Alliance for Qualification

Release Version 1.00

Juli 2025

A4Q Syllabus

AI Essentials zum

EU AI Act

Copyright Notiz und Disclaimer

© A4Q Copyright 2025 - Copyright Notiz

Alle Inhalte dieses Werks, insbesondere Texte und Grafiken, sind urheberrechtlich geschützt. Die Nutzung und Verwertung des Werks obliegt ausschließlich der A4Q. Insbesondere ist die Vervielfältigung oder Reproduktion des Werks – auch auszugsweise – untersagt. Bei Zuwiderhandlung behält sich die A4Q zivil- und strafrechtliche Schritte vor.

Revision History

Version	Date	Remark
1.00	01.07.2025	Intern geprüftes Dokument (V1.000)

Disclaimer

Die Inhalte dieses Syllabus wurden sorgfältig zusammengestellt und basieren u.a. auf den zum Zeitpunkt der Erstellung verfügbaren gesetzlichen Regelungen, insbesondere der Datenschutz-Grundverordnung (DSGVO) und dem EU AI Act.

Der Syllabus dient ausschließlich der allgemeinen Information. Die dargestellten Zusammenhänge können verkürzt, missverständlich, in falschem Kontext bzw. unpräzise formuliert sein.

Dieser Syllabus stellt ausdrücklich keine rechtliche Beratung dar und kann eine individuelle juristische Prüfung keinesfalls ersetzen.

Für die Umsetzung spezifischer rechtlicher Anforderungen oder die Beurteilung konkreter Sachverhalte wird empfohlen, einen qualifizierten Rechtsanwalt oder eine entsprechend autorisierte Beratungsstelle zu konsultieren.

Die Autoren übernehmen ausdrücklich keinerlei Haftung für Aktualität, Vollständigkeit oder Richtigkeit der dargestellten Informationen sowie für etwaige daraus resultierende Folgen.

Inhalt

Inhalt

Copyright Notice und Disclaimer 2
Inhalt 3
Draft Version (NICHT veröffentlicht) 6
0 Präambel 7
0.1 Zweck des Syllabus 7
0.2 Prüfungsrelevante Lernziele und kognitive Wissensstufen 7
0.3 Die “AI Essentials” Prüfung 7
0.4 Akkreditierung 8
0.5 Detaillierungsgrad 8
0.6 Struktur dieses Syllabus 8
0.7 Business Outcomes (BOs) 10
0.8 Akronyme 11
1 Einführung in das Thema „Künstliche Intelligenz“ (KI) 13
1.1 Was ist Künstliche Intelligenz (KI)? 13
1.2 Beispiele für KI im Alltag 13
1.3 Warum sollten Sie KI verstehen? 14
1.4 Zwei Hauptarten von KI-Systemen 14
1.5 Weitere KI-Technologien im Überblick 16
1.6 Was bedeutet das für Unternehmen? 17
1.7 Zusammenfassung 17
2 Überblick EU AI Act 18
2.1 Einleitung 18
2.2 Zielsetzung des EU AI Act 18
2.3 Geltungsbereich – Wer ist betroffen und ab wann? 18
2.4 Was ist ein KI-System laut AI Act? 19
2.5 Der risikobasierte Ansatz – vier Stufen 20

A4Q AI Essentials
©A4Q Copyright 2025

2.6 Zusammenspiel mit anderen Gesetzen 21
2.7 Internationale Bedeutung 22
2.8 Kritik und Herausforderungen 22
2.9 Chancen und positive Effekte 22
2.10 Fazit 22
3 Transparenz & Kennzeichnung 24
3.1 Einleitung 24
3.2 Was bedeutet Transparenz im EU AI Act? 25
3.3 Rechtsgrundlage: Artikel 52 EU AI Act ..... **Error! Bookmark not defined.**
3.4 Drei Transparenzpflichten im Überblick: 25
3.5 Grenzen und Ausnahmen 26
3.6 Bezug zur DSGVO 27
3.7 Pflichten für Anbieter und Betreiber 27
3.8 Gestaltungshinweise für gute Transparenz 27
3.9 Relevanz für verschiedene Risikoklassen 28
3.10 Zusammenfassung 28
4 Verbindung zu DSGVO-Grundprinzipien 30
4.1 Einleitung 30
4.2 Was sind personenbezogene Daten? 30
4.3 Grundprinzipien der DSGVO 30
4.4 Datenminimierung im KI-Kontext 31
4.5 Rechtsgrundlagen für KI-Systeme 32
4.6 Fazit 32
5 Menschliche Aufsicht 33
5.1 Einleitung 33
5.2 Warum ist menschliche Aufsicht wichtig? 33
5.3 Rechtsgrundlage im EU AI Act 33
5.4 Drei Formen menschlicher Aufsicht 34
5.5 Eingriffsmöglichkeiten und Anforderungen 34

A4Q AI Essentials

©A4Q Copyright 2025

5.6 Beispiele aus der Praxis 35
5.7 Grenzen menschlicher Aufsicht 35
5.8 Fazit 35
6 Risiken & Ethik 37
6.1 Einleitung 37
6.2 Was bedeutet Fairness bei KI? 37
6.3 Was ist Bias? 37
6.4 Beispiele für Diskriminierung durch KI 38
6.5 Gesetzliche Anforderungen 38
6.6 Ethische Leitlinien für vertrauenswürdige KI 38
6.7 Verantwortung im Unternehmen 39
6.8 Was können Organisationen konkret tun? 39
6.9 Fazit 39
7 Einführung in die Gestaltung wirksamer Prompts für KI-Systeme (Prompt Engineering) 41
7.1 Einleitung – Warum ist Prompt Engineering wichtig? 41
7.2 Grundprinzipien guter Prompts 42
7.3 Typische Prompt-Typen mit Beispielen 42
7.4 Häufige Fehler und wie man sie vermeidet 43
7.5 Der Prompt-Feedback-Zyklus (4 Schritte) 43
7.6 Erweiterte Techniken für Fortgeschrittene 43
7.7 Abschlusstipps für die Praxis 43
7.8 Fazit 44
8 Literatur 45

A4Q AI Essentials
©A4Q Copyright 2025

Release Version 1.00

Dieses Dokument wurde am 01.07.2025 offiziell durch die A4Q GmbH veröffentlicht.

©A4Q Copyright 2025

A4Q
AI Essentials

0 Präambel

0.1 Zweck des Syllabus

Dieser Syllabus beschreibt die angestrebten Lernziele (Learning Objectives) und grundlegenden Konzepte der KI-Basisschulung für Mitarbeitende in Organisationen, die KI-Systeme entwickeln, betreiben oder beschaffen. Die Schulung ist für die Anforderungen des EU AI Act, insbesondere gemäß Art. 4(4) zur Förderung von Kompetenz und Bewusstsein im Umgang mit KI konzipiert.

Die Inhalte richten sich an nicht-technische und technische Mitarbeitende und ist als Basismodul mit Fokus auf die wichtigsten Grundlagen konzipiert.

0.2 Prüfungsrelevante Lernziele und kognitive Wissensstufen

Die Lernziele (Learning Objectives) dienen als Grundlage für die Inhalte des abschließenden Tests. Der bestandene Test belegt die erfolgreiche Teilnahme an der Schulung und das Erreichen der Lernziele. Von den Teilnehmenden kann erwartet werden, dass sie Inhalte je Kapitel des Syllabus wiedergeben, Verständnis nachweisen und einfache Szenarien analysieren können.

Die Wissensstufen (Knowledge Levels) der jeweiligen Lernziele (Learning Objectives) werden zu Beginn jedes Kapitels angegeben und wie folgt klassifiziert:

- K1 – Erinnern:
  Fakten, Begriffe und Informationen gezielt abrufen und wiedergeben.
- K2 – Verstehen:
  Bedeutungen erfassen, interpretieren und erklären.
- K3 – Anwenden:
  Anwenden von Wissen in konkreten Situationen oder zur Lösung von Aufgaben.

0.3 Die “AI Essentials” Prüfung

Die „AI Essentials“ Prüfung basiert auf diesem Syllabus. Antworten auf Prüfungsfragen können die Nutzung von Inhalten aus mehreren Abschnitten dieses Syllabus erfordern. Alle Abschnitte des Syllabus sind prüfungsrelevant, mit Ausnahme der Einleitung und der Optional – Kapitel und Anhänge. Standards, Bücher und gesetzliche Vorschriften können als Referenzen herangezogen werden; deren Inhalte sind jedoch nur insoweit prüfungsrelevant, wie sie in diesem Syllabus zusammengefasst sind.

A4Q AI Essentials

©A4Q Copyright 2025

Die Prüfung besteht aus 16 Single-Choice-Fragen. Zu jedem LO wird eine Frage gestellt. Jede richtige Antwort wird mit einem Punkt bewertet. Zum Bestehen der Prüfung ist eine Mindestpunktzahl von 75% (d. h. mindestens 12 korrekt beantwortete Fragen) erforderlich. Für die Bearbeitung der Prüfung stehen 20 Minuten zur Verfügung.

0.4 Akkreditierung

Schulungsanbieter, die Trainings zum *Certified AI Essentials* anbieten möchten, sollten von A4Q akkreditiert sein und die offiziellen Schulungsunterlagen verwenden.

0.5 Detaillierungsgrad

Dieser Syllabus besteht aus:

- Business Objektives die festlegen, was Teilnehmende nach der Lerneinheit konkret leisten können, um geschäftliche Herausforderungen effektiv zu bewältigen.
- allgemeinen Lernzielen, die die Zielsetzung der Zertifizierung beschreiben,
- häufig zusammen mit einer Liste von Begriffen, die die Teilnehmenden erklären können müssen,
- Lernzielen für jedes Wissensgebiet, die den jeweils zu erreichenden kognitiven Lernfortschritt beschreiben,
- einer Beschreibung der entsprechenden zentralen Konzepte, einschließlich Verweisen auf Quellen wie anerkannte Fachliteratur oder Standards.

