AGENT AI
INSTITUT FÜR DIGITALE KOMPETENZ

KOSTENLOSER SELBSTTEST · STAND OKTOBER 2026

Der AI-Act-Check für dein Unternehmen

90 Pflichtpunkte, die seit 2025 und 2026 für jedes Unternehmen gelten, das KI nutzt. Auch für dich, auch wenn „nur" ein Mitarbeiter KI verwendet: ChatGPT, Copilot, ein Chatbot, ein Übersetzer, ein Bildtool oder die KI-Funktion in eurer Software. Plus: 22 echte Fälle aus Europa und der Welt, in denen Unternehmen für KI-Fehler bezahlt haben.

90
Pflichtpunkte in 11 Bereichen

22
echte Strafen & Schadensfälle mit Quelle

bis 7 %
des weltweiten Jahresumsatzes als Höchststrafe

WARUM DU DAS JETZT LESEN MUSST

Der EU AI Act gilt nicht nur für Konzerne. Er gilt für jeden Betrieb, der KI nutzt.

Sobald in deinem Unternehmen jemand **in irgendeiner Form KI** nutzt, egal ob ChatGPT, Copilot, Gemini, einen Chatbot, ein KI-Telefon, ein Bild- oder Übersetzungstool oder eine KI-Funktion in eurer Buchhaltung, eurem CRM oder Office-Paket, bist du rechtlich ein **„Betreiber"** von KI. Und damit hast du Pflichten. Viele davon gelten bereits.

SEIT	WAS GILT	WEN BETRIFFT ES
2. Feb. 2025	Verbot bestimmter KI-Praktiken (Art. 5) und Pflicht zur KI-Kompetenz aller Mitarbeiter, die KI nutzen (Art. 4)	Jedes Unternehmen, das KI einsetzt
2. Aug. 2025	Bußgeldrahmen des AI Act anwendbar, Pflichten für Anbieter von KI-Basismodellen	Alle
2. Aug. 2026	Transparenz- und Kennzeichnungspflichten (Art. 50): Chatbots, Voicebots, Deepfakes, KI-Inhalte. **Vom Digital Omnibus nicht verschoben.**	Jeder Betrieb mit Chatbot, KI-Telefon, KI-Bildern oder KI-Videos
2. Dez. 2026	Technische Markierung KI-erzeugter Inhalte auch für Bestandssysteme	Anbieter von KI-Systemen
2. Dez. 2027	Pflichten für Hochrisiko-KI (Anhang III): z. B. KI im Recruiting, bei Leistungsbewertung, Kreditwürdigkeit	Jeder Betrieb mit KI im HR- oder Finanzbereich

WAS EIN VERSTOSS KOSTEN KANN (ART. 99)

VERSTOSS	HÖCHSTSTRAFE
Verbotene KI-Praktiken	**35 Mio. € oder 7 % des Umsatzes**
Transparenzpflichten, Betreiberpflichten u. a.	**15 Mio. € oder 3 % des Umsatzes**
Falsche oder unvollständige Angaben gegenüber Behörden	**7,5 Mio. € oder 1 % des Umsatzes**
Daneben: Verstöße gegen die DSGVO bei KI-Nutzung	**20 Mio. € oder 4 % des Umsatzes**
Schadenersatz an jede betroffene Person (Art. 82 DSGVO). Laut EuGH gibt es keine Bagatellgrenze (C-300/21, Österreichische Post)	**pro Person, zusätzlich**
Persönliche Haftung der Geschäftsführung für Organisationsmängel (§ 25 GmbHG AT, § 43 GmbHG DE)	**mit Privatvermögen**
Abmahnungen von Mitbewerbern und Verbraucherschützern (UWG), Unterlassungsklagen	**Kosten + Vertragsstrafe**

> Für KMU gilt beim AI Act jeweils der **niedrigere** der beiden Werte. Bei 2 Mio. € Umsatz sind das bis zu **60.000 € pro Verstoß** gegen die Transparenzpflichten. Und es bleibt selten bei einem Verstoß. DSGVO-Bußgelder, Schadenersatz und Abmahnungen richten sich nicht nach der Firmengröße.

DIE PFLICHT, DIE FAST ALLE ÜBERSEHEN

Du musst deine Mitarbeiter schulen. Das ist kein Tipp. Das ist Gesetz.

Artikel 4 des EU AI Act verpflichtet jedes Unternehmen, das KI einsetzt, **Maßnahmen zu ergreifen, um die KI-Kompetenz aller Personen zu fördern, die in seinem Auftrag mit KI arbeiten**. Das gilt seit dem **2. Februar 2025**, seit 27. Juli 2026 in der Fassung des Digital Omnibus. Seit **August 2026** überwachen die nationalen Behörden die Einhaltung. Ein bestimmtes Zertifikat schreibt das Gesetz nicht vor. Aber du musst belegen können, **welche Maßnahmen du gesetzt hast**, und dafür ist eine dokumentierte, geprüfte Schulung der stärkste Beweis.

Jede Größe

Keine Ausnahme für Kleinbetriebe. Ein Mitarbeiter, der irgendeine KI nutzt, reicht.

Jede Rolle

Geschäftsführung, Büro, Vertrieb, Marketing, HR, Freelancer.

Jeder Nachweis

Wer, wann, was, mit welchem Ergebnis. Schriftlich.

Was passiert, wenn ein ungeschulter Mitarbeiter einen Fehler macht?

