AI GOVERNANCE & COMPLIANCE

für deutsche Unternehmen

DSGVO · EU AI Act · NIS2

Sebastian Schlaak

Impressum und rechtliche Hinweise

Herausgeberin
Schlaak Consulting GmbH

Sitz der Gesellschaft
Berlin

Anschrift
Elchdamm 74, 13503 Berlin

Handelsregister
Amtsgericht Berlin (Charlottenburg), HRB 270691 B

Vertretungsberechtigte Geschäftsführung
Sebastian Schlaak

Kontakt
s.schlaak@interimcto.de

Ausgabe
Erstauflage 2026

Haftungsausschluss
Dieses Buch dient ausschließlich der allgemeinen Information und stellt keine Rechtsberatung, Steuerberatung oder verbindliche Einzelfallbewertung dar. Trotz sorgfältiger Erstellung kann keine Gewähr für Vollständigkeit, Richtigkeit und Aktualität übernommen werden. Für konkrete Einzelfälle ist qualifizierter rechtlicher Rat einzuholen.

Inhaltsverzeichnis

Vorwort

Willkommen in der neuen Realität der Unternehmens-IT. Wenn Sie dieses Buch in den Händen halten, stehen Sie wahrscheinlich vor einer der größten Herausforderungen, die die Digitalisierung in den letzten Jahren hervorgebracht hat: dem perfekten Sturm aus Künstlicher Intelligenz, Datenschutz und Cybersicherheit.

Die rasante Verbreitung von KI-Tools wie ChatGPT, Claude oder Microsoft Copilot hat die Art und Weise, wie wir arbeiten, revolutioniert. Doch während die Produktivität steigt, wachsen auch die rechtlichen und sicherheitstechnischen Risiken. Die Europäische Union und der deutsche Gesetzgeber haben darauf mit einem dichten Netz an Regulierungen reagiert. Die Datenschutz-Grundverordnung (DSGVO) ist bereits ein alter Bekannter, doch nun gesellen sich der EU AI Act und die NIS2-Richtlinie (umgesetzt im neuen BSI-Gesetz) hinzu.

Dieses Buch richtet sich primär an eine klare Zielperson: Geschäftsführer oder IT-verantwortliche Leitung in deutschen KMU mit etwa 50 bis 500 Mitarbeitern, die KI bereits im Alltag sehen, aber noch kein belastbares Governance-System haben. Sekundär ist es für beratende Berufe geschrieben, die diese Unternehmen begleiten.

Das Ziel ist nicht, juristische Theorie zu vermitteln. Das Ziel ist, innerhalb weniger Wochen eine nachweisbare Mindest-Governance aufzubauen, die in einer Prüfung Bestand hat: Richtlinie, Schulung, Tool-Whitelist, Verantwortlichkeiten, Dokumentation. Es verzichtet auf unnötigen Fachjargon und konzentriert sich auf das, was wirklich zählt: Wie schützen Sie Ihr Unternehmen vor Bußgeldern, Datenabfluss und persönlicher Haftung?

Kapitel 1: Die neue Realität der AI Governance

1.1 Der perfekte Sturm: Warum jetzt handeln?

Die Einführung von Künstlicher Intelligenz in Unternehmen verläuft selten geordnet. Meist beginnt es als "Shadow AI": Ein Mitarbeiter nutzt ChatGPT, um eine E-Mail zu formulieren, ein Entwickler lässt sich von GitHub Copilot Code-Snippets generieren, und das Marketing-Team erstellt Bilder mit Midjourney. Was als harmloser Produktivitäts-Boost beginnt, entwickelt sich schnell zu einem unkontrollierbaren Risiko.

Gleichzeitig zieht der Gesetzgeber die Zügel an. Drei mächtige Regulierungen greifen nun ineinander und zwingen Unternehmen zum Handeln:

Die *DSGVO* schützt personenbezogene Daten und gilt seit Mai 2018 für jedes Unternehmen, das Daten von EU-Bürgern verarbeitet. Der *EU AI Act* reguliert KI-Systeme nach ihrem Risikopotenzial und ist das weltweit erste umfassende KI-Gesetz. Das neue *BSI-Gesetz (BSIG)*, die deutsche Umsetzung der NIS2-Richtlinie, fordert ein hohes Maß an Cybersicherheit für kritische und wichtige Einrichtungen und wurde am 5. Dezember 2025 im Bundesgesetzblatt veröffentlicht und trat am 6. Dezember 2025 in Kraft.

Das Tückische daran: Diese drei Regelwerke schließen sich nicht gegenseitig aus. Sie gelten nebeneinander und betrachten dasselbe KI-System aus unterschiedlichen Blickwinkeln.

1.2 Schnellcheck: Was trifft auf mein Unternehmen zu?

Viele Unternehmen glauben fälschlicherweise, sie seien zu klein oder in der falschen Branche, um von diesen Regulierungen betroffen zu sein. Der folgende

Schnellcheck schafft Klarheit:

Bedingung	Dann gilt…
Ihr Unternehmen verarbeitet Namen, E-Mails, IP-Adressen oder andere Daten von Personen.	*DSGVO* – immer, ohne Ausnahme, ohne Mindestgröße.
Ihr Unternehmen setzt irgendein KI-System ein (intern oder beim Kunden).	*EU AI Act* – für jeden KI-Einsatz in der EU.
Ihr Unternehmen gehört zu einem von 18 Sektoren (z.B. Energie, Transport, Gesundheit, IT, Maschinenbau) und hat mehr als 50 Mitarbeiter oder 10 Mio. € Umsatz.	*NIS2 (BSIG)* – Meldepflichten und strenge IT-Sicherheitsvorgaben.

Die Faustregel lautet: DSGVO und EU AI Act treffen *alle* Unternehmen, die KI einsetzen – ohne Ausnahme, ohne Mindestgröße.

1.3 Die drei Brillen der Compliance

Um die Anforderungen zu verstehen, hilft es, sich drei verschiedene "Brillen" aufzusetzen. Jede dieser Brillen betrachtet denselben KI-Einsatz aus einer anderen Perspektive, und alle drei müssen gleichzeitig getragen werden.

Die Datenschutz-Brille (DSGVO): Hier geht es ausschließlich um den Schutz von Menschen. Sobald ein KI-System mit personenbezogenen Daten gefüttert wird, greifen die strengen Regeln der DSGVO. Es braucht eine Rechtsgrundlage, Auftragsverarbeitungsverträge (AVV) und Transparenz gegenüber den Betroffenen.

Die Risiko-Brille (EU AI Act): Diese Brille betrachtet das KI-System selbst. Was tut die KI? Wie hoch ist das Risiko, dass sie Menschen diskriminiert, manipuliert oder in ihren Grundrechten verletzt? Je höher das Risiko, desto strenger die Auflagen – bis hin zum vollständigen Verbot.

Die Sicherheits-Brille (NIS2/BSIG): Hier steht die Resilienz der IT-Infrastruktur im Fokus. Ein KI-System ist ein potenzielles Einfallstor für Cyberangriffe. NIS2 verlangt ein umfassendes Risikomanagement, die Absicherung der Lieferkette und schnelle Meldewege bei Sicherheitsvorfällen.

1.4 Persönliche Haftung: Wenn Compliance zur Chefsache wird

Ein zentraler roter Faden, der sich durch alle drei Regulierungen zieht, ist die zunehmende persönliche Haftung der Geschäftsleitung. Unwissenheit schützt nicht mehr.

Sowohl bei DSGVO-Verstößen als auch unter dem neuen BSI-Gesetz kann das Unternehmen Bußgelder, die wegen mangelnder Governance verhängt wurden, über § 43 GmbHG oder § 93 AktG vom Geschäftsführer persönlich zurückfordern. Das neue BSIG normiert die Verantwortlichkeit ausdrücklich und macht deutlich, dass die Verantwortung für IT-Sicherheit nicht vollständig an die IT-Abteilung delegierbar ist. Cybersicherheit und AI Governance sind damit endgültig zur Chefsache avanciert.

Executive Summary: Was diese Woche zu tun ist

1. Entscheidung auf GF-Ebene dokumentieren: KI-Governance ist Leitungsaufgabe.
2. Schnellcheck aus 1.2 für das eigene Unternehmen schriftlich durchführen.
3. Für jedes aktive KI-System drei Prüfpfade öffnen: DSGVO, AI Act, NIS2/BSIG.
4. Verantwortliche Person benennen, die die Nachweise zentral sammelt.

Kapitel 2: Die Datenschutz-Brille (DSGVO)

Die Datenschutz-Grundverordnung (DSGVO) ist seit Mai 2018 in Kraft und vollständig anwendbar. Sie gilt für jedes Unternehmen, unabhängig von Größe oder Sektor, sobald Daten von EU-Bürgern verarbeitet werden.

2.1 Grundlagen der DSGVO im KI-Kontext

Wenn Mitarbeiter KI-Tools nutzen, fließen unweigerlich Daten ab. Ein Support-Ticket, das in Claude eingefügt wird, um eine Antwort zu formulieren, enthält oft Kundennamen und Vertragsnummern. Eine Meeting-Transkription über einen externen Dienst erfasst Stimmen und Aussagen der Teilnehmer. All dies sind personenbezogene Daten im Sinne der DSGVO.

Die DSGVO verlangt für jede Verarbeitung eine Rechtsgrundlage (z.B. Einwilligung, Vertragserfüllung oder berechtigtes Interesse). Bei der unkontrollierten Nutzung von privaten KI-Accounts (Shadow AI) fehlt diese Grundlage völlig – und damit ist jede Verarbeitung rechtswidrig.

2.2 Was bedeutet das konkret beim KI-Einsatz?

Um KI DSGVO-konform einzusetzen, müssen folgende Grundregeln beachtet werden:

Auftragsverarbeitungsvertrag (AVV): Jeder KI-Anbieter, der Personendaten verarbeitet, wird zum Auftragsverarbeiter nach Art. 28 DSGVO. Ein AVV ist zwingend erforderlich. Private Accounts (z.B. ChatGPT Plus) bieten keinen AVV und sind daher für Unternehmensdaten tabu. Wichtig: Der AVV für das Consumer-Produkt gilt *nicht* für die API-Nutzung desselben Anbieters. Wer die OpenAI-API nutzt, um eigene Systeme zu bauen, braucht einen separaten API-

AVV.

Hosting und Datenstandort: Es muss geprüft werden, wo die Daten verarbeitet werden. Bei US-Anbietern ist ein angemessenes Datenschutzniveau (z.B. über das EU-US Data Privacy Framework) nachzuweisen. Der US CLOUD Act erlaubt US-Behörden, von US-Unternehmen Herausgabe von Daten zu verlangen – auch wenn diese auf EU-Servern liegen. Dieses Risiko muss im Rahmen einer Datenschutz-Folgenabschätzung (DSFA) ernsthaft bewertet werden. Für hochsensible Branchen (Anwaltskanzleien, Medizin, Behörden) ist eine europäische Alternative oft zwingend erforderlich.

Informationspflicht: Betroffene (Kunden, Mitarbeiter) müssen darüber informiert werden, wenn ihre Daten durch KI-Systeme verarbeitet werden. Wenn ein Unternehmen seinen Kunden ein SaaS-Produkt liefert, das ein KI-Feature enthält, ohne die Datenschutzerklärung und AGB zu aktualisieren, drohen Abmahnungen und Bußgelder. Dasselbe gilt, wenn das eigene CRM-System (z.B. HubSpot mit Breeze AI) KI-gestützt mit Kunden kommuniziert – auch dann muss die Datenschutzerklärung entsprechend aktualisiert werden.

Zweckbindung, Training-Opt-out und Zero Data Retention: Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Das Training von KI-Modellen mit Kundendaten durch externe Anbieter muss vertraglich ausgeschlossen werden (Training-Opt-out). Davon zu unterscheiden ist "Zero Data Retention" (ZDR): ZDR bedeutet, dass Eingaben nach der Verarbeitung gar nicht erst gespeichert werden. Ein Anbieter kann ZDR anbieten, aber trotzdem Modell-Fine-Tuning auf separaten Systemen betreiben. Beides – Opt-out vom Training und Speicherdauer – muss explizit im Vertrag geregelt sein.

2.3 Automatisierte Entscheidungen und menschliche Aufsicht

Ein besonders kritischer Punkt ist Artikel 22 der DSGVO. Dieser verbietet grundsätzlich Entscheidungen, die ausschließlich auf einer automatisierten

Verarbeitung beruhen und rechtliche Wirkung entfalten oder die betroffene Person in ähnlicher Weise erheblich beeinträchtigen. Klassische Beispiele sind die automatische Kreditablehnung oder die KI-gesteuerte Bewerbervorauswahl. Ein oft übersehener Praxisfall: KI-gestützte Performance-Zusammenfassungen in HR-Tools wie Personio, die Beförderungs- oder Kündigungsentscheidungen beeinflussen.

> ⚠ Wenn Sie KI-Systeme für Entscheidungen einsetzen, die Menschen erheblich betreffen, müssen Sie zwingend einen "Human-in-the-Loop" (menschliche Aufsicht) einbauen. Der Betroffene hat das Recht auf menschliches Eingreifen, auf Erklärung der Entscheidung und auf Widerspruch. Fehlt dieses Verfahren, drohen Bußgelder bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes (Art. 83 Abs. 5 DSGVO) sowie direkte Schadensersatzklagen.

