// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

KI DSGVO-konform einsetzen: Leitfaden für KMU

ChatGPT & Co. DSGVO-konform nutzen: AVV, Rechtsgrundlagen, EU AI Act — ein klarer 5-Schritte-Leitfaden für DACH-KMU ohne Juristendeutsch.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
30. April 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/ki-dsgvo-konform-einsetzen-kmu/

Ein Marketingteam kopiert seit Monaten Kundennamen und Betreffzeilen in ChatGPT, um schneller auf Anfragen zu reagieren. Kein AVV abgeschlossen, kein Eintrag im Verzeichnis der Verarbeitungstätigkeiten, kein klares Bild davon, ob die Daten für das Training des Modells genutzt werden. Nicht böswillig — sondern schlicht, weil das Thema nie aufgekommen ist. Das ist kein Einzelfall.

Die DSGVO gilt auch beim Einsatz von KI-Tools — uneingeschränkt. Die gute Nachricht: Die Umsetzung ist machbar, ohne einen Datenschutzanwalt dauerhaft auf Retainer zu bezahlen. Dieser Leitfaden führt Sie durch fünf konkrete Schritte, erklärt, welche Anbieter einen Auftragsverarbeitungsvertrag (AVV) bieten, ordnet den EU AI Act für den KMU-Alltag ein und benennt branchenspezifische Risiken, die besondere Aufmerksamkeit verdienen.

Warum die DSGVO auch beim KI-Einsatz gilt – und zwar immer

KI-Tools verarbeiten fast zwangsläufig personenbezogene Daten. Schon ein vollständiger Name in einem Prompt reicht aus. Wer E-Mail-Texte, Kundenbeschwerden oder Bewerberunterlagen in ein KI-Tool eingibt, überträgt personenbezogene Daten an einen Dritten — und bleibt dabei als Verantwortlicher im Sinne der DSGVO haftbar. Der Anbieter des Tools ist in den meisten Fällen Auftragsverarbeiter, nicht Mitverantwortlicher. Das bedeutet: Die Pflichten bleiben bei Ihrem Unternehmen.

Drei Artikel der DSGVO sind in diesem Kontext besonders zentral:

- **Art. 5 DSGVO** — Grundsätze der Verarbeitung: Daten müssen zweckgebunden, sparsam und sicher verarbeitet werden.
- **Art. 25 DSGVO** — Privacy by Design und by Default: Datenschutz muss von Anfang an mitgedacht werden, nicht nachträglich.
- **Art. 28 DSGVO** — Auftragsverarbeitung: Jede Weitergabe an einen Dienstleister, der Daten in Ihrem Auftrag verarbeitet, setzt einen schriftlichen AVV voraus.

Praxisbeispiel: Ein Mitarbeitender kopiert eine Kundenbeschwerde inklusive Name und E-Mail-Adresse in ChatGPT und lässt eine Antwort formulieren. Die personenbezogenen Daten werden damit an OpenAI übertragen. Ohne AVV ist das ein Verstoß gegen Art. 28 DSGVO — unabhängig davon, ob der Output gut war.

Wann wird es wirklich kritisch?

Besonders heikel wird es bei besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO: Gesundheitsdaten, politische Meinungen, ethnische Herkunft, biometrische Daten. Wer solche Informationen auch nur versehentlich in einen Prompt eingibt, bewegt sich in einem Bereich mit erhöhten Anforderungen — explizite Einwilligung oder ein enger gesetzlicher Ausnahmetatbestand sind hier Pflicht.

Ein zweiter Risikopunkt ist die automatisierte Entscheidungsfindung nach Art. 22 DSGVO. Wer KI für das Screening von Bewerbungen, für Kreditentscheidungen oder für automatisierte Kundenbewertungen einsetzt, muss besondere Anforderungen erfüllen: unter anderem das Recht auf menschliche Überprüfung und transparente Kriterien.

