

PROINNOVA·KI

KI & DSGVO im Unternehmen

Wie du KI in deinem Unternehmen rechtssicher einsetzt, Bußgelder vermeidest und aus unkontrollierter Schatten-KI ein steuerbares System machst.

→ Die Lage in Zahlen · DSGVO & EU AI Act für Anwender · Typische Fehler · Fahrplan in 5 Schritten
· Konforme Anwendungsfälle

kiberatung24.de

Proinnova KI-Beratung — Thomas Schulten

WARUM DIESER REPORT

Mehr KI, weniger Risiko

KI ist im deutschen Mittelstand angekommen — die Rechtssicherheit hinkt spürbar hinterher. Diese Lücke schließt dieser Report, damit du KI produktiv einsetzt, ohne aus Unsicherheit vor der DSGVO zu bremsen.

Die Nutzung von KI-Tools in deutschen Unternehmen hat sich innerhalb weniger Jahre deutlich beschleunigt (Bitkom Digitalverband, Branchenumfragen 2024/2025). Gleichzeitig nennt ein erheblicher Teil der Unternehmen unklare Regulierung und strenge Datenschutzanforderungen als größte Hürde für den KI-Einsatz. Die Folge ist ein teurer Stillstand: KI wird entweder pauschal verboten und wandert in die „Schatten-IT“, oder sie läuft unbeobachtet weiter. Beides erhöht das Risiko, statt es zu senken.

TIPP

Der Kern des Problems: Nach wiederholten Erhebungen von IT-Sicherheitsanbietern geben Beschäftigte branchenübergreifend regelmäßig Firmendaten in KI-Tools ein — ein großer Teil davon über private, vom Unternehmen nicht verwaltete Accounts (u. a. LayerX Security, Browser-Sicherheitsstudien 2024/2025). Ob das auch in deinem Betrieb passiert, ist selten eine Frage des Ob, sondern des Wissens darüber.

Für wen dieser Report ist. Du führst ein Unternehmen zwischen 5 und einigen hundert Mitarbeitenden. Irgendwo in deinem Team tippt gerade jemand einen Kundennamen oder einen Vertragsentwurf in ein kostenloses KI-Tool — ohne dich zu fragen. Du willst die Produktivität, aber nicht die Schlagzeile. Dieser Report ersetzt keinen Anwalt, gibt dir aber die Übersicht, mit der du die richtigen Fragen stellst und die richtigen Entscheidungen triffst.

WAS DICH ERWARTET

#	Kapitel	Inhalt
1	Die Lage in Zahlen	Wie verbreitet Schatten-KI im Mittelstand wirklich ist.
2	Was rechtlich gilt	DSGVO-Kernpflichten, EU AI Act für Anwender, Bußgeldrahmen.
3	Wo deine Daten landen	Consumer- vs. Business-Tarif, AVV, Trainingsnutzung.
4	Typische Fehler	Drei Praxisbeispiele, die im Mittelstand immer wieder vorkommen.
5	Der Fahrplan	Fünf Schritte plus Checkliste, diese Woche startbar.
6	Konforme Anwendungsfälle	Sechs Einsatzfelder, die mit dem richtigen Setup laufen.

KAPITEL 1 · DIE LAGE

Wo der Mittelstand bei KI wirklich steht

Die Wahl, ob KI in dein Unternehmen kommt, ist in den meisten Fällen längst gefallen — nur nicht von dir. Vier Beobachtungen beschreiben die Lage, und sie hängen alle an derselben Ursache: Niemand steuert zentral, wer KI wie und mit welchen Daten nutzt.

1 · Adoption läuft, Leitplanken fehlen. Der Anteil der Unternehmen, die KI aktiv einsetzen, ist laut Bitkom-Digitalverband innerhalb weniger Jahre stark gestiegen. Die Nutzung ist da — Richtlinien, Schulungen und Freigabeprozesse halten in den meisten Betrieben nicht Schritt.

