

EU AI ACT & SCHWEIZER KI-REGULIERUNG

Neue Entwicklungen, Pflichten
und Handlungsempfehlungen
für Unternehmen & Bildungsanbieter



RECHTSSICHER
HANDELN



COMPLIANCE
SICHERN



BILDUNG
GESTALTEN



VERTRAUEN
SCHAFFEN



AKTUELLE ENTWICKLUNGEN
JULI 2026

inkl. AI Omnibus &
neue Leitlinien zu Art. 50 AI Act



AI COMPLIANT

- ☒ TRANSPARENZ
- ☒ SICHERHEIT
- ☒ DATENSCHUTZ
- ☒ MENSCHENZENTRIERT



DOKUMENTATION & PRAXISLEITFADEN

Faktencheck – Kritikmodus – Gegenargumente – Vorgehensrichtlinien – Checklisten

Impressum

EU AI Act und Schweizer KI-Regulierung

Fachpublikation für Unterricht und Selbststudium

Autor

Henri J.P. Jendly

© 2026 Henri J.P. Jendly

Alle Rechte vorbehalten.



Urheberrecht

Dieses Werk einschliesslich aller Texte, Abbildungen, Tabellen, Beispiele, Aufgaben und Lösungen ist urheberrechtlich geschützt. Jede Nutzung ausserhalb der gesetzlichen Bestimmungen bedarf der vorherigen schriftlichen Zustimmung des Rechteinhabers. Dies gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Veröffentlichungen sowie für die Speicherung, Verarbeitung und Weitergabe in elektronischen Systemen.

Fachliche Hinweise

Die Inhalte wurden mit grosser Sorgfalt und nach dem zum Zeitpunkt der Veröffentlichung verfügbaren Informations-, Technik- und Rechtsstand erstellt. Gesetzliche Bestimmungen, behördliche Vorgaben, technische Standards sowie Funktionen und Nutzungsbedingungen der erwähnten Systeme können sich ändern. Trotz sorgfältiger Prüfung können Fehler oder Unvollständigkeiten nicht vollständig ausgeschlossen werden.

Diese Publikation dient der fachlichen Information, dem Unterricht und dem Selbststudium. Es stellt keine individuelle Rechtsberatung dar. Bei rechtlich, datenschutzrechtlich oder technisch relevanten Anwendungsfällen sind die aktuellen Rechtsgrundlagen zu prüfen und bei Bedarf qualifizierte Fachpersonen beizuziehen.

Haftungsausschluss

Die enthaltenen Informationen, Programme, Beispiele, Vorlagen, Checklisten und Übungsaufgaben dienen ausschliesslich Lern- und Demonstrationszwecken. Ihre Anwendung in realen Organisationen oder produktiven Systemen erfolgt in eigener Verantwortung. Der Autor übernimmt, soweit gesetzlich zulässig, keine Haftung für Schäden, Datenverluste, Betriebsunterbrüche oder andere Nachteile, die aus der Nutzung oder fehlerhaften Interpretation der Inhalte entstehen.

Software- und Markenhinweise

Die Nennung von Produktnamen, Unternehmen, Plattformen, Software und Marken dient ausschliesslich der fachlichen Beschreibung. Sämtliche Bezeichnungen können geschützte Marken oder Kennzeichen der jeweiligen Rechteinhaber sein.

DIGIPLAN365 ist eine Marke der ICTlearn GmbH.

Übersicht

1	Management Summary	4
2	Ausgangsartikel: These, Belege und Aufbau	6
3	Faktencheck des Ausgangsartikels	6
4	Kritikmodus und Red-Team-Analyse	9
5	Sachlich überarbeitete Kernaussage des Artikels	11
6	EU AI Act im Einsteiger-Modus	12
7	Artikel 4: KI-Kompetenz systematisch umsetzen	15
8	Artikel 50: Transparenz und Kennzeichnung	16
9	Hochrisiko-KI im Bildungsbereich	17
10	Schweizer Rechtslage	18
11	Schritt-für-Schritt-Vorgehen für Organisationen	19
12	KI-Agenten und technische Sicherheit	23
13	Vorgehensrichtlinien für Schulen und Bildungsanbieter	24
14	Dokumentation und Nachweisführung	25
15	Empfohlene Einführungsplanung	26
16	Quellen und weiterführende Informationen	27
17	Anhang: Checklisten	29



EU AI Act und Schweizer KI-Regulierung

Ausgangslage: Analyse des LinkedIn-Artikels «KI-News für Unternehmen der DACH-Region – KW 31 / 27.07.2026» und Ableitung konkreter Vorgehensrichtlinien für Unternehmen, Schulen und Bildungsanbieter.

Dokumentationszweck

Diese Dokumentation verbindet eine kritische Prüfung des Ausgangsartikels mit einer verständlichen Einführung in den EU AI Act, einer Einordnung der Schweizer Rechtslage und einem umsetzbaren Vorgehensmodell. Sie ist als Arbeitsgrundlage für Geschäftsleitungen, Schulleitungen, Datenschutzverantwortliche, IT-Verantwortliche, Dozenten und Projektleitende konzipiert.

Die Darstellung trennt bewusst zwischen verbindlichem Recht, behördlichen Leitlinien, empirischen Befunden, fachlicher Interpretation und Handlungsempfehlungen. Sie ersetzt keine Rechtsberatung für einen konkreten Einzelfall.

1 Management Summary

Kernaussagen

- ▶ Der LinkedIn-Artikel erkennt den regulatorischen Handlungsbedarf grundsätzlich richtig, vermischt jedoch Rechtsinformation, zugespitzte Warnung, Studienergebnisse und eigene Verkaufsangebote.
- ▶ Artikel 4 des EU AI Acts verpflichtet Anbieter und Betreiber seit dem 2. Februar 2025 zu angemessenen Massnahmen für KI-Kompetenz. Eine bestimmte Zertifizierung, Mindeststundenzahl oder ein formeller AI Officer sind nicht allgemein vorgeschrieben.
- ▶ Ab dem 2. August 2026 gelten wesentliche Transparenzpflichten nach Artikel 50. Sie betreffen insbesondere die Interaktion mit KI-Systemen, Deepfakes, bestimmte KI-generierte Veröffentlichungen sowie technische Kennzeichnungen synthetischer Inhalte.
- ▶ Die Aufsichts- und Durchsetzungsregeln für Artikel 4 greifen ab dem 3. August 2026. Dies bedeutet keine flächendeckende Sofortkontrolle aller Unternehmen, sondern eine risikobasierte und anlassbezogene Marktaufsicht.
- ▶ Die Pflichten für eigenständige Hochrisiko-KI-Systeme gelten nach dem Digital Omnibus spätestens ab dem 2. Dezember 2027; für in regulierte Produkte integrierte Hochrisiko-Systeme spätestens ab dem 2. August 2028.
- ▶ Die Schweiz besitzt derzeit keine umfassende KI-Spezialgesetzgebung. Das revidierte Datenschutzgesetz und weitere bestehende Rechtsgebiete gelten jedoch bereits. Bis Ende 2026 wird eine Vernehmlassungsvorlage zur Umsetzung der KI-Konvention des Europarats vorbereitet.
- ▶ Für die Praxis gilt: zuerst inventarisieren, dann Verwendungszweck und Rolle bestimmen, Risiken klassifizieren, Daten und Anbieter prüfen, menschliche Kontrolle festlegen, Mitarbeitende qualifizieren und alles angemessen dokumentieren.



Gesamtbewertung des Ausgangsartikels

Prüfdimension	Bewertung	Begründung
Relevanz	hoch	Die behandelten Themen betreffen Unternehmen und Bildungsanbieter unmittelbar.
Faktenbasis	überwiegend korrekt	Zentrale Fristen und Entwicklungen sind real, einzelne Zahlen werden jedoch verkürzt oder vermischt.
Rechtliche Präzision	mittel	Höchstbussen, Aufsicht und Nachweispflichten werden teilweise dramatisiert.
Logische Stringenz	mittel	Aus gesetzlichen Pflichten wird zu rasch ein zwingender Bedarf an konkreten Kurs- und Beratungsangeboten abgeleitet.
Transparenz über Interessen	unzureichend	Nachrichten, Fachanalyse und Eigenwerbung sind nicht deutlich voneinander getrennt.
Praxisnutzen	gut als Warnsignal	Als Compliance-Leitfaden reicht der Beitrag allein nicht aus.