Was Bußgelder angeht: Konkrete KI-spezifische Verfahren in DACH laufen noch überwiegend, ohne öffentliche Abschlüsse zu haben. Die österreichische Datenschutzbehörde (DSB) und die deutschen Landesaufsichtsbehörden haben jedoch klargestellt, dass KI-Tools keine regulierungsfreie Zone sind. Der Trend geht klar in Richtung aktiver Durchsetzung — und erste Verwarnungen und Bußgelder bei KI-bezogenen Verstößen sind in verschiedenen EU-Ländern bereits ergangen.

Der 5-Schritte-Check: KI DSGVO-konform einsetzen

Schritt 1: Bestandsaufnahme – welche KI-Tools werden tatsächlich genutzt?

Bevor Sie irgendetwas regeln können, müssen Sie wissen, was in Ihrem Unternehmen überhaupt im Einsatz ist. Shadow IT ist dabei keine Ausnahme, sondern die Regel: Mitarbeitende nutzen ChatGPT, Grammarly, DeepL, Notion AI oder branchenspezifische KI-Assistenten oft ohne explizite Freigabe.

Was Sie jetzt tun können: Führen Sie eine kurze interne Abfrage durch — per E-Mail oder in einem Team-Meeting. Fragen Sie konkret: Welche KI-Tools nutzt ihr in eurer täglichen Arbeit, auch privat für berufliche Aufgaben? Die Ergebnisse werden erfahrungsgemäß überraschend sein.

Schritt 2: Datenkategorien prüfen – was landet tatsächlich in diesen Tools?

Nicht jede KI-Nutzung ist datenschutzrechtlich gleich riskant. Wer ChatGPT für generische Textentwürfe ohne Personendaten nutzt, bewegt sich in einem anderen Bereich als wer komplette Kundenkorrespondenz eingibt.

Was Sie jetzt tun können: Erstellen Sie eine einfache Liste: Tool — typische Eingaben — enthaltene Datenkategorien. Das muss keine juristische Analyse sein, sondern eine ehrliche Beschreibung des Alltags. Wo tauchen Namen auf? Wo Adressen, Gesundheitsinformationen, interne Finanzzahlen?

Schritt 3: Rechtsgrundlage klären (Art. 6 DSGVO)

Jede Datenverarbeitung braucht eine Rechtsgrundlage. Die drei relevantesten im KMU-Kontext sind:

- **Vertragserfüllung (Art. 6 Abs. 1 lit. b):** Verarbeitung ist zur Erfüllung eines Vertrags mit der betroffenen Person notwendig.
- **Berechtigtes Interesse (Art. 6 Abs. 1 lit. f):** Ihr betriebliches Interesse überwiegt die Interessen der betroffenen Person — hier ist eine Interessenabwägung zu dokumentieren.
- **Einwilligung (Art. 6 Abs. 1 lit. a):** Freiwillig, informiert, jederzeit widerrufbar. Im B2B-Kontext oft unpraktisch, im B2C-Kontext für bestimmte Anwendungen aber der sicherere Weg.

Was Sie jetzt tun können: Legen Sie für jeden identifizierten KI-Einsatz eine Rechtsgrundlage fest und dokumentieren Sie diese. Wenn keine passt — die Verarbeitung einschränken oder einstellen.

Schritt 4: AVV abschließen – mit jedem relevanten Anbieter

Sobald ein KI-Anbieter in Ihrem Auftrag personenbezogene Daten verarbeitet, ist ein schriftlicher Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO verpflichtend. Viele Anbieter stellen diesen online bereit — oft als Teil der Business- oder Enterprise-Tarife.

Was Sie jetzt tun können: Prüfen Sie für jedes identifizierte Tool, ob ein AVV verfügbar ist und schließen Sie diesen ab. Details dazu im nächsten Abschnitt.

Schritt 5: Verzeichnis der Verarbeitungstätigkeiten (VVT) aktualisieren

Das VVT nach Art. 30 DSGVO muss alle relevanten Verarbeitungen dokumentieren — einschließlich der eingesetzten KI-Tools als Auftragsverarbeiter. Bei einer Prüfung durch die Aufsichtsbehörde ist das eine der ersten Unterlagen, die angefragt werden.

