern eine ehrliche Einschätzung, wo Ihr Handlungsbedarf liegt: welche Tools Sie bereits sicher einsetzen, wo konkrete Lücken bestehen, und welche nächsten Schritte für Ihren Betrieb sinnvoll sind.

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