Alliance for Qualification

Version 1.0 DE

Oktober 2025

A4Q Syllabus

Certified Professional for AI Compliance (EU AI Act)



Copyright Notiz und Disclaimer

© A4Q Copyright 2025 - Copyright Notiz

Alle Inhalte dieses Werks, 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.

Disclaimer

Die Inhalte dieses Lehrplans wurden mit großer Sorgfalt erstellt und stützen sich unter anderem auf die zum Zeitpunkt der Veröffentlichung geltenden Rechtsvorschriften, insbesondere die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO) sowie die Verordnung (EU) 2024/1689 (Gesetz über Künstliche Intelligenz, AI Act).

Dieser Lehrplan dient ausschließlich allgemeinen Informations- und Ausbildungszwecken. Die dargestellten Informationen können verkürzt, vereinfacht oder in generalisierter Form wiedergegeben sein und spiegeln daher möglicherweise weder spezifische rechtliche Kontexte noch den neuesten Stand der Entwicklungen vollständig wider.

Dieser Lehrplan stellt keine Rechtsberatung dar und darf nicht als Ersatz für eine professionelle rechtliche Beurteilung im Einzelfall herangezogen werden.

Für die Umsetzung rechtlicher Anforderungen oder die Bewertung konkreter Sachverhalte wird ausdrücklich empfohlen, eine qualifizierte Rechtsanwältin bzw. einen qualifizierten Rechtsanwalt oder eine entsprechend befugte Beratungsstelle zu konsultieren.

A4Q und die Autorinnen und Autoren übernehmen keinerlei Verantwortung oder Haftung für die Aktualität, Vollständigkeit oder Richtigkeit der bereitgestellten Informationen sowie für etwaige Folgen, die sich aus deren Nutzung oder Interpretation ergeben.

Hinweis zum Einsatz von Künstlicher Intelligenz (KI):

Bei der Erstellung der Inhalte dieses Syllabus wurde Künstliche Intelligenz (KI) eingesetzt. Die generierten Inhalte wurden redaktionell geprüft, können jedoch trotz größtmöglicher Sorgfalt fehlerhaft, unvollständig, im falschen Kontext, oder interpretationsbedürftig sein. Bitte berücksichtigen Sie dies insbesondere bei der rechtlichen Einordnung oder Anwendung in der Praxis.

Inhalt

Copyright Notiz und Disclaimer 2
Inhalt 3
Version 9
0 Einführung 10
0.1 Zweck des Syllabus 10
0.2 Prüfungsrelevante Lernziele und kognitive Wissensstufen 10
0.3 Die “Certified Professional for AI Compliance” Prüfung 10
0.4 Akkreditierung 11
0.5 Detaillierungsgrad 11
0.6 Struktur dieses Syllabus 11
0.7 Business Outcomes (BOs) 13
0.8 Abkürzungen 18
1 Einführung in AI Compliance & den EU AI Act 21
1.1 Was ist Künstliche Intelligenz im regulatorischen Kontext 22
1.1.1 Regulatorische Teilbereiche 22
1.1.2 Strategische und regulatorische Bedeutung von KI im Unternehmen 22
1.1.3 Historischer und rechtlicher Kontext 23
1.1.4 Bedeutung für Governance und Compliance 23
1.2 Der EU AI Act im Überblick 24
1.2.1 Schlüsselprinzipien des AI Act 24
1.2.2 Akteursrollen und Verantwortlichkeiten 24
1.3 Zeitplan der Umsetzung (2024 – 2027) 25
1.4 Kernaussage 26
2 Risikobasierter Ansatz & Klassifikation 27
2.1 Grundprinzip des risikobasierten Ansatzes 28
2.2 Annex III – Automatisch hochrisikobehaftete KI-Systeme 28
2.3 Kriterien zur Risikoeinstufung 31
2.4 Pflichten und Maßnahmen nach Risikostufe 35
2.5 Risikodynamik und Re-Assessments 38

© A4Q Copyright 2025

2.6 Risikobasierte Priorisierung von Maßnahmen 38
3 Globale & sektorale Regulierungslandschaft (Überblick) 40
3.1 Globale KI-Regulierung: Status und Trends 41
3.2 Vergleich: EU AI Act ↔ Internationale Regelungen 43
3.3 Sektorale KI-Regulierung und Schnittstellen 44
3.4 Harmonisierung und Strategien für globale KI-Projekte 45
3.5 Zusammenfassung und Kernbotschaften 46
4 Verbotene KI-Praktiken (Art. 5 EU AI Act) 47
4.1 Überblick über die verbotenen Praktiken 48
4.2 Rechts- und Grundrechtsbegründung 48
4.3 Ausnahmen nach Art. 5 Abs. 2–3 49
4.4 Praktische Sensibilisierung 49
4.5 Praktische Beispiele 49
4.6 Zusammenfassung 52
5 Hochrisiko-Systeme und Pflichten (Art. 6–51 EU AI Act) 54
5.1 Identifikation von Hochrisiko-Systemen 55
5.2 Zentrale Pflichten für Hochrisiko-Systeme 56
5.3 Umsetzung im Unternehmen 58
5.4 Dokumentations- und Nachweispflichten (Audit Readiness) 60
5.5 Beispiel – Anwendung der Hochrisiko-Pflichten in der Praxis 62
6 Risikomanagement- und Qualitäts-managementsystem 66
6.1 Grundprinzipien des AI-Risikomanagements 67
6.2 Der Risikomanagementzyklus nach ISO/IEC 23894 und AI Act 67
6.3 Integration in bestehende Managementsysteme 68
6.4 Dokumentations- und Nachweispflichten 69
6.5 Governance, Rollen und Verantwortung 70
6.6 Bedeutung der Integration für Compliance und Qualität 71
7 Konformitätsbewertung und CE-Kennzeichnung 73
7.1 Grundlagen der Konformitätsbewertung (Art. 43 AI Act) 74
7.2 Inhalte der technischen Dokumentation (Art. 11 & Anhang IV) 76
7.3 Ablauf der CE-Kennzeichnung (Art. 49 AI Act) 80

© A4Q Copyright 2025

7.4 Rolle der benannten Stellen (Notified Bodies) ... 81
7.5 Eintrag in die EU-Datenbank für Hochrisiko-KI-Systeme (Art. 71) ... 82
7.6 Umgang mit wesentlichen Änderungen (Art. 43 Abs. 4) ... 83
7.7 Verbindung zu Qualitäts- und Managementsystemen ... 84
7.8 Praxisbeispiel: Konformitätsroute eines HR-Screening-Tools ... 85
7.9 Handlungsempfehlungen für die Praxis ... 87
8 Transparenzpflichten für Limited-Risk-Systeme (Art. 52 EU AI Act) ... 89
8.1 Artikel 52 EU AI Act – Transparenzpflichten ... 90
8.2 Anwendungsbereiche und Kennzeichnungspflichten ... 91
8.3 Gestaltungsempfehlungen für Interface-Design und Kennzeichnung ... 93
8.4 Organisatorische Umsetzung im Unternehmen ... 94
8.5 Typische Fehler und Compliance-Risiken ... 95
8.6 Praxisbeispiel: Kennzeichnung generativer Inhalte im Marketing ... 96
8.7 Empfehlungen für die Praxis ... 97
9 General Purpose AI (GPAI) & Systemic Risk ... 99
9.1 Rechtlicher Rahmen: Artikel 53 bis 55 EU AI Act ... 100
9.2 Pflichten der GPAI-Anbieter ... 101
9.3 Systemische Risiken & Governance ... 103
9.4 Compliance-Prüfung externer GPAI-Modelle (Checkliste) ... 104
9.5 Praxisbeispiel: Nutzung eines LLM im Kundenservice ... 106
9.6 Handlungsempfehlungen für Anwenderorganisationen ... 106
10 Fundamental Rights Impact Assessment (FRIA, Art. 27 EU AI Act) ... 108
10.1 Rechtsgrundlage und Anwendungsbereich ... 109
10.2 Struktur und empfohlene Schritte einer FRIA ... 109
10.3 Abgrenzung und Verknüpfung zur Datenschutz-Folgenabschätzung (DSFA) ... 110
10.4 Praktische Umsetzung einer FRIA – Schritt-für-Schritt-Vorgehen ... 111
10.5 Synergien mit bestehenden Managementsystemen ... 113
10.6 Beispiel einer FRIA in der Praxis ... 113
11 Post-Market-Monitoring, Reporting & Marktaufsicht ... 115
11.1 Pflichten nach der Inverkehrbringung gemäß Artikel 61 EU AI Act ... 116
11.2 Ziele des Post-Market-Monitoring ... 117

© A4Q Copyright 2025

11.3 Inhalt eines Monitoring-Plans 117
11.4 Serious-Incident-Reporting (Art. 62 EU AI Act) 119
11.5 Zusammenarbeit mit Marktaufsichtsbehörden und dem AI Office 122
11.6 Best Practice: Kontinuierliche Risikoevaluation 123
11.7 Praxisbeispiel: Post-Market-Monitoring und Behördenkooperation in der öffentlichen Verwaltung 124
12 Governance, Organisation & Rollen im Unternehmen 126
12.1 Struktur eines KI-Governance-Systems 126
12.2 Zentrale Rollen und Zuständigkeiten 127
12.3 AI Governance Committee 128
12.4 Interne Policies und Kontrollmechanismen 129
12.5 Schulung und Awareness-Programme 129
12.6 Schnittstellen zu bestehenden Managementsystemen 130
12.7 Beispiel – Governance-Implementierung in der Praxis 131
13 Minimales Risiko & freiwillige Governance („Ethical AI“) 133
13.1 Freiwillige Governance nach ISO/IEC 42001 134
13.2 OECD-, UNESCO- und IEEE-Leitlinien für vertrauenswürdige KI 134
13.3 Ethical Impact Assessment (EIA) 135
13.4 Verknüpfung von Ethik, CSR und ESG 135
13.5 Szenario: Ethical AI bei einem Telekommunikationsanbieter 136
14 Audit-Readiness, Prüfpfade & Sanktionen 137
14.1 Auditarten und Verantwortlichkeiten 138
14.2 Audit-Vorbereitung 138
14.3 Typische Audit-Findings und Mängelarten 140
14.4 Sanktionen gemäß EU AI Act (Art. 71) 141
14.5 Korrektur- und Verbesserungsmaßnahmen 141
14.6 Praxisfall: Audit-Vorbereitung Hochrisiko-System 142
14.7 Best Practices für Audit-Readiness 143
15 Harmonisierte Standards & Presumption of Conformity 145
15.1 Begriff und Funktion harmonisierter Normen 146
15.2 Presumption of Conformity – rechtlicher Hintergrund 146

© A4Q Copyright 2025

15.3 Aktuelle Normenlandschaft (Auswahl, 2025) 147
15.4 Integration harmonisierter Standards im Unternehmen 147
15.5 Zusammenarbeit von CEN/CENELEC und ISO bei der Normung 150
15.6 Best Practices für den Einsatz harmonisierter Normen 150
16 Globale Schnittstellen & Exportkontrolle 153
16.1 Datenexport und Datenlokalisierung 153
16.2 Dual-Use-Güter und Exportkontrolle 155
16.3 IP-Rechte und Lizenzfragen 158
16.4 Compliance in internationalen Lieferketten 161
17 Optional - Praktische Übungen & Fallstudien 165
17.1 Einführung in KI-Compliance & den EU AI Act 165
17.2 Risikobasierter Ansatz und Klassifikation 166
17.3 Globale & sektorale Regulierungslandschaft 166
17.4 Verbotene KI-Praktiken (Art. 5) 166
17.5 Hochrisiko-Systeme und Pflichten (Art. 6 – 51) 166
17.6 Risikomanagement- & Qualitätsmanagementsystem 167
17.7 Konformitätsbewertung und CE-Kennzeichnung 167
17.8 Transparenzpflichten für Limited-Risk-Systeme (Art. 52) 167
17.9 General Purpose AI (GPAI) & Systemic Risk 168
17.10 Fundamental Rights Impact Assessment (FRIA, Art. 27) 168
17.11 Post-Market-Monitoring, Reporting & Marktaufsicht 168
17.12 Governance, Organisation & Rollen 168
17.13 Minimales Risiko & freiwillige Governance („Ethical AI“) 169
17.14 Audit-Readiness, Prüfpfade & Sanktionen 169
17.15 Harmonisierte Standards & Presumption of Conformity 169
17.16 Globale Schnittstellen & Exportkontrolle 169
17.17 Optionales Übungskapitel – Vertiefende oder ergänzende Praxisaufgaben 169
17.18 Optionales Kapitel: Roadmap & Readiness Assessment 2025–2027 170
17.19 Optionales Kapitel: Zukunft & Weiterentwicklung des Regulierungsrahmens 170
18 Roadmap & Readiness Assessment 2025–2027 171

© A4Q Copyright 2025

18.1 Bausteine einer AI-Compliance-Roadmap 172
18.2 Typische Quick Wins und Prioritäten 172
18.3 Selbstbewertung des AI-Compliance-Reifegrads 174
18.4 Werkzeuge und Hilfsmittel für die Roadmap-Erstellung 176
18.5 Fazit 178
19 Zukunft & Weiterentwicklung des Regulierungsrahmens 179
19.1 Europäische Institutionen und Governance-Strukturen (Zeithorizont 2025–2030) 180
19.2 Frontier AI und Systemic Risk (Zeithorizont 2025 – 2030) 181
19.3 Erwartete Weiterentwicklungen des AI Act (Zeithorizont 2025–2030) 182
19.4 Globale Trends und internationale Konvergenz (Zeithorizont 2025–2030) 184
19.5 Strategische Implikationen für Organisationen (Zeithorizont 2025–2030) 185
19.6 Empfohlene Vertiefungsthemen (Zeithorizont 2025–2030) 185
20 Empfehlungen für Trainingsanbieter 187
21 Lernziele und kognitive Lernniveaus 190
22 Literatur 192
22.1 Fachliteratur 192
22.2 Fachartikel und Studien 193
22.3 Gesetzliche Regelungen und Strategiedokumente 195
22.4 Normen und Standards 196
22.5 Internationale Leitlinien / Ethik- und Governance-Frameworks für KI 198
22.6 Cybersecurity-Lagebilder (KI-Bezug) 198
23 Anhänge 200
23.1 Anhang A – Leitfaden für internationale Anbieter 200

© A4Q Copyright 2025

Version

Revision Historie

Version	Datum	Anmerkung
1.0	28.10.2025	Intern geprüftes Dokument, umfangreiche Erweiterungen

Die vorliegende Version ist die Version 1.0 DE, build 1.003.

Dieses Dokument wurde offiziell durch die A4Q GmbH veröffentlicht.

© A4Q Copyright 2025

0 Einführung

0.1 Zweck des Syllabus

Dieser Syllabus beschreibt die angestrebten Geschäftsergebnisse (Business Outcomes), Lernziele (Learning Objectives) und grundlegenden Konzepte der Certified Professional for AI Compliance (EU AI Act) Schulung und Zertifizierung.

0.2 Prüfungsrelevante Lernziele und kognitive Wissensstufen

Die Lernziele (Learning Objectives) unterstützen die Geschäftsergebnisse (Business Outcomes) und dienen als Grundlage für die Erstellung der zertifizierten Certified Professional for AI Compliance Prüfungen. Von den Teilnehmenden kann erwartet werden, dass sie Inhalte je Kapitel des Syllabus wiedergeben, Verständnis nachweisen, Wissen anwenden und 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 “Certified Professional for AI Compliance” Prüfung

Die „Certified Professional for AI Compliance“ 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 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.

Die Prüfung besteht aus 40 Multiple-Choice-Fragen. Jede richtige Antwort wird mit einem Punkt bewertet. Zum Bestehen der Prüfung ist eine Mindestpunktzahl von 65 % (d. h. mindestens 26 korrekt beantwortete Fragen) erforderlich. Für die Bearbeitung der Prüfung stehen 60 Minuten zur Verfügung. Ist die Muttersprache des Teilnehmenden nicht die Sprache der Prüfung, kann eine zusätzliche Prüfungszeit von 25 % (15 Minuten) gewährt.

.

© A4Q Copyright 2025

0.4 Akkreditierung

Schulungsanbieter, die Trainings zum *Syllabus* anbieten möchten, müssen von A4Q akkreditiert sein und die offiziellen Schulungsunterlagen verwenden.

0.5 Detaillierungsgrad

Dieser Syllabus besteht aus:

- Business Objectives, die festlegen, welche Kompetenzen Teilnehmende erwerben sollen, um geschäftliche Herausforderungen wirksam zu adressieren,
- Lernziele für die einzelnen Wissensbereiche, die den jeweils angestrebten kognitiven Lernfortschritt beschreiben,
- sowie eine Darstellung der zentralen Konzepte, einschließlich Verweisen auf anerkannte Fachliteratur, Standards und andere maßgebliche Quellen,
- gegebenenfalls Listen von Schlüsselbegriffen, die die Teilnehmenden verstehen sollen.

Der Syllabus erhebt keinen Anspruch auf Vollständigkeit des gesamten Fachgebiets der AI Compliance, sondern bildet jenen Detaillierungsgrad ab, der im Rahmen der jeweiligen Schulungen und der zugehörigen Zertifizierung vermittelt wird.

0.6 Struktur dieses Syllabus

Hinweis zur Zeitstruktur des Lehrplans

Der Lehrplan besteht aus 16 Kapiteln, deren Inhalte für die Zertifizierungsprüfung relevant sind, ergänzt durch drei zusätzliche Bonuskapitel, die optionales Lernmaterial bieten und nicht prüfungsrelevant sind. Jedes Kapitel enthält eine Zeitangabe für die empfohlene Unterrichtsdauer, die sich auf das jeweilige Kapitel als Ganzes bezieht. Innerhalb der Kapitel erfolgt keine weitere zeitliche Aufschlüsselung, eine feinere Granularität auf Unterkapitelebene ist nicht vorgesehen.

Für den Trainingskurs sieht der Lehrplan einen Umfang von etwa 16 Stunden Unterricht vor. Diese verteilen sich auf die einzelnen Kapitel sowie allenfalls ergänzende praktische Übungen. Die tatsächlich benötigte Unterrichtszeit kann je nach Vorwissen, Interesse und Schwerpunktsetzung der Teilnehmenden abweichen.

Die Zeitangaben dienen der Orientierung bei der Trainingsplanung und ermöglichen eine strukturierte Vorbereitung auf die Zertifizierungsprüfung. Sie stellen jedoch keine Mindest- oder Maximalzeiten dar und ersetzen keine didaktische oder methodische Kursgestaltung durch Trainerinnen und Trainer.

© A4Q Copyright 2025

Übersicht Unterrichtszeiten je Kapitel

Nr.	Kapitel	Unterrichtszeit (min)
1	Einführung in AI Compliance & EU AI Act	45
2	Risikobasierter Ansatz & Klassifikation	60
3	Globale & sektorale Regulierungslandschaft	70
4	Verbotene KI-Praktiken (Art. 5)	50
5	Hochrisiko-Systeme (Art. 6 – 51)	120
6	Risikomanagement & QMS (ISO 42001/23894)	60
7	Konformitätsbewertung & CE-Kennzeichnung	80
8	Limited-Risk & Transparenzpflichten (Art. 52)	90
9	GPAI & Systemic Risk (Art. 53–55)	75
10	FRIA (Fundamental Rights Impact Assessment)	45
11	Post-Market Monitoring & Marktaufsicht	60
12	Governance & Organisation im Unternehmen	45
13	Minimales Risiko & freiwillige Governance	40
14	Audit-Readiness & Sanktionen	30
15	Harmonisierte Standards & Conformity	30
16	Globale Schnittstellen & Exportkontrolle	60
17	Praktische Übungen & Fallstudien	-
18	Roadmap & Readiness Assessment 2025–2027	-
19	Zukunft & Weiterentwicklung des Rahmens	-
Gesamtsumme		**960min = 16 h ≈ 2 Tage**

© A4Q Copyright 2025

0.7 Business Outcomes (BOs)

Die Business Outcomes dieses Lehrplans beschreiben die angestrebten Kompetenzen, die Teilnehmende im Rahmen des zweitägigen Trainings erwerben oder weiterentwickeln sollen. Sie sind bewusst kompetenzorientiert, aber nicht leistungsbehauptend formuliert.
Da das Thema „AI Compliance“ ein breites, multidisziplinäres und sich dynamisch entwickelndes Fachgebiet ist, kann ein zweitägiger Kurs kein vollständiges, in allen Aspekten anwendungsreifes Können vermitteln.
Ziel ist vielmehr, Teilnehmende vorzubereiten und zu sensibilisieren, sodass sie zentrale Prinzipien, Rollen und Pflichten des EU AI Act verstehen, Risiken einschätzen und Compliance-Maßnahmen im eigenen beruflichen Kontext einordnen können.

Folgende Business Outcomes werden in den Kapiteln des Syllabus behandelt.

Kapitel	**BO-Nr.**	**Business Outcome (mit Unternehmensnutzen)**
Einführung in AI Compliance & EU AI Act	BO 1.1	Teilnehmende sind in der Lage, die von der EU-AI-Verordnung betroffenen Unternehmensbereiche zu identifizieren und aktiv zur Entwicklung wirksamer Compliance-Strategien beizutragen.
	BO 1.2	Teilnehmende sind vorbereitet, Verantwortlichkeit und Bewusstsein für KI-Compliance im Unternehmen zu fördern, sodass Risiken früh erkannt werden.
Risikobasierter Ansatz & Klassifikation	BO 2.1	Teilnehmende erwerben die Kompetenz, KI-Systeme nach den vier Risikostufen einzustufen und Pflichten zielgerichtet abzuleiten.
	BO 2.2	Teilnehmende sind vorbereitet, angemessene Maßnahmen zu planen und Prioritäten nach Risikograd zu setzen.
Globale & sektorale Regulierungslandschaft	BO 3.1	Teilnehmende entwickeln Verständnis für internationale KI-Regulierungen und sind befähigt, diese auf globale Projekte anzuwenden.
	BO 3.2	Teilnehmende sind vorbereitet, Harmonisierungspotenziale zwischen EU- und Nicht-EU-Vorgaben zu erkennen und im Unternehmen zu nutzen.

© A4Q Copyright 2025

Kapitel	BO-Nr.	Business Outcome (mit Unternehmensnutzen)
Verbotene KI-Praktiken (Art. 5)	BO 4.1	Teilnehmende entwickeln Sensibilität für unzulässige KI-Praktiken und sind befähigt, diese im eigenen Umfeld zu identifizieren.
	BO 4.2	Teilnehmende sind vorbereitet, Ausnahmen nach Art. 5 zu bewerten und umzusetzen.
Hochrisiko-Systeme & Pflichten (Art. 6–51)	BO 5.1	Teilnehmende erwerben die Fähigkeit, die relevanten Pflichten für Hochrisiko-KI-Systeme zu erkennen, ihre praktische Umsetzung im Unternehmen zu unterstützen und zur Einhaltung der gesetzlichen Anforderungen beizutragen..
	BO 5.2	Teilnehmende sind sensibilisiert, prüfungsfähige Dokumentationen und Nachweise zu erstellen, um die Audit-Sicherheit zu erhöhen.
Risikomanagement & QMS (ISO 42001 / 23894)	BO 6.1	Teilnehmende sind vorbereitet, am Aufbau oder der Anpassung eines AI-Risikomanagementsystems nach ISO 42001 mitzuwirken.
	BO 6.2	Teilnehmende erhalten einen Überblick über die Bedeutung der Integration von KI-Prozessen in bestehende Managementsysteme (QMS, ISMS, DSMS) und verstehen, wie diese Verknüpfung zur Sicherstellung von Compliance und Qualität beiträgt..
Konformitätsbewertung & CE-Kennzeichnung	BO 7.1	Teilnehmende entwickeln Verständnis für Konformitätsrouten und sind vorbereitet, deren Anwendung zu unterstützen.
	BO 7.2	Teilnehmende sind befähigt, CE-Kennzeichnung und EU-Datenbank-Eintragungen zu begleiten.
Limited-Risk & Transparenzpflichten (Art. 52)	BO 8.1	Teilnehmende sind vorbereitet, Transparenzanforderungen für Chatbots, Emotionserkennung und Deepfakes anzuwenden.
	BO 8.2	Teilnehmende erwerben Kompetenz, Kennzeichnungssysteme im Interface-Design zu bewerten und anzupassen.