Was Sie jetzt tun können: Ergänzen Sie Ihr VVT um die identifizierten KI-Tools. Wenn Sie noch kein VVT haben — jetzt ist der richtige Zeitpunkt, damit anzufangen. Ab 250 Mitarbeitenden ist es Pflicht; darunter in der Regel ebenfalls, wenn nicht-gelegentliche Verarbeitungen stattfinden.

Fünf-Schritt-Prozess zur DSGVO-konformen KI-Einführung in KMU: Bestandsaufnahme, Datenkategorien prüfen, Rechtsgrundlage, AVV abschließen, Schulung.

AVV mit KI-Anbietern: Was gilt, was fehlt, was Sie fordern sollten

Ein Auftragsverarbeitungsvertrag regelt, dass ein Dienstleister Daten ausschließlich nach Ihren Weisungen verarbeitet, geeignete technische und organisatorische Maßnahmen trifft, Subunternehmer offenlegt und Daten nach Beendigung der Zusammenarbeit löscht. Ohne dieses Dokument ist die Weitergabe personenbezogener Daten an den Anbieter rechtswidrig — unabhängig davon, wie gut die Datenschutzerklärung des Anbieters klingt.

Die folgende Übersicht basiert auf dem Stand Mitte 2025 und muss regelmäßig geprüft werden, da Anbieter ihre Bedingungen ändern:

TOOL	AVV VERFÜGBAR	SERVERSTANDORT (STANDARD)	TRAINING AUF NUTZERDATEN	HINWEIS
ChatGPT Free/Plus	Nein	USA	Ja (opt-out möglich)	Nicht für Kundendaten geeignet
ChatGPT Team	Ja	USA	Nein (standardmäßig)	AVV über Data Processing Agreement
ChatGPT Enterprise	Ja	USA	Nein	EU-Datenspeicherung optional
OpenAI API	Ja	USA	Nein (standardmäßig)	SCCs für Drittstaaten-Transfer prüfen
Microsoft Copilot (M365)	Ja	EU möglich	Nein	Im bestehenden M365-Vertrag geregelt
Azure OpenAI	Ja	EU-Region wählbar	Nein	Für Unternehmen mit EU-Anforderungen empfehlenswert
Google Gemini (Workspace)	Ja	EU möglich	Nein (für Workspace-Daten)	Im Workspace-Vertrag geregelt
Mistral (Le Chat Pro)	Ja	EU (Frankreich)	Nein	Kleinere Anbieter, aber solides EU-Hosting
Lokale LLMs (z.B. Ollama)	Nicht nötig	Ihr eigener Server	Nein	Technisch aufwendig, datenschutzrechtlich sauberste Lösung

Wichtiger Hinweis: Ein AVV allein genügt nicht, wenn Daten in Drittstaaten (insbesondere USA) übertragen werden. Hier greifen zusätzlich die Regelungen zu Drittstaaten-Transfers nach Art. 44 ff. DSGVO. Für US-Anbieter sind Standardvertragsklauseln (SCCs) und der EU-US Data Privacy Framework relevant — aber deren Bestand ist durch politische Entwicklungen grundsätzlich nicht dauerhaft gesichert. Wer maximale Rechtssicherheit will, wählt Anbieter mit EU-Serverstandort.

Diese Einschätzung ersetzt keine individuelle Rechtsberatung und muss regelmäßig auf Aktualität geprüft werden.

Was tun, wenn ein Anbieter keinen AVV stellt?

Die Antwort ist unbequem, aber klar: Entweder Sie beschränken die Nutzung konsequent auf nicht-personenbezogene Daten — also keine Namen, keine Adressen, keine Inhalte die einer Person zugeordnet werden können — oder Sie wechseln zu einem Anbieter, der einen AVV bietet. Eine dritte Option: Schalten Sie einen externen Datenschutzbeauftragten ein, der die Situation individuell bewertet.

Europäische Alternativen gewinnen hier an Bedeutung. Mistral (Frankreich), lokale LLM-Setups über Tools wie Ollama sowie zunehmend auch deutsche Angebote bieten EU-konformes Hosting mit klaren Datenschutzbedingungen.