2 · Shadow AI ist Alltag. Mehrere unabhängige Sicherheitsstudien kommen unabhängig voneinander zu demselben Bild: Ein großer Teil der KI-Nutzung am Arbeitsplatz läuft über private, kostenlose Accounts, die weder vertraglich noch technisch an das Unternehmen angebunden sind.

3 · Rechtsunsicherheit bremst. In Bitkom-Umfragen nennen Unternehmen regelmäßig unklare Regulierung und strenge Datenschutzanforderungen als eine der größten Hürden beim KI-Einsatz — noch vor Kosten- oder Kompetenzfragen.

4 · Governance fehlt. Nur eine Minderheit der deutschen Unternehmen verfügt laut Bitkom-Erhebungen über verbindliche Regeln zur KI-Nutzung. Die große Mehrheit arbeitet ohne dokumentierte Richtlinie.

TIPP

Am eigentlichen Problem ändert kein neues Tool etwas. Diese vier Baustellen verschwinden nicht, weil du ein anderes KI-Tool kaufst. Sie verschwinden erst, wenn eine Person, eine Richtlinie und ein Vertrag festlegen, was erlaubt ist — und was nicht.

VERBIETEN, LAUFEN LASSEN ODER STEUERN

Für den Umgang mit Schatten-KI gibt es im Kern drei Wege — zwei davon vergrößern das Risiko:

Weg	Was passiert
Verbieten	Klingt sicher, verlagert die Nutzung aber auf private Handys und Accounts. Du verlierst jede Sicht auf das Geschehen und behältst das volle Risiko.
Laufen lassen	Wer KI einfach gewähren lässt, sammelt unbemerkt Datenabflüsse, fehlende Verträge und Verstöße an. Das Risiko wächst mit jedem Tag.
Steuern	Klare Regeln, geprüfte Anbieter und ein zentraler Zugang machen aus dem Risiko einen Vorteil. Nur dieser Weg nutzt KI und hält die DSGVO gleichzeitig ein.

KAPITEL 2 · WAS RECHTLICH GILT

DSGVO und EU AI Act für Anwender

Du musst nicht spekulieren, woran deine KI-Nutzung gemessen wird. Der Kernsatz aus der abgestimmten Orientierungshilfe der deutschen Datenschutzaufsichtsbehörden zu KI (Stand 2024) ist unbequem einfach: Für jeden Verarbeitungsschritt, bei dem eine KI personenbezogene Daten verarbeitet, brauchst du eine Rechtsgrundlage.

Artikel	Was er beim KI-Einsatz verlangt
Art. 5, 6 DSGVO	Rechtsgrundlage und klare Zweckbindung für jeden Verarbeitungsschritt mit Personendaten.
Art. 28 DSGVO	Auftragsverarbeitungsvertrag (AVV) mit dem Anbieter, sobald dieser Personendaten in deinem Auftrag verarbeitet.
Art. 35 DSGVO	Datenschutz-Folgenabschätzung (DSFA), wenn ein hohes Risiko besteht — bei KI-Anwendungen häufig der Fall.
Art. 22 DSGVO	Menschliche Letztentscheidung mit echtem Spielraum bei Entscheidungen mit rechtlicher Wirkung für Personen (z. B. Bewerbungen).

Ein Vertrag nach Art. 28 DSGVO und abgeschaltetes Training sind wichtige Bausteine, aber kein Freibrief: Sie ersetzen weder Rechtsgrundlage und Zweckbindung noch Dokumentation. Auch Betroffenenrechte gelten technisch: Auskunft (Art. 15), Berichtigung (Art. 16) und Löschung (Art. 17) betreffen auch Ausgaben, die eine KI über eine Person erzeugt — selbst falsche.