© A4Q Copyright 2025

Kapitel	BO-Nr.	Business Outcome (mit Unternehmensnutzen)
GPAI & Systemic Risk (Art. 53–55)	BO 9.1	Teilnehmende sind vorbereitet, Pflichten von GPAI-Anbietern zu analysieren und Compliance-Lücken zu identifizieren.
	BO 9.2	Teilnehmende sind befähigt, den Einsatz externer GPAI-Modelle (z. B. LLMs, generative Systeme) im eigenen Unternehmenskontext hinsichtlich Transparenz, Risiko und Compliance zu prüfen und entsprechende Handlungsempfehlungen abzuleiten.
FRIA (Fundamental Rights Impact Assessment)	BO 10.1	Teilnehmende sind vorbereitet, eine FRIA zu strukturieren und in Entscheidungsprozesse einzubringen.
	BO 10.2	Teilnehmende sind befähigt, FRIA mit DSFA-Prozessen zu verknüpfen und Synergien zu nutzen.
Post-Market Monitoring & Marktaufsicht	BO 11.1	Teilnehmende entwickeln Verständnis für Post-Market-Prozesse und sind vorbereitet, Monitoring-Pläne anzuwenden.
	BO 11.2	Teilnehmende werden vorbereitet, mit Aufsichtsbehörden und dem AI Office zu kooperieren.
Governance & Organisation im Unternehmen	BO 12.1	Teilnehmende sind vorbereitet, Rollen und Verantwortlichkeiten im KI-Governance-System mitzugestalten.
	BO 12.2	Teilnehmende sind befähigt, interne Schulungs- und Policy-Programme zur Compliance-Kultur aufzubauen.
Minimales Risiko & freiwillige Governance	BO 13.1	Teilnehmende entwickeln Bewusstsein für freiwillige Governance-Ansätze nach ISO 42001 und OECD.
	BO 13.2	Teilnehmende sind vorbereitet, ethische Leitlinien mit CSR- und ESG-Zielen zu verbinden.
Audit-Readiness & Sanktionen	BO 14.1	Teilnehmende sind vorbereitet, interne und externe Audits strukturiert vorzubereiten.
	BO 14.2	Teilnehmende sind sensibilisiert, Korrektur- und Verbesserungsmaßnahmen aus Audit-Ergebnissen umzusetzen.

© A4Q Copyright 2025

Kapitel	BO-Nr.	Business Outcome (mit Unternehmensnutzen)
Harmonisierte Standards & Presumption of Conformity	BO 15.1	Teilnehmende entwickeln Verständnis für die Bedeutung harmonisierter Normen als Compliance-Nachweis.
	BO 15.2	Teilnehmende sind vorbereitet, aktuelle Standards zu bewerten und deren Anwendung im Projekt zu unterstützen.
Globale Schnittstellen & Exportkontrolle	BO 16.1	Teilnehmende sind vorbereitet, Risiken aus Datenexport, Dual-Use und IP-Rechten einzuschätzen.
	BO 16.2	Teilnehmende sind vorbereitet, Compliance-Anforderungen in internationalen Lieferketten zu unterstützen.
Optional: Praktische Übungen & Fallstudien	BO 17.1	Teilnehmende erwerben weitgehend Kompetenz, Risikoklassifizierung, FRIA und GPAI-Pflichten praktisch anzuwenden.
	BO 17.2	Teilnehmende sind befähigt, Compliance-Artefakte (Dokumentation, Label, Monitoring-Plan) zu entwickeln.
Optional: Roadmap & Readiness Assessment 2025–2027	BO 18.1	Teilnehmende sind vorbereitet, eine AI-Compliance-Roadmap mit Umsetzungsprioritäten zu erstellen.
	BO 18.2	Teilnehmende sind befähigt, den Reifegrad des Unternehmens hinsichtlich AI-Act-Readiness einzuschätzen.
Optional: Zukunft & Weiterentwicklung des Regulierungsrahmens	BO 19.1	Teilnehmende entwickeln Bewusstsein für kommende Trends (Frontier AI, AI Safety Institute etc.).
	BO 19.2	Teilnehmende sind vorbereitet, strategische Anpassungen für zukünftige Regulierungszyklen zu planen und zu kommunizieren.

Zuordnung der AI Act-Anforderungen zu den Business Outcomes (BOs)

Die Businessoutcomes entsprechen folgenden Anforderungen die der AI Act stellt. Alle wesentlichen Anforderungen, vor allem auch die der High Risk Systeme, werden prinzipiell abgedeckt.

Matrix: Business Outcomes ↔ EU AI Act-Artikel

© A4Q Copyright 2025

Kapitel / BO	Relevante Artikel / Abschnitte EU AI Act	Abgedeckte Themen / Anforderungen
BO 1.1 – 1.2 Einführung in AI Compliance & EU AI Act	Art. 1–3 (Subject Matter, Scope, Definitions) + Art. 4 (Principles of AI Systems)	Geltungsbereich, Definition KI-System, Rollen (Provider, Deployer, Importer, Distributor), Grundprinzipien, Verantwortlichkeiten.
BO 2.1 – 2.2 Risikobasierter Ansatz & Klassifikation	Art. 6 (Classification of AI Systems as High Risk) + Annex III (Domains) + Art. 7 – 8 (Updates & Transparency on Classification)	Risikokategorisierung, Annex-III-Domänen, Schwellen, Re-Klassifikation, Umgang mit mehrfachen Risikostufen.
BO 3.1 – 3.2 Globale & sektorale Regulierungslandschaft	Erwägungsgründe (13–15, 81 ff.), Art. 88–92 (International Cooperation & AI Office Mandate)	Globale Harmonisierung, internationale Zusammenarbeit, Vergleich mit nicht-EU-Systemen, Regulatorische Konvergenz.
BO 4.1 – 4.2 Verbotene KI-Praktiken	Art. 5 (Prohibited AI Practices) + Erwägungsgründe (31–34)	Erkennung und Ausschluss unzulässiger Praktiken (Manipulation, Social Scoring, Emotion Recognition, Biometrie in Echtzeit). Ausnahmen für Strafverfolgung.
BO 5.1 – 5.2 Hochrisiko-Systeme & Pflichten	Art. 9–15 + Art. 16 – 23	Vollständiger Pflichtenkanon: Risikomanagement, Data Governance, Technische Doku, Logging, Transparenz, Human Oversight, Robustness & Cybersecurity, QMS.
BO 6.1 – 6.2 Risikomanagement & QMS	Art. 9 (Risk Management) + Art. 17–23 (Quality Management System & Obligations of Provider) + ISO/IEC 42001 Referenz	Einrichtung eines AI-Managementsystems, Verknüpfung mit Unternehmens-QMS, Dokumentation und Nachweisführung.
BO 7.1 – 7.2 Konformitätsbewertung & CE-Kennzeichnung	Art. 43–51 (Conformity Assessment & CE Marking) + Annex VII (Procedures)	Interne/externe Bewertungsverfahren, Benannte Stellen, Konformitätserklärungen, CE-Label, EU-Datenbank.
BO 8.1 – 8.2 Limited Risk & Transparenzpflichten	Art. 52 (Transparency Obligations for Certain AI Systems)	Kennzeichnungspflichten für Chatbots, Emotion Recognition, Deepfakes und synthetische Inhalte.
BO 9.1 – 9.2 GPAI & Systemic Risk	Art. 53–55 (General-Purpose AI & Systemic Risk Models) + Art. 56 (Codes of Practice)	GPAI-Pflichten, Transparenzberichte, Copyright-Nachweise, Evaluation, Red-Team-Testing, Incident-Reporting.
BO 10.1 – 10.2 FRIA (Fundamental Rights Impact Assessment)	Art. 27 (FRIA) + Erwägungsgründe (73–78)	Pflicht für öffentliche Stellen & bestimmte Privatakteure, Integration in DSFA, Dokumentations-Template.
BO 11.1 – 11.2 Post-Market Monitoring & Marktaufsicht	Art. 61–65 (Post-Market Monitoring & Corrective Actions) + Art. 67–70 (Market Surveillance)	Post-Market-Monitoring-Plan, Incident-Meldung, Berichterstattung, Korrekturmaßnahmen, Behördenkooperation.
BO 12.1 – 12.2 Governance & Organisation im Unternehmen	Art. 17 – 23 (Provider Responsibilities) + Art. 29 – 31 (Deployer / Distributor / Importer Obligations)	Interne Rollen, Verantwortlichkeiten, Schulungspflichten, Eskalationsmechanismen, Organisatorische Verankerung.
BO 13.1 – 13.2 Minimales Risiko & freiwillige Governance	Erwägungsgründe (60–63) + Art. 69 (Voluntary Codes of Conduct)	Förderung ethischer Selbstregulierung, freiwillige Maßnahmen nach ISO 42001/OECD, CSR/ESG-Integration.

© A4Q Copyright 2025

Kapitel / BO	Relevante Artikel / Abschnitte EU AI Act	Abgedeckte Themen / Anforderungen
BO 14.1 – 14.2 Audit-Readiness & Sanktionen	Art. 71–74 (Enforcement & Penalties) + Art. 63 (Post-Market Reporting)	Vorbereitung auf Audits, Bußgelder, Korrekturprozesse, Behördenkommunikation.
BO 15.1 – 15.2 Harmonisierte Standards & Presumption of Conformity	Art. 40–42 (Harmonised Standards & Common Specifications)	Presumption of Conformity, Standards-Entwicklung (CEN/CENELEC), Standard-Mapping zu ISO 42001/23894.
BO 16.1 – 16.2 Globale Schnittstellen & Exportkontrolle	Art. 88–92 (International Cooperation) + DSGVO Kap. V Datenexport + Dual-Use-Verordnung (EU 2021/821)	Datenexport, Drittstaaten-Übermittlungen, Lieferketten-Compliance, IP und Handelsbeschränkungen.
BO 17.1 – 17.2 Praktische Übungen & Fallstudien	Art. 6 – 55 (Querschnitt) + Annex III	Anwendung der Pflichten in Praxisfällen (Annex III, GPAI, FRIA). Praktische Compliance-Dokumentation.
Optional BO 18.1 – 18.2 Roadmap & Readiness Assessment 2025–2027	Art. 84–87 (Implementation Timeline & Transition Periods) + Art. 90 (AI Office Tasks)	Planung der Umsetzungsphasen, Readiness-Bewertung, Interne Selbstkontrolle und Reporting.
Optional BO 19.1 – 19.2 Zukunft & Weiterentwicklung des Regulierungsrahmens	Erwägungsgründe (91–99) + Art. 88 – 92 (AI Board, Cooperation, Future Updates)	Beobachtung neuer Leitlinien, Frontier-AI-Risiken, AI Safety Institute, künftige Anpassungen.

0.8 Abkürzungen

Abkürzung	Langform	Bedeutung / Kontext
AI	Artificial Intelligence / Künstliche Intelligenz	Übergeordneter Themenbereich des Syllabus
AI Act	EU Artificial Intelligence Act	EU-Verordnung zur Regulierung von KI-Systemen
AI Office	European Artificial Intelligence Office	EU-Behörde zur Durchsetzung des AI Act
AI Officer	Verantwortliche Person für KI-Compliance	Rolle zur Überwachung der Einhaltung von KI-Vorgaben
AI RMF	Artificial Intelligence Risk Management Framework (NIST)	US-Rahmenwerk für das Management von KI-Risiken
AI Safety Institute (AISI)	AI Safety Institute	Geplante EU-/UK-Institution für Sicherheitsprüfungen
AI System	Künstliches Intelligenzsystem	Technisches System, das KI-Funktionalitäten bereitstellt
AI Trust Label	Vertrauenskennzeichnung für KI-Systeme	Geplantes EU-Kennzeichen für vertrauenswürdige KI
Annex III	Anhang III des EU AI Act	Liste der automatisch als „Hochrisiko“ eingestuften KI-Systeme
Art.	Artikel	Verweis auf Artikelnummern im EU AI Act oder anderen EU-Verordnungen
BO	Business Outcome	Übergeordnete Lern- oder Ergebniseinheit im Syllabus

© A4Q Copyright 2025

Abkürzung	Langform	Bedeutung / Kontext
CE	Conformité Européenne	EU-Konformitätskennzeichnung für Produkte
CE-Kennzeichnung	Conformité Européenne Marking	EU-Kennzeichen für Konformität
CEN	Comité Européen de Normalisation	Europäisches Komitee für Normung
CENELEC	Comité Européen de Normalisation Électrotechnique	Europäisches Komitee für elektrotechnische Normung
CRA	Cyber Resilience Act	EU-Verordnung zur Cybersicherheit von Produkten
CSR	Corporate Social Responsibility	Gesellschaftliche Verantwortung von Unternehmen
Data Act	EU Data Act	EU-Verordnung zur Nutzung und Weitergabe von Daten
DPA	Data Processing Agreement	Vereinbarung zur Datenverarbeitung (Datenschutz)
DPO	Data Protection Officer	Datenschutzbeauftragte:r nach DSGVO
DSA	Digital Services Act	EU-Verordnung zu digitalen Diensten
DSFA	Datenschutz-Folgenabschätzung	DSGVO-Instrument zur Bewertung von Datenschutzrisiken
DSGVO	Datenschutz-Grundverordnung (GDPR)	EU-Verordnung zum Schutz personenbezogener Daten
ENISA	European Union Agency for Cybersecurity	EU-Agentur für Cybersicherheit
ESG	Environmental, Social, Governance	Nachhaltigkeits- und Ethik-Kriterien für Unternehmensführung
EU	Europäische Union	Politische und rechtliche Organisation Europas
EU AI Board	European Artificial Intelligence Board	Gremium zur Koordination der nationalen Behörden
FRIA	Fundamental Rights Impact Assessment	Grundrechts-Folgenabschätzung gem. Art. 27 AI Act
GDPR	General Data Protection Regulation / DSGVO	EU-Datenschutz-Grundverordnung
GPAI	General Purpose Artificial Intelligence	Allgemeine KI-Modelle mit Mehrzweckcharakter
HLEG	High-Level Expert Group on AI	EU-Expertengruppe zu vertrauenswürdiger KI
HR	Human Resources	Personalwesen
HR-System / HR	Human Resources	Personalwesen, z. B. KI in Bewerbungsprozessen
IEC	International Electrotechnical Commission	Internationale Normenorganisation für Elektrotechnik
IP	Intellectual Property	Geistiges Eigentum
IPCT/XMP	Metadata Standards	Standardformate für technische Metadaten (bei KI-Kennzeichnung)
ISMS	Information Security Management System	Managementsystem zur Informationssicherheit (ISO 27001)
ISO	International Organization for Standardization	Internationale Normungsorganisation

© A4Q Copyright 2025

Abkürzung	Langform	Bedeutung / Kontext
ISO/IEC 22989	Artificial Intelligence – Concepts and Terminology	Grundlagen- und Begriffsstandard für KI
ISO/IEC 23053	Framework for Machine Learning (ML)	Rahmenwerk für maschinelles Lernen
ISO/IEC 23894	Artificial Intelligence — Risk Management	Norm für KI-Risikomanagement (ISO-Standard)
ISO/IEC 42001	Artificial Intelligence Management System	Internationale Norm für KI-Managementsysteme
ISO/IEC JTC 1/SC 42	Joint Technical Committee 1, Subcommittee 42	ISO/IEC-Gremium für KI-Standardisierung
JSON-LD	JavaScript Object Notation for Linked Data	Format zur maschinenlesbaren Kennzeichnung
K1–K6	Bloom's Taxonomy Knowledge Levels	Kognitive Wissensstufen für Lernziele (Erinnern bis Erschaffen)
KPI	Key Performance Indicator	Leistungskennzahl
LLM	Large Language Model	Sprachmodell (z. B. ChatGPT, Gemini etc.)
ML	Machine Learning	Maschinelles Lernen
NIST	National Institute of Standards and Technology	US-amerikanische Normungs- und Forschungseinrichtung
NIST AI RMF	NIST Artificial Intelligence Risk Management Framework	US-Rahmenwerk für KI-Risikomanagement
NLP	Natural Language Processing	Verarbeitung natürlicher Sprache
OECD	Organisation for Economic Co-operation and Development	Internationale Organisation zur wirtschaftlichen Zusammenarbeit
OECD AI Principles	Principles on Artificial Intelligence	Internationale Grundsätze für vertrauenswürdige KI
PIMS	Privacy Information Management System	Datenschutzmanagementsystem (nach ISO/IEC 27701)
QA	Quality Assurance	Qualitätssicherung
QM	Qualitätsmanagement	Systematische Qualitätssicherung (ISO 9001)
Red-Team-Testing	Red Team Testing	Sicherheitstestverfahren zur Simulation von Angriffen
RMF	Risk Management Framework	Rahmenwerk zur systematischen Risikosteuerung
SLA	Service Level Agreement	Vertragsvereinbarung zu Leistungsparametern
UI	User Interface	Benutzeroberfläche; z. B. für KI-Kennzeichnung
UN	United Nations	Vereinte Nationen – internationale Regulierungsebene
UX	User Experience	Nutzererlebnis; relevant bei Transparenzpflichten
WORM	Write Once, Read Many	Technische Sicherheitsfunktion für unveränderliche Speicherung

© A4Q Copyright 2025

1 Einführung in AI Compliance & den EU AI Act

Dauer & Zielsetzung

⏱️ Unterrichtszeit 45 Minuten

🎯 Business Outcomes:

- **BO 1.1:** Teilnehmende sind in der Lage, die von der EU-AI-Verordnung betroffenen Unternehmensbereiche zu identifizieren und aktiv zur Entwicklung wirksamer Compliance-Strategien beizutragen.
- **BO 1.2:** Teilnehmende sind vorbereitet, zentrale Begriffe, Rollen und Ziele des EU AI Act zu verstehen und Verantwortlichkeit für KI-Compliance im Unternehmen zu fördern.

Lernziele (Learning Objectives - LO)

- LO 1.1 (K1): Teilnehmende erkennen die grundlegende Bedeutung von Künstlicher Intelligenz als Schlüsseltechnologie und können den Begriff sowie zentrale Teilbereiche (Maschinelles Lernen, regelbasierte Systeme u. a.) benennen.
- LO 1.2 (K2): Teilnehmende erläutern, wie KI strategische Wertschöpfung und gleichzeitig neue Compliance- und Risikofelder im Unternehmen beeinflusst.
- LO 1.3 (K2): Teilnehmende beschreiben die Zielsetzung und Grundprinzipien des EU AI Act sowie die beteiligten Akteursrollen (Provider, Deployer, Importer u. a.).
- LO 1.4 (K3): Teilnehmende ordnen den EU AI Act zeitlich und organisatorisch ein und können erste Implikationen für eigene Geschäftsprozesse und Governance-Strukturen ableiten.
- LO 1.5 (K1): Teilnehmende kennen den Anwendungsbereich des EU AI Act, insbesondere die Abgrenzung zwischen in und außerhalb der EU entwickelten KI-Systemen sowie deren Geltung für Anbieter und Verwender.

Wichtige Begriffe:
Künstliche Intelligenz (KI), Maschinelles Lernen (ML), Regelbasierte Systeme, EU AI Act, Provider, Deployer, Importer, Distributor, AI Office, AI Board, Risikobasierter Ansatz, Grundrechte, Compliance, Governance, Verantwortlichkeit, Transparenzpflicht, Geltungsbereich, Schlüsseltechnologie.

Einleitung

Dieses Kapitel bietet einen grundlegenden Einstieg in das Thema Künstliche Intelligenz und ihre Bedeutung für Organisationen, Wirtschaft und Gesellschaft. Es schafft ein gemeinsames Verständnis

© A4Q Copyright 2025

zentraler Begriffe und Konzepte und zeigt, warum der verantwortungsvolle und regelkonforme Umgang mit KI zunehmend an Bedeutung gewinnt. Damit legt es die Basis für das Verständnis späterer Themen wie Risikoklassifizierung, Governance und Compliance-Pflichten.

1.1 Was ist Künstliche Intelligenz im regulatorischen Kontext

Künstliche Intelligenz (KI) bezeichnet IT-Systeme, die Aufgaben übernehmen, die üblicherweise menschliche Intelligenz erfordern – etwa Mustererkennung, Sprachverarbeitung oder Entscheidungsfindung.
Im rechtlichen Sinne wird KI im EU AI Act (Art. 3 Abs. 1) als ein System beschrieben, das durch maschinelles Lernen, logik- oder wissensbasierte Ansätze oder statistische Verfahren Ergebnisse erzeugt, die das physische oder virtuelle Umfeld beeinflussen.
Damit unterscheidet sich die gesetzliche Definition von rein technischen Beschreibungen: sie zielt auf Funktion und Wirkung ab, nicht auf eine bestimmte Technologie.

Ziel dieser Definition ist es, alle Systeme zu erfassen, die Entscheidungen oder Inhalte generieren, die für Menschen rechtliche, wirtschaftliche oder soziale Konsequenzen haben – unabhängig davon, ob sie neuronale Netze, Entscheidungsbäume oder einfache regelbasierte Methoden nutzen.

1.1.1 Regulatorische Teilbereiche

Der EU AI Act unterscheidet keine Technologien, sondern bewertet Risikopotenzial und Einsatzkontext. Dennoch lassen sich typische Entwicklungsansätze regulatorisch einordnen:

- Regelbasierte Systeme – folgen festen Wenn-Dann-Regeln. Meist Minimal- oder Low-Risk, sofern keine automatisierten Entscheidungen mit Personenbezug getroffen werden.
- Maschinelles Lernen (ML) – Systeme lernen aus Daten; regulatorisch relevant, sobald Trainingsdaten Bias enthalten oder Entscheidungsprozesse nicht nachvollziehbar sind.
- Deep Learning / Neuronale Netze – gelten im AI Act häufig als Hochrisiko-Technologien, wenn sie sicherheits- oder grundrechtskritische Aufgaben ausführen.
- NLP & Computer Vision – fallen unter dieselben Anforderungen (Art. 10 Datenqualität, Art. 13–15 Transparenz und Oversight), sobald sie personenbezogene oder sicherheitsrelevante Daten verarbeiten.

1.1.2 Strategische und regulatorische Bedeutung von KI im Unternehmen

KI ist längst kein reines IT-Thema, sondern ein steuerungsrelevanter Unternehmensfaktor – mit Chancen für Innovation und zugleich Pflichten für Compliance und Governance.
Der EU AI Act, die DSGVO, das Produktsicherheitsrecht und branchenspezifische Vorschriften (z. B. Medizinprodukte-, Finanz- oder Arbeitsrecht) greifen hier ineinander.

© A4Q Copyright 2025

Perspektive	Relevante Aspekte aus Unternehmenssicht
Wertschöpfung & Effizienz	KI ermöglicht Automatisierung, Prozessoptimierung und datenbasierte Entscheidungen – dadurch entstehen neue Pflichten zur Nachvollziehbarkeit und Auditierbarkeit.
Innovation & Wettbewerb	Datengetriebene Services und generative Modelle fördern Innovation, müssen jedoch im Einklang mit Urheber- und Verbraucherschutzrecht stehen (vgl. Art. 53 AI Act – Transparenz bei GPAI).
Risiken & Compliance	„Black-Box-Entscheidungen" bergen Haftungs- und Diskriminierungsrisiken. Der AI Act fordert Fairness, Erklärbarkeit und menschliche Aufsicht (Art. 14–15).
Organisation & Transformation	Der Einsatz von KI erfordert Governance-Strukturen, neue Rollen (z. B. AI Compliance Officer, Data Steward) und **AI Literacy-Programme** für Mitarbeitende (Art. 4 AI Act).

Typische Anwendungsfelder mit regulatorischer Relevanz

- **Personalwesen (HR):** Screening-Tools und Chatbots → Risiko algorithmischer Diskriminierung → Hochrisiko nach Annex III (2).
- **Finanzen:** Kreditscoring und Fraud Detection → Hochrisiko gemäß Annex III (5).
- **Marketing:** Profiling & Targeting → Transparenz- und Informationspflichten (Art. 52).
- **Industrie:** Predictive Maintenance → Sicherheits- und Zuverlässigkeitsanforderungen (Art. 15).
- **Öffentliche Verwaltung:** KI-gestützte Antragsprüfung → Grundrechtsprüfung & FRIA-Pflicht (Art. 27).

1.1.3 Historischer und rechtlicher Kontext

Die Entwicklung der KI begann mit regelbasierten Systemen und Expertensystemen der 1980er Jahre und führte über maschinelles Lernen zum heutigen Deep Learning.
Mit der Verfügbarkeit großer Datenmengen und Rechenleistung entstanden neue gesellschaftliche und ethische Fragen.
Der EU AI Act ist die Antwort auf diese Entwicklung: Er überträgt die Leitprinzipien der DSGVO – Transparenz, Verantwortlichkeit und Rechenschaft – auf KI-Systeme.

1.1.4 Bedeutung für Governance und Compliance

KI ist strategisch entscheidend, aber auch regulatorisch anspruchsvoll.
Unternehmen, die KI einsetzen, müssen technologische Innovation mit rechtlicher Sorgfaltspflicht verbinden.
Der EU AI Act macht Governance, Risikomanagement und Dokumentation zur Pflicht und

© A4Q Copyright 2025

Führungsaufgabe.
Er verlangt, dass Organisationen:

- Risiken systematisch identifizieren und managen (Art. 9),
- Datenqualität und Fairness sicherstellen (Art. 10),
- menschliche Kontrolle gewährleisten (Art. 14),
- und über ein geeignetes Qualitäts- und Managementsystem verfügen (Art. 17–23, ISO/IEC 42001).