EU AI Act und DSGVO – was KMU 2025 wissen müssen

Der EU AI Act ist seit August 2024 in Kraft und wird stufenweise angewendet. Erste Verbote für „inakzeptable Risiko"-Systeme (z.B. Social Scoring durch staatliche Stellen, manipulative KI-Systeme) galten ab Februar 2025. Transparenzpflichten für bestimmte KI-Systeme folgen im August 2025. Die umfassenden Pflichten für Hochrisiko-KI-Systeme greifen ab August 2026.

DSGVO und EU AI Act gelten parallel — es gibt kein Entweder-oder. Der AI Act regelt, welche KI-Systeme unter welchen Bedingungen eingesetzt werden dürfen. Die DSGVO regelt den Umgang mit personenbezogenen Daten dabei. Beide Regelwerke müssen gleichzeitig eingehalten werden.

Hochrisiko-Kategorien im EU AI Act umfassen unter anderem: - KI-gestütztes Recruiting und HR-Systeme - Kreditvergabe und Bonitätsbewertung - Biometrische Erkennung - KI in der Bildung und kritischen Infrastruktur

Für ein typisches DACH-KMU, das KI für Marketing-Texte, Kundenkommunikation oder interne Recherche nutzt, fallen diese Anwendungen in der Regel in die niedrige Risikoklasse. Aber: Transparenzpflichten gelten dennoch. Wenn KI-generierte Inhalte Kunden präsentiert werden — etwa automatisch formulierte E-Mails oder Chatbot-Antworten — muss das erkennbar sein.

KMU-Erleichterungen gibt es im AI Act tatsächlich: Kleinere Anbieter von KI-Systemen genießen vereinfachte Dokumentationspflichten. Als Nutzer (nicht Anbieter) von KI-Tools sind die Anforderungen für KMU nochmals geringer. Das sollte aber nicht als Freifahrtschein missverstanden werden — die Grundpflichten gelten auch hier.

Einen strukturierten Überblick, was der EU AI Act konkret für Ihren Betrieb bedeutet, bietet der Artikel EU AI Act: Was müssen KMU jetzt wirklich tun?.

Ähnlich wie beim NIS2/NISG 2026 gilt auch hier: Auch wenn Ihr Unternehmen nicht direkt von allen Pflichten betroffen scheint, lohnt sich ein genauer Blick auf die Anforderungen — lesen Sie hier, was das NISG 2026 für österreichische KMU bedeutet.

Branchenspezifische Hinweise – wo die Risiken besonders hoch sind

HR und Recruiting

KI-gestütztes Bewerber-Screening ist eine der kritischsten Anwendungen. Art. 22 DSGVO gilt hier direkt: Wenn KI automatisiert Entscheidungen mit rechtlicher oder erheblicher Wirkung auf Personen trifft, besteht das Recht auf menschliche Überprüfung. Zusätzlich sind in vielen Unternehmen Betriebsrats- oder Personalvertretungsrechte zu beachten. Bewerberunterlagen können außerdem besondere Datenkategorien enthalten (z.B. Foto, Gesundheitsangaben, Religionszugehörigkeit).

Gesundheit und Healthcare

Patientendaten sind besondere Kategorie nach Art. 9 DSGVO. Die Messlatte für deren Verarbeitung liegt deutlich höher: explizite Einwilligung oder ein enger gesetzlicher Ausnahmetatbestand sind Pflicht. Wer im Gesundheitsbereich tätig ist und KI einsetzt — etwa für Terminverwaltung, Dokumentation oder Diagnoseunterstützung — braucht eine besonders sorgfältige DSGVO-Folgenabschätzung (DSFA nach Art. 35 DSGVO) und in vielen Fällen einen benannten Datenschutzbeauftragten.

Steuer- und Rechtsberatung

Kanzleien und Steuerberater unterliegen gesetzlicher Verschwiegenheitspflicht und Berufsgeheimnis. Die Eingabe von Mandantendaten in externe KI-Tools ist ohne explizite Einwilligung oder konkrete gesetzliche Grundlage problematisch — unabhängig von der DSGVO. Einen konkreten Praxisguide für österreichische Steuerberater bietet der Artikel ChatGPT für Steuerberater in Österreich: Praxisguide 2025.

