// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

API-Verbindungen in KI-Workflows DSGVO-konform absichern

API-Keys, AVV, Datensparsamkeit: So sichern DACH-KMU ihre KI-API-Integrationen technisch und rechtlich ab — Schritt für Schritt.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
13. Juli 2026

ONLINE LESEN
https://wissen.strukturaflow.it.com/api-verbindungen-ki-workflow-dsgvo-absichern/

Ein Steuerberater in München automatisiert seine Mandantenkommunikation mit der OpenAI API. Jede Anfrage enthält Mandantenname, Steuernummer und Jahresumsatz — im Klartext, über einen US-amerikanischen Server, ohne Auftragsverarbeitungsvertrag. Was hier passiert, ist kein Kavaliersdelikt: Es handelt sich um eine Drittlandsübermittlung personenbezogener Daten ohne ausreichende Rechtsgrundlage, mit potenziell empfindlichen Bußgeldern und ohne Audit-Spur, falls es zu einem Vorfall kommt.

Das ist kein Einzelfall. Die meisten DACH-KMU integrieren KI-APIs, weil die Tools funktionieren — nicht weil der Datenschutzprozess geklärt ist. Die Dokumentation ist englischsprachig, die Rechtslage wirkt komplex, und der IT-Dienstleister hat gerade keine Zeit für eine Grundsatzdiskussion.

Dieser Artikel liefert eine durchgängige Anleitung — von der API-Key-Verwaltung bis zum AVV-Abschluss mit dem Drittanbieter. Die einzelnen Schritte sind ohne eigene IT-Abteilung umsetzbar, und wo Code helfen kann, finden Sie konkrete Beispiele.

Warum API-Verbindungen in KI-Workflows eine eigene DSGVO-Risikoklasse bilden

Bei klassischer SaaS-Nutzung — etwa einem Buchhaltungsprogramm in der Cloud — konfigurieren Sie eine Oberfläche. Bei API-gestützter KI-Integration schreiben Sie aktiv Daten in ein externes Modell. Der Unterschied ist juristisch und technisch erheblich.

Wann verarbeiten Sie personenbezogene Daten über eine KI-API? Immer dann, wenn Ihre Prompts oder die daran angehängten Dokumente Informationen enthalten, die sich auf identifizierbare natürliche Personen beziehen. Das schließt Namen, E-Mail-Adressen, Vertragsnummern und IP-Adressen ebenso ein wie indirekte Identifikatoren — etwa „der Mandant mit dem Elektroinstallationsbetrieb in Graz, 12 Mitarbeitende“. Anonymisierte Prompts, bei denen keinerlei Rückschluss auf Personen möglich ist, fallen nicht unter die DSGVO — in der Praxis ist diese Grenze jedoch selten eindeutig.

Wann wird ein KI-API-Anbieter zum Auftragsverarbeiter? Nach Art. 28 DSGVO dann, wenn er personenbezogene Daten in Ihrem Auftrag verarbeitet — also auf Ihre Weisung hin und für Ihre Zwecke. Das ist bei API-Integrationen regelmäßig der Fall. Konsequenz: Sie benötigen einen Auftragsverarbeitungsvertrag (AVV), bevor Sie personenbezogene Daten übertragen.

US-Anbieter wie OpenAI, Anthropic und Google verarbeiten Daten standardmäßig in den USA. Nach dem Schrems-II-Urteil sind solche Übermittlungen nur unter bestimmten Bedingungen zulässig — in der Praxis über EU-Standardvertragsklauseln (SCCs), die in das jeweilige Data Processing Addendum (DPA) des Anbieters eingebettet sein müssen. Zusätzliche technische und organisatorische Maßnahmen (TOMs) — darunter Pseudonymisierung — sind empfohlen, um das Restrisiko zu minimieren.

EU AI Act und DSGVO: Was überschneidet sich? Ab 2025/2026 greifen für Hochrisiko-KI-Systeme zusätzliche Transparenz- und Dokumentationspflichten nach dem EU AI Act. Für die meisten KMU-Anwendungsfälle — Textgenerierung, E-Mail-Automatisierung, Dokumentenanalyse — liegt kein Hochrisiko-System vor. Trotzdem empfiehlt sich eine Einordnung. Unser Artikel zum EU AI Act für KMU gibt einen kompakten Überblick, was ab wann gilt.