1.2 Der EU AI Act im Überblick

Der EU AI Act ist Teil des europäischen Digitalrechtsrahmens („Digital Rulebook“) und ergänzt bestehende Gesetze wie die DSGVO, die Produktsicherheits- und Haftungsrichtlinien sowie sektorale Regulierungen (z. B. MDR, FinReg, E-Commerce-Richtlinie).
Er verfolgt das Ziel, ein vertrauenswürdiges KI-Ökosystem zu schaffen, das Innovation ermöglicht und gleichzeitig Grundrechte schützt.

1.2.1 Schlüsselprinzipien des AI Act

Der EU AI Act definiert eine Reihe zentraler Prinzipien, die die Grundlage für einen vertrauenswürdigen und rechtmäßigen Einsatz von Künstlicher Intelligenz in der Europäischen Union bilden.
Diese Prinzipien stellen sicher, dass KI-Systeme so entwickelt, getestet und eingesetzt werden, dass Sicherheit, Grundrechte und Transparenz gewahrt bleiben, während Innovation gleichzeitig gefördert wird.
Sie legen fest, wie Organisationen ihre Compliance-, Risikomanagement- und Governance-Prozesse über den gesamten Lebenszyklus eines KI-Systems hinweg strukturieren müssen.

- **Risikobasierter Ansatz (Art. 6 ff.)** – Einstufung von KI-Systemen nach Risiko und Anwendung.
- **Transparenz & Nachvollziehbarkeit (Art. 13–15)** – Pflicht zur Offenlegung und verständlichen Dokumentation.
- **Human Oversight & Sicherheit (Art. 14–15)** – Vermeidung autonomer Entscheidungen ohne menschliche Kontrolle.
- **Datenqualität & Governance (Art. 10)** – Anforderungen an Trainings- und Validierungsdaten.
- **Post-Market Monitoring & Korrekturmaßnahmen (Art. 61 ff.)** – Pflichten nach dem Inverkehrbringen.

1.2.2 Akteursrollen und Verantwortlichkeiten

Der EU AI Act definiert spezifische Rollen und Verantwortlichkeiten für alle Akteure, die an der Entwicklung, dem Vertrieb und der Nutzung von KI-Systemen beteiligt sind.

© A4Q Copyright 2025

Diese klar zugewiesenen Pflichten gewährleisten Transparenz, Verantwortlichkeit und eine einheitliche Compliance über die gesamte KI-Wertschöpfungskette hinweg – von der Entwicklung über die Markteinführung bis hin zur Nachmarktüberwachung.

Rolle	Zentrale Pflichten
Provider (Anbieter)	Entwickelt oder bringt KI-Systeme in Verkehr; trägt Verantwortung für Risikomanagement, technische Dokumentation, CE-Kennzeichnung und EU-Datenbank-Eintrag.
Deployer (Bereitsteller)	Verwendet KI-Systeme in eigener Verantwortung; muss sicherstellen, dass Systeme gemäß Anleitung betrieben und überwacht werden.
Importer	Führt KI-Systeme aus Drittstaaten in die EU ein; prüft CE-Kennzeichnung und Konformität.
Distributor (Händler)	Vertreibt KI-Systeme innerhalb der EU; überwacht Kennzeichnungen und informiert über Mängel.
Authorised Representative	Handelt im Auftrag eines Providers; fungiert als Kontaktstelle für Marktaufsichtsbehörden.

1.3 Zeitplan der Umsetzung (2024 – 2027)

Die Umsetzung des EU AI Act erfolgt in einem gestaffelten Zeitplan, um Unternehmen, Behörden und Marktteilnehmenden eine schrittweise Anpassung an den neuen Rechtsrahmen und die damit verbundenen Compliance-Pflichten zu ermöglichen.

Datum	Inkrafttreten / Pflichten
01 Aug 2024	Verordnung (EU) 2024/1689 tritt in Kraft.
02 Feb 2025	Verbotene Praktiken (Art. 5) und AI-Literacy-Pflichten (Art. 4) gelten.
02 Aug 2025	Pflichten für General-Purpose-AI-Modelle (GPAI) (Art. 53 – 55).
02 Aug 2026 – 2027	Hochrisiko-Pflichten (Art. 9 – 51) und Konformitätsverfahren voll anwendbar; Marktaufsichtsbehörden aktiv.

(Quelle: Art. 113 EU AI Act – Anwendungs- und Übergangsbestimmungen)

© A4Q Copyright 2025

1.4 Kernaussage

Der EU AI Act verpflichtet Unternehmen, den Einsatz von KI vorausschauend, kontrolliert und dokumentiert zu gestalten.
KI-Systeme müssen künftig nicht nur technisch sicher, sondern auch rechtlich überprüfbar sein.
Damit wird AI Compliance von einer optionalen Absicherung zu einem strategischen Bestandteil verantwortungsvoller Unternehmensführung.

© A4Q Copyright 2025

2 Risikobasierter Ansatz & Klassifikation

⏱ **Unterrichtszeit:** 60 Minuten

🎯 **Business Outcomes:**

- **BO 2.1:** Teilnehmende erwerben die Kompetenz, KI-Systeme nach den vier Risikostufen einzustufen und daraus die jeweils geltenden Pflichten abzuleiten.
- **BO 2.2:** Teilnehmende sind vorbereitet, angemessene Maßnahmen zu planen und Prioritäten nach Risikograd zu setzen, um Compliance-Ressourcen zielgerichtet einzusetzen.

Lernziele (Learning Objectives – LO)

- **LO 2.1 (K1):** Teilnehmende kennen die vier Risikostufen des EU AI Act (unzulässig, hoch, begrenzt, minimal) und verstehen deren grundlegende Bedeutung für den Marktzugang.
- **LO 2.2 (K2):** Teilnehmende können anhand typischer Anwendungsfälle KI-Systeme den jeweiligen Risikostufen zuordnen und diese Abgrenzung begründen.
- **LO 2.3 (K2):** Teilnehmende erläutern, welche regulatorischen Pflichten und Dokumentationsanforderungen sich aus den einzelnen Risikostufen ergeben.
- **LO 2.4 (K3):** Teilnehmende können auf Basis der Risikoklassifikation geeignete organisatorische und technische Maßnahmen priorisieren und deren Umsetzung planen.
- **LO 2.5 (K3):** Teilnehmende können Übergänge oder Änderungen der Risikokategorie erkennen, bewerten und geeignete Re-Assessment-Prozesse entwerfen.
- **LO 2.6 (K1):** Teilnehmende kennen den Zusammenhang zwischen Risikoklassifikation, Konformitätsbewertung und den daraus abgeleiteten Compliance-Pflichten.

Wichtige Begriffe:
Risikostufe, Unzulässiges Risiko, Hochrisiko, Begrenztes Risiko, Minimales Risiko, Annex III, Verhältnismäßigkeit, Risikodynamik, Re-Assessment, Human Oversight, AI-Risk-Review, Risikopriorisierung, Konformitätsprüfung.

Einleitung

Dieses Kapitel erläutert den risikobasierten Ansatz des EU AI Act und zeigt, wie KI-Systeme nach ihrem potenziellen Einfluss auf Sicherheit, Grundrechte und Gesellschaft klassifiziert werden. Die Teilnehmenden verstehen, warum die Unterscheidung zwischen unzulässigen, hochriskanten, begrenzt riskanten und minimalen Risikostufen entscheidend für die Anwendung der regulatorischen Pflichten ist. Dadurch wird ein Verständnis geschaffen, wie Risikoabwägung und Compliance in der Praxis zusammenwirken.

© A4Q Copyright 2025

2.1 Grundprinzip des risikobasierten Ansatzes

Der EU AI Act verfolgt das Prinzip der **Verhältnismäßigkeit**: Je höher das Risiko für Grundrechte, Gesundheit oder Sicherheit, desto strenger die Pflichten.
Der Risikograd bestimmt somit den gesamten Compliance-Aufwand und die Priorisierung interner Maßnahmen.

Risikostufe	Merkmale	Beispiele	Rechtsfolgen
Unzulässiges Risiko	Verletzung der Menschenwürde oder Grundrechte → Art. 5 AI Act	Social Scoring, Subliminale Manipulation, Echtzeit-Biometrie im öffentlichen Raum	**Verboten** – Marktzugang untersagt
Hohes Risiko	Entscheidung mit materiellen Auswirkungen auf Menschen (Anhang III)	Bewerbungstools, Kreditscoring, medizinische KI	Zulässig nur bei vollständiger Konformitätsbewertung und CE-Kennzeichnung
Begrenztes Risiko	Interaktion mit Menschen, Informations- oder Täuschungsrisiko	Chatbots, Emotionserkennung, Deepfakes	Zulässig mit Transparenz- und Kennzeichnungspflicht
Minimales Risiko	Keine Grundrechtsrelevanz, alltägliche Hilfssysteme	Spamfilter, Produktvorschläge	Frei verwendbar, keine Pflichten – Empfehlung: freiwillige Ethik-Standards

2.2 Annex III – Automatisch hochrisikobehaftete KI-Systeme

Der **Anhang III** des EU AI Act definiert acht Anwendungsbereiche, deren **Zweck** und **Einsatzkontext** als gesellschaftlich besonders sensibel gelten.
KI-Systeme, die in diesen Bereichen **zum jeweiligen Zweck** eingesetzt werden, sind **unabhängig von der Technologie oder Ausgestaltung** als **Hochrisiko-Systeme** einzustufen.
Maßgeblich ist nicht, *was die KI technisch kann*, sondern *wofür sie eingesetzt wird* – also der **Zweckbezug**.

Zweckdefinition laut EU AI Act

Ein System fällt unter Annex III, wenn es

- Entscheidungen oder Bewertungen über Menschen trifft,

© A4Q Copyright 2025

- Grundrechte, Bildung, Arbeit, Sicherheit oder Rechtsstaatlichkeit betrifft,
- oder den Zugang zu zentralen gesellschaftlichen Ressourcen steuert.

Hochrisiko-Kategorien gemäß Annex III mit Praxisbeispielen

Nr.	Bereich	Zweck der Regulierung	Beispiel aus der Praxis	Einstufung
1	**Biometrische Identifizierung und Kategorisierung**	Schutz vor Überwachung, Profiling und Diskriminierung; Begrenzung des Einsatzes sensibler biometrischer Verfahren.	Ein Bahnhof verwendet KI-gestützte Gesichtserkennung, um Personen auf Fahndungslisten in Echtzeit zu identifizieren.	**Hochrisiko**, teils mit Verbotstatbestand (Art. 5)
2	**Kritische Infrastrukturen**	Gewährleistung der öffentlichen Sicherheit und Versorgung; KI-Fehler dürfen keine physischen Schäden verursachen.	Eine Energieversorger-KI steuert automatisch die Lastverteilung im Stromnetz, um Blackouts zu verhindern.	**Hochrisiko**, da Fehlsteuerung Menschen gefährden kann
3	**Bildung und Berufsbildung**	Sicherstellung fairer und objektiver Bewertung von Lernenden; Verhinderung algorithmischer Benachteiligung.	Eine Lernplattform analysiert Schüleraufsätze und vergibt automatisch Noten oder Feedback, das in die Leistungsbeurteilung eingeht.	**Hochrisiko (Annex III Nr. 3)**
4	**Beschäftigung, Arbeitsverwaltung und Zugang zur Beschäftigung**	Schutz vor Diskriminierung im Berufsleben und Sicherung transparenter Auswahlprozesse.	Ein HR-System filtert Bewerbungen automatisiert nach Eignung und erstellt Ranking-Listen für Recruiter.	**Hochrisiko**
5	**Zugang zu wesentlichen privaten und**	Schutz wirtschaftlicher und sozialer Teilhabe; Entscheidungen über Kredit, Versicherung oder	Eine Bank nutzt KI-Scoring, um Kreditanträge automatisch zu	**Hochrisiko**, Art. 6 i. V. m. Annex III Nr. 5

© A4Q Copyright 2025

Nr.	Bereich	Zweck der Regulierung	Beispiel aus der Praxis	Einstufung
	öffentlichen Diensten	Sozialleistung dürfen nicht unfair sein.	genehmigen oder abzulehnen.	
6	**Strafverfolgung und Polizei**	Wahrung rechtsstaatlicher Verfahren, Vermeidung voreingenommener oder fehlerhafter Strafverfolgung.	Eine Ermittlungssoftware bewertet das Rückfallrisiko von Straftätern und unterstützt bei Haftentscheidungen.	**Hochrisiko**, ggf. unter Aufsichtspflicht
7	**Migration, Asyl und Grenzkontrolle**	Schutz der Grundrechte von Migrant:innen; Sicherstellung objektiver und menschenrechtskonformer Verfahren.	Eine KI-gestützte Grenzkontrolle analysiert Sprache, Gestik und Mimik von Reisenden, um Risikoindikatoren zu bewerten.	**Hochrisiko**, besondere ethische Sensitivität
8	**Justiz und demokratische Prozesse**	Wahrung der richterlichen Unabhängigkeit und Integrität demokratischer Entscheidungen.	Ein Gericht verwendet eine KI-gestützte Entscheidungshilfe, die Urteile früherer Fälle analysiert und Strafmaße vorschlägt.	**Hochrisiko**, Art. 6 i. V. m. Annex III Nr. 8

Beispiel: Bildung und Berufsbildung – Zweck und Abgrenzung

Der Zweck von Annex III Nr. 3 ist der **Schutz von Fairness und Chancengleichheit** bei der Bewertung oder Förderung von Lernenden.
Daher gilt:

Einsatzszenario	Zweckbezug	Einstufung
KI bewertet Lernleistungen, Prüfungen oder Zulassungen	Beeinflusst direkt Bildungschancen	**Hochrisiko**
KI unterstützt Lernende durch Feedback oder adaptive Aufgabensteuerung	Indirekte Steuerung des Lernwegs	**Hochrisiko**
Lehrende nutzen generative KI zur Unterrichts- oder Prüfungserstellung	Kein direkter Einfluss auf Lernende, rein vorbereitender Zweck	**Begrenztes Risiko (Art. 52)**

© A4Q Copyright 2025

Einsatzszenario	Zweckbezug	Einstufung
Schreib- oder Übersetzungshilfen im Unterricht	Unterstützungsfunktion, kein Bewertungszweck	**Begrenztes Risiko**

Interpretationshinweis :
Lehrende, die KI ausschließlich zur Erstellung oder Verbesserung von Unterrichtsmaterialien, Folien oder Aufgaben verwenden, **betreiben kein Hochrisiko-System**. Erst wenn die KI Ergebnisse von Lernenden bewertet oder Lernprozesse steuert, wird die Anwendung als **Hochrisiko** eingestuft.

Konsequenz

Systeme mit einem Zweck nach Anhang III gelten **automatisch als Hochrisiko-KI** und unterliegen den Pflichten nach **Art. 9–24 EU AI Act**, insbesondere:

- Einrichtung eines **Risikomanagementsystems** (Art. 9)
- Sicherstellung der **Datenqualität und Nichtdiskriminierung** (Art. 10)
- Vollständige **technische Dokumentation** (Art. 11)
- **Transparenz- und Human-Oversight-Pflichten** (Art. 13–14)
- **Konformitätsbewertung und CE-Kennzeichnung** (Art. 17–23)

Eine spätere **Zweckänderung** (z. B. Einsatz eines generativen Tools zur automatischen Lernbewertung) führt zu einer **Neubewertung** und ggf. Hochstufung der Risikoklasse (Art. 6 Abs. 3).

2.3 Kriterien zur Risikoeinstufung

Auch wenn ein System nicht in Anhang III aufgeführt ist, müssen Anbieter und gegebenenfalls Bereitsteller (Provider / Deployer) selbst bewerten, welche Risiken für Gesundheit, Sicherheit oder Grundrechte entstehen können – unter Berücksichtigung des beabsichtigten Zwecks und des Einsatzkontexts des Systems. Diese Bewertung entscheidet, **ob zusätzliche Pflichten** aus dem EU AI Act greifen (z. B. Risikomanagement, Dokumentation, Human Oversight).

Anwendung der Risikokriterien

Die folgenden fünf Kriterien helfen, die Risikostufe nachvollziehbar einzuschätzen. Sie sind **in Kombination** zu betrachten – kein einzelnes Kriterium entscheidet allein. Je mehr dieser Kriterien **mit „Ja“** beantwortet werden, desto wahrscheinlicher ist eine **höhere Risikostufe** (hoch / begrenztes Risiko).

© A4Q Copyright 2025

Kriterium	Leitfrage zur Beurteilung	Was bedeutet das in der Praxis?	Typische Folge
1. Zweck & Einfluss	Trifft das System Entscheidungen, die Menschen betreffen (z. B. Auswahl, Bewertung, Zugang)?	KI, die über Personen oder Rechte entscheidet, gilt als besonders sensibel.	Grundrechts- und Ethikprüfung erforderlich
2. Einsatzumfeld	Wird die KI in sicherheitskritischen oder öffentlichen Bereichen eingesetzt (z. B. Medizin, Verwaltung, Bildung)?	Je öffentlicher oder sicherheitsrelevanter der Einsatz, desto größer das Risiko für Dritte.	Kann zusätzliche Aufsichts-, Melde- oder Berichtspflichten durch zuständige nationale Behörden auslösen
3. Grad der Autonomie	Kann das System eigenständig handeln oder Entscheidungen treffen, ohne menschliche Freigabe?	Fehlentscheidungen können schwer korrigierbar sein; Menschen müssen eingreifen können.	Gilt nur bei Einstufung als Hochrisiko-System: Pflicht zur menschlichen Aufsicht nach Art. 14 EU AI Act
4. Betroffene Gruppe	Betrifft das System schutzbedürftige Personen (Kinder, Kranke, Beschäftigte, Migrant:innen)?	Diese Gruppen genießen erhöhten rechtlichen Schutz.	Verstärkte Sorgfaltspflichten und Monitoring
5. Wirkungsreichweite	Wie viele Personen sind potenziell betroffen oder können beeinflusst werden?	Systeme mit großem Nutzerkreis erhöhen das kollektive Risiko (z. B. Social Scoring).	Größerer Dokumentations- und Nachweisumfang

Bewertungslogik (Risikoprofil)

Bewertungsergebnis	Interpretation	Beispielhafte Einstufung
0–1 Kriterien zutreffend	Kein signifikanter Einfluss auf Menschen oder Rechte	→ **Minimales Risiko** (z. B. Rechtschreib-KI, Spamfilter)
2–3 Kriterien zutreffend	Potenzieller Einfluss auf Wahrnehmung oder Information	→ **Begrenztes Risiko** (z. B. Chatbot, Lernhilfe-KI)

© A4Q Copyright 2025

Bewertungsergebnis	Interpretation	Beispielhafte Einstufung
4–5 Kriterien zutreffend	Einfluss auf Grundrechte, Sicherheit oder Lebensumstände	→ **Hochrisiko** (z. B. Bewerberauswahl, Kreditbewertung)

Praxis-Hinweis zur Anwendung

1. **Startpunkt** – Zweck klären:
   Welches konkrete Ziel verfolgt die KI-Anwendung (z. B. informieren, bewerten, steuern)?
2. **Kontext erfassen:**
   In welchem Umfeld und mit welchen Personen wird sie eingesetzt?
3. **Autonomie prüfen:**
   Gibt es menschliche Kontrolle oder handelt die KI eigenständig?
4. **Auswirkungen analysieren:**
   Was passiert, wenn die KI Fehler macht – wer wäre betroffen?
5. **Dokumentieren:**
   Die Entscheidung über die Risikostufe muss **begründet und nachvollziehbar** sein (z. B. im AI Risk Register oder Annex 9-Dokumentation).

Der **EU AI Act** gibt **keine abschließende, numerische oder algorithmische Bewertungsmatrix** vor. Er schreibt in **Art. 6 Abs. 2–3** nur vor, **welche Faktoren zu berücksichtigen sind**, wenn ein System *nicht automatisch* (über Annex III) als Hochrisiko gilt. Diese Faktoren sind qualitativ formuliert:

„… taking into account the intended purpose, the output, and the impact of the system on the rights or safety of persons …“

Das heißt:

- **Es gibt keine fixen Punktzahlen oder Schwellenwerte.**
- **Die Bewertung ist immer kontextabhängig.**
- Diese Offenheit ist gewollt, weil KI-Systeme sehr unterschiedlich sind und starre Kriterien Innovation hemmen würden.

Die Folge: Die **Risikobewertung ist interpretativ**, also **„regelgeleitet, aber nicht regelbestimmt“** – ein juristisch bewusst gewählter Ansatz, der Verantwortlichkeit statt Automatisierung fördern soll.

Wie Präzision hergestellt werden soll: „Guidance“ und „Harmonisierte Standards“

Weil das Gesetz selbst so offen bleibt, wird die Präzisierung **auf nachgelagerter Ebene** erfolgen – durch:

© A4Q Copyright 2025

Quelle	Rolle	Status (Oktober 2025)
AI Office / AI Board	Erstellt *Guidelines for Risk Classification* (gemeinsame Kriterien für Behörden & Unternehmen)	Entwurf in Arbeit, Veröffentlichung Q1/2026
CEN/CENELEC JTC 21	Erarbeitet harmonisierte europäische Normen (u. a. EN ISO/IEC 42001, 23894 sowie den Entwurf ISO/IEC TR 42006 zu AI-Compliance-Frameworks)	Teilweise veröffentlicht
Europäische Kommission (Delegierte Rechtsakte)	Kann bestimmte Systeme „nachträglich“ als Hochrisiko deklarieren oder herabstufen	Laufend nach Art. 7 EU AI Act

Eine strukturiertere und harmonisierte Bewertung wird somit möglich sein, sobald diese Leitlinien und delegierten Rechtsakte formell von der Europäischen Kommission angenommen wurden. Bis dahin gilt: Unternehmen und Organisationen müssen **selbst dokumentieren, wie sie zu ihrem Urteil kamen**.

Warum das gewollt ist – und wo die Grenze zur Willkür liegt

Die Offenheit ist **kein Fehler, sondern Teil des Governance-Konzepts**:
Der AI Act soll nicht jeden Einzelfall normieren, sondern Unternehmen dazu zwingen,

- **Risiken zu erkennen, zu begründen und zu dokumentieren**,
- anstatt sich hinter formalistischen Schwellenwerten zu verstecken.

Aber: Die Bewertung darf **nicht willkürlich** sein. Sie muss **nachvollziehbar, begründet und konsistent** erfolgen – z. B. durch:

- schriftlich dokumentierte Begründung (z. B. im „AI Risk Register“),
- Bezug auf offizielle Definitionen (Art. 3, Art. 6, Annex III),
- Verwendung harmonisierter Standards (ISO/IEC 23894 als Referenzrahmen).

In Konformitätsbewertungen oder aufsichtsbehördlichen Audits nach Art. 43 bis 51 steht nicht eine numerische Bewertung im Vordergrund, sondern die nachvollziehbare und begründete Dokumentation der getroffenen Risikoeinstufung.

Fazit

Die Risikoeinstufung ist keine technische Bewertung, sondern eine **rechtlich-ethische Beurteilung des Einsatzzwecks**. Je stärker eine KI in menschliche Entscheidungen oder Rechte eingreift, desto höher ist ihre Risikostufe – und desto umfassender sind die Compliance-Pflichten.

© A4Q Copyright 2025

2.4 Pflichten und Maßnahmen nach Risikostufe

Die Pflichten eines Unternehmens hängen direkt von der **Risikostufe des KI-Systems** ab.
Je höher das Risiko für Menschen, Grundrechte oder Sicherheit, desto strenger sind die rechtlichen Anforderungen.
Die folgende Übersicht zeigt **die vier Stufen, ihre rechtlichen Grundlagen, typischen Pflichten** und **empfohlene Maßnahmen** zur Umsetzung im Unternehmen.

