AI-COMPLIANCE-SCHNELLCHECK

Für Unternehmen

Erste Standortbestimmung in ca. 20–25 Minuten

Welche KI-Systeme sind bereits erfasst?
Welche Anforderungen gelten für Ihr Unternehmen?
Wo bestehen Lücken oder Unsicherheiten?

Kostenlose allgemeine Arbeitshilfe

Stand: 17. August 2026

So nutzen Sie den Schnellcheck

Gehen Sie die Prüffragen zügig durch und markieren Sie pro Frage genau eine Antwort. Der Schnellcheck ist bewusst als erste Standortbestimmung aufgebaut. Er ersetzt weder ein vollständiges AI-Compliance-Assessment noch die rechtliche Prüfung oder Risikoklassifizierung des konkreten Einzelfalls.

JA	TEILWEISE / UNKLAR	NEIN	N. R.
Anforderung erkennbar erfüllt	nicht vollständig oder Nachweis unklar	Handlungsbedarf	für Ihr Unternehmen nicht relevant

★ **Kernfrage:** Ein „Nein“ bei einer Kernfrage sollte unabhängig vom Gesamteindruck zeitnah geprüft werden.

Wichtig: Die Ampel am Ende ist nur eine Orientierung. Sie ist keine Rechtsbewertung, kein Auditurteil und keine Aussage über Bußgeld- oder Haftungsrisiken. Bei möglichen Hochrisiko-Systemen ist zusätzlich die aktuell geltende Übergangsfrist zu beachten.

Ihre Angaben

Unternehmen	
Ansprechperson	
Datum	

1. KI-Governance und Überblick

u. a. Art. 3, Art. 4 und Art. 26 AI Act; KI-MIG

Nr.	Prüffrage	Bewertung
1	★ Gibt es einen aktuellen Überblick über alle offiziell eingesetzten und geplanten KI-Systeme im Unternehmen?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
2	★ Ist nachvollziehbar geregelt, wer Entscheidungen über Einführung, Freigabe, Nutzung und wesentliche Änderungen von KI-Systemen vorbereitet bzw. trifft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
3	Werden auch nicht offiziell eingeführte KI-Anwendungen („Shadow AI“) regelmäßig erfasst oder thematisiert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
4	Gibt es einen regelmäßigen Prüfzyklus für KI-Systeme, offene Maßnahmen und relevante Änderungen?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
5	Sind wesentliche Nachweise, Entscheidungen und Prüfungen zentral auffindbar und aktuell?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

2. Anwendungszweck, Geltungsbereich und Rollen

u. a. Art. 2, Art. 3, Art. 25 und Art. 26 AI Act

Nr.	Prüffrage	Bewertung
6	★ Ist für jedes wesentliche KI-System der konkrete Verwendungszweck einschließlich Nutzerkreis und betroffener Prozesse dokumentiert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
7	★ Ist geprüft, ob die eingesetzte Lösung unter den Geltungsbereich und die Definition eines KI-Systems nach dem AI Act fällt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
8	★ Ist je Anwendung bestimmt, welche Rolle Ihr Unternehmen einnimmt, z. B. Anbieter, Betreiber, Importeur, Händler oder Produkthersteller?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
9	Ist geprüft, ob eine wesentliche Änderung, Zweckänderung oder Bereitstellung unter eigenem Namen die Rolle Ihres Unternehmens verändern kann?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
10	Sind betroffene Personen, Unternehmensbereiche, Schnittstellen und wesentliche Auswirkungen der Nutzung nachvollziehbar beschrieben?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

3. Verbotene KI-Praktiken

u. a. Art. 5 AI Act in der aktuell geltenden Fassung

Nr.	Prüffrage	Bewertung
11	★ Werden neue und bestehende KI-Anwendungen darauf geprüft, ob eine verbotene KI-Praxis vorliegen könnte?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
12	★ Sind besonders sensible Einsatzbereiche wie Manipulation, Ausnutzung von Schutzbedürftigkeit, Social Scoring oder unzulässige biometrische Nutzung ausdrücklich berücksichtigt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
13	★ Werden KI-Anwendungen im Beschäftigungs- oder Bildungsbereich auf verbotene Formen der Emotionserkennung geprüft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
14	Sind Mitarbeitende über für ihr Tätigkeitsfeld relevante verbotene Nutzungen informiert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