Ausnahmen vom Verbot des Art. 22 DSGVO gibt es nur in drei Fällen: Vertragserfüllung, ausdrückliche Einwilligung oder gesetzliche Ermächtigung. Selbst dann muss das Recht auf menschliche Überprüfung gewährleistet sein.

2.4 Konsequenzen für Manager und Geschäftsführer

Die Durchsetzung der DSGVO ist längst Realität. EU-weit wurden seit 2018 Bußgelder in Höhe von fast 6 Milliarden Euro verhängt – der Großteil davon entfällt allerdings auf eine Handvoll Tech-Konzerne (allein Meta: 1,2 Mrd. € in einem Fall). Für KMU sieht die Realität anders aus, aber nicht harmloser.

Sanktion	Höhe / Grundlage	Durchsetzung
Bußgeld gegen Unternehmen (Stufe 1)	Bis 10 Mio. € oder 2 % des weltweiten Jahresumsatzes (Art. 83 Abs. 4 DSGVO, z.B. für Verstöße gegen Art. 22 oder technische Maßnahmen).	Aktiv durchgesetzt. Fehlende Richtlinien gelten als eigenständiger Verstoß.

Sanktion	Höhe / Grundlage	Durchsetzung
Bußgeld gegen Unternehmen (Stufe 2)	Bis 20 Mio. € oder 4 % des weltweiten Jahresumsatzes (Art. 83 Abs. 5 DSGVO, z.B. für Verstöße gegen Grundsätze oder Rechtsgrundlagen).	Aktiv durchgesetzt bei schweren Verstößen.
Persönlicher Regress	§ 43 GmbHG / § 93 AktG. Unternehmen kann Bußgeld vom GF zurückfordern.	Zunehmend. Gerichte bestätigen: GF haftet auch ohne eigene Kenntnis bei Organisationsverschulden.
Schadensersatz	Direkte Klagen von Betroffenen (Art. 82 DSGVO).	Zivilklagen nehmen zu. Voraussetzung ist jedoch ein tatsächlich eingetretener (immaterieller) Schaden (EuGH C-300/21).

Bußgelder in Deutschland: Was KMU wirklich trifft

Jahr	Bußgelder in DE	Gesamtsumme	Typische Höhe für KMU
2019	187	~14 Mio. €	100–10.000 €
2023	357	4,9 Mio. €	100–10.000 €
2024	266	nicht gemeldet	100–10.000 € (höchstes: 220.000 €)
2025	249	46,9 Mio. €	100–10.000 € (verzerrt durch Vodafone-45-Mio.-Fall)

Quellen: DSGVO-Portal / DLA Piper GDPR Survey / Landesbeauftragte für Datenschutz

Die statistische Wahrscheinlichkeit, als einzelnes KMU in Deutschland ein DSGVO-Bußgeld zu kassieren, liegt bei etwa 0,007 % pro Jahr (ca. 250–350 Bescheide bei 3,5 Millionen Unternehmen). Die typische Höhe für KMU: 100–10.000 €. Wer nur auf Bußgelder schaut, könnte zu dem Schluss kommen, das Risiko sei überschaubar. Das wäre ein Fehler.

Die fünf Risikokanäle — Bußgeld ist nur einer davon

Risikokanal	Jährliches Volumen in DE	Wahrscheinlichkeit für ein KMU	Typische Kosten pro Vorfall
Behörden-Bußgeld	~250–350 Bescheide/Jahr	Sehr gering (~0,007 %)	100–10.000 €
Datenpannen-Meldungen	~27.000 Meldungen/Jahr (2024)	Mittel — jede Meldung kann Prüfverfahren auslösen	5.000–30.000 € (Anwaltskosten + Aufwand)
Beschwerden von Betroffenen	Tausende/Jahr (2.000+ beim Bundesbeauftragten, dazu 16 Landesbehörden)	Mittel — ein unzufriedener Kunde oder Ex-Mitarbeiter reicht	2.000–15.000 € (Verfahrenskosten)
Schadensersatzklagen (Art. 82)	Steigende Tendenz seit EuGH C-300/21 (2023)	Gering bis mittel	500–5.000 € pro Betroffenem — bei vielen Betroffenen schnell sechsstellig
Abmahnungen	Keine zentrale Statistik, aber branchenüblich	Mittel — besonders bei fehlender Datenschutzerklärung, Cookies, KI-Hinweisen	3.000–10.000 € pro Abmahnung

Was die Zahlen wirklich bedeuten: Das Bußgeld ist nur die Spitze. 2024 wurden in Deutschland über 27.000 Datenpannen gemeldet — jede davon ein potenzielles Prüfverfahren. Dazu kommen Tausende Beschwerden, steigende Schadensersatzklagen und Abmahnungen. Der teuerste Posten ist selten das Bußgeld selbst, sondern die Kombination aus Anwaltskosten, Verfahrensaufwand, Reputationsschaden und — für den Geschäftsführer persönlich — der mögliche Regress nach § 43 GmbHG. Die entscheidende Frage bei einer Prüfung lautet nicht „Wie hoch wird das Bußgeld?", sondern: **„Können Sie nachweisen, dass Sie alles Zumutbare getan haben?"**

Genau dafür existieren die Anhänge dieses Buchs.

Rechenbeispiel: Was ein einziger Vorfall ein KMU kostet.
Ein Mitarbeiter gibt versehentlich eine Kundenliste (200 Kontakte) in ChatGPT Free ein. Was passiert?

(1) **Datenpanne melden** (72h-Frist, Art. 33 DSGVO) — Anwaltskosten: 3.000–5.000 €.
(2) **200 Betroffene benachrichtigen** (Art. 34 DSGVO) — Aufwand + Kommunikation: 2.000–5.000 €.
(3) **Behörde prüft:** Gab es eine KI-Richtlinie? Schulungen? War ChatGPT Free auf der Whitelist? Wenn nein: Bußgeld wegen Organisationsverschulden: 5.000–15.000 €.
(4) **Drei Kunden klagen** auf immateriellen Schadensersatz (Art. 82 DSGVO) — je 1.500 € plus Verfahrenskosten: 8.000–12.000 €.
(5) **Persönlicher Regress:** Das Unternehmen fordert das Bußgeld vom Geschäftsführer zurück (§ 43 GmbHG).

Gesamtkosten: 18.000–37.000 € — für einen Vorfall, der in 30 Sekunden passiert.
Kosten der Prävention (Richtlinie + Schulung + Whitelist nach den Anhängen dieses Buchs): ein Nachmittag und 0 €.

Praxisfall (Deutschland): Handwerksbetrieb mit 120 Mitarbeitern

Ausgangslage: Ein Vertriebsmitarbeiter exportiert Adressdaten aus dem CRM und nutzt ChatGPT Free zur Formulierung personalisierter Angebotsmails.

Fehler: Kein AVV für den genutzten Account, keine dokumentierte Richtlinie, keine Schulung, keine technische Sperre für private KI-Tools.

Folge: 72h-Meldung an die Behörde, Benachrichtigung von 430 Kontakten,

externer Rechtsbeistand, interne Sonderprüfung der IT-Prozesse.

Kostenbild: Externe Rechts- und Prozesskosten im mittleren fünfstelligen Bereich; der direkte Bußgeldanteil war nur ein Teil der Gesamtkosten.

Lernpunkt: Der teuerste Fehler war nicht die einzelne Eingabe, sondern die fehlende nachweisbare Organisation.

Executive Summary: Was diese Woche zu tun ist

1. Vollständige Liste aller genutzten KI-Tools und externer Berater/Dienstleister mit KI-Nutzung erstellen.
2. Alle KI-Accounts ohne AVV (inkl. private Accounts) sofort für Unternehmensdaten sperren.
3. Für HR-, CRM- und Support-Prozesse prüfen, ob Art. 22 DSGVO berührt ist.
4. Datenschutzerklärung und interne Richtlinie um KI-Nutzung ergänzen.
5. Für risikoreiche neue Anwendungsfälle eine DSFA-Prüfung als Pflichtschritt definieren.

Kapitel 3: Die Risiko-Brille (EU AI Act)

Der EU AI Act ist das weltweit erste umfassende Gesetz zur Regulierung von Künstlicher Intelligenz. Er trat im August 2024 in Kraft und verfolgt einen risikobasierten Ansatz: Je gefährlicher ein KI-System potenziell ist, desto strenger sind die Anforderungen.

3.1 Geltungsbereich und Zeitplan

Der AI Act gilt für jedes Unternehmen, das KI-Systeme in der EU einsetzt – unabhängig von der Unternehmensgröße und unabhängig davon, ob das Unternehmen seinen Sitz in der EU hat. Er unterscheidet zwischen *Anbietern* (die ein KI-System entwickeln, entwickeln lassen oder unter eigenem Namen auf den Markt bringen) und *Betreibern* (Unternehmen, die ein fremdes KI-System in eigener Verantwortung einsetzen). Viele Unternehmen sind zunächst als Betreiber betroffen, auch wenn sie KI nur einkaufen und nutzen.

Der Zeitplan für die Umsetzung ist gestaffelt [1]:

Datum	Was gilt?
Februar 2025	Verbotene KI-Praktiken sind untersagt. Die AI Literacy Pflicht (Art. 4) gilt.
August 2025	Neue General Purpose AI (GPAI) Systeme müssen die Vorgaben erfüllen.
August 2026	Grundsätzliche Anwendbarkeit des AI Acts. Hochrisiko-KI-Systeme (Anhang III) müssen alle Anforderungen umsetzen.
August 2027	Ende der Übergangsfristen für bestimmte Hochrisiko-Systeme, die bereits in anderen EU-Rechtsakten reguliert sind (Anhang II).

3.2 Die Risikoklassen im Überblick

Der AI Act teilt KI-Systeme in vier Risikoklassen ein, die jeweils unterschiedliche Pflichten nach sich ziehen:

Verbotene KI (Unvertretbares Risiko): Systeme, die eine klare Bedrohung für die Sicherheit, die Lebensgrundlagen und die Rechte der Menschen darstellen. Dazu gehören Social Scoring durch staatliche oder private Stellen, manipulative KI, die unterbewusste Beeinflussung nutzt, biometrische Massenüberwachung im öffentlichen Raum und Emotionserkennung am Arbeitsplatz (mit Ausnahmen für medizinische oder sicherheitsrelevante Gründe). Diese Systeme sind seit Februar 2025 strikt verboten. Verstöße werden mit bis zu 35 Mio. € oder 7 % des weltweiten Jahresumsatzes geahndet.

Hochrisiko-KI: Systeme, die in kritischen Bereichen eingesetzt werden. Anhang III des AI Acts listet die betroffenen Anwendungsfälle auf, darunter KI in der Personalbeschaffung (Lebenslauf-Analyse, Interviewauswertung), KI-gestützte Leistungsbewertung, bei der Kreditwürdigkeitsprüfung, in kritischen Infrastrukturen, im Bildungswesen und in der Strafverfolgung. Wichtig: Gängige HR-Tools wie Personio bieten Performance-Summaries und Bewerber-Scoring inzwischen standardmäßig an – das sind Hochrisiko-Anwendungen nach Anhang III. Hier gelten strenge Pflichten: Registrierung in einer EU-Datenbank, Konformitätsbewertung, technische Dokumentation, menschliche Aufsicht und Logging.

Begrenzt riskant: Systeme wie Chatbots oder KI zur Generierung von Texten und Bildern. Hier gilt primär eine *Transparenzpflicht*: Der Nutzer muss wissen, dass er mit einer KI interagiert (Art. 50 AI Act). Für KI-generierte Inhalte (Deepfakes, synthetische Texte) gelten Kennzeichnungspflichten. Diese Pflicht gilt auch für KI-generierte Vertriebs-E-Mails aus CRM-Systemen (HubSpot Breeze AI, Salesforce Einstein) und automatisierte Chatbot-Antworten im Kundenservice – nicht nur für offensichtliche Chatbot-Interfaces.

Minimal riskant: Systeme wie Spam-Filter oder einfache Empfehlungsalgorithmen. Hier gibt es keine spezifischen gesetzlichen Pflichten; freiwillige Verhaltenskodizes werden empfohlen.

3.3 Pflichten für Betreiber vs. Anbieter

Während Anbieter die Hauptlast der Zertifizierung tragen, haben auch *Betreiber* klare Pflichten nach Art. 26 AI Act. Sie müssen die Risikoklasse des eingesetzten Systems bestimmen, die Gebrauchsanweisung des Anbieters befolgen, die menschliche Aufsicht sicherstellen und relevante Logs aufbewahren.