Übersicht: Risikostufen, Pflichten und Unternehmensmaßnahmen

Risikostufe	Rechtsgrundlage & zentrale Pflichten	Was das praktisch bedeutet	Typische Maßnahmen im Unternehmen
Unzulässiges Risiko	**Art. 5 EU AI Act** – Verbot bestimmter Praktiken:• Subliminale Manipulation (unterbewusste Beeinflussung)• Ausnutzung von Schwächen (z. B. Kinder, Kranke)• Social Scoring durch Behörden• Echtzeit-Biometrie zur Überwachung im öffentlichen Raum	Diese Systeme **dürfen nicht entwickelt, verkauft oder eingesetzt** werden. Wenn sie identifiziert werden, müssen sie **sofort gestoppt** und der Aufsichtsbehörde gemeldet werden.	- Interner **Stop-Prozess** bei Verdacht auf Verbotstatbestand- **Abschaltung** und Sicherung aller Daten- **Meldung an Compliance/Behörde** (Incident Report)- **Ethik-Review**: Warum kam es dazu, und wie kann man das künftig vermeiden?
Hohes Risiko	**Art. 6–51 EU AI Act** – umfassende Pflichten:• **Risikomanagementsystem** (Art. 9)• **Anforderungen an Daten & Datenqualität** (Art. 10)• **Technische Dokumentation** (Art. 11)• **Transparenz & Benutzerinformation** (Art. 13)• **Human Oversight** – menschliche Aufsicht (Art. 14)• **Genauigkeit, Robustheit, Cybersecurity** (Art. 15)• **CE-Kennzeichnung & EU-**	Hochrisiko-Systeme dürfen **nur nach erfolgreicher Konformitätsbewertung** in Verkehr gebracht oder verwendet werden. Sie müssen jederzeit **prüf- und nachvollziehbar** sein.	- Aufbau eines **AI-Risikomanagementsystems** (z. B. nach ISO/IEC 23894)- Einrichtung eines **AI-Risk-Registers** für alle eingesetzten Systeme- **Dokumentation** aller Trainingsdaten, Modelle und Tests- **Human Oversight-Richtlinie**: wer darf eingreifen, wie?- **Regelmäßige Audits** und Nachweise für CE-Konformität- **Mitarbeiterschulung** zu Pflichten, Meldewegen und Oversight

© A4Q Copyright 2025

Risikostufe	Rechtsgrundlage & zentrale Pflichten	Was das praktisch bedeutet	Typische Maßnahmen im Unternehmen
	Konformitätserklärung (Art. 49)		
🟧 **Begrenztes Risiko**	**Art. 52 EU AI Act** – Transparenzpflichten:• Nutzer:innen müssen erkennen können, dass sie mit KI interagieren• Deepfakes, Chatbots, Emotionserkennung oder generative Inhalte müssen **gekennzeichnet** sein• Bei Deepfakes: Hinweis auf Manipulation oder Fiktion	Diese Systeme sind erlaubt, müssen aber **offenlegen, dass KI beteiligt ist**. Ziel ist der Schutz vor Täuschung oder Fehlinformation.	- **Hinweistext im UI** (z. B. „Antwort durch KI generiert“)- **Content-Kennzeichnung** (z. B. Wasserzeichen, Metadaten)- **Transparenzseite oder FAQ** über den Einsatz von KI- **Interne Prüfung**: Sind Nutzende ausreichend informiert?- **Opt-out-Möglichkeit** (z. B. bei Chatbots)
🟩 **Minimales Risiko**	Kein direkter Anwendungsfall im AI Act; freiwillige Orientierung an Standards:• Erwägungsgründe 81–84• ISO/IEC 42001 (AI Management System)• OECD- und UNESCO-Empfehlungen zu Ethik und Fairness	Diese Systeme haben **keine regulatorischen Pflichten**, weil sie keinen Einfluss auf Rechte oder Sicherheit haben (z. B. Spamfilter, UI-Helfer). Dennoch wird empfohlen, eine **freiwillige Governance** einzuführen, um Verantwortlichkeit zu zeigen.	- **AI-Governance-Leitlinie** (z. B. interne Ethik-Charta)- **Transparenz-Statement** auf Website („Wir setzen KI unterstützend ein…“)- **Dokumentation der Verantwortlichkeiten** (wer prüft, wer freigibt)- **Selbstbewertung** nach ISO/IEC 42001-Light (vereinfachte Umsetzung)

Erläuterung der Stufen im Unternehmenskontext

🟥 **Unzulässig – „Nicht betreiben, nicht verkaufen, nicht nutzen“**

- Diese Systeme sind **gesetzlich verboten**.
- Unternehmen müssen sicherstellen, dass **keine verbotene Funktion** Teil eines Produkts oder Services ist.
- Wenn ein Verstoß festgestellt wird, besteht **Meldepflicht** und **Sanktionsgefahr** (Bußgelder bis 35 Mio € oder 7 % Umsatz).

© A4Q Copyright 2025

🟧 **Hohes Risiko – „Zulässig, aber nur mit umfassender Kontrolle“**

- Hier liegt der **Kernbereich des EU AI Act**.
- Der gesamte Entwicklungs- und Einsatzprozess muss **nachweislich sicher, transparent und kontrollierbar** sein.
- Jedes Hochrisiko-System benötigt ein **technisches Dossier** und eine **CE-Kennzeichnung**, bevor es in Betrieb geht.
- In der Praxis betrifft das vor allem: Medizin, Bildung, HR, Kreditvergabe, Sicherheit, Justiz.

🟨 **Begrenztes Risiko – „Transparenzpflicht statt Auditpflicht“**

- Systeme dieser Kategorie dürfen **frei verwendet** werden, müssen aber **offenlegen**, dass KI beteiligt ist.
- Es geht hier nicht um Kontrolle des Algorithmus, sondern um **Schutz vor Täuschung**.
- Besonders relevant für Chatbots, Generative KI, Emotionserkennung oder Deepfakes.

🟩 **Minimales Risiko – „Gute Praxis statt Regulierung“**

- Diese Systeme liegen **unterhalb der Eingriffsschwelle** des AI Act.
- Der Gesetzgeber fördert hier **freiwillige Ethikstandards**, um Vertrauenswürdigkeit zu erhöhen.
- Auch wenn keine rechtliche Pflicht besteht, sind dokumentierte Selbstverpflichtungen ein wichtiges **Signal für Audit-Readiness**.

Beispielhafte Umsetzung in Unternehmen

Systemtyp	**Vermutete Risikostufe**	**Pflichten & Maßnahmen**
Bewerberauswahl-KI	Hochrisiko	CE-Kennzeichnung, Datenqualität, Oversight
Chatbot für Kundenservice	Begrenzt	Hinweis „Sie sprechen mit einer KI“, Logging
Lernunterstützende Erklär-KI	Begrenzt	Transparenzhinweis, Qualitätskontrolle

© A4Q Copyright 2025

Systemtyp	Vermutete Risikostufe	Pflichten & Maßnahmen
KI zur Gesichtserkennung im öffentlichen Raum	Unzulässig	Einsatzverbot, interne Meldung
Textzusammenfassungstool für Lehrende	Minimal	Freiwillige Governance, interne Prüfung

Fazit

Risikostufe bestimmt Pflichten.
Der AI Act will keine Technologie verbieten, sondern Verantwortlichkeit und Verhältnismäßigkeit sicherstellen.

Unternehmen müssen daher:

- für jedes KI-System eine **Risikostufe begründet dokumentieren**,
- die passenden **Pflichten aktiv umsetzen**,
- und bei jeder Zweckänderung **eine neue Bewertung durchführen**.

2.5 Risikodynamik und Re-Assessments

KI-Systeme können ihre Risikostufe im Lebenszyklus ändern (z. B. durch neue Funktionen oder Zweckänderung).
Unternehmen müssen daher Prozesse für regelmäßige **Re-Assessments** implementieren.

Auslöser	Mögliche Folge	Erforderliche Aktion
Funktionserweiterung → neue Entscheidungslogik	Begrenztes → Hochrisiko	Neue Konformitätsprüfung nach Art. 17–23
Einsatz in kritischem Bereich (z. B. Gesundheit)	Minimal → Hochrisiko	AI-Risk-Review und Behördenmeldung
Automatisierung ohne Human Oversight	Hoch → potenziell unzulässig	Systemstopp + Neubewertung

2.6 Risikobasierte Priorisierung von Maßnahmen

Die Risikostufe bestimmt nicht nur Pflichten, sondern auch die interne Priorität für Compliance-Aktivitäten.

© A4Q Copyright 2025

Prioritätsebene	Typische Felder	Empfohlene Maßnahmen
1 (Hochrisiko)	HR, Finanzwesen, Gesundheit, Justiz	Formales Risikomanagement, Audits, CE-Prozess
2 (Begrenzt)	Marketing, Kommunikation, Generative KI	Kennzeichnung, Transparenzberichte
3 (Minimal)	Interne Hilfssysteme, Prozessautomatisierung	Freiwillige Ethik-Checks, Awareness-Schulungen

→ Risikobasierte Priorisierung ermöglicht effizienten Einsatz begrenzter Compliance-Ressourcen.

© A4Q Copyright 2025

3 Globale & sektorale Regulierungslandschaft (Überblick)

⏱ Unterrichtszeit 70 Minuten

🎯 **Business Outcomes (BOs)**

- **BO 3.1:** Die Teilnehmenden entwickeln ein vertieftes Verständnis für internationale KI-Regulierungen und sind in der Lage, deren Anwendung auf globale Projekte kritisch zu reflektieren.
- **BO 3.2:** Die Teilnehmenden können Harmonisierungspotenziale zwischen EU- und Nicht-EU-Vorgaben erkennen und strategisch im Unternehmen nutzen.

Lernziele (Learning Objectives – LOs)

- **LO 3.1 (K2):** Teilnehmende können zentrale aktuelle KI-Regulierungsansätze (z. B. EU, USA, China, UK, Kanada, Brasilien, OECD, UN, Europarat) beschreiben und voneinander unterscheiden.
- **LO 3.2 (K3):** Teilnehmende können neuere Entwicklungen – wie etwa Chinas Kennzeichnungspflichten für KI-Inhalte ab 1. September 2025 – in die globale Governance-Landschaft einordnen und anhand eines Beispiels anwenden.
- **LO 3.3 (K3):** Teilnehmende können grundlegende Gemeinsamkeiten und Unterschiede zwischen dem EU AI Act und internationalen Rahmenwerken aufzeigen und erläutern.
- **LO 3.4 (K3):** Teilnehmende können zentrale Harmonisierungsmöglichkeiten in multinationalen Projekten identifizieren und praxisnahe Beispiele für Integrationsansätze darstellen.
- **LO 3.5 (K2):** Teilnehmende können sektorale Spezialregelungen (z. B. Gesundheit, Finanzen, Automotive, Verteidigung usw.) erläutern und deren Bezug zu KI-Regulierungen erklären.
- **LO 3.6 (K1):** Teilnehmende kennen die Bedeutung internationaler Kooperationen und Gremien (z. B. OECD, G7, UN, Council of Europe) für die Weiterentwicklung und Angleichung von KI-Regulierungen.

Wichtige Begriffe:

OECD AI Principles, UNESCO Recommendation on AI Ethics, NIST AI RMF, G7 Code of Conduct, Council of Europe CAI, AI Safety Summit, US Executive Order on AI, China Generative AI Regulation, AI Liability Directive, Data Act, Cyber Resilience Act (CRA), Digital Services Act (DSA), GDPR, DSFA.

Einleitung

© A4Q Copyright 2025

Dieses Kapitel bietet einen Überblick über die internationale und sektorale Regulierungslandschaft im Bereich Künstlicher Intelligenz. Es zeigt, wie verschiedene Regionen – darunter die Europäische Union, die USA, das Vereinigte Königreich, China und weitere Länder – unterschiedliche, aber zunehmend konvergierende Ansätze für den Umgang mit KI entwickeln. Die Teilnehmenden erkennen, wie globale Rahmenwerke, Leitlinien und Branchenstandards zur Harmonisierung von KI-Governance und Compliance beitragen.

3.1 Globale KI-Regulierung: Status und Trends

Europäische Union (EU)

Die EU-Verordnung über Künstliche Intelligenz (AI Act) gilt international als einer der umfassendsten und verbindlichsten Rechtsrahmen.
Mit der Umsetzung der **GPAI-Regeln** für Basismodelle im Jahr 2025 wurde der Druck auf große Anbieter generativer KI-Systeme erheblich erhöht.
Zentrale Elemente wie **Transparenzpflichten**, **Risikomanagement** und **CE-Konformität** setzen de facto globale Maßstäbe für Exporte und für den internationalen Wettbewerb.

China (Regelungsstand September 2025)

Bereits seit dem **15. August 2023** gelten die *Interim Measures for the Management of Generative AI Services*.
Diese verpflichten öffentliche Anbieter generativer KI-Dienste zur Einhaltung von Anforderungen an Inhaltsüberwachung, Datenqualität, Algorithmustransparenz und Beschwerdemechanismen.

Ab **1. September 2025** treten die neuen **Maßnahmen zur Kennzeichnung von KI-generierten Inhalten (Labeling Rules)** in Kraft.
Sie verpflichten Anbieter dazu, sowohl **sichtbare Labels** für Nutzerinnen und Nutzer als auch **unsichtbare Metadaten-Kennzeichnungen** in Text-, Bild-, Audio-, Video- und 3D-Inhalten anzubringen.
Digitale Plattformen (z. B. soziale Medien) müssen zudem KI-Inhalte automatisch erkennen, klassifizieren („bestätigt / möglich / verdächtig KI-generiert“) und gegebenenfalls nachkennzeichnen.

Ab **1. November 2025** definieren nationale technische Standards die Formate für Labels und Metadaten sowie Sicherheitsanforderungen für Datenannotation, Training und Fine-Tuning.
Parallel wurde der **Global AI Governance Action Plan 2025** veröffentlicht, mit dem China seinen Einfluss auf internationale Standardisierung und Normsetzung ausbauen möchte.

Implikationen für internationale Projekte:
Unternehmen, die Inhalte für den chinesischen Markt erzeugen oder verbreiten, müssen ab September 2025 die verpflichtende Kennzeichnung (Labels + Metadaten) umsetzen.
Diese Vorgaben sind technisch präzise festgelegt und erfordern Anpassungen bestehender Content-

© A4Q Copyright 2025

Pipelines.
Chinas regulatorischer Ansatz ist **modular** und reagiert rasch auf neue Technologien (z. B. Deep Synthesis, Empfehlungsalgorithmen).
Der globale Governance-Plan unterstreicht das Bestreben, die chinesischen Normen als internationale Referenz zu etablieren – sowohl als Beitrag zur Harmonisierung als auch als Instrument geopolitischer Einflussnahme.

Vereinigte Staaten von Amerika (USA)

In den USA existiert derzeit kein einheitliches Bundesgesetz zur Künstlichen Intelligenz.
Die Regulierung erfolgt sektoral und dezentral, insbesondere über:

- das **NIST AI Risk Management Framework (2023)** als freiwilligen Standard,
- verschiedene **Executive Orders** und politische Strategien (z. B. *AI Bill of Rights*),
- sowie über bundesstaatliche Initiativen (z. B. Kalifornien) zu Transparenz- und Accountability-Pflichten.

Der Fokus liegt auf **Selbstregulierung**, Verantwortlichkeit und **Risikomanagement durch Governance-Prozesse**.

Vereinigtes Königreich (UK)

Das Vereinigte Königreich verfolgt weiterhin einen **prinzipienbasierten, innovationsfreundlichen Ansatz** („pro-innovation approach“).
Statt eines eigenen KI-Gesetzes werden bestehende Regelwerke angepasst und durch Leitlinien ergänzt, die auf Transparenz, Fairness und Sicherheit abzielen.

Kanada

Der Entwurf zum **Artificial Intelligence and Data Act (AIDA)** enthält verbindliche Anforderungen an Risiko- und Folgenabschätzungen, Rechenschaftspflichten sowie Audits.
Der Gesetzesvorschlag orientiert sich stark am europäischen Modell und dürfte für internationale Anbieter mit Aktivitäten im kanadischen Markt besonders relevant werden.

Brasilien und Lateinamerika

Brasilien erarbeitet derzeit das Rahmengesetz **Marco Legal da Inteligência Artificial** (Entwurf 2024), das auf Risikobasierung, Transparenz und Ethik ausgerichtet ist.
Auch andere Staaten der Region orientieren sich zunehmend an der EU-Systematik.

© A4Q Copyright 2025

Internationale Organisationen und Soft Law

Die **OECD AI Principles (2019)**, die **UNESCO Ethics Recommendation (2021)** und der **Entwurf des Europarats für ein AI-Übereinkommen** bilden die Grundlage für einen internationalen Normdialog.
Diese *Soft-Law-Instrumente* fördern Angleichung und Kooperation in Ländern, die noch keine verbindliche KI-Gesetzgebung eingeführt haben.

3.2 Vergleich: EU AI Act ↔ Internationale Regelungen

Der folgende Vergleich zeigt, wie sich der EU AI Act von anderen internationalen Regulierungsrahmen unterscheidet und wo er mit ihnen übereinstimmt.
Er verdeutlicht unterschiedliche rechtliche Ansätze, Durchsetzungsmechanismen und Transparenzanforderungen und zeigt zugleich den globalen Trend zu einer risikobasierten Angleichung der Rechtsordnungen

Aspekt	**EU AI Act**	**China (Labeling ab Sept 2025)**	**USA / NIST Framework**	**Kanada (AIDA Entwurf)**	**UK / Prinzipienansatz**
Rechtsnatur	Verordnung – verbindlich und unmittelbar in der EU anwendbar	Verwaltungsvorschrift / technische Anordnung	Freiwilliges Rahmenwerk / Guidance	Gesetzesentwurf	Prinzipienbasierte Guidance
Risikobasierung	Vier Stufen: verboten – hoch – begrenzt – minimal	Gestufte Aufsicht ohne formale Risikoklassen	Prozessbasierte Risikobewertung	An EU-Modell angelehnt	Ohne formale Klassifizierung
Transparenz / Labeling	Verpflichtende Offenlegung und Kennzeichnung (Art. 52 ff.)	Ab 1. 9. 2025: sichtbare und unsichtbare Labels für alle KI-Inhalte	Empfehlungen zur Transparenz	Berichtspflichten geplant	Transparenz empfohlen, nicht verpflichtend

© A4Q Copyright 2025

Aspekt	EU AI Act	China (Labeling ab Sept 2025)	USA / NIST Framework	Kanada (AIDA Entwurf)	UK / Prinzipienansatz
Audit / Konformität	Externe Bewertung und CE-Kennzeichnung	Algorithmus-Filing und Sicherheitsprüfungen	Self-Assessment oder Third-Party-Review	Externe Reviews vorgesehen	Accountability optional
Sanktionen	Bußgelder bis 30 Mio € oder 6 % Umsatz	Lizenzentzug, Bußgelder, Blacklisting	Keine zentralen Sanktionen	Geplante Bußgelder	Geringe Verbindlichkeit

Bemerkung:
Chinas Labeling-Regelung (September 2025) ergänzt die bestehenden Vorschriften zur Generativen KI und legt erstmals präzise technische Kennzeichnungspflichten fest.
Viele nicht-europäische Regime (Kanada, Brasilien usw.) lehnen sich an die EU-Logik an, was die internationale Harmonisierung begünstigt, sofern regionale Sicherheits- und Datenanforderungen berücksichtigt werden.

3.3 Sektorale KI-Regulierung und Schnittstellen

Die Regulierung von Künstlicher Intelligenz überschneidet sich zunehmend mit sektorspezifischen Regelwerken, die zusätzliche Anforderungen an Sicherheit, Rechenschaftspflicht und Ethik stellen.
Die folgende Übersicht fasst zentrale Sektoren mit KI-bezogenen Vorschriften oder Standards zusammen und zeigt, wie diese mit den allgemeinen Governance-Pflichten des AI Act verknüpft sind.

Sektor	Relevante Regelungen	Zentrale KI-Anforderungen
Gesundheitswesen / MedTech	EU MDR / IVDR, FDA AI/ML Guidance (USA)	Sicherheit, Validierung von Trainingsdaten, Bias-Kontrolle, klinische Nachweise
Finanzwesen / Versicherungen	Basel Committee, EBA Guidelines, SEC / FINRA (USA)	Algorithmische Fairness, Auditability, Risikomanagement
Automotive / Mobilität	UNECE WP.29, ISO 26262, ISO 21448 (SOTIF)	Safety-by-Design, Echtzeit-Monitoring, Redundanz

© A4Q Copyright 2025

Sektor	Relevante Regelungen	Zentrale KI-Anforderungen
Verteidigung / Sicherheit	UN CCW, EU Dual-Use-Verordnung 2021/821	Abgrenzung zivil / militärisch, Exportkontrolle
Bildung / EdTech	UNESCO AI in Education (2023)	Schutz von Minderjährigen, Datenethik, Transparenz

3.4 Harmonisierung und Strategien für globale KI-Projekte

Um eine wirksame und konsistente Umsetzung internationaler KI-Compliance sicherzustellen, können Unternehmen mit globaler Ausrichtung folgende strategische und organisatorische Ansätze verfolgen:

(1) „Baseline + lokale Ergänzung“

- Aufbau eines zentralen **AI Compliance Frameworks** auf Basis des EU AI Act und ISO/IEC 42001.
- Ergänzung durch länderspezifische Module (z. B. chinesische Labeling-Vorgaben, US-Guidelines, kanadische AIDA-Pflichten).
- Nutzung modularer Policies und regionalspezifischer Compliance-Profile.

(2) Standards und „Presumption of Conformity“

- Frühzeitige Ausrichtung auf ISO/IEC 42001, ISO/IEC 23894, ISO/IEC 27001 sowie IEEE-Richtlinien.
- Einheitliche Standards erleichtern den Nachweis von Konformität auch außerhalb der EU.

(3) „Regulation Tracking & Gap Mapping“

- Fortlaufende Beobachtung internationaler Regulierungsentwicklungen (China, USA, Lateinamerika u. a.).
- Erstellung von Cross-Reference-Mappings (z. B. EU-Kennzeichnung ↔ chinesisches Labeling).
- Durchführung regelmäßiger Gap-Analysen und Ableitung von Prioritäten und Roadmaps.

(4) Globale Governance-Strukturen

- Einrichtung eines übergreifenden **AI Governance Boards** mit regionalen Compliance-Vertretungen.
- Etablierung von klaren Eskalations- und Berichtswegen.

(5) Content-Pipeline-Architektur und Modularität

- Aufbau von Content-Pipelines, die automatisches Labeling und regionale Prüfungen integrieren.
- Dynamische Umschaltung auf länderspezifische Policies (z. B. bei Veröffentlichungen in China).

© A4Q Copyright 2025

- Sicherstellung von Versionierung, Logging und Revisionsfähigkeit.

Beispiel:
Ein Unternehmen betreibt eine globale Content-Plattform (EU, China, Nordamerika).
Der zentrale Betrieb orientiert sich am EU AI Act und an ISO/IEC 42001.
Für den chinesischen Markt werden zusätzlich automatische Labels (sichtbar + Metadaten) gemäß den Pflichten ab 1. September 2025 integriert.
Das AI Governance Board überwacht laufend neue Anforderungen und priorisiert die Anpassung technischer und organisatorischer Prozesse.

3.5 Zusammenfassung und Kernbotschaften

- Die internationale KI-Regulierung befindet sich in dynamischer Entwicklung. China führt im September 2025 neue verbindliche Kennzeichnungspflichten ein, die technisch präzise umgesetzt werden müssen.
- Der EU AI Act stellt den derzeit strengsten rechtlichen Rahmen dar und prägt weltweit die Regulierungslogik.
- Soft-Law-Instrumente (OECD, UNESCO) tragen zur Annäherung zwischen Regimen bei.
- Unternehmen sollten ein modulares Compliance-System entwickeln, das lokale Besonderheiten abbildet und zugleich eine globale Governance ermöglicht.
- Langfristiges Ziel ist die Nutzung von Harmonisierungspotenzialen durch Standard-Alignment, Labeling-Schnittstellen und frühzeitiges Erkennen regulatorischer Konflikte.

© A4Q Copyright 2025

4 Verbotene KI-Praktiken (Art. 5 EU AI Act)

⏱ Unterrichtszeit: 50 Minuten

🎯 Business Outcomes:

BO 4.1 Teilnehmende entwickeln Sensibilität für unzulässige KI-Praktiken und sind befähigt, diese im eigenen Umfeld zu identifizieren.
BO 4.2 Teilnehmende sind vorbereitet, Ausnahmen nach Art. 5 zu bewerten und umzusetzen.

Lernziele (Learning Objectives)

- **LO 4.1 (K1):** Teilnehmende kennen die vier zentralen Verbotskategorien gemäß Art. 5 EU AI Act und deren grundlegende Abgrenzung.
- **LO 4.2 (K2):** Teilnehmende können erklären, warum bestimmte KI-Praktiken als unzulässig gelten und welche Grundrechte sie verletzen.
- **LO 4.3 (K3):** Teilnehmende können Beispiele unzulässiger KI-Anwendungen im eigenen Unternehmens- oder Behördenkontext identifizieren und deren Rechtsfolgen einschätzen.
- **LO 4.4 (K2):** Teilnehmende können die Voraussetzungen und Grenzen der in Art. 5 Abs. 2 bis 3 geregelten Ausnahmen erläutern.
- **LO 4.5 (K1):** Teilnehmende kennen die rechtlichen Konsequenzen und möglichen Sanktionsarten bei Verstößen gegen Art. 5 EU AI Act und verstehen deren Bedeutung für die Compliance-Praxis.

