ZeoAI
Klarheit schafft KI-Erfolg

CORIDAS
DSGVO Erste Hilfe Koffer

PRAXIS-REPORT 2026

DSGVO & EU AI ACT

Orientierung. Pflichten. Nächste Schritte.

Für Selbständige und inhabergeführte Unternehmen
mit 1-100 Mitarbeitenden in Deutschland



Corinna Göring
Geschäftsführerin · CORIDAS

Savas Kozluklu
Gründer & Inhaber · ZeoAI

AGENDA

Was Sie in diesem Report erwartet

Sechs Kapitel, ein Fahrplan, zwei Checklisten. Klicken Sie auf einen Eintrag, um direkt dorthin zu springen.

– **Warum dieser Report** 3
Vom Podcast in die Praxis

– **Über uns** 4
Corinna Göring (CORIDAS) und Savas Kozluklu (ZeoAI)

– **Das Wichtigste auf einer Seite** 5
Vier Grundbedingungen für rechtssichere KI

1 **Das eigentliche Problem: Schatten-KI** 6
Die Lage in Zahlen, drei Wege, sechs Datenkanäle

2 **Was wirklich gilt: DSGVO und EU AI Act** 8
Pflichten, Fristen, Bußgelder und persönliche Haftung

3 **Wo Ihre Daten landen** 11
Tarif statt Modell, Drittlandtransfer, sechs typische Fehler

4 **Ihr Fahrplan in sieben Schritten** 13
Drei Schichten, sieben Schritte, zwei Checklisten

5 **Acht Anwendungen, die sauber laufen** 17
Use Cases und die laufenden Pflichten im Betrieb

6 **Ehrliche Grenzen** 19
Restrisiko, selbst machen oder begleiten lassen

– **Fazit: Aus Pflicht wird Vorsprung** 21
Drei Stufen und Ihre 90-Tage-Prioritäten

– **So unterstützen wir Sie** 22
CORIDAS und ZeoAI, Kontakt und Podcast

– **Quellen und rechtlicher Hinweis** 23
Stand Oktober 2026

GUT ZU WISSEN

Begleitmaterial zum Podcast „Kann KI kreativ sein, wenn der AI Act mitredet?“

Dieser Report ist der Bonus zu unserer gemeinsamen Podcast-Folge. Was wir dort im Gespräch angerissen haben, finden Sie hier zum Nachlesen, mit Zahlen, Fristen und konkreten Schritten zum Abhaken.

VORWORT

Warum dieser Report

Mehr KI, weniger Risiko: so nutzen Sie KI, ohne ins Rechtsrisiko zu laufen

KI ist in deutschen Unternehmen angekommen. Die Rechtssicherheit noch nicht. Genau diese Lücke schließt dieser Report, damit Sie KI einsetzen und Ihre Zukunftsprojekte nicht aus Unsicherheit bremsen.

Der Druck ist real: **57 % der Unternehmen ab 20 Beschäftigten nutzen inzwischen KI**, vor einem Jahr waren es 36 %, vor zwei Jahren 20 % (Bitkom, September 2026). Ihre Wettbewerber testen längst, was KI bei Angeboten, im Kundenservice und in der Verwaltung spart.

Gleichzeitig bremst die Unsicherheit. Für Unternehmen, die KI bereits nutzen, sind die **Anforderungen an den Datenschutz das größte Hemmnis (66 %)**, 56 % nennen rechtliche Unsicherheit. Die Folge ist ein teurer Stillstand: Entweder wird KI verboten und wandert in den Untergrund, oder sie läuft ungesteuert weiter. Beides erhöht das Risiko. Dieser Report zeigt Ihnen den dritten Weg: **KI bewusst steuern.**

Für wen dieser Report ist

Sie sind selbstständig oder führen ein inhabergeführtes Unternehmen mit 1 bis 100 Mitarbeitenden. Ihr Alltag ist voll, und irgendwo tippt vielleicht gerade jemand einen Kundennamen oder einen Vertragsentwurf in ein kostenloses KI-Tool, ohne zu fragen. Sie wollen die Produktivität, aber nicht die Schlagzeile.

Wenn Sie spüren, dass KI in Ihrem Betrieb längst genutzt wird, nur eben unkontrolliert, und Sie daraus ein steuerbares, rechtssicheres System machen wollen, dann ist dieser Report für Sie. Er ersetzt keine Rechtsberatung. Aber er gibt Ihnen die Übersicht, mit der Sie die richtigen Entscheidungen treffen und die richtigen Fragen stellen.

So arbeiten Sie damit

Kapitel 1 bis 3 klären die Lage und die Rechtsgrundlagen. Ab Kapitel 4 wird es konkret: sieben Schritte, zwei Checklisten und acht Anwendungsfälle aus der Praxis. Wer wenig Zeit hat, liest zuerst die Seite **„Das Wichtigste auf einer Seite“** und das Fazit.

> TIPP
>
> **Warum Datenschutz und KI zusammengehören**
>
> Erfolgreich macht Sie selten das teuerste Tool. Entscheidend ist die richtige Reihenfolge: erst Regeln und Verträge, dann Technik. Deshalb haben wir diesen Report zu zweit geschrieben: Corinna Göring bringt rund 40 Jahre IT- und Datenschutzpraxis für kleine Unternehmen mit, Savas Kozluklu die KI-Umsetzung für inhabergeführte Betriebe.

ÜBER UNS

Zwei Perspektiven, ein Ziel

Datenschutz, der gelebt wird, und KI, die wirklich entlastet

Datenschutz ohne KI-Verständnis bremst. KI ohne Datenschutz wird teuer. Wir verbinden beides, praxisnah und auf Augenhöhe mit Selbstständigen und inhabergeführten Unternehmen.



Corinna Göring

GESCHÄFTSFÜHRERIN · CORIDAS GMBH

Corinna Göring ist seit 1986 in der IT zu Hause. 26 Jahre lang führte sie ein IT-Systemhaus und betreute vor allem kleine Unternehmen und Handwerksbetriebe in IT, Datensicherheit und Datenschutz. Als erfahrene Datenschutzbeauftragte sah sie 2016 das Problem: Für Einzelunternehmer und kleine Betriebe gab es keine praxistaugliche DSGVO-Lösung.

Also hat sie eine gebaut: den **DSGVO Erste Hilfe Koffer**. Seit den ersten Kundeneinsätzen 2017 setzen damit Hunderte Unternehmen ihren Datenschutz um, gemeinsam mit einem Berater, in rund vier Stunden. Ihr Motto: **Vertrauen verkauft besser als Rabatt.**

- Gastgeberin des Podcasts **„Datenschutz im OHR“** für Solo-Selbstständige und Kleinunternehmen
- Spezialisiert auf Solo-Selbstständige, kleine Firmen und Handwerksbetriebe
- Lizenzpartner-System seit 2022, Kundenbewertung 4,93 von 5 (ProvenExpert)

→ **dsgvo-erste-hilfe.de**



Savas Kozluklu (MBA)

GRÜNDER & CEO · ZEOAI

Savas Kozluklu hat mit 13 Jahren programmieren gelernt, ein Adventure-Spiel mit If-Then-Else-Logik, der Grundlage regelbasierter KI. Danach folgten über 26 Jahre in Führung, Vertrieb und Beratung, unter anderem bei SAP, SHS Viveon und Cubeware. 2021 gründete er TAXCAREER, eine KI-gestützte Recruiting-Plattform, noch vor ChatGPT.

