Schatten-KI im Mittelstand

Warum ungenehmigte KI-Nutzung Geschäftsführer schon heute persönlich haftbar macht, und warum der EU AI Act den Druck weiter erhöht

Ein Whitepaper von Avolang, KI-Compliance- und Datenschutzberatung

Stand: Juli 2026

> **Kernbotschaft in einem Satz:** In der überwiegenden Mehrheit der mittelständischen Unternehmen nutzen Beschäftigte generative KI wie ChatGPT längst ohne Genehmigung, während die Geschäftsführung meint, KI spiele bei ihr noch keine Rolle. Genau diese Lücke zwischen gelebter Praxis und dokumentierter Steuerung ist schon heute ein persönliches Haftungsrisiko der Leitungsebene, und der EU AI Act erhöht den Druck weiter.

Zusammenfassung für Eilige

1. **Schatten-KI ist der Normalfall, nicht die Ausnahme.** Je nach Studie nutzen zwischen rund der Hälfte und über 80 Prozent der Beschäftigten KI-Werkzeuge ohne formale Freigabe [61][65][102]. 78 Prozent bringen ihre eigenen Tools mit, in kleinen und mittleren Unternehmen sogar 80 Prozent (Microsoft/LinkedIn Work Trend Index) [56][57].
2. **Der Mittelstand ist besonders exponiert.** Nur rund 20 Prozent der mittelständischen Unternehmen setzen KI aktiv und gesteuert ein (KfW, DIHK) [28][38], während die Belegschaft die Technik längst privat verwendet. Vier von zehn Unternehmen mit mehr als 20 Beschäftigten gehen selbst davon aus, dass ihre Leute generative KI über Privatzugänge im Arbeitskontext nutzen (Bitkom) [32][101].
3. **Der Rechtsrahmen greift schon heute.** Die Pflicht zur KI-Kompetenz (Art. 4 AI Act) gilt seit dem 2. Februar 2025 und wurde durch den Digital Omnibus ausdrücklich nicht verschoben [3][10][124]. Verbotene Praktiken (Art. 5) sind seit Februar 2025 untersagt, mit Bußgeldern bis 35 Mio. Euro oder 7 Prozent des weltweiten Jahresumsatzes [5][7]. Die teureren Hochrisiko-Pflichten wurden vom 2. August 2026 auf den 2. Dezember 2027 verschoben, die grundlegenden Pflichten aber nicht [121][124].

4. **Die eigentliche Bombe ist die persönliche Haftung.** Bußgelder aus dem AI Act treffen zwar das Unternehmen. Über die Legalitäts- und Compliance-Pflicht (§ 43 GmbHG, § 93 AktG) und die Aufsichtspflicht (§ 130 OWiG) schlägt ein Verstoß aber auf die Geschäftsführung durch, bis ins Privatvermögen [75][77][78][7].
5. **Dokumentation entscheidet über die Haftung.** Wer nicht nachweisbar aufklärt, schult und steuert, verliert im Schadensfall den Schutz der Business Judgement Rule und trägt die Beweislast. Fehlende Dokumentation wirkt faktisch wie eine Beweislastumkehr zulasten des Geschäftsführers [78][35].
6. **Darauf wird kaum hingewiesen.** Die öffentliche Debatte dreht sich um Produktivität und Innovation. Dass unterlassene, undokumentierte Aufklärung über Schatten-KI die Leitungsebene persönlich angreifbar macht, ist im Mittelstand weitgehend unverstanden. Genau diese Aufklärungslücke schließt dieses Papier.

---

1. Was Schatten-KI ist und wie groß das Problem wirklich ist

Schatten-KI bezeichnet die Nutzung von KI-Werkzeugen durch Beschäftigte ohne Freigabe, ohne Kenntnis und ohne Kontrolle der IT-, Datenschutz- oder Compliance-Verantwortlichen [107][106]. Der Begriff ist die logische Fortsetzung der klassischen Schatten-IT: Wo früher heimlich ein Cloud-Speicher genutzt wurde, kopieren Mitarbeitende heute Kundenlisten, Vertragsentwürfe oder Quellcode in einen Chatbot, dessen Server außerhalb des Unternehmens und häufig außerhalb der EU stehen [42][43].

Die Zahlen sind eindeutig und stammen aus voneinander unabhängigen, methodisch seriösen Erhebungen:

Quelle	Befund
Microsoft/LinkedIn, Work Trend Index 2024	75 % der Wissensarbeiter nutzen KI am Arbeitsplatz, 78 % bringen eigene Tools mit ("Bring Your Own AI"), im Mittelstand 80 % [56][57]
UpGuard, State of Shadow AI (1.020 Beschäftigte + 542 Sicherheitsverantwortliche, Erhebung Jul./Aug. 2025, veröffentlicht 10.11.2025)	81 % der Beschäftigten nutzen nicht freigegebene KI-Tools, bei Sicherheitsverantwortlichen 88 bis 90 % [65][66]
Cyberhaven (2023, älteste hier zitierte Studie, weiterhin meistzitiert)	11 % aller Inhalte, die Beschäftigte in ChatGPT einfügen, sind vertraulich; Spitzenkategorien: interne Daten, Quellcode, Kundendaten [61][62][111]
Cisco, Data Privacy Benchmark 2025	46 % geben Mitarbeiter- oder Personendaten, 42 % nicht öffentliche Firmendaten, 31 % Kundendaten in GenAI-Tools ein [59][60]
KPMG/Univ. Melbourne, Trust in AI 2025 (47 Länder, 48.000 Befragte)	Die Hälfte der Beschäftigten nutzt KI, ohne zu wissen, ob es erlaubt ist; 44 % nutzen sie wissentlich unzulässig [50][51][52]
Handelsblatt/ZEW, 2025 (repräsentative Befragung, rund 1.500 Unternehmen, März/April 2026)	Sieben von zehn Beschäftigten (71 %) nutzen KI-Tools ohne Unternehmensfreigabe; nur 4 % (IT-Branche) bzw. 8 % (verarbeitendes Gewerbe) der Firmen verbieten die Nutzung ausdrücklich [102]
DFKI/Springer, "Von Schatten-IT zu Schatten-KI durch ChatGPT" (Högemann/Hauff/Thomas 2026, qualitative Praxisanalyse)	Bestätigt dieselben Risikomuster qualitativ: Datenlecks, Halluzinationen, fehlende Transparenz, unklare Berechtigungen; ohne eigene quantitative Kennzahl [42][43]

Bemerkenswert: Schatten-KI ist kein Phänomen der jungen Belegschaft allein, es zieht sich durch alle Generationen und Hierarchieebenen. Führungskräfte gehören zu den intensivsten Nutzern nicht freigegebener Werkzeuge [66][109]. Und die Nutzung erfolgt bewusst verdeckt: 52 Prozent der KI-Nutzer geben ihren Einsatz für wichtige Aufgaben nicht zu, aus Sorge, ersetzbar zu wirken [56].

Warum das gefährlich ist: Modelle wie ChatGPT, Gemini oder Claude nehmen Eingaben entgegen, verarbeiten sie auf externen Servern und können sie in den kostenlosen und einfachen Plänen zur Modellverbesserung weiterverwenden [3][61]. Eine einzige unbedachte Eingabe kann interne Informationen offenlegen. Landen diese Daten bei einem Anbieter außerhalb der EU, kann bereits darin ein DSGVO-Verstoß liegen [101][99].

---

2. Warum gerade der Mittelstand im Blindflug ist

Der deutsche Mittelstand steht vor einer besonderen Gefährdungslage, weil zwei Kurven auseinanderlaufen: Die private, ungesteuerte Nutzung eilt der offiziellen, gesteuerten Einführung weit voraus.

- Laut **KfW-Digitalisierungsbericht Mittelstand** setzen rund 20 Prozent der mittelständischen Unternehmen KI aktiv ein, eine Verfünffachung binnen sechs Jahren, aber eben nur ein Fünftel [28][29]

[30][31].

- Die **DIHK-Digitalisierungsumfrage 2026** (knapp 5.000 Unternehmen) bestätigt: Über alle Größen 41 Prozent aktive KI-Nutzung, im Mittelstand aber nur rund 20 Prozent. Größte Hürde ist nicht die Technik, sondern das Vertrauen; rund die Hälfte sorgt sich um Datensicherheit, 53 Prozent misstrauen außereuropäischen Anbietern [38].
- **Bitkom** (Studie 2026, Befragung KW 27 bis 32/2025) zeigt: 36 Prozent aller Unternehmen setzen KI bereits ein, eine Verdopplung gegenüber 20 Prozent im Vorjahr 2024. Beim Zugang zu generativer KI zeigt sich ein Größengefälle: 21 Prozent der Unternehmen mit 20 bis 49 Beschäftigten stellen ihn bereit, 31 Prozent bei 50 bis 499 Beschäftigten, 43 Prozent ab 500 Beschäftigten [32].
- Das **IW Köln** verortet Deutschland im EU-Vergleich nur auf Rang elf bei der KI-Implementierung, hinter Dänemark, Finnland und den Niederlanden [34][36].