Wichtige Begriffe:
Subliminale Manipulation, Verhaltenssteuerung, Social Scoring, Biometrische Kategorisierung, Echtzeit-Biometrie, Grundrechte, Menschenwürde, Sicherheitsinteresse, Ausnahmeregelung (Art. 5 Abs. 2–3), Marktverbot, Rechtsfolgen.

Einführung

Der EU AI Act stellt mit Artikel 5 eine „rote Linie“ auf: bestimmte Arten von KI-Anwendungen sind aus Gründen des Grundrechtsschutzes unzulässig. Diese Verbote gelten unabhängig davon, ob die Systeme technisch leistungsfähig oder wirtschaftlich attraktiv sind. Sie dienen dem Schutz der Menschenwürde, der freien Meinungsbildung und der Autonomie des Einzelnen.

© A4Q Copyright 2025

4.1 Überblick über die verbotenen Praktiken

Gemäß Artikel 5 Absatz 1 sind folgende KI-Praktiken verboten:

Nr.	Verbotene Praxis	Beschreibung / Beispiel	Schutzgut
1	**Subliminale Manipulation**	Systeme, die unterhalb der bewussten Wahrnehmung das Verhalten von Personen steuern (z. B. Nudging über unbemerkte Reizmuster).	Autonomie, freie Willensbildung
2	**Ausnutzung vulnerabler Personengruppen**	KI-Systeme, die Kinder, Ältere oder Menschen mit Behinderung gezielt beeinflussen (z. B. Spielzeug, das emotionale Bindungen ausnutzt).	Schutz besonders gefährdeter Gruppen
3	**Soziales Scoring durch staatliche Stellen**	Bewertung des Verhaltens oder der Persönlichkeit von Bürger:innen über mehrere Kontexte hinweg (z. B. Bonussysteme für „erwünschtes“ Verhalten).	Gleichbehandlung, Menschenwürde
4	**Echtzeit-biometrische Identifizierung im öffentlichen Raum**	Gesichtserkennung oder andere Biometrie-Systeme zur Überwachung (z. B. Crowd-Scanning auf öffentlichen Plätzen).	Privatsphäre, Bewegungsfreiheit

Diese Anwendungen sind grundsätzlich verboten – sie dürfen weder entwickelt, verkauft, noch eingesetzt werden.

4.2 Rechts- und Grundrechtsbegründung

Die Verbote beruhen auf der Europäischen Grundrechtecharta, insbesondere auf:

- Art. 1 Menschenwürde,
- Art. 7 Achtung des Privat- und Familienlebens,
- Art. 8 Schutz personenbezogener Daten,
- Art. 21 Nichtdiskriminierung.

Die Kommission betont, dass der AI Act nicht nur technische, sondern auch ethische Grenzen setzt – etwa gegen Überwachung, Manipulation und sozialen Druck durch automatisierte Bewertungssysteme.

© A4Q Copyright 2025

4.3 Ausnahmen nach Art. 5 Abs. 2–3

Unter strengen Voraussetzungen kann die Echtzeit-biometrische Identifizierung in öffentlichen Räumen zulässig sein, wenn sie:

- **gesetzlich vorgesehen** ist,
- **einem eng umgrenzten Zweck** dient (z. B. Aufklärung schwerer Straftaten, Terrorismusbekämpfung, Suche nach Vermissten),
- **von einer zuständigen Behörde** unter **richterlicher Genehmigung** durchgeführt wird,
- und **zeitlich und räumlich begrenzt** ist.

Die Beweislast für die Notwendigkeit und Verhältnismäßigkeit liegt bei der zuständigen Behörde. Unternehmen dürfen solche Systeme nicht eigenständig einsetzen, sondern nur auf behördliche Anordnung hin unter Beachtung nationaler Durchführungsgesetze.

4.4 Praktische Sensibilisierung

Zur Stärkung der Compliance-Kultur sollten Organisationen:

1. **KI-Register** führen, in dem alle aktiven und geplanten KI-Anwendungen aufgelistet sind.
2. **Prüf-Checklisten** verwenden, um zu erkennen, ob eine Anwendung potenziell in eine Verbotskategorie fällt.
3. **Ethik- und Rechtsprüfungen** vor Projektstart durchführen.
4. **Sensibilisierungstrainings** für Entwickelnde, Produktmanager:innen und Marketingteams anbieten, damit Manipulations- und Scoring-Mechanismen erkannt werden.

4.5 Praktische Beispiele

Praktische Beispiele, die die verbotenen KI-Praktiken verdeutlichen

Die folgenden Beispiele zeigen typische Anwendungsszenarien, in denen KI-Systeme gegen die in Artikel 5 EU AI Act festgelegten Verbote verstoßen würden.
Sie dienen der Sensibilisierung für potenziell unzulässige Praktiken und sollen verdeutlichen, wie technische Innovation mit rechtlichen und ethischen Grenzen in Einklang gebracht werden muss.

1 Subliminale Manipulation (unterbewusste Beeinflussung)

Beispiel 1: Emotionsbasierte Werbeanpassung

Eine Online-Werbeplattform nutzt KI, um über die Webcam Mikroausdrücke und Herzfrequenzmuster von

© A4Q Copyright 2025

Nutzer:innen zu analysieren und daraufhin Farben, Klänge oder Texte in Echtzeit anzupassen – ohne deren Wissen.
→ Dies stellt eine Form der subliminalen Beeinflussung dar, da emotionale Zustände unterhalb der bewussten Wahrnehmung manipuliert werden.

Beispiel 2: Neuro-Feedback-Spielsystem
Ein Virtual-Reality-Spiel erfasst Gehirnaktivitätsmuster und passt Schwierigkeitsgrad und Belohnungen so an, dass Spielzeiten maximiert werden – ohne ausdrückliche Zustimmung der Nutzenden.
→ Das System verändert Verhalten verdeckt durch Konditionierung und verletzt damit Autonomie und freie Willensbildung.

2 Ausnutzung vulnerabler Personengruppen

Beispiel 1: KI-gestütztes Spielzeug für Kinder
Eine interaktive Puppe mit generativer KI baut emotionale Bindungen auf und ermutigt Kinder, Käufe zu tätigen oder persönliche Daten zu teilen.
→ Das Vertrauen von Minderjährigen wird gezielt ausgenutzt – ein klarer Verstoß gegen den Schutz von Kindern und ethische Marketinggrundsätze.

Beispiel 2: Pflegeassistenz-System für ältere Personen
Ein KI-System in einem Pflegeheim nutzt manipulative Sprachmuster, um Bewohner:innen zum Einnehmen von Medikamenten oder zur Abgabe positiver Bewertungen zu bewegen.
→ Es missbraucht kognitive oder emotionale Verletzlichkeit und untergräbt informierte Zustimmung und Würde.

3 Soziales Scoring durch staatliche Stellen

Beispiel 1: Bürgerbewertungssystem
Eine Kommune vergibt auf Basis von Zahlungsdaten, Social-Media-Aktivitäten und Polizeiinformationen einen „Zuverlässigkeitsscore“, der über den Zugang zu Dienstleistungen entscheidet.
→ Diese kontextübergreifende Bewertung diskriminiert und verletzt Gleichbehandlung und Menschenwürde.

Beispiel 2: Rangordnung bei Sozialleistungen
Ein KI-System kombiniert Beschäftigungs-, Steuer- und Gesundheitsdaten, um Antragstellende nach „Leistungswürdigkeit“ zu sortieren.
→ Dies führt zu systematischer Benachteiligung und Stigmatisierung – ein klarer Verstoß gegen das Verbot automatisierter sozialer Klassifizierung.

4 Echtzeit-biometrische Identifizierung im öffentlichen Raum

© A4Q Copyright 2025

Beispiel 1: Personen-Scanning an Bahnhöfen
Eine Polizeibehörde setzt Gesichtserkennungskameras in Bahnhöfen ein, um Personen auf Fahndungslisten in Echtzeit zu identifizieren.
→ Diese Form der Dauerüberwachung verletzt Privatsphäre und Bewegungsfreiheit, sofern keine gesetzliche Ausnahme vorliegt.

Beispiel 2: Emotionserkennung bei Großveranstaltungen
Kameras auf einem Konzert analysieren mithilfe von KI Gesichtsausdrücke des Publikums, um „aufgeregte" Personen für den Sicherheitsdienst zu markieren.
→ Dies ist eine unzulässige Form biometrischer Profilbildung und Verhaltensüberwachung ohne rechtliche Grundlage.

Ausnahmen zu den verbotenen KI-Praktiken nach Artikel 5 EU AI Act

Die in Artikel 5 EU AI Act definierten Verbote gelten grundsätzlich absolut.
In eng begrenzten Ausnahmefällen können bestimmte Anwendungen jedoch **zulässig** sein, sofern sie **gesetzlich vorgesehen**, **verhältnismäßig**, **notwendig** und unter **menschlicher Kontrolle** durchgeführt werden.
Nachfolgend finden sich für jede der vier Verbotskategorien exemplarische Ausnahmefälle, die die Grundidee der Verhältnismäßigkeit und Zweckbindung verdeutlichen.

1 Subliminale Manipulation – Ausnahme

Beispiel: *Gesundheitskampagne mit milden Aufmerksamkeitsreizen*
Eine öffentliche Gesundheitsbehörde nutzt ein KI-gestütztes Informationsdisplay, das Hintergrundfarbe oder Musik leicht verändert, um Passant:innen auf Impf- oder Aufklärungshinweise aufmerksam zu machen.
→ Solange die Maßnahme keine unbewusste Verhaltenssteuerung bewirkt oder persönliche Schwächen ausnutzt und der Zweck eindeutig **im öffentlichen Interesse** liegt, handelt es sich **nicht um unzulässige subliminale Manipulation** im Sinne des Artikel 5.

2 Ausnutzung vulnerabler Gruppen – Ausnahme

Beispiel: *Assistive KI-Technologie für Kinder oder ältere Menschen*
Ein KI-basierter Lese- oder Sprachassistent passt Wortwahl und Tonfall an, um Kindern oder Senior:innen das Verständnis von Formularen oder behördlichen Informationen zu erleichtern.
→ Das System dient der **Unterstützung und Inklusion**, nicht der Beeinflussung. Wird es ausschließlich zur Förderung von **Barrierefreiheit und Selbstbestimmung** eingesetzt, ist der Einsatz **rechtlich zulässig**.

© A4Q Copyright 2025

3 Soziales Scoring durch staatliche Stellen – Ausnahme

Beispiel: *Risikobewertung im Rahmen von Betrugs- oder Compliance-Prüfungen*
Eine Steuer- oder Sozialbehörde verwendet KI, um auffällige Muster in Steuererklärungen oder Leistungsanträgen zu erkennen.
→ Die Analyse erfolgt **nur innerhalb eines klar abgegrenzten Verwaltungszwecks**, unterliegt **menschlicher Prüfung** und rechtlichen **Kontrollmechanismen**.
→ Solche Systeme sind **zulässig**, solange **keine moralische oder verhaltensbezogene Gesamtbewertung von Personen** erfolgt und die Maßnahme auf **rechtlicher Grundlage** beruht.

4 Echtzeit-biometrische Identifizierung im öffentlichen Raum – Ausnahme (Art. 5 Abs. 2–3)

Beispiel: *Fahndung nach einem vermissten Kind mit richterlicher Genehmigung*
Eine Polizeibehörde setzt eine Echtzeit-Gesichtserkennung an einem Bahnhof ein, um ein vermisstes Kind zu finden.
→ Der Einsatz ist **gesetzlich geregelt**, **richterlich genehmigt**, **zeitlich und örtlich begrenzt** sowie **verhältnismäßig zum Zweck**.
→ Damit handelt es sich um eine der ausdrücklich **zugelassenen Ausnahmen nach Artikel 5 EU AI Act**.

Fazit

Die in Artikel 5 EU AI Act festgelegten Verbote markieren die **rote Linie des europäischen KI-Rechtsrahmens**.
Zulässig sind nur eng definierte Ausnahmen, bei denen:

- ein **legitimes öffentliches Interesse** besteht,
- die Maßnahme **notwendig, verhältnismäßig und rechtlich legitimiert** ist, und
- **menschliche Aufsicht** sowie **transparente Rechenschaftspflicht** gewährleistet sind.

Diese Ausnahmen sind daher keine Schlupflöcher, sondern Ausdruck eines **balancierten Ansatzes zwischen Grundrechtsschutz und öffentlicher Sicherheit**.

4.6 Zusammenfassung

Kapitel 4 beschreibt die im **Artikel 5 Absatz 1 EU AI Act** ausdrücklich **verbotenen KI-Praktiken**, die unabhängig von technischer Leistungsfähigkeit oder wirtschaftlichem Nutzen untersagt sind. Dazu gehören:
(1) *subliminale Manipulation* (Art. 5 Abs. 1 a),

© A4Q Copyright 2025

(2) *Ausnutzung vulnerabler Gruppen* (Art. 5 Abs. 1 b),
(3) *soziales Scoring durch staatliche Stellen* (Art. 5 Abs. 1 c) sowie
(4) *Echtzeit-biometrische Identifizierung im öffentlichen Raum* (Art. 5 Abs. 1 d).
Diese Systeme dürfen in der EU **weder entwickelt noch in Verkehr gebracht oder betrieben** werden. **Ausnahmen** nach *Art. 5 Abs. 2–3* gelten ausschließlich für eng begrenzte Zwecke der Strafverfolgung (z. B. Suche nach Vermissten, Terrorismusprävention) und nur, wenn der Einsatz **gesetzlich vorgesehen, verhältnismäßig, zeitlich begrenzt** und **richterlich genehmigt** ist.

© A4Q Copyright 2025

5 Hochrisiko-Systeme und Pflichten (Art. 6–51 EU AI Act)

⏱ Unterrichtszeit: 120 Minuten

🎯 **Business Outcomes:**

BO 5.1 Teilnehmende erwerben die Fähigkeit, die relevanten Pflichten für Hochrisiko-KI-Systeme zu erkennen, ihre praktische Umsetzung im Unternehmen zu unterstützen und zur Einhaltung der gesetzlichen Anforderungen beizutragen.
BO 5.2 Teilnehmende sind sensibilisiert, prüfungsfähige Dokumentationen und Nachweise zu erstellen, um die Audit-Sicherheit zu erhöhen.

Lernziele (Learning Objectives – LO)

- **LO 5.1 (K1):** Teilnehmende kennen die grundlegende Einteilung von KI-Systemen als Hochrisiko nach Art. 6–7 EU AI Act und verstehen, welche Arten von Anwendungen darunterfallen.
- **LO 5.2 (K2):** Teilnehmende können die zentralen Pflichten für Hochrisiko-Systeme gemäß Art. 6–51 EU AI Act beschreiben.
- **LO 5.3 (K3):** Teilnehmende können ein betriebliches Vorgehen zur Umsetzung der Pflichten (Risikomanagement, Datenqualität, Human Oversight, Dokumentation) entwerfen.
- **LO 5.4 (K3):** Teilnehmende können prüfungsfähige Nachweise und Audit-Dokumentationen für Hochrisiko-Systeme erstellen oder bewerten.
- **LO 5.5 (K1):** Teilnehmende kennen die wichtigsten Artikel des Hochrisiko-Abschnitts (Art. 9 bis 15) und deren grundlegenden Zweck.

Wichtige Begriffe:
Hochrisiko-KI, Artikel 6–51 AI Act, Annex III Kategorien, Konformitätsbewertung, CE-Kennzeichnung, Risikomanagementsystem, Human Oversight, Dokumentationspflicht, Datenqualität, Technische Robustheit, Bias-Kontrolle, Audit-Trail, Lifecycle, AI Quality Management System.

Einleitung

Hochrisiko-Systeme bilden den Kernbereich des EU AI Act. Sie sind nicht verboten, aber nur unter strengen Auflagen zulässig. Die Artikel 6 bis 51 definieren ein kohärentes Pflichten-Set, das technische, organisatorische und dokumentarische Anforderungen verbindet. Ziel ist es, den Schutz von Grundrechten, Sicherheit und Fairness zu gewährleisten, ohne Innovation zu verhindern.

© A4Q Copyright 2025

Dieses Kapitel vermittelt praxisorientiert, wie Unternehmen die rechtlichen Anforderungen umsetzen, Dokumentations- und Nachweispflichten erfüllen und Audit-Readiness herstellen können.

5.1 Identifikation von Hochrisiko-Systemen

Ein KI-System gilt gemäß Artikel 6 in Verbindung mit Anhang III EU AI Act als *Hochrisiko-System*, wenn es in einem der dort genannten sensiblen Bereiche eingesetzt wird oder Bestandteil eines sicherheitsrelevanten Produkts ist, das bereits einer EU-Konformitätsbewertung unterliegt (z. B. Medizinprodukte, Aufzüge, Maschinen, Fahrzeuge).

Bereich	**Typisches Beispiel**	**Rechtsgrundlage / Referenz**
Personalwesen (HR)	Automatisierte Bewerberauswahl, Performance-Bewertung	Art. 6 i.V.m. Anhang III Nr. 4
Kredit- und Finanzwesen	Scoring- oder Bonitätsbewertungssysteme	Anhang III Nr. 5
Bildung & Ausbildung	Automatisierte Prüfungsbewertung, Zulassungssysteme	Anhang III Nr. 3
Gesundheitswesen	Diagnostische Entscheidungsunterstützung, Priorisierung	Anhang III Nr. 2
Strafjustiz & Sicherheit	Risiko- oder Rückfallprognosen, Beweisanalyse	Anhang III Nr. 6
Öffentliche Verwaltung	Automatisierte Leistungsbewertung, Sozialhilfebescheide	Anhang III Nr. 7

Kriterien (Art. 6 EU AI Act)

Ein System wird als Hochrisiko eingestuft, wenn:

1. es **wahrscheinlich wesentliche Auswirkungen auf Grundrechte** oder Sicherheit von Personen hat,
2. es **Entscheidungen oder Empfehlungen** in einem regulierten Bereich trifft,
3. es **automatisiert oder teilautomatisiert** arbeitet, und
4. es **nicht durch menschliche Kontrolle oder Transparenzmaßnahmen ausreichend kompensiert** werden kann.

© A4Q Copyright 2025

Praxis-Check für Unternehmen

Frage 1: Führt das System zu Entscheidungen mit *rechtlichen oder wirtschaftlichen Folgen* für Personen (z. B. Ablehnung, Zugang, Tarif)?
Frage 2: Wird das System in einem der in Anhang III genannten Sektoren eingesetzt?
Frage 3: Kann das System ohne menschliche Überprüfung Ergebnisse erzeugen oder Handlungen auslösen?
Frage 4: Besteht ein bestehender regulatorischer Rahmen (z. B. Medizinprodukt, Fahrzeug, Arbeitsrecht)?

Wenn mindestens eine dieser Fragen **mit „Ja“** beantwortet wird, ist eine Hochrisiko-Einstufung sehr wahrscheinlich und es kann ein formelles **Konformitätsbewertungsverfahren** nach Art. 16 ff. EU AI Act erforderlich sein.

Empfohlene Unternehmenspraxis

- Führen Sie ein **zentrales KI-Register** mit Zweck, Risiko-Einstufung und verantwortlicher Person.
- Verwenden Sie ein standardisiertes **Screening-Formular zur Risikoidentifikation** (z. B. basierend auf ISO/IEC 42001).
- Dokumentieren Sie **Begründung, Referenzen und Entscheidung zur Einstufung** im Audit-Dossier.
- Bei Unsicherheit: **Rücksprache mit Compliance- oder Rechtsabteilung** bzw. nationaler Aufsichtsbehörde.

5.2 Zentrale Pflichten für Hochrisiko-Systeme

Die Artikel 9 bis 24 des EU AI Act bilden das Pflichtenfundament für Hochrisiko-KI-Systeme. Sie regeln, wie Anbieter und Betreiber sicherstellen müssen, dass ihre Systeme über den gesamten Lebenszyklus hinweg verlässlich, nachvollziehbar und menschenkontrollierbar bleiben.

Die Anforderungen umfassen technische, organisatorische und dokumentarische Maßnahmen – von der Datenqualität über das Risikomanagement bis zur Nachmarktüberwachung.

Für Unternehmen bedeutet dies: Jedes Hochrisiko-System muss durch ein integriertes Compliance-Framework abgedeckt sein, das Prozesse, Verantwortlichkeiten und Nachweise eindeutig beschreibt.

Die folgende Übersicht zeigt die zentralen Pflichten, ihre rechtliche Grundlage sowie typische Umsetzungs- und Auditmaßnahmen in der Praxis.

© A4Q Copyright 2025

Themenbereich	Artikel(e)	Ziel	Praktische Umsetzung / Auditnachweis
Risikomanagementsystem	Art. 9	Systematische Erfassung, Bewertung und Minderung von Risiken über den gesamten Lebenszyklus	Einrichtung eines **AI-Risk-Registers**, Definition von Bewertungsmethoden, regelmäßige Neubewertung bei Änderungen
Datenqualität & Governance	Art. 10	Sicherstellung qualitativ hochwertiger, fairer und repräsentativer Trainings-, Validierungs- und Testdaten	Dokumentation der Datenquellen, **Bias-Analysen**, Fairness-Metriken, Freigabeprotokolle durch Data-Stewards
Technische Dokumentation	Art. 11	Vollständige Nachvollziehbarkeit und Rechenschaft gegenüber Aufsichtsbehörden	Erstellung eines **Technischen Dossiers** (Systembeschreibung, Modelle, Daten, Risiken, Testergebnisse), Versionierung und Archivierung
Logging & Audit-Trail	Art. 12	Nachvollziehbarkeit und Beweisführung jeder Systementscheidung	Implementierung **revisionssicherer Logs** mit Zeitstempel, Input/Output, User-ID; Hash- oder WORM-Speicherung
Transparenz & Nutzerinformation	Art. 13	Verständliche Information über Zweck, Funktion, Grenzen und Risiken	Standardisierte **Nutzerhinweise**, Erklärung der Entscheidungslogik („Explainability Layer“), interne Leitfäden
Human Oversight (menschliche Aufsicht)	Art. 14	Sicherstellung menschlicher Kontrolle und Eingreifbarkeit	Rollen- und Freigabekonzepte, **„Human-in-the-Loop“-Mechanismen**, Schulung und Nachweis der Eingriffsrechte
Robustheit, Genauigkeit & Cybersicherheit	Art. 15	Verlässlicher Betrieb auch unter Störungen oder Angriffen	Durchführung von **Stresstests**, Adversarial-Tests, Schwachstellenanalysen,

© A4Q Copyright 2025

Themenbereich	Artikel(e)	Ziel	Praktische Umsetzung / Auditnachweis
			definierte Backup- und Recovery-Prozesse
Konformitätsbewertung & CE-Kennzeichnung	Art. 16–23	Nachweis der Regelkonformität vor Inverkehrbringen	Interne oder externe Bewertung, Erstellung der **Konformitätserklärung**, CE-Kennzeichnung, Eintrag in EU-KI-Datenbank
Post-Market Monitoring & Incident-Reporting	Art. 24 ff.	Überwachung, Meldepflicht und kontinuierliche Verbesserung nach Markteintritt	Monitoring-Plan, Incident-Response-Prozess, Auditberichte, Feedback-Loop zu Risikomanagement
Änderungsmanagement & Re-Validierung	Art. 43 Abs. 2, Art. 61	Sicherstellung, dass wesentliche Änderungen erneut bewertet werden	**Change-Control-Prozess**, Dokumentation von Modell-Updates, erneute Risikoanalyse bei Trainings- oder Zieländerungen
Dokumentationspflicht & Audit-Readiness	Art. 11, 61	Nachweis aller Pflichten in prüfbarer Form	Einheitliches **Audit-Repository**, Checklisten, Schulungs- und Prüfprotokolle, Nachweiskette „von Daten bis Entscheidung“

5.3 Umsetzung im Unternehmen

Die praktische Umsetzung der Hochrisiko-Pflichten erfordert ein **koordiniertes Vorgehen zwischen Fachabteilungen, Compliance-Funktion und technischer Entwicklung**. Ziel ist ein nachweisbarer Prozess, der Risiken erkennt, Entscheidungen nachvollziehbar macht und Audit-Readiness sicherstellt.