SITUATION	OHNE SCHULUNGSNACHWEIS
Kundendaten landen in einem Gratis-KI-Tool	Datenschutzverstoß, Meldepflicht binnen 72 Stunden, Bußgeld bis 4 % des Umsatzes, Schadenersatz an jeden Betroffenen
Chatbot oder KI-Mail sagt dem Kunden etwas Falsches	Das Unternehmen haftet, als hätte ein Mitarbeiter es gesagt (OLG Hamm, 2026)
KI-Bild oder -Video ohne Kennzeichnung gepostet	Verstoß gegen Art. 50, bis 15 Mio. € oder 3 % des Umsatzes
Fake-Anruf vom „Chef“ mit KI-Stimme, Überweisung raus	Geld weg, Versicherung fragt nach Schulung und Freigabeprozess
Erfundene Zahlen oder Quellen im Angebot oder Gutachten	Gewährleistung, Schadenersatz, Rückforderung, Reputationsschaden

Der entscheidende Punkt: Kommt es zu einem Schaden, wird als Erstes gefragt, ob das Unternehmen seine Leute geschult hat. Fehlt der Nachweis, gilt das als Organisationsmangel, und der trifft die Firma und unter Umständen die Geschäftsführung persönlich.

DAS IST SCHON PASSIERT

Echte Strafen. Echte Unternehmen. Kein Szenario, kein Konjunktiv.

Wichtig zur Einordnung: Ein Bußgeld nach dem AI Act selbst ist bis heute nicht öffentlich bekannt, die Behörden haben ihre Aufsicht gerade erst aufgenommen. Bestraft wird KI-Einsatz trotzdem längst: über Datenschutz, Wettbewerbsrecht, Haftung und Arbeitsrecht. Wer bei den ersten AI-Act-Verfahren dabei ist, wird zum Präzedenzfall.

OKT. 2026 · NIEDERLANDE

DSGVO · KI-ENTSCHEIDUNG

824.990.000 €

Uber (Konzern)

Fahrerkonten wurden von einem Algorithmus automatisch gesperrt, ohne dass ein Mensch geprüft hat. Fahrer verloren ihr Einkommen. Uber hat Rechtsmittel eingelegt.

Quelle: edpb.europa.eu

JAN. 2024 · HONGKONG / UK

DEEPFAKE-BETRUG

25,6 Mio. US-$

Arup (Ingenieurkonzern)

Ein Mitarbeiter überwies nach einem Videocall mit einem KI-gefälschten Finanzchef und gefälschten Kollegen in 15 Überweisungen. Alles echt aussehend, alles fake.

Quelle: cnn.com via abc17news.com

SEP. 2025 · DEUTSCHLAND

DSGVO · ALGORITHMUS

492.000 €

Finanzdienstleister, Hamburg

Kreditkartenanträge wurden automatisch abgelehnt, auch bei guter Bonität, ohne menschliche Prüfung und ohne verständliche Begründung.

Quelle: Hamburgische Datenschutzbehörde / clydeco.com

MAI 2026 · DEUTSCHLAND

KMU · CHATBOT

Verurteilt

Ästhetik-Praxis (KMU)

Der Website-Chatbot nannte Facharzttitel, die die Ärzte nicht hatten. Das OLG Hamm: Der Betreiber haftet für jede Aussage seines Chatbots (4 UKl 3/25).

Quelle: justiz.nrw

2022 – 2024 · NL · IT · GR · FR

DSGVO · GESICHTSERKENNUNG

über 90 Mio. €

Clearview AI

Gesichtsdatenbank aus Internet-Fotos: 30,5 Mio. € in den Niederlanden, je 20 Mio. € in Italien, Griechenland und Frankreich, dazu 5,2 Mio. € Zwangsgeld.

Quelle: njb.nl / privacylaws.com / therecord.media

DEZ. 2025 · FRANKREICH

MITARBEITER-ÜBERWACHUNG

15 Mio. €

Amazon France Logistique

Lagermitarbeiter wurden über Scanner-Kennzahlen lückenlos überwacht, inklusive Leerlaufzeiten. Ursprünglich 32 Mio. €, vom Höchstgericht auf 15 Mio. € reduziert.

Quelle: CNIL / Conseil d'État

UND ES GEHT WEITER

Vom Kleinbetrieb bis zum Konzern. KI-Fehler kosten echtes Geld.

2019 · DEUTSCHLAND / UK — KI-STIMME · BETRUG

220.000 €

Tochter eines deutschen Energiekonzerns

Ein Betrüger imitierte per KI-Stimme den deutschen Konzernchef am Telefon. Das Geld ging nach Ungarn und war verloren.

Quelle: allianz-trade.de

MAI 2025 · ITALIEN — DSGVO · CHATBOT

5 Mio. €

Luka Inc. (Chatbot Replika)

Kein ausreichender Datenschutz, keine Rechtsgrundlage, keine wirksame Altersprüfung beim KI-Chatbot.

Quelle: Garante Privacy

JULI 2024 · ITALIEN — KMU · ARBEITSZEIT

120.000 €

Autohaus (KMU)

Arbeitszeiterfassung per Gesichtserkennung und jahrelang gespeicherte Leistungsdaten der Mitarbeiter.

Quelle: Garante Privacy / lentepubblica.it

AUG. 2025 · SPANIEN — KMU · BIOMETRIE

96.000 €

Fitnessstudio-Kette

Mitglieder kamen nur per Gesichtserkennung ins Studio, ohne Alternative und ohne Datenschutz-Folgenabschätzung.