Schritt 1 – API-Keys sicher generieren, speichern und rotieren

Der häufigste Fehler bei KI-API-Integrationen ist gleichzeitig der einfachste zu vermeiden: der API-Key direkt im Code. Wer einen Key in ein Python-Script schreibt und das Repository auf GitHub pusht — auch ein privates — riskiert einen Leak. Automatisierte Scanner suchen aktiv nach solchen Mustern.

Die Grundregel: API-Keys gehören in Umgebungsvariablen, nicht in den Code.

Für DACH-KMU ohne komplexe Cloud-Infrastruktur ist `python-dotenv` ein pragmatischer Einstieg:

```
# .env-Datei (NICHT ins Repository committen!)
OPENAI_API_KEY=sk-...

# Python-Script
from dotenv import load_dotenv
import os
import openai

load_dotenv()
openai.api_key = os.getenv(„OPENAI_API_KEY“)
```

Stellen Sie sicher, dass `.env` in Ihrer `.gitignore`-Datei steht.

Für produktive Umgebungen empfehlen sich dedizierte Secret Manager. Für KMU ohne AWS- oder Azure-Infrastruktur ist **Bitwarden Secrets Manager** eine zugängliche Option mit europäischen Hosting-Möglichkeiten. HashiCorp Vault ist mächtiger, erfordert aber mehr Administrations-Aufwand.

Key-Rotation: Alle 90 Tage sollten Sie API-Keys erneuern. Bei einem Mitarbeiterwechsel — insbesondere wenn jemand Zugriff auf Credentials hatte — gilt: sofort rotieren, nicht beim nächsten Wartungsfenster.

Least-Privilege-Prinzip: Verwenden Sie separate Keys für separate Anwendungsfälle. Ein Key für das Kundensupport-System, ein anderer für die interne Dokumentenanalyse. So begrenzen Sie den Schaden bei einem Leak auf einen Teilbereich.

Praktisches Beispiel: API-Key-Verwaltung in Make- und n8n-Workflows

In **Make.com** (ehemals Integromat) werden API-Credentials in der Verbindungsverwaltung gespeichert — auf Servern in den USA. Wer Make für Workflows mit personenbezogenen Daten nutzt, sollte das im Verfahrensverzeichnis und im AVV-Prozess berücksichtigen.

n8n bietet hier einen strukturellen Vorteil: Als self-hosted Lösung laufen Credentials und Workflow-Daten auf Ihrem eigenen Server — in der EU, unter Ihrer Kontrolle. Der Aufwand ist höher, die Datenschutz-Ausgangslage aber klar besser. Einen direkten Vergleich der beiden Plattformen finden Sie in unserem Artikel n8n vs. Zapier.

Fünf-Schritte-Prozess zur DSGVO-konformen Integration von KI-APIs: von der sicheren Key-Verwaltung über Transport-Verschlüsselung und Datensparsamkeit bis zum Vertragsabschluss und laufenden Monitoring. Der erste Schritt (sichere Key-Speicherung) ist hervorgehoben als kritischster Punkt.

Schritt 2 – Transport-Sicherheit: TLS, HTTPS und was KMU konkret prüfen müssen

Alle gängigen KI-APIs — OpenAI, Anthropic, Google — erzwingen HTTPS. Das ist der Mindeststandard, aber kein Garant für eine sicher konfigurierte Verbindung.

TLS-Versionen: TLS 1.0 und 1.1 gelten als veraltet und unsicher. TLS 1.2 ist das Minimum, TLS 1.3 der aktuelle Empfehlungsstandard. Die meisten modernen Python-Bibliotheken (requests, httpx) nutzen automatisch TLS 1.2+. Prüfen lässt sich das mit einem einfachen curl-Befehl:

```
curl -v https://api.openai.com/v1/models 2>&1 | grep „SSL connection“
```

Die Ausgabe zeigt die ausgehandelte TLS-Version.

Certificate Pinning — also das Fixieren des erwarteten Server-Zertifikats im Client — ist für die meisten KMU-Anwendungen Overkill. Es erhöht den Wartungsaufwand (jedes Zertifikats-Renewal kann Probleme verursachen) und bringt erst dann messbaren Sicherheitsgewinn, wenn ein gezielter Man-in-the-Middle-Angriff realistisch ist.