1 Risikomanagement (Art. 9 EU AI Act)

- Einrichtung eines **AI-Risk-Registers** mit eindeutiger System-ID, Zweckbestimmung und Verantwortlicher Person („Owner per Use Case“)
- Bewertung aller Risiken nach **Eintrittswahrscheinlichkeit × Schweregrad** unter Einbeziehung von Bias, Fehlentscheidungen und Missbrauchsszenarien

© A4Q Copyright 2025

- Definition von **Schwellenwerten und Eskalationspfaden** (z. B. „kritisch > 0,6“)
- Periodische **Re-Evaluierung** nach Modell-Updates, Datenänderungen oder neuen Einsatzkontexten
- Dokumentation der Ergebnisse im **Risikobericht** als Bestandteil der technischen Dokumentation

2 Dokumentation (Art. 11 und 17 EU AI Act)

- Pflichtinhalte: **Zweck, Funktionsweise, Modellbeschreibung, Datenbasis, Test- und Validierungsprotokolle, Einschränkungen, bekannte Risiken**
- **Versionierung:** Jede Änderung von Modell, Daten, Zielgruppe oder Entscheidungslogik muss mit Zeitstempel und Verantwortlichen dokumentiert werden
- **Freigabeverfahren** vor Inverkehrbringen oder Deployment (z. B. „four-eyes principle“)
- **Audit-Hinweis:** Fehlende oder veraltete Dokumentation gilt als Compliance-Mangel und kann zum Entzug der CE-Kennzeichnung führen
- Integration in ein **zentrales Audit-Repository** (z. B. nach ISO/IEC 42001 oder 23894)

3 Human Oversight (Art. 14 EU AI Act)

- Einbindung qualifizierter Personen **vor oder nach automatisierten Entscheidungen**, abhängig vom Risiko
- Implementierung technischer Kontrollmechanismen:
  - **Freigabe-, Prüf- oder Stop-Funktion** („Human-in-the-Loop“ / „Human-on-the-Loop“)
  - Visualisierung von **Unsicherheiten (Confidence Scores)**
- Nachweis der Wirksamkeit durch:
  - **Schulungsnachweise** (Art. 4(4))
  - **Protokolle menschlicher Eingriffe**
  - regelmäßige **Wirksamkeitsprüfungen** im Monitoring-Prozess

4 Technische und organisatorische Maßnahmen (Art. 12–15 EU AI Act)

- Implementierung manipulationssicherer **Logging-Systeme** mit Hash- oder WORM-Funktion
- Durchführung regelmäßiger **Security-Tests** (Penetration-Tests, Model-Drift-Analysen, Adversarial Tests)
- **Redundanz- und Fallback-Strategien** für fehlerhafte oder unsichere Ergebnisse

© A4Q Copyright 2025

- Etablierung eines **Lebenszyklus-Managements** mit festgelegten Re-Validierungsintervallen (z. B. alle 6–12 Monate)
- **Rollenbasierte Zugriffskontrolle** und Schnittstelle zu IT-Sicherheits- und Datenschutz-Managementsystemen (ISMS / PIMS)
- Ergebnisdokumentation im **Post-Market-Monitoring-Report** (Art. 24 AI Act)

Kurzfazit:
Diese vier Umsetzungsdimensionen, **Risiko, Dokumentation, Aufsicht und technische Maßnahmen**, bilden zusammen das operative Rückgrat des AI-Compliance-Systems. Unternehmen, die diese Bereiche systematisch integrieren, gewährleisten die Einhaltung der gesetzlichen Anforderungen und erhöhen die Audit-Sicherheit

5.4 Dokumentations- und Nachweispflichten (Audit Readiness)

Eine lückenlose und nachvollziehbare Dokumentation ist das zentrale Element der Compliance bei Hochrisiko-KI-Systemen.
Sie dient als Nachweis gegenüber Aufsichtsbehörden, internen Revisionen und externen Auditor:innen, dass das System die Anforderungen des EU AI Act erfüllt und kontinuierlich überwacht wird.

Leitgedanke:

Alles, was nicht dokumentiert ist, gilt als nicht erfolgt.

Dokumentation bedeutet daher nicht bloß Archivierung, sondern einen aktiven Rechenschaftsprozess, der den gesamten Lebenszyklus des KI-Systems abbildet – von Entwicklung über Betrieb bis zur Außerbetriebnahme.

1 Typische Nachweise und Zuständigkeiten

Nachweisart	**Inhalt / Zweck**	**Verantwortlich**
Technische Dokumentation	Beschreibung von Modell, Zweck, Funktionsweise, Trainings- und Testdaten, Validierung, Limitationen	Anbieter / Entwicklungsverantwortliche
Risk Assessment	Identifizierte Risiken, Gegenmaßnahmen, Freigaben, Verantwortlichkeiten	Compliance / KI-Officer

© A4Q Copyright 2025

Nachweisart	Inhalt / Zweck	Verantwortlich
Audit-Trail & Logging	Nachvollziehbarkeit von Eingaben, Entscheidungen, Systemeingriffen und Versionen	IT-Betrieb / Systemverantwortliche
Change-Log	Erfassung von Modell-, Daten- oder Parameteränderungen	Technische Leitung / QA
Schulungsnachweise	Teilnahmeprotokolle, Lerninhalte, Kompetenzprüfung der Mitarbeitenden (Art. 4 (4))	HR / KI-Officer
Incident-Reports	Meldungen, Ursachenanalysen, Maßnahmen und Wirksamkeitsprüfung (Art. 23 f.)	Compliance / Betrieb
Monitoring-Berichte	Leistungsdaten, Drift-Erkennung, Korrekturmaßnahmen	Fachbereiche / AI-Governance-Team

Diese Nachweise bilden gemeinsam das Konformitätsdossier (Art. 17 ff.) und müssen jederzeit prüfungsfähig, aktuell und nachvollziehbar sein.

2 Audit-Sicherheit erhöhen

Ein wirksames Audit-Managementsystem stellt sicher, dass alle Nachweise vollständig, standardisiert und leicht zugänglich sind.
Folgende Maßnahmen erhöhen die Audit-Sicherheit nachhaltig:

- **Einheitliches Dokumentationsschema:** Struktur gemäß ISO/IEC 42001 (AI Management System) oder ISO/IEC 23894 (Risikomanagement).
- **Regelmäßige interne Audits:** Mindestens einmal jährlich oder bei jeder wesentlichen Systemänderung.
- **Prüfpfad-Visualisierung:** Darstellung des Daten- und Entscheidungsflusses (Input → Modellverarbeitung → Output → menschliche Freigabe).
- **Zentralisierte Ablage:** Einheitliche Ablageorte mit Zugriffssteuerung und Versionierung.
- **Aufbewahrungspflicht:** Mindestens **10 Jahre** für Hochrisiko-Systeme (Art. 61 AI Act).
- **Audit-Trail-Schutz:** Fälschungssichere Speicherung (z. B. Hash, Blockchain, WORM-Systeme).
- **Audit-Kommunikation:** Vorab definierte Verantwortlichkeiten und Abläufe für Behördenanfragen oder Zertifizierungsprüfungen.

© A4Q Copyright 2025

Praxis-Tipp:
Vor einem externen Audit sollte ein interner „Pre-Audit-Check“ erfolgen, um Lücken oder veraltete Nachweise rechtzeitig zu erkennen und zu schließen.

3 Checkliste Audit-Readiness

Diese Checkliste kann Ihnen helfen, den aktuellen Stand der Auditvorbereitung zu bewerten

Checkliste Audit-Readiness

- Aktuelle **Systembeschreibung** mit Zweck, Version, Verantwortlichen und Einsatzbereich liegt vor.
- **Risikoregister** ist aktuell, vollständig und mit dokumentierten Maßnahmen verknüpft.
- **Test- und Validierungsprotokolle** sind vollständig archiviert.
- **Protokollierung** erfolgt revisionssicher, nachvollziehbar und versionsgeführt.
- **Incident-Response-Plan** ist dokumentiert und regelmäßig getestet.
- **Monitoring-Berichte** werden erstellt und laufend aktualisiert.
- **Schulungen** aller operativen Rollen sind nachweislich durchgeführt.
- **Änderungen und Updates** sind nachvollziehbar dokumentiert.
- **Freigaben** durch verantwortliche Personen sind protokolliert.
- **Audit-Termine und Verantwortlichkeiten** sind im Jahresplan festgelegt.

Fazit

Dokumentation ist ein zentraler Bestandteil wirksamer KI-Governance.
Durch die systematische Erfassung von Prozessen, Daten, Entscheidungen und Kontrollen lässt sich im Auditfall die Einhaltung des EU AI Act nachweisen und das Risiko von Beanstandungen verringern.
Ein klar aufgebautes Dokumentationssystem sorgt für Transparenz, eindeutige Verantwortlichkeiten und Nachvollziehbarkeit, intern wie extern.

5.5 Beispiel – Anwendung der Hochrisiko-Pflichten in der Praxis

Ausgangssituation:
Sie übernehmen die Rolle des **AI Compliance Officer** in einem Finanzunternehmen.
Ihr Verantwortungsbereich umfasst ein **KI-gestütztes Kredit-Scoring-System**, das automatisiert die Kreditwürdigkeit von Kund:innen bewertet und Empfehlungen für Kreditentscheidungen abgibt.

© A4Q Copyright 2025

Das System fällt gemäß **Anhang III Nr. 5 EU AI Act** in den Anwendungsbereich der Hochrisiko-KI-Systeme, da es unmittelbar Einfluss auf wirtschaftliche Rechte und Pflichten von Personen nimmt.

Ziel des Beispiels:
Ziel ist es, den Umgang mit den **zentrale(n) Compliance-Pflichten nach Art. 9–15 EU AI Act** praktisch zu trainieren, geeignete Nachweise zu identifizieren und die **Audit-Readiness** des Systems kritisch zu bewerten.

1. Identifikation der Pflichten

Die drei wichtigsten Pflichten im Zusammenhang mit einem KI-basierten Kredit-Scoring-System sind:

Pflicht (Artikel)	Inhalt / Ziel	Begründung für die Auswahl
Art. 9 – Risikomanagementsystem	Systematische Erfassung, Bewertung und Kontrolle aller potenziellen Risiken über den gesamten Lebenszyklus	Kreditentscheidungen betreffen unmittelbar Verbraucherrechte; daher ist ein formelles Risikomanagement zwingend erforderlich.
Art. 11 – Technische Dokumentation	Nachvollziehbare Beschreibung von Zweck, Funktion, Daten, Modellen, Testverfahren und Limitationen	Ohne vollständige Dokumentation kann die Funktionsweise des Systems im Audit oder bei Beschwerden nicht überprüft werden.
Art. 14 – Human Oversight	Sicherstellung, dass Menschen das System überwachen, prüfen und bei Bedarf eingreifen können	KI darf keine automatischen Entscheidungen ohne menschliche Verantwortung treffen; dies dient Fairness und Diskriminierungsschutz.

2. Erforderliche Nachweise und Zeitpunkt der Erstellung

Nachweis	Zweck / Bedeutung	Wann erstellt / aktualisiert
AI-Risk-Register	Enthält alle identifizierten Risiken, deren Bewertung (Eintritt × Schweregrad) und definierte Gegenmaßnahmen.	Bei jeder wesentlichen Systemänderung, mindestens halbjährlich.
Technisches Dossier	Belegt die Modellarchitektur, verwendeten Trainingsdaten, Testprotokolle und Systemgrenzen.	Vor der Markteinführung; Aktualisierung bei Modell- oder Datenänderung.

© A4Q Copyright 2025

Nachweis	Zweck / Bedeutung	Wann erstellt / aktualisiert
Freigabe- und Prüfprotokolle	Nachweis, dass geschulte Personen das System vor dem Einsatz geprüft und genehmigt haben.	Vor jedem Deployment oder größeren Update.

3. Bewertung der Audit-Readiness

Das System gilt als **audit-ready**, wenn:

- alle Nachweise **vollständig, aktuell und versioniert** vorliegen,
- **Verantwortlichkeiten** (Owner, Reviewer, Freigabeverantwortliche) klar dokumentiert sind,
- und alle relevanten Unterlagen im Auditfall **innerhalb von 24 Stunden** vorgelegt werden können.

Begründung:
Diese Bedingungen entsprechen dem Grundsatz der **Rechenschaftspflicht (Accountability)** gemäß Art. 11 und Art. 61 EU AI Act.
Fehlt eines dieser Elemente – etwa ein veraltetes Risikoregister oder fehlende Unterschriften auf Freigabeprotokollen – gilt das System als **nicht konform** und erfordert sofortige Korrekturmaßnahmen (z. B. Nachdokumentation, Re-Validierung).

Reflexion und mögliche Verbesserung

Reflexionsfrage:
Welche organisatorischen Maßnahmen könnten helfen, die Audit-Bereitschaft dauerhaft zu sichern?

Beispielhafte Antworten:

- Einführung eines **jährlichen internen Audits** zur Überprüfung der AI-Dokumentation.
- Nutzung eines **zentralen Audit-Repositories** mit Zugriffs- und Versionenkontrolle.
- Verpflichtende **Refresher-Schulungen** für AI-Officer und Fachabteilungen.
- Einrichtung eines **Compliance-Dashboards**, das automatisch anzeigt, welche Nachweise bald ablaufen.

Fazit

Hochrisiko-KI-Systeme wie das Kredit-Scoring sind **grundsätzlich erlaubt**, aber an **strenge Nachweis- und Auditpflichten** gebunden.
Ein strukturiertes, dokumentiertes und überprüfbares Vorgehen über den gesamten Lebenszyklus – von der Entwicklung über den Einsatz bis zur Überwachung – ist zwingend erforderlich.

© A4Q Copyright 2025

Unternehmen, die die Anforderungen der **Artikel 6–51 EU AI Act** konsequent erfüllen, gewährleisten nicht nur **Rechtskonformität**, sondern stärken auch **Vertrauen, Haftungssicherheit und Reputation**.

© A4Q Copyright 2025

6 Risikomanagement- und Qualitäts-managementsystem

⏱ 60 Minuten

🎯 **Business Outcomes:**

- **BO 6.1:** Teilnehmende sind vorbereitet, am Aufbau oder der Anpassung eines AI-Risikomanagementsystems nach ISO/IEC 42001 mitzuwirken.
- **BO 6.2:** Teilnehmende verstehen die Bedeutung der Integration von KI-Prozessen in bestehende Managementsysteme (QMS, ISMS, DSMS) und erkennen, wie diese Verknüpfung zur Sicherstellung von Compliance und Qualität beiträgt.

Lernziele (Learning Objectives – LO)

- **LO 6.1 (K2):** Teilnehmende können Aufbau und Zweck eines AI-Risikomanagementsystems nach Art. 9 EU AI Act und ISO/IEC 42001 erläutern.
- **LO 6.2 (K2):** Teilnehmende können die Wechselwirkungen zwischen AI-Act-Pflichten und bestehenden Managementsystemen (QMS, ISMS, DSMS) beschreiben.
- **LO 6.3 (K1):** Teilnehmende können die Phasen eines kontinuierlichen KI-Risikomanagementzyklus identifizieren (Risikobeurteilung, Maßnahmen, Überwachung, Verbesserung).
- **LO 6.4 (K1):** Teilnehmende können benennen, wie Dokumentation, Monitoring und Audits zur Audit-Readiness beitragen.
- **LO 6.5 (K1)**: Teilnehmende kennen die grundlegenden Schritte eines AI-Risikomanagementzyklus.

Wichtige Begriffe:
ISO/IEC 42001 (AI Management System), ISO/IEC 23894 (AI Risk Management), Risikomanagementzyklus, Proportionalität, Lebenszyklusabdeckung, Lessons Learned, Kontrollbericht, Stakeholderanalyse, Verantwortlichkeit, Nachvollziehbarkeit, Qualitätsmanagement (QM), ISMS, DSMS

Einleitung

Der EU AI Act verpflichtet Organisationen gemäß Artikeln 9 und 17–23 zur Einrichtung eines systematischen Risikomanagementsystems für Hochrisiko-KI-Systeme. Dieses System muss den gesamten Lebenszyklus abdecken – von der Entwicklung über den Einsatz bis zur Stilllegung.

© A4Q Copyright 2025

Internationale Normen wie **ISO/IEC 23894** (Risikomanagement für KI) und **ISO/IEC 42001** (AI Management System – AIMS) liefern dafür anerkannte Rahmenwerke und Methoden. Sie übersetzen die rechtlichen Pflichten des AI Acts in prüf- und auditfähige Prozesse.

Ziel dieses Kapitels ist es, Teilnehmenden die Kernprinzipien des AI-Risikomanagements zu vermitteln und die Integration in bestehende Qualitäts-, Informationssicherheits- und Datenschutzmanagementsysteme verständlich darzustellen.

6.1 Grundprinzipien des AI-Risikomanagements

Ein Risikomanagementsystem nach Art. 9 AI Act muss folgende Anforderungen erfüllen:

- **Lebenszyklusabdeckung:** Analyse von Design, Training, Einsatz, Monitoring und Stilllegung.
- **Regelmäßige Aktualisierung:** Wiederkehrende Überprüfung nach Änderungen von Modell, Daten oder Zweck.
- **Dokumentation und Nachvollziehbarkeit:** Alle Bewertungen und Maßnahmen sind schriftlich festzuhalten.
- **Proportionalität:** Tiefe und Umfang des Prozesses müssen im Verhältnis zum Risikopotenzial stehen.

Zentrale Ziele des Systems:

Ziel	**Beschreibung**
Schutz von Grundrechten	Vermeidung von Diskriminierung, Täuschung und Manipulation.
Technische Sicherheit	Robuster, verlässlicher und fehlertoleranter Systembetrieb.
Nachvollziehbarkeit	Jede Entscheidung muss ex post begründbar und prüfbar sein.
Verantwortlichkeit	Klare Rollen, Befugnisse und Eskalationswege innerhalb der Organisation.

Damit dient das AI-Risikomanagement nicht nur der gesetzlichen Pflichterfüllung, sondern auch der Qualitätssicherung und dem Vertrauensaufbau bei Kunden, Behörden und der Öffentlichkeit.

6.2 Der Risikomanagementzyklus nach ISO/IEC 23894 und AI Act

Der AI-Act-konforme Risikomanagementprozess folgt einem kontinuierlichen Zyklus aus Identifikation, Bewertung, Steuerung und Überwachung von Risiken.

© A4Q Copyright 2025

Phase	Zentrale Aktivitäten	Bezug zu Art. 9 AI Act
1 – Kontext und Ziele definieren	Bestimmung von Systemzweck, Stakeholdern, rechtlichem Rahmen und Grundrechtsbezug.	Abs. 2 a
2 – Risiken identifizieren	Erfassung technischer, organisatorischer und ethischer Risiken (z. B. Bias, Fehler, Datenschutz).	Abs. 2 b–c
3 – Risiken analysieren und bewerten	Bewertung nach Eintrittswahrscheinlichkeit und Auswirkung; Priorisierung nach Risikoklassen.	Abs. 2 d
4 – Risikosteuerung und Maßnahmen	Implementierung technischer und organisatorischer Kontrollen (z. B. Fallback, Human Oversight, Logging).	Abs. 3
5 – Überwachung und Verbesserung	Laufendes Monitoring gemäß Art. 24; Lessons Learned und Kontrollberichte.	Abs. 4

Der Prozess wird mindestens jährlich oder nach wesentlichen Änderungen wiederholt (z. B. neue Trainingsdaten, geänderter Zweck).

6.3 Integration in bestehende Managementsysteme

Ein isoliertes KI-Risikomanagement führt zu Redundanzen und Ineffizienz. Empfohlen wird eine enge Verzahnung mit bestehenden Systemen nach ISO/IEC 42001 (AIMS), ISO 9001 (QMS), ISO/IEC 27001 (ISMS) und ISO/IEC 27701 (DSMS).

Managementsystem	Zielsetzung	Beitrag zur KI-Compliance
QMS (ISO 9001)	Qualitätsmanagement und Prozesslenkung	Sicherstellung einheitlicher Dokumentation und regelmäßiger Audits.
ISMS (ISO/IEC 27001)	Informationssicherheit, Vertraulichkeit, Integrität	Schutz der Trainings- und Betriebsdaten vor Manipulation und Verlust.
DSMS (ISO/IEC 27701 / DSGVO)	Datenschutz-Compliance	Abstimmung zwischen DSFA und AI-Risikobewertung.

© A4Q Copyright 2025

Managementsystem	Zielsetzung	Beitrag zur KI-Compliance
AIMS (ISO/IEC 42001)	AI-Governance und Risikosteuerung	Zentrale Dokumentation und Nachweisführung für Art. 9 und 17–23 AI Act.

Die Integration führt zu einem „System of Systems“, in dem Prozesse, Auditzyklen und Rollen koordiniert werden. So entsteht ein kohärentes Governance-Framework, das technische und rechtliche Kontrollen vereint.

6.4 Dokumentations- und Nachweispflichten

Die Artikel 17–23 AI Act fordern eine umfassende Dokumentation und Nachweisführung. Diese dient dem Beleg der Konformität und der Audit-Readiness.

Pflichtdokumente:

1. Risikomanagementplan mit Bewertungsmatrix und Risikokriterien.
2. Technische Dokumentation nach Art. 11 (Architektur, Daten, Tests, Limitationen).
3. Protokolle über Monitoring, Vorfall- und Korrekturmaßnahmen.
4. Aktuelle Konformitätserklärung nach Art. 19 inkl. Versionierung und Verantwortlichkeiten.
5. Verknüpfung zu internen Auditberichten (QMS/ISMS).

Alle Dokumente müssen:

- nachvollziehbar, vollständig und versionssicher sein,
- zentral archiviert und zugriffsbeschränkt werden,
- bei Audits oder Behördenanfragen zeitnah bereitgestellt werden (max. 48 Stunden).

Dokumentation ist ein **kontinuierlicher Prozess** und muss bei Änderungen an Modellen, Daten, Einsatzkontext oder Governance-Strukturen aktualisiert werden.

Nach ISO/IEC 42001 (Abschnitte 7.4 und 9.2) ist die Dokumentation Teil des gesamten AIMS (Artificial Intelligence Management System), sie dient als Informationsrückgrat für Audits, Reviews und Managementbewertungen.

Zur Sicherstellung der Auditfähigkeit sollten Nachweise strukturiert und maschinenlesbar archiviert werden (z. B. PDF/A, XML) und eindeutig einer Systemversion sowie einem Verantwortlichen zuordenbar sein.

© A4Q Copyright 2025

Die Verantwortung für Pflege und Vollständigkeit liegt beim AI Compliance Officer bzw. bei der/dem Dokumentationsverantwortlichen im QMS.

6.5 Governance, Rollen und Verantwortung

Ein funktionierendes AI-Risikomanagementsystem setzt **klare Governance-Strukturen** und **eindeutig definierte Verantwortlichkeiten** voraus.
Nur wenn Zuständigkeiten, Entscheidungsbefugnisse und Kommunikationswege festgelegt und dokumentiert sind, kann das System im Sinne der **Art. 9, 17–23 EU AI Act** wirksam umgesetzt und regelmäßig überprüft werden.

Rollen und Aufgaben im AI-Risikomanagement:

Rolle	**Kernaufgaben und Zuständigkeiten**
AI Compliance Manager / KI-Officer	Gesamtkoordination des Risikomanagementprozesses, Erstellung und Pflege des Risikoregisters, Überwachung der Wirksamkeit von Maßnahmen, Vorbereitung interner und externer Audits, Kommunikation mit Behörden und Zertifizierungsstellen.
Fachverantwortliche / System-Owner	Identifikation und Bewertung neuer Risiken im operativen Betrieb, Meldung von Incidents und Modelländerungen, Sicherstellung, dass technische Änderungen dokumentiert und genehmigt werden.
Datenschutz- und Sicherheitsbeauftragte	Abstimmung zwischen Datenschutz-Folgenabschätzung (DSFA) und AI-Risikobewertung, Einbindung in Incident-Response-Prozesse, Sicherstellung der Kohärenz mit ISMS- und DSMS-Vorgaben.
Qualitätsmanagement / QMS-Verantwortliche	Integration des AI-Risikomanagements in bestehende Audit- und Dokumentationsprozesse, Harmonisierung der Verfahrensanweisungen und Prüfzyklen.
Ethik- oder Compliance-Komitee (optional)	Bewertung ethischer Implikationen, Konfliktlösung bei Zielkonflikten (z. B. Accuracy vs. Fairness), Freigabe sensibler Systeme oder Hochrisiko-Use-Cases.
Management / Board	Genehmigung der Risikostrategie, Festlegung der Governance-Politik, Ressourcenfreigabe, regelmäßige Berichterstattung über den Reifegrad des AI-Compliance-Systems.

© A4Q Copyright 2025

Alle Rollen müssen durch dokumentierte Stellvertretungs- und Eskalationsregeln ergänzt werden. Empfohlen wird die Abbildung der Verantwortlichkeiten in einer **RACI-Matrix** (Responsible – Accountable – Consulted – Informed), die regelmäßig überprüft und bei organisatorischen Änderungen aktualisiert wird.

Ein solcher Governance-Ansatz stellt sicher, dass Entscheidungen **nachvollziehbar**, **auditierbar** und **revisionssicher** getroffen werden. Er schafft zugleich die Voraussetzung für eine wirksame interne Kontrolle und die kontinuierliche Verbesserung des gesamten **Artificial Intelligence Management Systems (AIMS)** nach ISO/IEC 42001.