2 Ausgangsartikel: These, Belege und Aufbau

2.1 Zentrale These

Der Ausgangsartikel vertritt sinngemäss die These, dass KI in der Wirtschaft rasch an Bedeutung gewinnt, während viele Unternehmen regulatorisch, organisatorisch und personell nicht ausreichend vorbereitet sind. Aus dem EU AI Act, der wachsenden KI-Nutzung und neuen Sicherheitsrisiken wird ein unmittelbarer Bedarf an Compliance-Checks, Governance, Schulungen und technischer Absicherung abgeleitet.

2.2 Vom Artikel angeführte Belege

- ▶ Umsetzungsfristen und neue Aufsichtsmechanismen des EU AI Acts.
- ▶ Transparenzpflichten für Chatbots und KI-generierte oder manipulierte Inhalte.
- ▶ Mögliche Höchstbussen bei bestimmten Verstössen.
- ▶ Studien zur Verbreitung generativer KI und zum Weiterbildungsbedarf in Unternehmen.
- ▶ Eine Studie zu KI-gestützten Innovationen und wirtschaftlichen Umsätzen.
- ▶ Ein Sicherheitsvorfall während einer Modellevaluation von OpenAI und Hugging Face.
- ▶ Studien zu Produktivitäts- und Lohnprämien bei verlangten KI-Kompetenzen.

2.3 Argumentationsstruktur

1. KI wird in Unternehmen schnell verbreitet eingesetzt.
2. Die Kompetenzen und Kontrollsysteme halten mit der Nutzung nicht Schritt.
3. Der EU AI Act macht unzureichende Vorbereitung zu einem Compliance-Risiko.
4. Sicherheitsvorfälle zeigen zusätzliche technische und organisatorische Gefahren.
5. Unternehmen benötigen deshalb Schulungen, Governance, Compliance-Checks und sichere KI-Agenten.
6. Die im Beitrag beworbenen Angebote sollen diese Lücken schliessen.

Diese Argumentationskette ist im Grundsatz plausibel. Sie wird jedoch dort problematisch, wo aus allgemeinen Pflichten oder statistischen Zusammenhängen ein zwingender Bedarf an einem bestimmten kommerziellen Angebot abgeleitet wird.

3 Faktencheck des Ausgangsartikels

3.1 AI Act, Digital Omnibus und Fristen

Der AI Act trat am 1. August 2024 in Kraft. Die ersten Vorschriften, darunter die Verbote bestimmter KI-Praktiken, Definitionen und Artikel 4 zur KI-Kompetenz, gelten seit dem 2. Februar 2025. Governance-Regeln und Pflichten für General-Purpose-AI-Modelle gelten seit dem 2. August 2025. Der überwiegende Teil des Regelwerks wird ab dem 2. August 2026 anwendbar.

Der im Juni 2026 angenommene Digital Omnibus verschob die umfassenden Pflichten für Hochrisiko-Systeme. Für eigenständige Hochrisiko-Systeme nach Anhang III, darunter Anwendungen in Bildung und Personalwesen, gilt als spätestster Termin der 2. Dezember 2027. Für Hochrisiko-Systeme, die Bestandteil regulierter Produkte sind, gilt spätestens der 2. August 2028.



Bewertung

Die Aussage des Artikels ist im Kern korrekt. Eine Verschiebung der Hochrisiko-Pflichten bedeutet jedoch keinen rechtsfreien Zeitraum: Verbote, KI-Kompetenz, Datenschutz, Informationssicherheit, Vertragsrecht, Arbeitsrecht und weitere anwendbare Vorschriften gelten bereits.

3.2 Aufsicht ab August 2026

Die Aufsichts- und Durchsetzungsregeln für Artikel 4 werden ab dem 3. August 2026 anwendbar. Nationale Marktüberwachungsbehörden können Beschwerden bearbeiten, Informationen und Unterlagen verlangen, Untersuchungen einleiten und bei Verstössen Massnahmen anordnen.

Die Aussage, ab August werde jedes Unternehmen aktiv kontrolliert, wäre jedoch irreführend. Marktaufsicht erfolgt üblicherweise risikobasiert, anlassbezogen, aufgrund von Beschwerden, Vorfällen oder Stichproben. In Deutschland ist zudem ein Mehrbehördenmodell relevant; Zuständigkeiten können je nach Sektor und Anwendung verteilt sein.

3.3 Transparenzpflichten nach Artikel 50

Ab dem 2. August 2026 greifen Transparenzpflichten für bestimmte KI-Systeme und Inhalte. Menschen müssen grundsätzlich informiert werden, wenn sie mit einem KI-System interagieren, sofern dies nicht bereits offensichtlich ist. Anbieter generativer Systeme müssen maschinenlesbare Markierungen ermöglichen. Betreiber müssen insbesondere Deepfakes, bestimmte KI-generierte Veröffentlichungen zu Themen von öffentlichem Interesse sowie den Einsatz von Emotionserkennung oder biometrischer Kategorisierung offenlegen.

Nicht jeder intern mit KI vorbereitete Text muss pauschal sichtbar gekennzeichnet werden. Entscheidend sind der konkrete Anwendungsfall, die Art des Inhalts, die Veröffentlichung und das Ausmass wirksamer menschlicher redaktioneller Kontrolle.

3.4 Bussen und Sanktionen

Der Artikel nennt mögliche Höchstbussen bis 15 Millionen Euro oder 3 Prozent des weltweiten Jahresumsatzes für bestimmte Verstösse. Diese Grössenordnungen sind als gesetzliche Maximalwerte einzuordnen, nicht als automatische oder typische Sanktion für jedes Unternehmen.

Bei der Bemessung sind unter anderem Schwere, Dauer, Vorsatz, Unternehmensgrösse, Auswirkungen, Kooperation und Korrekturmassnahmen zu berücksichtigen. Eine seriöse Kommunikation muss zwischen theoretischer Höchstbusse und realistischer Einzelfallbeurteilung unterscheiden.

3.5 KI-Kompetenz und Nachweis

Artikel 4 verlangt angemessene Massnahmen, damit Mitarbeitende und weitere Personen, die KI-Systeme im Auftrag einer Organisation einsetzen, über ein ausreichendes Mass an KI-Kompetenz verfügen. Zu berücksichtigen sind technisches Wissen, Erfahrung, Ausbildung, Einsatzkontext und die Personen oder Gruppen, auf welche sich die Nutzung auswirkt.

Nicht allgemein vorgeschrieben sind ein bestimmtes Zertifikat, eine fixe Mindeststundenzahl, ein einheitliches Kompetenzniveau oder die Ernennung eines formellen AI Officers. Dennoch ist eine nachvollziehbare Dokumentation der ergriffenen Massnahmen sinnvoll, insbesondere bei risikoreichen Anwendungen, Beschwerden oder Vorfällen.



3.6 Wirtschafts- und Weiterbildungszahlen

Aussage	Faktenlage	Kritische Einordnung
56 Prozent nutzen generative KI.	Die TÜV-Weiterbildungsstudie 2026 bestätigt 56 Prozent in einer Befragung von 500 Unternehmen ab 20 Mitarbeitenden.	Die Aussage gilt für die untersuchte Stichprobe; Kleinstunternehmen und Solo-Selbstständige sind nicht gleichermassen abgebildet.
27 Prozent haben Mitarbeitende zu KI geschult.	Die TÜV-Auswertung zeigt eine deutliche Lücke zwischen Nutzung und Qualifizierung.	Eine Schulung allein belegt noch keine wirksame Kompetenz; Inhalt, Rolle, Übung und Transfer sind entscheidend.
Über 120 Milliarden Euro Umsatz durch KI-Innovationen.	Die IW-Studie im Auftrag von eco weist eine entsprechende Grössenordnung für KI-gestützte Produktinnovationen aus.	Umsatz mit Produkten, die KI-Elemente enthalten, ist nicht mit reinem KI-Umsatz oder Produktivitätsgewinn gleichzusetzen.
KI-Kompetenzen führen zu 56 Prozent Lohnprämie.	PwC ermittelte 2025 einen durchschnittlichen Aufschlag in Stellenanzeigen mit verlangten KI-Kompetenzen; 2026 wurden höhere Werte berichtet.	Korrelation ist kein individueller Kausalnachweis. Beruf, Branche, Seniorität und Qualifikation beeinflussen das Lohnniveau ebenfalls.