DER EU AI ACT TRIFFT DICH SCHON HEUTE

Wer ChatGPT, Copilot oder ein vergleichbares Werkzeug im Betrieb nutzt, ist rechtlich „Anwender“ (Deployer), nicht „Anbieter“, und fällt in der Regel nicht unter die schweren Hochrisiko-Pflichten. Trotzdem gelten seit dem 2. Februar 2025 zwei Dinge verbindlich: das Verbot bestimmter KI-Praktiken und die KI-Kompetenz-Pflicht nach Art. 4 AI Act — für jeden Betreiber, unabhängig von der Unternehmensgröße.

TIPP

Wo aus reiner Nutzung Hochrisiko wird: sobald eine KI in Personalentscheidungen (Bewerber-Screening, Ranking) oder in die Kreditwürdigkeitsprüfung eingreift (Anhang III AI Act). Dann greifen weitergehende Pflichten, unter anderem echte menschliche Aufsicht und ggf. die Information des Betriebsrats. Das ist die Grenze, die du kennen musst.

BUSSGELDER — UND EINE PERSÖNLICHE HAFTUNG

DSGVO und EU AI Act sanktionieren getrennt, für denselben Vorgang können beide Rahmen greifen. Der teuerste Teil steht selten in der Pressemeldung: Die Geschäftsführung kann neben dem Unternehmen persönlich mithaften, wenn ein dokumentiertes Datenschutz- und Governance-System fehlt (Sorgfaltspflicht nach § 43 GmbHG).

Rahmen	Obere Stufe	Greift bei
Art. 83 DSGVO	bis 20 Mio. € oder 4 % des weltweiten Jahresumsatzes	Verstöße gegen Grundsätze, Rechtsgrundlage, Betroffenenrechte, Drittlandtransfer

Rahmen	Obere Stufe	Greift bei
Art. 99 AI Act	bis 35 Mio. € oder 7 % (nur verbotene Praktiken), sonst niedrigere Stufen	Deployer-, Transparenz- und Anbieterpflichten

Dass diese Zahlen keine Theorie sind, zeigen mehrere öffentlich bekannte Verfahren europäischer Datenschutzbehörden der vergangenen Jahre: gegen Gesichtserkennungs-Anbieter wegen Verarbeitung ohne Rechtsgrundlage, gegen Chat-/Companion-Apps wegen fehlender Rechtsgrundlage und Alterskontrolle, sowie mehrere Verfahren rund um KI-Trainingsdaten und internationale Datenübermittlung. Die kumulierten DSGVO-Bußgelder seit 2018 liegen europaweit im hohen einstelligen Milliardenbereich.

KAPITEL 3 · WO DEINE DATEN LANDEN

Der Vertrag entscheidet, nicht das Modell

Ob ein KI-Tool DSGVO-tauglich ist, hängt selten am Modell und fast immer am Tarif und Vertrag dahinter. Dasselbe Sprachmodell ist im kostenlosen Privat-Account ein Datenschutz-Problem, im Business- oder Enterprise-Vertrag dagegen beherrschbar. Vier Fragen trennen das eine vom anderen:

Frage	Worauf es ankommt
Training	Werden deine Eingaben zum Modelltraining genutzt? Bei Business-/Enterprise-Tarifen und API in der Regel nein, bei kostenlosen Consumer-Versionen häufig per Default ja.
AVV	Gibt es einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO? Bei Business-Tarifen üblich, beim kostenlosen Privat-Account in der Regel nicht vorhanden.
EU-Residenz	Kannst du Speicherung und Verarbeitung in der EU erzwingen? Zunehmend ja — oft aber nur für ruhende Daten, nicht für die eigentliche Verarbeitung.
Rechtszugriff	Wessen Recht regelt den Zugriff auf deine Daten? Ein EU-Rechenzentrum beantwortet nur, wo die Daten liegen — nicht, welches Recht für den Zugriff gilt (Stichwort US CLOUD Act).

