



HANDOUT · BETEILIGUNG UND KÜNSTLICHE INTELLIGENZ

EU AI Act kompakt.

Handout für Mitarbeitende und Führungskräfte. Praxiswissen für einen informierten, verantwortungsvollen und organisationsbezogenen Umgang mit KI.

BE:KI Schulungsmodul

270 Minuten

Stand: 05.10.2026

Version 1.0

1. Worum geht es?

Der EU AI Act reguliert künstliche Intelligenz risikobasiert. Für die betriebliche Praxis ist entscheidend, **welches System** für **welchen Zweck** eingesetzt wird, **welche Rolle** die Organisation dabei hat und **welche Personen** von den Ergebnissen betroffen sind. [1][2]



Typische Rolle der Organisation

Wer ein fremdes KI-System unter eigener Aufsicht beruflich nutzt, ist regelmäßig **Betreiber** im Sinne des AI Acts. Einzelne Mitarbeitende werden dadurch nicht automatisch selbst zu Betreibern. [2]

Wichtig

Ein allgemein verwendbares KI-System ist nicht allein deshalb „Hochrisiko-KI“. Maßgeblich sind insbesondere Zweckbestimmung, Einsatzgebiet und gesetzliche Kriterien. [1][2]

Die fünf Fragen für jede KI-Anwendung

- 1 Was soll das System konkret tun?
- 2 Welche Daten werden verarbeitet?
- 3 Welche Menschen sind von Ergebnissen betroffen?
- 4 Welche Folgen kann ein Fehler haben?
- 5 Wer prüft, entscheidet und trägt Verantwortung?

Quellen: [1] Verordnung (EU) 2024/1689, konsolidierte Fassung 27.07.2026. [2] Bundesnetzagentur, „Akteure und Pflichten“.

2. KI-Kompetenz nach Art. 4 AI Act

Art. 4 verpflichtet Anbieter und Betreiber, Maßnahmen zu ergreifen, die die Entwicklung von KI-Kompetenz bei Beschäftigten und weiteren Personen unterstützen, die in ihrem Auftrag mit KI-Systemen arbeiten. Dabei sind technisches Wissen, Erfahrung, Ausbildung, der Einsatzkontext und die betroffenen Personengruppen zu berücksichtigen. Ein bestimmtes individuelles Kompetenzniveau muss nicht garantiert werden. [1]

KI-Kompetenz bedeutet mehr als Bedienwissen: KI verstehen, Chancen nutzen, Grenzen erkennen, Ergebnisse kritisch prüfen, Risiken einschätzen und Verantwortung übernehmen. Die Definition der KI-Kompetenz im AI Act stellt auf informierte Nutzung sowie Bewusstsein für Chancen, Risiken und mögliche Schäden ab. [1]

Verstehen

Was kann das System? Was kann es nicht? Wie entstehen typische Fehler?

Anwenden

Welche Aufgaben sind geeignet? Welche Daten dürfen verwendet werden?

Prüfen

Sind Fakten, Quellen, Schlussfolgerungen und Bewertungen tragfähig?

Einordnen

Welche Risiken entstehen im konkreten Einsatzkontext?

Verantworten

Wer trifft die Entscheidung und kann sie fachlich vertreten?

Aktualisieren

Kompetenz muss mit Technik und Nutzungspraxis weiterentwickelt werden. [3]

Was Art. 4 nicht vorgibt

- keine einheitliche Mindeststundenzahl,
- keinen standardisierten Einheitskurs,
- keine verpflichtende externe Zertifizierung der Schulungsmaßnahme,
- kein zu garantierendes Kompetenzniveau jeder einzelnen Person. [3]

Quellen: [1] Art. 3 Nr. 56 und Art. 4 AI Act, konsolidierte Fassung 27.07.2026. [3] Bundesnetzagentur, „KI-Kompetenz“.

