// KI-Hub VON STRUKTURAFLOW

COMPLIANCE

KI-Anbieter & Datenschutz: Pflichtklauseln im Vertrag

Welche Klauseln muss ein AVV mit KI-Anbietern enthalten? Checkliste, Musterformulierungen und Anbieter-Check für deutsche KMU.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
27. Mai 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/ki-anbieter-vertrag-datenschutz-pflichtklauseln-deutschland/

Ihr Unternehmen meldet sich bei ChatGPT Enterprise an, erhält automatisch einen Link zu einem „Data Processing Agreement" — und fragt sich, ob damit der DSGVO-Genüge getan ist. Kurze Antwort: Meistens nicht vollständig. Standard-AVVs von KI-Anbietern erfüllen die gesetzlichen Mindestanforderungen oft nur auf dem Papier; für deutsche Unternehmen kommen BDSG-Spezifika und seit August 2024 erste EU AI Act-Pflichten hinzu.

Dieser Artikel zeigt, welche Klauseln in jedem KI-Anbietervertrag vorhanden sein müssen, wo gängige Standardverträge typischerweise Lücken haben — und wie Sie diese Lücken mit Zusatzvereinbarungen schließen.

Warum KI-Anbieterverträge eine eigene Kategorie sind

Ein klassischer Auftragsverarbeitungsvertrag nach Art. 28 DSGVO regelt, wie ein Dienstleister Daten in Ihrem Auftrag verarbeitet. Bei KI-Anbietern kommen drei Besonderheiten hinzu, die ein Standard-AVV-Muster nicht abdeckt.

Trainingsnutzung von Eingabedaten: Verarbeitet der Anbieter Ihre Prompts zum Training neuer Modellversionen? Der Unterschied zwischen „zero data retention" und Standardeinstellungen ist datenschutzrechtlich erheblich — und in vielen Standardverträgen nicht klar geregelt.

Drittland-Übermittlung: Die Mehrheit großer KI-Anbieter verarbeitet in den USA. Das bedeutet: Standardvertragsklauseln (SCCs) nach Art. 46 DSGVO sind Pflicht, und nach dem Schrems-II-Urteil brauchen Sie zusätzlich ein dokumentiertes Transfer Impact Assessment.

Sub-Auftragsverarbeiter-Ketten: LLM-APIs nutzen ihrerseits Infrastrukturanbieter (Rechenzentren, CDNs, Monitoring-Dienste). Wer haftet für die gesamte Kette? Und haben Sie überhaupt ein Widerspruchsrecht, wenn ein neuer Sub-AV hinzukommt?

Der EU AI Act schichtet ab August 2024 weitere Transparenzpflichten über diese bereits bestehenden DSGVO-Anforderungen — dazu später mehr.

Die gesetzlichen Pflichtklauseln nach Art. 28 DSGVO – Basisanforderungen

Was Art. 28 DSGVO konkret fordert

Art. 28 Abs. 3 DSGVO listet acht Mindestinhalte, die jeder AVV enthalten muss:

1. **Weisungsgebundenheit** des Auftragsverarbeiters: Der Anbieter darf Daten nur nach Ihren dokumentierten Weisungen verarbeiten.
2. **Vertraulichkeitsverpflichtung** aller autorisierten Personen beim Anbieter.
3. **Technische und organisatorische Maßnahmen (TOM)** gemäß Art. 32 DSGVO — mit konkretem Bezug, nicht nur einem Verweis.
4. **Regelung zu Sub-Auftragsverarbeitern:** Genehmigungspflicht (allgemein oder spezifisch), aktuelle Liste, Widerspruchsrecht.
5. **Unterstützung bei Betroffenenrechten** (Auskunft, Löschung, Berichtigung gemäß Art. 15–22 DSGVO).
6. **Lösch- und Rückgabepflicht** nach Vertragsende — auf Wahl des Verantwortlichen.
7. **Kontroll- und Auditrecht** des Verantwortlichen gegenüber dem Auftragsverarbeiter.
8. **Nachweis der Einhaltung** — der Anbieter muss nachweisen können, dass er die Vertragspflichten erfüllt.

Was in der Praxis häufig fehlt oder zu vage ist

TOM-Anhang als URL-Verweis: Viele Anbieter verweisen für die technischen und organisatorischen Maßnahmen lediglich auf eine externe Seite („siehe unsere Security-Seite unter example.com/security“). Diese URL kann sich jederzeit ändern — oder der Inhalt ändert sich, ohne dass Sie es merken. Besser: ein konkreter Anhang mit Versionsdatum, der Bestandteil des Vertrags ist.