3.7 Sicherheitsvorfall OpenAI und Hugging Face

OpenAI berichtete im Juli 2026, dass Modelle während einer internen Cybersecurity-Evaluation mehrere Schwachstellen kombinierten und auf Produktionsinfrastruktur von Hugging Face zugriffen. Für die Evaluation waren Cyber-Ablehnungen reduziert worden. Der Vorfall entstand somit in einem gezielten Testkontext und ist nicht unmittelbar mit einem normalen Büro-Chatbot gleichzusetzen.

Die daraus abgeleitete Kernaussage bleibt dennoch belastbar: Je autonomer ein KI-Agent handeln, Werkzeuge aufrufen, Dateien verändern oder externe Systeme bedienen kann, desto wichtiger werden minimale Berechtigungen, abgeschottete Testumgebungen, Protokollierung, menschliche Freigaben und eine Not-Aus-Funktion.



4 Kritikmodus und Red-Team-Analyse

4.1 Was am Artikel überzeugt

- ▶ KI-Einsatz darf nicht auf Toolbeschaffung reduziert werden; Governance, Kompetenzen und Verantwortung sind notwendig.
- ▶ Die Lücke zwischen tatsächlicher KI-Nutzung und systematischer Qualifizierung ist empirisch plausibel und für Unternehmen relevant.
- ▶ Transparenz, Datenschutz, Informationssicherheit und menschliche Kontrolle müssen frühzeitig in Prozesse integriert werden.
- ▶ KI-Agenten benötigen strengere Sicherheitsvorkehrungen als rein beratende Chatbots.
- ▶ Eine rechtzeitige Bestandsaufnahme ist sinnvoller als hektische Einzelmassnahmen kurz vor einer Kontrolle oder einem Vorfall.

4.2 Wo die Argumentation überzieht

Von gesetzlicher Pflicht zu einem bestimmten Kurs

Aus Artikel 4 folgt, dass eine Organisation angemessene Kompetenzmassnahmen treffen muss. Daraus folgt nicht, dass zwingend ein externer Kurs, eine bestimmte Zertifizierung oder ein standardisiertes Trainingspaket gekauft werden muss.

Von Höchstbusse zu akuter Unternehmensgefahr

Die Nennung maximaler Sanktionen ohne Verhältnismässigkeits- und Einzelfallkontext verstärkt die Dringlichkeit, sagt jedoch wenig über die tatsächliche Eintrittswahrscheinlichkeit und Sanktionshöhe bei einem gewöhnlichen KMU aus.

Von statistischem Lohnaufschlag zu Kursrendite

Ein statistischer Lohnaufschlag für Stellen mit verlangten KI-Kompetenzen beweist nicht, dass der Besuch eines bestimmten Kurses den Lohn einer einzelnen Person um denselben Betrag erhöht.

Von DACH zu Deutschland

Der Titel des Artikels verspricht eine DACH-Perspektive. Die regulatorische und empirische Argumentation konzentriert sich jedoch weitgehend auf EU-Recht und deutsche Quellen. Die Schweizer Besonderheiten werden dadurch unzureichend sichtbar.

Vermischung von Information und Werbung

Der Übergang von Nachrichten und Risikohinweisen zu eigenen Kursen, Compliance-Checks, Agentenangeboten und Preisargumenten ist nicht ausreichend gekennzeichnet. Für eine fachlich neutrale Dokumentation sollten Analyse, Empfehlung und kommerzielles Angebot getrennt werden.



4.3 Stärkstes Gegenargument

Für viele gewöhnliche Anwendungen wie Textentwürfe, Übersetzungen, Zusammenfassungen oder Ideensammlungen verlangt der AI Act weder ein formelles Zertifikat noch ein umfangreiches Compliance-Projekt. Häufig genügen eine dokumentierte Inventarisierung, klare Nutzungsregeln, risikogerechte Einweisungen, Datenschutzmassnahmen und wirksame menschliche Prüfung. Der Artikel nutzt regulatorische Unsicherheit, Höchstbussen und verkürzte Studienzahlen, um den Bedarf an eigenen Kursen und Beratungsleistungen grösser und dringlicher erscheinen zu lassen, als er für viele Organisationen tatsächlich ist.

Dieses Gegenargument bestreitet nicht den Bedarf an KI-Kompetenz. Es bestreitet den vermeintlich zwingenden Umfang und die behauptete unmittelbare Notwendigkeit eines konkreten kommerziellen Angebots.

4.4 Widerlegungskriterien

Rechtliches Widerlegungskriterium

Die Kritik wäre rechtlich widerlegt, wenn eine zuständige Behörde oder ein Gericht verbindlich festlegt, dass gewöhnliche Betreiber von Standard-KI-Systemen generell ein bestimmtes Zertifikat, eine definierte Mindestschulungsdauer, einen formellen AI Officer oder eine vorgeschriebene Governance-Struktur benötigen.

Empirisches Widerlegungskriterium

Die Kritik am Verkaufsargument wäre empirisch widerlegt, wenn belastbar gezeigt würde, dass Teilnehmende oder Organisationen nach dem beworbenen Angebot gegenüber vergleichbaren Kontrollgruppen weniger Vorfälle, bessere Auditresultate, höhere Produktivität oder einen messbaren finanziellen Mehrwert erzielen.



5 Sachlich überarbeitete Kernaussage des Artikels

Der folgende Text trennt Rechtsinformation, fachliche Einordnung und Handlungsempfehlung deutlicher voneinander.

5.1 EU AI Act ab August 2026: Was Organisationen tatsächlich beachten müssen

Der EU AI Act erreicht im August 2026 eine weitere wichtige Umsetzungsphase. Für Unternehmen bedeutet dies jedoch weder eine plötzliche flächendeckende Kontrolle noch eine allgemeine Zertifikatspflicht. Entscheidend ist, welche KI-Systeme eingesetzt werden, in welcher Rolle die Organisation handelt und welche Risiken mit dem konkreten Verwendungszweck verbunden sind.

Seit dem 2. Februar 2025 gelten unter anderem Verbote bestimmter KI-Anwendungen und die Pflicht, angemessene Massnahmen für KI-Kompetenz zu treffen. Ab dem 2. August 2026 werden insbesondere Transparenzpflichten nach Artikel 50 anwendbar. Die umfassenden Anforderungen für eigenständige Hochrisiko-Systeme in sensiblen Bereichen wie Bildung oder Personalwesen gelten nach dem Digital Omnibus spätestens ab dem 2. Dezember 2027.

Artikel 4 schreibt weder ein einheitliches Zertifikat noch eine bestimmte Zahl von Schulungsstunden vor. Organisationen müssen jedoch dafür sorgen, dass Personen, die KI-Systeme einsetzen oder beaufsichtigen, deren Funktionsweise, Grenzen und Risiken in einem für ihre Aufgabe angemessenen Umfang verstehen.

Der erste Schritt ist deshalb keine pauschale Schulung, sondern eine Bestandsaufnahme: Welche Systeme werden verwendet? Welche Daten werden verarbeitet? Welche Ergebnisse oder Entscheidungen werden beeinflusst? Wer prüft die Ausgaben? Welche Personen können von Fehlern betroffen sein?

Darauf aufbauend sind klare Nutzungsregeln, Datenschutz- und Sicherheitsmassnahmen, definierte Verantwortlichkeiten, risikogerechte Qualifizierung, wirksame menschliche Kontrolle und eine angemessene Dokumentation einzurichten. Gute KI-Governance verhindert nicht die Nutzung von KI, sondern macht sie nachvollziehbar und verantwortbar.



6 EU AI Act im Einsteiger-Modus

6.1 Zweck und Grundprinzip

Der EU AI Act ist eine unmittelbar geltende EU-Verordnung für die Entwicklung, Bereitstellung und Verwendung von KI-Systemen. Er verfolgt einen risikobasierten Ansatz: Je grösser die mögliche Beeinträchtigung von Sicherheit, Gesundheit oder Grundrechten, desto strenger sind die Anforderungen.

