

COMPLIANCE

KI-Tool Löschkonzept DSGVO: Vorlage für österreichische KMU

Löschkonzept für KI-Tools nach DSGVO: Was österreichische KMU dokumentieren müssen – mit ausfüllbarer Vorlage und Anbieter-Checkliste.

AUTOR

Strukturaflow-Team

VERÖFFENTLICHT

21. Juli 2026

ONLINE LESEN

<https://wissen.strukturaflow.it.com/ki-tool-loeschkonzept-dsgvo-kmu-oesterreich-vorlage/>

KI-Tool Löschkonzept nach DSGVO: Vorlage + Anleitung für österreichische KMU

Ihr Auftraggeber fragt nach dem Löschkonzept, der Wirtschaftsprüfer möchte die Datenschutzdokumentation sehen — und Ihnen fällt auf, dass ChatGPT, Microsoft Copilot oder das KI-Buchungstool darin gar nicht vorkommt. Genau das passiert gerade vielen österreichischen KMU, die KI-Tools im Alltag nutzen, aber ihr Löschkonzept noch aus der Vor-KI-Ära stammt. Dieser Artikel erklärt, was ein Löschkonzept für KI-Tools im österreichischen Kontext konkret enthalten muss — und stellt eine direkt ausfüllbare Vorlage zur Verfügung.

Wichtiger Hinweis vorab: Dieser Artikel ersetzt keine Rechtsberatung und bildet den Stand nach aktueller Rechtslage ab. Bei komplexen Einzelfällen — insbesondere mit Gesundheitsdaten oder mehreren sensiblen Datenkategorien — empfiehlt sich die Rücksprache mit einer Datenschutzfachkraft.

Was ist ein Löschkonzept – und warum reicht das Standard-Muster bei KI-Tools nicht?

Ein Löschkonzept legt fest, welche personenbezogenen Daten wann und wie gelöscht werden. Die Grundlage dafür bildet Art. 5 Abs. 1 lit. e DSGVO (Speicherbegrenzung) in Verbindung mit der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO — Sie müssen nicht nur datensparsam handeln, sondern das auch dokumentieren können.

Klassische Löschkonzepte behandeln CRM-Systeme, E-Mail-Archive und Buchhaltungssoftware. KI-Tools erzeugen jedoch zusätzliche Datenkategorien, die in diesen Mustern schlicht nicht vorkommen.

Was bei KI-Tools zusätzlich dokumentiert werden muss

Prompt-Historien und Gesprächsverläufe: ChatGPT Free speichert Ihre Eingaben und Konversationen standardmäßig — und kann sie für das Training nutzen. ChatGPT Enterprise schließt das vertraglich aus, erfordert aber einen aktiven Auftragsverarbeitungsvertrag (AVV). Microsoft Copilot speichert Interaktionsdaten in Ihrem Microsoft-365-Tenant, sofern entsprechende Audit-Logs aktiviert sind.

Inferenz-Logs: Viele KI-APIs protokollieren, welche Anfragen wann über ihre Systeme liefen. Diese Logs können personenbezogene Daten enthalten, wenn Ihre Mitarbeitenden Kundennamen oder -details in Prompts eingeben.

Trainingsdaten und Fine-Tuning-Daten: Wenn Sie ein KI-Modell mit eigenen Daten feinabgestimmt haben, speichert der Anbieter diese Daten zusätzlich. Wann werden sie gelöscht, wenn Sie das Modell nicht mehr nutzen?

Modell-Outputs mit personenbezogenen Daten: Ein KI-generiertes Angebot, das den Namen und die Adresse eines Kunden enthält, ist ein personenbezogenes Datum — egal ob es von einer KI oder von Hand geschrieben wurde. Auch diese Outputs gehören ins Löschkonzept.