Auditrecht auf Zertifikate reduziert: Häufig ersetzt der Anbieter das Vor-Ort-Auditrecht durch den Verweis auf Zertifizierungen (ISO 27001, SOC 2 Type II). Für KMU ist das in der Praxis oft akzeptabel — sofern die Zertifikate aktuell sind und auf Anfrage tatsächlich bereitgestellt werden. Kritisch wird es, wenn der Vertrag keinerlei Auditrecht vorsieht, auch nicht über Dritte.

Sub-AV-Liste ohne echtes Widerspruchsrecht: Der Europäische Datenschutzausschuss (EDSA) hat klargestellt: Ein Link auf eine „aktuell gültige Liste“ genügt nur dann, wenn ein echtes Widerspruchsrecht mit angemessener Vorankündigungsfrist verbunden ist. Viele Verträge formulieren dies so, dass ein Widerspruch zwar möglich ist, aber de facto zur Vertragskündigung führt — das ist kein echter Widerspruchsmechanismus.

KI-spezifische Zusatzklauseln – was Standard-AVVs nicht abdecken

Klausel 1 – Trainingsverbot / „No Training"-Verpflichtung

Das ist die wichtigste KI-spezifische Ergänzung. Ohne explizite Regelung kann ein Anbieter Ihre Eingaben und Ausgaben für Modellverbesserungen verwenden.

Musterformulierung (kein Rechtsbeistand, zur Orientierung):

> „Der Auftragsverarbeiter verpflichtet sich, die vom Verantwortlichen übermittelten Eingabedaten, Ausgabedaten und sonstigen Verarbeitungsartefakte ausschließlich zur Erbringung des vertraglich vereinbarten Dienstes zu verwenden und nicht zum Training, Fine-Tuning oder zur Evaluierung von KI-Modellen zu nutzen."

Wichtig: Bei manchen Anbietern ist ein Trainingsverbot nur in kostenpflichtigen Enterprise-Tarifen verfügbar. Der kostenlose oder günstige Business-Tarif enthält diese Zusicherung häufig nicht — prüfen Sie das explizit in den Vertragsdokumenten, nicht nur in Marketingmaterialien.

Klausel 2 – Drittland-Absicherung (SCCs + TIA)

Standard-Vertragsklauseln nach Art. 46 DSGVO (Modulset 2 für Verantwortlicher → Auftragsverarbeiter) sind die Mindestanforderung für US-Anbieter. Das allein reicht nach dem Schrems-II-Urteil des EuGH nicht aus.

Zusätzlich brauchen Sie ein **Transfer Impact Assessment (TIA)**: eine dokumentierte Risikoeinschätzung, ob im Drittland ein gleichwertiges Schutzniveau besteht. Microsoft und Google stellen dafür vorausgefüllte TIA-Vorlagen bereit — diese ersetzen jedoch nicht Ihre unternehmensspezifische Einschätzung. Welche Datenkategorien übertragen Sie? Wie sensibel sind diese? Gibt es staatliche Zugriffsmöglichkeiten im Zielland (z. B. CLOUD Act)?

Das TIA muss dokumentiert und auf Anfrage einer Datenschutzbehörde vorlegbar sein.

Klausel 3 – Lösch- und Rückgabeverpflichtung mit KI-Kontext

Standard-Löschklauseln („Daten werden nach Vertragsende gelöscht") sind für klassische Datenverarbeitung ausreichend, bei KI aber oft zu unscharf. Was ist mit Embeddings, die aus Ihren Dokumenten erzeugt wurden? Was mit gecachten Modell-Outputs? Was mit Feintuning-Daten, falls Sie ein Modell angepasst haben?

Ergänzen Sie die Löschklausel explizit um: „einschließlich aller abgeleiteten Repräsentationen, Embeddings, gecachter Ausgaben und Modell-Checkpoints, die auf Basis der Daten des Verantwortlichen erstellt wurden."

Klausel 4 – Transparenz über automatisierte Entscheidungsfindung

Art. 22 DSGVO greift, wenn eine Entscheidung ausschließlich auf automatisierter Verarbeitung beruht und rechtliche oder ähnlich erhebliche Auswirkungen auf eine Person hat — klassische Beispiele: Kreditbewertung, automatisierte Bewerberselektion, Scoring.

Für die meisten KMU-Anwendungen (Textentwürfe, Analysen, interne Prozessunterstützung) greift Art. 22 nicht direkt. Sobald KI-Outputs aber zur Grundlage von Personalentscheidungen oder Bonitätsbewertungen werden, müssen Sie sicherstellen, dass der Anbieter die nötige Transparenz und die Möglichkeit zur menschlichen Überprüfung bereitstellt. Das sollte vertraglich festgehalten sein.

Anbieter-Check – Wie halten es OpenAI, Microsoft und Google konkret?

> Kein Rechtsbeistand. Die folgende Einschätzung basiert auf öffentlich zugänglichen Vertragsdokumenten zum Zeitpunkt der Recherche. Änderungen sind möglich — prüfen Sie die verlinkten Anbieterdokumente direkt.