Wenn Ihr Unternehmen ein KI-Modell – ob Open-Source oder kommerziell – wesentlich anpasst und daraus ein Produkt macht, werden Sie rechtlich vom „Betreiber" zum „Anbieter" (Art. 25 Abs. 1 EU AI Act). Typische Fälle: Fine-Tuning eines GPT-Modells auf eigenen Daten, Aufbau eines RAG-Systems auf internen Dokumenten, Entwicklung eines eigenen Chatbots, der intern oder an Kunden ausgerollt wird. Das gilt unabhängig davon, ob das Grundmodell Open-Source oder lizenziert ist – entscheidend ist, dass Sie aus einem bestehenden Modell ein eigenes System machen und es bereitstellen. Damit treffen Sie plötzlich die vollen Pflichten des AI Acts – inklusive Konformitätsbewertung und technischer Dokumentation.

3.4 AI Literacy: Die sofortige Schulungspflicht (Art. 4)

Eine der wichtigsten und am häufigsten übersehenen Pflichten gilt bereits seit *Februar 2025*: Die AI Literacy Pflicht nach Art. 4 AI Act.

Unternehmen müssen sicherstellen, dass alle Mitarbeiter, die mit KI arbeiten, ausreichend geschult sind. Ein informelles Selbststudium der Mitarbeiter reicht nicht aus. Die Geschäftsführung ist verantwortlich für die systematische Schulung und deren *Dokumentation*. Fehlt diese Dokumentation, liegt ein nachweisbarer Organisationsmangel vor. Art. 4 selbst ist zwar nicht direkt bußgeldbewehrt, aber der fehlende Nachweis wirkt bei jedem DSGVO-Vorfall,

jeder Schadensersatzklage und jedem Regress-Verfahren gegen die Geschäftsführung als belastender Umstand. Die Schulungspflicht schützt nicht primär vor dem AI Act – sie schützt vor der Haftung, wenn etwas schiefgeht.

Die unbequeme Wahrheit – und warum sie nicht schützt: Art. 4 AI Act gilt seit Februar 2025. Aber die Bundesnetzagentur als zuständige Aufsichtsbehörde baut ihre KI-Kapazitäten gerade erst auf. Es gibt heute keine aktiven Kontrollen und keine direkte Bußgeldbewehrung für fehlende Schulungen. Wer nur auf die Durchsetzungslage schaut, könnte denken: „Kann warten." Das wäre aus drei Gründen ein Fehler.

Grund 1 – Die Schulungsdokumentation schützt bei DSGVO-Vorfällen. Wenn ein Mitarbeiter Kundendaten in ein KI-Tool eingibt, prüft die Datenschutzbehörde nicht Art. 4 AI Act – sie prüft, ob das Unternehmen seine Organisationspflichten nach DSGVO erfüllt hat: Gab es eine Richtlinie? Wurden Mitarbeiter geschult? Gibt es eine Teilnehmerliste? Wenn nein, liegt Organisationsverschulden vor – und das wird heute schon sanktioniert.

Grund 2 – Ab August 2026 werden die Hochrisiko-Pflichten scharf. Wer KI-gestützte Personalentscheidungen oder Kreditscoring einsetzt, muss dann ein Qualitätsmanagementsystem mit dokumentierten Schulungen nachweisen. Wer heute anfängt, hat bis dahin zwei dokumentierte Schulungszyklen vorzuweisen.

Grund 3 – 30 Minuten heute, 30.000 Euro gespart. Die Schulung nach Anhang C dieses Buchs kostet 30 Minuten pro Mitarbeiter und keine externen Kosten – verglichen mit den Kosten eines einzigen DSGVO-Vorfalls (→ Kapitel 2.4) die beste

Investition, die ein Geschäftsführer tätigen kann.

Die Schulung nach Anhang C dieses Buchs erfüllt die AI-Literacy-Pflicht und die DSGVO-Organisationspflicht gleichzeitig.

Stand der AI-Literacy-Durchsetzung (März 2026)	
Pflicht gilt seit	2. Februar 2025
Zuständige Behörde (DE)	Bundesnetzagentur (BNetzA)
Aktive Kontrollen bisher	Keine. Aufbauphase läuft.
Direkte Bußgelder für fehlende Schulungen	Nicht vorgesehen. Art. 4 ist ein verpflichtender Grundsatz, keine bußgeldbewehrte Einzelpflicht.
Indirekte Haftung	Ja – DSGVO Art. 83 (Organisationsverschulden), § 43 GmbHG / § 93 AktG (GF-Haftung), ab August 2026 über AI Act Hochrisiko-Pflichten
Empfohlene Frequenz	Jährlich + Onboarding + anlassbezogen bei neuen KI-Systemen
Nachweis	Dokumentierte Teilnehmerliste (→ Anhang C), mind. 3 Jahre aufbewahren

3.5 Konsequenzen bei Verstößen

Die Sanktionen unter dem EU AI Act sind drakonisch und übersteigen sogar die der DSGVO:

Verstoß	Bußgeld
Einsatz verbotener KI	Bis zu 35 Mio. € oder 7 % des weltweiten Jahresumsatzes
Verstoß gegen Hochrisiko-Pflichten (Art. 26)	Bis zu 15 Mio. € oder 3 % des Jahresumsatzes
Falsche Angaben gegenüber Behörden	Bis zu 7,5 Mio. € oder 1 % des Jahresumsatzes

Verstoß	Bußgeld
Verstoß gegen AI Literacy (Art. 4)	Bußgelder gegen das Unternehmen; Gefahr des persönlichen Regresses gegen die GF

Praxisfall (Deutschland): Maschinenbauer mit KI-gestützter Bewerbervorauswahl

Ausgangslage: Ein mittelständischer Maschinenbauer aktiviert KI-Scoring in seinem HR-System, um Bewerbungen vorzusortieren.

Fehler: Einsatz wurde intern als "Tool-Feature" behandelt, nicht als Hochrisiko-Anwendungsfall. Es gab keine formale Einstufung, keine dokumentierte menschliche Aufsicht und keine Schulungsnachweise.

Folge: Bei externer Prüfung musste das Verfahren ausgesetzt werden, bis Prozess, Dokumentation und Rollen neu aufgesetzt waren.

Lernpunkt: Das Risiko entsteht nicht erst beim Bußgeld, sondern schon beim Betriebsstopp eines zentralen HR-Prozesses.

Executive Summary: Was diese Woche zu tun ist

1. Jedes KI-System in vier Risikoklassen des AI Acts einordnen und dokumentieren.
2. Für alle Hochrisiko-Kandidaten einen Maßnahmenplan bis August 2026 definieren.
3. AI-Literacy-Schulung mit Teilnehmerliste als Pflichtprozess etablieren.
4. Betreiber- vs. Anbieter-Rolle je System schriftlich festhalten.

Kapitel 4: Die Sicherheits-Brille (NIS2 & BSIG)

Während die DSGVO Daten schützt und der AI Act die KI-Modelle reguliert, zielt die NIS2-Richtlinie auf die fundamentale Sicherheit der IT-Infrastruktur ab. KI-Systeme sind mächtige Werkzeuge, aber sie sind auch komplexe Software, die angegriffen, manipuliert oder als Einfallstor in Unternehmensnetzwerke genutzt werden kann.

4.1 Von NIS zu NIS2: Das neue BSI-Gesetz in Deutschland

Die NIS2-Richtlinie (EU) 2022/2555 wurde in Deutschland durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in nationales Recht überführt. Kernstück ist das neu gefasste BSI-Gesetz (BSIG), das am 5. Dezember 2025 im Bundesgesetzblatt veröffentlicht wurde und am 6. Dezember 2025 in Kraft trat [2].

Das neue BSIG modernisiert den regulatorischen Rahmen für IT-Sicherheit grundlegend. Die Zahl der regulierten Einrichtungen in Deutschland steigt damit von bislang etwa 4.500 auf rund 29.000 [2]. Eine generelle Übergangsfrist ist nicht vorgesehen – das Gesetz gilt mit sofortiger Wirkung.

4.2 Wer ist betroffen?

Das Gesetz unterscheidet zwischen "besonders wichtigen Einrichtungen" und "wichtigen Einrichtungen". Die Einstufung erfolgt nach der sogenannten *Size-Cap-Rule*, einer Kombination aus Sektorzugehörigkeit und Unternehmensgröße.

Erfasst sind 18 Sektoren, darunter Energie, Transport, Finanzwesen, Gesundheit, Digitale Infrastrukturen, aber auch Abfallbewirtschaftung, Maschinenbau, Chemie und Forschung [2].

Kategorie	Kriterien	Bußgeldrahmen
Wichtige Einrichtungen	50–249 Mitarbeiter, 10–50 Mio. € Umsatz, in einem der 18 Sektoren	Mindestens 7 Mio. € oder 1,4 % des Umsatzes (als gesetzliche Untergrenze für den Maximalrahmen)
Besonders wichtige Einrichtungen	> 250 Mitarbeiter oder > 50 Mio. € Umsatz, in einem der 18 Sektoren	Mindestens 10 Mio. € oder 2 % des Umsatzes (als gesetzliche Untergrenze für den Maximalrahmen)

Es gibt keine behördliche Benachrichtigung! Unternehmen müssen eigenständig feststellen, ob sie betroffen sind, und sich beim BSI registrieren [2]. Die Feststellung der Betroffenheit ist eine Leitungsaufgabe der Geschäftsführung. Wer sich nicht registriert, obwohl er betroffen ist, begeht bereits einen Verstoß.

4.3 Kernpflichten: Risikomanagement, Lieferkette, Dokumentation

Zentraler Anknüpfungspunkt ist § 30 BSIG. Er verlangt ein systematisches Informationssicherheits-Managementsystem (ISMS). Es reicht nicht mehr, eine Firewall und einen Virenscanner zu betreiben. Gefordert wird ein ganzheitlicher Ansatz, der mindestens folgende Elemente umfasst:

Risikomanagement: Kontinuierliche Bewertung von Cyberrisiken und Implementierung technischer und organisatorischer Maßnahmen. Das schließt KI-Systeme explizit ein – ein schlecht gesichertes KI-System ist ein Angriffsvektor.

Sicherheit der Lieferkette: Dies ist ein massiver Hebel. Unternehmen müssen sicherstellen, dass auch ihre Dienstleister und Zulieferer (inklusive KI-Anbieter) hinreichende Sicherheitsstandards erfüllen. Ein KI-Anbieter, der keine ISO 27001-Zertifizierung vorweisen kann, ist ein Risiko in der Lieferkette.

Dokumentation: Alle Risikoanalysen und Maßnahmen müssen nachvollziehbar dokumentiert werden, um im Prüfungsfall gegenüber dem BSI bestehen zu können. Die Beweislast liegt beim Unternehmen.

4.4 Meldepflichten im Ernstfall

Bei erheblichen Sicherheitsvorfällen gelten extrem straffe, mehrstufige Meldepflichten an das BSI [2]:

Frist	Inhalt
24 Stunden	Erstmeldung (Frühwarnung): Vorfallstyp, betroffene Systeme, erste Einschätzung.
72 Stunden	Detaillierte Meldung mit erster Ursachenanalyse und Schadensausmaß.
1 Monat	Umfassender Abschlussbericht mit Ursache, Auswirkungen und getroffenen Maßnahmen.

4.5 Sanktionen und persönliche Haftung der Geschäftsleitung

Das BSIG macht Cybersicherheit endgültig zur Chefsache. Nach § 38 BSIG muss die Geschäftsleitung die Sicherheitsmaßnahmen nicht nur genehmigen, sondern aktiv überwachen. Zudem besteht eine Pflicht zur regelmäßigen Schulung (mindestens alle drei Jahre) [2].

Die Verantwortung ist nicht vollständig delegierbar. Bei Versäumnissen droht die persönliche Haftung der Geschäftsleiter. Das Benennen einer zuständigen IT-Sicherheitsperson entlastet die Geschäftsführung nur dann, wenn diese Person auch tatsächlich handlungsfähig ist: mit Befugnissen, Budget und direktem Zugang zur Geschäftsführung. Fehlen diese Elemente, ist die Delegation unwirksam.

Praxisfall (Deutschland): Zulieferer ohne NIS2-Selbsteinstufung

Ausgangslage: Ein Industriezulieferer (ca. 180 Mitarbeiter) war als "nicht kritisch" eingestuft und hatte keine BSI-Registrierung vorgenommen.

Fehler: Die eigene Sektorzuordnung und Größenprüfung wurde nie formal durchgeführt; Sicherheitsmaßnahmen waren vorhanden, aber nicht auf BSIG-Nachweise ausgerichtet.

Folge: Im Rahmen einer Kundenprüfung wurde die fehlende NIS2-Transparenz eskaliert. Der Kunde machte Vertragsverlängerung von einem dokumentierten Maßnahmen- und Registrierungsplan abhängig.

Lernpunkt: Fehlende Nachweisfähigkeit kann schon vor einer Behördenprüfung zu Umsatzrisiken führen.

Executive Summary: Was diese Woche zu tun ist

1. NIS2-Betroffenheit (Sektor + Size-Cap-Rule) formal prüfen und protokollieren.
2. Falls betroffen: BSI-Registrierung und Meldeprozess (24h/72h/1 Monat) vorbereiten.
3. KI-Anbieter als Teil der Lieferkette in das ISMS aufnehmen.
4. Verantwortlichkeit der Geschäftsleitung mit Befugnissen und Reporting-Rhythmus festschreiben.