Rechtliche Grundlagen – was in Österreich gilt

Die DSGVO-Grundlagen gelten EU-weit einheitlich: Art. 5 (Grundsätze), Art. 17 (Recht auf Löschung) und Art. 30 (Verarbeitungsverzeichnis) sind die zentralen Normen. Österreich hat keine dem deutschen BDSG vergleichbare Parallelstruktur — das österreichische Datenschutzgesetz (DSG) ergänzt die DSGVO punktuell, etwa beim Klagerecht oder beim Schutz vor behördlicher Verarbeitung.

Zuständige Aufsichtsbehörde ist die Datenschutzbehörde (DSB) in Wien. Datenpannen, die ein hohes Risiko für Betroffene darstellen, sind nach Art. 33 DSGVO innerhalb von 72 Stunden zu melden. Das gilt auch, wenn der Vorfall beim KI-Anbieter passiert — als verantwortliches Unternehmen sind Sie in der Pflicht.

Für den EU AI Act gilt: Ab August 2026 greifen Transparenzpflichten und für Hochrisiko-KI-Systeme zusätzliche Dokumentationspflichten nach Art. 11 und 12 EU AI Act. Einen strukturierten Überblick zu den Fristen finden Sie im Artikel EU AI Act: Was müssen KMU jetzt wirklich tun?.

Erste österreichspezifische Anlaufstellen: Die WKO bietet datenschutzrechtliche Leitfäden an, die DSB veröffentlicht Empfehlungen und Musterdokumente unter dsb.gv.at.

Wer braucht kein Löschkonzept – und wer unbedingt?

Theoretisch entfällt die Pflicht, wenn ausschließlich vollständig anonymisierte Daten in KI-Tools eingegeben werden. Praktisch ist das kaum realistisch: Sobald ein Mitarbeitender „Schreib mir ein Mahnschreiben an Herrn Huber wegen offener Rechnung vom 3. März“ eintippt, sind personenbezogene Daten im Spiel.

Ein Löschkonzept für KI-Tools ist jedenfalls nötig, wenn Kundendaten, Mitarbeiterdaten, Gesundheitsdaten oder buchführungsrelevante Daten in KI-Prompts einfließen — was in den meisten österreichischen KMU täglich passiert.

KI-spezifische Datenkategorien – was Sie löschen müssen (und wo)

Ebene 1 – Daten beim KI-Anbieter

Hier liegt der größte blinde Fleck. Die folgende Übersicht zeigt den Stand nach aktueller Datenlage – Anbieterbedingungen ändern sich, prüfen Sie die aktuellen Datenschutzhinweise regelmäßig:

ANBIETER	STANDARDSPEICHERDAUER	LÖSCHOPTION	AVV FÜR BUSINESS MÖGLICH?
OpenAI (ChatGPT Free)	Unbegrenzt, bis zu manuell gelöscht; 30 Tage nach Konto-Löschung	Manuell in Einstellungen; Training opt-out möglich	Nein (Free)
OpenAI (ChatGPT Team/Enterprise)	Konfigurierbar, kein Training mit Daten	API oder Admin-Panel	Ja (Data Processing Agreement)
Microsoft Copilot (M365)	Entsprechend M365-Tenant-Einstellungen	Microsoft Admin Center	Ja (im M365-Vertrag enthalten)
Google Gemini (Workspace)	18 Monate Standard, konfigurierbar	Google Admin Console	Ja (Google Workspace -Vertrag)

Konkrete Schritte beim Anbieter: Trainingsnutzung deaktivieren (bei OpenAI unter Einstellungen → [Datenschutz](#) → „Verbesserungen für alle“), Datenlöschungsanfragen über den jeweiligen Support-Kanal stellen und die Bestätigung aufbewahren.

Ebene 2 – Daten in Ihrem eigenen System

KI-generierte Inhalte landen auch lokal: als Word-Dokumente, in E-Mails, in Integrations-Logs. Wenn Sie Zapier oder [n8n](#) für KI-Automatisierungen nutzen, entstehen dort Protokolldateien mit den verarbeiteten Inhalten. Chatbot-Protokolle auf der eigenen Website liegen häufig in der Datenbank des jeweiligen CMS oder Chatbot-Anbieters.