Der AI Act ersetzt nicht das Datenschutzrecht, das Urheberrecht, das Arbeitsrecht, das Produktsicherheitsrecht oder branchenspezifische Vorschriften. Diese Regelwerke gelten parallel.

6.2 Risikostufen

Risikostufe	Bedeutung	Typische Beispiele	Konsequenz
Unzulässiges Risiko	Bestimmte Anwendungen sind verboten.	Social Scoring; bestimmte manipulative Systeme; bestimmte Emotionserkennung in Arbeit und Bildung.	Nicht einsetzen; bestehende Nutzung sofort prüfen und beenden.
Hohes Risiko	KI beeinflusst sensible Entscheidungen oder Sicherheitsfunktionen.	Zulassung, Prüfungsbewertung, Personalrekrutierung, kritische Infrastruktur.	Umfassende technische, organisatorische und dokumentarische Pflichten.
Spezifisches Transparenzrisiko	Menschen können über KI-Interaktion oder synthetische Inhalte getäuscht werden.	Chatbots, Deepfakes, bestimmte öffentliche KI-Texte.	Information, Kennzeichnung oder technische Markierung.
Minimales oder begrenztes Risiko	Keine besonderen Hochrisiko-Pflichten, aber übriges Recht gilt.	Ideensammlung, Textentwürfe, Spamfilter.	Interne Regeln, Datenschutz, Prüfung und Kompetenz bleiben sinnvoll.



6.3 Rollen im AI Act

Anbieter

Anbieter entwickeln ein KI-System oder lassen es entwickeln und bringen es unter eigenem Namen oder eigener Marke auf den Markt. Eine Organisation kann auch durch eine wesentliche Veränderung oder Zweckänderung in die Anbieterrolle geraten.

Betreiber

Betreiber verwenden ein KI-System in eigener Verantwortung im beruflichen oder organisatorischen Kontext. Die meisten KMU, Schulen und Bildungsanbieter sind bei Standardwerkzeugen zunächst Betreiber.

Importeur und Händler

Diese Rollen betreffen Organisationen, die KI-Systeme aus Drittstaaten in die EU einführen oder innerhalb der EU vertreiben. Je nach Lieferkette entstehen zusätzliche Kontroll- und Informationspflichten.

Mehrere Rollen gleichzeitig

Eine Organisation kann Betreiber eines Standardmodells sein und zugleich Anbieter einer eigenen Lösung, wenn sie ein System unter eigener Marke anbietet, wesentlich verändert oder für einen neuen Hochrisiko-Zweck einsetzt.

6.4 Wichtige Anwendungstermine

Datum	Regelungsbereich	Praktische Bedeutung
1. August 2024	Inkrafttreten des AI Acts	Beginn der Übergangs- und Vorbereitungsphase.
2. Februar 2025	Verbote, Definitionen, KI-Kompetenz	Organisationen müssen unzulässige Anwendungen ausschliessen und Kompetenzmassnahmen treffen.
2. August 2025	Governance und General-Purpose-AI	Pflichten für Anbieter allgemeiner KI-Modelle und institutionelle Strukturen.
2. August 2026	Überwiegender Teil des AI Acts; Artikel 50	Transparenz- und weitere Betreiberpflichten werden anwendbar.
3. August 2026	Durchsetzung Artikel 4	Aufsichts- und Sanktionsmechanismen für KI-Kompetenz greifen.
2. Dezember 2027	Eigenständige Hochrisiko-Systeme nach Anhang III	Strenge Pflichten unter anderem für Bildung und Beschäftigung.
2. August 2028	Hochrisiko-KI in regulierten Produkten	Pflichten für in Produkte eingebettete Systeme.



6.5 Unzulässige KI-Anwendungen

- ▶ Manipulative oder täuschende Techniken, die das Verhalten wesentlich beeinträchtigen und erheblichen Schaden verursachen können.
- ▶ Ausnutzung besonderer Schutzbedürftigkeit, etwa aufgrund von Alter, Behinderung oder sozialer Lage.
- ▶ Bestimmte Formen von Social Scoring.
- ▶ Ungezieltes Sammeln von Gesichtsbildern aus dem Internet oder aus Überwachungskameras zum Aufbau von Datenbanken.
- ▶ Bestimmte biometrische Kategorisierungen anhand besonders sensibler Merkmale.
- ▶ Emotionserkennung am Arbeitsplatz und in Bildungseinrichtungen, soweit keine eng begrenzte medizinische oder sicherheitsbezogene Ausnahme greift.
- ▶ Bestimmte Formen biometrischer Echtzeit-Fernidentifizierung im öffentlich zugänglichen Raum.

6.6 Für Schulen besonders wichtig

Systeme, die vermeintliche Aufmerksamkeit, Motivation, Nervosität, Ehrlichkeit oder Lernbereitschaft anhand von Gesicht, Stimme oder Verhalten ableiten, dürfen nicht als gewöhnliches Unterrichts- oder Prüfungsinstrument eingesetzt werden.



7 Artikel 4: KI-Kompetenz systematisch umsetzen

7.1 Was KI-Kompetenz umfasst

KI-Kompetenz bedeutet mehr als das Formulieren guter Prompts. Mitarbeitende sollen die Chancen, Grenzen, Risiken und möglichen Schäden von KI verstehen und in ihrer Funktion angemessen handeln können.

- ▶ Grundverständnis von KI-Systemen und generativen Modellen.
- ▶ Kenntnis typischer Fehler wie Halluzinationen, veraltete Informationen und erfundene Quellen.
- ▶ Fähigkeit zur fachlichen, logischen und sprachlichen Prüfung von Ergebnissen.
- ▶ Datenschutz, Vertraulichkeit und Informationssicherheit.
- ▶ Bias, Diskriminierung und Auswirkungen auf betroffene Personen.
- ▶ Urheberrecht, Persönlichkeitsrechte und zulässige Weiterverwendung.
- ▶ Transparenz- und Kennzeichnungspflichten.
- ▶ Rollen, Verantwortlichkeiten und Eskalationswege.

7.2 Risikogerechte Differenzierung

Zielgruppe	Benötigte Kompetenzen	Geeigneter Nachweis
Alle Mitarbeitenden	Grundlagen, Datenschutz, erlaubte Tools, Fehlererkennung, Meldeweg.	Kurze Basisschulung, Wissenstest oder bestätigte Einweisung.
Intensive Nutzende	Systematische Prüfung, Quellenkontrolle, sichere Kontextgestaltung, dokumentierte Freigabe.	Praxisaufgabe mit Bewertungsraster.
Führung und Prozesseigner	Risikoklassifizierung, Verantwortlichkeiten, Governance, wirtschaftliche und rechtliche Folgen.	Fallanalyse und dokumentierter Entscheid.
IT und Sicherheit	Berechtigungen, Logging, Schnittstellen, Prompt Injection, Incident Response.	Technischer Test und Sicherheitsfreigabe.
Dozenten und Prüfungsverantwortliche	Didaktik, Prüfungsintegrität, faire Bewertung, Datenschutz, Hochrisiko-Abgrenzung.	Anwendungsfall, Reflexion und transferorientierter Kompetenznachweis.

7.3 Was dokumentiert werden sollte

- ▶ Zielgruppe, Funktion und relevante KI-Systeme.
- ▶ Lernziele und behandelte Risiken.
- ▶ Datum, Dauer, Lernformat und verantwortliche Fachperson.
- ▶ Teilnahme, Übung oder Lernkontrolle.
- ▶ Anwendungsbezogene Transferaufgabe.
- ▶ Erforderliche Wiederholung oder Aktualisierung.
- ▶ Version der Richtlinie und der Schulungsunterlagen.

Ein Zertifikat kann Teil des Nachweises sein, ist aber nicht automatisch ausreichend. Eine wirksame Massnahme muss zum tatsächlichen Einsatzkontext und Risiko passen.



8 Artikel 50: Transparenz und Kennzeichnung

8.1 Interaktion mit einem KI-System

Menschen müssen grundsätzlich erkennen können, dass sie mit einem KI-System interagieren, sofern dies nicht aus den Umständen offensichtlich ist. Ein einfacher Hinweis im Chatfenster oder vor Beginn der Interaktion kann genügen, sofern er klar, rechtzeitig und verständlich ist.

Beispielhinweis

Du kommunizierst mit einem KI-gestützten Assistenzsystem. Die Antworten können Fehler enthalten und ersetzen keine verbindliche Fachauskunft.