3. Risikoorientierung: die BE:KI-Ampel

Die Ampel ist eine **didaktische Orientierung**, keine amtliche Klassifikation. Die Bundesnetzagentur weist darauf hin, dass Risikostufen und Pflichten sich nicht zwingend gegenseitig ausschließen und kumulativ relevant sein können. [2]

ROT

Verbotene Praktiken

Bestimmte KI-Praktiken sind nach Art. 5 unzulässig. Dazu gehören unter den jeweiligen gesetzlichen Voraussetzungen etwa bestimmte manipulative Anwendungen sowie bestimmte Formen biometrischer oder emotionsbezogener Nutzung. Emotionserkennung am Arbeitsplatz ist grundsätzlich verboten, soweit keine gesetzliche Ausnahme greift. [1]

ORANGE

Hochrisiko / besonders reguliert

Bestimmte Systeme in sensiblen Bereichen können Hochrisiko-KI sein, beispielsweise bestimmte Anwendungen bei Einstellung, Personalauswahl, Entscheidungen über Arbeitsbedingungen, Beförderung oder Beendigung von Beschäftigungsverhältnissen. [1]

GELB

Transparenz- und besondere Informationspflichten

Art. 50 enthält Pflichten für bestimmte interaktive und generative Systeme, etwa hinsichtlich der Information über KI-Interaktion und bestimmter synthetischer oder manipulierter Inhalte. [1][4]

GRÜN

Allgemeine Anwendungen

Textentwürfe, Strukturierung, Brainstorming oder Zusammenfassungen können regelmäßig geringere AI-Act-Risiken aufweisen. Datenschutz, Vertraulichkeit, Urheberrecht, fachliche Qualität und interne Regeln bleiben dennoch zu beachten.

Praxisbeispiele

ANWENDUNG	ERSTE EINORDNUNG	WAS IST ZU PRÜFEN?
KI erstellt Einladungstext	regelmäßig niedrigeres Risiko	Daten, Qualität, Freigabe
KI rankt Bewerbungen	Hochrisiko-Prüfung naheliegend	Anhang III, Human Oversight, Datenschutz, Beteiligung
KI erkennt „Motivation“ aus Stimme/Gesicht	sehr kritische / möglicherweise verbotene Nutzung	Art. 5, Zweck und Ausnahmen
öffentlicher KI-Chatbot	Transparenzrelevanz	Art. 50, Daten, Fehlerrisiken

Quellen: [1] Art. 5, Anhang III und Art. 50 AI Act. [2] Bundesnetzagentur, „Akteure und Pflichten“. [4] Europäische Kommission, Leitlinien-/Informationsstand zu Art. 50.

4. Human Oversight: Menschliche Kontrolle muss wirksam sein

Bei Hochrisiko-KI müssen Betreiber geeignete natürliche Personen mit erforderlicher Kompetenz, Ausbildung und Befugnis für die menschliche Aufsicht einsetzen. Die Aufsicht soll nicht nur formal bestehen, sondern **tatsächlich ein Eingreifen ermöglichen**. [1][2]

Eingabe prüfen → KI einsetzen → Ergebnis prüfen → Entscheidung verantworten

Keine wirksame Kontrolle

- „Die KI wird schon recht haben.“
- Output wird wegen Zeitdruck automatisch übernommen.
- Die kontrollierende Person versteht das System nicht.
- Es gibt keine Möglichkeit, das Ergebnis zu verwerfen.

Wirksame Kontrolle

- Zweck und Grenzen sind bekannt.
- Daten und Fehlerquellen werden berücksichtigt.
- Ergebnisse werden fachlich geprüft.
- Menschen können stoppen, korrigieren oder nicht verwenden.
- Die Entscheidung bleibt nachvollziehbar verantwortet.

Selbstcheck vor einer Entscheidung

- ☐ Würde dieselbe Entscheidung auch ohne den KI-Output fachlich begründet werden können?
- ☐ Ist nachvollziehbar, welche Informationen die KI verwendet hat?
- ☐ Sind offensichtliche Lücken, Verzerrungen oder falsche Tatsachen ausgeschlossen?
- ☐ Ist klar, wer die Verantwortung für die Entscheidung trägt?