Das Ergebnis ist eine trügerische Ruhe in vielen Chefetagen: Weil KI "offiziell" kaum eingeführt ist, hält die Geschäftsführung das Thema für nachrangig. Tatsächlich ist die Belegschaft längst dabei, nur eben unsichtbar. Genau in dieser Kombination aus hoher realer Nutzung und niedriger dokumentierter Steuerung liegt das Haftungsrisiko. Der Mittelstand verfügt zudem seltener als Konzerne über dedizierte Compliance-, Datenschutz- und IT-Sicherheitsfunktionen, die das Problem auffangen könnten [38][40].

---

3. Der Rechtsrahmen: Was der EU AI Act wann verlangt

Der **EU AI Act** (Verordnung (EU) 2024/1689) ist seit dem 1. August 2024 in Kraft und gilt unmittelbar in allen Mitgliedstaaten, ohne nationale Umsetzung [1][2][82]. Er wirkt gestaffelt, und die Termine der Hochrisiko-Ebene wurden 2026 durch den **Digital Omnibus** nach hinten verschoben (Details in Abschnitt 3.5):

Datum	Was gilt
2. Februar 2025	Verbotene Praktiken (Art. 5) und **KI-Kompetenzpflicht (Art. 4)**, beide durch den Digital Omnibus **nicht** verschoben [3][4][124]
2. August 2025	Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (GPAI)
2. August 2026	Transparenzpflichten (Art. 50); Wasserzeichen-Schonfrist für laufende Systeme bis 2. Dezember 2026 [124][125]
2. Dezember 2027	Hochrisiko-Pflichten Anhang III (nach Verschiebung durch den Digital Omnibus, zuvor 2. August 2026) [121][124]
2. August 2028	Hochrisiko-KI als Sicherheitskomponente in regulierten Produkten (Anhang I) [122]

Für den Mittelstand sind vier Bausteine besonders relevant.

3.1 Die KI-Kompetenzpflicht (Art. 4), seit Februar 2025 bindend

Art. 4 verpflichtet **Anbieter und Betreiber**, ein ausreichendes Maß an KI-Kompetenz ihres Personals und aller Personen sicherzustellen, die in ihrem Auftrag KI-Systeme betreiben oder nutzen [3][10][11]. Das gilt

unabhängig von Größe und Branche und erfasst ausdrücklich auch Unternehmen, die "nur" ChatGPT, Übersetzungstools oder KI-gestützte Recruiting-Software einsetzen [113][114].

Wichtig zu verstehen: Art. 4 ist kein starres Curriculum, sondern eine **Organisationspflicht**. Wie ein Unternehmen sie erfüllt, bleibt ihm überlassen: durch Schulungen, interne Richtlinien, Multiplikatorenprogramme [113]. Die Europäische Kommission hat dazu ein "Living Repository" mit über 40 Praxisbeispielen veröffentlicht, weist aber ausdrücklich darauf hin, dass deren Kopie **keine** automatische Konformitätsvermutung begründet [8][9]. Überwacht wird Art. 4 durch die nationalen Marktüberwachungsbehörden [9]. Zwei Präzisierungen dazu: Art. 99 listet Art. 4 nicht unter den bußgeldbewehrten Vorschriften, es gibt also **keinen eigenen Bußgeldtatbestand** für Verstöße gegen die KI-Kompetenzpflicht als solche [131]. Und praktisch durchsetzen (mit Aufsichtsmaßnahmen) können die Marktüberwachungsbehörden erst, seit sie selbst eingerichtet sind, in Deutschland also erst mit dem KI-Durchführungsgesetz 2026 [131]. Rechtlich bindend war Art. 4 aber ununterbrochen bereits seit dem 2. Februar 2025, und ein Verstoß kann, wie gezeigt, andere Haftungstatbestände (Sorgfaltspflicht, Beweislast) auslösen, auch ohne eigenes Bußgeld.

Entscheidend für die Haftungsfrage: Auch wenn Art. 4 kein unmittelbares Bußgeld auslöst, empfehlen praktisch alle Fachstellen eine **lückenlose Dokumentation**, wer wann mit welchen Inhalten geschult wurde, um im Schadensfall die Sorgfaltspflicht belegen zu können [113][116][117].

3.2 Hochrisiko-KI, besonders im Personalwesen

Anhang III der Verordnung stuft KI-Systeme im **Beschäftigungskontext** ausdrücklich als hochriskant ein: das Schalten von Stellenanzeigen, das Screening und Matching von Bewerbern, die Bewertung im Auswahlprozess sowie Systeme, die über Beförderung oder Beendigung von Arbeitsverhältnissen mitentscheiden [83][84]. Diese Pflichten greifen nach der Verschiebung durch den Digital Omnibus ab dem **2. Dezember 2027** (siehe 3.5), inhaltlich unverändert. Es sind fünf Kernpflichten [83][84][121]:

1. **Menschliche Aufsicht** über jede personalrelevante Entscheidung (Art. 14). Die KI darf vorbereiten und priorisieren, aber nicht autonom aussortieren.
2. **Transparenz** gegenüber Bewerbern über den KI-Einsatz.
3. **Dokumentation und Nachvollziehbarkeit** der Systeme.
4. **KI-Kompetenz** des eingesetzten Personals (Art. 4, seit Februar 2025).
5. **Aktive Prüfung auf Verzerrung und Diskriminierung**.

Viele mittelständische Unternehmen setzen solche Systeme bereits ein, ohne sich der Hochrisiko-Einstufung bewusst zu sein. Verstöße gegen Hochrisiko-Pflichten werden mit bis zu **15 Mio. Euro oder 3 Prozent** des Jahresumsatzes geahndet [83][7].

3.3 Das Sanktionsregime (Art. 99), gestaffelt und größenabhängig

Verstoß	Bußgeldrahmen
Verbotene Praktiken (Art. 5)	bis 35 Mio. Euro oder **7 %** des weltweiten Jahresumsatzes [5] [7]
Pflichten für Betreiber/Anbieter von Hochrisiko-KI	bis 15 Mio. Euro oder 3 % [7][83]
Falsche/irreführende Angaben gegenüber Behörden	bis 7,5 Mio. Euro oder 1 % [7]

Für Großunternehmen gilt jeweils der **höhere** Wert, für KMU und Start-ups der **niedrigere**, ausdrücklich als Erleichterung gedacht [1][12]. Bei den 35 Mio. Euro handelt es sich also nicht um eine flächendeckende Drohung für jeden ChatGPT-Fehltritt, sondern um die Höchststrafe für verbotene Praktiken. Diese Präzision ist wichtig, weil populäre Darstellungen die Zahl oft pauschal verwenden [I][II]. Der eigentliche Hebel für den Mittelstand liegt nicht in der theoretischen Maximalstrafe, sondern in der Kombination aus DSGVO-Bußgeldern, zivilrechtlichem Schadenersatz und, wie unten gezeigt, der persönlichen Organhaftung.

3.4 Nationale Umsetzung: die Bundesnetzagentur wird Aufsicht

Deutschland hat im Sommer 2026 das **Gesetz zur Durchführung der KI-Verordnung** verabschiedet (Bundestag 11. Juni, Bundesrat 10. Juli 2026) [16][18]. Zentrale Marktüberwachungsbehörde wird die **Bundesnetzagentur**, bei der ein Koordinierungs- und Kompetenzzentrum (KoKIVO) entsteht [17][19]. Jeder Mitgliedstaat muss mindestens ein **KI-Reallabor** bereitstellen; die entsprechende Frist wurde durch den Digital Omnibus vom 2. August 2026 auf den **2. August 2027** verschoben [130]. KMU und Start-ups erhalten priorisierten und kostenlosen Zugang, vereinfachte Dokumentationsformulare und reduzierte Konformitätsgebühren [20][12]. Die Aufsicht ist damit nicht mehr abstrakt, sie hat einen konkreten Adressaten und Durchsetzungsapparat.

3.5 Der Digital Omnibus: Verschiebung der Hochrisiko-Pflichten (Stand Juli 2026)

Mit dem sogenannten **Digital Omnibus**, dem Vereinfachungspaket zum AI Act, haben die EU-Institutionen den Anwendungsbeginn der Hochrisiko-Pflichten nach hinten verschoben. Das EU-Parlament stimmte am 16. Juni 2026 zu, der Rat gab am 29. Juni 2026 grünes Licht, unterzeichnet wurde der Rechtsakt am 8. Juli 2026; die Veröffentlichung im Amtsblatt, die die Verschiebung rechtsverbindlich macht, stand zum Redaktionsschluss dieses Papiers noch aus [121][123][125][132]. Solange sie nicht erfolgt ist, gilt formal noch der ursprüngliche Zeitplan des AI Act, auch wenn mit einer zeitnahen Veröffentlichung zu rechnen ist. Die neuen (noch nicht rechtsverbindlichen) Termine:

- **Hochrisiko-KI nach Anhang III** (eigenständige Systeme, etwa im Recruiting): statt 2. August 2026 nun **2. Dezember 2027** [121][124].
- **Hochrisiko-KI nach Anhang I** (KI als Sicherheitskomponente in regulierten Produkten): **2. August 2028** [122][123].
- **Art. 50 Transparenzpflichten** bleiben beim 2. August 2026; nur die Kennzeichnungspflicht (Wasserzeichen) für bereits laufende generative Systeme erhält eine Schonfrist bis 2. Dezember 2026 [124][125].