Mit **ZeoAI** führt er inhabergeführte Unternehmen mit 1 bis 100 Mitarbeitenden aus der KI-Unklarheit in die Handlungsfähigkeit: mit Strategie, Struktur und messbaren Ergebnissen. **Ohne Buzzwords. Ohne Blackbox.**

- KI-Potenzialanalyse, Umsetzung in 30 bis 90 Tagen, externe KI-Abteilung und externer Chief AI Officer
- KI-Kompetenz-Schulungen nach Art. 4 AI Act mit Teilnahmebestätigung
- Claim: **Klarheit schafft KI-Erfolg**
- Kundenbewertung 5,0 von 5 bei 35 Bewertungen (Trustmarkt, agenturmarkt.de)

→ **zeoai.de**

GUT ZU WISSEN

Warum wir gemeinsam schreiben

CORIDAS sorgt dafür, dass das Fundament steht: Verzeichnis, Verträge, Informationspflichten, technische und organisatorische Maßnahmen. ZeoAI sorgt dafür, dass KI auf diesem Fundament produktiv läuft. Beides zusammen ergibt das, was dieser Report beschreibt: **KI, die entlastet und rechtssicher ist.**

DAS WICHTIGSTE AUF EINER SEITE (MANAGEMENT-SUMMARY)

Ja, KI geht rechtssicher

Vier Grundbedingungen, sechs Kapitel, ein Fahrplan

Die Kernantwort vorab: Ja, Sie können KI DSGVO-konform einsetzen, wenn Ihr Unternehmen vier Grundbedingungen erfüllt. Sie sind der Mindeststandard, auf dem alles Weitere aufbaut.

#	GRUNDBEDINGUNG	WAS DAS KONKRET HEISST
1	**Vertrag nach Art. 28 DSGVO**	Verarbeitet ein Anbieter personenbezogene Daten in Ihrem Auftrag, brauchen Sie einen Auftragsverarbeitungsvertrag (AVV). Andere Rollen, etwa gemeinsame Verantwortung, regeln Sie gesondert.
2	**Rechtsgrundlage und Zweck**	Für jeden Verarbeitungsschritt mit Personendaten dokumentieren Sie eine Rechtsgrundlage und einen klaren Zweck.
3	**Nichts Persönliches in offene Systeme**	Kundendaten, Bewerbungen und Geschäftsgeheimnisse gehören nie in kostenlose Privat-Accounts ohne Vertrag.
4	**Der Mensch entscheidet**	Hat eine Entscheidung rechtliche Wirkung für Menschen (Art. 22 DSGVO), entscheidet am Ende ein Mensch mit echtem Spielraum.

Dazu kommt der EU AI Act: Seit Februar 2025 müssen Unternehmen, die KI nutzen, Maßnahmen zur **KI-Kompetenz** ihrer Mitarbeitenden ergreifen (Art. 4). Der Digital Omnibus hat den Wortlaut im Juli 2026 entschärft, die Pflicht aber nicht gestrichen. Je nach Einsatz kommen weitere Pflichten hinzu, etwa Datenschutz-Folgenabschätzung, Kennzeichnung von KI-Inhalten, Prüfung von Drittlandtransfers oder die Beteiligung des Betriebsrats.

Was Sie in den sechs Kapiteln erwartet

1. **Das eigentliche Problem.** Die Lage in Zahlen, der Teufelskreis und die Kanäle des Datenabflusses.
2. **Was wirklich gilt.** DSGVO und AI Act für Anwender, Fristen, Bußgelder und persönliche Haftung.
3. **Wo Ihre Daten landen.** Tarife im Vergleich, Drittlandtransfer und sechs typische Fehler.
4. **Ihr Fahrplan.** Drei Schichten, sieben Schritte, zwei Checklisten, Prioritäten nach Betriebsgröße.
5. **Konforme Anwendungen.** Acht Use Cases und die laufenden Pflichten im Betrieb.
6. **Ehrliche Grenzen.** Was ein sauberes Setup leistet, was bleibt und wo Hilfe sinnvoll ist.

KAPITEL 1

Das eigentliche Problem: Schatten-KI

Wo kleine und mittlere Unternehmen bei KI wirklich stehen

Die Frage, ob KI in Ihr Unternehmen kommt, ist längst entschieden, nur oft nicht von Ihnen. Offen ist nur noch, ob das kontrolliert oder unkontrolliert passiert.

Die Lage in vier Zahlen

57 %
der Unternehmen ab 20 Beschäftigten nutzen KI (Vorjahr 36 %)
Bitkom, Sep. 2026

42 %
berichten oder vermuten private KI-Nutzung ihrer Beschäftigten
Bitkom, Okt. 2025

66 %
der KI-Nutzer sehen Datenschutz als größtes Hemmnis
Bitkom, Sep. 2026

~ 1/4
der Unternehmen haben Regeln für den KI-Einsatz
Bitkom, Okt. 2025

Die Zahlen hängen an derselben Ursache: **Niemand steuert, wer KI wie und mit welchen Daten nutzt.** Laut Institut der deutschen Wirtschaft verwenden 29 % der Beschäftigten, die beruflich KI nutzen, Werkzeuge, die ihr Arbeitgeber gar nicht bereitgestellt hat (IW-Kurzbericht 63/2026). Und bei Beschäftigten, die generative KI nutzen, haben 77 % schon Daten in ein KI-Tool kopiert, 82 % dieser Eingaben liefen über private, nicht verwaltete Accounts (LayerX, Okt. 2025).

> **GUT ZU WISSEN**
> Die Bitkom-Zahlen beziehen sich auf Unternehmen ab 20 Beschäftigten. In kleineren Betrieben ist die Lage nicht entspannter, sondern meist undurchsichtiger: Es gibt selten eine IT-Abteilung, die mitbekommt, welche Tools genutzt werden.

Verbieten, laufen lassen oder steuern

Schatten-KI ist jede KI-Nutzung, die an klaren Regeln vorbeiläuft: der Vertragsentwurf, der zur Prüfung in ChatGPT wandert, das private Tool für Meeting-Protokolle. Kein böser Wille, nur der Versuch, schneller fertig zu werden. Für den Umgang damit gibt es drei Wege, zwei davon vergrößern das Risiko.

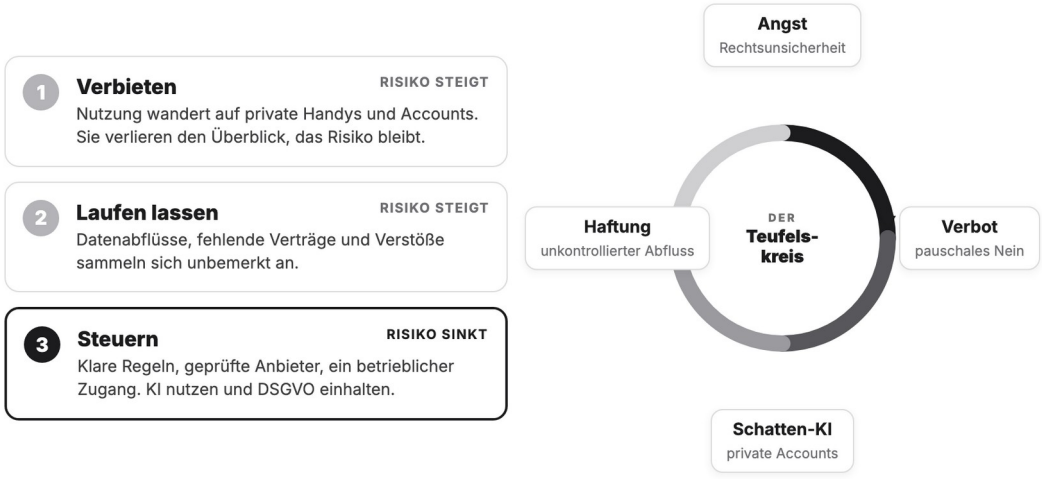

Abb. 1: Drei Wege im Umgang mit KI und der Teufelskreis aus Angst und Verbot

Ein Verbot wirkt wie Kontrolle, verlagert die Nutzung aber genau dorthin, wo keine Kontrolle mehr möglich ist. Aus Angst wird Verbot, aus Verbot wird Schatten-KI, aus Schatten-KI wird Haftung. Der Ausweg heißt **gesteuerte KI**.