Alle diese Speicherorte müssen im Löschkonzept auftauchen – nicht nur der KI-Anbieter.

Ebene 3 – Backups und Archiv

Ein häufig übersehener Punkt: Wenn Ihre nächtliche Datensicherung auch das Verzeichnis mit KI-generierten Dokumenten miterfasst, landen personenbezogene Daten im Backup. Die Löschfrist im Backup muss mit der Löschfrist im Produktivsystem harmonisieren – oder Sie dokumentieren, dass Backups nach X Monaten automatisch überschrieben werden.

Vergleichstabelle zeigt vier KI-Anbieter mit deren Speicherdauer und Löschoptionen sowie Verfügbarkeit von Auftragsverarbeitungsverträgen für österreichische KMU.

Löschfristen – eine Orientierungstabelle für österreichische KMU

Löschfristen richten sich nach dem Verarbeitungszweck, nicht allein nach der Datenkategorie. Die folgende Tabelle ist eine Orientierung – die rechtliche Einzelfallprüfung bleibt empfohlen.

DATENKATEGORIE	TYPISCHER ZWECK	EMPFOHLENE FRIST (AT)	RECHTSGRUND-LAGE
Kundenkommunikation via KI-Chatbot	Vertragsabwicklung	3–7 Jahre	UGB § 212
Mitarbeiterbezogene Prompts (HR, Zeugnisse)	HR- <u>Prozesse</u>	Beschäftigungsdauer + 3 Jahre	AVRAG / DSGVO
Gesundheitsdaten (Arztpraxis, Physiotherapie)	Behandlungsdokumentation	10 Jahre	ÄrzteG § 51
Rechnungsrelevante KI-Outputs	Buchführungspflicht	7 Jahre	BAO § 132
Interessentenanfragen via KI-Chatbot	Marketing/Vertrieb	6 Monate bis 2 Jahre	DSGVO Art. 17
KI-generierte Angebote mit Kundendaten	Vertragsanbahnung	3 Jahre (Verjährung)	ABGB

Die Vorlage – Löschkonzept für KI-Tools (direkt ausfüllbar)

Kein Download erforderlich. Kopieren Sie die folgende Struktur in ein Word- oder Google-Docs-Dokument und füllen Sie die markierten Felder aus.

Pflichtbestandteile des Löschkonzepts

1. Verantwortlicher – Unternehmensname: [Name] – Adresse: [Adresse] – Datenschutzkontakt: [Name / E-Mail]

2. Übersicht der eingesetzten KI-Tools

KI-TOOL	ANBIETER	ZWECK IM BETRIEB	AVV ABGESCHLOSSEN?	SEIT WANN IM EINSATZ?
[z. B. ChatGPT Team]	[OpenAI]	[Angebotserstellung]	[Ja / Nein]	[Datum]

3. Datenkategorien je Tool Für jedes Tool: Welche personenbezogenen Daten werden eingegeben oder erzeugt? (z. B. Kundennamen, Adressen, Mitarbeiterdaten)

4. Speicherorte – Anbieter-Cloud (Standort EU / Drittland): [Angabe je Tool] – Eigene Systeme (lokale Ablage, Netzlaufwerk, CRM): [Angabe] – Backup-System: [Angabe, Backup-Intervall und Aufbewahrungsdauer]

5. Löschfristen je Datenkategorie und Speicherort Verwenden Sie die Orientierungstabelle oben als Ausgangspunkt.

6. Zuständige Person für Löschung – Name / Funktion: [z. B. Büroleitung, IT-Verantwortliche/r] – Vertretung: [Name]

7. Löschnachweis / Dokumentationspflicht Wie wird die erfolgte Löschung dokumentiert? (z. B. Eintrag in Löschprotokoll, E-Mail-Bestätigung des Anbieters)

8. Überprüfungsintervall Empfohlen: jährlich, sowie bei Einführung jedes neuen KI-Tools. Nächste geplante Überprüfung: [Datum]