Drei Punkte sind für die Haftungsfrage entscheidend und werden leicht überlesen:

1. **Art. 4 (KI-Kompetenz) und Art. 5 (verbotene Praktiken) wurden ausdrücklich NICHT verschoben.** Sie gelten unverändert seit dem 2. Februar 2025 [124][126]. Die Pflicht, Beschäftigte im Umgang mit KI kompetent zu machen, besteht also heute, nicht erst 2027.
2. **Der Omnibus verschiebt nur den Anwendungsbeginn, nicht die inhaltlichen Anforderungen** (Art. 6 bis 27) [121][123]. Die Verschiebung ist zudem an die Verfügbarkeit harmonisierter Normen und Unterstützungswerkzeuge gekoppelt; das Zieldatum 2. Dezember 2027 kann sich also nur weiter nach hinten, nicht nach vorn verschieben [124][126].
3. **Für die Geschäftsführung ist das keine Entwarnung**, sondern eine Verschiebung der teuersten, nicht der grundlegenden Pflichten. Die heute geltenden Anker der persönlichen Haftung (Art. 4, DSGVO, § 43 GmbHG, § 130 OWiG, GeschGehG) bleiben unberührt, und ein Hochrisiko-Konformitätsverfahren bindet ohnehin Monate an Vorlauf.

---

4. Der zweite Rechtskreis: Datenschutz und Geheimnisschutz

Der AI Act ist nur eine von mehreren Rechtsordnungen, die bei Schatten-KI parallel gelten. Für den Mittelstand ist der Datenschutz oft der schnellere und teurere Angriffspunkt.

4.1 DSGVO: schon die Eingabe kann ein Verstoß sein

Kopieren Beschäftigte Kundennamen, E-Mails oder Vertragsdetails in ChatGPT, verarbeiten sie personenbezogene Daten. Ohne Rechtsgrundlage (Art. 6), ohne Auftragsverarbeitungsvertrag (Art. 28) und ohne zulässigen Drittlandtransfer (Art. 44) liegt ein Verstoß nahe [99][100]. Einen Auftragsverarbeitungsvertrag bietet OpenAI nur in den Team-/Enterprise-Plänen, nicht im Standardtarif [99]. Der DSGVO-Bußgeldrahmen reicht bis **20 Mio. Euro oder 4 Prozent** des weltweiten Jahresumsatzes.

Dass die Aufsicht ernst macht, aber auch wie voraussetzungsvoll Durchsetzung ist, zeigt der Fall **OpenAI**: Die italienische Datenschutzbehörde Garante verhängte mit Bescheid Nr. 755 vom **2. November 2024** ein Bußgeld von **15 Mio. Euro** wegen angeblich fehlender Rechtsgrundlage, unzureichender Transparenz und mangelnden Jugendschutzes, zusätzlich zu einer verpflichtenden sechsmonatigen Aufklärungskampagne (öffentlich bekannt wurde der Bescheid erst im Dezember 2024) [97][98][129]. Das Tribunale di Roma hob dieses Bußgeld mit Urteil vom 18. März 2026 (R.G. Nr. 4785/2025) wieder auf, allerdings rein aus **Zuständigkeitsgründen**: Weil OpenAI bereits seit dem 15. Februar 2024 eine irische Niederlassung unterhielt, hätte nach dem DSGVO-Mechanismus der federführenden Aufsichtsbehörde ("One-Stop-Shop", Art. 55/56 DSGVO) die irische Datenschutzbehörde zuständig sein müssen, nicht der Garante. Über die eigentlichen DSGVO-Vorwürfe in der Sache (Art. 33, 5(2), 6, 5(1)(a), 12, 13, 24, 25(1), 83(5)(e) DSGVO) wurde damit **nicht** entschieden, weder zugunsten noch zulasten von OpenAI, das Gericht hat sie ausdrücklich "assorbiti" (nicht geprüft), da bereits der erste Klagegrund durchgriff [129]. Das Urteil erging in erster Instanz durch eine Einzelrichterin am Tribunale di Roma; ob der Garante Revision einlegt, war zum Redaktionsschluss dieses Papiers nicht bekannt [128][129]. Für die Praxis heißt das: Das Verfahren zeigt, dass Aufsichtsbehörden bei generativer KI zu Millionenbußgeldern bereit sind, aber auch, dass Zuständigkeitsfragen (insbesondere bei Anbietern mit EU-Sitz) Verfahren zu Fall bringen können, ein Schutz, den ein rein national tätiges deutsches Unternehmen ohne eigene Auslandsniederlassung im eigenen Fall nicht hat. Der **Europäische Datenschutzausschuss (EDPB)** hat mit dem Bericht seiner

ChatGPT-Taskforce (23. Mai 2024) unabhängig davon den gemeinsamen Prüfmaßstab der Aufsichtsbehörden für Rechtmäßigkeit, Fairness, Richtigkeit und Transparenz festgelegt [13][14].

Für die Praxis maßgeblich ist die **Orientierungshilfe "Künstliche Intelligenz und Datenschutz"** der deutschen Datenschutzkonferenz (DSK) vom Mai 2024, ergänzt um Leitlinien zu technisch-organisatorischen Maßnahmen (Juni 2025) und zu RAG-Systemen (Oktober 2025) [24][25][26][27]. Sie ist die faktische Checkliste, an der sich Aufsichtsbehörden orientieren.

4.2 Geschäftsgeheimnisse: der stille Rechtsverlust

Das **Geschäftsgeheimnisgesetz (GeschGehG)** schützt vertrauliche Informationen nur, solange der Inhaber "angemessene Geheimhaltungsmaßnahmen" ergreift [89][90]. Wer zulässt, dass Beschäftigte Konstruktionsdaten, Kalkulationen oder Strategiepapiere in einen öffentlichen Chatbot eingeben, riskiert, dass die Information ihren rechtlichen Schutzstatus verliert, ganz ohne Bußgeldbescheid, aber mit unmittelbarem Wettbewerbsschaden [88][91].

Der prominenteste Fall ist **Samsung** (2023): Innerhalb von 20 Tagen kam es zu drei dokumentierten Datenabflüssen, unter anderem Halbleiter-Quellcode und interne Meetingprotokolle, die Ingenieure zur Fehlersuche und Zusammenfassung in ChatGPT eingaben. Samsung begrenzte daraufhin die Eingabelänge und führte verpflichtende Schulungen ein [88][103][104][105]. Der Fall ist zum Lehrstück geworden, gerade weil er zeigt: Nicht böse Absicht, sondern gut gemeinte Produktivität verursacht den Schaden.

---

5. Die eigentliche Bombe: die persönliche Haftung der Geschäftsführung

Hier liegt der Kern dieses Papiers, und der am meisten unterschätzte Punkt. Populäre Schlagzeilen datieren die "persönliche Haftung" gern auf einen einzelnen Stichtag [I][II]. Das ist doppelt irreführend: Erstens wurde die Hochrisiko-Ebene durch den Digital Omnibus auf Dezember 2027 verschoben (Abschnitt 3.5), zweitens hängt die persönliche Haftung gar nicht an diesem Datum. Sie ergibt sich aus heute geltendem deutschen Recht in Verbindung mit den bereits anwendbaren Pflichten (Art. 4, DSGVO). Der Mechanismus ist erklärungsbedürftig, und genau deshalb wird er im Mittelstand übersehen.

5.1 Der Übertragungsweg vom Unternehmen zur Person

Die Bußgelder des AI Act richten sich formal gegen das **Unternehmen**. Persönlich haftbar wird die Geschäftsführung über das **deutsche Gesellschafts- und Ordnungswidrigkeitenrecht**:

- **Legalitäts- und Compliance-Pflicht (§ 43 Abs. 1 GmbHG, § 93 Abs. 1 AktG):** Der Geschäftsführer muss dafür sorgen, dass sich das Unternehmen rechtmäßig verhält. Ein Verstoß des Unternehmens gegen den AI Act oder die DSGVO ist zugleich eine mögliche **Pflichtverletzung des Organs** und begründet die **Innenhaftung**: Die Gesellschaft (oder ein Insolvenzverwalter) kann Regress beim Geschäftsführer nehmen, mit dessen Privatvermögen [75][77][78].
- **Aufsichtspflicht (§ 130 OWiG):** Unterlässt die Leitungsperson Aufsichtsmaßnahmen, die eine betriebsbezogene Zuwiderhandlung (etwa den DSGVO-Verstoß eines Mitarbeiters durch Schatten-KI) verhindert hätten, droht ein **Bußgeld gegen die Person selbst**. Über §§ 9, 30 OWiG kann zusätzlich eine Verbandsgeldbuße gegen das Unternehmen treten [77][78].
- **Neue Produkthaftung:** Die modernisierte Produkthaftungsrichtlinie (EU) 2024/2853 definiert Software und KI ausdrücklich als Produkte. Für Produkte, die nach dem 9. Dezember 2026 in Verkehr gebracht

werden, haften Hersteller **verschuldensunabhängig** für Schäden durch fehlerhafte Software, einschließlich Fehlern aus kontinuierlichem Lernen [79][81].