Quelle: AEPD / xataka.com

FEB. 2024 · ITALIEN — KMU · ZUTRITT

103.000 €

Deponiebetreiber + 4 Dienstleister

Zutritt der Mitarbeiter per Gesichtserkennung, um Fehlzeiten zu bekämpfen. Auch die Dienstleister wurden bestraft.

Quelle: Garante Privacy / cybersecurity360.it

2022 · UNGARN — EMOTIONSERKENNUNG

ca. 670.000 €

Ungarische Bank

Eine KI analysierte in Kundenanrufen Emotionen und Schlüsselwörter. Heute ist Emotionserkennung am Arbeitsplatz durch den AI Act sogar verboten.

Quelle: NAIH / williamfry.com

NOV. 2024 · ITALIEN — ALGORITHMUS · PERSONAL

5 Mio. €

Foodinho / Glovo

Gesichtserkennung bei Fahrern und automatische Kontosperren ohne Hinweis auf das Recht auf menschliche Prüfung.

Quelle: Garante Privacy

JAN. 2024 · ITALIEN — ÖFFENTLICHE HAND

50.000 €

Gemeinde Trento

KI-Auswertung von Kamera-, Mikrofon- und Social-Media-Daten in Forschungsprojekten. Strafe plus Löschung aller Daten.

Quelle: Garante Privacy / ladige.it

UND ES GEHT WEITER

Keine Branche ist sicher. Auch deine nicht.

MAI 2023 · SÜDKOREA — MITARBEITER · DATENLECK

KI-Verbot

Samsung Electronics

Ingenieure kopierten internen Quellcode in ChatGPT. Danach: generative KI für alle Mitarbeiter verboten, Kündigung bei Verstößen angedroht.

Quelle: mobilesyrup.com

NOV. 2025 · ÖSTERREICH — KANZLEI · HALLUZINATION

Zurückgewiesen

Strafverteidiger vor dem OGH

Das Rechtsmittel zitierte OGH-Entscheidungen, die es nicht gibt. Der OGH geht von KI-Erstellung ohne fachliche Kontrolle aus und wies es zurück.

Quelle: borncity.com

SEP. 2026 · DEUTSCHLAND — HALLUZINATION

3.000 € Gebühr

Beschwerdeführer, BayVerfGH

Eine Verfassungsbeschwerde stützte sich auf erfundene, vermutlich KI-generierte Urteile. Unzulässig, Höchstgebühr.

Quelle: it-recht-kanzlei.de

FEB. 2024 · KANADA — CHATBOT-HAFTUNG

Haftet

Air Canada (Konzern)

Der Chatbot erfand eine Erstattungsregel. Das Argument, der Bot sei selbst verantwortlich, wurde verworfen. Das Unternehmen haftet.

Quelle: cxtoday.com

OKT. 2025 · AUSTRALIEN — BERATUNG · KI-FEHLER

97.000 AU-$ zurück

Deloitte Australia

Ein Regierungsbericht enthielt ein erfundenes Gerichtszitat und Studien, die es nicht gibt. Deloitte musste einen Teil des Honorars zurückzahlen.

Quelle: cfodive.com

JUNI 2026 · DEUTSCHLAND — KI-AUSSAGEN · HAFTUNG

Einstw. Verfügung

Google (AI Overviews)

Die KI-Übersicht brachte zwei Münchner Verlage ohne Beleg mit Betrug in Verbindung. LG München I: Google haftet unmittelbar (nicht rechtskräftig).

Quelle: onlinemarketing.de

AUG. 2023 · USA — KI IM RECRUITING

365.000 US-$

iTutorGroup

Die Bewerbersoftware sortierte Frauen ab 55 und Männer ab 60 automatisch aus. Vergleich mit der Gleichstellungsbehörde.

Quelle: foley.com

JULI 2025 · USA — KI-CHATBOT · DATENLECK

64 Mio. Datensätze

McDonald's / Paradox.ai

Beim KI-Bewerbungschatbot lagen Chatverläufe und Bewerberdaten offen. Admin-Passwort: 123456.

Quelle: bleepingcomputer.com

WAS IN DEINEM BÜRO GERADE PASSIERT

Deine Mitarbeiter nutzen KI längst. Die Frage ist nur: wie?

78 %

der KI-Nutzer bringen ihre eigenen KI-Tools mit in die Arbeit. Nur **39 %** wurden vom Arbeitgeber geschult.

Microsoft & LinkedIn Work Trend Index 2024, 31.000 Befragte

73,8 %

der ChatGPT-Nutzung am Arbeitsplatz läuft über private Accounts, also außerhalb jeder Kontrolle des Unternehmens.

Cyberhaven 2024

66 %

der Beschäftigten übernehmen KI-Ergebnisse, ohne sie zu prüfen. 57 % verheimlichen ihre KI-Nutzung vor dem Arbeitgeber.

KPMG & University of Melbourne 2025, 48.000 Befragte

4 von 10

deutschen Unternehmen gehen davon aus, dass ihre Beschäftigte private KI-Tools nutzen. Tendenz steigend.

Bitkom 2025

Heißt für dich: Die Frage ist nicht, ob in deinem Betrieb KI genutzt wird. Die Frage ist, ob es geregelt, geschult und nachweisbar ist. Wenn nicht, trägt das Unternehmen das Risiko für jeden Fehler, jedes Datenleck und jede falsche Auskunft.