Corporate Proxies sind ein echtes Risiko: Viele Unternehmen leiten HTTPS-Traffic über interne Proxies zur Inspektion — dabei wird TLS aufgebrochen und neu aufgebaut. Wenn Ihr Proxy nicht korrekt konfiguriert ist, können Zertifikatsfehler auftreten, die Python-Bibliotheken stillschweigend ignorieren. Prüfen Sie, ob in Ihrer Umgebung `REQUESTS_CA_BUNDLE` oder ähnliche Variablen gesetzt sind, und ob die API-Calls wirklich end-to-end verschlüsselt ankommen.

Für eine schnelle Überprüfung der TLS-Konfiguration eignet sich SSL Labs — primär für eigene Server, aber auch nützlich, um den Status bekannter API-Endpunkte zu prüfen.

Schritt 3 – Datensparsamkeit: Was darf in den Prompt, was nicht?

Art. 5 Abs. 1 lit. c DSGVO — das Prinzip der Datensparsamkeit — gilt uneingeschränkt auch für KI-Prompts. Nur Daten, die für den konkreten Verarbeitungszweck tatsächlich notwendig sind, dürfen übertragen werden.

Problematische Datentypen in Prompts: - Klarnamen kombiniert mit anderen Identifikatoren (Adresse, Geburtsdatum) - Finanzielle Informationen mit Personenbezug (Kontonummern, Jahresumsätze einzelner Personen) - Gesundheitsdaten (besondere Kategorie nach Art. 9 DSGVO — besonders streng) - HR-Daten (Gehaltsangaben, Krankheitstage, Performancebewertungen)

Pseudonymisierung vor dem API-Call ist die wirksamste Maßnahme. Die Idee: Sie ersetzen personenbezogene Angaben vor der Übertragung durch künstliche Identifikatoren — das Mapping von Original auf Pseudonym speichern Sie lokal.

```
import hashlib
import openai
import os

# Lokales Mapping (in der Praxis: sichere Datenbank verwenden)
pseudonym_map = {}

def pseudonymize(value: str) -> str:
    „“„Erstellt einen konsistenten, nicht umkehrbaren Pseudonym-Hash.“„“
    hashed = hashlib.sha256(value.encode()).hexdigest()[:12]
    pseudonym_map[hashed] = value  # Nur lokal speichern!
    return f„PERSON_{hashed}“

# Originaldaten
mandant_name = „Maria Mustermann“
anliegen = „Frage zur Umsatzsteuer-Vorauszahlung Q3“

# Pseudonymisierung vor dem API-Call
pseudo_name = pseudonymize(mandant_name)
prompt = f„Beantworte folgende Anfrage von {pseudo_name}: {anliegen}“

# API-Call ohne Klarnamen
client = openai.OpenAI(api_key=os.getenv(„OPENAI_API_KEY“))
response = client.chat.completions.create(
    model=„gpt-4o“,
    messages=[{„role“: „user“, „content“: prompt}]
)

print(response.choices[0].message.content)
```

Gesundheitswesen und HR-Automatisierung sind Hochrisikobereiche: Daten nach Art. 9 DSGVO (Gesundheit, Gewerkschaftszugehörigkeit, biometrische Daten) unterliegen erhöhten Anforderungen. Eine Pseudonymisierung allein reicht hier oft nicht aus — in vielen Fällen ist eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO erforderlich, bevor Sie den Workflow in Betrieb nehmen.

Was tun, wenn Nutzer-Input unstrukturierte personenbezogene Daten enthält?

Wenn Endnutzer frei in ein Textfeld tippen können, geben sie früher oder später Daten ein, die sie nicht eingeben sollten — Namen von Dritten, Krankengeschichten, Kreditkartennummern. Zwei Schutzebenen helfen:

Input-Validierung: Reguläre Ausdrücke oder NER-Bibliotheken (Named Entity Recognition) können bekannte Muster wie IBAN, Sozialversicherungsnummern oder E-Mail-Adressen erkennen und vor der Weiterverarbeitung blockieren oder maskieren.

OpenAI Moderation API: Für Inhaltsmoderation gedacht, aber auch nützlich als vorgeschalteter Filter. Sie können Nutzer-Inputs zuerst durch die Moderation API schicken und bei auffälligen Mustern die Verarbeitung stoppen.

Schritt 4 – Auftragsverarbeitungsvertrag (AVV) mit KI-API-Anbietern

Der AVV nach Art. 28 DSGVO ist kein bürokratisches Beiwerk — er ist die rechtliche Grundlage dafür, dass Sie personenbezogene Daten überhaupt an einen externen Dienstleister weitergeben dürfen. Ohne AVV ist die Übermittlung unzulässig, Punkt.