4. Risikoklassifizierung und Hochrisiko-Vorprüfung

u. a. Art. 6, Anhang I und Anhang III AI Act; Übergangsfristen beachten

Nr.	Prüffrage	Bewertung
15	★ Ist für jedes wesentliche KI-System dokumentiert, ob es als verboten, potenziell hochriskant, transparenzpflichtig oder sonstig einzuordnen ist?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
16	★ Wird bei möglichen Hochrisiko-Anwendungen systematisch geprüft, ob Anhang I oder Anhang III des AI Acts einschlägig sein kann?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
17	Ist bei potenziellen Hochrisiko-Systemen ein Umsetzungsplan vorhanden, der die aktuell geltenden Übergangsfristen berücksichtigt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
18	Ist bei bereits länger eingesetzten potenziellen Hochrisiko-Systemen geprüft, ob Übergangsregelungen oder wesentliche Änderungen relevant sind?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
19	Wird die Risikoeinordnung bei Änderungen von Zweck, Modell, Daten, Anbieter oder Einsatzkontext erneut geprüft und dokumentiert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

5. Transparenz und Kennzeichnung

u. a. Art. 50 AI Act; Transparenzpflichten seit 2. August 2026

Nr.	Prüffrage	Bewertung
20	★ Werden Personen darüber informiert, dass sie mit einem KI-System interagieren, soweit der AI Act dies verlangt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
21	★ Werden Deepfakes und sonstige KI-generierte oder manipulierte Bild-, Audio- oder Videoinhalte gekennzeichnet, soweit eine Kennzeichnungspflicht besteht?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
22	★ Wird bei KI-generierten oder manipulierten Texten zu Angelegenheiten von öffentlichem Interesse geprüft, ob eine Kennzeichnung erforderlich ist oder eine Ausnahme greift?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
23	Ist bei zulässiger Emotionserkennung oder biometrischer Kategorisierung geprüft, welche Informationspflichten gegenüber betroffenen Personen bestehen?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
24	Falls Ihr Unternehmen Anbieter eines generativen KI-Systems ist: Sind technische Maßnahmen zur maschinenlesbaren Erkennbarkeit KI-generierter Inhalte geprüft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

6. KI-Kompetenz, interne Regeln und Beschäftigte

u. a. Art. 4 AI Act; ggf. BetrVG und AGG

Nr.	Prüffrage	Bewertung
25	★ Werden geeignete Maßnahmen getroffen, um ausreichende KI-Kompetenz entsprechend Rolle, Erfahrung, Einsatzkontext und Risiken zu fördern?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
26	Ist klar kommuniziert, welche KI-Anwendungen und Verwendungszwecke im Unternehmen freigegeben sind?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
27	Ist verständlich geregelt, welche personenbezogenen, vertraulichen oder geschützten Informationen nicht in KI-Systeme eingegeben werden dürfen?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
28	Werden Schulungen, Unterweisungen oder andere Kompetenzmaßnahmen nachvollziehbar dokumentiert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
29	Wird bei mitarbeiterbezogenen KI-Systemen geprüft, ob Mitbestimmungs-, Gleichbehandlungs- oder weitere arbeitsrechtliche Anforderungen zu beachten sind?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

7. Datenschutz, Daten und Vertraulichkeit

u. a. DSGVO/BDSG; bei Hochrisiko-Systemen zusätzlich Art. 10 AI Act

Nr.	Prüffrage	Bewertung
30	★ Wird bei KI-Systemen mit personenbezogenen Daten gesondert geprüft, ob DSGVO und BDSG eingehalten werden, einschließlich Rechtsgrundlage und ggf. DSFA?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
31	Werden besondere Kategorien personenbezogener Daten und deren zulässige Verarbeitung gesondert geprüft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
32	Werden Herkunft, Eignung und Qualität von Eingabe-, Referenz- oder Trainingsdaten angemessen bewertet, soweit dies für den Einsatz relevant ist?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
33	★ Ist bekannt, ob Eingaben, Ausgaben oder hochgeladene Dateien durch den Anbieter gespeichert, weiterverwendet oder für Training genutzt werden?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
34	Sind Geschäftsgeheimnisse, vertrauliche Informationen und interne Dokumente durch geeignete Nutzungs- und Zugriffsvorgaben geschützt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