Der Inhalt des Syllabus stellt keine vollständige Darstellung des gesamten Wissensgebiets der AI Compliance und des EU AI Acts dar, sondern spiegelt den Detaillierungsgrad wider, der in den Schulungen und der Prüfung auf AI Essentials-Level behandelt wird.

Dieser Syllabus enthält keine spezifischen Lernziele in Bezug auf bestimmte Vorgehensmodelle oder Entwicklungsansätze in der Softwareentwicklung, oder der AI-Entwicklung.

0.6 Struktur dieses Syllabus

Der Kurs ist primär als webbasiertes Selbstlerntraining konzipiert; eine Durchführung durch eine qualifizierte Lehrperson kann den Lernerfolg jedoch zusätzlich unterstützen.

Es gibt sechs Kapitel mit prüfungsrelevantem Inhalt. Für jedes Kapitels wird die vorgesehene Zeitdauer angegeben; innerhalb der Kapitel erfolgt keine weitere Zeitangabe auf Unterebene.

A4Q AI Essentials

©A4Q Copyright 2025

Der A4Q AI Essentials-Trainingskurs sieht laut Lehrplan jedenfalls eine Mindestdauer von einer Stunde vor, verteilt auf sechs prüfungsrelevante Kapitel. Da der Kurs online im Internet aufrufbar sein soll, kann die Zeit individuell praktisch beliebig verlängert werden

Kapitel 1: Einführung in KI – 10 Minuten

Kapitel 2: Überblick EU AI Act – 10 Minuten

Kapitel 3: Transparenz & Kennzeichnung – 10 Minuten

Kapitel 4: DSGVO-Grundprinzipien – 10 Minuten

Kapitel 5: Menschliche Aufsicht – 10 Minuten

Kapitel 6: Risiken & Ethik – 10 Minuten

Optional - Kapitel 7: Prompt Engineering Einführung – 15 Minuten

A4Q AI Essentials

©A4Q Copyright 2025

0.7 Business Outcomes (BOs)

Kapitel 1 – KI-Grundlagen:

BO 1.1: Mitarbeitende verstehen grundlegende Konzepte, Funktionsweisen und typische Anwendungsfelder von Künstlicher Intelligenz im beruflichen Kontext.

BO 1.2: Mitarbeitende unterscheiden regelbasierte und lernende KI-Systeme und erkennen deren grundlegende Bedeutung für den risikobasierten Regulierungsansatz des EU AI Act.

Kapitel 2 – Überblick EU AI Act:

BO 2.1: Mitarbeitende kennen das Ziel, den Geltungsbereich und die Idee des EU AI Act in Grundzügen – insbesondere in Bezug auf die regulatorische Zielsetzung.

BO 2.2: Mitarbeitende können KI-Systeme den vier Risikokategorien des EU AI Act – unzulässig, hoch, begrenzt und minimal – zuordnen und verstehen, welche Anforderungen jeweils aus dem EU AI Act resultieren.

Kapitel 3 – Transparenz & Kennzeichnung:

BO 3.1: Mitarbeitende können kennzeichnungspflichtige KI-Anwendungen im Unternehmen identifizieren und sicherstellen, dass deren Einsatz gemäß den Transparenzanforderungen des EU AI Act kommuniziert wird (z. B. bei Chatbots, KI-generierten Inhalten oder biometrischen Analysen).

BO 3.2: Mitarbeitende verstehen die rechtlichen Pflichten zur Offenlegung von KI-Nutzung und können aktiv dazu beitragen, Benutzeroberflächen, Informationshinweise oder Kommunikationsprozesse transparent und regelkonform mitzugestalten.

Kapitel 4 – DSGVO-Grundprinzipien

BO 4.1: Mitarbeitende verstehen die Grundlagen des Datenschutzes nach DSGVO und erkennen, welche Arten von Daten besonders geschützt sind. Sie tragen dadurch aktiv dazu bei, datenschutzkonforme KI-Projekte umzusetzen, unnötige Datenerhebungen zu vermeiden und das Risiko rechtlicher Verstöße und Reputationsschäden für das Unternehmen zu reduzieren.

Kapitel 5 – Menschliche Aufsicht:

BO 5.1: Mitarbeitende wissen, dass KI-Systeme überwacht werden müssen, und können benennen, wie sie im Unternehmen zur menschlichen Kontrolle von KI beitragen.

A4Q AI Essentials

©A4Q Copyright 2025

Kapitel 6 – Risiken & Ethik:

BO 6.1: Mitarbeitende erkennen Risiken von Diskriminierung durch KI-Systeme frühzeitig und fördern so faire, gesetzeskonforme und verantwortungsvolle Entscheidungen im Unternehmen.

Optional-Kapitel 7 – Einführung in das Prompt Engineering (Nicht prüfungsrelevant)

BO 7.1: Mitarbeitende können KI-Systeme effizienter und zielgerichteter einsetzen, da sie in der Lage sind, Prompts klar, kontextbezogen und unternehmensrelevant zu formulieren.

0.8 Akronyme

Verwendete Abkürzungen und ihre Erklärungen

Abkürzung	Erklärung
AI	Artificial Intelligence (Künstliche Intelligenz)
A4Q	Alliance for Qualification
BOs	Business Outcomes
DSGVO	Datenschutz-Grundverordnung
EU AI Act	Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz
HITL	Mensch in der Schleife (Human-in-the-Loop)
HOOTL	Mensch außerhalb der Schleife (Human-out-of-the-Loop)
HOTL	Mensch überwachend in der Schleife (Human-on-the-Loop)
K1	Erinnern (Wissensstufe)
K2	Verstehen (Wissensstufe)
K3	Anwenden (Wissensstufe)
KI	Künstliche Intelligenz

A4Q AI Essentials ©A4Q Copyright 2025

Abkürzung	Erklärung
LOs	Lernziele (Learning Objectives)
ML	Maschinelles Lernen
NLP	Natural Language Processing
RLHF	Reinforcement Learning from Human Feedback (Kontext Sprachmodelle)
SIEM	Security Information and Event Management
TLS	Transport Layer Security (Verschlüsselungsprotokoll)
TOM	Technische und organisatorische Maßnahmen

A4Q AI Essentials

©A4Q Copyright 2025

1 Einführung in das Thema „Künstliche Intelligenz“ (KI)

Dauer: ca. 10 Minuten

Lernziele dieses Kapitels (LOs):

LO 1.1: Künstliche Intelligenz definieren und von klassischer Software abgrenzen (K1)

LO 1.2: Arten von KI-Systemen (regelbasiert vs. maschinelles Lernen) unterscheiden (K2)

LO 1.3: Relevanz der KI-Unterscheidung im Kontext des EU AI Act begründen (K2)

1.1 Was ist Künstliche Intelligenz (KI)?

Künstliche Intelligenz – kurz KI oder international AI (Artificial Intelligence) – bezeichnet die Fähigkeit von Maschinen und Computersystemen, Aufgaben auszuführen, die typischerweise menschliche Intelligenz erfordern. Dazu gehören unter anderem das Erkennen von Sprache, das Verstehen von Texten, das Treffen von Entscheidungen, das Erkennen von Bildern und Mustern sowie das Lernen aus Erfahrung.

Anders gesagt: KI-Systeme können Informationen aufnehmen, analysieren, interpretieren und daraus Schlussfolgerungen ziehen oder Empfehlungen ableiten – oft schneller und in größerem Umfang als der Mensch.

KI ist ein Sammelbegriff für viele Technologien – von einfachen regelbasierten Entscheidungsstrukturen bis hin zu komplexen lernenden Systemen (z. B. neuronalen Netzen), die mit riesigen Datenmengen trainiert werden.

1.2 Beispiele für KI im Alltag

KI ist längst in unserem Alltag und Berufsleben angekommen. Typische Anwendungen sind:

- **Sprachassistenten** wie Siri, Alexa oder Google Assistant – zur Terminplanung, Informationsermittlung oder Diktat im Büroalltag.
- **Navigationssysteme mit Echtzeit-Verkehrsdaten** – etwa für Außendienst, Logistik und Transportplanung.
- **Empfehlungsfunktionen** bei YouTube, Netflix oder Amazon – vergleichbar mit personalisierten Lernplattformen, CRM-Systemen oder Produktvorschlägen im E-Commerce.
- **Chatbots im Kundenservice** – beantworten Anfragen, filtern Tickets vor oder unterstützen beim Self-Service rund um die Uhr.
- **Gesichtserkennung** – z. B. für Zutrittskontrolle zu Gebäuden oder Login-Prozesse an gesicherten Arbeitsplätzen.

A4Q AI Essentials

©A4Q Copyright 2025

- **Kredit-Scoring und Risikoprüfung** – im Banken- und Versicherungswesen zur automatisierten Bewertung von Anträgen oder Bonitätsprüfungen.
- **KI-gestützte Dokumentenklassifikation** – automatisches Erfassen, Zuordnen und Bearbeiten von Rechnungen, Verträgen oder E-Mails.
- **Bewerbungsscreening und Lebenslaufanalyse** – automatisierte Vorauswahl von Kandidat:innen in HR-Abteilungen.
- **Predictive Maintenance** – Vorhersage von Wartungsbedarf bei Maschinen in der Industrieproduktion.
- **Verkaufs- und Umsatzprognosen** – in Vertrieb und Controlling zur datenbasierten Entscheidungsunterstützung.
- **Texterstellung durch generative KI** – z. B. für Produktbeschreibungen, E-Mail-Vorschläge oder Social-Media-Beiträge im Marketing.
- **Übersetzungstools mit KI** – automatische Textübersetzung für internationale Kommunikation oder Dokumentenverarbeitung.

Diese Anwendungen machen deutlich, dass KI bereits heute Entscheidungen beeinflusst – oft ohne dass es den Nutzenden bewusst ist. Genau deshalb ist es wichtig, ein Grundverständnis zu entwickeln.

1.3 Warum sollten Sie KI verstehen?

Die Funktionsweise von KI zu verstehen ist entscheidend, um sie im Unternehmen **rechtskonform, ethisch und sicher** einsetzen zu können. Gerade im Rahmen des **EU AI Act**, der spezifische Anforderungen an den Einsatz von KI stellt, ist dieses Wissen unerlässlich.