DER CHECK

90 Punkte. Hake ehrlich ab.

Setze ein Häkchen nur, wenn der Punkt **heute erledigt und schriftlich dokumentiert** ist. „Machen wir eh irgendwie" zählt nicht. Bei einer Prüfung zählt nur, was du nachweisen kannst.

01 KI-Inventur & Rollen

Grundlage für alle anderen Pflichten

Grundlage

- [ ] 01 **Vollständige Liste aller KI-Tools im Unternehmen**
  ChatGPT, Copilot, Gemini, DeepL, Canva-KI, Meeting-Transkription, KI im CRM, ERP, Buchhaltung oder Telefonanlage. Ohne Liste keine Compliance.
- [ ] 02 **Schatten-KI erfasst**
  Welche Mitarbeiter nutzen private Accounts, Gratis-Versionen oder KI-Apps am Handy für Firmenarbeit? In fast jedem Betrieb: mehr, als die Geschäftsführung glaubt.
- [ ] 03 **Versteckte KI in bestehender Software erkannt**
  Microsoft 365, Google Workspace, Zoom, Teams, Adobe und viele Branchenprogramme schalten KI-Funktionen per Update automatisch frei. Auch die zählen.
- [ ] 04 **Browser-Erweiterungen und Handy-Apps mit KI erfasst**
  KI-Schreibhilfen, Übersetzer, Grammatik-Plug-ins: Sie lesen oft alles mit, was im Browser steht.
- [ ] 05 **Rolle je System geklärt: Betreiber oder Anbieter?**
  Wer ein KI-System unter eigenem Namen anbietet oder wesentlich verändert, kann selbst zum Anbieter mit deutlich strengeren Pflichten werden (Art. 25).
- [ ] 06 **Zweck, Datenarten und Verantwortliche je System dokumentiert**
  Für jedes Tool: Wofür, mit welchen Daten, wer ist zuständig, wer darf es nutzen?
- [ ] 07 **Risikoklasse je System eingestuft**
  Verboten, Hochrisiko, Transparenzpflicht oder geringes Risiko. Die Einstufung entscheidet über alle weiteren Pflichten.
- [ ] 08 **Freigabeprozess für neue KI-Tools**
  Niemand führt ein neues KI-Tool ein, ohne dass es geprüft und freigegeben wurde.

02 Mitarbeiterschulung: gesetzliche Pflicht

Art. 4 · KI-Kompetenz fördern seit 2. Februar 2025 · Aufsicht ab 2. August 2026

Pflicht für jeden Betrieb

- [ ] 09 **Jeder Mitarbeiter, der KI nutzt, ist geschult**
  Art. 4 verlangt Maßnahmen zur Förderung der KI-Kompetenz, unabhängig von der Firmengröße. Schon wenn eine einzige Person irgendeine KI nutzt: für Mails, Angebote, Übersetzungen, Bilder, Social Media oder über eine KI-Funktion in eurer Software.
- [ ] 10 **Geschäftsführung selbst geschult**
  Wer KI-Einsatz verantwortet und Regeln vorgibt, muss die Risiken selbst beurteilen können. Organisationsverschulden trifft die Führung.
- [ ] 11 **Schulung passt zu Rolle und Risiko**
  Vertrieb, Buchhaltung, HR, Marketing, Kundenservice und Geschäftsführung brauchen unterschiedliches Wissen. Eine Pauschal-Folie reicht nicht.

- [ ] 12 **Grundlagen: Wie KI funktioniert und wo sie Fehler macht**
  Halluzinationen erkennen, Ergebnisse prüfen, Grenzen kennen. Erfundene Zahlen, Quellen und Urteile sind keine Seltenheit.
- [ ] 13 **Datenschutz: Was darf in die KI, was nicht**
  Kundendaten, Gesundheitsdaten, Personaldaten, Bankdaten: Mitarbeiter müssen im Alltag sofort wissen, wo die Grenze ist.
- [ ] 14 **Geschäftsgeheimnisse geschützt**
  Kalkulationen, Angebote, Quellcode, Verträge, Baupläne. Was einmal im falschen Tool ist, ist nicht mehr zurückzuholen.
- [ ] 15 **Kennzeichnungspflichten bekannt**
  Wann KI-Bilder, -Videos, -Stimmen und Chatbots gekennzeichnet werden müssen. Seit 2. August 2026 Pflicht.
- [ ] 16 **Urheberrecht und Markenrecht bekannt**
  KI-Bilder, Logos, Texte und Musik können Rechte Dritter verletzen. Die Abmahnung geht an das Unternehmen.
- [ ] 17 **Deepfakes und KI-Betrug erkennen**
  Gefälschte Stimmen und Videos von Chefs oder Lieferanten: Mitarbeiter müssen wissen, wie man Zahlungsaufforderungen verifiziert.
- [ ] 18 **Sicherer Umgang mit KI-Agenten und Automationen**
  Was eine KI selbstständig tun darf (Mails senden, buchen, bestellen) und wo immer ein Mensch freigibt.
- [ ] 19 **Auch Freelancer, Leiharbeiter und Dienstleister erfasst**
  Art. 4 umfasst alle Personen, die in deinem Auftrag mit deinen KI-Systemen arbeiten.
- [ ] 20 **Neue Mitarbeiter vor der ersten KI-Nutzung geschult**
  Onboarding-Pflicht. Der erste Tag ohne Schulung ist der erste Tag mit Risiko.
- [ ] 21 **Wissen geprüft, nicht nur Folien gezeigt**
  Ein Test oder eine Prüfung belegt, dass die Schulung angekommen ist. Anwesenheit allein beweist nichts.
- [ ] 22 **Schulung dokumentiert: wer, wann, was, wie lange**
  Teilnehmerliste, Inhalte, Datum, Ergebnis. Ohne Nachweis gilt: nicht passiert.
- [ ] 23 **Zertifikat oder Teilnahmebestätigung je Mitarbeiter abgelegt**
  Bei einer Behördenanfrage, einem Schadensfall oder einem Rechtsstreit ist das dein wichtigstes Beweisstück.
- [ ] 24 **Regelmäßige Auffrischung**
  Bei neuen Tools, neuen Funktionen und neuen Leitlinien der Behörden. KI ändert sich monatlich.
- [ ] 25 **KI-Richtlinie von jedem Mitarbeiter unterschrieben**
  Nur was schriftlich geregelt und bestätigt ist, lässt sich arbeitsrechtlich durchsetzen.