Handel und E-Commerce

Personalisierung, produktbasiertes Profiling und KI-gestützte Empfehlungssysteme berühren Datenschutzrecht und oft auch das Cookie-Regime. Transparenz und Opt-out-Möglichkeiten sind Pflicht. Wer KI für dynamische Preisgestaltung oder automatisierte Kundensegmentierung einsetzt, sollte prüfen, ob eine DSFA notwendig ist.

Was Sie intern regeln müssen – Mitarbeitende und KI-Nutzung

Eine interne KI-Richtlinie (oft „AI Policy" genannt) ist eines der wirkungsvollsten und am meisten unterschätzten Instrumente. Sie ist schnell erstellt, kostet nichts, und schützt das Unternehmen — sowohl datenschutzrechtlich als auch haftungsrechtlich, falls ein Mitarbeitender gegen die Vorgaben verstößt.

Was eine KI-Richtlinie mindestens enthalten sollte:

- **Erlaubte Tools:** Welche KI-Tools sind offiziell freigegeben und unter welchen Bedingungen?
- **Verbotene Datenkategorien für Prompts:** Welche Daten dürfen unter keinen Umständen eingegeben werden (z.B. Kundendaten mit Namen, Passwörter, Gesundheitsdaten)?
- **Umgang mit KI-generierten Outputs:** Müssen Ergebnisse vor Weitergabe von einem Menschen geprüft werden? Müssen KI-generierte Inhalte als solche gekennzeichnet werden?
- **Meldepflicht bei Datenpannen:** Was passiert, wenn versehentlich sensible Daten in ein KI-Tool eingegeben wurden?
- **Zuständigkeiten:** Wer ist Ansprechperson für Fragen zu KI-Nutzung und Datenschutz?

Schulungen müssen nicht aufwendig sein: Ein 20-minütiges Team-Meeting mit konkreten Beispielen („Was ist erlaubt, was ist verboten?") ist oft wirksamer als ein ausführliches Dokument, das niemand liest.

Schwachstellen im IT-Umfeld entstehen übrigens nicht nur durch KI-Tools — was die Bug-Bounty-Schließungen für Ihre IT-Sicherheit bedeuten, lesen Sie in diesem Artikel.

Praxis-Tipp – So starten Sie ohne großes Budget DSGVO-konform mit KI

Der häufigste Fehler: Entweder warten, bis alles perfekt geregelt ist (und dabei gar nicht starten), oder alles sofort einsetzen ohne jede Prüfung. Der pragmatische Mittelweg ist machbar.

Empfohlener Einstiegsweg für KMU ohne eigenen Datenschutzbeauftragten:

1. Starten Sie mit einem einzigen Tool, das einen AVV bietet und EU-Hosting ermöglicht — z.B. Microsoft Copilot innerhalb einer bestehenden M365-Umgebung oder die OpenAI API über Azure.
2. Beschränken Sie die Nutzung in der Anfangsphase auf generische Aufgaben ohne Personenbezug: Textformulierungen, Brainstorming, interne Dokumentation ohne echte Daten.
3. Erstellen Sie eine kurze AI Policy — eine Seite reicht für den Start.
4. Ergänzen Sie Ihr VVT um den eingesetzten Anbieter.

Externe Datenschutzbeauftragte gibt es für KMU als Dienstleistung — sinnvoll ab dem Moment, wo Sie regelmäßig sensible Daten verarbeiten, mehr als 20 Mitarbeitende beschäftigen oder KI-Anwendungen in kritischen Prozessen einsetzen wollen. Die Kosten liegen je nach Anbieter bei einigen hundert Euro pro Jahr und sind damit deutlich überschaubar im Vergleich zu möglichen Bußgeldern.

Häufig gestellte Fragen

Darf ich ChatGPT für die Arbeit mit Kundendaten nutzen?