Anbieter / Tarif	Training mit deinen Daten?	AVV möglich?	Einordnung
ChatGPT — Free/Plus (Consumer)	Ja, per Default	Nein	Für Business ungeeignet ohne Zusatzvertrag
ChatGPT — Team/Enterprise/API	Nein (vertraglich zugesichert)	Ja	Geeigneter Weg für den Betrieb
Microsoft 365 Copilot (Business)	Nein (vertraglich zugesichert)	Ja	EU-Residenz beachten, Einstellungen prüfen
Claude — Consumer	Ja, per Default	Nein	Für Business ungeeignet ohne Zusatzvertrag
Claude for Work / API	Nein (vertraglich zugesichert)	Ja	Geeigneter Weg für den Betrieb
Google Gemini — Consumer	Ja, per Default	Nein	Für Business ungeeignet ohne Zusatzvertrag
Gemini Workspace / Vertex AI	Nein (vertraglich zugesichert)	Ja	Geeigneter Weg für den Betrieb

Angaben nach öffentlicher Anbieter-Dokumentation, Stand der Reporterstellung. Anbieterbedingungen ändern sich — vor dem produktiven Einsatz die aktuellen AVV- und Trainings-Angaben des jeweiligen Anbieters selbst prüfen.

TIPP

Der teuerste Vertrag ist der, den es nicht gibt. Ein Business- oder Enterprise-Tarif mit abgeschaltetem Training und Auftragsverarbeitungsvertrag bringt dich in Tagen in einen datenschutzfreundlicheren Zustand. Rechtsgrundlage, Zweckbindung und Dokumentation musst du trotzdem je Verarbeitung selbst sicherstellen — der Vertrag allein macht dich nicht konform.

KAPITEL 4 · TYPISCHE FEHLER

Wo Mittelständler am häufigsten stolpern

Die meisten DSGVO-Verstöße bei KI passieren aus Unwissen, nicht aus böser Absicht. Drei Muster tauchen im Mittelstand immer wieder auf.

FEHLER 1 · KUNDENDATEN IM PRIVATEN ACCOUNT

Ein Mitarbeiter kopiert eine Kundenliste oder einen Vertragsentwurf in seinen kostenlosen, privaten KI-Account, um schneller fertig zu werden. In vielen Consumer-Tarifen ist das Training auf Eingaben standardmäßig aktiv, ein AVV existiert nicht. Damit fehlen Rechtsgrundlage, Vertragsgrundlage und Transfer-Absicherung gleichzeitig.

Stattdessen: klare Nutzungsrichtlinie, betriebliche Business-Accounts mit AVV, wo möglich Pseudonymisierung, bevor Daten in ein Modell gehen.

FEHLER 2 · DAS MEETING, DAS UNBEMERKT MITSCHREIBT

Ein KI-Notiztool sitzt automatisch in Videocalls und transkribiert mit, ohne dass Teilnehmende informiert werden. Verarbeitet wird häufig auf Servern außerhalb der EU. Aus einer Bequemlichkeit wird schnell ein Datenschutz- und je nach Fall auch ein strafrechtliches Thema (heimliche Aufzeichnung nichtöffentlich gesprochener Worte, § 201 StGB).

Stattdessen: Teilnehmende aktiv informieren und Widerspruch ermöglichen, ein EU-Tool mit Löschkonzept wählen, den Betriebsrat bei Bedarf einbinden.

FEHLER 3 · BEWERBER-VORWAHL OHNE MENSCH

Die Personalabteilung lässt Bewerbungen von einer KI vorsortieren und ranken, faktisch ohne echte menschliche Prüfung. Das kollidiert mit Art. 22 DSGVO (keine ausschließlich automatisierte Entscheidung mit rechtlicher Wirkung) und gilt zugleich als sensibler Bereich im EU AI Act.

Stattdessen: menschliche Letztentscheidung dokumentieren, Bewerber informieren, Business-Account mit AVV nutzen, bei Bedarf eine DSFA einplanen.

KAPITEL 5 · DER FAHRPLAN

Fünf Schritte, diese Woche startbar

Ein umfangreicher Compliance-Apparat ist nicht nötig — eine handhabbare Reihenfolge reicht. Jeder Schritt baut auf dem vorigen auf.