03 Verbotene KI-Praktiken

Art. 5 · gilt seit 2. Februar 2025

bis 35 Mio. € / 7 %

- [ ] 26 **Keine Emotionserkennung bei Mitarbeitern**
  Stimmungsanalyse in Callcenter-Software oder Video-Meetings ist am Arbeitsplatz verboten (Ausnahmen nur aus medizinischen oder Sicherheitsgründen).
- [ ] 27 **Keine manipulativen KI-Techniken**
  KI, die Kunden unterschwellig so beeinflusst, dass sie Entscheidungen treffen, die sie sonst nicht treffen würden.
- [ ] 28 **Keine Ausnutzung von Schwächen**
  KI, die gezielt Alter, Behinderung oder wirtschaftliche Notlage ausnutzt.
- [ ] 29 **Keine biometrische Kategorisierung nach sensiblen Merkmalen**
  Rückschlüsse auf Herkunft, politische Meinung, Religion oder sexuelle Orientierung aus Gesicht oder Stimme.
- [ ] 30 **Kein Social Scoring**
  Bewertung von Personen nach Sozialverhalten mit nachteiligen Folgen in anderen Zusammenhängen.
- [ ] 31 **Keine Gesichtsdatenbanken aus dem Internet**
  Ungezieltes Auslesen von Gesichtsbildern aus Internet oder Videoüberwachung ist verboten. Clearview AI wurde dafür in mehreren EU-Ländern bestraft.

04 Hochrisiko-Check

Anhang III · Betreiberpflichten ab 2. Dezember 2027

bis 15 Mio. € / 3 %

- [ ] 32 **KI im Recruiting?**
  CV-Screening, Bewerber-Ranking, Analyse von Video-Interviews: Hochrisiko-KI. Auch in vielen Bewerbermanagement-Tools eingebaut.
- [ ] 33 **KI bei Beförderung, Kündigung, Schichtplanung oder Leistungsüberwachung?**
  Ebenfalls Hochrisiko. Betrifft viele HR- und Zeiterfassungs-Tools, die heute schon laufen.
- [ ] 34 **KI bei Kreditwürdigkeit, Versicherung oder Bonität von Personen?**
  Hochrisiko, mit umfangreichen Dokumentations- und Aufsichtspflichten.
- [ ] 35 **Menschliche Aufsicht durch kompetente Person benannt**
  Eine geschulte Person muss Ergebnisse überwachen und eingreifen können (Art. 26).
- [ ] 36 **Logs mindestens 6 Monate aufbewahrt**
  Automatisch erzeugte Protokolle sind aufzubewahren und bei Prüfungen vorzulegen (Art. 26).
- [ ] 37 **Beschäftigte und Betriebsrat vorab informiert**
  Vor dem Einsatz am Arbeitsplatz, nicht danach (Art. 26).
- [ ] 38 **Grundrechte-Folgenabschätzung, wo vorgeschrieben**
  Pflicht u. a. für öffentliche Stellen und bestimmte Banken und Versicherer (Art. 27).

05 Transparenz & Kennzeichnung

Art. 50 · gilt seit 2. August 2026, nicht verschoben

bis 15 Mio. € / 3 %

- [ ] 39 **Chatbot gibt sich als KI zu erkennen**
  Auf Website, WhatsApp, Instagram, Messenger, auch als eingebettetes Widget eines Drittanbieters.
- [ ] 40 **KI-Telefonassistent sagt, dass er eine KI ist**
  Spätestens zu Beginn des Gesprächs.
- [ ] 41 **KI-Bilder und -Videos realer Personen, Orte oder Objekte gekennzeichnet**
  Deepfakes, KI-Avatare, KI-bearbeitete Produkt- und Immobilienfotos, die echt wirken.
- [ ] 42 **Geklonte und synthetische Stimmen gekennzeichnet**
  Werbespots, Erklärvideos, Warteschleifen und Social-Media-Videos mit KI-Stimme.
- [ ] 43 **KI-Texte zu Themen öffentlichen Interesses gekennzeichnet**
  Sofern sie nicht von einem Menschen redigiert und verantwortet werden.
- [ ] 44 **Betroffene über Emotionserkennung oder biometrische Kategorisierung informiert**
  Wo diese Systeme überhaupt erlaubt sind.
- [ ] 45 **Kennzeichnung klar, rechtzeitig und barrierefrei**
  Spätestens bei der ersten Interaktion, nicht versteckt im Kleingedruckten.
- [ ] 46 **Vorlagen und Prozess für Kennzeichnung im Team bekannt**
  Wer postet, entscheidet im Alltag. Ohne Vorlage wird die Kennzeichnung vergessen.