6.6 Bedeutung der Integration für Compliance und Qualität

Die Integration des AI-Risikomanagements in bestehende Managementsysteme (z. B. QMS, ISMS, DSMS) ist ein zentraler Erfolgsfaktor für nachhaltige Compliance. Sie sorgt dafür, dass Pflichten aus dem EU AI Act nicht isoliert, sondern im Rahmen bewährter Organisationsstrukturen erfüllt werden.

Vorteile der Integration:

- **Reduktion von Doppelprüfungen:** Datenschutz-Folgenabschätzung (DSFA) und AI-Risikobewertung können kombiniert durchgeführt werden, wodurch Redundanzen entfallen.
- **Konsistenz der Nachweise:** Dokumente, Reports und Audit-Logs folgen einheitlichen Versionierungs-, Freigabe- und Archivierungsstandards.
- **Verbesserte Nachvollziehbarkeit:** Einheitliche Prozesse und gemeinsame Auditzyklen ermöglichen eine lückenlose Rückverfolgbarkeit von Entscheidungen und Änderungen.
- **Qualitätsgewinn und Effizienz:** Risiken werden früher erkannt, Maßnahmen systematisch dokumentiert und präventive Korrekturen im Lebenszyklus eingeleitet.
- **Ganzheitliche Governance:** Die Integration stärkt die Verbindung zwischen technischen, rechtlichen und organisatorischen Kontrollen – ein wesentlicher Aspekt der ISO/IEC 42001-Anforderungen.

Organisationen, die diese Integration konsequent umsetzen, erreichen eine **„Presumption of Conformity“** gemäß **Art. 40 EU AI Act**.
Damit können sie ihre Nachweispflichten gegenüber Aufsichts- und Zertifizierungsstellen effizient erfüllen und zugleich eine **höhere Prozess- und Produktqualität** nachweisen.

© A4Q Copyright 2025

© A4Q Copyright 2025

7 Konformitätsbewertung und CE-Kennzeichnung

⏱ Unterrichtszeit: 80 Minuten

🎯 **Business Outcomes**

BO 7.1 Teilnehmende entwickeln Verständnis für Konformitätsrouten und sind vorbereitet, deren Anwendung zu unterstützen.

BO 7.2 Teilnehmende sind befähigt, CE-Kennzeichnung und EU-Datenbank-Eintragungen zu begleiten.

Lernziele (Learning Objectives – LO)

- **LO 7.1** Teilnehmende können interne und externe Konformitätsbewertungsverfahren gemäß Art. 43–51 AI Act beschreiben. (K2)
- **LO 7.2** Teilnehmende können beurteilen, wann eine benannte Stelle (Notified Body) einzubeziehen ist. (K2)
- **LO 7.3** Teilnehmende können die Inhalte der technischen Dokumentation und deren Audit-Relevanz erläutern. (K2)
- **LO 7.4** Teilnehmende können den Ablauf der CE-Kennzeichnung für Hochrisiko-Systeme darstellen. (K1)
- **LO 7.5** Teilnehmende können den Prozess der Registrierung in der EU-Datenbank und die Verantwortlichkeiten im Unternehmen benennen. (K1)
- **LO 7.6** Teilnehmende können die Pflichten nach wesentlichen Änderungen am System einschätzen und eine erneute Bewertung anstoßen. (K3)
- **LO 7.7 (K1):** Teilnehmende kennen die zentralen Elemente einer Konformitätsbewertung nach Art. 43 EU AI Act.

Wichtige Begriffe:

Konformitätsbewertung, Technische Dokumentation, EU-Konformitätserklärung, CE-Kennzeichnung, Notifizierte Stelle, Providerpflichten, Marktüberwachung, Artikel 43 AI Act, Prüfverfahren, Internes Kontrollverfahren, Prüfpfad, Audit-Nachweis.

Einführung

© A4Q Copyright 2025

Die Konformitätsbewertung ist das zentrale Instrument zur rechtlichen Zulassung von Hochrisiko-KI-Systemen im Rahmen des EU AI Act. Sie prüft, ob ein System alle gesetzlich vorgeschriebenen Anforderungen erfüllt – von Datenqualität und Risikomanagement über Transparenz bis hin zur menschlichen Aufsicht. Das Verfahren endet mit der CE-Kennzeichnung und dem Eintrag in die europäische Datenbank für KI-Systeme. Es stellt den entscheidenden Schritt zwischen Entwicklung und Inverkehrbringen dar.

7.1 Grundlagen der Konformitätsbewertung (Art. 43 AI Act)

Ziel der Bewertung ist die **objektive Feststellung**, dass ein KI-System alle **wesentlichen Anforderungen der Verordnung** erfüllt – insbesondere zu Sicherheit, Datenqualität, Transparenz, menschlicher Aufsicht und Risikomanagement.
Die Konformitätsbewertung dient somit als Brücke zwischen technischer Entwicklung und rechtlicher Marktfreigabe.

Die Bewertung kann auf zwei Arten erfolgen:

Verfahrenstyp	**Merkmale**	**Anwendungsfälle**
Interne Konformitätsbewertung	Eigenverantwortliche Prüfung durch den Anbieter. Umfasst die Erstellung der technischen Dokumentation, die Durchführung interner Tests und das Erstellen der EU-Konformitätserklärung.	Standardfälle ohne besondere gesellschaftliche oder sicherheitskritische Bedeutung, etwa KI-gestützte Personalprozesse oder Kreditbewertungssysteme mit begrenztem Einsatzbereich.
Bewertung durch benannte Stelle	Externe Prüfung durch eine akkreditierte Organisation („Notified Body“). Die Stelle überprüft das Qualitätsmanagementsystem, führt stichprobenartige technische Prüfungen durch und bescheinigt die Einhaltung der Anforderungen.	Hochkritische Anwendungen wie biometrische Identifikation, medizinische Diagnostik oder sicherheitsrelevante Infrastruktursteuerung.

Bei beiden Verfahren gilt:
Die **Gesamtverantwortung** für die Richtigkeit, Vollständigkeit und Aktualität der Unterlagen liegt **immer beim Anbieter**, auch wenn eine externe Stelle beteiligt ist.

© A4Q Copyright 2025

Ablauf einer Konformitätsbewertung – in vier Schritten

1. **Vorbereitung und Dokumentation:**
   Sammlung aller Nachweise zu Risikomanagement, Datenqualität, Human Oversight und Robustheit.
   Erstellung des technischen Dossiers nach Anhang IV AI Act.
2. **Durchführung der Bewertung:**
   - *intern:* Prüfung durch interne Fachverantwortliche (z. B. AI Compliance Manager, Qualitätsmanagement).
   - *extern:* Audit und Dossier-Review durch eine benannte Stelle.
3. **Ergebnis & Nachweis:**
   Erstellung des **Konformitätsberichts** und ggf. Ausstellung einer **EU-Baumusterprüfbescheinigung**.
   Auf Basis dieses Nachweises darf die **EU-Konformitätserklärung** erstellt und das **CE-Zeichen** angebracht werden.
4. **Nachverfolgung:**
   Kontinuierliche Überwachung, insbesondere bei Systemänderungen oder neuen Trainingsdaten (Post-Market Monitoring).

Hinweis zur Entscheidungslogik

Die Wahl zwischen **interner** und **externer Konformitätsbewertung** hängt von drei Faktoren ab:

1. **Risikoklasse des Systems (Art. 6 ff. AI Act)**
   Nur **Hochrisiko-Systeme** unterliegen einer formellen Konformitätsbewertung.
   Systeme mit geringem oder minimalem Risiko benötigen kein CE-Verfahren.
2. **Art der Anwendung (Annex III AI Act)**
   Innerhalb der Hochrisiko-Systeme unterscheidet der AI Act:
   - **Standardisierte Hochrisiko-Anwendungen** (z. B. HR- oder Kredit-Scoring-Systeme) → *interne Bewertung möglich*
   - **Sicherheits- oder grundrechtskritische Anwendungen** (z. B. biometrische Identifikation, Medizinprodukte, kritische Infrastrukturen) → *externe Prüfung durch eine benannte Stelle erforderlich*
3. **Vorhandensein eines zertifizierten Managementsystems**
   Wenn der Anbieter bereits ein anerkanntes Qualitäts- oder AI-Managementsystem betreibt

© A4Q Copyright 2025

(z. B. nach **ISO/IEC 42001** oder **ISO 9001**),
kann die interne Konformitätsbewertung als gleichwertig anerkannt werden.
Fehlt ein solches System, ist die **Einbindung einer benannten Stelle** in der Regel verpflichtend.

Kurz gesagt:

Voraussetzungen	**Zulässiges Verfahren**	**Beispiel**
Hochrisiko-System, standardisierte Anwendung, internes Qualitätsmanagement vorhanden	**Interne Konformitätsbewertung**	KI für Bewerbungsanalyse oder Kreditprüfung
Hochrisiko-System mit sicherheits- oder grundrechtsrelevanter Funktion, kein zertifiziertes Managementsystem	**Bewertung durch benannte Stelle**	Gesichtserkennung im öffentlichen Raum, medizinische Diagnosesoftware
Begrenztes oder minimales Risiko	**Keine formelle CE-Bewertung erforderlich**	Chatbot mit Nutzerhinweis

Praxisbeispiel

Ein Hersteller eines KI-gestützten Bewerbungs-Tools führt eine interne Konformitätsbewertung durch.
Da das System in Annex III Abschnitt 4 („Verwaltung von Arbeitsverhältnissen“) fällt, dokumentiert er alle Risikomaßnahmen und erstellt die technische Dokumentation.
Für eine spätere Version mit biometrischer Bewerber-Verifikation wäre hingegen eine **Notified Body-Prüfung** zwingend vorgeschrieben.

Empfehlung:
Die Konformitätsbewertung ist kein einmaliger Akt, sondern ein kontinuierlicher Prozess über den gesamten Lebenszyklus.
Sie bildet den Kern der Nachweisführung im Audit und ist Voraussetzung für die CE-Kennzeichnung sowie den Eintrag in die EU-Datenbank.

7.2 Inhalte der technischen Dokumentation (Art. 11 & Anhang IV)

Die **technische Dokumentation** ist das zentrale Nachweisdokument im Konformitätsverfahren.
Sie dient dazu, gegenüber Behörden und benannten Stellen nachzuweisen, dass das KI-System **alle wesentlichen Anforderungen** des EU AI Act erfüllt.

© A4Q Copyright 2025

Sie muss **vor dem Inverkehrbringen** vollständig vorliegen, **laufend aktualisiert** werden und **jederzeit prüfbereit** sein.

A. Zwingend vorgeschriebene Bestandteile (verbindlich nach Art. 11 i. V. m. Anhang IV EU AI Act)

Diese Elemente **müssen** enthalten sein, um die Konformitätsbewertung bestehen zu können:

1. **Beschreibung des KI-Systems**
   – Zweckbestimmung, Architektur, Hauptfunktionen, Grenzen der Nutzung.
   (Begründung: erforderlich zur Risikoeinstufung und Funktionsnachvollziehbarkeit)

2. **Risikomanagementverfahren und -ergebnisse (Art. 9)**
   – Darstellung der identifizierten Risiken, Bewertung ihrer Schwere und Wirksamkeit der Gegenmaßnahmen.
   (Pflicht für alle Hochrisiko-Systeme)

3. **Daten- und Datenqualitätsnachweise (Art. 10)**
   – Angaben zu Trainings-, Validierungs- und Testdaten, Quellen, Repräsentativität, Bias-Kontrolle.
   (Zentral für Fairness, Robustheit und Nichtdiskriminierung)

4. **Nachweise zur technischen Sicherheit, Genauigkeit und Robustheit (Art. 15)**
   – Testergebnisse, Performance-Metriken, Sicherheitsprüfungen, Cybersecurity-Maßnahmen.

5. **Beschreibung der Human-Oversight-Mechanismen (Art. 14)**
   – Darstellung, wie menschliche Kontrolle, Eingriff und Überwachung technisch umgesetzt sind.

6. **Bedienungsanleitung und Nutzungsbedingungen**
   – Klare Beschreibung, wie das System korrekt einzusetzen ist, einschließlich Einschränkungen und Warnhinweise.
   (Pflicht, um Fehlanwendung und Haftungsrisiken zu vermeiden)

7. **Post-Market-Monitoring-Konzept (Art. 61)**
   – Darstellung, wie das System nach Inverkehrbringen überwacht wird, inkl. Rückmelde- und Incident-Prozess.

8. **Entwurf der EU-Konformitätserklärung (Art. 48)**
   – Erklärung des Anbieters über die Einhaltung der relevanten Vorschriften.
   (Voraussetzung für CE-Kennzeichnung)

B. Optionale bzw. ergänzende Nachweise (empfohlen, aber nicht zwingend)

Diese Bestandteile sind **nicht explizit vorgeschrieben**, erhöhen jedoch **Audit-Fähigkeit, Transparenz und Nachvollziehbarkeit**:

© A4Q Copyright 2025

9. **Bewertung der Übereinstimmung mit harmonisierten Normen**
   – Bezug auf ISO/IEC 42001 (AI Managementsystem), ISO/IEC 23894 (Risikomanagement) oder DIN SPEC 92001-2.
   (Optional, aber kann „Presumption of Conformity" begründen – erleichtert Audit und CE-Prüfung.)

10. **Protokollierungs- und Monitoringkonzepte (Detailniveau über Mindestanforderung hinaus)**
    – Konkrete Log-Struktur, Zugriffskontrollen, Audit-Trail-Mechanismen.
    (Empfohlen für fortlaufende Auditfähigkeit und Sicherheitsnachweise.)

11. **Nachweise zur internen Qualitätssteuerung**
    – Dokumentation, dass ein funktionsfähiges Qualitätsmanagementsystem (z. B. nach ISO 9001 oder 42001) besteht.
    (Erleichtert interne Konformitätsbewertung nach Art. 43 Abs. 2 lit. b)

Begründung der Trennung

- **Pflichtteile** ergeben sich direkt aus den Artikeln 9–15 und Anhang IV AI Act.
- **Optionale Teile** sind zwar nicht zwingend, werden aber von benannten Stellen häufig angefordert, um eine vollständige Beurteilung vorzunehmen oder bei internen Audits Zeit und Kosten zu sparen.

Empfehlung: Unternehmen sollten sich an den harmonisierten Standards orientieren – sie gelten als anerkannte Nachweise der „Presumption of Conformity" und verringern Prüfrisiken erheblich.

Empfehlung: Orientierung an harmonisierten Standards

Unternehmen sollten sich bei der Erstellung ihrer technischen Dokumentation und beim Aufbau ihres KI-Managementsystems **an den von der EU-Kommission anerkannten harmonisierten Normen** orientieren.
Diese Normen werden im Amtsblatt der EU veröffentlicht und bilden die Grundlage für die sogenannte **„Presumption of Conformity"** – also die gesetzliche Vermutung, dass ein System die Anforderungen des EU AI Act erfüllt, sofern es nach diesen Normen entwickelt und betrieben wird.

Empfohlene harmonisierte Standards für den EU AI Act

Norm / Standard	**Titel / Inhaltlicher Fokus**	**Bezug zum AI Act**	**Veröffentlichung / Status**
ISO/IEC 42001:2023	*Artificial Intelligence Management System (AIMS)* – Anforderungen an Aufbau, Steuerung, Überwachung und	Entspricht Art. 17–23 (Qualitäts- und Risikomanagement).	**Veröffentlicht 2023**, ISO-zertifizierbar seit Q2 2024.

© A4Q Copyright 2025

Norm / Standard	Titel / Inhaltlicher Fokus	Bezug zum AI Act	Veröffentlichung / Status
	kontinuierliche Verbesserung von KI-Managementsystemen.	Grundlage für interne Konformitätsbewertung.	
ISO/IEC 23894:2023	*Artificial Intelligence - Guidance on Risk Management.* Integriert KI-spezifische Risiken in bestehende Managementsysteme.	Deckt Art. 9 (AI-Risikomanagementsystem) ab.	**Veröffentlicht 2023**, internationale Anwendung empfohlen.
ISO/IEC 22989:2022	*Artificial Intelligence - Concepts and Terminology.* Gemeinsame Begriffe und Definitionen zur Vereinheitlichung von Dokumentation und Audits.	Unterstützt Art. 11 (Technische Dokumentation) und Anhang IV.	**Veröffentlicht 2022**, Grundlage vieler Folge-Normen.
ISO/IEC 23053:2022	*Framework for Machine Learning (ML) - Lifecycle management.* Lebenszyklusmodell für ML-Systeme.	Unterstützt Art. 10 (Daten) und Art. 15 (Robustheit).	**Veröffentlicht 2022**, in Überarbeitung für AI-Act-Harmonisierung (erwartet 2026).
ISO/IEC 24028:2020	*Overview of Trustworthiness in Artificial Intelligence.* Leitfaden zu Sicherheit, Resilienz und Zuverlässigkeit.	Ergänzt Art. 15 (Cybersicherheit und Robustheit).	**Veröffentlicht 2020**, Überarbeitung geplant 2026.
DIN SPEC 92001-1:2020	*Qualitätsanforderungen an KI-Systeme – Grundlagen.*	Nationale Vorstufe zu ISO/IEC 42001, praxisnah für deutsche Unternehmen.	**Veröffentlicht 2020**, gilt als Übergangsstandard.
DIN SPEC 92001-2:2021	*Qualitätsanforderungen an KI-Systeme – Prüfkriterien.*	Hilft bei Audit-Vorbereitung und Nachweisführung.	**Veröffentlicht 2021**.
ISO/IEC 27001:2022	*Information Security Management System (ISMS).*	Unterstützt Datensicherheitspflichten aus Art. 15.	**Veröffentlicht 2022** (aktuelle Fassung).

© A4Q Copyright 2025

Norm / Standard	Titel / Inhaltlicher Fokus	Bezug zum AI Act	Veröffentlichung / Status
ISO/IEC 27701:2019	*Privacy Information Management System (PIMS)* – Erweiterung zu ISO 27001.	Ergänzt Datenschutzanforderungen aus Art. 10 und Art. 15.	**Veröffentlicht 2019**, Überarbeitung erwartet 2026.

Hinweis zur Harmonisierung (Stand 2025)

- Die **Europäische Kommission** arbeitet mit **CEN/CENELEC JTC 21** an der **Überführung dieser ISO-Normen in europäische harmonisierte Standards (EN-ISO)**.
- Die **erste Tranche harmonisierter Normen** für den AI Act wird **voraussichtlich im 1. Halbjahr 2026** im Amtsblatt der EU veröffentlicht.
- Bis dahin gelten die oben genannten ISO/IEC-Normen als **anerkannte „good practice“** und werden bereits von **benannten Stellen (Notified Bodies)** in Audits akzeptiert.

Warum diese Standards wichtig sind

- Sie **strukturieren** die technische Dokumentation und erleichtern deren Prüfung.
- Sie **reduzieren Interpretationsspielräume** bei Audits und Behördenkontrollen.
- Sie ermöglichen die **Kombination von KI- und Qualitätsmanagement**, wodurch interne Bewertungen (Art. 43 Abs. 2 lit. b AI Act) anerkannt werden können.
- Sie gelten als **Beweismittel für Konformität** im Streit- oder Auditfall.

7.3 Ablauf der CE-Kennzeichnung (Art. 49 AI Act)

Nach erfolgreichem Abschluss der Konformitätsbewertung stellt der Anbieter eine **schriftliche EU-Konformitätserklärung** aus.
Sie bestätigt, dass das KI-System **alle einschlägigen Anforderungen der Verordnung** erfüllt.
Erst danach darf die **CE-Kennzeichnung** angebracht werden – sie gilt als sichtbarer Nachweis der Regelkonformität und Marktfreigabe innerhalb der EU.

Schritte zur CE-Kennzeichnung

© A4Q Copyright 2025

Schritt	Inhalt / Begründung
1. Abschluss der Konformitätsbewertung (intern oder extern)	Nachweis, dass das System die Anforderungen der Artikel 9–15 erfüllt. Grundlage ist das vollständige technische Dossier gemäß Anhang IV.
2. Erstellung und Unterzeichnung der EU-Konformitätserklärung (Art. 48)	Rechtlich bindende Erklärung des Anbieters, dass das System konform ist. Sie muss Name, Systemidentifikation, angewandte Standards und Datum enthalten.
3. Anbringung des CE-Zeichens	Das CE-Symbol darf erst nach der Erklärung angebracht werden – auf der Benutzeroberfläche, Verpackung oder Dokumentation, je nach Systemtyp.
4. Registrierung in der EU-Datenbank für Hochrisiko-KI-Systeme (Art. 71)	Pflichtschritt vor dem Inverkehrbringen. Der Eintrag enthält Anbieter, Systemzweck, Risikokategorie, ggf. Notified Body und Datum der Konformitätserklärung.
5. Aufbewahrung der Dokumentation für mindestens 10 Jahre (Art. 50)	Langzeitnachweis für Marktaufsicht, Audits und Haftungsfälle. Gilt auch bei Systemabschaltung oder Betreiberwechsel.

Wichtiger Hinweis

- Die CE-Kennzeichnung gilt **nur für die geprüfte Systemversion** in ihrer **bewerteten Konfiguration**.
- **Wesentliche Änderungen** – etwa neue Trainingsdaten, geänderte Modelle, Einsatz in neuen Domänen oder Integration in andere Produkte – **lösen zwingend eine erneute Konformitätsbewertung** aus.
- Der Anbieter muss prüfen, ob die Änderung als „wesentlich“ im Sinne von **Art. 43 Abs. 4** gilt.

7.4 Rolle der benannten Stellen (Notified Bodies)

Benannte Stellen werden von den **Mitgliedstaaten der EU** akkreditiert und anschließend von der **Europäischen Kommission im NANDO-Register (New Approach Notified and Designated Organisations)** veröffentlicht.
Sie sind für die **Durchführung externer Konformitätsbewertungsverfahren** bei Hochrisiko-KI-Systemen zuständig, wenn eine interne Bewertung nicht ausreicht oder gesetzlich ausgeschlossen ist.

© A4Q Copyright 2025

Aufgaben und Prüfbereiche:

- Bewertung des **Risikomanagement- und Qualitätssystems** des Anbieters
- **Stichprobenprüfung** der technischen Dokumentation und Prüfberichte
- Bewertung von **Test- und Validierungsergebnissen** auf Plausibilität
- Durchführung von **Audits vor Ort** bei Hersteller oder Betreiber
- Ausstellung einer **EU-Baumusterprüfbescheinigung** als Grundlage der CE-Kennzeichnung

Beispiele benannter Stellen (EU-weit):

- **TÜV Rheinland**, **DEKRA** (Deutschland)
- **Bureau Veritas**, **SGS** (Frankreich/Schweiz, EU-weit anerkannt)
- **Applus+ Laboratories** (Spanien)
- **IMQ S.p.A.** (Italien)
- **VTT Expert Services Ltd** (Finnland)

Alle benannten Stellen, die im **NANDO-Verzeichnis der Europäischen Kommission** gelistet sind, können EU-weit tätig werden.

Die Auswahl hängt vom **Akkreditierungsumfang** und dem **betroffenen Sektor** (z. B. Biometrie, Medizin, kritische Infrastrukturen) ab.

7.5 Eintrag in die EU-Datenbank für Hochrisiko-KI-Systeme (Art. 71)

Bevor ein Hochrisiko-KI-System in Verkehr gebracht oder in Betrieb genommen werden darf, **muss es in der zentralen EU-Datenbank für KI-Systeme registriert werden.**
Diese Registrierung ist verpflichtend und gilt als **offizieller Nachweis**, dass das System ein Konformitätsverfahren erfolgreich durchlaufen hat.

Einzutragende Informationen:

- **Name und Kontaktdaten des Anbieters** (Hersteller oder Inverkehrbringer)
- **Bezeichnung und Beschreibung des KI-Systems**, einschließlich seines **Zwecks und Einsatzbereichs**
- **Risikokategorie** des Systems und **Verweis auf den relevanten Abschnitt des Anhangs III**
- **Art des Konformitätsverfahrens** (interne oder externe Bewertung nach Art. 43)

© A4Q Copyright 2025

- **Angabe der benannten Stelle**, falls eine externe Prüfung erfolgt ist
- **Datum und Referenznummer** der **EU-Konformitätserklärung** sowie der **CE-Kennzeichnung**

Zweck der Datenbank:
Die EU-Datenbank dient der **Transparenz, Marktüberwachung und Nachvollziehbarkeit**.
Sie ermöglicht es:

- **Behörden**, die Konformität und Marktaufsicht effizient zu prüfen,
- **Unternehmen und Kund:innen**, sich über zugelassene KI-Systeme zu informieren,
- und der **Öffentlichkeit**, nachvollziehen zu können, welche Hochrisiko-KI-Systeme im EU-Raum eingesetzt werden.

Die Registrierung erfolgt **elektronisch über das EU-Portal**, das von der **Europäischen Kommission** betrieben wird.
Nur nach erfolgreicher Eintragung darf das System mit CE-Kennzeichnung **in Verkehr gebracht** oder **vermarktet** werden.