1 Bestandsaufnahme (Shadow-AI-Audit)

Erfasse, welche KI-Tools bereits laufen — offiziell und inoffiziell. Ohne diese Inventur weißt du nicht, wo deine Daten heute schon abfließen. Aufwand: wenige Tage.

2 KI-Nutzungsrichtlinie erlassen

Eine Whitelist zugelassener Tools und Zwecke plus klare Verbote. Konkrete Beispiele wirken besser als abstrakte Verbote. Aufwand: 1–2 Wochen.

3 Schulung nach Art. 4 AI Act

Die KI-Kompetenzpflicht gilt seit 02.02.2025 für jeden Betreiber. Ein rollen- und risikobezogenes, dokumentiertes Format reicht. Aufwand: initial 1–2 Wochen, danach laufend.

4 Anbieter- und AVV-Check

Prüfe für jedes eingesetzte Tool: Auftragsverarbeitungsvertrag, EU-Hosting, Trainings-Opt-out. Aufwand: wenige Tage je Tool.

5 Freigabeprozess und Monitoring

Lege fest, wie neue Tools genehmigt werden, und prüfe laufend nach. Governance ist eine Routine ohne Enddatum.

TIPP

Schritte 2 und 3 sind der schnellste Hebel. Beide sind in wenigen Wochen mit kleinem Budget umsetzbar und decken bereits den größten Risikoteil ab: die ungesteuerte Schatten-KI und die Kompetenzpflicht aus Art. 4 AI Act. Mit einer sauberen Richtlinie gehörst du zur Minderheit der Unternehmen, die KI-Regeln überhaupt dokumentiert hat.

CHECKLISTE · WAS IN DIE KI-NUTZUNGSRICHTLINIE GEHÖRT

- Zugelassene Tools und Zwecke als Whitelist mit klaren Grenzen
- Verbot, personenbezogene Daten oder Geschäftsgeheimnisse in offene Systeme einzugeben
- Besondere Vorsicht bei sensiblen Datenkategorien nach Art. 9 DSGVO (Gesundheit, Religion u. a.)
- Pflicht zur Ergebnisprüfung durch einen Menschen mit echtem Entscheidungsspielraum
- Nutzung nur über betriebliche Accounts und Geräte
- Klarer Meldeweg für Zweifelsfälle

KAPITEL 6 · KONFORME ANWENDUNGSFÄLLE

Sechs Einsatzfelder für den Alltag

Der Bauplan steht — jetzt zählt, was er im Alltag möglich macht. Die folgenden sechs Einsatzfelder sind im Mittelstand am häufigsten gefragt und mit dem richtigen Setup konform umsetzbar: ein Auftragsverarbeitungsvertrag mit dem Anbieter, eine dokumentierte Rechtsgrundlage samt Zweckbindung, und die Regel, dass keine Personendaten in offene Systeme wandern.

Anwendungsfall	Was es tut	DSGVO-Hinweis
E-Mail- & Angebotsbearbeitung	Entwürfe, Antworten und Angebote vorformulieren	Kundendaten nur über betrieblichen Account mit AVV, kein Training auf Eingaben
Meeting-Zusammenfassungen	Gespräche transkribieren und in Protokolle fassen	Vor Aufnahme Rechtsgrundlage/Einwilligung sichern, geschlossenes System nutzen
Dokumentenanalyse	Felder und Kernaussagen aus Dokumenten ziehen	Bei Personenbezug Verarbeitungsverzeichnis führen, Ergebnis menschlich prüfen
Interner Wissensassistent	Fragen aus eigenem Firmenwissen beantworten (RAG)	Rechte- und Zugriffskonzept, EU-Hosting, Löschkonzept
Support-Chatbot	Kundenanfragen automatisiert vorqualifizieren	Transparent machen, dass ein Bot antwortet; kein Personenbezug ins offene Modell
Recruiting-Unterstützung	Bewerbungen vorsortieren und aufbereiten	Keine automatisierte Letztentscheidung, Mensch entscheidet, DSFA einplanen

Das Muster hinter allen sechs Fällen ist dasselbe: ein geschlossenes oder Business-System, ein AVV mit dem Anbieter, keine Personendaten in offenen Modellen, und ein Mensch prüft das Ergebnis. Wer dieses Muster einmal aufsetzt, kann Anwendungsfall für Anwendungsfall anschließen, ohne jedes Mal bei null zu beginnen.