06 Datenschutz bei KI (DSGVO)

gilt laufend · KI ist Prüfschwerpunkt der Behörden

bis 20 Mio. € / 4 %

- [ ] 47 **Auftragsverarbeitungsvertrag mit jedem KI-Anbieter**
  Ohne AVV keine Kundendaten in KI-Tools.
- [ ] 48 **Keine personenbezogenen Daten in Gratis-Versionen**
  Eine kopierte Kunden-Mail im kostenlosen ChatGPT ist bereits eine Datenverarbeitung, oft ohne Rechtsgrundlage.
- [ ] 49 **Training mit euren Daten abgeschaltet**
  Viele Tools nutzen Eingaben standardmäßig zum Training. Abschalten und dokumentieren.
- [ ] 50 **Rechtsgrundlage je KI-Verarbeitung geklärt**
  Für jeden Einsatzzweck einzeln.
- [ ] 51 **Datenschutzerklärung nennt den KI-Einsatz**
  Informationspflichten nach Art. 13 und 14 DSGVO.
- [ ] 52 **Verzeichnis der Verarbeitungstätigkeiten um KI ergänzt**
  Jedes KI-Tool, das personenbezogene Daten verarbeitet, gehört ins Verzeichnis (Art. 30).
- [ ] 53 **Datenübermittlung in Drittländer geprüft**
  Viele KI-Anbieter verarbeiten Daten in den USA oder in China.
- [ ] 54 **Datenschutz-Folgenabschätzung, wo erforderlich**
  Bei hohem Risiko für Betroffene verpflichtend (Art. 35).

- [ ] 55 **Keine rein automatisierten Entscheidungen mit Rechtswirkung**
  Ohne menschliche Prüfung unzulässig (Art. 22). Der EuGH hat das 2023 im SCHUFA-Urteil bestätigt.
- [ ] 56 **Auskunfts- und Löschanfragen auch für KI-Daten beantwortbar**
  Betroffene können fragen, was eure KI über sie gespeichert hat. Antwort binnen eines Monats.

07 Arbeitsrecht

ArbVG (AT) · BetrVG (DE) · gilt laufend

Unwirksamkeit & Streit

- [ ] 57 **Betriebsrat eingebunden**
  KI-Systeme, die Mitarbeiter kontrollieren oder Personaldaten verarbeiten, können eine Betriebsvereinbarung erfordern (§§ 96, 96a ArbVG; § 87 BetrVG).
- [ ] 58 **Ohne Betriebsrat: Zustimmung der Mitarbeiter, wo nötig**
  Kontrollmaßnahmen, die die Menschenwürde berühren, brauchen in Österreich die Zustimmung jedes Einzelnen (§ 10 AVRAG).
- [ ] 59 **Verbindliche Regeln, welche KI erlaubt ist**
  Was nicht geregelt ist, ist im Streitfall kaum durchsetzbar.
- [ ] 60 **Konsequenzen bei Verstößen festgelegt**
  Was passiert, wenn jemand Kundendaten in ein privates KI-Tool kopiert?
- [ ] 61 **Haftung bei KI-Fehlern intern geregelt**
  Wer haftet, wenn ein Mitarbeiter mit KI einen teuren Fehler macht? Ohne Schulung trägt das oft der Arbeitgeber.
- [ ] 62 **Keine KI-Überwachung von Leistung oder Verhalten ohne Prüfung**
  Tastatur-, Bildschirm- und Gesprächsanalyse mit KI ist rechtlich hochriskant.

08 Haftung, Verträge & Geschäftsgeheimnisse

gilt laufend

Schadenersatz & Unterlassung

- [ ] 63 **Ihr haftet für jede Aussage eures Chatbots**
  OLG Hamm, 12. Mai 2026 (4 UKl 3/25): Eine Praxis für ästhetische Medizin wurde wegen falscher Chatbot-Auskünfte zur Unterlassung verurteilt.
- [ ] 64 **Geschäftsführung kennt ihre persönliche Haftung**
  Geschäftsführer haften der Gesellschaft für Schäden aus mangelhafter Organisation (§ 25 GmbHG in AT, § 43 GmbHG in DE). Fehlende Regeln und Schulungen sind ein Organisationsmangel.
- [ ] 65 **Keine Geschäftsgeheimnisse in KI-Tools ohne Freigabe**
  Kalkulationen, Angebote, Kundenlisten, Baupläne, Quellcode.
- [ ] 66 **Kundenverträge und NDAs erlauben die KI-Verarbeitung**
  Viele Verträge verbieten die Weitergabe an Dritte, und ein KI-Anbieter ist ein Dritter.
- [ ] 67 **Urheberrecht am KI-Output geprüft**
  Wem gehören KI-Texte und -Bilder, und verletzen sie Rechte Dritter?
- [ ] 68 **Verträge mit KI-Anbietern geprüft**
  Wird mit euren Daten trainiert? Wer haftet bei Fehlern? Wo stehen die Server?

- [ ] 69 **KI-Ergebnisse vor Weitergabe fachlich geprüft**
  Angebote, Gutachten, Berechnungen, Rechtsauskünfte: Fehler der KI sind Fehler eures Unternehmens.
- [ ] 70 **Versicherungsschutz für KI-Schäden geklärt**
  Deckt eure Betriebs- oder Cyber-Versicherung Schäden durch KI-Fehler und KI-Betrug?