Kapitel 5: KI-Reifegrade und Governance-Szenarien

Je tiefer KI in die Unternehmensprozesse eindringt, desto komplexer wird die Governance. Das folgende Reifegradmodell beschreibt fünf Entwicklungsstufen, die jeweils eigene Risiken, Verantwortlichkeiten und Sofortmaßnahmen mit sich bringen. Entscheidend ist: Die meisten Unternehmen überschätzen ihre eigene Reife und unterschätzen die damit verbundenen Risiken.

5.1 Stufe 1: Shadow AI – Das unsichtbare Risiko

Das Szenario: Das Unternehmen hat keine offizielle KI-Lösung. Mitarbeiter nutzen private Accounts (ChatGPT Free/Plus, Claude Pro) für berufliche Zwecke – aus Eigeninitiative, ohne Wissen der Geschäftsführung.

Was dabei passiert: Kundendaten, Quellcode, Strategiepapiere und Personalinformationen fließen unkontrolliert an US-Server ab. Es gibt keinen AVV, keine Rechtsgrundlage, keine Kontrolle. Die Eingaben können für das Modelltraining des Anbieters genutzt werden.

Die Haftung: Das Unternehmen haftet voll (DSGVO Art. 83). Fehlende Richtlinien gelten als Organisationsverschulden der Geschäftsführung. "Ich wusste nicht, dass Mitarbeiter das tun" ist keine Verteidigung – es ist das Organisationsverschulden.

Sofortmaßnahmen:

#	Maßnahme	Priorität
1	KI-Nutzungsrichtlinie einführen (Anhang A) und von allen Mitarbeitern unterschreiben lassen.	**Sofort**
2	Schulung aller Mitarbeiter mit Dokumentation (Anhang C).	**Sofort**
3	Private Accounts für berufliche Zwecke explizit verbieten.	**Sofort**

#	Maßnahme	Priorität
4	Offizielles Tool mit AVV einführen (z.B. ChatGPT Business).	Kurzfristig

5.2 Stufe 2: Kontrollierte Nutzung

Das Szenario: Offizielle Tools (z.B. ChatGPT Business) mit AVV sind eingeführt. Aber das Wissen ist ungleich verteilt, systematische Schulungen fehlen, und "versteckte" KI in Tools wie Notion AI oder Slack AI läuft unkontrolliert mit. Externe Berater nutzen weiterhin private Tools.

Was dabei passiert: Der AI Act (Art. 4 AI Literacy) wird verletzt, weil dokumentierte Schulungen fehlen. Kategorie-5-Tools (Produktivitätssoftware mit eingebetteter KI) verarbeiten Daten über Sub-Processors (z.B. Notion → OpenAI, HubSpot → OpenAI), ohne dass dies im AVV erfasst ist. Bei CRM-Systemen sind das direkt Kundendaten; bei HR-Tools Gesundheits- und Gehaltsdaten nach Art. 9 DSGVO.

Sofortmaßnahmen:

#	Maßnahme	Priorität
1	Dokumentierte Schulungen für alle Mitarbeiter durchführen (AI Literacy Pflicht).	**Sofort**
2	Alle Produktivitätstools auf eingebettete KI-Features prüfen (Notion AI, Slack AI, Jira AI etc.).	**Sofort**
3	Dienstleisterverträge um KI-Klauseln ergänzen.	Kurzfristig
4	AVVs der Hauptanbieter auf Sub-Processor-Ketten prüfen.	Kurzfristig

5.3 Stufe 3: Eigene KI-Projekte

Das Szenario: Das Unternehmen baut eigene KI-Anwendungen: RAG-Systeme auf internen Daten, eigene Chatbots über APIs (OpenAI API, Anthropic API), KI-

Features im eigenen Produkt.

Das Kernproblem: Das Unternehmen denkt noch in Stufe-2-Kategorien ("Haben wir den AVV?"), entwickelt aber in Stufe-3-Realität. Eigene KI-Entwicklung bedeutet neue Rollen, neue Pflichten und neue Haftungsrisiken, die kein AVV mit einem Tool-Anbieter abdeckt.

Was dabei passiert:

Typische Situation	Was dabei passiert	Rechtliches Risiko
KI-System als Feature im eigenen Produkt – Kunden wurden nicht informiert	Kunden wissen nicht, dass ihre Daten KI-verarbeitet werden. Datenschutzerklärung und AGB wurden nicht aktualisiert.	**Hoch** –DSGVO Art. 13/14 – Informationspflicht. Abmahnrisiko + Bußgeld.
Automatisierte Entscheidungen ohne menschliche Aufsicht	System trifft Entscheidungen (Bonitätsprüfung, Bewerbungsvorauswahl) vollautomatisch ohne menschliche Prüfung.	**Hoch** –DSGVO Art. 22. Bußgeld + Schadensersatz.
API-Nutzung ohne separaten AVV	Kundendaten werden an OpenAI API gesendet. Consumer-AVV gilt nicht für API-Nutzung.	**Hoch** –DSGVO Art. 28 – Auftragsverarbeitung ohne AVV.
Keine DSFA durchgeführt	Neues KI-System verarbeitet personenbezogene Daten systematisch, ohne vorherige Datenschutz-Folgenabschätzung.	**Hoch** –DSGVO Art. 35 – Pflicht vor Go-Live. Gesamte Verarbeitung rechtswidrig.
Keine technische Dokumentation	Kein Nachweis was das System tut, wie es trainiert wurde, welche Tests durchgeführt wurden.	**Mittel** –EU AI Act Art. 11 (Hochrisiko) + erhöhtes GF-Haftungsrisiko.

Sofortmaßnahmen vor Go-Live:

#	Maßnahme	Priorität
1	Risikoklassen-Check nach EU AI Act für jedes KI-Projekt (Anhang III prüfen).	**Vor Projektstart**
2	DSFA durchführen und dokumentieren (Art. 35 DSGVO).	**Vor Go-Live**

#	Maßnahme	Priorität
3	API-AVV mit Modell-Anbieter abschließen (separater Vertrag!).	**Vor erster Produktivdaten-Verarbeitung**
4	Informationspflichten aktualisieren: Datenschutzerklärung, AGB, KI-Transparenzhinweise.	**Vor Marktstart**
5	Technische Dokumentation einführen: Architektur, Datenquellen, Modell-Versionen, Tests.	Ab Entwicklungsbeginn
6	Menschliche Aufsicht definieren: Wer prüft automatisierte Entscheidungen? Wie wird dokumentiert?	**Vor Go-Live**

Stufe 3 ist der kritischste Übergang im Reifegrad-Modell. Die meisten Unternehmen unterschätzen, was eigene KI-Entwicklung regulatorisch bedeutet. Wer vorher nur Nutzer war, wird jetzt Verantwortlicher – mit allen Pflichten, die das mitbringt.

5.4 Stufe 4: Strukturierte KI-Governance (Risk Framework)

Das Szenario: Das Unternehmen hat mehrere KI-Projekte erfolgreich gelauncht und wächst als KI-getriebenes Unternehmen. Die ad-hoc-Governance aus Stufe 3 reicht nicht mehr. Die Lösung: eine dedizierte Person oder Funktion übernimmt AI Governance – ein AI Owner, Head of AI oder erster Chief AI Officer (CAIO).

Das Kernproblem: Governance-Strukturen wurden eingeführt, aber noch nicht institutionalisiert. Der Unterschied zwischen einer Governance, die im Alltag funktioniert, und einer, die nur auf dem Papier existiert, ist in Stufe 4 besonders groß.

Typische Situation	Was dabei passiert	Governance-Risiko
AI Owner ernannt – aber Mandat, Budget und Befugnisse fehlen	Die Person kann warnen, aber nichts stoppen. Kein Vetorecht, kein Budget für externe Audits.	**Mittel** –Governance-Theater. GF haftet trotzdem persönlich.
Risk Framework existiert auf Papier – wird nicht angewendet	Entwicklungsteams umgehen den Prozess unter Zeitdruck. "Das ist nur ein kleines Feature."	**Mittel** –Compliance-Lücke: Ein nicht geprüftes Hochrisiko-System bleibt ein Hochrisiko-System.
Hochrisiko-Systeme aus Stufe 3 nie formal eingestuft	Ab August 2026 müssen alle Hochrisiko-Systeme EU AI Act konform sein. Keine Bestandsschutzklausel.	**Hoch** –EU AI Act Art. 26 – Betriebsverbot + bis 15 Mio. € / 3 % Umsatz.
KI-Modelle werden ausgetauscht – Governance folgt nicht	Modellwechsel (z.B. GPT-4 auf GPT-5) löst erneute Prüfpflichten aus (DSFA, VVT-Update).	**Mittel** –Compliance-Schulden akkumulieren sich.

Maßnahmen für Stufe 4:

#	Maßnahme	Priorität
1	AI Owner mit echtem Mandat ausstatten: Vetorecht, Budget, direkter Zugang zur GF.	**Sofort**
2	Alle bestehenden KI-Systeme inventarisieren und nach EU AI Act einstufen.	**Sofort** – Frist August 2026 läuft
3	KI-Projekt-Gate einführen: Kein Projekt in Produktion ohne Governance-Durchlauf.	Kurzfristig
4	Logging- und Monitoring-Konzept für alle KI-Systeme etablieren.	Kurzfristig
5	Change-Management-Prozess für Modellwechsel: Jeder Wechsel = neue Implementierung.	Mittelfristig
6	Erste externe Prüfung / Pre-Audit vorbereiten, bevor die Aufsichtsbehörde prüft.	Vor August 2026

5.5 Stufe 5: KI-Governance als Wettbewerbsvorteil

Das Szenario: Das Unternehmen hat alle Compliance-Hausaufgaben erledigt – und geht weiter. KI-Governance ist kein internes Pflichtprogramm mehr, sondern ein aktiver Teil der Marktpositionierung. Kunden fragen gezielt nach: Wie geht ihr mit unseren Daten um? Habt ihr ein Zertifikat? Partner machen Governance-Nachweise zur Voraussetzung für Zusammenarbeit.

Der entscheidende Unterschied zu Stufe 4: In Stufe 4 wird Governance intern gelebt. In Stufe 5 wird sie extern kommuniziert und nachgewiesen.

Hebel	Was das konkret bedeutet	Wettbewerbsvorteil
ISO 42001 Zertifizierung	Unabhängige Zertifizierungsstelle bestätigt ein funktionierendes KI-Managementsystem.	In B2B-Ausschreibungen zunehmend gefordert.
Öffentliche KI-Grundsätze	Veröffentlichung der eigenen KI-Prinzipien: Welche Systeme werden nicht gebaut? Wie werden Betroffene geschützt?	Vertrauen bei Kunden und Bewerbern.
Externe Audits als Marketing-Asset	Audit-Berichte werden aktiv kommuniziert: im Jahresbericht, auf der Website, in Kundenpräsentationen.	Reduziert Vendor-Assessment-Aufwand bei Großkunden erheblich.
CAIO in der Unternehmensführung	Chief AI Officer ist Mitglied der Geschäftsleitung oder hat direkten, regelmäßigen Zugang.	Signalisiert strategische KI-Reife. Investoren und Großkunden erwarten das zunehmend.
Proaktives Engagement mit Regulatoren	Teilnahme an EU-Konsultationen, Kontakt zur Marktüberwachungsbehörde.	Frühe Information über regulatorische Entwicklungen. Reputation als verantwortungsvoller Akteur.

Stufe 5 ist kein Endzustand, sondern eine Haltung. Regulierung entwickelt sich weiter, Technologie entwickelt sich weiter. Unternehmen auf Stufe 5 haben die Strukturen, um mit dieser Dynamik umzugehen – proaktiv statt reaktiv.

5.6 Übersicht: Die fünf Reifegrade im Vergleich

Stufe	Kerncharakteristik	Governance-Lücke
Stufe 1 – Shadow AI	KI-Nutzung ohne Wissen oder Erlaubnis der GF	Keine Grundlage – akutes Bußgeld- und Strafrechtsrisiko
Stufe 2 – Kontrollierte Nutzung	Offizielle Tools eingeführt, Schulung & Dokumentation fehlen	Compliance begonnen, aber nicht abgeschlossen
Stufe 3 – Eigene KI-Projekte	Eigene Anwendungen entwickelt, Deployer-Pflichten nicht erkannt	Keine Systematik – jedes Projekt kämpft allein mit Compliance
Stufe 4 – Risk Framework	AI Owner + strukturierter Prozess, aber nicht vollständig institutionalisiert	Governance funktioniert im Guten, bricht unter Druck zusammen
Stufe 5 – Wettbewerbsvorteil	Governance gelebt, zertifiziert, extern kommuniziert	Keine Lücke – Governance ist Teil des Produkts und der Marktpositionierung

Praxisfall (Deutschland): Fehleinschätzung "Wir sind schon Stufe 4"

Ausgangslage: Ein SaaS-KMU mit mehreren KI-Features sieht sich selbst auf Stufe 4, weil ein "AI Owner" benannt wurde.

Fehler: Der AI Owner hatte weder Budget noch Vetorecht; Modellwechsel wurden ohne Re-Assessment in Produktion gebracht.

Folge: Bei Due-Diligence durch einen Großkunden fielen fehlende Nachweise auf. Der Abschluss verzögerte sich um mehrere Monate.