Wie funktioniert das in der Praxis?

Die großen KI-Anbieter stellen standardisierte Data Processing Addenda (DPAs) bereit, die Sie online akzeptieren können:

- **OpenAI:** Das DPA findet sich in den Unternehmens-Kontoeinstellungen (API > Data Controls). Es enthält EU-SCCs, schließt aber das Modelltraining mit Ihren Daten standardmäßig aus — vorausgesetzt, Sie haben das opt-out aktiviert (mehr dazu im Abschnitt „Häufigste Fehler“).
- **Anthropic:** Stellt ein DPA auf Anfrage bereit; für Teams und Enterprise-Pläne ist es direkt verfügbar. Die Datenverarbeitung findet primär in den USA statt.
- **Azure OpenAI Service:** Microsoft verarbeitet Daten in EU-Rechenzentren, wenn Sie die entsprechende Azure-Region wählen. Das macht Azure OpenAI für viele DACH-KMU zur datenschutzrechtlich unkompliziertesten Option — zu einem etwas höheren operativen Aufwand.
- **Google Vertex AI:** Bietet EU-Datenresidenz für bestimmte Modelle; das DPA ist im Google Cloud DPA enthalten.

Mindestinhalte eines AVV mit KI-Anbieter (Checkliste):

1. Gegenstand und Dauer der Verarbeitung
2. Art und Zweck der Verarbeitung
3. Kategorien der verarbeiteten personenbezogenen Daten
4. Pflichten und Rechte des Verantwortlichen (Sie)
5. Weisungsgebundenheit des Auftragsverarbeiters
6. Regelung zu Unterauftragsverarbeitern (wichtig: OpenAI nutzt Microsoft Azure als Infrastruktur)
7. Technische und organisatorische Maßnahmen (TOMs)

Fehlt einer dieser Punkte oder ist der AVV nicht rechtswirksam abgeschlossen, ist die gesamte Datenübermittlung angreifbar. Bei US-Anbietern ohne explizite EU-Datenresidenz kommen zusätzlich die EU-SCCs als Grundlage für die Drittlandsübermittlung hinzu.

Wer grundsätzlich weniger abhängig von einzelnen US-KI-Anbietern werden möchte, findet in unserem Artikel zur digitalen Souveränität und Anbieter-Unabhängigkeit einen strukturierten Einstieg.

Schritt 5 – Monitoring und Audit-Logging von API-Calls

Die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO verlangt, dass Sie nachweisen können, wie personenbezogene Daten verarbeitet wurden. Das gilt auch für API-Calls an KI-Systeme.

Was geloggt werden muss — und was nicht:

Loggen Sie: Zeitstempel, API-Endpunkt, verwendetes Modell, HTTP-Statuscode, Anzahl der Token, aufrufende Anwendung oder Nutzer-ID.

Nicht loggen: Den vollständigen Prompt mit personenbezogenen Daten. Das würde eine zweite, unkontrollierte Kopie dieser Daten in Ihren Log-Systemen erzeugen.

```
import logging
import time
import openai
import os

# Strukturiertes Logging ohne personenbezogene Daten
logging.basicConfig(
    level=logging.INFO,
    format='%(asctime)s %(levelname)s %(message)s'
)
logger = logging.getLogger(„ki_api_audit“)

def call_openai_with_logging(model: str, token_estimate: int, use_case: str) -> dict:
    start = time.time()
    try:
        client = openai.OpenAI(api_key=os.getenv(„OPENAI_API_KEY“))
        response = client.chat.completions.create(
            model=model,
            messages=[{„role“: „user“, „content“: „[PSEUDONYMISIERTER PROMPT]“}]
        )
        duration = round(time.time() - start, 3)
        logger.info({
            „event“: „api_call_success“,
            „model“: model,
            „use_case“: use_case,
            „duration_s“: duration,
            „tokens_used“: response.usage.total_tokens,
            „status“: „200“
        })
        return response
    except openai.APIError as e:
        logger.error({
            „event“: „api_call_error“,
            „model“: model,
            „use_case“: use_case,
            „error_code“: e.status_code,
        })
        raise
```

Log-Aufbewahrungsfristen: 30 Tage für risikoarme Workflows, 90 Tage für Anwendungen mit sensibleren Daten. Definieren Sie die Frist schriftlich — im Verfahrensverzeichnis.