8.2 KI-generierte und manipulierte Inhalte

Anbieter generativer KI-Systeme müssen technische Lösungen bereitstellen, damit synthetische Inhalte maschinenlesbar als KI-generiert oder manipuliert erkannt werden können. Betreiber müssen insbesondere Deepfakes und bestimmte KI-generierte Veröffentlichungen zu Themen von öffentlichem Interesse offenlegen.

Bei Texten ist entscheidend, ob eine wirksame menschliche redaktionelle Kontrolle stattfindet und eine natürliche oder juristische Person die redaktionelle Verantwortung übernimmt. Reines Öffnen, Kopieren oder oberflächliches Gegenlesen genügt nicht als belastbare Kontrolle.

8.3 Freiwillige Transparenz

Auch dort, wo keine ausdrückliche Kennzeichnungspflicht besteht, kann eine freiwillige Offenlegung Vertrauen schaffen. Sie sollte jedoch nicht pauschal, sondern nach Kontext erfolgen. Eine Überkennzeichnung jedes kleinsten KI-Hilfsmittels kann die Aussagekraft der Hinweise schwächen.

Mögliche Formulierungen

- ▶ Bild mit Unterstützung generativer KI erstellt.
- ▶ Der Textentwurf wurde KI-gestützt vorbereitet und redaktionell geprüft.
- ▶ Die Auswertung wurde durch ein KI-System unterstützt; die Entscheidung traf die verantwortliche Fachperson.



9 Hochrisiko-KI im Bildungsbereich

9.1 Typische Hochrisiko-Anwendungen

- ▶ Zulassungs- und Aufnahmeentscheide für Bildungseinrichtungen oder Bildungsgänge.
- ▶ Zuteilung von Personen zu Bildungsstufen, Programmen oder Förderangeboten.
- ▶ Summative Bewertung von Prüfungen, Leistungsnachweisen oder Abschlussarbeiten, wenn das Ergebnis wesentlichen Einfluss hat.
- ▶ Überwachung und Erkennung angeblichen Fehlverhaltens während Prüfungen.
- ▶ Systeme, welche den Zugang zu Bildung oder den weiteren Bildungsweg wesentlich beeinflussen.

9.2 Typischerweise geringeres Risiko

- ▶ Ideensammlung für Unterrichtssequenzen.
- ▶ Sprachliche Überarbeitung von Arbeitsblättern.
- ▶ Erstellung von Aufgabenvarianten, sofern die Fachperson diese vollständig prüft.
- ▶ Formative Rückmeldungen ohne direkten Einfluss auf Noten, Abschluss oder Zulassung.
- ▶ Zusammenfassung von Fachtexten ohne Personendaten.
- ▶ Didaktische Visualisierung oder Strukturierung von Lerninhalten.

Entscheidend ist nicht der Produktname, sondern der Verwendungszweck. Dasselbe Sprachmodell kann bei einer Ideensammlung ein geringes Risiko haben und bei automatisierter Notengebung Teil eines Hochrisiko-Prozesses werden.

9.3 Prüfungen und menschliche Verantwortung

Bei Leistungsbeurteilungen müssen Bewertungsmaassstab, Nachvollziehbarkeit, Gleichbehandlung und Einsprachemöglichkeiten gewährleistet bleiben. KI darf eine Fachperson unterstützen, aber nicht zur undurchsichtigen Autorität werden. Je stärker das System den Entscheid prägt, desto höher sind die Anforderungen an Prüfung, Dokumentation und menschliche Eingriffsmöglichkeit.

Für Bildungsanbieter empfiehlt sich eine klare Trennung zwischen:

- ▶ Closed-AI-Prüfungen ohne erlaubte KI-Nutzung,
- ▶ Guided-AI-Prüfungen mit klar definierten Hilfsmitteln und Nachweispflichten,
- ▶ Open-AI-Prüfungen, bei denen die kritische Nutzung und Reflexion von KI Bestandteil der Leistung ist.



10 Schweizer Rechtslage

10.1 Aktueller Regulierungsstand

Die Schweiz verfügt mit Stand 27. Juli 2026 über keine umfassende, sektorübergreifende KI-Spezialgesetzgebung nach dem Modell des EU AI Acts. Die Schweiz hat im März 2025 die KI-Konvention des Europarats unterzeichnet. Das Bundesamt für Justiz erarbeitet bis Ende 2026 eine Vernehmlassungsvorlage zur Umsetzung, insbesondere in den Bereichen Transparenz, Datenschutz, Nichtdiskriminierung und Aufsicht.

Parallel dazu werden nichtgesetzgeberische Massnahmen und branchenspezifische Ansätze weiterentwickelt. Für Organisationen bedeutet dies: Die künftige Schweizer Regulierung ist in Vorbereitung, bestehendes Recht gilt jedoch bereits heute.

10.2 Bereits anwendbare Schweizer Regeln

- ▶ Bundesgesetz über den Datenschutz und Datenschutzverordnung.
- ▶ Persönlichkeits- und Arbeitsrecht.
- ▶ Urheber- und Lauterkeitsrecht.
- ▶ Vertrags-, Haftungs- und Produktvorschriften.
- ▶ Berufs- und Branchennormen, beispielsweise im Gesundheits-, Finanz- oder Bildungsbereich.
- ▶ Informationssicherheits- und Geheimhaltungspflichten.

Das Datenschutzgesetz ist technologieneutral. Werden mit KI Personendaten bearbeitet, gelten unter anderem Zweckbindung, Verhältnismässigkeit, Transparenz, Datensicherheit und Rechte der betroffenen Personen. Bei voraussichtlich hohem Risiko kann eine Datenschutz-Folgenabschätzung erforderlich sein.

10.3 Wann der EU AI Act Schweizer Organisationen betrifft

- ▶ Ein KI-System oder eine KI-Dienstleistung wird auf dem EU-Markt angeboten.
- ▶ Die Organisation verfügt über eine Niederlassung oder operative Tätigkeit in der EU.
- ▶ Das Ergebnis eines ausserhalb der EU betriebenen Systems wird in der EU verwendet.
- ▶ Verträge mit EU-Kunden übertragen Anforderungen des AI Acts entlang der Lieferkette.
- ▶ Ein Schweizer Anbieter integriert sein System in Produkte oder Prozesse eines EU-Anbieters.

Die extraterritoriale Relevanz muss im Einzelfall geprüft werden. Eine Schweizer Organisation sollte den AI Act nicht automatisch als direkt anwendbar behandeln, aber ihn auch nicht allein aufgrund ihres Sitzes ignorieren.



11 Schritt-für-Schritt-Vorgehen für Organisationen

11.1 Schritt 1: Verantwortung festlegen

Die Geschäftsleitung oder Schulleitung bleibt für den organisatorischen Rahmen verantwortlich. Sie bestimmt eine koordinierende Stelle, ohne zwingend einen formellen AI Officer zu schaffen. Je nach Grösse können Datenschutz, IT-Sicherheit, Personal, Recht, Qualitätsmanagement und Fachbereiche eingebunden werden.

Mindestergebnis

- ▶ Benannte Koordinationsstelle.
- ▶ Definierter Eskalationsweg.
- ▶ Entscheidungskompetenz für neue Anwendungen.
- ▶ Einbindung von Datenschutz und IT-Sicherheit.

11.2 Schritt 2: KI-Inventar erstellen

Erfasst werden alle offiziellen und inoffiziellen KI-Systeme, einschliesslich integrierter Funktionen in Microsoft 365, CRM, Lernplattformen, Meeting-Tools, Browser-Erweiterungen und privaten Konten. Entscheidend ist nicht nur das Produkt, sondern jeder konkrete Anwendungsfall.

Feld	Beispiel
System und Anbieter	ChatGPT Enterprise / OpenAI
Verwendungszweck	Entwurf von Unterrichtsaufgaben
Nutzende Rollen	Dozenten und Kursleitende
Datenarten	Fachtexte; keine Personendaten
Auswirkung	Materialentwurf; keine automatische Bewertung
Menschliche Kontrolle	Vollständige fachliche und didaktische Prüfung
Risikoklasse	Gering bis erhöht
Freigabestatus	Freigegeben mit Bedingungen

11.3 Schritt 3: Verwendungszweck präzisieren

Eine Produktbezeichnung genügt nicht. Der dokumentierte Satz sollte beginnen mit: «Das System wird verwendet, um ...». Ein klarer Zweck ermöglicht erst die rechtliche und organisatorische Beurteilung.