Quellen: [1] AI Act, insbesondere Art. 14 und Art. 26. [2] Bundesnetzagentur, „Akteure und Pflichten“.

5. Praktische Regeln für Mitarbeitende

Vor der Eingabe

- Ist das verwendete System dienstlich freigegeben?
- Dürfen die Daten in dieses System?
- Kann die Aufgabe anonymisiert oder abstrahiert werden?
- Ist KI für diese Aufgabe überhaupt sinnvoll?

Nach der Ausgabe

- Fakten prüfen.
- Quellen tatsächlich öffnen und kontrollieren.
- Fehlenden Kontext ergänzen.
- Bewertungen und Stereotype hinterfragen.
- Endergebnis selbst verantworten.

Datenampel

GRÜN	GELB	ROT / FREIGABE ERFORDERLICH
öffentliche Informationen fiktive Beispiele allgemeine Formulierungen	interne Konzepte nicht öffentliche Arbeitsabläufe interne Kennzahlen	Personalakten Gesundheits- oder Sozialdaten Klient:innendaten Zugangsdaten Geschäftsgeheimnisse

Die Ampel ersetzt keine Datenschutz- oder Informationsschutzprüfung. Entscheidend sind das konkrete System, seine Vertrags- und Datenschutzeinstellungen, die Rechtsgrundlage und interne Vorgaben.

Wenn etwas schiefgeht

Fehlerhafte oder problematische KI-Nutzung sollte nicht „still korrigiert“ werden, wenn daraus relevante Risiken entstehen. Interne Meldewege, Datenschutz, Informationssicherheit oder zuständige Führung sind entsprechend der Organisationsregelung einzubeziehen.

6. Zusätzliche Verantwortung von Führungskräften

Führung bedeutet beim KI-Einsatz nicht, jede technische Einzelheit selbst zu beherrschen. Erforderlich ist, dass der Einsatz **organisiert, begrenzt, nachvollziehbar und kompetent begleitet** wird.

1. Nutzung sichtbar machen

Welche KI-Systeme werden tatsächlich verwendet – offiziell und informell?

2. Zweck definieren

Welche Aufgaben darf ein System unterstützen, welche nicht?

3. Verantwortung zuordnen

Wer gibt frei, wer beaufsichtigt, wer entscheidet bei Vorfällen?

4. Kompetenz organisieren

Schulungstiefe an Rolle, Risiko, System und Betroffenheit ausrichten. [1][3]

5. Beteiligung sichern

Datenschutz, IT, Informationssicherheit und Interessenvertretung frühzeitig einbeziehen.

6. Nutzung überprüfen

Regeln, Systeme und Schulungsbedarf regelmäßig an tatsächliche Praxis und technische Entwicklung anpassen. [3]

Führungskräfte-Check vor Freigabe

- ☐ Der konkrete Use Case ist beschrieben.
- ☐ Die Rolle der Organisation im AI Act ist geklärt.
- ☐ Risikoeinstufung und verbotene Praktiken wurden geprüft.
- ☐ Daten- und Berechtigungskonzept sind geklärt.
- ☐ Menschliche Aufsicht ist praktisch umsetzbar.
- ☐ Beschäftigte verfügen über passende KI-Kompetenz.
- ☐ Beteiligungs- und Mitbestimmungsfragen wurden geprüft.
- ☐ Evaluation und Vorfallsmeldung sind geregelt.

Quellen: [1] Art. 4 und Betreiberpflichten des AI Acts. [2] Bundesnetzagentur, „Akteure und Pflichten“. [3] Bundesnetzagentur, „KI-Kompetenz“.