Bemerkenswert ist, was **weggefallen** ist: Die geplante KI-Haftungsrichtlinie (AI Liability Directive), die Geschädigten Beweiserleichterungen bringen sollte, wurde von der EU-Kommission im Februar 2025 zurückgezogen und im Oktober 2025 formal aus dem Verfahren genommen [79][80][81]. Das entlastet Unternehmen nicht, im Gegenteil: Es bleibt bei den allgemeinen, für Geschäftsführer eher strengeren nationalen Haftungsregeln [79].

5.2 Warum Dokumentation über Haftung entscheidet

Der entscheidende Schutzmechanismus für die Geschäftsführung ist die **Business Judgement Rule** (§ 93 Abs. 1 S. 2 AktG, für die GmbH analog): Wer unternehmerisch entscheidet, haftet nicht, **sofern** er auf Grundlage **angemessener Information** und zum Wohl der Gesellschaft handelt. Ohne dokumentierte Risikoanalyse, ohne KI-Governance, ohne nachweisbare Schulung fehlt genau diese angemessene Informationsbasis, und der Haftungsschutz entfällt [75][78].

Hinzu kommt die **Beweislast**: Nach § 93 Abs. 2 S. 2 AktG (bzw. der Beweislastverteilung des § 43 GmbHG) muss der Geschäftsführer im Streitfall darlegen und beweisen, dass er sorgfältig gehandelt hat. Fehlt die Dokumentation des KI-Einsatzes und der Aufklärung, wirkt das faktisch wie eine **Beweislastumkehr zulasten der Leitungsebene** [77][78]. Fachstellen formulieren es klar: "Wer keine ausreichende KI-Governance vorhält, haftet persönlich." Verlangt werden ein KI-Verzeichnis, Risikoanalysen, interne Richtlinien und Mitarbeiterschulungen [77][78].

Damit schließt sich der Bogen zur These dieses Papiers: **Nicht die Nutzung von KI ist das primäre Haftungsproblem, sondern das undokumentierte Nichtstun.** Ein Geschäftsführer, der Schatten-KI ignoriert und weder aufklärt noch schult noch dokumentiert, kann sich im Schadensfall nicht entlasten. Ein Geschäftsführer, der eine Richtlinie erlässt, schult und beides belegt, verlagert das Risiko dorthin, wo es hingehört, und schützt sich selbst.

5.3 Die D&O-Versicherung schließt die Lücke nur teilweise

Viele Geschäftsführer verlassen sich auf ihre D&O-Versicherung (Managerhaftpflicht). Das ist riskant:

- Standardpolicen decken "KI-Fehlentscheidungen" häufig **noch gar nicht** ausdrücklich ab; reine KI-Policen sind selten, meist gibt es nur Erweiterungen bestehender Deckungen [75].
- **Wissentliche Pflichtverletzungen** sind vom Versicherungsschutz ausgeschlossen. Wer die Schatten-KI-Problematik kennt (spätestens nach Lektüre dieses Papiers) und nichts tut, riskiert, sich außerhalb der Deckung zu bewegen [75].
- Versicherer nutzen AI-Act-Compliance zunehmend als **Underwriting-Kriterium**: Wer Risikobewertungen dokumentiert, menschliche Aufsicht implementiert und KI klassifiziert hat, erhält bessere Konditionen; andere zahlen höhere Prämien oder bekommen bestimmte Risiken nicht mehr gedeckt [75].

Nicht ohne Grund führen KI-Risiken inzwischen die Sorgenlisten der Wirtschaft an: Im **Allianz Risk Barometer 2026** springen KI-Risiken auf Platz zwei der globalen Unternehmensrisiken, eng verzahnt mit Cyber auf Platz eins [73][74].

---

6. Was passiert, wenn es schiefgeht: belastbare Fälle und Kosten

Die Risiken sind nicht theoretisch. Vier dokumentierte Referenzpunkte:

- **Air Canada (2024):** Ein Chatbot der Fluggesellschaft erteilte einem Kunden eine falsche Auskunft zu Trauertarifen. Das Civil Resolution Tribunal of British Columbia entschied (Moffatt v. Air Canada, 2024 BCCRT 149, Urteil vom 14. Februar 2024), das Unternehmen hafte für die Aussage des Chatbots wie für jede andere Angabe auf seiner Website, und sprach 650,88 CAD Schadenersatz zuzüglich Zinsen und Verfahrenskosten zu (insgesamt 812,02 CAD). Die "Halluzination" sei kein entschuldigender Bug, sondern ein Haftungsgrund [92][93][94]. Kernsatz für jede Chefetage: **Wer KI nach außen einsetzt, haftet für ihre Fehler.**
- **Mata v. Avianca (USA, 2023):** Anwälte reichten einen von ChatGPT erfundenen, mit Falschzitaten gespickten Schriftsatz ein (S.D.N.Y., Az. 22-cv-1461, Richter P. Kevin Castel) und wurden im Juni 2023 mit 5.000 Dollar nach Rule 11 der Federal Rules of Civil Procedure sanktioniert. Der Fall ist weltweit zum Sinnbild der KI-Halluzination geworden [95][96]. Kernsatz: **Ungeprüfte KI-Ergebnisse sind ein Reputations- und Haftungsrisiko.**
- **Samsung (2023):** Drei Datenabflüsse in 20 Tagen durch gut gemeinte Produktivität, Reaktion: verpflichtende Schulungen [88][103]. Kernsatz: **Der Schaden entsteht durch normale Mitarbeiter, nicht durch Angreifer.**
- **IBM Cost of a Data Breach 2025:** Bei jedem fünften Datenleck war Schatten-KI im Spiel; solche Vorfälle verteuern sich um durchschnittlich **670.000 Dollar** und dauern eine Woche länger. 97 Prozent der von KI-Vorfällen betroffenen Organisationen hatten keine KI-Zugriffskontrollen, 63 Prozent keine KI-Governance [46][47]. Kernsatz: **Ungesteuerte KI ist messbar teurer.**

Der Ausblick verstärkt das Bild: **Gartner** erwartet, dass bis 2027 über 40 Prozent der KI-bezogenen Datenlecks auf unsachgemäße, grenzüberschreitende GenAI-Nutzung zurückgehen und dass bis 2030 über 40 Prozent der Organisationen weltweit Sicherheits- oder Compliance-Vorfälle durch nicht autorisierte KI erleiden werden [67][68]. Der **Stanford AI Index** zählte 2025 bereits 362 dokumentierte KI-Vorfälle gegenüber 233 im Vorjahr, ein deutlicher Anstieg, während die Governance dem Tempo hinterherhinkt [69][70].

---

7. Warum darauf nicht richtig hingewiesen wird

Wenn das Risiko so klar ist, warum handelt der Mittelstand nicht? Vier Gründe erklären die Aufklärungslücke, und begründen den Anlass für dieses Papier:

1. **Die Debatte ist auf Chancen gepolt.** Öffentliche Kommunikation, Anbieter und Verbände betonen Produktivität und Wettbewerbsfähigkeit. Die Haftungsseite wird als "Innovationsbremse" empfunden und leise gehalten.
2. **Die 35-Millionen-Zahl lähmt statt zu warnen.** Sie klingt nach Konzernthema. Dass der reale Hebel im Mittelstand über DSGVO, Geheimnisschutz und persönliche Organhaftung läuft, geht in der Schlagzeile unter [I][II].
3. **Das "Nichts-passiert"-Gefühl trügt.** Weil KI offiziell kaum eingeführt ist, unterschätzt die Geschäftsführung die reale, verdeckte Nutzung, und damit die eigene Aufsichtspflicht [38][40].

4. **KI-Kompetenz fehlt an der Spitze.** Nur 39 Prozent der KI-Nutzer weltweit haben je eine Schulung erhalten [56]. Die niedrige KI-Kompetenz trifft die Leitungsebene genauso wie die Belegschaft und verhindert, dass die Rechtslage überhaupt eingeordnet wird [50].

Das Ergebnis ist eine **Governance-Lücke**: hohe Adoption, niedrige Steuerung. Genau diese Lücke ist der wunde Punkt, an dem Aufsicht, Zivilkläger und im Ernstfall der eigene Insolvenzverwalter ansetzen.