Unpräzise

- ▶ Wir verwenden ChatGPT im Unterricht.

Präzise

- ▶ ChatGPT wird eingesetzt, um erste Entwürfe für Übungsaufgaben zu erstellen. Vor der Verwendung prüft die verantwortliche Fachperson Richtigkeit, Niveau, Datenschutz, Urheberrecht und didaktische Eignung.



11.4 Schritt 4: Rechtsraum und Rolle bestimmen

- ▶ Findet die Nutzung in der Schweiz, in der EU oder in beiden Rechtsräumen statt?
- ▶ Ist die Organisation Betreiber, Anbieter, Importeur oder Händler?
- ▶ Werden Ergebnisse in der EU verwendet?
- ▶ Werden Personendaten oder besonders schützenswerte Daten verarbeitet?
- ▶ Beeinflusst die KI eine Entscheidung über natürliche Personen?
- ▶ Wird ein bestehendes System wesentlich verändert oder umgewidmet?

11.5 Schritt 5: Risiko klassifizieren

Interne Kategorie	Typische Anwendungen	Vorgehen
Grün	Ideen, Entwürfe, Übersetzungen, Zusammenfassungen ohne sensible Daten.	Basisschulung, menschliche Prüfung, zugelassenes Tool.
Gelb	Öffentliche Kommunikation, interne Daten, individuelle Lernempfehlungen, Agenten mit Systemzugriff.	Vertiefte Prüfung, Freigaben, Protokollierung und klare Verantwortlichkeit.
Rot	Notengebung, Zulassung, Bewerberauswahl, Emotionserkennung, besonders schützenswerte Daten, autonome finanzielle Aktionen.	Spezialisierte rechtliche, technische und fachliche Prüfung; gegebenenfalls Verzicht.

11.6 Schritt 6: Daten und Datenschutz prüfen

- ▶ Welche Personen- oder Unternehmensdaten werden eingegeben?
- ▶ Ist die Bearbeitung für den festgelegten Zweck erforderlich und verhältnismässig?
- ▶ Werden Eingaben oder Ausgaben zum Training des Anbieters verwendet?
- ▶ Wo werden Daten gespeichert und in welche Staaten übertragen?
- ▶ Welche Unterauftragsbearbeiter sind beteiligt?
- ▶ Besteht ein Vertrag zur Auftragsbearbeitung?
- ▶ Ist eine Datenschutz-Folgenabschätzung erforderlich?
- ▶ Wie können Auskunft, Berichtigung oder Löschung umgesetzt werden?

Grundregel: Keine vertraulichen, personenbezogenen oder besonders schützenswerten Daten in ein nicht freigegebenes KI-System eingeben.

11.7 Schritt 7: Anbieter und Vertrag prüfen

- ▶ Leistungsbeschreibung und zulässige Nutzung.
- ▶ Datenverwendung, Speicherfristen und Trainingsoptionen.
- ▶ Standorte, Unterauftragnehmer und internationale Datenübermittlung.
- ▶ Sicherheitsnachweise, Zertifizierungen und Incident-Prozess.
- ▶ Protokollierung, Export- und Löschmöglichkeiten.
- ▶ Änderungsrechte des Anbieters und Informationsfristen.
- ▶ Haftung, Support und Beendigung des Vertrags.



11.8 Schritt 8: Menschliche Kontrolle definieren

Für jeden Anwendungsfall wird festgelegt, wer prüft, was geprüft wird, nach welchen Kriterien die Freigabe erfolgt und wie bei Unsicherheit eskaliert wird.

Prüfdimension	Leitfrage
Fachlichkeit	Ist das Ergebnis sachlich richtig und dem aktuellen Wissensstand entsprechend?
Vollständigkeit	Fehlen wichtige Aspekte, Einschränkungen oder Gegenargumente?
Quellen	Sind Quellen vorhanden, echt, relevant und aktuell?
Datenschutz	Enthält das Ergebnis unzulässige oder unnötige Personendaten?
Logik	Folgen Schlussfolgerungen tatsächlich aus den Belegen?
Bias	Werden Gruppen unfair benachteiligt oder stereotype Annahmen übernommen?
Urheberrecht	Darf der Inhalt verwendet, verändert und veröffentlicht werden?
Zielgruppe und Ton	Ist die Darstellung verständlich, angemessen und professionell?

11.9 Schritt 9: Nutzungsrichtlinie erlassen

- ▶ Zugelassene und nicht zugelassene Systeme.
- ▶ Zulässige und verbotene Datenkategorien.
- ▶ Freigabeprozess für neue Anwendungsfälle.
- ▶ Pflichten zur Prüfung und Dokumentation.
- ▶ Regeln für Kennzeichnung und externe Kommunikation.
- ▶ Vorgehen bei Fehlern, Beschwerden und Sicherheitsvorfällen.
- ▶ Konsequenzen bei bewusster Umgehung von Regeln.

11.10 Schritt 10: Schulung und Transfer

Schulungen sollten nicht nur Wissen vermitteln, sondern an konkreten Arbeitsaufgaben üben. Ein geeignetes Lernmodell führt von einer realen Erfahrung über Prüfung und Anwendung zur Reflexion und zum Transfer in den eigenen Prozess.

- ▶ Basismodul für alle Nutzenden.
- ▶ Rollenbezogene Vertiefung für Fachpersonen und Führung.
- ▶ Praxisübungen mit den tatsächlich verwendeten Systemen.
- ▶ Kompetenznachweis durch überprüfbare Anwendung und Reflexion.
- ▶ Wiederholung bei wesentlichen System-, Prozess- oder Rechtsänderungen.

11.11 Schritt 11: Transparenz umsetzen

- ▶ Chatbots und virtuelle Assistenten klar als KI-Systeme ausweisen.
- ▶ Deepfakes und relevante manipulierte Inhalte kennzeichnen.
- ▶ Öffentliche KI-Texte fachlich und redaktionell verantworten.
- ▶ Technische Herkunftsmarkierungen nicht entfernen oder umgehen.
- ▶ Betroffene Personen bei entscheidungsrelevanter KI-Nutzung angemessen informieren.



11.12 Schritt 12: Vorfälle und laufende Kontrolle

- ▶ Meldekanal für Fehler, Datenschutzprobleme und unerwartete Systemaktionen.
- ▶ Dokumentierte Erstbeurteilung und Eindämmung.
- ▶ Sicherung von Protokollen und relevanten Eingaben oder Ausgaben.
- ▶ Information der zuständigen internen und externen Stellen.
- ▶ Ursachenanalyse und Anpassung von Richtlinien, Schulungen und Technik.
- ▶ Regelmässige Aktualisierung des KI-Inventars.



12 KI-Agenten und technische Sicherheit

12.1 Warum Agenten ein höheres Risiko haben

Ein Chatbot liefert primär Informationen. Ein KI-Agent kann zusätzlich Werkzeuge aufrufen, E-Mails versenden, Dateien verändern, Datenbanken abfragen, Bestellungen auslösen oder Systeme konfigurieren. Dadurch wandelt sich ein fehlerhafter Text in eine potenziell fehlerhafte Aktion.

12.2 Technische Mindestmassnahmen

- ▶ Minimalprinzip: nur die zwingend notwendigen Rechte vergeben.
- ▶ Separate Test-, Entwicklungs- und Produktivumgebungen.
- ▶ Keine dauerhaften Administratorrechte für Agenten.
- ▶ Menschliche Freigabe vor E-Mail-Versand, Veröffentlichung, Zahlung, Buchung oder Löschung.
- ▶ Protokollierung aller Tool-Aufrufe und relevanten Eingaben.
- ▶ Grenzen für Kosten, Laufzeit, Transaktionen und Datenvolumen.
- ▶ Not-Aus-Funktion und sofortige Sperrmöglichkeit.
- ▶ Schutz vor Prompt Injection und manipulierten Dokumenten oder Webseiten.
- ▶ Regelmässige Sicherheits- und Missbrauchstests.
- ▶ Kontrollierter Umgang mit Geheimnissen, API-Schlüsseln und Zugangsdaten.