Ein grundlegendes Verständnis hilft dabei:

- Risiken einzuschätzen
- geeignete Maßnahmen zur Überwachung oder Dokumentation zu ergreifen
- und zu erkennen, wann externe Unterstützung notwendig ist

1.4 Zwei Hauptarten von KI-Systemen

Im Rahmen dieser Basisschulung unterscheiden wir zwei grundlegende Formen:

1. Regelbasierte KI

A4Q AI Essentials

©A4Q Copyright 2025

Diese Systeme arbeiten mit fest einprogrammierten **Wenn-Dann-Regeln**.

Beispiel:
„Wenn die Spesen über 150 € liegen, leite zur Genehmigung weiter."

Merkmale:

- Kein Lernen aus Daten
- Klare, nachvollziehbare Logik
- Geringe Komplexität
- Sehr gut prüfbar und dokumentierbar

Vorteil: Transparent und zuverlässig bei klaren Regeln
Nachteil: Nicht flexibel bei neuen oder unvorhersehbaren Situationen

2. Maschinelles Lernen (ML)

Hier lernt das System **selbstständig aus Daten** – es erkennt Muster und leitet Entscheidungen ab, ohne dass jede Regel vorgegeben ist.

Beispiel:
Ein System analysiert Bewerbungsunterlagen und lernt, welche Merkmale mit erfolgreichen Einstellungen zusammenhängen.

Typen von ML:

Überwachtes Lernen:
Beispiel: Ein KI-System wird mit Lebensläufen und der Info „eingestellt" oder „abgelehnt" trainiert. Es lernt, neue Bewerbungen anhand dieser Muster zu bewerten.

Unüberwachtes Lernen:
Beispiel: Eine KI analysiert Kundendaten ohne Vorgaben und erkennt automatisch Gruppen mit ähnlichem Kaufverhalten (z. B. „Schnäppchenjäger", „Markentreue").

Bestärkendes Lernen:
Beispiel: Ein Roboter lernt, ein Objekt aufzuheben, indem er für erfolgreiche Versuche Belohnung erhält und für Fehlgriffe keine – so verbessert er sein Verhalten über viele Durchläufe.

Merkmale:

- Lernfähig und leistungsstark
- Hohe Flexibilität
- Teilweise schwer nachvollziehbare Entscheidungen (*Black Box*)

A4Q AI Essentials
©A4Q Copyright 2025

- Abhängigkeit von Datenqualität und Datenmenge

1.5 Warum ist diese Unterscheidung für den EU AI Act wichtig?

Das Risikopotenzial ist unterschiedlich hoch

Regelbasierte Systeme (z. B. „Wenn A, dann B“) sind **transparent, vorhersehbar und gut prüfbar**. Ihr Verhalten lässt sich deterministisch nachvollziehen.

Maschinelles Lernen (ML) nutzt Daten, erkennt Muster selbstständig und trifft Entscheidungen, die **nicht vollständig erklärbar** sein müssen. Das birgt Risiken wie:

- Intransparente Entscheidungslogik (Black Box)
- Bias und Diskriminierung durch fehlerhafte Trainingsdaten
- schwer prüfbare oder reproduzierbare Ergebnisse

→ **ML-Systeme haben deshalb ein höheres Risiko** und fallen häufiger unter Hochrisiko-Kategorien.

Die Pflichten nach Risiko richten sich oft indirekt nach der Art der KI

Der EU AI Act regelt zwar nach Anwendungsbereich und Risiko, nicht nach Technologie. In der Praxis zeigt sich aber:

- **ML-basierte Systeme** in Bereichen wie Personalmanagement, Kreditvergabe, Medizin oder Strafverfolgung werden **regelmäßig als Hochrisiko** eingestuft.
- **Regelbasierte Systeme** mit identischer Funktion können teilweise **unter geringeres Risiko** fallen, weil sie erklärbar und kontrollierbar sind.

Fazit: Organisationen, die ML-basierte Systeme einsetzen, müssen mit **höherem regulatorischem Aufwand, mehr Dokumentationspflichten und intensiveren Prüfverfahren** rechnen. Ein systematisches Verständnis dieser Unterschiede hilft daher bei der Risikoklassifizierung, Systembewertung und Einhaltung der regulatorischen Anforderungen.

1.6 Weitere KI-Technologien im Überblick

Neben den beiden Grundtypen gibt es spezialisierte Formen:

- **Deep Learning:** Neuronale Netze mit vielen Schichten – stark bei Spracherkennung und Bildanalyse
- **NLP (Natural Language Processing):** Versteht und verarbeitet menschliche Sprache (z. B. Chatbots, Übersetzungen)

A4Q AI Essentials

©A4Q Copyright 2025

- **Computer Vision:** Erkennt Inhalte in Bildern und Videos
- **Generative KI:** Erzeugt neue Texte, Bilder oder Musik (z. B. ChatGPT, DALL·E)

1.7 Was bedeutet das für Unternehmen?

Unternehmen müssen unterscheiden können:

- welche Art von KI sie einsetzen
- wie nachvollziehbar und kontrollierbar deren Entscheidungen sind
- ob sie unter den **EU AI Act** als Hochrisiko-Systeme fallen
- welche KI-Anwendungen unter die verbotenen Praktiken des EU AI Act fallen – etwa manipulative Systeme, soziale Bewertung (Social Scoring) oder ungerechtfertigte emotionale Überwachung

Insbesondere bei der Entwicklung oder Beschaffung von Systemen ist es entscheidend, diese Grundlagen zu verstehen, um Haftungsrisiken, Reputationsschäden oder gesetzliche Verstöße zu vermeiden.

1.8 Zusammenfassung

- **KI** beschreibt Systeme, die menschenähnliches Verhalten nachbilden.
- Es gibt **regelbasierte Systeme** (nach festen Regeln) und **lernende Systeme** (Maschinelles Lernen).
- **Maschinelles Lernen** ist flexibler, aber auch weniger transparent – daher im EU AI Act besonders stark reguliert.
- Das Wissen über diese Grundlagen ist wichtig für **Compliance, Risikomanagement und Governance**.

A4Q AI Essentials

©A4Q Copyright 2025

2 Überblick EU AI Act

Dauer: ca. 10 Minuten

Lernziele dieses Kapitels (LOs):

LO 2.1: Ziel und Grundprinzipien des EU AI Act benennen (K1)

LO 2.2: Den Anwendungsbereich des EU AI Act auf Anbieter, Betreiber und internationale Kontexte beschreiben (K2)

LO 2.3: Die Definition eines KI-Systems im Sinne des EU AI Act wiedergeben und erläutern (K2)

LO 2.4: Die vier Risikoklassen des EU AI Act benennen und ihre Unterschiede erläutern (K2)

2.1 Einleitung

Der **EU AI Act** ist das weltweit erste umfassende Gesetz zur Regulierung von Künstlicher Intelligenz (KI). Er wurde im **Mai 2024 offiziell veröffentlicht** und ist im **Juni 2024 in Kraft getreten**. Ziel ist es, die technologische Entwicklung von KI zu fördern und zugleich grundlegende Werte wie **Menschenrechte, Sicherheit und Transparenz** zu wahren.

Der Act bietet einen gemeinsamen, rechtssicheren Rahmen für alle EU-Mitgliedstaaten und soll sicherstellen, dass KI in Europa **ethisch, verantwortungsvoll und vertrauenswürdig** eingesetzt wird.

2.2 Zielsetzung des EU AI Act

Der AI Act verfolgt vier zentrale Ziele:

1. **Grundrechtsschutz**: Vermeidung von Diskriminierung, Verletzung der Privatsphäre oder automatisierter Willkür
2. **Vertrauensaufbau**: Förderung der Akzeptanz von KI durch Transparenz und Nachvollziehbarkeit
3. **Rechtssicherheit**: Einheitlicher Rechtsrahmen für alle Beteiligten innerhalb der EU
4. **Förderung von Innovation**: Ermöglichung wettbewerbsfähiger und sicherer KI-Entwicklung durch klare Regeln

Der risikobasierte Ansatz des Gesetzes stellt sicher, dass der regulatorische Aufwand sich am tatsächlichen Gefährdungspotenzial eines Systems orientiert.

2.3 Geltungsbereich – Wer ist betroffen und ab wann?

Der Geltungsbereich des EU AI Act ist sehr weit gefasst. Er betrifft:

- **Anbieter (Hersteller)** von KI-Systemen

A4Q AI Essentials ©A4Q Copyright 2025

- **Importeure und Händler** von KI-Produkten
- **Betreiber und Anwender**, also Organisationen, die KI intern einsetzen
- **Bereitsteller von KI-Diensten**, z. B. über Cloud-Plattformen
- **Öffentliche Stellen**, z. B. Behörden, Schulen, Hochschulen, Gesundheitseinrichtungen
- **Private Unternehmen** jeder Größe, vom Start-up bis zum Konzern
- **Internationale Anbieter**, wenn ihre Systeme in der EU verwendet werden

Die Regeln gelten also auch für **außereuropäische Unternehmen**, sofern sie KI-Systeme in der EU bereitstellen oder anwenden.

Was gilt ab wann? – Zeitplan für die Umsetzung (Stand: Juni 2025)

Zeitpunkt	Regelung
Juni 2024	Inkrafttreten des EU AI Act
ab Ende 2024	Verbotene KI-Praktiken sind sofort verboten und dürfen nicht angeboten oder genutzt werden
ab Mitte 2025 (12 Monate nach T0)	Erste Pflichten für General-Purpose AI (GPAI) – z. B. Transparenzpflichten, Dokumentationsanforderungen
ab Mitte 2026 (24 Monate nach T0)	Hauptpflichten für Hochrisiko-KI-Systeme treten in Kraft (z. B. Konformität, Risikomanagement, Aufsicht)
ab 2027 (36 Monate nach T0)	Vollanwendung inkl. Marktaufsicht, Sanktionen, Meldepflichten und EU-KI-Datenbank

2.4 Was ist ein KI-System laut AI-Act?

Ein KI-System ist laut EU AI Act jede Software, die mit gewisser Autonomie Ziele verfolgt und dabei Technologien wie:

- **Maschinelles Lernen (ML)**
- **Logik- und Regelbasierte Systeme**
- **Statistische Verfahren**

einsetzt, um **aus Daten Muster zu erkennen, Vorhersagen zu treffen oder Entscheidungen zu unterstützen**.