---

8. Was Geschäftsführer jetzt konkret tun müssen: der 10-Punkte-Plan

Die gute Nachricht: Der Weg aus der Haftung ist klar, verhältnismäßig und für den Mittelstand machbar. Jeder Schritt erzeugt zugleich das **Dokument**, das im Ernstfall entlastet.

1. **KI-Bestandsaufnahme (KI-Inventar).** Erfassen, welche KI-Tools tatsächlich genutzt werden, auch privat und "still". Ein zentrales Register ist der erste Nachweis der Aufsicht [46][45].
2. **Risikoklassifizierung.** Jedes System nach AI Act einordnen (verboten, hochriskant, Transparenzpflicht, minimal), besonders im Personalwesen [83][84].
3. **KI-Richtlinie erlassen.** Klar regeln, welche Tools erlaubt sind und welche Daten (öffentlich, intern, vertraulich, personenbezogen) wo eingegeben werden dürfen, mit Sanktionsklausel. Muster liefern u. a. GDD und AlgorithmWatch [44][45][116]. Ohne Sanktionsklausel bleibt die Richtlinie unverbindlich.
4. **KI-Kompetenz nach Art. 4 aufbauen und dokumentieren.** Schulungen für alle KI-nutzenden Rollen, mit Teilnahmenachweis, Datum und Inhalt. Die Dokumentation ist der Haftungsanker [3][113][117].
5. **Datenschutz nachziehen.** Verarbeitungsverzeichnis (Art. 30) ergänzen, Auftragsverarbeitung und Drittlandtransfer klären, Enterprise-Verträge statt privater Gratiszugänge nutzen [24][99].
6. **Geschäftsgeheimnisse absichern.** Vertrauliche Informationen kategorisieren und technisch wie organisatorisch vor der Eingabe in öffentliche Tools schützen, um den GeschGehG-Schutz zu erhalten [89][91].
7. **Menschliche Aufsicht verankern.** Für Hochrisiko-Anwendungen (besonders Recruiting) sicherstellen, dass ein Mensch entscheidet und Ergebnisse geprüft werden; die Pflicht wird ab 2. Dezember 2027 verbindlich, der Aufbau braucht aber Vorlauf [83][121].
8. **Betriebsrat einbinden.** Bei arbeitgeberseitig bereitgestellten Tools und bei Personalauswahl greift die Mitbestimmung (§ 87 Abs. 1 Nr. 6 BetrVG); eine Betriebsvereinbarung schafft Rechtssicherheit [85][86][33]. (Bei rein privaten, vom Arbeitgeber nicht einsehbaren Accounts besteht nach ArbG Hamburg, Beschluss vom 16. Januar 2024, Az. 24 BVGa 1/24, kein Mitbestimmungsrecht, wohl aber ein faktisches Steuerungsproblem [87].)
9. **Managementsystem und Versicherung prüfen.** ISO/IEC 42001 als zertifizierbares KI-Managementsystem aufsetzen oder in bestehende ISO-27001-Strukturen integrieren [118][119][120]; D&O-Police auf KI-Deckung und Ausschlüsse prüfen [75].
10. **Verantwortlichkeit und Turnus festlegen.** KI-Verantwortliche benennen, Richtlinie und Inventar mindestens jährlich aktualisieren, Vorstands-/Geschäftsführungsbeschlüsse protokollieren. So entsteht die "angemessene Informationsbasis" der Business Judgement Rule [78].

Als Orientierung dienen etablierte Rahmenwerke: die **DSK-Orientierungshilfe** [24], die **BSI-Handreichung zu großen KI-Sprachmodellen** [21][22][23], die **OWASP Top 10 für LLM-Anwendungen** [71] sowie

ISO/IEC 42001 [118]. Für KMU bietet der AI Act zudem echte Erleichterungen (Reallabore, reduzierte Gebühren, niedrigere Bußgeldobergrenze), die aktiv genutzt werden sollten [12][20].

---

9. Fazit

Schatten-KI ist im Mittelstand bereits Realität, nicht Zukunft. Das persönliche Haftungsrisiko der Geschäftsführung ist es ebenfalls: Es beruht auf heute geltenden Regeln, der KI-Kompetenzpflicht (Art. 4, seit Februar 2025), der DSGVO sowie den Legalitäts- und Aufsichtspflichten des deutschen Rechts, die bis in das Privatvermögen reichen. Der Digital Omnibus hat die teure Hochrisiko-Ebene auf den 2. Dezember 2027 verschoben, an dieser Grundhaftung aber nichts geändert. Die zentrale, im Mittelstand kaum verstandene Erkenntnis lautet: **Nicht der Einsatz von KI, sondern die undokumentierte Untätigkeit ist der Haftungstatbestand.** Wer aufklärt, schult, regelt und all das nachweist, verlagert das Risiko und schützt sich selbst. Wer schweigt, haftet.

Der Aufwand ist verhältnismäßig, der Zeitpunkt ist jetzt. Die heute geltenden Pflichten dulden keinen Aufschub, und der Vorlauf bis zur Hochrisiko-Stufe im Dezember 2027 ist für ein Konformitätsverfahren knapp bemessen. Der entscheidende erste Schritt ist in beiden Fällen derselbe: Inventar, Richtlinie, Schulung, Dokumentation. Genau dabei unterstützt Avolang.

Über Avolang

Avolang ist eine auf KI-Compliance und Datenschutz spezialisierte Beratung für kleine und mittlere Unternehmen. Wir übersetzen die Anforderungen aus EU AI Act, DSGVO und Geheimnisschutz in verhältnismäßige, dokumentierte Maßnahmen: KI-Inventar, KI-Richtlinie, Art.-4-Schulungen mit Nachweis, Datenschutz-Nachzug und ein prüffestes Governance-Paket, das im Ernstfall entlastet. Kontakt und Terminvereinbarung über die im Anschreiben genannten Wege.

Methodik und Hinweise

Dieses Whitepaper wertet über 130 reputable Quellen aus, mit Schwerpunkt auf europäischen und mittelstandsbezogenen Belegen: amtliche Rechtstexte und Originalurteile (EUR-Lex, Europäische Kommission, Rat der EU, EDPB, Gerichtsentscheidungen im Volltext), deutsche Behörden (Bundesnetzagentur, BSI, Datenschutzkonferenz, Bundestag/Bundesregierung), Forschungs- und Wirtschaftsinstitute (KfW, IW Köln, ZEW, Bitkom, DIHK, Stanford HAI), Beratungs- und Sicherheitsstudien (McKinsey, KPMG, PwC, Deloitte, IBM, Cisco, Gartner, Netskope, Cyberhaven, Microsoft/LinkedIn), einschlägige Rechtsprechung, das EU-Gesetzgebungsupdate zum Digital Omnibus sowie Fachkanzleien und Fachpresse. Alle statistischen und rechtlichen Aussagen sind mit Quellennummern belegt. In einer zweiten Verifikationsrunde am 20. Juli 2026 wurden die tragenden Belege gegen real geöffnete Primärquellen geprüft (Protokoll und Zitate siehe `BELEG-REGISTER.md`); drei dabei gefundene Korrekturbedarfe (OpenAI-Bußgelddatum, Zuschreibung einer Bitkom-Kennzahl, eine nicht verifizierbare McKinsey-Aussage) wurden behoben, Einzelheiten siehe `FAKTENCHECK.md`.

Kein Rechtsrat: Dieses Papier dient der Information und ersetzt keine Rechts- oder Steuerberatung im Einzelfall. Rechtsstand Juli 2026; die Rechtslage entwickelt sich dynamisch, insbesondere durch den zum Redaktionsschluss noch nicht im Amtsblatt veröffentlichten Digital Omnibus (siehe Abschnitt 3.5). Populäre

Sekundärquellen zur "persönlichen Haftung ab August" [I][II] werden bewusst durch die genaue rechtliche Herleitung in Abschnitt 5 eingeordnet.