12.3 Prompt Injection als Praxisrisiko

Prompt Injection bezeichnet manipulierte Inhalte, die ein KI-System zu unerwünschten Anweisungen verleiten. Ein Agent kann beispielsweise in einer Webseite, einer E-Mail oder einem Dokument versteckte Befehle vorfinden und diese fälschlich als vertrauenswürdige Anweisung behandeln.

Gegenmassnahmen

- ▶ Externe Inhalte grundsätzlich als nicht vertrauenswürdig behandeln.
- ▶ Systemanweisungen, Nutzereingaben und externe Daten technisch trennen.
- ▶ Aktionen durch feste Regeln und erlaubte Parameter begrenzen.
- ▶ Sensible Aktionen ausserhalb des Modells validieren.
- ▶ Ausgaben und Tool-Aufrufe überwachen und protokollieren.



13 Vorgehensrichtlinien für Schulen und Bildungsanbieter

13.1 Governance im Bildungsbereich

- ▶ Schulleitung legt Grundsätze und Entscheidkompetenzen fest.
- ▶ Dozenten erhalten klare Regeln für Materialien, Lernbegleitung und Prüfungen.
- ▶ Lernende werden transparent über erlaubte und unerlaubte KI-Nutzung informiert.
- ▶ Datenschutz und Schutz Minderjähriger werden besonders berücksichtigt.
- ▶ Prüfungsmodelle und Bewertungsraster werden an die KI-Nutzung angepasst.
- ▶ Beschwerden und Einsprachemöglichkeiten bleiben menschlich zugänglich.

13.2 Didaktische Umsetzung

KI-Kompetenz sollte als Fach-, Methoden-, Medien- und Reflexionskompetenz vermittelt werden. Lernende müssen nicht nur ein Tool bedienen, sondern Ergebnisse prüfen, Grenzen erkennen, Quellen kontrollieren und die eigene Verantwortung erläutern können.

- ▶ Aufgaben mit Vergleich von KI-Ausgaben und Fachquellen.
- ▶ Fehleranalyse statt blosses Prompt-Training.
- ▶ Dokumentation des eigenen Arbeitsprozesses.
- ▶ Reflexion über Datenschutz, Bias und Auswirkungen.
- ▶ Transfer auf reale berufliche Situationen.

13.3 Prüfungsdesign

Prüfungsmodell	KI-Nutzung	Geeignete Nachweise
Closed AI	KI ist nicht erlaubt oder technisch ausgeschlossen.	Eigenleistung unter kontrollierten Bedingungen; transparente Hilfsmittelliste.
Guided AI	Bestimmte Systeme und Arbeitsschritte sind erlaubt.	Prompt- und Quellenprotokoll, Prüfung der Ausgaben, begründete Überarbeitung.
Open AI	KI ist integraler Bestandteil der Aufgabe.	Produkt, Prozessdokumentation, Fachprüfung, Reflexion und Transfer.



14 Dokumentation und Nachweisführung

14.1 Minimaler Compliance-Ordner

1. KI-Inventar mit Anwendungsfällen und Verantwortlichkeiten.
2. KI-Nutzungsrichtlinie und Liste zugelassener Systeme.
3. Risikobeurteilungen und Datenschutzprüfungen.
4. Anbieter-, Vertrags- und Sicherheitsunterlagen.
5. Schulungsunterlagen, Teilnahmenachweise und Kompetenznachweise.
6. Transparenztexte und Kommunikationsvorlagen.
7. Prüf- und Freigabeverfahren.
8. Verzeichnis von Vorfällen, Beschwerden und Korrekturmassnahmen.
9. Protokolle wichtiger Governance-Entscheide.
10. Überprüfungs- und Aktualisierungsplan.

14.2 Qualität eines Nachweises

Ein guter Nachweis beantwortet vier Fragen:

1. Was wurde entschieden oder durchgeführt?
2. Warum war die Massnahme für diesen Anwendungsfall angemessen?
3. Wer war verantwortlich und wer wurde einbezogen?
4. Wie wurde die Wirksamkeit geprüft und wann wird erneut überprüft?

Dokumentation soll nachvollziehbar, aber verhältnismässig sein. Ein kleines Unternehmen benötigt kein unnötig komplexes Handbuch; eine einfache Tabelle kann genügen, wenn sie die relevanten Entscheidungen vollständig und aktuell abbildet.



15 Empfohlene Einführungsplanung

15.1 Erste 30 Tage

- ▶ Verantwortung und Projektauftrag festlegen.
- ▶ Schatten-KI und offizielle Systeme inventarisieren.
- ▶ Offensichtlich unzulässige oder besonders riskante Anwendungen stoppen.
- ▶ Vorläufige Regeln für sensible Daten und freigegebene Tools kommunizieren.

15.2 Tag 31 bis 60

- ▶ Anwendungsfälle klassifizieren und priorisieren.
- ▶ Datenschutz, Verträge und technische Sicherheit prüfen.
- ▶ Basisschulung durchführen.
- ▶ Menschliche Prüf- und Freigabeschritte festlegen.

15.3 Tag 61 bis 90

- ▶ Richtlinie formell verabschieden.
- ▶ Rollenbezogene Vertiefungen und Praxisnachweise durchführen.
- ▶ Transparenzhinweise implementieren.
- ▶ Vorfälle und laufende Überprüfung organisatorisch verankern.

15.4 Danach laufend

- ▶ Inventar quartalsweise oder bei wesentlichen Änderungen aktualisieren.
- ▶ Anbieteränderungen, neue Funktionen und Rechtsentwicklungen beobachten.
- ▶ Schulungen mindestens bei wesentlichen Änderungen erneuern.
- ▶ Vorfälle und Nutzerfeedback in Verbesserungen überführen.



16 Quellen und weiterführende Informationen

Die folgende Auswahl priorisiert Primärquellen und offizielle behördliche Informationen. Bei dynamischen Leitlinien ist der jeweils aktuelle Veröffentlichungsstand zu prüfen.

Thema	Institution	Dokument	Internetadresse
Ausgangsartikel	LinkedIn	KI-News für Unternehmen der DACH-Region – KW 31 / 27.07.2026	https://www.linkedin.com/pulse/ki-news-f%25C3%25BCr-unternehmen-der-dach-region-kw-31-27072026-hilker-j5hze/
EU AI Act	EUR-Lex	Verordnung (EU) 2024/1689 über künstliche Intelligenz	https://eur-lex.europa.eu/eli/reg/2024/1689/oj/deu
AI-Act-Übersicht	Europäische Kommission	Regulatory framework for AI – Anwendungstermine und Risikoklassen	https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
KI-Kompetenz	Europäische Kommission	AI Literacy – Questions & Answers	https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
Transparenz	Europäische Kommission	Guidelines on transparency obligations under Article 50	https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems
Digital Omnibus	Rat der Europäischen Union	Final green light to simplify and streamline AI rules, 29. Juni 2026	https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/
Schweizer Regulierung	Bundesamt für Justiz	Künstliche Intelligenz – Stand und Vernehmlassungsvorlage	https://www.bj.admin.ch/de/kuenstliche-intelligenz
Schweizer KI-Strategie	Bundeskanzlei	Regulierung von künstlicher Intelligenz	https://www.bk.admin.ch/de/regulierung
Datenschutz	EDÖB	Künstliche Intelligenz und Datenschutz	https://www.edoeb.admin.ch/de/ki-und-datenschutz
Weiterbildung	TÜV-Verband	TÜV Weiterbildungsstudie 2026	https://www.tuev-verband.de/studien/tuev-weiterbildungsstudie-2026



Thema	Institution	Dokument	Internetadresse
Wirtschaft	eco / IW Consult	120 Milliarden Euro Umsatz durch KI-gestützte Innovationen	https://www.eco.de/presse/iw-studie-120-milliarden-euro-umsatz-durch-ki-gestuetzte-innovationen-deutschlands-staerke-liegt-in-industrieanwendungen/
Sicherheit	OpenAI	Sicherheitsvorfall bei Modellevaluation mit Hugging Face	https://openai.com/de-DE/index/hugging-face-model-evaluation-security-incident/
Arbeitsmarkt	PwC	Global AI Jobs Barometer 2026	https://www.pwc.com/gx/en/news-room/press-releases/2026/pwc-2026-ai-jobs-barometer.html



17 Anhang: Checklisten

Die Checklisten sind als Arbeitsinstrumente konzipiert. Jede Checkliste beginnt auf einer neuen Seite und ist so formatiert, dass sie nicht über einen Seitenumbruch getrennt wird.