Wo Ihre Daten unbemerkt das Haus verlassen

Schatten-KI ist kein Hackerangriff. Die Daten verlassen Ihr Unternehmen freiwillig, Prompt für Prompt, Upload für Upload. Und selbst eine offiziell eingekaufte KI kann zum Abflusskanal werden, wenn Rechte und Einstellungen nicht stimmen.

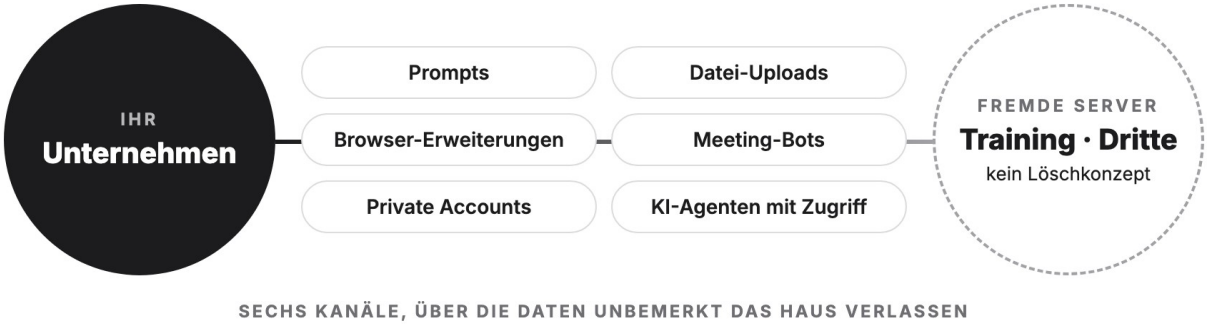

Abb. 2: Sechs typische Kanäle des Datenabflusses

> **ACHTUNG**
>
> **Auch ohne Hacker, auch ohne bösen Willen**
>
> Bei Samsung reichten 2023 wenige Eingaben eigener Ingenieure, um internen Quellcode und Inhalte eines Meetings an ChatGPT zu übergeben. Das Verbot kam erst danach. In etwa 40 % der Datei-Uploads in KI-Tools stecken personenbezogene oder Zahlungsdaten (LayerX, 2025). Ob Ihre Leute KI nutzen, ist entschieden. Offen ist nur, ob Sie es sehen.

KAPITEL 2

Was wirklich gilt: DSGVO und EU AI Act

Woran Aufsichtsbehörden Ihren KI-Einsatz messen

Sie müssen nicht spekulieren, woran eine deutsche Behörde Ihren KI-Einsatz prüft. Der Kernsatz ist unbequem einfach: Für jeden Schritt, in dem eine KI personenbezogene Daten verarbeitet, brauchen Sie eine Rechtsgrundlage.

Die DSGVO lässt KI zu, solange Sie steuern

Die deutschen Datenschutzaufsichtsbehörden haben ihre Erwartungen in der **Orientierungshilfe „KI und Datenschutz“ der Datenschutzkonferenz (Mai 2024)** festgehalten und im Juni 2025 um Empfehlungen zu technischen und organisatorischen Maßnahmen ergänzt. Für Sie als Anwender sind vor allem diese Artikel entscheidend:

ARTIKEL	WAS ER BEIM KI-EINSATZ VERLANGT	WANN ER GREIFT
Art. 5, 6 DSGVO	Rechtsgrundlage und klare Zweckbindung für jeden Schritt	Sobald Personendaten eingegeben, verarbeitet oder ausgegeben werden
Art. 28 DSGVO	Auftragsverarbeitungsvertrag (AVV) mit dem Anbieter	Wenn der Anbieter Personendaten in Ihrem Auftrag verarbeitet
Art. 35 DSGVO	Datenschutz-Folgenabschätzung (DSFA) vorab	Bei voraussichtlich hohem Risiko, laut Aufsicht bei KI vielfach der Fall
Art. 22 DSGVO	Menschliche Letztentscheidung mit echtem Spielraum	Bei Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung
Art. 15–17 DSGVO	Auskunft, Berichtigung, Löschung, auch für KI-Ausgaben	Sobald eine KI Daten über eine Person verarbeitet oder erzeugt

> ACHTUNG
>
> **Das Bewerbungs-Beispiel der Behörden**
>
> Eine KI wertet Bewerbungen aus und verschickt selbst die Einladungen zum Gespräch. Das verstößt gegen Art. 22 DSGVO. Eine nur formale Beteiligung eines Menschen reicht nicht. Ein Klick unter Zeitdruck ist kein echter Entscheidungsspielraum.

Entwarnung, wo sie berechtigt ist: Einsatzfelder ganz ohne Personendaten fallen nicht unter das Datenschutzrecht. Und das berechtigte Interesse (Art. 6 Abs. 1 lit. f DSGVO) kann eine Verarbeitung tragen, wenn Sie die Abwägung dokumentiert haben. Wichtig: Ein AVV und ein abgeschaltetes Training sind Pflichtbausteine, aber kein Freibrief. Sie ersetzen weder Rechtsgrundlage noch Dokumentation.

Der AI Act trifft Sie schon heute

Wer ChatGPT, Copilot oder Gemini nutzt, ist **Betreiber** (englisch Deployer), nicht Anbieter, und fällt meist nicht unter die schweren Hochrisiko-Pflichten. Verbindlich gilt trotzdem schon jetzt: das Verbot bestimmter KI-Praktiken und die Pflicht zur KI-Kompetenz, beide seit dem 2. Februar 2025, sowie seit dem 2. August 2026 die Transparenzpflichten.



Abb. 3: Zeitstrahl des AI Act nach dem Digital Omnibus (Verordnung (EU) 2026/1744)

NEU SEIT SOMMER 2026	WAS DAS FÜR SIE BEDEUTET
Digital Omnibus zur KI	Verordnung (EU) 2026/1744, im Amtsblatt am 24.07.2026, in Kraft seit 27.07.2026. Hochrisiko-Pflichten für Anhang III verschoben auf den **02.12.2027**, für Anhang I auf den **02.08.2028**.
Art. 4 neu gefasst	Sie müssen Maßnahmen ergreifen, die die KI-Kompetenz Ihrer Mitarbeitenden fördern. Ein bestimmtes Kompetenzniveau müssen Sie nicht mehr garantieren. Dokumentieren Sie Zielgruppen, Inhalte und Teilnahme trotzdem.
Neue Verbote ab 02.12.2026	Verboten werden KI-Systeme, die intime Darstellungen realer Personen ohne Zustimmung erzeugen, sowie Systeme zur Erzeugung von Missbrauchsdarstellungen von Kindern.
Aufsicht in Deutschland	Das KI-Marktüberwachungsgesetz (KI-MIG) gilt seit dem 29.07.2026. Die **Bundesnetzagentur** ist zentrale Marktüberwachungs-, Anlauf- und Beschwerdestelle. Branchenaufsichten wie die BaFin bleiben daneben zuständig.