A4Q AI Essentials

©A4Q Copyright 2025

Die Definition ist technologieoffen, um auch künftige Ansätze (z. B. hybride Systeme, multimodale Modelle) einzubeziehen.

2.5 Der risikobasierte Ansatz – vier Stufen

Die Risikokategorien im EU AI Act – Einfach erklärt

Der EU AI Act unterteilt KI-Systeme in vier Risikostufen. Je höher das Risiko für Menschen oder Gesellschaft, desto strenger die gesetzlichen Vorgaben:

1. Verbotene KI-Praktiken (Unzulässiges Risiko)

Diese Systeme sind in der EU **grundsätzlich verboten**, weil sie die **Menschenwürde, Grundrechte oder demokratische Werte** gefährden.

Beispiele für verbotene Anwendungen:

- **Social Scoring:** Bewertung des Verhaltens von Menschen, auch durch Behörden
- **Manipulative Systeme:** KI, die gezielt Schwächen oder Abhängigkeiten ausnutzt
- **Emotionserkennung am Arbeitsplatz oder in der Schule**
- **Biometrische Fernüberwachung in Echtzeit** im öffentlichen Raum (z. B. per Gesichtserkennung) – **nur in sehr engen Ausnahmen erlaubt**

2. Hochrisiko-KI-Systeme

Diese Systeme kommen in **sensiblen Bereichen** zum Einsatz, in denen KI-Entscheidungen trifft, die für Menschen wichtige Folgen haben können.

Typische Einsatzbereiche:

- Bewerbungsverfahren & Personalmanagement
- Kreditvergabe & Zugang zu Finanzprodukten
- Polizei, Justiz & Strafverfolgung
- Medizin & Diagnostik
- Bildung & Prüfungssysteme
- Migrations- und Grenzkontrollen

Für Hochrisiko-Systeme gelten strenge Auflagen:

- Ein **Risikomanagementsystem** muss Gefahren erkennen und minimieren
- Die verwendeten **Daten müssen hochwertig und fair** sein (keine Diskriminierung)

A4Q AI Essentials ©A4Q Copyright 2025

- Es braucht **klare technische Dokumentation**
- Nutzer:innen müssen die **Funktionsweise nachvollziehen** können
- Es ist eine **menschliche Aufsicht** vorgeschrieben (z. B. Eingriffsmöglichkeiten)
- Das System muss **zertifiziert** werden, bevor es auf den Markt kommt
- Es sind **laufende Überwachung und Meldung von Problemen** vorgeschrieben

3. KI mit begrenztem Risiko

Diese Systeme können Menschen beeinflussen, aber in **überschaubarem Rahmen** – z. B. durch Kommunikation oder automatische Inhalte.

Beispiele:

- Chatbots
- Generative KI (z. B. Text- oder Bildgeneratoren)

Pflicht:
Nutzer:innen müssen **klar erkennen können**, dass sie mit einer KI interagieren oder dass Inhalte KI-generiert sind (z. B. durch Hinweise oder Kennzeichnungen).

4. Minimales Risiko

Die meisten KI-Anwendungen gehören in diese Kategorie. Sie gelten als **unbedenklich** und **haben kaum Einfluss auf Rechte oder Sicherheit**.

Beispiele:

- Spamfilter
- Produktempfehlungen in Online-Shops
- Autokorrektur oder Rechtschreibprüfung

Regelung:
Für diese Systeme gelten **keine gesetzlichen Pflichten**. Es wird aber empfohlen, **ethische Grundprinzipien wie Fairness, Datenschutz und Sicherheit** freiwillig zu beachten.

2.6 Zusammenspiel mit anderen Gesetzen

Der EU AI Act ergänzt bestehende Vorschriften, z. B.:

- **DSGVO** (Datenschutz-Grundverordnung)

A4Q AI Essentials
©A4Q Copyright 2025

- **Produktsicherheitsgesetz**
- **Medizinprodukteverordnung**
- **Sektorale Vorschriften** (z. B. im Finanzwesen)

Organisationen müssen sicherstellen, dass sie auch **datenschutzrechtliche Anforderungen** parallel erfüllen, insbesondere wenn KI personenbezogene Daten verarbeitet.

2.7 Internationale Bedeutung

- Der EU AI Act wirkt über die EU hinaus.
- Er beeinflusst globale Anbieter, da sie sich bei KI-Exporten in die EU anpassen müssen.
- Er gilt als **Referenzrahmen für andere Länder**, vergleichbar mit der DSGVO im Datenschutzbereich.
- Erste Staaten (z. B. Kanada, Brasilien, Japan) entwickeln bereits ähnliche Regelungen.

2.8 Kritik und Herausforderungen

Kritikpunkte am EU AI Act:

- hoher administrativer Aufwand, v. a. für KMU
- schwierige Risikoeinstufung bei komplexen Systemen
- Innovationshemmnisse durch Überregulierung befürchtet
- fehlende Praxisleitlinien zur Anwendung (noch in Arbeit)

2.9 Chancen und positive Effekte

Trotz Herausforderungen bietet der Act wichtige Vorteile:

- **Vertrauen und Sicherheit** im Markt
- **Wettbewerbsvorteil** durch geprüfte Systeme
- **Klarheit und Einheitlichkeit** statt nationaler Alleingänge
- **Schutz vor Reputationsrisiken und Haftungsfällen**
- **Transparente Rahmenbedingungen für Forschung und Entwicklung**

2.10Fazit

Der EU AI Act ist ein Meilenstein für die Entwicklung und Nutzung von vertrauenswürdiger KI in Europa. Für alle Organisationen mit KI-Bezug bedeutet das:

A4Q AI Essentials

©A4Q Copyright 2025

- **Sofortige Prüfung** verbotener Praktiken
- **Schrittweise Vorbereitung** auf Hochrisiko-Pflichten bis 2026
- **Stärkung interner Governance, Transparenz und Compliance**

Je früher mit der Umsetzung begonnen wird, desto geringer sind langfristige Risiken und Umstellungskosten.

A4Q AI Essentials

©A4Q Copyright 2025

3 Transparenz & Kennzeichnung

Dauer: ca. 10 Minuten

Lernziele dieses Kapitels (LOs):

LO 3.1: Die Bedeutung von Transparenz im EU AI Act benennen (K1)

LO 3.2: Transparenzpflichten kennen (z.B. Interaktion, generative KI) aufzählen (K1)

LO 3.3: Die Transparenzanforderungen für Anbieter und Betreiber von KI-Systemen beschreiben (K2)

3.1 Einleitung

Transparenz ist eines der grundlegenden Prinzipien des EU AI Act – und ein entscheidender Faktor für die Vertrauenswürdigkeit von Künstlicher Intelligenz im Alltag wie im beruflichen Umfeld. Nur wenn Menschen verstehen, dass und wie eine KI beteiligt ist, können sie fundierte Entscheidungen treffen, Risiken einschätzen und ihre Rechte wahrnehmen.

Der Gesetzgeber geht davon aus, dass viele KI-Systeme auf eine Weise agieren, die für Laien nicht direkt als „nicht-menschlich“ erkennbar ist. Deshalb verpflichtet der EU AI Act Anbieter und Betreiber dazu, klar und rechtzeitig offenzulegen, wenn eine KI eine Rolle spielt – sei es in der Kommunikation, bei Entscheidungen oder bei der Erzeugung von Inhalten.

Diese Transparenz soll nicht nur Täuschung vermeiden, sondern auch autonomes Handeln und informierte Einwilligung ermöglichen. Die betroffenen Personen müssen nachvollziehen können, was die KI tut, auf welcher Grundlage sie dies tut und welche Folgen daraus entstehen können.

Beispielsweise besonders betroffen sind KI-Systeme, die:

- **mit Menschen interagieren**, z. B. in Form von Chatbots, Sprachassistenten oder automatisierten Dialogsystemen
- **Inhalte erzeugen**, die für menschlich geschaffene Texte, Bilder oder Videos gehalten werden könnten (z. B. bei generativer KI)

In solchen Fällen besteht die Gefahr, dass Nutzer:innen die KI entweder nicht erkennen oder ihr mehr Autorität oder Menschlichkeit zuschreiben, als tatsächlich gerechtfertigt wäre.

Ziel der Transparenzpflichten ist es daher:

- **Irreführung zu verhindern**, z. B. durch vermeintlich „menschliche“ Kommunikation oder nicht gekennzeichnete KI-generierte Inhalte
- **Persönliche Autonomie zu schützen**, also die Fähigkeit, auf Basis klarer Informationen zu entscheiden

A4Q AI Essentials

©A4Q Copyright 2025

- **Vertrauen in KI-Anwendungen zu fördern**, indem Anbieter Verantwortung übernehmen und ihren Einsatz offenlegen

Transparenz ist damit nicht nur ein rechtlicher Mechanismus, sondern auch ein Instrument zur Förderung von ethischem, sicherem und akzeptierten KI-Einsatz – ein zentrales Anliegen des EU AI Act.

3.2 Was bedeutet Transparenz im EU AI Act?

Transparenz ist eines der wichtigsten Mittel, um Nutzer:innen in die Lage zu versetzen, informierte Entscheidungen im Umgang mit KI-Systemen zu treffen. Im Kontext des EU AI Act bedeutet Transparenz: Menschen müssen wissen, dass sie es mit KI zu tun haben – und in welcher Form.

Der Einsatz von Künstlicher Intelligenz darf nicht „unsichtbar" bleiben, wenn dadurch das Vertrauen, die Selbstbestimmung oder die Rechte der Betroffenen beeinträchtigt werden könnten.