Nur unter bestimmten Voraussetzungen. Für den kostenlosen und Plus-Tarif von ChatGPT steht kein AVV zur Verfügung — damit ist die Eingabe personenbezogener Daten nicht DSGVO-konform. Für ChatGPT Team oder Enterprise stellt OpenAI einen AVV bereit. Trotzdem bleibt der Serverstandort (USA) ein Punkt, der bei jedem Einsatz mit Personendaten geprüft werden sollte.

Brauche ich für jeden KI-Anbieter einen eigenen AVV?

Ja, sofern der Anbieter personenbezogene Daten in Ihrem Auftrag verarbeitet. Das gilt für jeden Anbieter separat. In der Praxis schließen Sie den AVV meist digital ab — viele Anbieter haben ihn als standardisierten Vertrag in ihren Geschäftsbedingungen für Business-Tarife hinterlegt.

Gilt der EU AI Act schon jetzt für mein KMU?

Teilweise. Die Verbote für „inakzeptable Risiko"-Systeme galten ab Februar 2025. Transparenzpflichten für bestimmte Systeme folgen im August 2025. Die umfassenden Hochrisiko-Pflichten gelten ab August 2026. Für die meisten KMU, die KI für generische Büroaufgaben nutzen, ist die direkte Betroffenheit gering — aber die stufenweise Umsetzung sollte beobachtet werden.

Was passiert, wenn ich KI ohne DSGVO-Konformität einsetze?

Theoretisch drohen Bußgelder von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes — je nachdem, was höher ist. In der Praxis beginnt die Aufsichtsbehörde bei KMU oft mit Verwarnungen und Auflagen. Das eigentliche Risiko ist aber nicht nur finanziell: Ein Datenschutzvorfall, der öffentlich wird, beschädigt Kundenvertrauen und Reputation dauerhaft. Panikmache ist nicht nötig — aber Ignoranz ist keine Strategie.

Reicht es, wenn ich KI nur intern nutze und keine Kundendaten eingebe?

Nicht automatisch. Mitarbeiterdaten sind ebenfalls personenbezogene Daten. Wer intern KI für HR-Zwecke, Leistungsbeurteilungen oder interne Kommunikation nutzt, bewegt sich weiterhin im DSGVO-Geltungsbereich. Die Grenze liegt beim echten Personenbezug — eine generische Textvorlage ohne Namen oder identifizierende Merkmale ist unproblematisch, der Entwurf einer personalisierten Abmahnung nicht.

Nächste Schritte – so gehen Sie jetzt konkret vor

Die fünf Kernmaßnahmen auf einen Blick:

- **Bestandsaufnahme:** Welche KI-Tools werden in Ihrem Unternehmen tatsächlich genutzt — auch ohne offizielle Freigabe?
- **Datenkategorien:** Was landet konkret in diesen Tools, und welche Personendaten sind betroffen?
- **Rechtsgrundlage:** Für jede Verarbeitung eine DSGVO-konforme Basis festlegen und dokumentieren.
- **AVV:** Mit jedem Anbieter, der Personendaten verarbeitet, einen Auftragsverarbeitungsvertrag abschließen.
- **VVT aktualisieren:** KI-Tools als Auftragsverarbeiter im Verzeichnis der Verarbeitungstätigkeiten erfassen.

DSGVO-konformer KI-Einsatz ist kein einmaliges Projekt. Anbieter ändern ihre Bedingungen, neue Tools kommen hinzu, die Regulierung entwickelt sich weiter. Aber der erste Schritt ist machbar — und er ist es wert.

Wenn Sie gerade nicht sicher sind, wo KI-Nutzung in Ihrem Unternehmen bereits stattfindet, welche Ihrer aktuellen Tools einen AVV bieten oder wie Sie den ersten DSGVO-Check strukturieren sollen: Genau das ist das Ziel des kostenlosen 30-Minuten-Beratungsgesprächs von Strukturaflow. Kein Juristendeutsch, keine Verkaufspräsentation — sondern ein konkreter Blick auf Ihre aktuelle Situation und klare Empfehlungen für den nächsten sinnvollen Schritt.

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