Quellenverzeichnis

Amtliche EU-Quellen und Rechtstexte

1. Verordnung (EU) 2024/1689 (KI-Verordnung / AI Act), EUR-Lex. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
2. Amtsblatt der EU, L 2024/1689 (HTML-Fassung), EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL_202401689
3. Art. 4 KI-VO (KI-Kompetenz), artificialintelligenceact.eu. https://artificialintelligenceact.eu/article/4/
4. Art. 5 KI-VO (Verbotene Praktiken). https://artificialintelligenceact.eu/article/5/
5. Art. 99 KI-VO (Sanktionen). https://artificialintelligenceact.eu/article/99/
6. AI Act Service Desk der Europäischen Kommission, Art. 5. https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-5
7. AI Act Service Desk, Art. 99 (Penalties). https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-99
8. Europäische Kommission, Repository of AI literacy practices. https://digital-strategy.ec.europa.eu/en/policies/repository-ai-literacy-practices
9. Europäische Kommission, Living repository to foster learning and exchange on AI literacy. https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy
10. Europäische Kommission, AI Literacy Questions & Answers. https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
11. Europäische Kommission, AI talent, skills and literacy. https://digital-strategy.ec.europa.eu/en/policies/ai-talent-skills-and-literacy
12. artificialintelligenceact.eu, Leitfaden für kleine Unternehmen zum AI Act. https://artificialintelligenceact.eu/small-businesses-guide-to-the-ai-act/
13. EDPB, Report of the work undertaken by the ChatGPT Taskforce (23.05.2024), PDF. https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf
14. EDPB, ChatGPT Taskforce (Übersichtsseite). https://www.edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-chatgpt-taskforce_en

Deutsche Behörden und Gesetzgebung

1. Bundesregierung, Umsetzung der KI-Verordnung. https://www.bundesregierung.de/breg-de/aktuelles/umsetzung-ki-verordnung-2406638
2. Deutscher Bundestag, Ja zur Durchführung der KI-Verordnung (KW24/2026). https://www.bundestag.de/dokumente/textarchiv/2026/kw24-de-ki-1183820
3. Deutscher Bundestag, Zuspruch für Bundesnetzagentur als KI-Marktüberwachungsbehörde (KW13). https://www.bundestag.de/dokumente/textarchiv/2026/kw13-pa-digitales-1155576
4. BMDS, Gesetz zur Durchführung der KI-Verordnung. https://bmds.bund.de/service/gesetzgebungsverfahren/gesetz-zur-durchfuehrung-der-ki-verordnung

5. Bundesnetzagentur, Marktüberwachung KI. https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/14_Marktueberwachung/start.html
6. Bundesnetzagentur, KI-Reallabore / Innovationen. https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/5_Innovationen/start.html
7. BSI, Aktualisierte Fassung: Chancen und Risiken großer KI-Sprachmodelle (Presse). https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/LLM-Chancen-Risiken_240502.html
8. BSI, Generative KI-Modelle: Chancen und Risiken für Industrie und Behörden (Download). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Generative_KI-Modelle.html
9. BSI, Themenseite Künstliche Intelligenz für Unternehmen und Organisationen. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html
10. Datenschutzkonferenz (DSK), Orientierungshilfe KI und Datenschutz (06.05.2024), PDF. https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf
11. LDI NRW, DSK-Orientierungshilfe KI für Unternehmen und Behörden. https://www.ldi.nrw.de/dsk-orientierungshilfe-ki-fuer-unternehmen-und-behoerden
12. Sächsischer Datenschutzbeauftragter, DSK-Orientierungshilfe zu RAG-Systemen. https://www.datenschutz.sachsen.de/dsk-veroeffentlicht-orientierungshilfe-zu-ki-systemen-mit-retrieval-augmented-generation-rag-7768.html
13. Berliner Datenschutzbeauftragte, DSK-Orientierungshilfe RAG. https://www.datenschutz-berlin.de/pressemitteilung/dsk-veroeffentlicht-orientierungshilfe-zu-ki-systemen-mit-retrieval-augmented-generation-rag/

Forschung, Kammern und Verbände (Mittelstand/Deutschland)

1. KfW Research, KI im Mittelstand (Fokus Volkswirtschaft Nr. 533, Feb. 2026), PDF. https://www.kfw.de/PDF/Download-Center/Konzernthemen/Research/PDF-Dokumente-Fokus-Volkswirtschaft/Fokus-2026/Fokus-Nr.-533-Februar-2026-KI-Mittelstand.pdf
2. KfW, Einsatz von Künstlicher Intelligenz im Mittelstand (News). https://www.kfw.de/%C3%9Cber-die-KfW/Newsroom/Aktuelles/News-Details_880960.html
3. KfW, KI kommt im Mittelstand immer häufiger zum Einsatz (Pressemitteilung). https://www.kfw.de/%C3%9Cber-die-KfW/Newsroom/Aktuelles/Pressemitteilungen-Details_880896.html
4. KfW-Digitalisierungsbericht Mittelstand 2025 (News). https://www.kfw.de/%C3%9Cber-die-KfW/Newsroom/Aktuelles/News-Details_891136.html
5. Bitkom, Künstliche Intelligenz in Deutschland, Studienbericht (PDF). https://www.bitkom.org/sites/main/files/2026-02/bitkom-studienbericht-ki.pdf
6. Bitkom, Leitfaden Künstliche Intelligenz und Mitbestimmung (PDF). https://www.bitkom.org/sites/main/files/2026-02/bitkom-leitfaden-kuenstliche-intelligenz-und-mitbestimmung.pdf
7. IW Köln, Wie wird KI die Produktivität in Deutschland verändern? https://www.iwkoeln.de/studien/vera-demary-michael-groemling-christian-kestermann-marc-scheufen-stefanie-seele-oliver-stettes-marco-trenz-wie-wird-ki-die-produktivitaet-in-deutschland-veraendern.html
8. IW Köln, Gutachten Produktivität-KI (2025), PDF. https://www.iwkoeln.de/fileadmin/user_upload/Studien/Gutachten/PDF/2025/Gutachten_2025-Produktivit%C3%A4t-KI-barrierefrei.pdf

9. IW Köln, IW-Report KI als Wettbewerbsfaktor (2025), PDF. https://www.iwkoeln.de/fileadmin/user_upload/Studien/Report/PDF/2025/IW-Report_2025-KI-als-Wettbewerbsfaktor.pdf
10. ZEW, Innovativer Mittelstand 2025. https://www.zew.de/en/publications/innovativer-mittelstand-2025-herausforderungen-trends-und-handlungsempfehlungen-fuer-wirtschaft-und-politik
11. DIHK, Digitalisierung 2026: Unternehmen halten Kurs. https://www.dihk.de/de/newsroom/digitalisierung-2026-unternehmen-halten-kurs-163290
12. bidt, Zunahme beim Einsatz Künstlicher Intelligenz in deutschen Unternehmen. https://www.bidt.digital/themenmonitor/zunahme-beim-einsatz-kuenstlicher-intelligenz-in-deutschen-unternehmen/
13. Creditreform, Mittelstand entdeckt KI. https://www.creditreform.de/aktuelles-wissen/pressemeldungen-fachbeitraege/news-details/show/mittelstand-entdeckt-ki
14. BVMW, Der AI Act: die KI-Verordnung der EU. https://www.bvmw.de/de/internet-und-digitalisierung/news/der-ai-act-die-kuenstliche-intelligenz-ki-verordnung-der-eu
15. DFKI, Von Schatten-IT zu Schatten-KI durch ChatGPT. https://www.dfki.de/web/forschung/projekte-publikationen/publikation/16817
16. Springer, Wirtschaftsinformatik & Management: Von Schatten-IT zu Schatten-KI durch ChatGPT. https://link.springer.com/article/10.1365/s35764-026-00588-3
17. GDD, Musterrichtlinie zum Einsatz Künstlicher Intelligenz. https://www.gdd.de/publikationen/gdd-musterrichtlinie-einsatz-von-kuenstliche-intelligenz/
18. AlgorithmWatch, Vorschlag für eine Generative-KI-Richtlinie. https://algorithmwatch.org/de/generative-ki-richtlinie/

Internationale Studien (Shadow AI, Governance, Sicherheit)

1. IBM, Cost of a Data Breach Report 2025. https://www.ibm.com/reports/data-breach
2. IBM Newsroom, 13% of organizations reported breaches of AI models/applications, 97% lacked AI access controls. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls
3. (entfernt) McKinsey, The State of AI 2025: Aussage am 20.07.2026 gestrichen, da die Quelle in der Recherche-Umgebung trotz mehrfachem Versuch (Direkt-Download und Browser-Abruf) nicht real öffnbar war; siehe BELEG-REGISTER.md, C048.
4. (entfernt) McKinsey, The State of AI (Übersicht): siehe Eintrag 48.
5. KPMG, Global study reveals trust of AI remains a critical challenge (Pressemitteilung). https://kpmg.com/xx/en/media/press-releases/2025/04/trust-of-ai-remains-a-critical-challenge.html
6. KPMG/University of Melbourne, Trust, attitudes and use of AI: A Global Study 2025 (Report, PDF). https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2025/05/trust-attitudes-and-use-of-ai-global-report.pdf.coredownload.inline.pdf
7. University of Melbourne / MBS, Trust and AI. https://mbs.edu/faculty-and-research/trust-and-ai
8. PwC, 2025 Responsible AI Survey: From policy to practice. https://www.pwc.com/us/en/tech-effect/ai-analytics/responsible-ai-survey.html
9. PwC Deutschland, Responsible AI. https://www.pwc.de/en/risk-regulatory/responsible-ai.html