Konkret heißt das: Betroffene müssen unter anderem erkennen können,

- **dass sie mit einem KI-System interagieren** (z. B. wenn sie mit einem Chatbot kommunizieren),
- **dass Inhalte von einem KI-System erzeugt wurden** (z. B. Texte, Bilder, Videos),

Diese Pflicht gilt **immer dann**, wenn der KI-Einsatz für eine durchschnittliche Nutzerin oder einen durchschnittlichen Nutzer **nicht offensichtlich erkennbar ist**. Es soll verhindert werden, dass Menschen KI-Systeme für menschliche Interaktionspartner, neutrale Information oder nicht-automatisierte Prozesse halten – was ihre Einschätzung oder ihr Verhalten beeinflussen könnte.

3.3 Transparenzpflichten im Überblick:

1. Interaktion mit KI-Systemen

Wann relevant:
Wenn eine KI so gestaltet ist, dass sie als Mensch wirken kann – z. B. durch Sprache, Erscheinung oder Interaktion.

Typische Beispiele:

- Chatbots im Kundenservice
- Sprachassistenten mit menschenähnlicher Stimme

Pflicht:
Nutzer:innen muss **klar, rechtzeitig und in verständlicher Sprache** mitgeteilt werden, dass sie mit einem KI-System sprechen.
Beispiel:

„Dieses Gespräch wird von einem KI-System geführt."

©A4Q Copyright 2025

Ziel:

Missverständnisse und unbeabsichtigte Täuschung vermeiden, besonders in sensiblen Kontexten wie Bewerbungsgesprächen oder rechtlicher Beratung.

2. Generative KI-Systeme

Wann relevant:

Wenn Inhalte (Text, Bild, Ton, Video) durch KI erzeugt und veröffentlicht werden.

Typische Beispiele:

- automatisch generierte Produkttexte im Onlinehandel
- KI-erstellte Bilder oder Bewerbungsfotos
- synthetische Stimmen („Deepfakes“) in Medienbeiträgen

Pflicht:

Solche Inhalte müssen **klar als KI-generiert** gekennzeichnet werden.

Beispiel:

„Dieser Text wurde automatisch von einem KI-System erzeugt.“

Empfehlung:

- **Technische Kennzeichnung** wie Wasserzeichen, Metadaten oder maschinenlesbare Labels
- Hinweise an der sichtbaren Nutzeroberfläche, z. B. durch Symbole oder Infoboxen

Ziel:

Vermeidung von Täuschung, insbesondere im Kontext von Meinungsbildung, Desinformation oder Urheberrecht.

3.4 Grenzen und Ausnahmen

In bestimmten Fällen kann auf die Kennzeichnung verzichtet werden, z. B.:

- wenn gesetzliche Geheimhaltung besteht (z. B. verdeckte Ermittlungen),
- wenn die Offenlegung den Zweck gefährden würde (z. B. Sicherheit),
- wenn der KI-Einsatz **offensichtlich erkennbar** ist (z. B. digital animierte Avatare).

Grundsatz:

Im Zweifel ist die **offene Kommunikation über KI-Einsatz vorzuziehen**, um Missverständnisse, Beschwerden oder rechtliche Risiken zu vermeiden.

A4Q AI Essentials

©A4Q Copyright 2025

3.5 Bezug zur DSGVO

Die Transparenzpflicht im AI Act **ergänzt** die bereits bestehenden **Informationspflichten aus der DSGVO** (Art. 12–14), indem sie nicht nur personenbezogene Daten schützt, sondern auch:

- auf den **technischen Ursprung** von Entscheidungen oder Inhalten hinweist,
- die **Interaktion mit KI** in den Vordergrund stellt,
- die **informierte Einwilligung** oder bewusste Entscheidung ermöglicht.

Beispiel:
Eine automatische Ablehnung durch ein KI-gestütztes Kreditbewertungssystem muss sowohl **nach DSGVO** begründet als auch **nach AI Act** als KI-basiert kenntlich gemacht werden.

3.6 Pflichten für Anbieter und Betreiber

Sowohl Anbieter als auch Betreiber eines KI-Systems tragen Verantwortung dafür, dass die gesetzlichen Transparenzanforderungen im Sinne des EU AI Act vollständig und korrekt umgesetzt werden.

- **Anbieter** (also Entwickler oder Verkäufer eines KI-Systems) sind verantwortlich für die **grundlegende Kennzeichnung und Dokumentation**.
- **Betreiber** (z. B. Unternehmen, Behörden, Bildungseinrichtungen) müssen sicherstellen, dass das System **im realen Einsatz korrekt informiert** und alle Hinweise technisch sichtbar und organisatorisch eingebunden sind.

Konkret bedeutet das:

- Gestaltung von Benutzeroberflächen mit **klaren, gut sichtbaren Hinweisen**
- Integration von **Tooltips, akustischen Signalen** oder Bildschirmtexten
- **Schulung von Mitarbeitenden** im Umgang mit der Transparenzpflicht
- **Dokumentation** der eingesetzten Informationsmechanismen und deren Umsetzung

3.7 Gestaltungshinweise für gute Transparenz

Damit Transparenz wirksam ist und den Anforderungen des EU AI Act entspricht, kommt es auf eine **zielgruppengerechte und verständliche Gestaltung** an. Die Informationen müssen nicht nur vorhanden, sondern auch **so gestaltet sein, dass sie wahrgenommen und verstanden werden können**.

Empfohlene Maßnahmen:

A4Q AI Essentials
©A4Q Copyright 2025

Klar und einfach formulieren:
Verwenden Sie einfache, verständliche Sprache – ohne technische oder juristische Fachbegriffe. Die Hinweise sollten eindeutig vermitteln, dass es sich um eine KI-Anwendung handelt.

Hinweise vor der Interaktion geben:
Transparenz muss rechtzeitig erfolgen – also **vor** dem Beginn der KI-Interaktion oder -Analyse. Ein späterer Hinweis genügt nicht den gesetzlichen Anforderungen.

Symbole oder Icons ergänzen:
Visuelle Hinweise (z. B. ein KI-Symbol oder ein stilisierter Roboter) können dabei helfen, Informationen intuitiv zu vermitteln – insbesondere bei nicht-textlichen Interfaces.

Barrierefreiheit sicherstellen:
Die Hinweise müssen auch für Personen mit Einschränkungen zugänglich sein – z. B. durch **Screenreader-Kompatibilität**, klare Kontraste, Vorlesefunktionen oder visuelle Alternativen.

3.8 Relevanz für verschiedene Risikoklassen

Transparenzanforderungen gelten nicht einheitlich für alle KI-Systeme – sie hängen von der **Risikokategorie** ab:

- **Bei KI-Systemen mit begrenztem Risiko**
  Transparenzpflichten sind **verpflichtend** (Art. 52). Diese Systeme dürfen nur betrieben werden, wenn Nutzer:innen korrekt und rechtzeitig informiert werden.
- **Bei Hochrisiko-KI-Systemen**
  Es gelten **zusätzliche Offenlegungs- und Dokumentationspflichten** (z. B. Art. 13 und 14), die über die reine Kennzeichnung hinausgehen – z. B. Erklärbarkeit, Nutzerschulungen, Risikoaufklärung.
- **Bei Systemen mit minimalem Risiko**
  Transparenz ist nicht gesetzlich vorgeschrieben, aber aus ethischen oder reputationsbezogenen Gründen ausdrücklich empfohlen – etwa zur Förderung von Kundenvertrauen und freiwilliger Verantwortung.

3.9 Zusammenfassung

- Transparenz bedeutet: Menschen sollen wissen, wann KI beteiligt ist.
- Art. 52 des EU AI Act verpflichtet zur Offenlegung bei **Interaktion**, **Emotionserkennung** und **generativer KI**.
- Die Informationspflicht gilt immer dann, wenn die KI-Nutzung nicht offensichtlich ist.

A4Q AI Essentials
©A4Q Copyright 2025

- Anbieter und Betreiber teilen sich die Verantwortung – in Entwicklung, Anwendung und Kommunikation.
- Transparenz ist nicht nur rechtlich erforderlich, sondern auch **ethisch und vertrauensbildend**.

©A4Q Copyright 2025

4 Verbindung zu DSGVO-Grundprinzipien

Dauer ca. 10 Minuten

Lernziele dieses Kapitels (LOs):

LO 4.1: Personenbezogene Daten benennen und deren besondere Schutzbedürftigkeit im Datenschutz beschreiben (K2)

LO 4.2: Das Prinzip der Datenminimierung im Datenschutz benennen und einfache Beispiele dafür wiedergeben (K1)

4.1 Einleitung

Die Datenschutz-Grundverordnung (DSGVO) bildet seit Mai 2018 das zentrale Datenschutzrecht in der Europäischen Union. Sie regelt, wie personenbezogene Daten verarbeitet werden dürfen und welche Rechte betroffene Personen dabei haben.

Auch im Kontext von Künstlicher Intelligenz (KI) spielt die DSGVO eine entscheidende Rolle – insbesondere dann, wenn KI-Systeme Daten verarbeiten, mit denen Menschen identifiziert werden können oder Rückschlüsse auf sie möglich sind.

Wer KI in der EU entwickelt, einsetzt oder bereitstellt, muss deshalb nicht nur die Anforderungen des EU AI Act, sondern auch die der DSGVO erfüllen.

4.2 Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dazu zählen unter anderem:

- Name, Adresse, Geburtsdatum
- E-Mail-Adresse, Telefonnummer
- IP-Adressen, Standortdaten
- Gesundheits- und biometrische Daten
- Online-Kennungen oder Verhaltensmuster

Beispiel:
Ein KI-gestütztes Bewerbungstool, das Lebensläufe verarbeitet, wertet personenbezogene Daten aus und fällt damit unter die DSGVO.

4.3 Grundprinzipien der DSGVO

Die DSGVO legt in Artikel 5 sieben zentrale Grundsätze fest, die für jede Datenverarbeitung gelten – auch im Zusammenhang mit KI-Systemen.