8. Anbieter, Verträge, Lieferkette und GPAI

u. a. Art. 25, Art. 26 und Art. 53–55 AI Act; je nach Rolle

Nr.	Prüffrage	Bewertung
35	★ Sind die wesentlichen KI-Anbieter und externen Dienstleister erfasst und vor Einsatz angemessen geprüft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
36	Werden Vertragsbedingungen, Datenverwendung, Unterauftragnehmer, Speicherorte, Sicherheitsangaben und wesentliche Änderungen berücksichtigt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
37	★ Stellt der Anbieter ausreichend Informationen und Dokumentation bereit, damit Ihr Unternehmen seine eigenen Pflichten erfüllen kann?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
38	Ist geprüft, ob Ihr Unternehmen selbst Anbieter eines KI-Modells mit allgemeinem Verwendungszweck (GPAI) ist oder ein solches Modell lediglich nutzt bzw. integriert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
39	Falls Ihr Unternehmen GPAI-Anbieter ist: Sind die einschlägigen Pflichten zu Dokumentation, Informationen für nachgelagerte Anbieter, Urheberrecht und öffentlicher Trainingsdaten-Zusammenfassung geprüft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

9. Menschliche Kontrolle, Qualität und Sicherheit

u. a. Art. 14, Art. 15 und Art. 26 AI Act; je nach Risikoklasse

Nr.	Prüffrage	Bewertung
40	★ Ist festgelegt, welche KI-Ergebnisse vor Verwendung, Veröffentlichung oder Entscheidung von einem Menschen geprüft werden müssen?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
41	Können die zuständigen Personen Grenzen und typische Fehler des Systems erkennen und Ergebnisse korrigieren, verwerfen oder die Nutzung stoppen?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
42	Werden Genauigkeit, Zuverlässigkeit und wiederkehrende Fehlermuster angemessen zum Einsatzbereich getestet?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
43	Werden Risiken wie Prompt Injection, unberechtigter Zugriff, Datenabfluss oder Manipulation der Eingaben und Ergebnisse berücksichtigt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
44	Gibt es bei Ausfall, unzuverlässigen Ergebnissen oder Sicherheitsproblemen einen praktikablen manuellen Ersatz- oder Eskalationsweg?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

10. Dokumentation, Protokollierung und Änderungen

u. a. Art. 12, Art. 18, Art. 26 und Art. 72 AI Act; je nach Rolle und Risikoklasse

Nr.	Prüffrage	Bewertung
45	★ Sind Zweck, Anbieter, Modell/Version, wesentliche Einstellungen, Nutzergruppen und Einsatzbereich je KI-System nachvollziehbar dokumentiert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
46	Werden wesentliche Tests, Entscheidungen, Freigaben, Einschränkungen und Änderungen nachvollziehbar festgehalten?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
47	Werden relevante Protokolle (Logs) aufbewahrt, soweit dies erforderlich oder angemessen ist, und mit Datenschutz- und Sicherheitsanforderungen abgestimmt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
48	★ Führt eine wesentliche Änderung von Anbieter, Modell, Zweck, Datenbasis oder Funktionsumfang zu einer erneuten Compliance-Prüfung?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

11. Vorbereitung auf besondere Hochrisiko-Pflichten

u. a. Art. 8–27, Art. 43 und Art. 49 AI Act; soweit zukünftig bzw. bereits anwendbar