Ausgefülltes Beispiel – Handwerksbetrieb Österreich

Unternehmen: Tischlerei Moser GmbH, Graz, 8 Mitarbeitende

KI-Tools im Einsatz: – ChatGPT Team (OpenAI) für Angebotserstellung und Kundenkommunikation – Lexoffice mit KI-Buchhalter-Funktion für Belegerfassung

Datenkategorien: – ChatGPT: Kundennamen, Projektbeschreibungen, gelegentlich Adressen – Lexoffice: Kundenstammdaten, Rechnungsbeträge, UID-Nummern

Speicherorte: – ChatGPT: OpenAI-Server (EU-Datenspeicherung lt. DPA), kein Training mit Unternehmens-Daten (AVV abgeschlossen) – Lexoffice: EU-Server (Deutschland), AVV im Rahmen des Abonnements enthalten – Lokal: Exportierte Angebote als .docx auf Netzlaufwerk W:\Angebote\

Löschfristen: – Kundendaten in ChatGPT-Verlauf: Manuelle Löschung nach Auftragsabschluss, spätestens nach 7 Jahren (UGB) – Lexoffice-Belege: 7 Jahre (BAO § 132) – Lokal gespeicherte Angebote: 3 Jahre nach Angebotsablauf, dann Papierkorb + Backup-Überschreibung

Zuständig: Karin Moser (Geschäftsführerin), Vertretung: Thomas Huber (Büro)

Löschnachweis: Jährlicher Eintrag im internen Löschprotokoll (Excel-Datei), Anbieter-Löschbestätigung per E-Mail archivieren.

Ausgefülltes Beispiel – Online-Shop (E-Commerce AT)

Unternehmen: Bergzeit Outdoor GmbH, Salzburg, 12 Mitarbeitende

KI-Tools im Einsatz: – KI-Chatbot (Tidio mit GPT-Integration) für Kundenservice auf der Website
– Jasper AI für Produkttexterstellung

Datenkategorien: – Chatbot: Kundennamen, E-Mail-Adressen, Bestellnummern, Reklamationsinhalte – Jasper: Produktbezeichnungen, gelegentlich Testkundendaten (intern)

Speicherorte: – Tidio: Tidio-Server (EU), Chatverläufe in Tidio-Dashboard abrufbar; AVV im Business-Tarif enthalten – Chatbot-Protokolle: Zusätzlich in WooCommerce-Datenbankbackup mitgesichert – Jasper: US-Server (Standardcontract Clauses), kein Training mit Eingaben laut Vertrag – Lokal: Fertige Produkttexte in WordPress-Datenbank

Löschfristen: – Chatbot-Protokolle mit Kundendaten: 6 Monate nach letztem Kontakt, längstens 2 Jahre – Tidio-Chatverläufe: Manuelle Löschung im Dashboard nach Fallabschluss + automatische Löschung nach 12 Monaten (lt. Tidio-Einstellungen konfiguriert) – Datenbankbackups: Überschreibung nach 90 Tagen (Hosting-Einstellung) – Produkttexte ohne personenbezogene Daten: Kein Löschbedarf

Zuständig: Lena Bergmann (Shopmanagerin), Vertretung: IT-Dienstleister XY

Wie Sie prüfen, ob Ihr KI-Anbieter die Löschpflichten einhält – Checkliste

Als verantwortliches Unternehmen haften Sie nicht für jeden Fehler des Anbieters – aber Sie müssen sorgfältig auswählen und die Einhaltung kontrollieren. Das ist der Kern der Auftragsverarbeitung nach Art. 28 DSGVO.