A4Q AI Essentials
©A4Q Copyright 2025

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
    - Es muss eine rechtliche Grundlage für die Datenverarbeitung vorliegen (z. B. Einwilligung, Vertrag).
    - Die Verarbeitung muss fair und nachvollziehbar sein.
    - Betroffene Personen müssen wissen, was mit ihren Daten geschieht.
2. Zweckbindung
    - Daten dürfen nur für vorher klar definierte und legitime Zwecke verwendet werden.
    - Eine spätere Nutzung zu anderen Zwecken ist nur eingeschränkt zulässig.
3. Datenminimierung
    - Es dürfen nur Daten erhoben werden, die für den jeweiligen Zweck erforderlich sind.
    - Überflüssige oder unnötig detaillierte Informationen sind zu vermeiden.
4. Richtigkeit
    - Daten müssen korrekt, vollständig und aktuell sein.
    - Falsche Daten sind zu berichtigen oder zu löschen.
5. Speicherbegrenzung
    - Daten dürfen nur so lange gespeichert werden, wie sie für den jeweiligen Zweck erforderlich sind.
    - Löschfristen oder Anonymisierungsmaßnahmen müssen vorgesehen werden.
6. Integrität und Vertraulichkeit
    - Daten sind vor unbefugtem Zugriff, Manipulation oder Verlust zu schützen.
    - Es sind geeignete technische und organisatorische Sicherheitsmaßnahmen erforderlich.
7. Rechenschaftspflicht (Accountability)
    - Verantwortliche müssen die Einhaltung aller Datenschutzprinzipien nachweisen können.
    - Dazu gehören Dokumentationen, Prozesse, Rollenbeschreibungen und interne Schulungen.

4.4 Datenminimierung im KI-Kontext

Das Prinzip der Datenminimierung ist im Bereich der KI besonders herausfordernd, da viele Systeme große Mengen an Trainingsdaten benötigen. Dennoch ist auch hier eine **bewusste Beschränkung auf das Notwendige gesetzlich verpflichtend**.

Beispiele:

- Ein Support-Chatbot benötigt keine Angaben zur ethnischen Herkunft oder Religion.

A4Q AI Essentials ©A4Q Copyright 2025

- Ein Empfehlungsalgorithmus kann anonymisierte Interaktionsdaten verwenden, ohne Klarnamen zu speichern.

Technische und organisatorische Maßnahmen:

- Nur erforderliche Datenfelder in Formularen bereitstellen
- Trainingsdaten pseudonymisieren oder anonymisieren
- „Privacy by Default“ als Standard-Einstellung aktivieren
- Einsatz synthetischer oder aggregierter Daten prüfen

4.5 Rechtsgrundlagen für KI-Systeme

Damit eine Verarbeitung personenbezogener Daten durch KI zulässig ist, muss sie auf einer der in **Art. 6 Abs. 1 DSGVO** genannten Rechtsgrundlagen beruhen. Häufig relevant im KI-Kontext sind:

- **Einwilligung** (lit. a): Nutzer:innen stimmen der Datenverarbeitung freiwillig zu
- **Vertragserfüllung** (lit. b): z. B. bei Dienstleistungsverträgen
- **Berechtigtes Interesse** (lit. f): z. B. bei internen Optimierungen oder Fraud Detection
- Weitere: rechtliche Verpflichtung (lit. c), lebenswichtige Interessen (lit. d), öffentliches Interesse (lit. e)

Achtung: Bei besonders sensiblen Daten (z. B. Gesundheitsdaten, biometrische Merkmale) gelten zusätzliche Einschränkungen nach **Art. 9 DSGVO**.

4.6 Fazit

Die DSGVO gilt uneingeschränkt für KI-Systeme, sobald diese personenbezogenen Daten verarbeiten. Unternehmen müssen daher:

- die Grundprinzipien der DSGVO einhalten
- die **Rechtsgrundlage** jeder Verarbeitung sorgfältig prüfen
- das **Prinzip der Datenminimierung** auch bei datengetriebenen Systemen umsetzen
- durch geeignete Maßnahmen **Rechenschaft und Transparenz** sicherstellen

Ein KI-System, das gegen Datenschutzprinzipien verstößt, kann nicht nur Bußgelder nach sich ziehen, sondern auch das Vertrauen von Nutzenden und Stakeholdern dauerhaft beschädigen.

A4Q AI Essentials

©A4Q Copyright 2025

5 Menschliche Aufsicht

Dauer 10 Minuten

Lernziele dieses Kapitels (LOs):

LO 5.1: Den Zweck menschlicher Aufsicht im Sinne des EU AI Act beschreiben (K2)

LO 5.2: Eingriffsmöglichkeiten und Kontrollpflichten bei KI-Systemen mit menschlicher Aufsicht erklären (K2)

5.1 Einleitung

Im Zentrum des EU AI Act steht das Prinzip, dass KI-Systeme nicht vollständig autonom über Menschen entscheiden dürfen – besonders dann nicht, wenn diese Entscheidungen erhebliche Auswirkungen auf Rechte, Pflichten oder Lebenschancen haben. Deshalb ist die sogenannte **menschliche Aufsicht** (englisch: *human oversight*) eine zentrale Anforderung an viele KI-Systeme, insbesondere im Hochrisikobereich.

5.2 Warum ist menschliche Aufsicht wichtig?

Künstliche Intelligenz kann schneller, objektiver und in größerem Umfang analysieren als der Mensch – aber sie ist nicht unfehlbar. Fehlerhafte Daten, algorithmische Verzerrungen (*Bias*), unvorhergesehene Situationen oder Sicherheitsrisiken können dazu führen, dass ein KI-System falsche oder sogar schädliche Entscheidungen trifft.

Menschliche Aufsicht soll diese Risiken minimieren. Sie schafft eine zusätzliche Kontroll- und Verantwortungsebene, um:

- ungewollte Ergebnisse zu verhindern
- Grundrechte zu schützen
- Vertrauen in den KI-Einsatz zu fördern

5.3 Rechtsgrundlage im EU AI Act

Artikel 14 des EU AI Act verpflichtet Anbieter dazu, Hochrisiko-KI-Systeme so zu gestalten, dass Menschen in der Lage sind:

- das System angemessen zu **überwachen**,
- **Fehler zu erkennen** und zu korrigieren,
- im Bedarfsfall **einzugreifen** oder die Nutzung zu beenden.

Die Anforderungen richten sich nach:

A4Q AI Essentials

©A4Q Copyright 2025

- dem **Einsatzzweck** des Systems
- der **Bedeutung** der Entscheidung
- der Rolle der Nutzer:innen im Prozess

5.4 Drei Formen menschlicher Aufsicht

Die menschliche Aufsicht kann auf unterschiedliche Weise ausgestaltet sein – je nach Einsatzbereich und Risiko. In der Praxis werden drei Hauptformen unterschieden:

1. Human-in-the-Loop (HITL)

- Jede Entscheidung der KI wird von einem Menschen **vor der Umsetzung geprüft**
- Hohe Kontrolle, langsamerer Prozess
- **Beispiel:** Kreditentscheidung wird durch Mitarbeitende bestätigt, bevor sie gültig ist

2. Human-on-the-Loop (HOTL)

- Mensch **überwacht** das System im Betrieb und kann bei Bedarf eingreifen
- Die KI arbeitet autonom, wird aber überwacht
- **Beispiel:** Verkehrsmanagement beobachtet KI-Ampelsteuerung und kann sie übersteuern

3. Human-out-of-the-Loop (HOOTL)

- **Keine Eingriffsmöglichkeit** durch den Menschen vorgesehen
- Unzulässig bei Hochrisiko-KI
- **Beispiel:** Bewerbungsfilter trifft Entscheidungen ohne menschliche Kontrolle

5.5 Eingriffsmöglichkeiten und Anforderungen

Damit menschliche Aufsicht mehr ist als ein Lippenbekenntnis, müssen konkrete **Eingriffsmöglichkeiten** vorgesehen sein:

- Benutzeroberflächen mit Kontrollfunktionen
- Protokollierung von Entscheidungen und menschlichen Eingriffen
- Möglichkeit zur **Abschaltung oder Korrektur** der KI-Entscheidungen
- Schulung der verantwortlichen Personen

Die Aufsicht muss in der Praxis nutzbar, wirksam und verantwortungsvoll delegiert sein.

A4Q AI Essentials

©A4Q Copyright 2025

5.6 Beispiele aus der Praxis

Beispiel 1: Bewerbungssystem mit HITL

Ein KI-System ordnet Bewerbungen nach Relevanz. Die finale Entscheidung trifft ein:e Personalverantwortliche:r. So bleibt der Mensch aktiv in der Entscheidungsschleife.

Beispiel 2: HOTL im Verkehrsmanagement

Ein KI-System schlägt Ampelschaltungen vor. Der Mensch überwacht die Ausführung und kann bei Störungen eingreifen.

Beispiel 3: HOOTL ohne Kontrolle

Ein Versicherer lässt eine KI automatisch Anträge ablehnen, ohne dass ein Mensch prüft oder widersprechen kann – das ist bei Hochrisiko-KI unzulässig.

5.7 Grenzen menschlicher Aufsicht

In der Praxis können bestimmte Faktoren die Wirksamkeit menschlicher Aufsicht einschränken:

- hoher Automatisierungsgrad
- Zeitdruck oder Arbeitslast
- unklare Rollen oder Zuständigkeiten
- mangelnde Fachkenntnis
- technologische Intransparenz („Black Box“)

Daher sind **organisatorische und technische Maßnahmen** notwendig, um sicherzustellen, dass Aufsicht realistisch ausgeübt werden kann.

5.8 Fazit

Menschliche Aufsicht ist ein zentrales Element für **vertrauenswürdige KI**. Sie dient dem Schutz von Rechten, der Risikominimierung und der Stärkung der Nutzerakzeptanz.

Voraussetzungen für wirksame Aufsicht:

- klare Definition von Rollen und Verantwortlichkeiten
- tatsächliche Eingriffs- und Kontrollmöglichkeiten
- transparente Systemgestaltung
- gezielte Schulungen und Awareness-Maßnahmen

Der EU AI Act macht deutlich: Künstliche Intelligenz darf den Menschen nicht ersetzen – sie muss durch ihn begleitet und kontrolliert werden.