Lernpunkt: Reifegrad ist nicht Titel, sondern belastbarer Prozess unter Zeitdruck.

Executive Summary: Was diese Woche zu tun ist

1. Eigenen Reifegrad ehrlich einstufen und mit Nachweisen belegen.

2. Für den aktuellen Reifegrad genau die nächste Stufe als Ziel definieren.
3. AI Owner nur dann benennen, wenn Mandat, Budget und Vetorecht geklärt sind.
4. Modellwechsel-Prozess als Pflicht-Gate in die Entwicklung integrieren.

Kapitel 6: Tool-Vergleich: ChatGPT-Ersatz im Unternehmensalltag

Sobald Shadow AI verboten wird, muss eine legale Alternative her. Die zentrale Frage lautet: Welches Tool darf rechtlich genutzt werden – und unter welchen Bedingungen? Die folgende Übersicht zeigt die fünf Kategorien von Lösungen mit Datenschutzbewertung und notwendigen Voraussetzungen.

> **Hinweis zu den Preisen:** Alle Preise in USD, Stand März 2026. Preise können sich ändern – vor Beschaffung aktuelle Preisliste des Anbieters prüfen.

6.1 Kategorie 1: US-Anbieter mit Enterprise-Vertrag

Die bekanntesten KI-Tools (ChatGPT, Claude, Gemini) sind US-amerikanische Dienste. Für den Unternehmenseinsatz gibt es Business- und Enterprise-Tarife mit AVV und Zero Data Retention – also ohne Nutzung der Eingaben für das Modelltraining. Das Kernrisiko bleibt: Als US-Unternehmen unterliegen sie dem CLOUD Act.

Tool / Tarif	Preis (pro User/Monat)	PII erlaubt?	Datenstandort, Bedingungen & CLOUD Act Risiko
ChatGPT Free / Plus / Pro	$0 / $20 / $200	Nein	USA. Kein AVV. Eingaben können für Modelltraining genutzt werden. Kein Unternehmenskonto. Nutzung mit PII grundsätzlich verboten.
Claude Free / Pro	$0 / $20	Nein	USA. Kein AVV. Gilt auch für Berater/Freelancer – das Unternehmen haftet trotzdem. Nutzung mit PII verboten.

Tool / Tarif	Preis (pro User/Monat)	PII erlaubt?	Datenstandort, Bedingungen & CLOUD Act Risiko
ChatGPT Business	$25 (jährl.) / $30 (monatl.), min. 2 User	Ja *	USA – EU-Server optional buchbar. AVV enthalten. Keine Nutzung für Training. Nur über Unternehmenskonto. CLOUD Act: Mittel.
ChatGPT Enterprise	~$60 (custom, jährl.)	Ja **	USA – EU-Server wählbar. AVV + Zero Data Retention. Erweiterte Compliance-Features. Min. 150 User empfohlen. CLOUD Act: Mittel.
Claude Team	$25 (jährl.) / $30 (monatl.), min. 5 User	Ja *	USA (AWS). AVV enthalten. Keine Nutzung für Training. CLOUD Act: Mittel.
Claude Enterprise	~$125+ (custom, jährl.)	Ja **	USA / AWS – EU-Region wählbar. AVV + HIPAA-Option. SSO, Audit-Logs. Min. 20 Seats. CLOUD Act: Mittel.
Google Gemini for Workspace	$30 Add-on (zu bestehendem Workspace-Abo)	Ja *	USA – EU-Server optional. AVV über Google-Vertrag. Zero Data Retention konfigurierbar. Setzt Google Workspace voraus. CLOUD Act: Mittel.

Bedingungen für PII-Nutzung (Business-/Team-Tarif): 1. Nur über den gebuchten Unternehmens-Account – kein privater oder kostenloser Account. 2. AVV muss vorliegen. Bei vielen Business-Tarifen ist er in den Standardbedingungen enthalten, dies muss jedoch je nach Vertragsversion und Buchungsweg geprüft werden. Zudem ist zu prüfen, ob der Standard-DPA alle spezifischen deutschen Anforderungen nach Art. 28 Abs. 3 DSGVO erfüllt. 3. Eingaben werden nicht für das Modelltraining genutzt – aber auf US-Servern des Anbieters verarbeitet (CLOUD Act Restrisiko). 4. Besonders sensible Daten (Gesundheit, Anwalt, Behörde) sollten auch in diesen Tarifen nicht eingegeben werden – hier europäische Lösung prüfen.

Bedingungen für PII-Nutzung (Enterprise-Tarif, zusätzlich): 5. EU-Server-Region muss beim Vertragsabschluss aktiv gewählt und schriftlich bestätigt werden – Standard ist US-Region. 6. Zero Data Retention (ZDR) muss explizit im Vertrag

vereinbart sein – nicht alle Enterprise-Verträge enthalten dies automatisch.

Warnung für Berater & Freelancer: Arbeitet ein externer Dienstleister mit Daten des Unternehmens, bleibt das Unternehmen DSGVO-Verantwortlicher. Der Berater ist Auftragsverarbeiter (Art. 28 DSGVO) – das Unternehmen muss vertraglich sicherstellen, dass er keine privaten KI-Accounts (ChatGPT Pro, Claude Pro etc.) für Auftragsdaten einsetzt. "Der hat das ohne mein Wissen gemacht" schützt nicht. Das Unternehmen hätte es vertraglich ausschließen und kontrollieren müssen. Fehlende Kontrolle ist selbst ein DSGVO-Verstoß.

6.2 Kategorie 2: Microsoft 365 Copilot – Der Sonderfall

Microsoft nimmt eine Sonderrolle ein: Als einziger der großen US-Anbieter hat Microsoft eine EU Data Boundary-Zusage gegeben – Daten von EU-Kunden werden in EU-Rechenzentren (Frankfurt, Amsterdam) verarbeitet und gespeichert, nicht nur gehostet. Das macht Copilot zur rechtlich stärksten US-Lösung für die meisten deutschen Unternehmen.

Wichtig: Copilot ist ein Add-on – es setzt eine bestehende Microsoft 365 Lizenz voraus. Die Gesamtkosten sind daher höher als der reine Copilot-Preis.

Variante	Preis (Copilot Add-on + Gesamt)	Datenstandort	Besonderheit
M365 Copilot Business (bis 300 User)	~$21 Add-on (Promo bis 03/26), normal $30. Gesamt: ~$34/User/Monat	EU-Rechenzentren (Frankfurt/Amsterdam), EU Data Boundary. PII erlaubt.	Günstigster Einstieg für KMU. Gleiche Funktionen wie Enterprise-Version. AVV im M365-Vertrag enthalten.

Variante	Preis (Copilot Add-on + Gesamt)	Datenstandort	Besonderheit
M365 Copilot Enterprise (unbegrenzt)	$30 Add-on (jährl.). Gesamt: ~$52/User/Monat (inkl. E3-Lizenz)	EU-Rechenzentren, EU Data Boundary. PII erlaubt.	Volle M365-Integration: Word, Excel, Teams, Outlook. Zugriff auf SharePoint, E-Mails. AVV enthalten.

⚠ **Copilot-Risiko:** Copilot greift auf alle M365-Daten des Nutzers zu – E-Mails, Teams, SharePoint. Wenn Berechtigungskonzepte schlecht gepflegt sind, kann Copilot auf Dokumente zugreifen, die ein Nutzer eigentlich nicht sehen sollte. Vor Aktivierung: Berechtigungskonzept und Datenzugriffsrechte prüfen. Sensitivity Labels in SharePoint setzen.

6.3 Kategorie 3: Europäische Anbieter – Kein CLOUD Act

Für Unternehmen mit erhöhten Datenschutzanforderungen – oder die grundsätzlich keine US-Anbieter einsetzen wollen – gibt es europäische Alternativen. Kein CLOUD Act, EU-Datenschutz, volle DSGVO-Konformität ohne Kompromisse.

Tool / Anbieter	Preis (pro User/Monat)	PII & Datenstandort	Für wen geeignet?
Mistral Le Chat Team (Mistral AI, Frankreich)	$25 (jährl.), Pro (Einzel): €14,99	Ja *. EU-Server (FR), kein CLOUD Act.	KMU, die bewusst keinen US-Anbieter wollen. Sehr gutes Preis-Leistungs-Verhältnis.
Aleph Alpha (Deutschland, Heidelberg)	Enterprise: nur auf Anfrage (gehobenes Preissegment)	Ja. Deutschland, BSI-konform.	Behörden, Rüstung, Medizin, Kanzleien – überall wo US-Anbieter ausgeschlossen sind. Für normale KMU zu teuer.

Bedingungen für PII-Nutzung (Mistral Le Chat Team): 1. AVV muss separat mit Mistral abgeschlossen werden – er ist nicht automatisch aktiv, sondern muss explizit angefordert und unterzeichnet werden. 2. Nur über den gebuchten Team-Account – kein privater oder kostenloser Account. 3. No-Telemetry-Modus muss in den Account-Einstellungen aktiviert werden.

6.4 Kategorie 4: Open Source – Maximale Kontrolle, höherer Aufwand

Open-Source-Modelle (Llama, Mistral Open, Qwen) können selbst betrieben werden – entweder auf eigener Hardware, bei europäischen Cloud-Anbietern oder bei US-Anbietern auf deutschen Servern. Der entscheidende Unterschied: Kein Datenabfluss an einen Drittanbieter, kein AVV nötig, volle Kontrolle. Der Preis: mehr technischer Aufwand.

Variante	Kosten (ca.)	PII & Datenstandort	Aufwand & CLOUD Act Risiko
Eigene Infrastruktur (On-Premises)	Hardware: €5.000–50.000. Modelle: kein laufender API-Preis.	Ja – kein Drittanbieter. Eigene Server. Kein CLOUD Act.	Hoch: GPU-Hardware nötig, IT-Betrieb, Updates. Keine SaaS-Benutzeroberfläche.
Europäischer Cloud-Anbieter (Hetzner, IONOS, OVHcloud, Telekom)	Server-Miete: ~€50–500/Monat (je nach GPU-Leistung).	Ja – kein CLOUD Act. EU-Server. Kein AVV mit KI-Anbieter nötig.	Mittel: Cloud-Server mieten, Modell installieren und betreiben.
US-Cloud auf deutschen Servern (AWS Frankfurt, Azure Germany)	Server-Miete: ~€100–800/Monat.	Bedingt. DE-Server, aber US-Vertrag. CLOUD Act: Restrisiko.	Mittel: Technisch auf deutschem Server, aber Vertragspartner ist US-Unternehmen.

6.5 Kategorie 5: Produktivitätstools mit eingebetteter KI – Das unterschätzte Risiko

Notion, Confluence, Slack, Jira, Asana, Monday.com, Miro und viele weitere Tools haben inzwischen KI-Funktionen direkt eingebaut. Das Risiko ist hier strukturell anders als bei ChatGPT – und wird deshalb häufig unterschätzt.

Der entscheidende Unterschied zu ChatGPT: Der Mitarbeiter entscheidet bei ChatGPT aktiv, was er eingibt. Bei eingebetteter KI kann das Modell passiv auf alle im Tool gespeicherten Daten zugreifen – Projektdokumente, Kundendaten, Personalakten – ohne dass jemand etwas eingetippt hat.

Dazu kommt: Die Verarbeitungskette ist länger. Notion AI beispielsweise nutzt OpenAI-Modelle als Sub-Processor. Das bedeutet: Unternehmen → Notion (AVV nötig) → OpenAI (AVV nötig) → US-Server. Beide AVVs müssen in der Kette funktionieren.

Tool	PII erlaubt?	Besonderes Risiko	Was zu prüfen ist
Notion AI *Texte, Zusammenfassungen, Datenbank-Abfragen*	Bedingt *	KI greift auf gesamten Workspace zu – inkl. Kundendatenbanken, Meeting-Notizen, interne Dokumente. Sub-Processor OpenAI: doppelte AVV-Kette nötig.	AVV mit Notion prüfen. KI-Feature separat deaktivieren bis Prüfung abgeschlossen.
Slack AI *Kanal-Zusammenfassungen, Antwortvorschläge*	Bedingt *	KI indexiert alle Kanal-Nachrichten – inkl. vertraulicher Unterhaltungen, Kundennamen. Betrifft auch historische Daten.	Slack AI in Enterprise-Einstellungen prüfen. Prüfen, ob es bereits aktiv ist.
Confluence / Jira (Atlassian AI) *Dokumentzusammenfassungen, Issue-Analyse*	Bedingt *	Confluence enthält oft Verträge, HR-Policies. Jira enthält Kundenprojekte, Bug-Reports mit Kundendaten.	Atlassian Intelligence in Admin-Einstellungen prüfen. EU-Datenresidenz konfigurieren.