TIPP

Die Verschiebung ist kein Freibrief

Verbote, KI-Kompetenz und Transparenz gelten unverändert, und die DSGVO wird vom AI Act ohnehin nicht berührt. Der Omnibus verschafft nur denen Luft, die echte Hochrisiko-Systeme betreiben. Hochrisiko wird es zum Beispiel, sobald KI in Personalentscheidungen (Bewerber-Ranking, Video-Interview-Scoring) oder in die Kreditwürdigkeitsprüfung eingreift. Dann gelten auch für Sie als Betreiber die Pflichten aus Art. 26 AI Act, etwa echte menschliche Aufsicht und die Information der Beschäftigten.

Zwei Bußgeldrahmen, eine persönliche Haftung

DSGVO und AI Act sanktionieren getrennt. Für denselben Vorgang können beide greifen. Und der teuerste Teil steht selten in der Pressemeldung: Die Geschäftsführung kann neben dem Unternehmen persönlich haften.

RAHMEN	OBERE STUFE	UNTERE STUFE	GREIFT BEI
DSGVO (Art. 83)	bis 20 Mio. € oder 4 % des weltweiten Jahresumsatzes	bis 10 Mio. € oder 2 %	Grundsätze, Rechtsgrundlage, Betroffenenrechte, Drittlandtransfer, AVV
AI Act (Art. 99)	bis 35 Mio. € oder 7 % (nur verbotene Praktiken)	bis 15 Mio. € oder 3 % (sonstige Pflichten)	Betreiber-, Transparenz- und Anbieterpflichten

Für kleine und mittlere Unternehmen gilt beim AI Act jeweils der **niedrigere** der beiden Werte (Art. 99 Abs. 6). Die DSGVO kennt diesen Deckel nicht. Wie ernst es die Behörden meinen, zeigen die Zahlen: Seit 2018 wurden in Europa DSGVO-Bußgelder von **rund 7,1 Mrd. €** verhängt, allein 2025 **rund 1,2 Mrd. €** (DLA Piper, Jan. 2026).

72 Std.
Frist, eine Datenpanne an die Aufsichtsbehörde zu melden (Art. 33)
DSGVO

5.000 €
Schadensersatz, für den ein Geschäftsführer persönlich neben der GmbH haftete
OLG Dresden, 4 U 1158/21

5 Mio. €
Bußgeld gegen den KI-Chatbot Replika: keine Rechtsgrundlage, keine Altersprüfung
Garante, 2025

GUT ZU WISSEN

Was die Behörden prüfen

Die italienische Aufsicht verhängte 2024 gegen OpenAI 15 Mio. €. Das Landgericht Rom hob den Bescheid am 18.03.2026 auf, allerdings aus Zuständigkeitsgründen, nicht in der Sache. Der Fall zeigt trotzdem, worauf Behörden schauen: Rechtsgrundlage, Transparenz, Altersprüfung. Wer diese Punkte offen lässt, ist ein Kandidat für das nächste Verfahren.

KAPITEL 3

Wo Ihre Daten landen

Über Ihre Daten entscheidet der Vertrag, nicht das Modell

Ob ein KI-Tool DSGVO-tauglich ist, hängt fast nie am Modell und fast immer am Tarif und Vertrag dahinter. Dasselbe ChatGPT ist im kostenlosen Privat-Account ein Datenschutzproblem, im Business-Vertrag dagegen beherrschbar.

Vier Fragen, die über jedes KI-Tool entscheiden

1. **Training:** Werden Ihre Eingaben zum Training verwendet? Bei Business-, Enterprise- und API-Tarifen in der Regel nein, bei kostenlosen und privaten Tarifen meist ja, oft voreingestellt.
2. **AVV:** Gibt es einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO? Bei Business-Tarifen ja, beim privaten Account in der Regel nicht.
3. **Speicherort:** Können Sie Speicherung und Verarbeitung in der EU festlegen? Zunehmend ja, oft aber nur für gespeicherte Daten, nicht für jede Verarbeitung.
4. **Rechtsraum:** Wessen Recht regelt den Zugriff? Der oft übersehene Knackpunkt, dazu gleich mehr.

TARIF-TYP	TRAINING MIT IHREN DATEN?	AVV?	EINSCHÄTZUNG
Kostenlose und private Tarife (z. B. ChatGPT Free/Plus, Claude Free/Pro, Gemini privat)	meist ja, voreingestellt; abschaltbar per Einstellung	nein	für Personen- und Firmendaten **ungeeignet**
Business-, Team- und Enterprise-Tarife großer US-Anbieter	nein, vertraglich zugesagt	ja	nutzbar mit AVV, Transferprüfung und Richtlinie
EU-Anbieter / EU-Plattformen mit EU-Hosting	nein	ja	datenschutzfreundlich, Unterauftragnehmer prüfen
Selbst betriebene Open-Source-Modelle	nein, volle Kontrolle	entfällt	am souveränsten, aber Betrieb und Sicherheit liegen bei Ihnen

Stand: Oktober 2026. Anbieter ändern ihre Bedingungen regelmäßig. Prüfen Sie vor jedem Vertragsabschluss die aktuellen Datenschutz- und Vertragsunterlagen.

Ein Server in Frankfurt schützt nicht vor US-Zugriff

Fast jeder große US-Anbieter wirbt mit einem Rechenzentrum in der EU. Das beantwortet aber nur, wo die Daten liegen, nicht wessen Recht den Zugriff regelt. Der **US CLOUD Act** verpflichtet US-Anbieter, Daten unter ihrer Kontrolle auf behördliche Anordnung herauszugeben, unabhängig vom Speicherort. Microsoft Frankreich räumte im Juni 2025 vor dem französischen Senat ein, einen solchen Zugriff nicht ausschließen zu können.

Für Übermittlungen in die USA gibt es seit Juli 2023 das **EU-US Data Privacy Framework (DPF)**. Ist ein Anbieter dort zertifiziert, sind keine zusätzlichen Garantien für den Transfer nötig. Aber: Das Gericht der EU hat die Klage dagegen am 03.09.2025 zwar abgewiesen, das Rechtsmittel liegt jedoch beim Europäischen Gerichtshof (C-703/25 P). Die beiden Vorgänger-Abkommen hat der EuGH bereits gekippt.

TIPP

Ihre Faustregel für die Anbieterwahl

Erstens: EU-Anbieter ohne US-Mutter und echtes Self-Hosting in der EU sind die sauberste Option. **Zweitens:** Bei US-Anbietern zuerst den DPF-Status prüfen (dataprivacyframework.gov). **Drittens:** Ohne DPF-Zertifizierung brauchen Sie Standardvertragsklauseln plus eine Transfer-Folgenabschätzung. In allen Fällen gilt: Ein EU-Serverstandort löst die Frage, wo Daten liegen, nicht die Frage, wer zugreifen darf.