A4Q AI Essentials

©A4Q Copyright 2025

©A4Q Copyright 2025

6 Risiken & Ethik

Dauer: ca. 10 Minuten

Lernziele dieses Kapitels (LOs):

LO 6.1: Den Begriff algorithmischer Bias benennen können (K1)

LO 6.2: Beispiele für unbeabsichtigte Benachteiligung durch KI benennen können (K1)

6.1 Einleitung

Künstliche Intelligenz bietet enorme Potenziale für Innovation, Effizienz und Automatisierung. Doch der Einsatz von KI kann auch unbeabsichtigte negative Folgen haben – etwa durch diskriminierende Entscheidungen oder intransparente Prozesse.

Deshalb fordert der EU AI Act nicht nur technische Sicherheit, sondern auch ethische Verantwortung. Dieses Kapitel behandelt die wichtigsten Risiken im Zusammenhang mit Diskriminierung und Bias sowie die Bedeutung von Fairness und gesellschaftlicher Verantwortung bei der Entwicklung und Anwendung von KI-Systemen.

6.2 Was bedeutet Fairness bei KI?

Fairness heißt: Alle Menschen sollen gleichbehandelt werden – unabhängig von Alter, Geschlecht, ethnischer Herkunft, Religion, Behinderung oder sozialem Status.

Ein faires KI-System:

- benachteiligt keine Person oder Gruppe systematisch
- bezieht unterschiedliche Perspektiven mit ein
- erkennt bestehende Ungleichheiten und wirkt ihnen entgegen

Wichtig: KI trifft Entscheidungen auf Basis von Daten. Wenn diese Daten verzerrt oder unvollständig sind, kann die KI bestehende Ungleichheiten **ungewollt verstärken** statt abbauen.

6.3 Was ist Bias?

Bias ist der englische Begriff für „Verzerrung“ oder „Voreingenommenheit“. In KI-Systemen kann Bias auf verschiedenen Ebenen entstehen:

- **Datenbias**: Die Trainingsdaten sind nicht repräsentativ (z. B. zu wenige Frauen, bestimmte Altersgruppen fehlen).
- **Label-Bias**: Bewertungen oder Zuordnungen durch Menschen sind subjektiv oder ungenau.
- **Algorithmic Bias**: Die Logik oder Gewichtung der Berechnung benachteiligt bestimmte Gruppen.

A4Q AI Essentials ©A4Q Copyright 2025

Bias entsteht oft ungewollt – etwa durch historische Daten, gesellschaftliche Stereotype oder technische Modellentscheidungen.

6.4 Beispiele für Diskriminierung durch KI

- Ein Bewerberfilter bevorzugt Bewerbungen von Männern, weil historische Erfolgsdaten fast nur männliche Karrieren enthalten.
- Ein Sprachsystem erkennt Dialekte oder nicht-akzentfreies Deutsch schlechter und bewertet diese Nutzer:innen als „weniger kompetent“.
- Ein Kreditbewertungssystem vergibt schlechtere Scores an Menschen mit ausländischen Namen – weil sie in der Vergangenheit häufiger abgelehnt wurden.

Solche Fälle zeigen: Selbst „neutrale“ Algorithmen können diskriminierend wirken, wenn keine Gegenmaßnahmen ergriffen werden.

6.5 Gesetzliche Anforderungen

EU AI Act

Der AI Act schreibt vor, dass insbesondere Hochrisiko-KI-Systeme:

- auf Diskriminierungsrisiken geprüft werden müssen
- faire und repräsentative Trainingsdaten nutzen
- Testverfahren zur Fairnessbewertung implementieren
- Erklärbarkeit und menschliche Kontrolle sicherstellen

DSGVO

Auch die Datenschutz-Grundverordnung verbietet diskriminierende automatisierte Entscheidungen:

- **Art. 22 DSGVO**: Schutz vor ausschließlich automatisierten Entscheidungen mit erheblichen Auswirkungen
- **Art. 5**: Rechtmäßigkeit, Transparenz, Fairness
- **Art. 9**: Schutz besonderer Kategorien personenbezogener Daten (z. B. ethnische Herkunft, Religion, Gesundheit)

6.6 Ethische Leitlinien für vertrauenswürdige KI

Neben rechtlichen Anforderungen gibt es ethische Prinzipien und Leitlinien – z. B. die Ethikrichtlinien der EU-Kommission für vertrauenswürdige KI:

Zentrale Werte:

A4Q AI Essentials

©A4Q Copyright 2025

- **Menschenzentrierung**: Der Mensch steht im Mittelpunkt – nicht die Maschine.
- **Transparenz**: Entscheidungen müssen nachvollziehbar sein.
- **Gerechtigkeit**: Kein systematischer Ausschluss oder Ben Nachteil von Gruppen.
- **Verantwortlichkeit**: Zuständigkeiten und Haftung müssen klar geregelt sein.
- **Sicherheit und Robustheit**: Schutz vor Fehlern, Missbrauch oder Angriffen.

Diese Leitlinien helfen Organisationen, nicht nur regelkonform, sondern auch verantwortungsbewusst mit KI umzugehen.

6.7 Verantwortung im Unternehmen

Fairness ist keine rein technische Herausforderung – sie ist auch eine **unternehmerische und kulturelle Aufgabe**.

Unternehmen sollten sicherstellen:

- dass ethische Risiken frühzeitig in Projekten adressiert werden
- dass **Diversität** in Daten, Teams und Tests berücksichtigt wird
- dass es **Anlaufstellen für Beschwerden** und Überprüfung gibt
- dass Mitarbeitende für ethische und soziale Auswirkungen sensibilisiert sind

6.8 Was können Organisationen konkret tun?

Maßnahmen für faire KI-Nutzung:

- **Bias-Audits** und **Fairness-Checks** vor der Markteinführung
- Einbindung interdisziplinärer Teams (Technik, Recht, Ethik, Fachbereiche)
- **Richtlinien für KI-Design** und Datenqualität festlegen
- **Schulungen** und Awareness-Formate für Mitarbeitende
- **Dokumentation** und kontinuierliche Kontrolle im Betrieb
- **Stakeholder einbeziehen** – etwa durch Ethik-Beiräte oder Nutzerfeedback

6.9 Fazit

Künstliche Intelligenz ist nie „neutral“. Sie verarbeitet Daten – und Daten tragen immer Spuren von Geschichte, Gesellschaft und Entscheidungen.

Deshalb gilt:

- Bias und Diskriminierung sind reale Risiken – sie entstehen oft unbeabsichtigt.

A4Q AI Essentials ©A4Q Copyright 2025

- Fairness ist technisch messbar, aber ethisch zu bewerten.
- Unternehmen tragen die Verantwortung, KI **gerecht und verantwortungsvoll** einzusetzen.

Leitfragen für fairen KI-Einsatz:

- Ist das Ziel des Systems ethisch vertretbar?
- Sind die Daten vollständig und vielfältig genug?
- Wird regelmäßig auf Diskriminierung getestet?
- Gibt es Eingriffsmöglichkeiten bei Fehlverhalten?

Nur wenn wir diese Fragen stellen – und konsequent beantworten – entsteht vertrauenswürdige KI, die nicht nur funktioniert, sondern verantwortlich wirkt.

A4Q AI Essentials

©A4Q Copyright 2025

7 Einführung in die Gestaltung wirksamer Prompts für KI-Systeme (Prompt Engineering)

Hinweis: Dieses Kapitel ist **nicht prüfungsrelevant** und wird als **optionaler Bonusbestandteil** der Schulung angeboten. Es dient der praktischen Vertiefung des KI-Wissens und der Anwendung im Arbeitsalltag.

Dauer: ca. 20 Minuten

Lernziele dieses Kapitels (LOs):

LO 7.1: Den Begriff „Prompt Engineering“ und dessen Bedeutung für den Einsatz von KI-Systemen kennen (K1)

LO 7.2: Unterschiedliche Arten von Prompts kennen (K1)

LO 7.3: Merkmale eines wirksamen Prompts anhand von Beispielen analysieren und Verbesserungspotenziale erkennen (K2)

7.1 Einleitung – Warum ist Prompt Engineering wichtig?

KI-Systeme wie ChatGPT, Claude oder Gemini können komplexe Aufgaben bewältigen: Texte schreiben, Inhalte analysieren, Informationen zusammenfassen, Entscheidungen unterstützen. Damit sie das zielgerichtet und korrekt tun, brauchen sie klare Anweisungen – sogenannte **Prompts**.

Ein **Prompt** ist eine Eingabe oder Anfrage an die KI, die eine gewünschte Antwort auslöst. **Prompt Engineering** ist die Fähigkeit, diese Eingaben so zu gestalten, dass die KI qualitativ hochwertige und nützliche Ergebnisse liefert.

Beispiel 1:
Schwacher Prompt: *„Schreib mir etwas über Datenschutz.“*
Stärkerer Prompt: *„Erkläre in einfachen Worten, was Datenschutz im Kontext der DSGVO bedeutet, und nenne drei typische Beispiele aus dem Arbeitsalltag.“*

Beispiel 2:
Unklar: *„Was ist ein Vertrag?“*
Klarer: *„Erkläre einem 16-jährigen Schüler, was ein Arbeitsvertrag ist, und nenne zwei Rechte und Pflichten.“*

A4Q AI Essentials
©A4Q Copyright 2025

7.2 Grundprinzipien guter Prompts

1. **Klarheit:**
   Formuliere so konkret wie möglich, was du willst.
2. **Kontext:**
   Gib Hintergrundinformationen: Zielgruppe, Format, Zweck.
3. **Struktur:**
   Nutze Listen, Bullet Points oder Gliederungen.
4. **Rollenanweisung:**
   Bitte die KI, in einer bestimmten Rolle zu antworten: *„Du bist eine Datenschutzbeauftragte …“*
5. **Begrenzungen:**
   Begrenze den Umfang: *„in maximal 150 Wörtern“, „als Tabelle“.*
6. **Iteration:**
   Passe den Prompt schrittweise an, bis das Ergebnis passt.