Nr.	Prüffrage	Bewertung
49	Falls Ihr Unternehmen möglicher Anbieter eines Hochrisiko-Systems ist: Sind Anforderungen wie Risikomanagement, Daten-Governance, technische Dokumentation, Protokollierung, Transparenz, menschliche Aufsicht, Genauigkeit, Robustheit und Cybersicherheit eingeplant?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
50	★ Falls Ihr Unternehmen möglicher Betreiber eines Hochrisiko-Systems ist: Sind künftige Betreiberpflichten wie Nutzung nach Anleitung, menschliche Aufsicht, geeignete Eingabedaten, Überwachung und Protokollaufbewahrung vorbereitet?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
51	Ist geprüft, ob für den konkreten Einsatz eine Grundrechte-Folgenabschätzung nach Art. 27 AI Act erforderlich werden kann?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
52	Ist bei möglichen Registrierungs-, Konformitätsbewertungs- oder Meldepflichten geklärt, welche Schritte und Fristen künftig relevant sind?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

12. Überwachung, Vorfälle und Beschwerden

u. a. Art. 26, Art. 72, Art. 73 und Aufsichtsregelungen des AI Acts

Nr.	Prüffrage	Bewertung
53	★ Gibt es einen bekannten internen Meldeweg für erhebliche KI-Fehler, schädliche Ausgaben, Sicherheitsvorfälle oder vermutete Rechtsverstöße?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
54	Werden relevante Vorfälle bewertet, dokumentiert und bei Bedarf an Anbieter, zuständige Stellen oder andere interne Funktionen eskaliert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
55	Werden Beschwerden und Rückmeldungen von Mitarbeitenden, Kunden oder anderen Betroffenen erfasst und für Verbesserungen genutzt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

13. Regelmäßige Überprüfung und Nachweisführung

u. a. Art. 4, Art. 26 und Rechenschafts-/Governance-Anforderungen; je nach Rolle

Nr.	Prüffrage	Bewertung
56	★ Werden KI-Compliance-Maßnahmen regelmäßig überprüft und bei Änderungen von Recht, Systemen, Anbietern oder Nutzung angepasst?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
57	Sind zentrale Nachweise wie KI-Inventar, Rollen- und Risikoeinordnung, Anbieterprüfungen, Richtlinien, Schulungsnachweise, Freigaben und Vorfälle aktuell und auffindbar?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
58	Erhält die Unternehmensleitung einen verständlichen Überblick über wesentliche KI-Risiken, offene Maßnahmen und relevante Änderungen?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

Schnellauswertung

Betrachten Sie nicht nur die Anzahl der Markierungen, sondern vor allem die Kernfragen (★) und die Themenbereiche, in denen mehrere Punkte „Teilweise / unklar“ oder „Nein“ markiert wurden. Nicht relevante Fragen werden bei der Gesamteinschätzung nicht negativ gewertet.

GRÜN	**Gute Grundlage** Die wesentlichen KI-Systeme sind bekannt und die aktuell relevanten Pflichten sind überwiegend adressiert. Einzelne offene Punkte gezielt prüfen und den Stand regelmäßig aktualisieren.
GELB	**Verbesserungsbedarf** Mehrere Punkte sind nur teilweise geklärt oder Nachweise fehlen. Prioritäten festlegen und insbesondere Rollen, aktuelle Transparenzpflichten, interne Regeln und Anbieterprüfung nachziehen.
ORANGE	**Deutlicher Handlungsbedarf** Mindestens eine wichtige Kernfrage ist mit „Nein“ beantwortet oder mehrere KI-Systeme sind nicht vollständig erfasst bzw. eingeordnet. Eine strukturierte AI-Compliance-Prüfung und ein Maßnahmenplan sind sinnvoll.
ROT	**Zeitnah prüfen** Mehrere Kernfragen sind offen, verbotene oder transparenzpflichtige Nutzungen sind nicht geprüft oder grundlegende Rollen-, Risiko- und Nachweisdokumentationen fehlen. AI Compliance sollte zeitnah systematisch überprüft werden.

Ihre wichtigsten nächsten Schritte

1. _____
2. _____
3. _____
4. _____
5. _____

Kernfragen mit „Nein“ oder „unklar“

- _____
- _____
- _____

Wo steht Ihre AI Compliance heute?

Wenn der Schnellcheck offene Punkte zeigt, können Sie die Ergebnisse im ANDLIS-Orientierungsgespräch einordnen lassen. Sie erhalten eine verständliche erste Einschätzung, bevor Sie über weitere Schritte entscheiden.

Kein Verkaufsgespräch. Sondern Klarheit für Ihre nächsten Entscheidungen.