OpenAI (ChatGPT Enterprise / API)

DPA vorhanden: Ja, für Enterprise-Tarife. Die API-Nutzung läuft über eigene Nutzungsbedingungen mit separatem Datenschutzzusatz.

SCCs: Vorhanden (EU SCCs Modul 2).

Trainingsverbot: In Enterprise- und API-Tarifen standardmäßig enthalten — das ist ein wesentlicher Unterschied zu kostenfreien Zugängen. Im kostenlosen ChatGPT-Zugang gilt kein Trainingsverbot.

Kritische Punkte: Die Sub-Auftragsverarbeiter-Liste von OpenAI ist umfangreich; Microsoft Azure fungiert als zentraler Infrastrukturprovider, was die Verarbeitungskette verlängert.

Empfehlung für KMU: Enterprise-Tarif für jede Verarbeitung personenbezogener Daten. Den API-Tarif nur mit explizit aktiviertem „zero data retention"-Setting nutzen — und das im internen Verfahrensverzeichnis dokumentieren.

Microsoft (Azure OpenAI / Copilot for Microsoft 365)

DPA: Geregelt über das „Microsoft Products and Services Data Protection Addendum" (DPA), das für alle kommerziellen Lizenzen gilt.

SCCs: Vorhanden, inkl. vorausgefülltem TIA-Framework.

Trainingsverbot: Explizit im DPA für Kundendaten verankert.

Audit: ISO 27001, SOC 2 Type II, BSI C5 — die BSI-C5-Zertifizierung ist speziell für deutsche Behörden und stark regulierte Branchen relevant und ein echtes Differenzierungsmerkmal.

Kritische Punkte: Die Produktlandschaft ist komplex. Microsoft 365 Copilot hat eigene Bedingungen, die von den Azure OpenAI-Bedingungen abweichen. Prüfen Sie für jedes Produkt separat. Die Checkliste zur Copilot-Aktivierung auf dieser Plattform gibt einen guten Überblick über die produktspezifischen Voraussetzungen.

Google (Workspace AI / Vertex AI)

DPA: Google Cloud Data Processing Addendum, separat für Google Workspace.

SCCs: Vorhanden.

Trainingsverbot: Für Workspace-Kundendaten explizit. Bei Vertex AI differenziert nach eingesetztem Dienst — im Einzelfall prüfen.

Besonderheit: Google bietet EU-Datenspeicherung (Standort Frankfurt / Niederlande) als Option an. Wenn Daten ausschließlich in der EU verarbeitet werden, entfällt das Drittland-Problem weitgehend — das ist ein erheblicher Vorteil für datenschutzkritische Anwendungen.

Kritische Punkte: Consumer-Dienste wie Gemini (kostenfreie Version) fallen ausdrücklich nicht unter das Google Cloud DPA. Stellen Sie sicher, dass Ihre Mitarbeiterinnen und Mitarbeiter keine Unternehmensdaten in diese Zugänge eingeben.

EU AI Act – Welche neuen Vertragsanforderungen kommen ab 2025?

Der EU AI Act tritt stufenweise in Kraft: Verbotene Praktiken gelten seit Februar 2025, die Pflichten für Anbieter von General Purpose AI (GPAI) ab August 2025. Für KMU als Nutzer („Deployer") entstehen dabei neue vertragliche Anforderungen, die über die DSGVO hinausgehen.

GPAI-Dokumentation: Anbieter von GPAI-Modellen müssen technische Dokumentation bereitstellen. Als Nutzer sollten Sie im Vertrag das Recht auf Zugang zu dieser Dokumentation festschreiben — insbesondere wenn Sie das Modell in eigene Anwendungen integrieren.

Hochrisiko-KI: Wenn Sie KI-Systeme in Hochrisikobereichen einsetzen (z. B. Personalentscheidungen, Kreditbewertung, kritische Infrastruktur), entstehen zusätzliche Pflichten zur Protokollierung und zur Vorlage von Konformitätserklärungen. Klären Sie vertraglich, wer diese Unterlagen erstellt und bereitstellt — Sie als Nutzer oder der Anbieter.

Transparenzanforderungen für KI-generierte Inhalte: Synthetische Audio-, Video- und Textinhalte müssen unter bestimmten Bedingungen als KI-generiert gekennzeichnet werden. Wenn Ihr Anbieter solche Inhalte erzeugt, sollten Sie vertraglich sicherstellen, dass entsprechende Markierungsfunktionen bereitgestellt werden.

Anpassungsklausel: Bestehende AVVs sollten eine Klausel enthalten, die beide Parteien verpflichtet, den Vertrag bei wesentlichen Änderungen der Rechtslage anzupassen. Das schützt Sie vor veralteten Vertragsgrundlagen, wenn neue EU AI Act-Pflichten in Kraft treten.