Tools für KMU: Wer LLM-Workflows überwachen will, ohne ELK Stack aufzusetzen, findet in **Langfuse** (open source, self-hostbar) eine praxistaugliche Lösung — speziell für LLM-Monitoring gebaut, mit Token-Tracking, Latenz-Metriken und Trace-Ansichten. **Highlight.io** ist eine weitere Option für allgemeines Application-Monitoring.

Audit-Logs und API-Dokumentation sollten auf europäischer Infrastruktur gespeichert werden. Nextcloud Hub eignet sich als selbstgehostete Ablage für Dokumentation, Verfahrensverzeichnisse und Logs — DSGVO-konform und ohne US-Drittlandsübermittlung.

Anomalie-Erkennung: Eine ungewöhnlich hohe API-Call-Frequenz — etwa 10x das Tagesdurchschnitt-Volumen in einer Stunde — kann auf ein kompromittiertes API-Credential oder eine fehlerhafte Schleife im Workflow hinweisen. Setzen Sie Rate-Limits auf Ebene der Anbieter-Konsole und konfigurieren Sie Alerts bei Schwellwertüberschreitungen.

Was im Falle eines Sicherheitsvorfalls zu tun ist (72-Stunden-Frist nach Art. 33 DSGVO)

Wenn personenbezogene Daten durch einen API-Leak, ein kompromittiertes Credential oder eine fehlerhafte Konfiguration unbefugt zugänglich wurden, gilt: Prüfen Sie sofort, ob eine meldepflichtige Datenpanne vorliegt.

Die Meldepflicht greift, wenn ein Risiko für die Rechte und Freiheiten natürlicher Personen nicht auszuschließen ist. Die Frist: 72 Stunden ab Kenntnis des Vorfalls.

Zuständige Aufsichtsbehörden im DACH-Raum: - **Deutschland:** Zuständig ist die Behörde des Bundeslandes, in dem Ihr Unternehmen seinen Sitz hat — z.B. das BayLDA für Bayern, der LfDI für Baden-Württemberg. - **Österreich:** Datenschutzbehörde (DSB) in Wien. - **Schweiz:** Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB) — die CH gilt als Drittland für DSGVO-Zwecke, hat aber ein ähnliches Datenschutzregime.

Die häufigsten Fehler in DACH-KMU – und wie Sie sie vermeiden

1. API-Key direkt im Frontend-Code JavaScript im Browser ist für jeden lesbar — ein dort eingebetteter API-Key ist öffentlich. Lösung: API-Calls immer über ein Backend (Node.js, Python-Server) routen, nie direkt aus dem Frontend.

2. Kein AVV mit US-Anbieter abgeschlossen Das DPA von OpenAI gilt nicht automatisch — Sie müssen es aktiv akzeptieren, meist über die Konsoleneinstellungen. Prüfen Sie für jeden Anbieter, ob ein gültiger AVV vorliegt.

3. Produktionsdaten zum Testen verwendet Wenn Sie einen neuen Prompt entwickeln, verwenden Sie synthetische oder anonymisierte Testdaten — niemals echte Mandanten- oder Kundendaten. Das ist nicht nur ein DSGVO-Risiko, sondern auch ein professioneller Standard.

4. Keine Datensparsamkeit beim Prompt-Design Vollständige Kundendatensätze in den Prompt zu kopieren, weil es einfacher ist, ist ein Fehler. Übertragen Sie nur die Felder, die der Workflow tatsächlich benötigt.

5. Logging deaktiviert aus Performanzgründen Logging verlangsamt Anwendungen messbar — aber ohne Log-Spur können Sie weder DSGVO-Rechenschaftspflichten erfüllen noch Sicherheitsvorfälle rekonstruieren. Strukturiertes, schlankes Logging (wie im Beispiel oben) ist kein Performanz-Killer.

6. Keine Zugriffsbeschränkung auf API-Credentials im Team Wenn drei Mitarbeitende denselben API-Key kennen und einer das Unternehmen verlässt, müssen Sie rotieren — aber wissen Sie, wer noch Zugriff hatte? Verwenden Sie Credential-Management-Systeme mit Rollen und Zugriffsprotokollen. Nextcloud bietet als selbstgehostete Plattform sichere Möglichkeiten zur Ablage und Versionierung sensibler Konfigurationsdokumente.