7.3 Typische Prompt-Typen mit Beispielen

1. Informationsabfrage

„Was sind die Hauptpflichten bei der Verarbeitung personenbezogener Daten laut DSGVO?“

2. Zusammenfassung

„Fasse den folgenden Text in drei Stichpunkten zusammen …“

3. Rollenbasiert

„Du bist eine Führungskraft. Formuliere eine kurze E-Mail, um dein Team über KI-Nutzung zu informieren.“

4. Vergleich

„Vergleiche Hochrisiko-KI-Systeme mit Systemen mit begrenztem Risiko gemäß EU AI Act in einer Tabelle.“

5. Kreativitätsförderung

„Nenne fünf kreative Ideen, wie Schulen KI einsetzen können, ohne Datenschutz zu verletzen.“

6. Prüfungsaufgaben generieren

„Erstelle fünf Multiple-Choice-Fragen zum Thema KI und DSGVO mit Lösung.“

7. Sprachstil ändern

„Formuliere diesen Absatz höflicher und formeller …“

A4Q AI Essentials
©A4Q Copyright 2025

8. Übersetzung/Vereinfachung

„Übersetze diesen juristischen Absatz in verständliches Deutsch …“

7.4 Häufige Fehler und wie man sie vermeidet

- **Zu offen:** *„Erzähl mir was.“* → Unpräzise Antwort
- **Mehrdeutig:** Unklare Begriffe → Missverständnisse
- **Kein Kontext:** Die KI rät
- **Zu viele Aufgaben in einem Prompt** → Überforderung der Antwortlogik
- **Keine Rückmeldung:** Prompt wird nicht verbessert

7.5 Der Prompt-Feedback-Zyklus (4 Schritte)

1. Prompt schreiben
2. Ergebnis prüfen
3. Prompt verfeinern
4. Neues Ergebnis bewerten

7.6 Erweiterte Techniken für Fortgeschrittene

1. Chain-of-Thought Prompting

„Beschreibe erst das Problem, dann die Ursachen, dann die Lösung.“

2. Few-shot Prompting

„Hier sind zwei gute Einleitungen juristischer Texte. Schreibe eine neue zum Thema DSGVO …“

3. Zero-shot Prompting

„Schreibe einen informativen Text über Bias in KI-Systemen.“

4. Meta-Prompts

„Beurteile deine eigene Antwort aus Sicht eines Juristen. Ist sie korrekt und verständlich?“

7.7 Abschlusstipps für die Praxis

- Formuliere dein Ziel klar (Was willst du erreichen?)
- Denke an die Zielgruppe (Für wen ist die Antwort?)

A4Q AI Essentials

©A4Q Copyright 2025

- Teste Varianten und vergleiche die Ergebnisse
- Halte bewährte Prompts fest (für Wiederverwendung im Team)
- Nutze Rollen, Vorgaben und Strukturhilfen

7.8 Fazit

Prompt Engineering ist keine technische Spezialdisziplin, sondern eine praktische Kommunikationsfertigkeit. Wer gute Prompts schreiben kann, macht aus einer KI ein wertvolles Werkzeug.

In Organisationen, die KI einsetzen, sollte diese Fähigkeit durch Schulungen, interne Bibliotheken und praktische Übungen gefördert werden.

Merksatz: Die Qualität der Antwort hängt direkt von der Qualität des Prompts ab.

A4Q AI Essentials

©A4Q Copyright 2025

8 Literatur

Bücher

[1] Andreas Klein, Künstliche Intelligenz in Unternehmen: Grundlagen, Anwendungen und Implikationen, Springer Gabler, 2021
[2] Jürgen Gallmann, Künstliche Intelligenz: Was auf Unternehmen zukommt, Redline Verlag, 2020
[3] Thomas Ramge, Mensch und Maschine: Wie Künstliche Intelligenz und Roboter unser Leben verändern, Reclam Verlag, 2020
[4] Tobias Kollmann (Hrsg.), Künstliche Intelligenz in Wirtschaft und Gesellschaft: Eine multidisziplinäre Betrachtung, Springer Gabler, 2021
[5] Peter Buxmann, Holger Schmidt, Künstliche Intelligenz: Mit Algorithmen zum wirtschaftlichen Erfolg, Springer Gabler, 2019
[6] Karl-Heinz Land, Erde 5.0: Die Zukunft provozieren – Digitalisierung, Künstliche Intelligenz und der Mensch, Murmann Publishers, 2018
[7] Richard David Precht, Künstliche Intelligenz und der Sinn des Lebens, Goldmann Verlag, 2020
[8] Pascal Finette, Jeffrey Rogers, The Disruption Map: AI and the Future of Business, Singularity University Press, 2022

Fachartikel und Studien

[9] Bitkom e.V., Künstliche Intelligenz: Einsatz, Nutzen und Herausforderungen in der deutschen Wirtschaft, Bitkom Research, 2023
[10] Roland Berger, Artificial Intelligence – Chancen für Unternehmen in Deutschland, Roland Berger Insights, 2022
[11] McKinsey & Company, The State of AI in 2023: Generative AI's Breakout Year, McKinsey Global Report, 2023
[12] Deloitte Deutschland, AI in Unternehmen: Reifegrade, Trends und Best Practices, Deloitte Insights, 2022
[13] Boston Consulting Group (BCG), Mind the Gap: AI Adoption in Europe's Businesses, BCG Report, 2022
[14] Fraunhofer IAO, Leitfaden: Einführung von KI in Unternehmen, Fraunhofer Verlag, 2022
[15] Accenture Research, AI: Built to Scale – Erfolgsfaktoren für KI in Unternehmen, Accenture Global Report, 2021
[16] Stifterverband, KI-Strategien in deutschen Unternehmen: Erfolgsfaktoren und Hindernisse, Stifterverband Report, 2021
[17] EY, Wie Unternehmen Künstliche Intelligenz nachhaltig skalieren können, EY Insights, 2023
[18] Capgemini Research Institute, AI and the Ethical Conundrum: Managing AI Responsibly, Capgemini

A4Q AI Essentials
©A4Q Copyright 2025

Report, 2020
[19] PwC Deutschland, Künstliche Intelligenz und Wirtschaft: Strategien, Chancen und Risiken, PwC Studie, 2022
[20] SAP, Wie Unternehmen KI erfolgreich in Geschäftsprozesse integrieren, SAP Whitepaper, 2021
[21] IBM Research, Global AI Adoption Index 2023, IBM Insights, 2023
[22] Swiss Digital Initiative, Vertrauenswürdige KI: Anforderungen an Unternehmen in der Schweiz, SDI Report, 2022
[23] ETH Zürich, Künstliche Intelligenz in Schweizer Unternehmen: Status und Herausforderungen, ETH Zürich Studie, 2021
[24] Österreichisches Wirtschaftsministerium, Anwendungsfelder von KI in der österreichischen Wirtschaft, BMDW Bericht, 2021
[25] Center for the Governance of AI, AI Governance: A Research Agenda, University of Oxford, 2018
[26] Zukunftsinstitut, Smart Business – Wie Künstliche Intelligenz Wertschöpfung neu definiert, Zukunftsinstitut Trendstudie, 2022
[27] German AI Association (KI Bundesverband), Position Paper: Anforderungen an eine zukunftsfähige KI-Politik für Unternehmen, KI Bundesverband, 2022

Gesetzliche Regelungen und Strategiedokumente

[28] Europäische Kommission, Verordnung über Künstliche Intelligenz (EU AI Act), beschlossen am 13. März 2024 durch das Europäische Parlament, Veröffentlichung im Amtsblatt der EU 2024 erwartet
[29] Datenschutz-Grundverordnung (DSGVO), Verordnung (EU) 2016/679, gültig seit 25. Mai 2018
[30] Bundesministerium für Wirtschaft und Klimaschutz (BMWK), Deutsche KI-Strategie, Deutschland, aktualisiert 2020
[31] Eidgenössisches Departement für Wirtschaft, Bildung und Forschung (WBF), Strategie Künstliche Intelligenz Schweiz, 2020
[32] Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW), Strategie für Künstliche Intelligenz – Österreich, 2021
[33] Bundesministerium der Justiz, Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG), Deutschland, in Kraft seit 1. Dezember 2021
[34] Bundesdatenschutzgesetz (BDSG), Gesetz zum Schutz personenbezogener Daten, Deutschland, gültig seit 25. Mai 2018 (angepasst 2021)
[35] Datenschutzgesetz (DSG Österreich), Bundesgesetz über den Schutz personenbezogener Daten, Österreich, zuletzt novelliert 2018
[36] Eidgenössisches Datenschutz- und Öffentlichkeitsgesetz (nDSG Schweiz), Bundesgesetz über den Datenschutz, gültig seit 1. September 2023

Normen und Standards

A4Q AI Essentials
©A4Q Copyright 2025

[37] ISO/IEC 22989, Künstliche Intelligenz – Konzepte und Terminologie, Internationale Organisation für Normung (ISO), 2022

[38] ISO/IEC 23053, Rahmenwerk für maschinelles Lernen, Internationale Organisation für Normung (ISO), 2022

[39] ISO/IEC TR 24028, Technischer Bericht: Sicherheit und Resilienz von KI-Systemen, Internationale Organisation für Normung (ISO), 2020

[40] ISO/IEC 23894, Risikomanagement für KI, Internationale Organisation für Normung (ISO), 2023

[41] DIN SPEC 92001-1, Qualitätsanforderungen an KI-Systeme – Grundlagen, Deutsches Institut für Normung (DIN), 2020

[42] DIN SPEC 92001-2, Qualitätsanforderungen an KI-Systeme – Prüfkriterien, Deutsches Institut für Normung (DIN), 2021

[43] ISO/IEC 27001, Informationssicherheits-Managementsysteme (ISMS), Internationale Organisation für Normung (ISO), aktualisierte Ausgabe 2022

[44] ISO/IEC 27701, Datenschutz-Managementsysteme (Erweiterung von ISO 27001), Internationale Organisation für Normung (ISO), 2019

A4Q AI Essentials

©A4Q Copyright 2025