7-Punkte-Checkliste Anbieter-Check

- [] **AVV abgeschlossen?** Ohne Auftragsverarbeitungsvertrag dürfen personenbezogene Daten nicht an den Anbieter übermittelt werden.
- [] **Speicherort dokumentiert?** Liegt der Server in der EU oder in einem Drittland? Bei Drittländern: Welche Übertragungsgrundlage (Standardvertragsklauseln, Angemessenheitsbeschluss)?
- [] **Standardspeicherdauer bekannt?** Wie lange behält der Anbieter Ihre Eingaben standardmäßig — und ist das mit Ihren Löschfristen vereinbar?
- [] **Löschanfrage-Verfahren bekannt?** Können Sie Daten per Self-Service löschen, oder brauchen Sie ein Support-Ticket? Wie lange dauert die Umsetzung?
- [] **Trainingsnutzung deaktiviert?** Ist vertraglich oder technisch sichergestellt, dass Ihre Eingaben nicht für das Training des Modells genutzt werden?
- [] **Löschbestätigung erhältlich?** Stellt der Anbieter eine Bestätigung aus, dass Daten gelöscht wurden? Das ist Ihr Nachweis gegenüber der DSB.
- [] **Datenpannen-Meldung geregelt?** Ist der Anbieter verpflichtet, Sie bei Sicherheitsvorfällen unverzüglich zu informieren (Art. 33 DSGVO)?

Praxishinweis: Viele kostenlose oder günstige KI-Tools haben keinen EU-konformen AVV. Das ist kein Formalfehler — ohne AVV ist der Einsatz mit personenbezogenen Daten nach aktueller Rechtslage unzulässig. Mehr dazu im Artikel DSGVO & ChatGPT im Unternehmen: Was gilt 2026?.

Häufige Fehler österreichischer KMU beim KI-Löschkonzept

Fehler 1: Löschkonzept für klassische IT erstellt, KI-Tools vergessen. Das passiert, wenn das bestehende Konzept aus 2019 oder 2021 stammt und seitdem nicht aktualisiert wurde. KI-Tools kommen oft schnell und ohne formellen Beschaffungsprozess in den Betrieb.

Fehler 2: AVV mit KI-Anbieter fehlt oder ist veraltet. Anbieter aktualisieren ihre Verträge. Der AVV, den Sie 2022 für einen Dienst abgeschlossen haben, deckt möglicherweise neue Funktionen (z. B. KI-Features, die später dazugekommen sind) nicht mehr ab.

Fehler 3: Keine Unterscheidung zwischen Free-Tier und Business-Tier. Im kostenlosen ChatGPT-Plan werden Eingaben standardmäßig für das Training genutzt, sofern Sie das nicht explizit deaktivieren. Im Team- oder Enterprise-Plan ist das vertraglich ausgeschlossen. Wer im Betrieb den kostenlosen Plan nutzt und dabei Kundendaten eingibt, bewegt sich auf dünnem Eis.

Fehler 4: Löschfristen für Backups nicht berücksichtigt. Die Löschung aus dem Produkktivsystem reicht nicht, wenn die Daten noch drei Jahre lang im Backup liegen. Entweder werden Backups nach einer definierten Frist überschrieben, oder Sie dokumentieren, wie mit sensiblen Daten in Backups umgegangen wird.

Fehler 5: Löschkonzept einmalig erstellt, nie aktualisiert. Neue KI-Tools kommen hinzu, Anbieter ändern ihre AGB, Mitarbeitende wechseln. Ein Löschkonzept, das nicht gepflegt wird, verliert seinen Wert — und schlimmer: Es suggeriert Compliance, die nicht mehr besteht.

Ein Löschkonzept schützt nicht vor allem. Aber es zeigt der DSB im Prüffall, dass Sie die Rechenschaftspflicht ernst nehmen — und das hat in der Praxis erhebliches Gewicht.

Besonderheiten nach EU AI Act – was sich ab 2025/2026 ändert

Der EU AI Act gilt schrittweise ab Februar 2025, die meisten KMU-relevanten Pflichten greifen ab August 2026. Einen detaillierten Zeitplan finden Sie im Artikel EU AI Act: Was müssen KMU jetzt wirklich tun?.

Für Hochrisiko-KI-Systeme — das betrifft z. B. KI in der Personalauswahl oder im medizinischen Bereich — schreibt Art. 12 EU AI Act eine umfassende technische Dokumentation vor, die auch das Datenmanagement und die Löschprozesse abdeckt. Das geht über das DSGVO-Löschkonzept hinaus.