Hinweise zur Verwendung

Diese Checkliste ist eine allgemeine Arbeitshilfe zur ersten Orientierung. Sie erhebt keinen Anspruch auf Vollständigkeit für jede Branche, Rolle oder KI-Anwendung und ersetzt weder die rechtliche Prüfung des konkreten Einzelfalls noch eine vollständige Risikoklassifizierung, Konformitätsbewertung oder Zertifizierung.

Welche Pflichten gelten, hängt insbesondere von der Rolle Ihres Unternehmens, dem Verwendungszweck, der Risikoklasse, dem Einsatzgebiet, den betroffenen Personen, den verarbeiteten Daten und ggf. produktspezifischen oder branchenspezifischen Regelungen ab. Fragen zu Hochrisiko-Systemen können daher mit „N. r.“ beantwortet werden, wenn diese Einordnung für Ihr Unternehmen nachweislich nicht einschlägig ist.

Anwendungsstand des EU AI Acts – Stand 17. August 2026

• Die Verordnung (EU) 2024/1689 (AI Act) gilt in wesentlichen Teilen seit 2. August 2026.

• Verbotene KI-Praktiken gelten bereits seit 2. Februar 2025; die Regeln zu GPAI-Modellen gelten grundsätzlich seit 2. August 2025.

• Die Transparenzpflichten nach Art. 50 gelten seit 2. August 2026.

• Durch die Verordnung (EU) 2026/1744 (AI Omnibus) gelten die Hochrisiko-Regeln für Anhang-III-Systeme ab 2. Dezember 2027 und für in regulierte Produkte nach Anhang I eingebettete Systeme ab 2. August 2028.

• Die Verordnung (EU) 2026/1744 hat außerdem u. a. Art. 4 zur KI-Kompetenz angepasst. Die jeweils aktuelle konsolidierte Fassung des AI Acts ist maßgeblich.

Rechtsgrundlagen – Auswahl

• Verordnung (EU) 2024/1689 über künstliche Intelligenz (AI Act), in der aktuell geltenden Fassung

• Verordnung (EU) 2026/1744 (Digital Omnibus on AI / AI Omnibus)

• Gesetz zur Marktüberwachung und Innovationsförderung von künstlicher Intelligenz (KI-Marktüberwachungs-und-Innovationsförderungs-Gesetz - KI-MIG)

• Datenschutz-Grundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG), soweit personenbezogene Daten betroffen sind

• Je nach Einsatz zusätzlich z. B. Betriebsverfassungsgesetz (BetrVG), Allgemeines Gleichbehandlungsgesetz (AGG), Urheberrecht, Geschäftsgeheimnisschutz, Cybersicherheits- und produktspezifische Regelungen

Normen und fachliche Standards – Auswahl

Normen sind nicht automatisch gesetzlich verbindlich. Je nach Unternehmen, System und Nachweisziel können sie jedoch als fachlicher Orientierungsrahmen, für Managementsysteme, Risikoanalysen, Informationssicherheit oder Audits relevant sein.

• ISO/IEC 42001 – Managementsysteme für künstliche Intelligenz
• ISO/IEC 23894 – Risikomanagement für künstliche Intelligenz
• ISO/IEC 22989 – Begriffe und Konzepte der künstlichen Intelligenz
• ISO/IEC 23053 und ISO/IEC 5338 – Rahmen bzw. Lebenszyklusprozesse für KI-Systeme
• ISO/IEC 27001 / 27002 – Informationssicherheitsmanagement und Sicherheitsmaßnahmen
• ISO/IEC 27701 – Datenschutz-Informationsmanagement; ISO 31000 – Risikomanagement

Wichtige Themen in diesem Schnellcheck

KI-Inventar und Rollen · verbotene KI-Praktiken · Risikoklassifizierung · Transparenz und Kennzeichnung · KI-Kompetenz · Datenschutz und Vertraulichkeit · Anbieter- und GPAI-Prüfung · menschliche Kontrolle · Qualität und Sicherheit · Dokumentation und Änderungen · Hochrisiko-Vorbereitung · Vorfälle und regelmäßige Überprüfung.

Stand: 17.08.2026