Sechs Fehler, die teuer werden

Die meisten Datenschutzverstöße bei KI passieren schlicht aus Unwissen. Diese sechs tauchen in der Praxis immer wieder auf:

FEHLER	WAS PASSIERT	BESSER SO
1 · Der Telefonassistent, der sich nicht zu erkennen gibt	KI nimmt Anrufe an und zeichnet auf. Niemand sagt dem Anrufer, dass er mit einer Maschine spricht, kein AVV. Heimliche Aufnahmen können strafbar sein (§ 201 StGB).	KI-Hinweis zuerst, Einwilligung vor jeder Aufzeichnung, EU-Hosting, AVV, DSFA prüfen
2 · Das Meeting, das heimlich mitschreibt	Ein Notiz-Tool sitzt automatisch in jedem Videocall und transkribiert auf US-Servern, ohne die Teilnehmenden zu informieren.	Vorab informieren, Widerspruch ermöglichen, EU-Tool, Löschkonzept
3 · Bewerbungen durch ChatGPT jagen	Bewerbungen werden über einen Gratis-Account vorsortiert. Faktisch entscheidet die Maschine (Art. 22 DSGVO, Hochrisiko nach AI Act).	Mensch entscheidet nachweisbar, Business-Account mit AVV, DSFA
4 · Kundendaten im Privat-Account	Eine Kundenliste landet im kostenlosen Account, Training ist voreingestellt aktiv.	Richtlinie, betriebliche Zugänge mit AVV, Daten vorher reduzieren
5 · Fehlende Kennzeichnung	KI-erzeugte Bilder oder Audios realer Personen werden ohne Hinweis veröffentlicht. Für solche Deepfakes gilt seit 02.08.2026 die Offenlegungspflicht (Art. 50 Abs. 4).	Täuschend echte synthetische Inhalte klar als KI-generiert kennzeichnen
6 · KI-Assistent ohne Rechte-Check	Ein Assistent wie Microsoft 365 Copilot zeigt jedem alles, worauf er Leserechte hat. Die Gehaltsliste mit „Jeder im Unternehmen“-Link wird für alle auffindbar.	Vorher Berechtigungen aufräumen, Least-Privilege, Pilot statt Big Bang

NÄCHSTER SCHRITT

Sie erkennen einen dieser Fehler in Ihrem Betrieb wieder? In einem kurzen, kostenlosen Gespräch klären wir, wo Ihre größten Lücken liegen, bevor daraus ein Verfahren wird.

Datenschutz-Gespräch mit Corinna Göring vereinbaren →

KI-Erstgespräch mit Savas Kozluklu vereinbaren →

KAPITEL 4

Ihr Fahrplan in sieben Schritten

Erst Menschen und Regeln, dann Verträge und Technik, dann die KI

Die meisten starten bei der KI und vergessen den Unterbau. Konforme KI trägt nur, wenn drei Schichten in der richtigen Reihenfolge stehen. Wer oben anfängt, baut auf Sand.

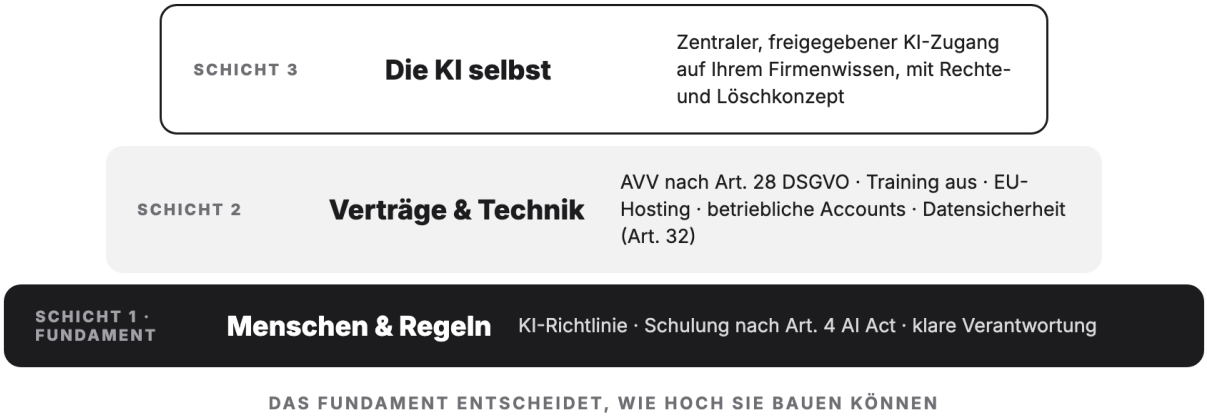

Abb. 4: Das 3-Schichten-Modell für rechtssichere KI

Die vier Wege zur konformen KI

Bevor Sie an einzelne Tools denken, entscheiden Sie sich für einen Weg. Die Aufsicht hält **technisch geschlossene Systeme** ausdrücklich für vorzugswürdig, weil Ihre Eingaben dort den geschützten Bereich nicht verlassen.

	WEG	PASST FÜR	AUFWAND / KONTROLLE
A	**Bekanntes Tool im Business-Vertrag** (Training aus, AVV)	schneller, konformer Start	gering / mittel
B	**EU-Plattform oder EU-Anbieter**	datenschutzsensible Branchen	gering bis mittel / hoch
C	**Eigene Infrastruktur, lokal**	hochsensible Daten, eigene IT	hoch / sehr hoch
D	**Zentraler KI-Arbeitsplatz** auf Ihrem Firmenwissen	unternehmensweite Nutzung	mittel / hoch

ACHTUNG

Der teuerste Weg ist der Flickenteppich

Ein Dutzend Einzeltools, jedes mit eigenem Login, keines mit geprüftem Vertrag, und niemand weiß, wer was nutzt. So entsteht Schatten-KI. Selten passt nur ein Weg, aber es sollte immer ein bewusst gewählter sein.

Der Fahrplan, den Sie diese Woche starten können

Ein 200-seitiger Compliance-Apparat ist nicht nötig. Eine handhabbare Reihenfolge reicht. Jeder Schritt baut auf dem vorigen auf, die ersten drei schaffen Sie in wenigen Wochen.