Tool	PII erlaubt?	Besonderes Risiko	Was zu prüfen ist
Google Workspace (Gemini) *E-Mail-Entwürfe, Meeting-Transkription, Drive-Suche*	Bedingt *	Gemini greift auf alle Workspace-Daten zu – Gmail, Drive, Kalender. KI-Features teilweise standardmäßig aktiviert.	CDPA in der Admin Console akzeptieren. Gemini-Features und Data Regions konfigurieren.
Microsoft 365 Copilot *E-Mail-Zusammenfassungen, Meeting-Protokolle*	Ja *	Copilot greift auf alle M365-Daten des Nutzers zu. Schlechte Berechtigungskonzepte = Copilot sieht mehr als der Nutzer sollte.	Berechtigungskonzept und Sensitivity Labels prüfen bevor Copilot aktiviert wird.
Miro / Asana / Monday AI *Board-Analysen, Aufgaben-Zusammenfassungen*	Bedingt *	Projektboards enthalten Kundennamen, Projektdetails, Meilensteine. KI-Feature oft standardmäßig aktiviert ohne expliziten Hinweis.	AGB und Datenschutzrichtlinie auf KI-Features und Sub-Processors prüfen.
Personio / HiBob / BambooHR *Performance-Summaries, Bewerber-Scoring*	Bedingt *	Art. 9 DSGVO: Gehalt, Krankmeldungen, Bewerbungen. KI-Personalentscheidungen = Hochrisiko nach EU AI Act Anhang III.	DSFA vor Aktivierung. AVV auf KI-Sub-Processors prüfen. Human-in-the-Loop für alle personalrelevanten KI-Empfehlungen.
HubSpot / Salesforce / Pipedrive AI *Lead-Scoring, E-Mail-Generierung, Chatbots*	Bedingt *	KI greift auf gesamten Kundendatenbestand zu. Sub-Processor-Ketten (z.B. HubSpot → OpenAI). KI-Kundenkommunikation: Kennzeichnungspflicht Art. 50 AI Act.	AVV auf KI-Sub-Processors prüfen. Datenschutzerklärung um KI-Hinweis ergänzen. Lead-Scoring auf Art. 22 prüfen.

Praxis-Tipp Google Workspace: Der AVV heißt bei Google „Cloud Data Processing Addendum" (CDPA) und wird nicht per Unterschrift, sondern per Klick in der Admin Console akzeptiert (*Konto → Rechtliches und Compliance*). Viele Unternehmen nutzen Workspace seit Jahren, ohne diesen Schritt je gemacht zu haben. Zusätzlich sollte dort die Anwendbarkeit des EU-Datenschutzrechts

bestätigt und der Datenschutzbeauftragte eingetragen werden. **Die kostenlose Workspace-Version bietet keinen AVV – sie ist für Unternehmensdaten tabu.**

HR-Software ist kein normales Produktivitätstool. Personio, HiBob, BambooHR und ähnliche HR-Plattformen verarbeiten nicht nur personenbezogene Daten, sondern regelmäßig besondere Kategorien nach Art. 9 DSGVO – Gesundheitsdaten (Krankmeldungen, eAU), Gehalt, Leistungsbeurteilungen, Bewerberdaten. Gleichzeitig stuft der EU AI Act KI in der Personalbeschaffung und Leistungsbewertung als Hochrisiko ein (Anhang III). Das bedeutet:

1. Eine DSFA nach Art. 35 DSGVO ist vor Aktivierung der KI-Features in der Regel Pflicht.
2. Wenn KI-generierte Performance-Zusammenfassungen Beförderungs- oder Kündigungsentscheidungen beeinflussen, muss ein Human-in-the-Loop sichergestellt sein (Art. 22 DSGVO).
3. Ab August 2026 gelten die vollen Hochrisiko-Pflichten des AI Acts – inklusive Logging, menschlicher Aufsicht und Registrierung.

CRM-Systeme mit KI betreffen nicht nur interne Daten – sie betreffen Ihre Kunden direkt. HubSpot, Salesforce und ähnliche CRM-Plattformen nutzen KI, die auf den gesamten Kundendatenbestand zugreift. Zwei Punkte werden regelmäßig übersehen:

1. Wenn KI E-Mails an Kunden generiert oder Chatbots Kundenanfragen beantworten, greift die Kennzeichnungspflicht nach Art. 50 EU AI Act – der Kunde muss wissen, dass KI im Spiel ist.
2. Viele CRM-Anbieter nutzen für ihre generativen KI-Features externe LLM-Anbieter als Sub-Processors (z.B. HubSpot → OpenAI). Prüfen Sie im AVV, ob diese Kette erfasst ist.

Wichtige Regel: KI-Feature ≠ Tool genehmigt. Die Genehmigung des Basistools (z.B. Notion, Slack) gilt nicht automatisch für das KI-Feature. Jedes KI-Feature ist separat zu prüfen und freizugeben. In der Whitelist (Anhang B) müssen Tool und

KI-Feature als getrennte Einträge geführt werden.

6.6 Entscheidungsmatrix: Welche Lösung für welches Unternehmen?

Unternehmensprofil	Empfohlene Lösung	Begründung	Mindestbedingung
KMU, bereits M365-Nutzer, pragmatischer Ansatz	*M365 Copilot Business* (~$21 Add-on)	Stärkste EU-Datenschutzzusage eines US-Anbieters, nahtlose Integration, keine neue Software nötig	Berechtigungskonzept prüfen, AVV im MS-Vertrag aktivieren
KMU ohne M365, will einfachen ChatGPT-Ersatz	*ChatGPT Business oder Claude Team* (~$25/User)	Schnell einführbar, AVV vorhanden, Zero Data Retention, vertraute Oberfläche	Business-Tarif buchen (kein privater Account), AVV abschließen
Unternehmen will bewusst keinen US-Anbieter	*Mistral Le Chat Team* ($25/User)	Französisches Unternehmen, EU-Server, kein CLOUD Act, gutes Preis-Leistungs-Verhältnis	AVV vor PII-Nutzung abschließen
Hochsensible Daten (Anwalt, Medizin, Behörde)	*Aleph Alpha oder Open Source EU-Cloud*	Keine US-Verbindung, volle Datensouveränität, BSI-Option bei Aleph Alpha	IT-Ressourcen für Betrieb einplanen
Maximale Kontrolle, IT-Ressourcen vorhanden	*On-Premises* (Llama 3, Mistral Open)	Kein Datenabfluss, kein AVV nötig, volle Kontrolle	GPU-Hardware + IT-Betrieb, kein SaaS-Komfort

Wichtigste Erkenntnis: Jeder der genannten Business-/Enterprise-Tarife ist rechtlich nutzbar – sofern der AVV abgeschlossen ist und kein privater Account verwendet wird. Der Unterschied liegt im Risikoprofil (CLOUD Act) und im Aufwand. Für die meisten deutschen KMU ist M365 Copilot oder ChatGPT Business der pragmatische Einstieg.

6.7 Berater & Dienstleister: Haftung und Vertragspflichten im Detail

Die Frage der Haftung bei externen Dienstleistern ist komplex und wird von vielen Unternehmen unterschätzt.

Wer haftet, wenn der Berater ChatGPT Pro nutzt? Das beauftragende Unternehmen – nicht der Berater persönlich. Der Berater ist Auftragsverarbeiter nach Art. 28 DSGVO. Das Unternehmen ist und bleibt Verantwortlicher und muss sicherstellen, dass der Berater geeignete technische und organisatorische Maßnahmen einsetzt.

Was muss das Unternehmen vertraglich regeln? Jeder externe Dienstleister, der mit Unternehmensdaten arbeitet, braucht einen AVV nach Art. 28 DSGVO. Der AVV mit dem Berater muss mindestens regeln: welche KI-Tools er einsetzen darf (Verweis auf die Whitelist), dass private oder kostenlose KI-Accounts für Auftragsdaten ausdrücklich verboten sind, dass er Datenpannen (auch durch KI-Tools) unverzüglich meldet, und dass Unterauftragnehmer denselben Pflichten unterliegen.

Was sollte der Berater konkret nutzen? Option A (empfohlen): Der Berater bucht selbst ChatGPT Business oder Claude Team auf seinem eigenen Unternehmenskonto – dann hat er selbst einen AVV mit dem Anbieter. Option B: Das beauftragende Unternehmen stellt dem Berater Zugang zu seinem eigenen genehmigten Tool-Stack bereit (z.B. einen Gast-Account im eigenen ChatGPT Business) – dann gelten die bestehenden AVV und Richtlinien des Unternehmens automatisch.

Praxisfall (Deutschland): Falscher Tarif, richtiger Anbieter

Ausgangslage: Ein Handelsunternehmen entscheidet sich "für ChatGPT", lässt aber Mitarbeitern die Wahl zwischen privaten Plus-Accounts und Business-Zugang.

Fehler: Das Unternehmen steuerte den Tarif nicht zentral und konnte nicht

nachweisen, welche Daten über welche Vertragsbasis verarbeitet wurden.

Folge: Nach einer Beschwerde musste die Nutzung vollständig neu aufgesetzt werden: zentrale Beschaffung, zentrale Konten, neue Whitelist, erneute Mitarbeiterschulung.

Lernpunkt: Nicht der Anbietername entscheidet, sondern der gebuchte Tarif und die vertragliche Kette.

Executive Summary: Was diese Woche zu tun ist

1. Nur zentral beschaffte KI-Tarife erlauben; private Accounts konsequent ausschließen.
2. Für jedes freigegebene Tool Tarif, AVV, Datenregion und Sub-Processor dokumentieren.
3. HR- und CRM-KI-Features als Sonderfall mit zusätzlicher Prüfung behandeln.
4. Beraterverträge um verbindliche KI-Klauseln erweitern.

Kapitel 7: Der Sonderfall: Autonome KI-Agenten (OpenClaw & Co.)

Während Chatbots wie ChatGPT auf eine Eingabe (Prompt) warten, markieren autonome KI-Agenten eine völlig neue Risikoklasse. Sie agieren selbstständig, dauerhaft und oft unsichtbar im Hintergrund.

7.1 Was sind autonome KI-Agenten?

Ein prominentes Beispiel für diese neue Kategorie sind Open-Source-Projekte wie *OpenClaw* (oder ähnliche Frameworks wie AutoGPT, BabyAGI). Diese Tools erlangten schnell Bekanntheit als vielgenutzte Open-Source-KI-Projekte. Sie laufen lokal auf dem Rechner des Nutzers, verbinden sich mit Messaging-Apps (WhatsApp, Telegram, Slack, iMessage, Signal u.a.) und führen eigenständig Aufgaben aus – ohne dass jemand aktiv etwas eintippen muss.

Der entscheidende technische Unterschied zu allen anderen KI-Tools: OpenClaw hat einen sogenannten *Heartbeat* – einen internen Takt, der das System regelmäßig aufweckt, um eigenständig Aufgaben zu erledigen, Daten zu analysieren und Aktionen auszuführen. Es schläft nicht. Es wartet nicht. Es agiert.

7.2 OpenClaw vs. ChatGPT: Ein grundlegender Unterschied

Merkmal	ChatGPT Business / Copilot	OpenClaw (autonomer Agent)
Nutzung	Aktiv: Nutzer gibt Prompt ein, erhält Antwort	Passiv + Aktiv: Läuft dauerhaft, agiert auch ohne Prompt
Datenzugriff	Nur was eingegeben wird	Alle verbundenen Systeme: E-Mail, Dateien, Slack, Kalender, Code

Merkmal	ChatGPT Business / Copilot	OpenClaw (autonomer Agent)
Aktivität	Nur auf Anfrage	Heartbeat: regelmäßige eigenständige Aktionen auch nachts/am Wochenende
Lokale Installation	SaaS – läuft in der Cloud des Anbieters	Läuft auf dem Rechner des Nutzers – lokaler Vollzugriff
Erweiterbarkeit	Definierter Funktionsumfang	100+ AgentSkills – jeder Skill ist ausführbarer Code von Dritten
Governance-Sichtbarkeit	Klar abgegrenzte Tool-Nutzung	Dauerhafter, unsichtbarer Hintergrundprozess – schwer zu erkennen
AVV / Datenschutz	Business-Tarif mit AVV verfügbar	Open Source – kein Anbieter, kein AVV, keine Datenschutzgarantie

7.3 Das Berater-Szenario: Die unterschätzte Gefahr

Der häufigste Fall ist der eigene Mitarbeiter: OpenClaw auf dem Firmenrechner installiert, verbunden mit Unternehmens-Slack, Firmen-E-Mail, GitHub, Jira – aus echtem Produktivitätsinteresse, nicht aus böser Absicht. Der Mitarbeiter denkt, er optimiert seinen Workflow. Das Unternehmen weiß nichts davon.

Daneben gibt es einen zweiten, oft übersehenen Fall: externe Berater und Entwickler, die OpenClaw auf ihrem eigenen Laptop haben und diesen mit Kundensystemen verbinden. Hier verliert das Unternehmen zusätzlich die technische Kontrolle über das Gerät selbst.