7. Der BE:KI 10-Fragen-Check für neue KI-Anwendungen

- 1 **System:** Welches KI-System soll eingesetzt werden?
- 2 **Zweck:** Welche konkrete Aufgabe soll es übernehmen?
- 3 **Rolle:** Ist die Organisation Anbieter, Betreiber oder in einer anderen Rolle?
- 4 **Daten:** Welche Daten werden verarbeitet?
- 5 **Betroffene:** Wer kann durch Ergebnisse oder Entscheidungen betroffen sein?
- 6 **Risiko:** Welche Fehler, Schäden oder Grundrechtsauswirkungen sind realistisch?
- 7 **Recht:** Welche AI-Act-, Datenschutz- und sonstigen Anforderungen greifen?
- 8 **Beteiligung:** Welche internen Stellen und Interessenvertretungen müssen eingebunden werden?
- 9 **Verantwortung:** Wer kontrolliert, entscheidet, dokumentiert und stoppt bei Bedarf?
- 10 **Kompetenz:** Welche Kenntnisse benötigen die Nutzenden vor dem Einsatz?

Grundsatz: Ein KI-System kann mehrere Use Cases haben. Jeder Use Case kann eine andere Risikoeinstufung und andere Anforderungen auslösen. Ein Textassistent und eine personenbezogene Entscheidungsunterstützung sind deshalb nicht als derselbe Anwendungsfall zu behandeln.

8. Fall zur Selbstanwendung

Situation: Eine Organisation führt einen KI-Assistenten ein. Er kann Texte erstellen, interne Dokumente durchsuchen, Sitzungen zusammenfassen und Beschäftigte bei fachlichen Entscheidungen unterstützen. Perspektivisch sollen auch personenbezogene Informationen verarbeitet werden.

PRÜFFELD	EIGENE NOTIZEN
Zweck / Nutzen	
Daten	
betroffene Personen	
Risiken / sensible Funktionen	
Transparenz	
menschliche Kontrolle	
Beteiligung / Mitbestimmung	
KI-Kompetenz	
Freigabe / Verantwortung	
Evaluation / Vorfälle	

9. Die fünf Merksätze

1

Der AI Act reguliert KI **risiko- und rollenbezogen**.

2

Art. 4 verlangt geeignete Maßnahmen zur **Unterstützung der KI-Kompetenz**, keinen Einheitskurs. [1][3]

3

Je stärker KI Menschen bewertet oder Entscheidungen beeinflusst, desto höher ist der **Prüfbedarf**.

4

Menschliche Aufsicht muss **wirksam** sein und tatsächliches Eingreifen ermöglichen. [1][2]

5

Verantwortliche KI-Governance verbindet **Technik, Recht, Datenschutz, Organisation, Kompetenz und Beteiligung**.

10. Quellen und Rechtsstand

[1] Europäische Union: Verordnung (EU) 2024/1689 über künstliche Intelligenz (Artificial Intelligence Act), konsolidierte Fassung vom 27.07.2026. EUR-Lex: eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng

[2] Bundesnetzagentur: *Akteure und Pflichten* zur KI-Verordnung. bundesnetzagentur.de – Akteure und Pflichten

[3] Bundesnetzagentur: *KI-Kompetenz*. Hinweise zu Art. 4, Kontextbezug, fehlender Standardisierung und fehlender Zertifizierungspflicht. bundesnetzagentur.de – KI-Kompetenz

[4] Europäische Kommission: Informationen und Leitlinienentwicklung zu den Transparenzpflichten nach Art. 50 AI Act. digital-strategy.ec.europa.eu – Article 50

[5] Europäische Kommission: *AI Literacy – Questions & Answers*. digital-strategy.ec.europa.eu – AI Literacy Q&A

Dieses Handout dient der Schulung und ersten betrieblichen Orientierung. Es ersetzt keine rechtliche Einzelfallprüfung. Bei konkreten KI-Einführungen können je nach System und Einsatzkontext insbesondere zusätzliche Anforderungen aus Datenschutzrecht, Arbeits- bzw. Mitarbeitervertretungsrecht, Informationssicherheit und Fachrecht relevant sein.