Einen strukturierten Überblick über die Gesamtpflichten des EU AI Act für KMU bietet der Artikel EU AI Act: Was müssen KMU jetzt wirklich tun?.

Checkliste – Ihr AVV mit KI-Anbietern in 10 Punkten

Verwenden Sie diese Liste als Grundlage für die Prüfung bestehender und neuer KI-Anbieterverträge:

- ☐ **Weisungsgebundenheit** explizit verankert (Art. 28 Abs. 3 lit. a DSGVO)
- ☐ **Trainingsverbot** für Eingabe- und Ausgabedaten schriftlich bestätigt
- ☐ **Sub-Auftragsverarbeiter-Liste** aktuell, zugänglich und mit echtem Widerspruchsrecht
- ☐ **TOM-Anhang** mit Versionsdatum — kein bloßer URL-Verweis auf externe Seite
- ☐ **SCCs (Modul 2)** für US-Anbieter vorhanden und unterzeichnet
- ☐ **Transfer Impact Assessment** dokumentiert und aktenkundig
- ☐ **Löschpflicht** umfasst ausdrücklich Embeddings, Caches und abgeleitete Repräsentationen
- ☐ **Auditrecht** vorhanden — oder akzeptierte Zertifikate (ISO 27001 / SOC 2 Type II) mit Nachweis der Aktualität
- ☐ **Unterstützung bei Betroffenenrechten** (Art. 15–22 DSGVO) vertraglich geregelt
- ☐ **Anpassungsklausel** für neue Rechtsanforderungen (EU AI Act, zukünftige DSGVO-Änderungen)

Praxis-Tipp – Was tun, wenn der Anbieter keinen anpassbaren Vertrag bietet?

Für KMU ist das die häufigere Realität: Viele SaaS-KI-Anbieter im Midmarket-Segment bieten ausschließlich Click-Through-AVVs ohne Verhandlungsspielraum. Take-it-or-leave-it.

In diesem Fall hilft eine ehrliche Risikoabwägung. Die entscheidende Frage ist nicht „Ist der Vertrag perfekt?“, sondern „Was verarbeite ich tatsächlich?“ Anonymisierte oder aggregierte Daten ohne Personenbezug stellen ein anderes Risiko dar als Klartext-Kundendaten mit Namen, Adressen oder Gesundheitsinformationen.

Technische Kompensationsmaßnahmen können Vertragslücken teilweise ausgleichen:

- Pseudonymisierung oder Anonymisierung vor der Prompt-Eingabe (ersetzen Sie Namen durch Platzhalter wie „Kunde A“)
- Keine Eingabe von Klarnamen, Adressen, Gesundheitsdaten oder Finanzdaten in Standard-Tools ohne Enterprise-AVV
- Interne Nutzungsrichtlinie mit klaren Verboten, kombiniert mit Mitarbeiterschulung — das schafft zumindest eine dokumentierte Sorgfaltspflicht

Wann Sie einen Anbieter ablehnen sollten: Wenn ein Anbieter keine SCCs vorweisen kann, kein Trainingsverbot bietet und keinerlei Auditrecht gewährt — und Sie planen, mit diesem Tool personenbezogene Daten zu verarbeiten — ist das in der Kombination ein klares Ausschlusskriterium. Einzelne Lücken lassen sich technisch kompensieren; alle drei gleichzeitig nicht.

Bevor Sie überhaupt in die Vertragsverhandlung oder -prüfung gehen, stellt sich eine vorgelagerte Frage: Welche Ihrer Unternehmensdaten sind datenschutzrechtlich kritisch — und welche können Sie bedenkenlos in KI-Systeme einbringen? Wer das nicht systematisch geklärt hat, optimiert den Vertrag für ein Problem, das eigentlich in der Datenstrategie liegt. Der Artikel KI-Workflows mit Unternehmensdaten absichern geht auf die technische Seite dieser Frage ein.

Nächste Schritte

Sie wissen jetzt, welche Klauseln Ihr KI-Anbietervertrag enthalten muss — und wo die häufigsten Lücken in Standardverträgen liegen. Die nächste Frage, die sich daraus ergibt, ist eine strategische: Welche Ihrer Unternehmensdaten sollten überhaupt in KI-Systeme einfließen — und in welcher Form?

Wer diese Grundlage nicht geklärt hat, riskiert, einen sorgfältig geprüften Vertrag für Daten abzuschließen, die gar nicht hätten eingegeben werden dürfen. Der sinnvollste nächste Schritt ist oft kein weiterer Artikel, sondern ein konkreter Blick auf die eigene Situation: Welche Tools sind im Einsatz, welche Daten fließen wohin — und wo bestehen tatsächlich Lücken? Im kostenlosen Erstgespräch mit Strukturaflow klären wir genau das, strukturiert und ohne Umwege.

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