10. Deloitte, State of AI in the Enterprise (2026). https://www.deloitte.com/ce/en/issues/generative-ai/state-of-ai-in-enterprise.html
11. Microsoft/LinkedIn, Work Trend Index 2024: AI at Work Is Here. Now Comes the Hard Part. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part
12. Microsoft/LinkedIn, 2024 Work Trend Index Annual Report, Executive Summary (PDF). https://assets-c4akfrf5b4d3f4b7.z01.azurefd.net/assets/2024/05/2024_Work_Trend_Index_Annual_Report_Executive_Summary_663b2135860a9.pdf
13. Microsoft News, Microsoft and LinkedIn release the 2024 Work Trend Index. https://news.microsoft.com/source/2024/05/08/microsoft-and-linkedin-release-the-2024-work-trend-index-on-the-state-of-ai-at-work/
14. Cisco, 2025 Data Privacy Benchmark Study (PDF). https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2025.pdf
15. Cisco Newsroom, 2025 Data Privacy Benchmark Study. https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m04/cisco-2025-data-privacy-benchmark-study-privacy-landscape-grows-increasingly-complex-in-the-age-of-ai.html
16. Cyberhaven, 11% of data employees paste into ChatGPT is confidential. https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt
17. Cyberhaven, Majority of corporate AI tools present critical data security risks. https://www.cyberhaven.com/press-releases/cyberhaven-report-majority-of-corporate-ai-tools-present-critical-data-security-risks
18. Netskope, Cloud and Threat Report: Shadow AI and Agentic AI 2025. https://www.netskope.com/resources/cloud-and-threat-reports/cloud-and-threat-report-shadow-ai-and-agentic-ai-2025
19. Netskope, Cloud and Threat Report: Generative AI 2025. https://www.netskope.com/resources/cloud-and-threat-reports/cloud-and-threat-report-generative-ai-2025
20. UpGuard, The State of Shadow AI. https://www.upguard.com/resources/the-state-of-shadow-ai
21. Cybersecurity Dive, Shadow AI is widespread and executives use it the most. https://www.cybersecuritydive.com/news/shadow-ai-employee-trust-upguard/805280/
22. Gartner, Predicts 40% of AI Data Breaches Will Arise from Cross-Border GenAI Misuse by 2027. https://www.gartner.com/en/newsroom/press-releases/2025-02-17-gartner-predicts-forty-percent-of-ai-data-breaches-will-arise-from-cross-border-genai-misuse-by-2027
23. Infosecurity Magazine, Gartner: 40% of Firms to Be Hit By Shadow AI Security Incidents. https://www.infosecurity-magazine.com/news/gartner-40-firms-hit-shadow-ai/
24. Stanford HAI, 2025 AI Index Report, Responsible AI. https://hai.stanford.edu/ai-index/2025-ai-index-report/responsible-ai
25. Stanford HAI, 2026 AI Index Report. https://hai.stanford.edu/ai-index/2026-ai-index-report
26. OWASP Top 10 for LLM Applications 2025 (Überblick, mend.io). https://www.mend.io/blog/2025-owasp-top-10-for-llm-applications-a-quick-guide/
27. Allianz Commercial, Allianz Risk Barometer 2025. https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2025/de.html

28. Allianz, Risk Barometer 2026: Cyber und KI als größte Unternehmensrisiken. https://www.allianz.com/de/mediencenter/news/artikel/260203-allianz-risk-barometer-2026-cyber-ki-groesste-unternehmensrisiken.html
29. Allianz Commercial, Allianz Risk Barometer 2026. https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2026/de.html

Haftung, Recht, Kanzleien

1. VOV, KI und Managerhaftung: Haftungsrisiken und D&O-Schutz. https://vov.eu/wissen/fachblog/ki-und-managerhaftung/
2. Taylor Wessing, Die neuen Verbote der KI-Verordnung und ihre Auswirkungen auf die Versicherungswirtschaft. https://www.taylorwessing.com/de/insights-and-events/insights/2025/04/die-neuen-verbote-der-ki-verordnung-und-ihre-auswirkungen-auf-die-versicherungswirtschaft
3. GmbHchef, Europäische KI-Verordnung: Haftungsrisiken und Handlungsoptionen für Geschäftsführer. https://www.gmbhchef.de/europaeische-ki-verordnung-ai-act-kuenstliche-intelligenz-haftungsrisiken-und-handlungsoptionen-fuer-geschaeftsfuehrer/
4. PMPG, Künstliche Intelligenz: Haftungsrisiken und Handlungsoptionen für Geschäftsführer. https://www.pmpg.de/wissenswertes/kuenstliche-intelligenz-haftungsrisiken-und-handlungsoptionen-fuer-geschaeftsfuehrer/
5. IAPP, European Commission withdraws AI Liability Directive from consideration. https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration
6. Europäisches Parlament, Legislative Train: AI Liability Directive. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-ai-liability-directive
7. datenschutzticker, EU-Kommission: Vorerst keine KI-Haftungsrichtlinie. https://www.datenschutzticker.de/2025/03/eu-kommission-vorerst-keine-ki-haftungsrichtlinie/
8. White & Case, Long-awaited EU AI Act becomes law after publication in the EU's Official Journal. https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-eus-official-journal
9. DLA Piper, AI Act: Leitlinien-Entwürfe zur Klassifizierung von Hochrisiko-KI-Systemen. https://www.dlapiper.com/de-de/insights/blogs/employment-blog-germany/2026/ai-act--leitlinien-entwurfe-zur-klassifizierung-von-hochrisiko-ki-systemen
10. KPMG Law, KI und Arbeitsrecht: Das bedeutet der AI Act für den HR-Bereich. https://kpmg-law.de/ki-und-arbeitsrecht-das-bedeutet-der-ai-act-fuer-den-hr-bereich/
11. Bird & Bird, Erstes Urteil zu Rechten des Betriebsrats bei Einsatz von KI. https://www.twobirds.com/de/insights/2024/germany/erstes-urteil-zu-rechten-des-betriebsrats-bei-einsatz-von-kuenstlicher-intelligenz
12. Haufe, Mitbestimmung des Betriebsrats bei ChatGPT im Betrieb. https://www.haufe.de/personal/arbeitsrecht/mitbestimmung-des-betriebsrats-bei-chatgpt-im-betrieb_76_618400.html
13. Kliemt.blog, Kein Mitbestimmungsrecht des Betriebsrats bei Nutzung privater ChatGPT-Accounts. https://kliemt.blog/2024/03/13/kein-mitbestimmungsrecht-des-betriebsrats-bei-der-nutzung-privater-chatgpt-accounts/

14. Härting Rechtsanwälte, Samsung's ChatGPT Leak: AI Risks in the Workplace. https://haerting.de/en/insights/samsungs-chatgpt-leak-ai-risks-in-the-workplace/
15. RDP Rechtsanwälte, Künstliche Intelligenz und Geschäftsgeheimnisse. https://www.rdp-law.de/blog/blog-details/kuenstliche-intelligenz-und-geschaeftsgeheimnisse.html
16. Luther Rechtsanwaltsgesellschaft, Schutz von Daten als Geschäftsgeheimnis (GeschGehG). https://www.luther-lawfirm.com/en/newsroom/blog/detail
17. Baker Tilly, ChatGPT: So schützen Sie Ihre Geschäftsgeheimnisse. https://www.bakertilly.de/en/post/chatgpt-how-to-protect-your-trade-secrets
18. beck-aktuell, Falschauskunft vom Chatbot: Airline muss zahlen (Air Canada). https://www.beck-aktuell.de/heute-im-recht/rechtsprechung/kanada-falschauskunft-chatbot-airline-kuenstliche-intelligenz-2024-03-05
19. Haufe, Fluglinie haftet für unrichtige Auskunft eines Chatbots. https://www.haufe.de/recht/kanzleimanagement/fluglinie-haftet-fuer-unrichtige-auskunft-eines-chatbots_222_619118.html
20. Hogan Lovells, KI-Haftung: Verantwortlichkeit für Fehlinformationen eines Chatbots. https://www.hoganlovells.com/de/publications/neuigkeiten-im-bereich-der-ki-haftung-verantwortlichkeit-fur-fehlinformationen-eines-chatbots
21. Wikipedia, Mata v. Avianca, Inc. https://en.wikipedia.org/wiki/Mata_v._Avianca,_Inc.
22. Seyfarth Shaw, Update on the ChatGPT Case: Counsel Who Submitted Fake Cases Are Sanctioned. https://www.seyfarth.com/news-insights/update-on-the-chatgpt-case-counsel-who-submitted-fake-cases-are-sanctioned.html
23. Lewis Silkin, OpenAI faces EUR 15 million fine as the Italian Garante strikes again. https://www.lewissilkin.com/insights/2025/01/14/openai-faces-15-million-fine-as-the-italian-garante-strikes-again-102jtqc
24. Euronews, Italy's privacy watchdog fines OpenAI EUR 15 million after probe into ChatGPT data collection. https://www.euronews.com/next/2024/12/20/italys-privacy-watchdog-fines-openai-15-million-after-probe-into-chatgpt-data-collection
25. IT-Recht Kanzlei, Der Einsatz von ChatGPT verstößt aktuell gegen den Datenschutz. https://www.it-recht-kanzlei.de/chatgpt-datenschutz-verbot-aufsichtsbehoerde-empfehlungen-personenbezogene-daten.html
26. eRecht24, ChatGPT Datenschutz: Ist ChatGPT DSGVO-konform? https://www.e-recht24.de/ki/13409-chatgpt-datenschutz.html