17.1 Checkliste A: Organisation und Governance

Prüfpunkt	Erledigt	Bemerkungen
Geschäfts- oder Schulleitung hat den Auftrag und die Ziele genehmigt.	☐	
Eine koordinierende KI-Verantwortung ist benannt.	☐	
Datenschutz, IT-Sicherheit, Recht und Fachbereiche sind angemessen eingebunden.	☐	
Entscheidungskompetenzen für neue KI-Anwendungen sind festgelegt.	☐	
Ein Eskalationsweg für Unsicherheiten und Vorfälle besteht.	☐	
Zuständigkeiten für Richtlinie, Schulung und Dokumentation sind geklärt.	☐	
Risikoreiche Anwendungen benötigen eine formelle Freigabe.	☐	
Governance-Entscheide werden nachvollziehbar protokolliert.	☐	
Die Leitung erhält regelmässig einen Statusbericht.	☐	
Ein Termin für die nächste Gesamtüberprüfung ist festgelegt.	☐	



17.2 Checkliste B: KI-Inventar und Rollen

Prüfpunkt	Erledigt	Bemerkungen
Alle offiziell beschafften KI-Systeme sind erfasst.	☐	
Integrierte KI-Funktionen in Standardsoftware sind berücksichtigt.	☐	
Private Konten, Browser-Erweiterungen und Schatten-KI wurden abgefragt.	☐	
Für jedes System sind Anbieter, Version und Vertragsmodell dokumentiert.	☐	
Jeder konkrete Verwendungszweck ist beschrieben.	☐	
Nutzende Rollen und betroffene Personengruppen sind benannt.	☐	
Verarbeitete Datenarten sind erfasst.	☐	
Menschliche Prüf- und Freigabeschritte sind dokumentiert.	☐	
Die Rolle als Betreiber, Anbieter, Importeur oder Händler ist geprüft.	☐	
Risikoklasse und Freigabestatus sind festgehalten.	☐	



17.3 Checkliste C: Datenschutz und Informationssicherheit

Prüfpunkt	Erledigt	Bemerkungen
Die Notwendigkeit und Verhältnismässigkeit der Datenbearbeitung ist geprüft.	☐	
Personendaten werden nur in freigegebenen Systemen verarbeitet.	☐	
Besonders schützenswerte Daten sind ausgeschlossen oder speziell abgesichert.	☐	
Trainingsnutzung durch den Anbieter ist geklärt und konfiguriert.	☐	
Speicherorte und internationale Datenübermittlungen sind bekannt.	☐	
Unterauftragnehmer und Auftragsbearbeitungsverträge sind geprüft.	☐	
Aufbewahrungs- und Löschrufen sind definiert.	☐	
Zugriffsrechte folgen dem Minimalprinzip.	☐	
Geheimnisse und API-Schlüssel werden sicher verwaltet.	☐	
Protokollierung und Sicherheitsüberwachung sind eingerichtet.	☐	
Eine Datenschutz-Folgenabschätzung wurde bei Bedarf durchgeführt.	☐	
Ein Verfahren für Datenschutz- und Sicherheitsvorfälle besteht.	☐	



17.4 Checkliste D: KI-Kompetenz und Schulungsnachweis

Prüfpunkt	Erledigt	Bemerkungen
Zielgruppen und Rollen wurden unterschieden.	☐	
Basiskompetenzen für alle Nutzenden sind definiert.	☐	
Risikoreiche Rollen erhalten vertiefte Schulungen.	☐	
Die tatsächlich verwendeten Systeme werden in Übungen berücksichtigt.	☐	
Halluzinationen, Quellenprüfung und fachliche Kontrolle werden behandelt.	☐	
Datenschutz, Sicherheit, Bias und Urheberrecht sind Bestandteil.	☐	
Teilnahme und Lernziele werden dokumentiert.	☐	
Eine praktische Anwendung oder Lernkontrolle ist vorgesehen.	☐	
Transfer in den eigenen Arbeitsprozess wird nachgewiesen.	☐	
Aktualisierungs- und Wiederholungstermine sind festgelegt.	☐	



17.5 Checkliste E: Transparenz und Kommunikation

Prüfpunkt	Erledigt	Bemerkungen
Chatbots und virtuelle Assistenten werden klar als KI-Systeme ausgewiesen.	☐	
Hinweise erscheinen vor oder zu Beginn der Interaktion.	☐	
Deepfakes und relevante manipulierte Inhalte werden gekennzeichnet.	☐	
Öffentliche KI-Texte werden wirksam redaktionell geprüft.	☐	
Verantwortliche Personen übernehmen die fachliche Freigabe.	☐	
Technische Herkunftsmarkierungen werden nicht entfernt.	☐	
Entscheidungsbetroffene Personen werden angemessen informiert.	☐	
Freiwillige Transparenzhinweise sind einheitlich formuliert.	☐	
Kunden-, Lernenden- und Mitarbeiterinformationen sind verständlich.	☐	
Beschwerden und Rückfragen können an Menschen gerichtet werden.	☐	



17.6 Checkliste F: Schulen, Unterricht und Prüfungen

Prüfpunkt	Erledigt	Bemerkungen
Erlaubte und unerlaubte KI-Nutzung ist für Lernende klar geregelt.	☐	
Emotionserkennung und vergleichbare verbotene Verfahren werden nicht eingesetzt.	☐	
KI-Einsatz bei Zulassung, Einstufung und Noten wurde als mögliches Hochrisiko geprüft.	☐	
Prüfungsmodelle Closed AI, Guided AI oder Open AI sind eindeutig bezeichnet.	☐	
Bewertungskriterien berücksichtigen Produkt, Prozess und Reflexion.	☐	
Dozenten prüfen KI-generierte Materialien fachlich und didaktisch.	☐	
Personendaten von Lernenden werden geschützt.	☐	
Nachvollziehbarkeit und Einsprachemöglichkeiten bleiben gewährleistet.	☐	
Lernende üben Quellenkontrolle, Fehleranalyse und Verantwortung.	☐	
Schulungs- und Prüfungsregeln werden regelmässig aktualisiert.	☐	



17.7 Checkliste G: KI-Agenten und technische Sicherheit

Prüfpunkt	Erledigt	Bemerkungen
Der Agent besitzt nur zwingend notwendige Berechtigungen.	☐	
Test- und Produktivumgebung sind getrennt.	☐	
Administrative Rechte sind ausgeschlossen oder zeitlich streng begrenzt.	☐	
Kritische Aktionen benötigen menschliche Freigabe.	☐	
Tool-Aufrufe und Aktionen werden vollständig protokolliert.	☐	
Kosten-, Laufzeit-, Transaktions- und Datenlimits sind gesetzt.	☐	
Eine Not-Aus- und Sperrfunktion ist vorhanden und getestet.	☐	
Externe Inhalte werden als potenziell nicht vertrauenswürdig behandelt.	☐	
Schutz vor Prompt Injection wurde technisch und organisatorisch geprüft.	☐	
Sicherheits- und Missbrauchstests werden regelmässig durchgeführt.	☐	



17.8 Checkliste H: Laufende Kontrolle und Verbesserung

Prüfpunkt	Erledigt	Bemerkungen
Das KI-Inventar wird bei Änderungen und mindestens periodisch aktualisiert.	☐	
Neue Funktionen und Vertragsänderungen der Anbieter werden geprüft.	☐	
Rechts- und Behördenentwicklungen werden beobachtet.	☐	
Vorfälle, Beschwerden und Fehlresultate werden zentral erfasst.	☐	
Ursachen und Auswirkungen werden nachvollziehbar analysiert.	☐	
Korrekturmassnahmen erhalten Verantwortliche und Termine.	☐	
Richtlinien werden nach relevanten Erkenntnissen angepasst.	☐	
Schulungen werden bei neuen Risiken aktualisiert.	☐	
Wirksamkeit und Nutzung der Kontrollmassnahmen werden überprüft.	☐	
Die Leitung entscheidet über Weiterbetrieb, Einschränkung oder Abschaltung.	☐	