09 IT-Sicherheit & KI-Betrug

gilt laufend · NIS2 für viele Branchen

Totalverlust möglich

- [ ] 71 **Freigabeprozess für Zahlungen, der Deepfakes standhält**
  Rückruf über bekannte Nummer, Vier-Augen-Prinzip. Ein gefälschter Video-Call hat 2024 einen Konzern 25 Mio. US-Dollar gekostet.
- [ ] 72 **Firmen-Accounts statt privater KI-Accounts**
  Nur so lassen sich Zugänge sperren, wenn jemand das Unternehmen verlässt.
- [ ] 73 **Zwei-Faktor-Anmeldung für alle KI-Tools**
  KI-Accounts enthalten oft den gesamten Gesprächsverlauf mit Firmendaten.
- [ ] 74 **Rechte von KI-Assistenten begrenzt**
  Copilot und Co. sehen alles, worauf der Nutzer Zugriff hat. Falsch gesetzte Freigaben werden so für alle sichtbar.
- [ ] 75 **Schutz vor Prompt-Injection bei KI-Agenten**
  Manipulierte Mails oder Webseiten können KI-Agenten zu falschen Aktionen bringen.
- [ ] 76 **Meldewege für KI-Vorfälle bekannt**
  Datenpanne: 72 Stunden. NIS2-pflichtige Betriebe: Frühwarnung binnen 24 Stunden.

10 Marketing & Kundenkommunikation

UWG · Verbraucherrecht · gilt laufend

Abmahnung & Klage

- [ ] 77 **Keine KI-generierten Kundenbewertungen oder Testimonials**
  Gefälschte Bewertungen sind in der EU ausdrücklich verboten und abmahnfähig.
- [ ] 78 **Keine KI-Personen, die als echte Mitarbeiter oder Kunden auftreten**
  Ohne Kennzeichnung irreführend.
- [ ] 79 **Werbeaussagen über KI sind belegbar**
  "KI-gestützt" oder "mit KI optimiert" muss stimmen. Behörden in den USA strafen "AI Washing" bereits ab.
- [ ] 80 **KI-Produktbilder zeigen das echte Produkt**
  Geschönte KI-Bilder von Produkten, Häusern oder Ergebnissen können irreführende Werbung sein.
- [ ] 81 **Rechte an Stimmen, Gesichtern und Musik geklärt**
  Geklonte Stimmen und Gesichter realer Personen ohne Einwilligung verletzen Persönlichkeitsrechte.
- [ ] 82 **Automatisierte Antworten auf Anfragen geprüft**
  KI-Mails und Chat-Antworten an Kunden enthalten Preise, Fristen und Zusagen. Die gelten.

11 Governance & Nachweis

laufend · Grundlage bei jeder Prüfung

bis 7,5 Mio. € / 1 %

- [ ] 83 **Schriftliche KI-Richtlinie**
  Was ist erlaubt, was verboten, wer entscheidet?
- [ ] 84 **Verantwortliche Person für KI benannt**
  Ein Ansprechpartner, der den Überblick hat und Änderungen verfolgt.
- [ ] 85 **Menschliche Kontrolle vor Veröffentlichung**
  Kein KI-Output geht ungeprüft an Kunden oder in die Öffentlichkeit.
- [ ] 86 **Notfallprozess bei KI-Fehlern und Datenpannen**
  Wer tut was in der ersten Stunde?
- [ ] 87 **Nachweisordner für Behördenanfragen**
  Falsche oder unvollständige Angaben gegenüber Behörden sind selbst bußgeldbewehrt.
- [ ] 88 **Lieferanten und Partner nach KI-Einsatz gefragt**
  Eure Dienstleister nutzen KI mit euren Daten. Habt ihr das geregelt?
- [ ] 89 **Laufende Beobachtung neuer Leitlinien**
  EU-Kommission, KI-Servicestelle der RTR, Datenschutzbehörden veröffentlichen laufend neue Vorgaben.
- [ ] 90 **Jährliches Review aller Systeme und Schulungen**
  KI-Tools ändern sich monatlich, die Pflichten bleiben.

AUSWERTUNG

Wie viele Häkchen hast du? _____ / 90

0 – 59

Akutes Risiko. Dein Unternehmen nutzt KI ohne rechtliche Absicherung. Jede Prüfung, jede Kundenbeschwerde und jeder Mitarbeiterkonflikt kann teuer werden.

60 – 79

Deutliche Lücken. Die Basis ist da, aber genau die fehlenden Punkte sind die, nach denen bei Prüfungen gefragt wird.

80 – 90

Stark aufgestellt. Wichtig ist jetzt, die Dokumentation laufend aktuell zu halten, weil sich Tools und Leitlinien laufend ändern.

Und jetzt die ehrliche Frage: **Wer in deinem Unternehmen soll das alles machen?**

Jeder dieser Punkte heißt: Tools erfassen, rechtlich einordnen, Dokumente erstellen, Mitarbeiter schulen, Nachweise ablegen, und das Ganze bei jedem neuen Tool und jeder Gesetzesänderung wiederholen. Die Regeln kommen aus dem AI Act, der DSGVO, dem Arbeitsverfassungsgesetz, dem Wettbewerbsrecht und dem Urheberrecht, und sie greifen gleichzeitig.