Fachpresse und Medien (Schatten-KI, KI-Kompetenz)

1. heise online, 80 Prozent der Firmen nutzen KI: Microsoft warnt vor gefährlicher Schatten-KI. https://www.heise.de/news/80-Prozent-der-Firmen-nutzen-KI-Microsoft-warnt-vor-gefaehrlicher-Schatten-KI-11172238.html
2. Handelsblatt, ZEW-Studie: Nutzung von KI-Anwendungen in wenigen Firmen verboten. https://www.handelsblatt.com/unternehmen/zew-studie-nutzung-von-ki-anwendungen-in-wenigen-firmen-verboten/100230767.html
3. Golem, Samsung-Ingenieure leaken interne Daten an ChatGPT. https://www.golem.de/news/kuenstliche-intelligenz-samsung-ingenieure-leaken-interne-daten-an-chatgpt-2304-173220.amp.html

4. t3n, Datenleck bei Samsung: Ingenieure schicken vertrauliche Daten an ChatGPT. https://t3n.de/news/samsung-semiconductor-daten-chatgpt-datenleck-1545913/
5. derStandard, Samsung-Mitarbeiter verraten unabsichtlich Firmengeheimnisse an ChatGPT. https://www.derstandard.de/story/2000145238988/samsung-mitarbeiter-verraten-unabsichtlich-firmengeheimnisse-an-chatgpt
6. Computer Weekly, Schatten-KI: Die stille Gefahr. https://www.computerweekly.com/de/meinung/Schatten-KI-Die-stille-Gefahr
7. Security-Insider, Was ist Schatten-KI? https://www.security-insider.de/was-ist-schatten-ki-a-bf0c83154ce19fd2c6ca7ea4f0a8dce0/
8. it-daily, Schatten-KI: Unterschätzte Gefahr im Verborgenen? https://www.it-daily.net/it-management/ki/schatten-ki-unterschaetzte-gefahr-im-verborgenen
9. CIO.com, Roughly half of employees are using unsanctioned AI tools, and enterprise leaders are major culprits. https://www.cio.com/article/4124760/roughly-half-of-employees-are-using-unsanctioned-ai-tools-and-enterprise-leaders-are-major-culprits.html
10. Journal of Accountancy, Lurking in the shadows: The costs of unapproved AI tools. https://www.journalofaccountancy.com/news/2025/nov/lurking-in-the-shadows-the-costs-of-unapproved-ai-tools.html
11. Dark Reading, Employees Are Feeding Sensitive Business Data to ChatGPT. https://www.darkreading.com/cyber-risk/employees-feeding-sensitive-business-data-chatgpt-raising-security-fears
12. HR Dive, Rising 'bring your own AI' trend can spell trouble for employers. https://www.hrdive.com/news/rising-bring-your-own-ai-trend-can-spell-trouble-for-employers/824319/

KI-Kompetenz (Art. 4), Kammern und Weiterbildung

1. IHK Rhein-Neckar, EU AI Act 2025: Vorschriften, Anforderungen und KI-Weiterbildung (Art. 4). https://www.ihk.de/rhein-neckar/ausbildung-weiterbildung/weiterbildung-channel/eu-ai-act-artikel-4-6434562
2. IHK Schleswig-Holstein, AI Act Literacy: KI-Schulungspflicht. https://www.ihk.de/schleswig-holstein/standortpolitik/sicherheit/ai-act-literacy-ki-schulungspflicht-6434794
3. IHK Hannover, AI Act: Unternehmen müssen Mitarbeitende in KI schulen. https://www.ihk.de/hannover/hauptnavigation/digitalisierung/aktuell-digitalisierung/ai-act-unternehmen-muessen-mitarbeitende-in-ki-schulen-6470624
4. Haufe Akademie, KI-Schulungspflicht: Was der EU AI Act fordert. https://www.haufe-akademie.de/digital-suite/blog/ds-ki-schulungspflicht
5. TÜV Rheinland Consulting, KI-Kompetenz nach Art. 4 EU AI Act. https://consulting.tuv.com/aktuelles/ki-im-fokus/ki-kompetenz-art-4-eu-ai-act

Standards und Managementsysteme

1. ISO/IEC 42001:2023, AI management systems. https://www.iso.org/standard/42001
2. TÜV SÜD, ISO/IEC 42001: Zertifizierung für KI-Managementsysteme. https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/iso-42001
3. KPMG, ISO/IEC 42001: KI-Managementstandard für AI-Compliance. https://kpmg.com/ch/de/themen/kuenstliche-intelligenz/iso-iec-42001.html

EU-Gesetzgebungsupdate: Digital Omnibus (AI-Act-Vereinfachung), Stand Juli 2026

1. Gibson Dunn, EU AI Act Omnibus Agreement: Postponed High-Risk Deadlines and Other Key Changes. https://www.gibsondunn.com/eu-ai-act-omnibus-agreement-postponed-high-risk-deadlines-and-other-key-changes/
2. DLA Piper, The Digital AI Omnibus: Deferral of high-risk AI obligations under the AI Act. https://knowledge.dlapiper.com/dlapiperknowledge/globalemploymentlatestdevelopments/2026/The-Digital-AI-Omnibus-Proposed-deferral-of-high-risk-AI-obligations-under-the-AI-Act
3. Travers Smith, EU agrees to delay key AI Act compliance deadlines. https://www.traverssmith.com/knowledge/knowledge-container/eu-agrees-to-delay-key-ai-act-compliance-deadlines/
4. aiactblog.nl, The Digital Omnibus and the postponement of high-risk obligations to December 2027. https://www.aiactblog.nl/en/posts/digital-omnibus-high-risk-postponement-december-2027
5. Hogan Lovells (Engage), EU legislators agree to delay for high-risk AI rules. https://www.hlc.com/en/publications/eu-legislators-agree-to-delay-for-highrisk-ai-rules
6. Cloud Security Alliance, Research Note: EU AI Act Omnibus, high-risk deadline delay to December 2027. https://labs.cloudsecurityalliance.org/research/csa-research-note-eu-ai-act-omnibus-vii-deadline-delay-20260/

Aktualisierung: Aufhebung des OpenAI-Bußgelds durch das Tribunale di Roma (März 2026)

1. Wilson Sonsini, OpenAI Prevails in Landmark Italian AI and GDPR Enforcement Case. https://www.wsgr.com/en/insights/openai-prevails-in-landmark-italian-ai-and-gdpr-enforcement-case.html
2. ANSA, Tribunale Roma annulla multa da 15 milioni di euro del Garante Privacy a OpenAI (20.03.2026). https://www.ansa.it/canale_tecnologia/notizie/tecnologia/2026/03/20/tribunale-roma-annulla-multa-da-15-milioni-di-euro-del-garante-privacy-a-openai_6560fadd-4099-451e-99a0-7fcbc9a285c1.html
3. Tribunale di Roma, Sentenza n. 4153/2026 (R.G. 4785/2025), veröffentlicht 18.03.2026, Volltext-Mirror. https://dei.web.uniroma1.it/sites/default/files/allegati/2026-05/Trib_Roma_OpenAI_Garante_2026.pdf
4. Rat der Europäischen Union (Consilium), Artificial Intelligence: Council gives final green light to simplify and streamline rules (offizielle Pressemitteilung, 29.06.2026). https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/
5. Ropes & Gray, Five Takeaways From the EU Commission's AI Literacy Q&As (Enforcement erst ab Einrichtung der Marktüberwachungsbehörden). https://www.ropesgray.com/en/insights/viewpoints/102kbn5/five-takeaways-from-the-eu-commissions-ai-literacy-qas
6. Freshfields, EU AI Act unpacked #34: The final Digital Omnibus on AI (Unterzeichnung 8.07.2026, Amtsblatt-Veröffentlichung ausstehend). https://www.freshfields.com/en/our-thinking/blogs/technology-quotient/eu-ai-act-unpacked-34-the-final-digital-omnibus-on-ai-key-amendments-to-the-a-102nber

Populäre Sekundärquellen (bewusst als solche gekennzeichnet und in Abschnitt 5 rechtlich eingeordnet)

- [I] Börse-Express, EU AI Act: Persönliche Haftung für Geschäftsführer ab August. https://www.boerse-express.com/news/articles/eu-ai-act-persoenliche-haftung-fuer-geschaeftsfuehrer-ab-august-925505

- [II] S+P Unternehmerforum, Schatten-KI: Haftungsrisiko für Geschäftsführer steigt. https://sp-unternehmerforum.de/schatten-ki/

Erstellt von Avolang. Alle Quellen zuletzt im Juli 2026 geprüft. Für Rückfragen, Datenquellen im Original oder eine mandantenspezifische Risikoeinschätzung stehen wir zur Verfügung.