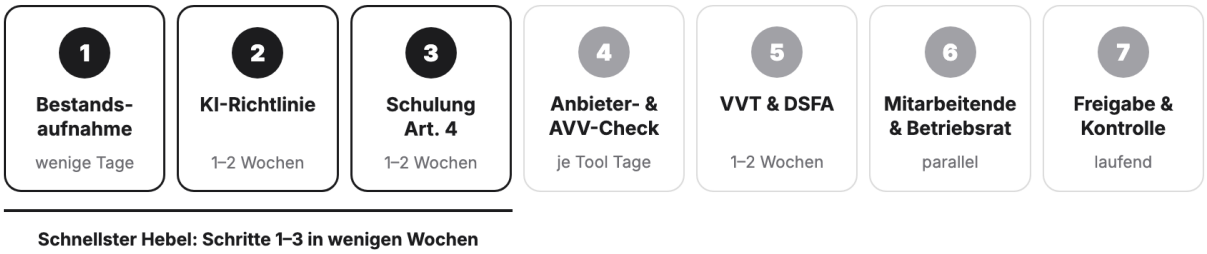

Abb. 5: Sieben Schritte zur gesteuerten KI

SCHRITT	WAS ZU TUN IST
1 · Bestandsaufnahme	Erfassen Sie, welche KI-Tools schon laufen, offiziell und inoffiziell. Legen Sie Zweck und Verantwortung fest. Ohne Inventur wissen Sie nicht, wo Daten heute schon abfließen.
2 · KI-Richtlinie	Das Herzstück: eine Liste zugelassener Tools und Zwecke plus klare Verbote. Konkrete Beispiele für Erlaubtes und Verbotenes wirken besser als abstrakte Regeln.
3 · Schulung nach Art. 4	Rollenbezogen, dokumentiert und regelmäßig aufgefrischt. Ein bestimmtes Zertifikat verlangt das Gesetz nicht, Nachweise helfen aber im Ernstfall.
4 · Anbieter- und AVV-Check	Je Tool: AVV nach Art. 28, Hosting, Training aus, Transfergrundlage. Den Unterschied macht der Vertrag.
5 · VVT und DSFA	Tragen Sie die Verarbeitung ins Verzeichnis der Verarbeitungstätigkeiten ein (Art. 30) und prüfen Sie, ob eine Folgenabschätzung nötig ist. Bei KI ist das laut Aufsicht vielfach der Fall.
6 · Mitarbeitende und Betriebsrat	Informieren Sie Ihr Team transparent. Gibt es einen Betriebsrat und ist ein Tool zur Leistungs- oder Verhaltenskontrolle geeignet, greift die Mitbestimmung (§ 87 Abs. 1 Nr. 6 BetrVG).
7 · Freigabe und Kontrolle	Legen Sie fest, wie neue Tools genehmigt werden, und prüfen Sie regelmäßig nach (Art. 24 DSGVO). Steuerung ist eine Routine ohne Enddatum.

TIPP

Schritte 2 und 3 sind der schnellste Hebel

Mit kleinem Budget und in wenigen Wochen decken Richtlinie und Schulung bereits den größten Risikoteil ab: die ungesteuerte Schatten-KI und die Kompetenzpflicht aus Art. 4 AI Act. Nur rund ein Viertel der Unternehmen hat überhaupt Regeln. Mit einer sauberen Richtlinie gehören Sie zur Minderheit, die vorbereitet ist.

Zwei Checklisten zum Abhaken

CHECKLISTE 1 · WAS IN IHRE KI-RICHTLINIE GEHÖRT

- ☐ Zugelassene Tools und Zwecke als Positivliste mit klaren Grenzen
- ☐ Verbot, personenbezogene Daten oder Geschäftsgeheimnisse in offene Systeme einzugeben. Namen entfernen reicht nicht, Personenbezug entsteht auch aus dem Kontext.
- ☐ Besondere Vorsicht bei sensiblen Daten nach Art. 9 DSGVO (Gesundheit, Religion, Gewerkschaft)
- ☐ Pflicht, KI-Ergebnisse durch einen Menschen zu prüfen, keine automatische Letztentscheidung
- ☐ Nutzung nur über betriebliche Accounts und Geräte
- ☐ Kennzeichnung von KI-Inhalten, wo sie Pflicht ist
- ☐ Ansprechpartner und Meldeweg für Zweifelsfälle und Datenpannen

CHECKLISTE 2 · PFLICHTINHALTE DES AVV NACH ART. 28 ABS. 3 DSGVO

- ☐ Verarbeitung nur auf dokumentierte Weisung (lit. a)
- ☐ Vertraulichkeit der eingesetzten Personen (lit. b)
- ☐ Technische und organisatorische Maßnahmen nach Art. 32 (lit. c)
- ☐ Unterauftragnehmer nur mit Genehmigung, gleiche Pflichten weitergereicht (lit. d)
- ☐ Unterstützung bei Betroffenenrechten und Ihren Pflichten (lit. e, f)
- ☐ Löschung oder Rückgabe aller Daten nach Vertragsende, inklusive Kopien (lit. g)
- ☐ Nachweise bereitstellen, Prüfungen ermöglichen (lit. h)

Was Sie zuerst tun, nach Betriebsgröße

IHR PROFIL	IHRE PRIORITÄTEN
Solo und 1–9 Mitarbeitende	Schritte 1 bis 4: Bestandsaufnahme, kurze Richtlinie, dokumentierte Schulung und AVV-Check für jedes Tool, das Personendaten verarbeitet. Betriebliche Accounts statt privater Logins. Verzeichnis der Verarbeitungstätigkeiten aktuell halten, denn die DSGVO gilt unabhängig von der Größe.
10–19 Mitarbeitende	Zusätzlich: klare Zuständigkeit für Datenschutz und KI, Meldeprozess für Datenpannen festlegen.
20–100 Mitarbeitende	Zusätzlich: Datenschutzbeauftragte(n) benennen, wenn mindestens 20 Personen ständig automatisiert Personendaten verarbeiten (§ 38 BDSG). Freigabeprozess für neue Tools, DSFA-Praxis, Betriebsrat einbinden, zentraler KI-Zugang statt Insellösungen.

GUT ZU WISSEN

Eine Anhebung der Schwelle für Datenschutzbeauftragte von 20 auf 50 Personen wird politisch diskutiert, ist aber Stand Oktober 2026 nicht beschlossen. Unabhängig von der Kopfzahl kann KI die Benennungspflicht auslösen: Ist wegen umfangreichen Profilings oder Scorings eine DSFA nötig, braucht auch der kleine Betrieb eine(n) Datenschutzbeauftragte(n).

NÄCHSTER SCHRITT

Sie möchten Ihr Fundament in einem halben Tag aufsetzen und danach KI gezielt einführen? Genau dafür arbeiten wir zusammen.

Datenschutz-Gespräch mit Corinna Göring vereinbaren →

KI-Erstgespräch mit Savas Kozluklu vereinbaren →

KAPITEL 5

Acht Anwendungen, die sauber laufen

Vom Posteingang bis zum Bewerbungsprozess

Die häufigsten Einstiegsfälle sind konform machbar, wenn das Fundament stimmt: AVV mit dem Anbieter, dokumentierte Rechtsgrundlage samt Zweck und die Regel, dass keine Personendaten in offene Systeme wandern.

Vier Anwendungen für den Alltag

USE CASE	WAS ES TUT	AUFWAND	DATENSCHUTZ-HINWEIS
1 · E-Mails und Angebote	Entwürfe, Antworten und Angebote vorformulieren	gering	Kundendaten nur über betrieblichen Account mit AVV, kein Training
2 · Meeting-Protokolle	Gespräche transkribieren und zusammenfassen	gering bis mittel	Vorher informieren und Rechtsgrundlage oder Einwilligung sichern (§ 201 StGB), Alternative ohne Aufnahme anbieten
3 · Dokumente auswerten	Felder und Kernaussagen aus Dokumenten ziehen	mittel	Bei Personenbezug VVT-Eintrag, ggf. DSFA, Ergebnis immer menschlich prüfen
4 · Wissensassistent	Fragen aus dem eigenen Firmenwissen beantworten	mittel bis hoch	Rechte- und Zugriffskonzept, EU-Hosting, Löschkonzept, Beschäftigtendaten besonders schützen

Vier Anwendungen, bei denen die Kennzeichnung zählt

Diese Fälle erreichen Kunden oder Bewerbende direkt. Deshalb kommen die Transparenzpflichten aus Art. 50 AI Act hinzu, und eine Maschine darf keine rechtlich wirksame Letztentscheidung über Menschen treffen.