FAZIT

Aus Pflicht wird Vorsprung

Die DSGVO ist nicht dein eigentliches Problem. Dein Problem ist unkontrollierte KI-Nutzung, die häufig gerade aus der Angst vor der DSGVO entsteht. Wer KI verbietet oder unbeobachtet laufen lässt, hat das Risiko schon im Haus. Wer sie steuert, macht aus der Compliance-Frage einen Vorsprung: schnellere Prozesse, offene Nutzung im Team, Vertrauen bei Kunden.

DEINE PRIORITÄTEN FÜR DIE NÄCHSTEN 90 TAGE

Zeitraum	Priorität
Diese Woche	Bestandsaufnahme: Frag in jeder Abteilung, welche KI-Tools bereits genutzt werden — offiziell und inoffiziell.
Diesen Monat	KI-Nutzungsrichtlinie erlassen und die Schulung nach Art. 4 AI Act aufsetzen.
Dieses Quartal	Anbieter und Verträge prüfen, Architektur entscheiden, erste Anwendungsfälle offiziell freigeben.

ACHTUNG

Dieser Report ist Orientierung, keine Rechtsberatung. Für verbindliche Rechtsfragen im Einzelfall — etwa die konkrete Rechtsgrundlage, eine Betriebsvereinbarung oder eine formale Datenschutz-Folgenabschätzung — zieh einen Datenschutzanwalt oder deinen Datenschutzbeauftragten hinzu. Eine gute Beratung ersetzt das nicht, sie sorgt dafür, dass du mit den richtigen Fragen dorthin kommst.

NÄCHSTER SCHRITT

Erst telefonieren, dann richtig hinsehen

Ein kurzes Telefonat zur Bedarfsklärung kostet nichts und verpflichtet zu nichts. Wenn wir uns deinen Fall wirklich ansehen sollen, geht es weiter mit 30 Minuten Videoberatung für 49,00 € inkl. MwSt. — bei Auftrag innerhalb von drei Monaten wird der Betrag vollständig angerechnet: kiberatung24.de/erstgesprach

kiberatung24.de · info@kiberatung24.de · 0176 61518248

ÜBER DIESEN REPORT

Herausgeber und rechtlicher Hinweis

Herausgegeben von Proinnova — Thomas Schulten, Mittelstraße 1, 56379 Winden, Deutschland. E-Mail: info@kiberatung24.de, Telefon: 0176 61518248. Vollständiges Impressum unter kiberatung24.de/impressum.

Proinnova ist eine KI-Beratung für den deutschen Mittelstand: persönliche Beratung vor Ort, Konzeption und Umsetzung von KI-Lösungen — von Telefon- und Chat-Agenten über Prozessautomatisierung bis zu DSGVO-konformen internen KI-Arbeitsplätzen.

Rechtlicher Hinweis. Dieser Report fasst öffentlich zugängliche Informationen zu DSGVO und EU AI Act laienverständlich zusammen und ersetzt keine Rechtsberatung im Einzelfall. Er begründet kein Mandatsverhältnis und keine Beratungsleistung im rechtlichen Sinne. Verwendete Zahlen und Studienangaben stammen aus öffentlich zugänglichen Quellen (u. a. Bitkom Digitalverband, IT-Sicherheitsstudien) zum Zeitpunkt der Reporterstellung und können sich ändern. Für verbindliche Aussagen zu deinem Einzelfall zieh bitte einen Datenschutzanwalt oder deinen Datenschutzbeauftragten hinzu.

© 2026 Proinnova — Innovative KI. Alle Rechte vorbehalten.