7. OpenAI-Modelltraining nicht opt-out gesetzt Standardmäßig kann OpenAI API-Daten zur Modellverbesserung nutzen — sofern Sie das nicht deaktiviert haben. In der API-Plattform unter „Data Controls" können Sie das Training mit Ihren Daten abschalten. Für jede Produktivintegration mit personenbezogenen Daten ist das Pflicht, keine Option.

8. Kein Eintrag im Verfahrensverzeichnis Jede Verarbeitung personenbezogener Daten muss nach Art. 30 DSGVO dokumentiert werden — auch API-gestützte KI-Workflows. Fehlt der Eintrag, fehlt die Grundlage für jede Aufsichtsbehörden-Anfrage.

Praxis-Tipp: Sicherheits-Audit Ihrer bestehenden KI-API-Integration in 60 Minuten

Sie nutzen bereits KI-APIs und wollen den aktuellen Stand einschätzen? Dieser Selbst-Check gibt Ihnen in fünf Schritten ein klares Bild:

Schritt 1: API-Key-Inventar erstellen Listen Sie alle KI-API-Keys auf, die in Ihrem Unternehmen aktiv sind. Wer hat Zugriff? Wo sind die Keys gespeichert? Gibt es Keys im Code oder in Slack-Nachrichten? Dieses Inventar ist die Grundlage für alles Weitere.

Schritt 2: AVV-Status bei jedem Anbieter prüfen Öffnen Sie die Konsoleneinstellungen jedes genutzten Anbieters (OpenAI, Anthropic, Google, Microsoft). Ist ein DPA/AVV aktiv akzeptiert? Wenn Sie die Antwort nicht sicher wissen, ist das die Antwort.

Schritt 3: Einen exemplarischen API-Call auf personenbezogene Daten analysieren Wählen Sie einen typischen Workflow und analysieren Sie den tatsächlich übertragenen Prompt. Welche Datenfelder sind enthalten? Sind sie für den Verarbeitungszweck notwendig? Könnten Sie Felder weglassen oder pseudonymisieren?

Schritt 4: Log-Konfiguration überprüfen Werden API-Calls geloggt? Wo werden die Logs gespeichert? Wie lange werden sie aufbewahrt? Enthalten die Logs personenbezogene Daten, die dort nicht sein sollten?

Schritt 5: Ergebnis im Verfahrensverzeichnis dokumentieren Tragen Sie den KI-API-Workflow in Ihr Verarbeitungsverzeichnis nach Art. 30 DSGVO ein — mit Zweck, Datenkategorien, Anbieter, Rechtsgrundlage und TOMs. Wenn dieses Verzeichnis noch nicht existiert, ist das der dringlichste Handlungspunkt.

Wenn Sie diesen Audit durchgeführt haben und offene Fragen bleiben — insbesondere zur rechtlichen Einordnung Ihres konkreten Use Cases oder zur technischen Umsetzung in Ihrem Workflow — lohnt sich ein strukturiertes Gespräch mit jemandem, der beide Seiten kennt.

FAQ

Muss ich für jede KI-API einen eigenen Auftragsverarbeitungsvertrag abschließen? Ja, sofern personenbezogene Daten verarbeitet werden — für jeden Anbieter separat. Viele große Anbieter stellen standardisierte DPAs bereit, die Sie online akzeptieren können. Das reicht in vielen Fällen als AVV-Grundlage aus, sofern der Inhalt die Mindestanforderungen des Art. 28 DSGVO erfüllt.

Ist die Nutzung von OpenAI in Deutschland überhaupt DSGVO-konform möglich? Unter bestimmten Voraussetzungen ja: mit abgeschlossenem DPA, deaktiviertem Modelltraining und Pseudonymisierung der Eingabedaten. Eine pauschale Aussage ist nach aktueller Rechtslage nicht möglich — die Risikoabwägung hängt vom Einzelfall ab. Unser Artikel zu DSGVO und ChatGPT im Unternehmen geht auf die konkreten Bedingungen ein.

Was passiert, wenn ich versehentlich personenbezogene Daten in einem Prompt an eine KI-API gesendet habe? Prüfen Sie zunächst, ob eine Datenpanne im Sinne von Art. 33 DSGVO vorliegt. Entscheidend ist: Besteht ein Risiko für die Rechte und Freiheiten der betroffenen Personen? Bei hohem Risiko gilt eine 72-Stunden-Meldepflicht gegenüber der zuständigen Aufsichtsbehörde.