Szenario	Was passiert	Rechtliches Risiko
Mitarbeiter installiert OpenClaw auf dem Firmenrechner – verbunden mit Unternehmens-Slack und Firmen-E-Mail	OpenClaw läuft dauerhaft im Hintergrund, liest alle Slack-Kanäle und E-Mails des Mitarbeiters – inkl. Kundenkommunikation, HR-Themen, interne Strategie. Auch nachts, auch am Wochenende.	□ DSGVO Art. 28 – kein AVV für autonome Verarbeitung. Art. 5 – Kontrollverlust über eigene Systeme. Das Unternehmen haftet als Verantwortlicher.
Mitarbeiter verbindet OpenClaw im Homeoffice über sein privates Gerät mit Firmen-GitHub und Jira	Quellcode, alle Issues, Kundenprojekte liegen dauerhaft auf einem privaten Gerät, das das Unternehmen weder kontrolliert noch sichern kann. OpenClaw kann bei entsprechenden Skills auch Änderungen vornehmen.	□ DSGVO + GeschGehG – Quellcode ist Geschäftsgeheimnis. Privates Gerät = außerhalb jeder BYOD-Kontrolle. Bei Datenpanne: 72h-Meldepflicht.
Berater hat OpenClaw mit Zugang zum Kunden-Slack verbunden	OpenClaw liest alle Kanäle, auf die der Berater Zugriff hat: interne Strategiediskussionen, HR-Kanäle, Kundenprojekte, technische Details. Alles wird lokal auf dem Berater-Laptop gespeichert und verarbeitet.	□ DSGVO Art. 28 – Sub-Auftragsverarbeitung ohne Genehmigung. Das Unternehmen haftet als Verantwortlicher auch für eigenständiges Handeln des Beraters.
Entwickler-Freelancer verbindet OpenClaw mit Kunden-GitHub und Kunden-Jira	OpenClaw hat dauerhaften Lesezugriff auf alle Repositories, alle Issues, alle Kommentare. Kann bei entsprechenden Skills auch Änderungen vornehmen. Quellcode, Kundendaten in Testdaten, Sicherheitslücken – alles liegt auf einem privaten Laptop.	□ DSGVO + GeschGehG + IT-Sicherheit – Kein AVV für die autonome Verarbeitung. Bei Datenpanne: Meldepflicht innerhalb 72h.
Mitarbeiter oder Berater nutzt KI-Agenten-Skills aus Drittanbieter-Repositories – darunter ein kompromittierter Skill	Viele dieser Agenten lassen sich durch Plugins oder "Skills" von Dritten erweitern. Da diese oft ungeprüft aus der Community stammen, ist das Risiko von Schwachstellen oder bösartigem Code hoch. Ein kompromittierter Skill auf einem Gerät mit Zugang zu Unternehmenssystemen = direkter Angriffspfad.	□ IT-Sicherheit + DSGVO – Datenpanne durch Drittsoftware. Das Unternehmen muss angemessene technische und organisatorische Maßnahmen nachweisen (Art. 32 DSGVO).

7.4 Sofortmaßnahmen: Schutz vor unkontrollierten KI-Agenten

#	Maßnahme	Priorität
1	*Beraterverträge um KI-Agenten-Klausel ergänzen:* Explizites Verbot von autonomen KI-Agenten (OpenClaw, ähnliche Tools) auf Geräten, die auf Unternehmenssysteme zugreifen. Verstoß als außerordentlichen Kündigungsgrund definieren.	**Sofort**
2	*API-Token und Zugangsdaten mit minimalem Scope vergeben:* Externe Berater erhalten nur die Berechtigungen, die für ihre konkrete Aufgabe nötig sind. Was nicht zugänglich ist, kann nicht abfließen.	**Sofort**
3	*OAuth-Verbindungen und API-Token regelmäßig prüfen und rotieren:* Wer hat welchen Zugang zu Unternehmens-Slack, GitHub, Jira? Liste aller aktiven OAuth-Apps in der Admin-Konsole prüfen. OpenClaw-Verbindungen sind als OAuth-Apps in den Systemeinstellungen sichtbar.	Kurzfristig
4	*BYOD-Richtlinie um KI-Agenten-Verbot erweitern:* Wenn Mitarbeiter oder Berater eigene Geräte nutzen, muss die BYOD-Richtlinie explizit autonome KI-Agenten verbieten.	Kurzfristig
5	*Mitarbeiter und Berater aktiv informieren:* Nicht nur verbieten – erklären, warum OpenClaw ein anderes Risiko ist als ChatGPT. Viele Nutzer installieren es aus echtem Produktivitätsinteresse ohne die Konsequenzen zu kennen.	Mittelfristig
6	*Incident-Response-Prozess für KI-Agenten-Vorfälle definieren:* Was passiert, wenn bekannt wird, dass ein Berater OpenClaw mit Kundensystemen verbunden hatte? Wer entscheidet, ob eine DSGVO-Meldepflicht (72h, Art. 33) ausgelöst wurde?	Mittelfristig

OpenClaw ist heute das bekannteste Beispiel – aber nicht das letzte. Autonome KI-Agenten sind 2026 die am schnellsten wachsende Softwarekategorie. Jede Governance-Struktur muss heute schon regeln, wie mit dieser Kategorie umgegangen wird – nicht erst wenn der nächste Vorfall passiert ist.

Praxisfall (Deutschland): Agent auf Berater-Laptop

Ausgangslage: Ein externer Entwickler verbindet einen autonomen Agenten mit Kunden-Jira und Slack, um schneller Tickets zusammenzufassen.

Fehler: Kein Vertragsverbot für autonome Agenten, keine Prüfung von OAuth-Apps, keine klare BYOD-Grenze für Kundensysteme.

Folge: Nach Sicherheitsalarm mussten Tokens rotiert, Zugänge neu vergeben und ein Incident-Prozess rückwirkend aufgebaut werden.

Lernpunkt: Der kritische Moment ist die erste OAuth-Freigabe, nicht erst der eigentliche Vorfall.

Executive Summary: Was diese Woche zu tun ist

1. Autonome KI-Agenten in BYOD- und Dienstleisterregeln explizit verbieten.
2. Alle aktiven OAuth-Apps und API-Tokens in Slack/GitHub/Jira prüfen.
3. Minimalrechte für externe Zugänge technisch durchsetzen.
4. Incident-Ablauf für Agentenfälle inkl. DSGVO-72h-Entscheidung definieren.

Kapitel 8: Praxis-Guide: Governance im Unternehmen einführen

Wie bringen Sie all diese Anforderungen nun auf die Straße? Für ein kleines Unternehmen reicht ein einziger Nachmittag, um die rechtliche Mindestgrundlage zu schaffen. Die folgenden vier Schritte decken alles ab, was rechtlich nötig ist.

8.1 Was muss unterschrieben werden – und was nicht?

Bevor wir in die Schritte einsteigen, klären wir die häufigste Frage: Was muss tatsächlich unterschrieben werden?

Dokument	Unterschrift nötig?	Von wem?	Warum?
Anhang A: KI-Nutzungsrichtlinie	Ja – zwingend	Jeder Mitarbeiter einzeln	Ohne Unterschrift kein Nachweis, dass der Mitarbeiter die Verbote kannte. Ohne diesen Nachweis ist der GF bei Verstößen schutzlos.
Anhang B: Whitelist genehmigter Tools	Nein – nicht nötig	Entfällt	Die Whitelist ist ein internes Steuerungsdokument. Entscheidend ist, dass sie nachweisbar bekannt gemacht wurde – z.B. per E-Mail oder in der Schulung.
Anhang C: Schulungsdokumentation	Ja – zwingend	Jeder Teilnehmer + GF zur Abzeichnung	Die Teilnehmerliste mit Unterschriften ist der zentrale Nachweis der Aufsichtspflichterfüllung. Dieses Dokument schützt die GF gegenüber Behörden und im Schadensfall.

8.2 Schritt-für-Schritt-Rollout

Schritt 1: Richtlinie & Whitelist finalisieren

Passen Sie Anhang A und B an Ihr Unternehmen an: Firmennamen eintragen, konkrete Tools eintragen, Ansprechpartner benennen. Lassen Sie die Richtlinie vom Datenschutzbeauftragten (intern oder extern) prüfen. Das Ergebnis sind unterschriftsreife Dokumente.

Schritt 2: Schulung durchführen (30–60 Minuten)

Rufen Sie alle Mitarbeiter zusammen – physisch oder per Videocall. Gehen Sie folgende Inhalte durch: Was ist DSGVO, welche Tools sind erlaubt, was darf niemals eingegeben werden, was passiert bei Verstößen. Zeigen und erklären Sie die Whitelist. Das Ergebnis ist ein gemeinsames Verständnis bei allen Mitarbeitern.

Schritt 3: Unterschriften einholen

Legen Sie Anhang C aus: Jeder Teilnehmer trägt Name und Datum ein und unterschreibt. Die Geschäftsführung zeichnet das Dokument am Ende ab. Das Ergebnis ist eine unterschriebene Teilnehmerliste (Anhang C).

Schritt 4: Dokumente ablegen & Whitelist kommunizieren

Legen Sie Anhang C in die Personalakte jedes Mitarbeiters (physisch oder digital). Kommunizieren Sie Anhang B im Intranet, in einem geteilten Ordner oder per E-Mail – mit dem Hinweis, dass das die offizielle genehmigte Liste ist. Das Ergebnis ist der Nachweis der Aufsichtspflichterfüllung – die Geschäftsführung ist geschützt.

8.3 Umgang mit neuen Mitarbeitern

Die Richtlinie und Schulung werden Teil des Onboardings. Neue Mitarbeiter erhalten Anhang A beim ersten Arbeitstag, unterschreiben direkt und nehmen

an einer kurzen Einführung teil. Anhang C wird um eine neue Zeile ergänzt oder als separates Einzel-Dokument angelegt. Empfehlung: Onboarding-Checkliste um den Punkt "KI-Richtlinie unterschrieben" ergänzen.

8.4 Umgang mit Änderungen der Whitelist

Wird ein Tool neu aufgenommen oder gesperrt, reicht eine nachweisbare Kommunikation: E-Mail an alle Mitarbeiter mit der aktualisierten Liste, Versionsnummer und Datum. Diese E-Mail aufbewahren – sie ist der Nachweis, dass die Änderung bekannt gemacht wurde. Eine neue Unterschrift ist nur nötig, wenn sich grundlegende Verbote in Anhang A ändern.

8.5 Dokumentation und Nachweisbarkeit

Erinnern Sie sich an die persönliche Haftung der Geschäftsführung? Ihr einziger Schutzschild ist die Dokumentation. Bewahren Sie die unterschriebenen Schulungslisten (Anhang C) mindestens drei Jahre auf – auch nach Ausscheiden des Mitarbeiters. Aktualisieren Sie Ihr Verarbeitungsverzeichnis (VVT) um die neuen KI-Systeme. Dokumentieren Sie die Risikoeinstufung nach dem EU AI Act für jedes eingesetzte System. Wenn die Aufsichtsbehörde anklopft, haben Sie die Nachweise griffbereit.

Praxisfall (Deutschland): 14-Tage-Rollout in einem Dienstleistungs-KMU

Ausgangslage: Ein Beratungsunternehmen mit 85 Mitarbeitern wollte KI-Nutzung nicht verbieten, sondern kontrolliert erlauben.

Vorgehen: In zwei Wochen wurden Richtlinie (Anhang A), Whitelist (Anhang B), Schulung und unterschriebene Teilnehmerliste (Anhang C) umgesetzt.

Ergebnis: Das Unternehmen konnte gegenüber einem Großkunden im Vendor-Assessment innerhalb eines Tages vollständige KI-Governance-Nachweise

liefern.

Lernpunkt: Für die erste rechtssichere Basis braucht es vor allem Entscheidungen und Disziplin, nicht ein Großprojekt.

Executive Summary: Was diese Woche zu tun ist

1. Zentrales Inventar einführen: alle KI-Tools, alle KI-Features in Bestandssoftware und alle Berater mit KI-Nutzung.
2. Richtlinie (A), Whitelist (B) und Schulungsdokumentation © als verbindliches Paket einführen.
3. Eine Erstschulung für alle Mitarbeiter terminieren und unterschrieben dokumentieren.
4. Onboarding- und Offboarding-Prozesse um KI-Pflichten ergänzen.
5. Nachweisablage zentral aufsetzen, damit Prüfunterlagen jederzeit abrufbar sind.

Anhänge: Templates & Muster

Die folgenden Muster dienen als Startpunkt für Ihre interne Governance. Bitte passen Sie diese an Ihre spezifischen Unternehmensbedürfnisse an und lassen Sie sie rechtlich prüfen.

Anhang A: Muster KI-Nutzungsrichtlinie

Dokumentenname	KI-Nutzungsrichtlinie
Version	1.0
Gültig ab	
Verantwortlich	Geschäftsführung
Gilt für	Alle Mitarbeiterinnen und Mitarbeiter des Unternehmens
Nächste Überprüfung	(empfohlen: jährlich)

1. Zweck dieser Richtlinie

Der Einsatz von KI-Tools am Arbeitsplatz bietet erhebliche Produktivitätsvorteile, birgt aber gleichzeitig rechtliche Risiken: Datenschutzverstöße nach DSGVO, Verletzung von Geschäftsgeheimnissen und strafrechtliche Risiken bei unsachgemäßer Nutzung. Diese Richtlinie legt fest, wie KI-Tools im Unternehmen erlaubt genutzt werden dürfen, welche Eingaben verboten sind und wer bei Fragen verantwortlich ist.

2. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiterinnen und Mitarbeiter, Praktikanten, Freelancer und externe Dienstleister, die im Auftrag des Unternehmens tätig sind. Sie gilt für jede berufliche Nutzung von KI-Tools – unabhängig davon, ob auf Unternehmensgeräten oder privaten Geräten.

3. Erlaubte KI-Tools

Ausschließlich die in Anhang B (Whitelist) aufgeführten Tools dürfen für berufliche Zwecke genutzt werden. Alle anderen KI-Dienste – auch kostenlose oder bereits privat genutzte – sind für berufliche Zwecke nicht erlaubt. Die aktuelle Whitelist ist unter [Ablageort / Intranet-Link] verfügbar.

4. Was niemals eingegeben werden darf (Public-Tools vs. Enterprise-Tools)

Die Eingabe von Daten hängt vom verwendeten Tool ab. Wir unterscheiden zwischen *Public-Tools* (z.B. kostenloses ChatGPT, private Accounts) und *Enterprise-Tools* (vom Unternehmen bereitgestellte Accounts mit AVV und Zero Data Retention, siehe Whitelist).

In Public-Tools absolut verboten:

Verbotene Kategorie	Beispiele	Warum verboten
Personenbezogene Daten von Kunden oder Mitarbeitern	Namen, E-Mails, Adressen, Vertragsnummern, Gesundheitsdaten, Gehalt	DSGVO-Verstoß – kein AVV auf privatem Account

In ALLEN Tools (auch Enterprise) absolut verboten:

Verbotene Kategorie	Beispiele	Warum verboten
Zugangsdaten & Secrets	Passwörter, API-Keys, Connection Strings, SSH-Keys	Sicherheitsrisiko – Kompromittierung ganzer Systeme möglich
Vertrauliche Geschäftsinformationen	Preisstrategie, Margen, interne Budgets, M&A-Informationen, Strategiepapiere	GeschGehG – Verlust des Geheimnisschutzes
NDA-geschützte Kundeninformationen	Architekturdetails, Projektinformationen unter Vertraulichkeitsvereinbarung	Vertragsbruch – direkte Haftung gegenüber Kunden
Vollständige Meeting-Aufzeichnungen ohne Einwilligung	Transkripte, Zusammenfassungen von Gesprächen mit externen Personen	DSGVO + § 201 StGB (Strafrecht)
Echte Produktionsdaten als Testdaten	Echter Datenbankinhalt, API-Responses mit Kundendaten	DSGVO – Datenpanne, Meldepflicht

5. KI-Meeting-Recorder – Sonderregeln

Tools, die Meetings automatisch aufzeichnen oder transkribieren (z.B. Fathom, Fireflies, Otter.ai, tl;dv, Microsoft Copilot in Teams), unterliegen besonderen Regeln, da sie Dritte ohne deren aktives Zutun erfassen:

Vor jeder Aufzeichnung müssen alle Teilnehmer aktiv und nachweisbar einwilligen – eine mündliche Ansage allein reicht nicht. Bei externen Teilnehmern (Kunden, Bewerber, Lieferanten) ist die Einwilligung schriftlich oder per Klick einzuholen, bevor das Meeting beginnt. Bei internen Meetings mit HR-Bezug (Abmahnungen, Gespräche über Krankheit, Gehalt) ist die Aufzeichnung grundsätzlich verboten ohne ausdrückliche Zustimmung aller Beteiligten und Betriebsratsbeteiligung. Heimliche Aufzeichnung ist eine Straftat nach § 201 StGB – betrifft den aufzeichnenden Mitarbeiter persönlich.

6. Pflichten der Mitarbeiter

Mitarbeiter sind verpflichtet, ausschließlich genehmigte Tools aus der Whitelist zu verwenden, verbotene Inhalte niemals in KI-Tools einzugeben – auch nicht "kurz mal schnell" –, verdächtige Vorfälle (z.B. versehentliche Eingabe von Kundendaten) sofort dem Datenschutzbeauftragten zu melden, und KI-generierte Inhalte vor Verwendung zu prüfen. Die Verantwortung für das Ergebnis liegt beim Mitarbeiter.

7. Konsequenzen bei Verstößen

Verstöße gegen diese Richtlinie können abhängig von Schwere und Auswirkung folgende Konsequenzen haben: Abmahnung, fristlose Kündigung, persönliche zivilrechtliche Haftung gegenüber dem Unternehmen oder betroffenen Personen sowie im Fall von § 201 StGB ein Ermittlungsverfahren.

8. Ansprechpartner

Thema	Zuständig	Kontakt
Datenschutzfragen / Meldung von Vorfällen	Datenschutzbeauftragter (DSB)	
Tool-Freigaben / Whitelist-Änderungen	IT / [Verantwortliche Person]	
Allgemeine Fragen zur Richtlinie	Geschäftsführung	

9. Unterschrift & Kenntnisnahme

Ich habe die KI-Nutzungsrichtlinie gelesen, verstanden und verpflichte mich zur Einhaltung.

(Unterschrift wird im Rahmen der Schulungsdokumentation erfasst – siehe Anhang C)

Anhang B: Muster Whitelist genehmigter KI-Tools

Nur die hier aufgeführten Tools sind für berufliche Zwecke freigegeben. Alle anderen sind gesperrt – auch wenn sie privat bekannt oder kostenlos verfügbar sind.

Stand: | Verantwortlich: | Nächste Prüfung:

Tool / Anbieter	Tarif / Version & AVV	Erlaubte Zwecke	Verbotene Zwecke
ChatGPT (OpenAI)	Team / Enterprise. AVV: Ja (im Vertrag enthalten)	Texte, Zusammenfassungen, interne Recherche, Brainstorming	Keine Kundendaten, keine Passwörter, kein NDA-Inhalt

Tool / Anbieter	Tarif / Version & AVV	Erlaubte Zwecke	Verbotene Zwecke
Claude (Anthropic)	Team / Enterprise. AVV: Ja (im Vertrag enthalten)	Texte, Analysen, Code-Unterstützung (ohne Produktivdaten)	Keine Kundendaten, keine Secrets
Microsoft 365 Copilot	M365 Business/Enterprise. AVV: Ja (MS-Vertrag)	Office-Dokumente, Teams-Zusammenfassungen (nur interne Meetings mit Einwilligung)	Keine externen Meeting-Aufzeichnungen ohne Einwilligung
GitHub Copilot	Business / Enterprise. AVV: Ja (Business-Vertrag)	Code-Unterstützung, Dokumentation – nur ohne Produktivdaten	Keine echten Kundendaten, keine Secrets, kein NDA-Code
Personio	Core / Professional / Enterprise. AVV: Ja (prüfen: KI-Sub-Processors erfasst?)	Personalverwaltung, Abwesenheiten, Dokumentenmanagement	KI-Performance-Summaries nur mit DSFA und Human-in-the-Loop. Kein automatisiertes Bewerber-Scoring ohne menschliche Prüfung.
HubSpot	Professional / Enterprise. AVV: Ja (DPA prüfen: KI-Sub-Processors erfasst?)	CRM, E-Mail-Marketing, Sales-Pipeline – KI-Features nur nach DSGVO-Prüfung	Kein automatisiertes Lead-Scoring ohne Human-in-the-Loop. Keine KI-generierten Kunden-E-Mails ohne Kennzeichnung.

Tool / Anbieter	Tarif / Version & AVV	Erlaubte Zwecke	Verbotene Zwecke
Salesforce	Enterprise / Unlimited. AVV: Ja (DPA + Einstein-Addendum prüfen)	CRM, Service Cloud – Einstein-Features nur nach DSGVO-Prüfung	Kein Einstein GPT für automatisierte Kundenentscheidungen ohne Aufsicht. Sub-Processor-Kette (OpenAI) prüfen.
[Tool eintragen]	[Tarif]. AVV: [ ] Ausstehend	[Zweck eintragen]	[Verbote eintragen]

Hinweis zur AVV-Pflicht: Kein Tool darf für die Verarbeitung personenbezogener Daten genutzt werden, bevor ein Auftragsverarbeitungsvertrag (AVV) abgeschlossen ist. Tools mit ausstehendem AVV sind bis zur Klärung ausschließlich für anonymisierte, nicht-personenbezogene Inhalte freigegeben.

Anhang C: Muster Schulungsdokumentation KI-Nutzung

Diese Dokumentation dient als Nachweis, dass Mitarbeiter über die KI-Nutzungsrichtlinie informiert und geschult wurden. Sie schützt die Geschäftsführung bei Pflichtverletzungen durch Mitarbeiter.

Schulungsthema	KI-Nutzung im Unternehmen – Rechtliche Grundlagen & Richtlinie
Schulungsform	[ ] Präsenzschulung [ ] Online / E-Learning (mit Wissenstest) [ ] Einzelgespräch
Datum der Schulung	
Dauer	(empfohlen: min. 30 Minuten)
Durchgeführt von	(Name, Funktion)

Besprochene Inhalte	DSGVO-Grundlagen beim KI-Einsatz, verbotene Eingaben, Whitelist genehmigter Tools, Meldepflichten, Meeting-Recorder-Sonderregeln, Konsequenzen bei Verstößen
Verwendete Unterlagen	KI-Nutzungsrichtlinie v_ | *Whitelist genehmigter Tools v_*
Nächste Wiederholung	(empfohlen: jährlich oder bei wesentlicher Änderung)

Teilnehmerliste & Bestätigung

Jede teilnehmende Person bestätigt mit ihrer Unterschrift: Ich habe an der Schulung zur KI-Nutzungsrichtlinie teilgenommen, die Inhalte verstanden und die aktuelle Richtlinie sowie Whitelist erhalten.

#	Name (Druckbuchstaben)	Abteilung / Funktion	Datum	Unterschrift	Richtlinie erhalten?
1					[ ] Ja
2					[ ] Ja
3					[ ] Ja
4					[ ] Ja
5					[ ] Ja
6					[ ] Ja
7					[ ] Ja
8					[ ] Ja
9					[ ] Ja
10					[ ] Ja

Abzeichnung durch die Geschäftsführung:

Name (Geschäftsführung)	Datum & Unterschrift

Hinweis zur Aufbewahrung: Dieses Dokument ist mindestens 3 Jahre aufzubewahren – auch nach Ausscheiden des Mitarbeiters. Es dient als Nachweis der Aufsichtspflichterfüllung gegenüber Datenschutzbehörden und im Rahmen von DSGVO-Prüfungen. Empfohlener Ablageort: Personalakte (physisch oder digital verschlüsselt).

Anhang D: Sonderfall – OpenClaw & autonome KI-Agenten

Dieser Anhang richtet sich an Unternehmen, die externe Berater, Entwickler oder Freelancer einsetzen – sowie an IT- und Datenschutzverantwortliche, die verstehen wollen, warum autonome KI-Agenten eine eigene Risikokategorie bilden.

OpenClaw ist kein Chatbot. Es ist ein dauerhaft laufender autonomer Agent mit Vollzugriff auf alle verbundenen Systeme – rund um die Uhr, auch ohne aktive Nutzerinteraktion.

Muster-Klausel für Beraterverträge:

Der Auftragnehmer verpflichtet sich, bei der Erbringung der vertragsgegenständlichen Leistungen ausschließlich die vom Auftraggeber genehmigten KI-Tools (gemäß aktueller Whitelist des Auftraggebers) zu verwenden. Der Einsatz von autonomen KI-Agenten (insbesondere, aber nicht beschränkt auf OpenClaw, ähnliche dauerhaft laufende Agenten-Systeme) auf Geräten, die Zugriff auf Systeme, Daten oder Kommunikationskanäle des Auftraggebers haben, ist ausdrücklich untersagt. Ein Verstoß gegen diese Verpflichtung berechtigt den Auftraggeber zur außerordentlichen Kündigung des Vertrages und begründet Schadensersatzansprüche.

Technische Schutzmaßnahmen – Checkliste:

Maßnahme	Erledigt?
Beraterverträge um KI-Agenten-Klausel ergänzt	[ ]
API-Token und Zugangsdaten mit minimalem Scope vergeben (Least Privilege)	[ ]
OAuth-Verbindungen in Admin-Konsolen aller Systeme (Slack, GitHub, Jira) geprüft	[ ]
BYOD-Richtlinie um KI-Agenten-Verbot erweitert	[ ]
Mitarbeiter und Berater über OpenClaw-Risiken informiert	[ ]
Incident-Response-Prozess für KI-Agenten-Vorfälle definiert	[ ]
Regelmäßige Rotation von API-Tokens und OAuth-Zugängen eingeführt	[ ]

Referenzen

[1] Europäische Kommission. "AI Act Implementation Timeline." Artificial Intelligence Act EU. https://artificialintelligenceact.eu/implementation-timeline/

[2] Bundesministerium des Innern und für Heimat (BMI). "Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG)." Bundesgesetzblatt, Dezember 2025.

[3] Europäisches Parlament. "Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates (EU AI Act)." Amtsblatt der Europäischen Union, 12. Juli 2024. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32024R1689

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI). "BSI-Gesetz (BSIG) – Neufassung 2025." https://www.bsi.bund.de

[5] Datenschutz-Grundverordnung (DSGVO). "Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates." https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679