USE CASE	WAS ES TUT	AUFWAND	DATENSCHUTZ-HINWEIS
5 · Website-Chatbot	Kundenanfragen automatisch beantworten	mittel	Offenlegen, dass ein Bot antwortet, AVV, keine Personendaten in offene Modelle
6 · Telefonassistenz	Anrufe annehmen und Anliegen erfassen	mittel bis hoch	KI-Hinweis zu Beginn, Einwilligung vor Aufzeichnung, EU-Hosting, sensible Daten vermeiden
7 · Content und Marketing	Texte, Posts und Kampagnen erstellen	gering	Täuschend echte Bilder, Videos, Stimmen kennzeichnen (Art. 50 Abs. 4), Urheberrechte prüfen
8 · Bewerbungen vorbereiten	Unterlagen sortieren und aufbereiten	mittel	Hochrisiko-Bereich: Mensch entscheidet, Bewerbende informieren, DSFA einplanen

TIPP

Das Muster hinter allen acht Fällen

Geschlossenes oder Business-System, AVV mit dem Anbieter, keine Personendaten in offene Modelle, ein Mensch prüft das Ergebnis, und wo Kunden oder Bewerbende betroffen sind, kommt die Kennzeichnung dazu. Wer dieses Muster einmal aufsetzt, kann Anwendung für Anwendung anschließen, ohne jedes Mal bei null zu beginnen.

Was die Geschäftsführung im laufenden Betrieb schuldet

Betroffenenrechte praktisch umsetzen. Gibt jemand Personendaten in eine KI ein, entstehen beim Anbieter Protokolle, und die sind auskunftspflichtig (Art. 15 DSGVO). Auskunftsfähig bleiben Sie über ein aktuelles Verzeichnis, welches Tool welche Daten verarbeitet, plus die vertragliche Zusage des Anbieters, Sie bei Anfragen zu unterstützen. Auch eine falsche KI-Ausgabe über eine Person kann ein personenbezogenes Datum sein und ist dann zu berichtigen oder zu löschen.

Beschäftigtendaten. Seit dem Urteil des Europäischen Gerichtshofs vom 30.03.2023 (C-34/21) gilt die deutsche Sonderregel in § 26 Abs. 1 BDSG als europarechtlich angreifbar. Stützen Sie Verarbeitungen im Arbeitsverhältnis deshalb zusätzlich auf Art. 6 DSGVO. Ein eigenes Beschäftigtendatengesetz ist angekündigt, gilt aber noch nicht. Eine lückenlose KI-Leistungsüberwachung lässt sich nach heutigem Recht regelmäßig nicht rechtfertigen.

DER 72-STUNDEN-MELDEPROZESS BEI EINER DATENPANNE

1. **Kenntnis:** Ab hier läuft die Frist, Wochenenden zählen mit.
2. **Risiko prüfen:** Kein Risiko, keine Meldung. Sonst binnen 72 Stunden an die Aufsichtsbehörde (Art. 33 DSGVO).
3. **Betroffene informieren:** Bei hohem Risiko zusätzlich die betroffenen Personen benachrichtigen (Art. 34 DSGVO).
4. **Dokumentieren:** Jede Verletzung intern festhalten, auch die nicht gemeldete (Art. 33 Abs. 5 DSGVO). Ihr KI-Anbieter muss Ihnen Pannen unverzüglich melden, diese Pflicht gehört in den AVV.

> **ACHTUNG**
>
> **Das Haftungsrisiko ist persönlich**
>
> Ein dokumentiertes Datenschutz- und KI-System gehört zur Sorgfaltspflicht der Geschäftsführung (§ 43 GmbHG). Dieselbe Dokumentation ist im Ernstfall Ihr bester Entlastungsnachweis.

KAPITEL 6

Ehrliche Grenzen

Warum 100 % Sicherheit niemand seriös verspricht

Compliance ist kein Schalter, der Ihr Risiko auf null stellt. Ein sauberes Setup drückt das Restrisiko deutlich nach unten, ganz verschwindet es nie. Wer das ehrlich einplant, wird nicht überrascht.



Abb. 6: Ein sauberes Setup senkt das Risiko, ein Restrisiko bleibt

WAS IN BEWEGUNG BLEIBT	BEISPIEL
Das Recht ändert sich	Der Digital Omnibus hat den AI Act 2026 geändert, die DSGVO-Reform wird in Brüssel noch verhandelt. Das Data Privacy Framework steht beim EuGH auf dem Prüfstand. Standardvertragsklauseln plus technische Schutzmaßnahmen bleiben deshalb die Rückfallebene.
Die Technik erzeugt neue Lücken	Die Sicherheitslücke „EchoLeak“ (CVE-2025-32711) brachte Microsoft 365 Copilot 2025 dazu, interne Daten über eine einzige präparierte E-Mail preiszugeben, ganz ohne Klick. Microsoft hat sie geschlossen, die Angriffsart betrifft aber jeden KI-Assistenten mit Zugriff auf interne Daten.
Anbieter ändern Bedingungen	Seit Frühjahr 2026 erlaubt „Flex Routing“ bei Microsoft 365 Copilot die Verarbeitung außerhalb der EU-Datengrenze bei Lastspitzen, für neue EU-Tenants voreingestellt aktiv. Wer das nicht weiß, schaltet es nicht ab.
Modelle halluzinieren	KI-Ergebnisse können plausibel klingen und trotzdem falsch sein. Deshalb gehört die menschliche Prüfung in jede Richtlinie.

TIPP

Auch der vermeintlich sicherste Weg hat Kosten

Ein eigenes Open-Source-Modell auf einem EU-Server klingt günstig und löst die Souveränitätsfrage am saubersten. Aber Betrieb, IT-Sicherheit, Modellqualität und Wartung liegen dann komplett bei Ihnen. Verantwortlicher im Sinne der DSGVO bleiben Sie ohnehin.

Selbst machen oder begleiten lassen

Vieles können Sie selbst stemmen. Anderes kostet Sie als Fachfremden Monate und trotzdem Fehler. Die ehrliche Antwort ist selten „alles selbst“ oder „alles abgeben“. Meist trägt ein Mittelweg: Routine intern, die teuren Weichenstellungen mit Erfahrung.

DAS SCHAFFEN SIE GUT SELBST	DA ZAHLT SICH ERFAHRUNG AUS
Bestandsaufnahme: erfassen, welche KI-Tools laufen. Fleißarbeit, keine Raketenwissenschaft.	**Anbieterauswahl:** Speicherort ist nicht gleich Souveränität. Routing, CLOUD Act und AVV-Details entscheiden.
KI-Richtlinie: Positivliste plus Verbot, Personendaten in offene Systeme zu geben.	**Architektur und Integration:** ein zentraler KI-Zugang statt Flickenteppich aus Einzeltools.
Schulung organisieren: rollenbezogen, dokumentiert, regelmäßig aufgefrischt.	**Datenschutz-Fundament und DSFA:** Verzeichnis, Verträge, Folgenabschätzung sauber aufsetzen.

ACHTUNG

Eine klare Grenze

Dieser Report ist Orientierung, keine Rechtsberatung. Für verbindliche Rechtsfragen, etwa die Rechtsgrundlage im Einzelfall, eine Betriebsvereinbarung oder die formale DSFA, binden Sie eine Fachanwältin oder einen Fachanwalt bzw. Ihre(n) Datenschutzbeauftragte(n) ein. Gute Begleitung sorgt dafür, dass Sie mit den richtigen Fragen dorthin kommen.

FAZIT

Aus Pflicht wird Vorsprung

Ihr Weg vom versteckten Risiko zum Wettbewerbsvorteil

Die DSGVO ist nicht Ihr eigentliches Problem. Ihr Problem ist unkontrollierte KI-Nutzung, die aus der Angst vor der DSGVO entsteht. Wer KI verbietet oder unbeobachtet laufen lässt, hat das Risiko schon im Haus. Wer sie steuert, macht daraus einen Vorsprung.