Selbst machen

- ✕ Wochen an Einarbeitung in Verordnung, Leitlinien und Fristen
- ✕ Externe Rechtsberatung für jede Unsicherheit
- ✕ Schulungen selbst konzipieren und dokumentieren
- ✕ Keine Bestätigung, dass die Schulung ausreicht
- ✕ Jedes Update wieder von vorne
- ✕ Zeit, die dir im Tagesgeschäft fehlt

Mit Agent AI

- ✓ KI-Inventur und Risikoeinstufung für deinen Betrieb
- ✓ Fertige KI-Richtlinie, Kennzeichnungs-Vorlagen und Nachweisordner
- ✓ TÜV-zertifizierte Schulung für dein Team, Prüfungskosten inklusive
- ✓ Ein KI-Experte für dein Unternehmen: selbst ausgebildet oder von uns gestellt
- ✓ Laufende Updates, wenn sich Gesetz oder Tools ändern
- ✓ Plattform mit fertigen KI-Automationen, die dir Zeit und Geld sparen

SO SCHLIESST DU DIE LÜCKEN

Drei Wege. Selbst aufbauen oder den Profi bekommen.

Agent AI ist das Institut für digitale Kompetenz: Wir bilden Menschen zu TÜV-zertifizierten KI-Profis aus, sichern damit ihre Zukunft und bringen sie mit Betrieben zusammen, die genau diese Leute brauchen. Für dich heißt das:

WEG 1 · STUFE 1

KI-Agenten aufbauen

17.850 €

zzgl. USt. · 6-Monats-Raten-Garantie

- KI-Agenten für deinen Betrieb
- 1:1 & Live-Calls mit Luis Zauchner
- Team mitgeschult, Art. 4 inklusive

WEG 2 · KEINE ZEIT

KI-Profi bekommen

Netzwerk

zertifizierte Absolventen aus Österreich & DACH

- Wir bringen dich mit einem KI-Profi zusammen
- Als Mitarbeiter, Projekt oder laufende Betreuung
- Er übernimmt Inventur, Richtlinie, Kennzeichnung, Schulung

WEG 3 · STUFE 2

Eigene KI-Tools

35.700 €

zzgl. USt. · 6-Monats-Raten-Garantie

- Alles aus Stufe 1, inkl. 1:1 mit Luis
- Eigene KI-Tools & Geschäftsmodelle
- Stufe 3: + Chris Steiner & Philipp Kuhn

WAS PERSÖNLICH DRIN IST

LEISTUNG	STUFE 1 17.850 €	STUFE 2 35.700 €	STUFE 3 100.000 €
Selbstlern-Videokurs, 6 Module + TÜV-Zertifikat	✔	✔	✔
KI-Richtlinie, Nachweisordner, Tools & Vorlagen	✔	✔	✔
3 Gruppen-Calls pro Woche	✔	✔	✔
1:1-Begleitung & Live-Calls mit Luis Zauchner	✔	✔	✔
Eigene KI-Tools & KI-Geschäftsmodell	–	✔	✔
Done-With-You KI-Agentur-Aufbau	–	–	✔
1:1 & Live-Calls mit Chris Steiner & Philipp Kuhn	–	–	✔

Stufen 1–3 zzgl. USt.; 6-Monats-Finanzierungsraten-Garantie nach Leistungsvereinbarung (Stufe 1 & 2). Netzwerk: Wir stellen den Kontakt zwischen Betrieben und Absolventen her; kein Vermittlungs- oder Erfolgsversprechen. Verbindlich sind Leistungsvereinbarung und AGB.

Kostenloser AI-Act-Strategie-Call

30 Minuten. Wir gehen deinen Check gemeinsam durch, zeigen dir, welche Lücken wirklich kritisch sind, und wie du sie in kürzester Zeit nachweisbar schließt, ohne dich selbst damit beschäftigen zu müssen.

Jetzt Termin sichern → calendly.com/luis-poza-ki/agent-ai-erstgesprach

BIST DU VORBEREITET?

5 Fragen, die du bei einer Prüfung sofort beantworten können musst

1	„Zeigen Sie mir bitte Ihr Verzeichnis aller eingesetzten KI-Systeme.“
2	„Wie haben Sie die KI-Kompetenz Ihrer Mitarbeiter sichergestellt, und wo ist der Nachweis?“
3	„Wo auf Ihrer Website und am Telefon wird der KI-Einsatz gekennzeichnet?“
4	„Welche Verträge haben Sie mit Ihren KI-Anbietern, und wohin fließen die Daten?“
5	„Wer ist in Ihrem Unternehmen für KI verantwortlich?“

Wenn du bei **einer einzigen** dieser Fragen zögerst, buch dir den kostenlosen Call. Wir zeigen dir, wie du alle fünf in kürzester Zeit mit fertigen Unterlagen beantworten kannst.

Chris Steiner
Unternehmer, Speaker, Buchautor

Philipp Kuhn
Keynote-Speaker, Sales-Coach

Luis Zauchner
KI-Systeme & Automationen

Dieser Check ist eine Orientierungshilfe und ersetzt keine Rechtsberatung im Einzelfall. Rechtsgrundlagen: Verordnung (EU) 2024/1689 (KI-Verordnung) in der Fassung der Verordnung (EU) 2026/1744 (Digital Omnibus), Verordnung (EU) 2016/679 (DSGVO), Arbeitsverfassungsgesetz (ArbVG); OLG Hamm, Urteil vom 12.05.2026, 4 UKl 3/25. Stand: Oktober 2026.