Für die meisten KMU-Nutzer von General Purpose AI (GPAI) wie ChatGPT oder Copilot sind die Pflichten als Nutzer deutlich geringer als für Anbieter. Trotzdem empfiehlt es sich, im Löschkonzept bereits einen Abschnitt „KI-spezifische Dokumentationspflichten EU AI Act“ anzulegen — auch wenn Ihre Tools heute noch nicht als Hochrisiko eingestuft sind. Die Einstufung kann sich ändern, und dann haben Sie bereits eine Grundstruktur.

Praktisch relevant ab August 2026: KI-Chatbots auf der eigenen Website unterliegen Transparenzpflichten. Nutzer müssen erkennen können, dass sie mit einer KI kommunizieren. Das betrifft auch die Protokollierung dieser Interaktionen — und damit Ihr Löschkonzept.

Praxis-Tipp – So integrieren Sie das Löschkonzept in Ihren Betrieb ohne Mehraufwand

Das Löschkonzept für KI-Tools muss kein separates Dokument sein. Führen Sie es als Anhang zum bestehenden Verzeichnis von Verarbeitungstätigkeiten (VVT). Das ist übersichtlicher, reduziert Doppelarbeit und erleichtert die Prüfung.

Setzen Sie eine halbjährliche Erinnerung im Kalender: Neue KI-Tools prüfen, Anbieterverträge kontrollieren, Fristen aktualisieren. Das dauert bei einem gut strukturierten Konzept 30–60 Minuten.

Benennen Sie eine interne Zuständige für Datenschutz und Löschung — das muss keine ausgebildete Datenschutzbeauftragte sein. Eine Büroleitung oder IT-verantwortliche Person ist ausreichend, solange die Zuständigkeit klar dokumentiert ist.

Die WKO bietet kostenlose VVT-Vorlagen an, die als Ausgangspunkt geeignet sind (wko.at/datenschutz). Die DSB stellt unter dsb.gv.at Musterformulare und Empfehlungen bereit.

Wenn Sie gerade KI-Tools systematisch in Ihrem Betrieb einführen, lohnt es sich, Datenschutz und Workflow-Gestaltung von Anfang an zusammenzudenken — statt nachträglich Lücken zu schließen. Gerade bei der Frage, welche KI-Tools für Ihre Branche überhaupt DSGVO-konform einsetzbar sind, helfen erfahrungsbasierte Einschätzungen mehr als allgemeine Ratgeber. Mehr dazu im Artikel KI DSGVO-konform einsetzen: Leitfaden für KMU.

Nächste Schritte – und wann ein Fachgespräch sinnvoll ist

Was Sie heute tun können: Kopieren Sie die Vorlage aus diesem Artikel, gehen Sie die Anbieter-Checkliste durch, und aktualisieren Sie Ihr Verarbeitungsverzeichnis um den KI-Anhang. Das sind drei konkrete Schritte, die keine juristische Vorbildung erfordern.

Die Vorlage reicht nicht mehr aus, wenn Ihr Betrieb mit Gesundheitsdaten, biometrischen Daten oder anderen besonderen Kategorien nach Art. 9 DSGVO arbeitet. Auch bei mehr als drei bis vier unterschiedlichen KI-Tools im Einsatz, bei Kundendaten aus sensiblen Bereichen oder bei bevorstehenden Datenschutzprüfungen durch Auftraggeber oder Behörden stoßen Mustervorlagen an ihre Grenzen.

In diesen Fällen ist ein strukturiertes Gespräch sinnvoller als weiteres Selbststudium. Bei Strukturaflow bieten wir ein unverbindliches 30-minütiges Beratungsgespräch an, in dem wir gemeinsam einschätzen, wo Ihr Betrieb beim Thema KI und Datenschutz steht — welche Tools problematisch sind, was die DSB im Prüffall sehen will, und welche nächsten Schritte für Ihre konkrete Situation sinnvoll wären. Kein allgemeiner Ratgeber, sondern eine Einschätzung auf Basis Ihrer tatsächlichen Situation.

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>