Abb. 7: Drei Stufen vom ungesteuerten KI-Einsatz zum Wettbewerbsvorteil

Die meisten Unternehmen stehen noch auf Stufe eins, ohne es zu wissen. Den vollständigen Fahrplan finden Sie in Kapitel 4. Hier ist er auf drei Prioritäten verdichtet, mit denen Sie in 90 Tagen am weitesten kommen:

WANN	WAS
Diese Woche	Machen Sie die Bestandsaufnahme. Fragen Sie im Team, welche KI-Tools schon genutzt werden, offiziell und inoffiziell. Diese eine Stunde bringt Sie von Stufe eins auf den Weg nach oben, ohne einen Euro Budget.
Diesen Monat	Erlassen Sie die KI-Richtlinie und setzen Sie die Schulung nach Art. 4 AI Act auf (Schritte 2 und 3). Prüfen Sie, ob Ihr Datenschutz-Fundament steht: Verzeichnis, AVV, Informationspflichten.
Dieses Quartal	Prüfen Sie Anbieter und Verträge, wählen Sie einen Weg und geben Sie die ersten Anwendungsfälle offiziell frei (Schritte 4 bis 7).

TIPP

Datenschutz als Verkaufsargument

Vertrauen verkauft besser als Rabatt. Wer zeigen kann, dass Kundendaten sicher sind und KI verantwortungsvoll eingesetzt wird, hebt sich ab, gerade gegenüber größeren Auftraggebern, die ihre Lieferanten zunehmend danach fragen.

NÄCHSTER SCHRITT

So unterstützen wir Sie

Erst das Fundament, dann die KI, aus zwei Händen, die zusammenarbeiten

Sie müssen das nicht allein lösen. Wählen Sie den Einstieg, der zu Ihrer Situation passt, oder sprechen Sie uns beide an.

CORIDAS
DSGVO Erste Hilfe Koffer

DSGVO Erste Hilfe Koffer: Ihr Datenschutz-Fundament in rund vier Stunden

- Gemeinsam mit einer erfahrenen Beraterin bzw. einem Berater, online und verständlich
- Weitgehend vorausgefüllte Mustervorlagen und ein Verzeichnis mit rund 80 praxisnahen Verfahren
- Transparente Festpreise für Solo-Selbstständige, kleine Firmen und Handwerksbetriebe
- Teilnahme-Emblem und Vertrauensforum, damit Kunden sehen, was Sie für Datenschutz tun

Jetzt Kontakt aufnehmen →

CORIDAS GmbH · Corinna Göring · Tel. 08252 9090288 · backoffice@dsgvo-erste-hilfe.de · dsgvo-erste-hilfe.de

ZeoAI

KI, die Ihr Unternehmen spürbar entlastet, sicher und mit System

- **KI-Potenzialanalyse (KIPA):** in zwei Wochen zur priorisierten KI-Roadmap
- **KI-Kompetenz-Schulung nach Art. 4 AI Act** mit personenbezogener Teilnahmebestätigung
- **Umsetzung in 30 bis 90 Tagen**, DSGVO- und AI-Act-konform, in Ihre bestehenden Systeme
- **Externe KI-Abteilung** und auf Wunsch externer Chief AI Officer

Kostenloses 15-Minuten-Erstgespräch →

ZeoAI · Savas Kozluklu (MBA) · Tel. 08138 6680638 · kontakt@zeoai.de · zeoai.de

GUT ZU WISSEN

Mehr hören: unsere Podcast-Folge „Kann KI kreativ sein, wenn der AI Act mitredet?“

Sie möchten tiefer einsteigen? In der Folge sprechen wir darüber, wie Kreativität, KI und Regulierung zusammenpassen. Weitere Folgen rund um Datenschutz für Selbstständige und kleine Unternehmen finden Sie im Podcast „Datenschutz im OHR“.

Zum Podcast „Datenschutz im OHR“ →

ANHANG

Quellen und rechtlicher Hinweis

Alle Angaben mit Stand Oktober 2026

[1] Bitkom (14.09.2026): Erstmals nutzt die Mehrheit der Unternehmen KI www.bitkom.org/Presse/Presseinformation/Erstmals-nutzt-Mehrheit-Unternehmen-KI

[2] Bitkom (21.10.2025): Beschäftigte nutzen Schatten-KI www.bitkom.org/Presse/Presseinformation/Beschaeftigte-nutzen-Schatten-KI

[3] IW-Kurzbericht 63/2026: Schatten-KI www.iwkoeln.de/fileadmin/user_upload/Studien/Kurzberichte/PDF/2026/IW-Kurzbericht_2026-Schatten-KI.pdf

[4] LayerX (Okt. 2025): Enterprise AI and SaaS Data Security Report go.layerxsecurity.com/the-layerx-enterprise-ai-saas-data-security-report-2025

[5] Verordnung (EU) 2024/1689 (AI Act) eur-lex.europa.eu/eli/reg/2024/1689/oj

[6] Verordnung (EU) 2026/1744 (Digital Omnibus zur KI) eur-lex.europa.eu/eli/reg/2026/1744/oj

[7] Bundesnetzagentur (29.07.2026): Zentrale Rolle bei der Umsetzung der KI-Verordnung (KI-MIG) www.bundesnetzagentur.de/1112336

[8] Datenschutzkonferenz: Orientierungshilfe KI und Datenschutz (Mai 2024) und TOM-Empfehlungen (Juni 2025) www.datenschutzkonferenz-online.de/

[9] DLA Piper (Jan. 2026): GDPR Fines and Data Breach Survey www.dlapiper.com/en/insights/publications/2026/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2026

[10] EuGH, Urteil vom 30.03.2023, C-34/21 (Beschäftigtendatenschutz) curia.europa.eu/juris/liste.jsf?num=C-34/21

[11] EuGH, Rechtsmittel C-703/25 P (Latombe / Data Privacy Framework) eur-lex.europa.eu/eli/C/2025/6610/oj

[12] Microsoft Learn: Flex Routing für Microsoft 365 Copilot learn.microsoft.com/en-us/microsoft-365/copilot/copilot-flex-routing

[13] OpenAI Help Center: Data Controls in ChatGPT help.openai.com/en/articles/7730893-data-controls-faq

[14] NVD: CVE-2025-32711 (EchoLeak) nvd.nist.gov/vuln/detail/CVE-2025-32711

[15] EU-US Data Privacy Framework: Liste zertifizierter Unternehmen www.dataprivacyframework.gov/list

ACHTUNG

Rechtlicher Hinweis

Dieser Report gibt eine fundierte Übersicht und die richtigen Fragen an die Hand. Er ist keine Rechtsberatung im Einzelfall und kann nicht alle Fragen behandeln, die sich in einem konkreten Fall stellen. Für verbindliche Auskünfte wenden Sie sich an eine Rechtsanwältin oder einen Rechtsanwalt. Alle Angaben wurden sorgfältig recherchiert, Stand Oktober 2026. Gesetze, Rechtsprechung und Anbieterbedingungen ändern sich, eine Gewähr für Vollständigkeit und Aktualität übernehmen wir nicht.

Herausgeber: CORIDAS GmbH, Corinna Göring, Dreiweiherweg 1A, 86529 Schrobenhausen · ZeoAI, Savas Kozluklu (MBA), Eulenweg 2, 85253 Erdweg. © 2026. Weitergabe des unveränderten Reports ausdrücklich erwünscht.