7.6 Umgang mit wesentlichen Änderungen (Art. 43 Abs. 4)

Ein KI-System gilt **nur in der Form als konform**, in der es ursprünglich bewertet und CE-gekennzeichnet wurde.
Wenn das System nach der Konformitätsbewertung **wesentlich verändert** wird, muss eine **erneute Konformitätsbewertung** durchgeführt werden, bevor es weiter eingesetzt oder erneut vermarktet werden darf.

Als wesentliche Änderung gelten insbesondere:

- **Änderung des vorgesehenen Zwecks** oder der **Funktionslogik**, z. B. wenn ein KI-System nicht mehr zur Bewerberauswahl, sondern zur Leistungsbewertung eingesetzt wird.
- **Verwendung neuer Trainings- oder Validierungsdaten**, deren Qualität, Repräsentativität oder Bias-Struktur nicht dokumentiert oder geprüft wurde.
- **Anpassung der Systemarchitektur oder Integration in neue Software- oder Hardwareplattformen**, die Einfluss auf das Verhalten, die Sicherheit oder die Leistung des Systems haben.
- **Einsatz in einer anderen Anwendungsdomäne oder Rechtsumgebung**, z. B. Übertragung eines HR-Screening-Systems auf medizinische Eignungsprüfungen.

© A4Q Copyright 2025

Verantwortlichkeit:
Die Prüfung, ob eine Änderung als „wesentlich“ einzustufen ist, liegt beim **Anbieter** (Hersteller oder Inverkehrbringer).
Er muss dokumentieren,

- welche Änderungen vorgenommen wurden,
- ob sie das Risiko-, Daten- oder Funktionsprofil beeinflussen,
- und welche Nachweise ggf. für eine erneute Bewertung erforderlich sind.

Praxisempfehlung:
Unternehmen sollten ein **Änderungsmanagement-Verfahren** einführen, das technische Anpassungen, neue Trainingsläufe oder Funktionserweiterungen automatisch auf mögliche Relevanz für die Konformität prüft.
So lassen sich unbeabsichtigte Regelverstöße und Audit-Risiken frühzeitig vermeiden.

7.7 Verbindung zu Qualitäts- und Managementsystemen

Der **EU AI Act** sieht eine sogenannte **„Presumption of Conformity“** (Vermutung der Konformität) vor: Wenn ein Unternehmen bei Entwicklung, Betrieb und Überwachung seines KI-Systems **harmonisierte europäische oder internationale Standards** anwendet, wird **vermutet**, dass das System die entsprechenden **rechtlichen Anforderungen** des AI Act erfüllt.
Das erleichtert Nachweise im Konformitätsverfahren und beschleunigt die CE-Kennzeichnung.

Relevante Standards und Managementsysteme:

- **ISO/IEC 42001:2023 – AI Management System (AIMS)**
  Struktur für Aufbau, Betrieb und Überwachung eines KI-Managementsystems.
- **ISO/IEC 23894:2023 – AI Risk Management**
  Rahmen für systematisches KI-Risikomanagement im Einklang mit Art. 9 AI Act.
- **ISO/IEC 27001:2022 / 27701:2019 – Informations- und Datenschutzmanagement**
  Nachweis der Sicherheit und Vertraulichkeit von Daten gemäß Art. 10 und 15.
- **DIN SPEC 92001-1/-2:2020/2021 – Qualitätsanforderungen an KI-Systeme**
  Nationale Leitlinie für Dokumentation, Test und Auditvorbereitung.

Vorteil für Unternehmen:
Die Anwendung dieser Normen schafft **Struktur und Nachvollziehbarkeit**,

- erleichtert **Audits und Marktaufsicht**,
- reduziert **Interpretationsspielräume** bei benannten Stellen,

© A4Q Copyright 2025

- und kann die **CE-Kennzeichnung beschleunigen**.

.

7.8 Praxisbeispiel: Konformitätsroute eines HR-Screening-Tools

Dieses Beispiel zeigt den typischen Ablauf einer **Konformitätsbewertung für ein Hochrisiko-System** im Personalwesen – etwa ein KI-gestütztes Tool zur automatisierten Vorauswahl von Bewerber:innen.
Das System fällt unter **Anhang III Nr. 4 (Beschäftigung, Arbeitsverwaltung)** des EU AI Act und erfordert daher eine **formelle Konformitätsbewertung** und **CE-Kennzeichnung**.

Ablauf der Konformitätsroute

Schritt	**Ziel / Inhalt**	**Verantwortung im Unternehmen**	**Erforderliches Dokument / Nachweis**
1. Risikobewertung (Art. 6–9)	Identifikation, ob das System als Hochrisiko-Anwendung einzustufen ist, und Beschreibung potenzieller Auswirkungen auf Grundrechte und Fairness.	**AI Compliance Manager** in Abstimmung mit Datenschutz und HR	**Risikobericht** (inkl. Einstufungsbegründung, Anhang III-Bezug)
2. Implementierung des Risikomanagements (Art. 9)	Einrichtung eines kontinuierlichen Prozesses zur Risikoüberwachung, Definition von Gegenmaßnahmen und Prüfmechanismen.	**Entwicklungsteam** gemeinsam mit **Qualitätsmanagement**	**Risikoregister** mit Maßnahmenmatrix und Verantwortlichkeiten
3. Erstellung der technischen Dokumentation (Art. 11, Anhang IV)	Vollständige Dokumentation des Systems, Datenquellen, Trainingsprozesse, Testprotokolle, Human Oversight Mechanismen.	**Fachbereich HR + Qualitätssicherung**	**Technisches Dossier** nach Anhang IV

© A4Q Copyright 2025

Schritt	Ziel / Inhalt	Verantwortung im Unternehmen	Erforderliches Dokument / Nachweis
4. Interne Konformitätsbewertung (Art. 43 Abs. 2)	Prüfung der Vollständigkeit und Nachweise im Dossier, interne Auditierung und Erstellung des Konformitätsberichts.	**AI Officer / Compliance Team**	**Interner Konformitätsbericht** mit Prüfergebnissen
5. Erstellung und Unterzeichnung der EU-Konformitätserklärung (Art. 48)	Formelle Bestätigung, dass das System alle Anforderungen (Art. 9–15) erfüllt.	**Geschäftsführung / Legal Representative**	**EU-Konformitätserklärung** (rechtlich verbindlich)
6. Registrierung in der EU-Datenbank (Art. 71)	Offizieller Eintrag in das EU-Portal für Hochrisiko-KI-Systeme, Voraussetzung für Inverkehrbringen.	**AI Officer / Compliance**	**Registrierungsformular** mit System-ID, CE-Nummer, Risikokategorie
7. Anbringung des CE-Zeichens (Art. 49)	Sichtbarer Nachweis der Konformität auf Produkt, Benutzeroberfläche oder Begleitdokumentation.	**Produktmanagement**	**CE-Label + Begleitunterlagen**
8. Jährliches Audit / Review (Art. 61, Post-Market Monitoring)	Überprüfung, ob das System weiterhin konform betrieben wird (z. B. bei Updates, neuen Daten, Prozessänderungen).	**Qualität & Compliance / interne Audit-Funktion**	**Audit-Report** + Aktualisiertes Risikoregister

B. Lernrelevante Erkenntnisse

- Die **Verantwortung liegt beim Anbieter**, auch wenn einzelne Aufgaben intern verteilt sind.
- Die **Dokumentationskette** (Risiko → Maßnahmen → Bewertung → Erklärung → Audit) muss **lückenlos** und **prüfbar** sein.
- **Regelmäßige Reviews** sind notwendig, da sich Systeme durch Retraining oder Software-Änderungen weiterentwickeln.

© A4Q Copyright 2025

- Die Einhaltung dieser Schritte ermöglicht die **rechtssichere CE-Kennzeichnung** und schützt das Unternehmen vor Haftungs- und Reputationsrisiken.

7.9 Handlungsempfehlungen für die Praxis

Damit die Konformitätsbewertung effizient, nachvollziehbar und auditfest durchgeführt werden kann, sollten Unternehmen einige **bewährte Vorgehensweisen** beachten.
Diese Empfehlungen unterstützen die **dauerhafte Aufrechterhaltung der CE-Konformität** und reduzieren Haftungs- und Auditrisiken.

1. **Frühzeitige Einbindung von Rechts- und Compliance-Abteilungen**
   Bereits in der Planungsphase eines KI-Projekts sollten juristische und Compliance-Expert:innen eingebunden werden.
   So lassen sich Risikoklasse, Datenanforderungen und Dokumentationspflichten frühzeitig korrekt festlegen.

2. **Pflege einer Checkliste zur Konformitätsbewertung (Art. 9–23 AI Act)**
   Eine standardisierte Prüfliste hilft, alle erforderlichen Nachweise (Risikomanagement, Datenqualität, Human Oversight usw.) systematisch zu erfassen und Lücken rechtzeitig zu erkennen.

3. **Verknüpfung mit bestehenden Managementsystemen**
   Die Integration der KI-Compliance-Prozesse in vorhandene Systeme wie **Qualitätsmanagement (ISO 9001)**, **Informationssicherheits-Management (ISO/IEC 27001)** oder **AI Management System (ISO/IEC 42001)** schafft Synergien, reduziert Doppelaufwand und erleichtert Audits.

4. **Regelmäßige interne Audits zur CE-Konformität**
   Durch interne Audits können Änderungen, Schwachstellen oder Abweichungen frühzeitig erkannt werden.
   Dokumentierte Auditberichte sind zugleich wertvolle Nachweise für Behörden- und Zertifizierungsprüfungen.

5. **Einrichtung eines zentralen Dokumentenregisters mit Versionierung und Audit-Trail**
   Alle Dokumente zur Konformität (Risiko-, Prüf-, Test- und Freigabenachweise) sollten in einem kontrollierten Repository verwaltet werden.
   Versionierung und Änderungsprotokolle gewährleisten Nachvollziehbarkeit und Beweiskraft bei Audits.

© A4Q Copyright 2025

© A4Q Copyright 2025

8 Transparenzpflichten für Limited-Risk-Systeme (Art. 52 EU AI Act)

⏱ Unterrichtszeit: 90 Minuten

🎯 **Business Outcomes (BOs)**

- **BO 8.1:** Teilnehmende sind vorbereitet, Transparenzanforderungen für Chatbots, Emotionserkennung und Deepfakes anzuwenden.
- **BO 8.2:** Teilnehmende erwerben Kompetenz, Kennzeichnungssysteme im Interface-Design zu bewerten und anzupassen.

Lernziele (Learning Objectives – LO)

- **LO 8.1 (K2):** Teilnehmende können die Transparenzanforderungen nach Art. 52 EU AI Act erklären und deren Bedeutung für Limited-Risk-Systeme darstellen.
- **LO 8.2 (K2):** Teilnehmende können Unterschiede zwischen Hochrisiko-Transparenz (Art. 13 f.) und begrenztem Risiko (Art. 52) erläutern.
- **LO 8.3 (K3):** Teilnehmende können geeignete Interface-Kennzeichnungen und Nutzerhinweise gestalten, um Transparenzpflichten praktisch umzusetzen.
- **LO 8.4 (K3):** Teilnehmende können bestehende Systeme (z. B. Chatbots, Emotionserkennung, generative Medien) auf Einhaltung der Kennzeichnungspflichten prüfen.
- **LO 8.5 (K1):** Teilnehmende kennen die grundlegenden Transparenzpflichten für Systeme mit begrenztem Risiko und verstehen deren Zielsetzung zur Stärkung von Nutzervertrauen.

Wichtige Begriffe:
Begrenztes Risiko, Transparenzpflicht, Kennzeichnungspflicht, Interaktion mit Menschen, Chatbot-Hinweis, Emotionserkennung, Deepfake-Kennzeichnung, Informationspflicht, Verbraucherschutz, Accountability, Dokumentationsnachweis.

Einleitung

Limited-Risk-Systeme, wie Chatbots, Emotionserkennung oder Deepfake-Generatoren, sind nach dem EU AI Act grundsätzlich zulässig, unterliegen aber besonderen Informations- und Kennzeichnungspflichten (Art. 52).

© A4Q Copyright 2025

Der Zweck dieser Vorschrift besteht darin, Nutzerinnen und Nutzer vor Täuschung zu schützen und sicherzustellen, dass sie jederzeit erkennen können, wenn sie mit einem KI-System interagieren oder KI-erzeugte Inhalte konsumieren.

Transparenz ist damit kein freiwilliger ethischer Standard, sondern eine **verbindliche Compliance-Anforderung**, die in der Benutzeroberfläche und in der Kommunikation des Systems sichtbar umgesetzt werden muss.

Hinweis: Einstufung von Emotionserkennung und biometrischer Kategorisierung

Emotionserkennungs- und biometrische Kategorisierungssysteme sind **nicht automatisch Limited-Risk-Systeme**.
Ihre Risikostufe hängt vom **Einsatzkontext und den Auswirkungen auf betroffene Personen** ab:

- **Limited-Risk (Art. 52 Abs. 2 AI Act):**
  Wenn die Erkennung ausschließlich zu Informations- oder Komfortzwecken erfolgt (z. B. Stimmungserkennung in Fahrzeugen, Service-Chatbots zur Freundlichkeitsanalyse), gilt die Transparenzpflicht – jedoch **keine Zulassungs- oder CE-Pflicht**.
- **High-Risk (Art. 6 i. V. m. Anhang III):**
  Sobald die Emotionserkennung oder biometrische Kategorisierung Einfluss auf **Entscheidungen über Bildung, Beschäftigung, Zugang zu Dienstleistungen oder Sicherheit** hat, wird sie als **Hochrisiko-KI-System** eingestuft.
  In diesen Fällen gelten die erweiterten Pflichten aus **Art. 9–24** (Risikomanagement, Dokumentation, Human Oversight, CE-Kennzeichnung).
- **Unzulässig (Art. 5 Abs. 1 lit. a–b):**
  Der Einsatz ist **verboten**, wenn emotionale Zustände ausgenutzt werden, um Menschen unbemerkt zu manipulieren oder besonders schutzbedürftige Gruppen (z. B. Kinder) zu beeinflussen.

8.1 Artikel 52 EU AI Act – Transparenzpflichten

Artikel 52 legt drei zentrale Pflichten fest:

Pflichtenbereich	Beschreibung	Beispiele
a) Interaktionserkennung	Personen müssen erkennen können, dass sie mit einem KI-System interagieren.	Chatbots, Voicebots, virtuelle Assistenten

© A4Q Copyright 2025

Pflichtenbereich	Beschreibung	Beispiele
b) Emotionserkennung & biometrische Kategorisierung	Nutzer müssen informiert werden, wenn ihre Emotionen oder Merkmale analysiert werden.	Kamera-basierte Kundenerkennung, Stimm- oder Blickanalyse
c) Deepfakes & KI-generierte Medien	KI-erzeugte oder manipulierte Inhalte müssen eindeutig als solche gekennzeichnet werden.	KI-Videos, synthetische Stimmen, Bilder

Ziel: **Vermeidung von Täuschung, Förderung von Vertrauen und Schutz der Grundrechte.**

8.2 Anwendungsbereiche und Kennzeichnungspflichten

Die praktischen Anforderungen an Transparenz und Kennzeichnung unterscheiden sich je nach Typ des KI-Systems.
Artikel 52 verpflichtet Anbieter und Betreiber insbesondere in den drei folgenden Anwendungsbereichen zu klaren, für Nutzende verständlichen Hinweisen und Kennzeichnungen.

a) Chatbots und Voicebots

Chatbots und sprachbasierte Assistenten gelten als Limited-Risk-Systeme, sofern sie keine Entscheidungen mit rechtlichen oder wirtschaftlichen Auswirkungen treffen. Sie unterliegen der Informationspflicht gemäß Art. 52 Abs. 1 AI Act.
Ziel ist, sicherzustellen, dass Nutzende jederzeit erkennen können, dass sie mit einem KI-System interagieren.

Empfohlene Umsetzungsmaßnahmen:

- **Deutliche Offenlegung der KI-Interaktion** beim Start der Kommunikation, z. B. durch Hinweis: *„Sie sprechen mit einem KI-basierten Assistenten."*
- **Wiederholte Erinnerung** bei längeren Dialogen oder Themenwechseln.
- **Option zum Opt-Out** bzw. Wechsel zu einem menschlichen Ansprechpartner.
- **Protokollierung der Nutzerinformation und Zustimmung** im System- oder Session-Log.

b) Emotionserkennungssysteme

© A4Q Copyright 2025

Systeme, die Mimik, Stimme oder physiologische Signale auswerten, um emotionale Zustände zu erkennen, fallen unter Art. 52 Abs. 2 AI Act.
Sie dürfen nur eingesetzt werden, wenn Nutzende zuvor eindeutig informiert wurden und eine rechtmäßige Grundlage (z. B. Einwilligung oder berechtigtes Interesse) besteht.

Eine rechtmäßige Grundlage bedeutet, dass die Verarbeitung personenbezogener Daten – insbesondere biometrischer oder sensibler Informationen – mit den Vorgaben der **Datenschutz-Grundverordnung (DSGVO)** im Einklang steht. Dies kann zum Beispiel erfolgen durch:

- **Einwilligung (Art. 6 Abs. 1 lit. a DSGVO):**
  Die betroffene Person stimmt der Emotionserkennung ausdrücklich und freiwillig zu, nachdem sie über Zweck und Umfang der Verarbeitung informiert wurde.
- **Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):**
  Der Einsatz dient einem klaren, nachvollziehbaren Zweck (z. B. Verbesserung der Servicequalität), ohne die Rechte der betroffenen Personen zu beeinträchtigen. In diesem Fall ist eine **Interessenabwägung** und gegebenenfalls eine ergänzende **Datenschutz-Folgenabschätzung (DSFA)** erforderlich.

Fehlt eine dieser rechtlichen Voraussetzungen, darf das System **nicht eingesetzt oder aktiviert** werden.

Erforderliche Transparenzmaßnahmen:

- **Vorabinformation** über Zweck, Art und Umfang der Datenauswertung, z. B.:
  „Dieses System analysiert Mimik und Stimme, um Emotionen zu erkennen.“
- **Verbot verdeckter Analyse** ohne ausdrückliche Zustimmung der betroffenen Person.
- **Speicherung von Emotionsergebnissen** nur, wenn sie technisch notwendig und rechtlich zulässig ist.
- **Transparente Darstellung der Bewertungsskalen**, etwa durch Angabe von Wahrscheinlichkeiten:
  „Wahrscheinlichkeit positiver Emotion = 73 %.“

Hinweis: Wird Emotionserkennung in sensiblen Kontexten (z. B. Beschäftigung, Bildung, Strafverfolgung) eingesetzt, kann sie gemäß **Art. 6 i. V. m. Anhang III** als **Hochrisiko-KI** eingestuft werden.

c) Deepfakes und generative Medien

Bei KI-erzeugten oder KI-veränderten Inhalten (z. B. Bilder, Videos, Audio) greift Art. 52 Abs. 3 AI Act.
Ziel ist, Täuschung zu vermeiden und die Herkunft der Inhalte eindeutig kenntlich zu machen.

© A4Q Copyright 2025

Erforderliche Kennzeichnungsmaßnahmen:

- **Sichtbare Overlays oder Textmarkierungen** wie *„KI-generiert“*, *„synthetische Darstellung“* oder *„erstellt mit Künstlicher Intelligenz“*.
- **Maschinenlesbare Kennzeichnung** in den Dateimetadaten (z. B. IPTC/XMP-Tag ai-generated=true).
- **Verantwortung** für korrekte Kennzeichnung liegt sowohl bei den **Erstellenden** als auch bei den **Verbreitenden** (z. B. Marketing- oder Medienagenturen).
- **Ausnahmen** gelten nur für genehmigte Einsätze im Bereich **öffentlicher Sicherheit oder Strafverfolgung** gemäß Art. 52 Abs. 3 Unterabsatz 2.

8.3 Gestaltungsempfehlungen für Interface-Design und Kennzeichnung

Zur Umsetzung der Transparenzpflichten nach **Artikel 52 EU AI Act** müssen Hinweise auf KI-generierte Inhalte oder Interaktionen so gestaltet werden, dass sie von allen Nutzerinnen und Nutzern eindeutig wahrgenommen, verstanden und technisch nachvollzogen werden können.
Die nachstehende Übersicht zeigt zentrale **Gestaltungsprinzipien** für rechtssichere und nutzerfreundliche Kennzeichnungen im Interface-Design.

Prinzip	**Beschreibung**	**Beispiel im UI-Design**
Sichtbarkeit	Kennzeichnungen müssen für Nutzerinnen und Nutzer unmittelbar erkennbar sein, ohne dass sie aktiv danach suchen müssen.	Label *„KI-Antwort“* oberhalb des Chatverlaufs; Wasserzeichen *„KI-generiert“* in Bildern oder Videos.
Verständlichkeit	Formulierungen sollen klar, laienverständlich und kulturneutral sein, um Missverständnisse zu vermeiden.	Hinweistext: *„Dieser Text wurde automatisch durch ein KI-System erstellt.“*
Konsistenz	Kennzeichnungen müssen in allen Anwendungen einheitlich gestaltet sein, um Wiedererkennung und Vertrauen zu fördern.	Einheitlicher Hinweisstil und Wortlaut auf Website, in App und E-Mail-Bot.
Dauerhaftigkeit	Hinweise müssen über die gesamte Interaktion sichtbar bleiben und dürfen nicht automatisch ausgeblendet werden.	Sichtbarer Footer-Hinweis oder fixiertes Label während des gesamten Dialogs.

© A4Q Copyright 2025

Prinzip	Beschreibung	Beispiel im UI-Design
Maschinenlesbarkeit	Transparenzkennzeichnungen sollen zusätzlich in maschinenlesbarer Form implementiert werden, um Nachvollziehbarkeit und Interoperabilität zu sichern.	HTML-Metatag: <meta name="AI-content" content="true"> oder IPTC/XMP-Metadatenfeld *ai-generated = true*.
Barrierefreiheit	Kennzeichnungen müssen für alle Nutzergruppen zugänglich sein, einschließlich Personen mit Seh- oder Hörbeeinträchtigungen.	ARIA-Label oder Screenreader-Ausgabe: *„KI-generierte Antwort“* bzw. *„AI-generated content“*.

Praktischer Tipp:
Kennzeichnung sollte **in der Designphase** berücksichtigt werden – nicht nachträglich als rechtlicher Zusatz. Das UX- und Legal-Team sollte gemeinsam ein internes **Kennzeichnungs-Pattern-Set** entwickeln (z. B. für Buttons, Labels, Banner).

8.4 Organisatorische Umsetzung im Unternehmen

Die Einhaltung der Transparenzpflichten nach **Artikel 52 EU AI Act** erfordert nicht nur technische, sondern auch organisatorische Maßnahmen.
Unternehmen sollten klare Verantwortlichkeiten, standardisierte Verfahren und nachvollziehbare Nachweise etablieren, um eine rechtskonforme und konsistente Kennzeichnung sicherzustellen.

Empfohlene Umsetzungsschritte:

1. **Inventarisierung von KI-Systemen**
   Erfassen Sie alle Systeme, die mit Nutzerinnen und Nutzern interagieren oder mediale Inhalte erzeugen (z. B. Chatbots, Sprachassistenten, generative Tools).
   Ziel ist eine vollständige Übersicht, um Transparenzpflichten systematisch zuzuordnen.

2. **Risikoprüfung**
   Analysieren Sie für jedes System, ob ein Täuschungs-, Vertrauens- oder Grundrechtsrisiko besteht.
   Diese Bewertung bildet die Grundlage für die Einstufung als Limited-Risk oder High-Risk nach Artikel 6 AI Act.

© A4Q Copyright 2025

3. **Kennzeichnungsrichtlinie**
   Entwickeln Sie interne Standards für Text-, Farb- und Metadaten-Labels, um eine einheitliche und nachvollziehbare Kennzeichnung zu gewährleisten.
   Diese Richtlinie sollte Bestandteil des UX-Design-Systems oder der Corporate-Design-Guidelines sein.

4. **Freigabeprozess**
   Veröffentlichen Sie KI-gestützte Anwendungen oder Inhalte erst nach einer Sichtprüfung durch die zuständige **Compliance-Abteilung** oder den **AI Compliance Officer**.
   Der Freigabeprozess stellt sicher, dass Transparenzhinweise vollständig und korrekt umgesetzt sind.

5. **Audit- und Nachweisdokumentation**
   Erfassen Sie Belege zur Einhaltung der Transparenzpflichten, z. B. Screenshots der Benutzeroberfläche, technische Dokumentation, Logfiles und Versionsstände.
   Diese Nachweise dienen als Audit-Trail und ermöglichen eine revisionssichere Prüfung.

6. **Schulung und Sensibilisierung**
   Schulen Sie Designer:innen, Entwickler:innen und Marketing-Teams regelmäßig zu den Transparenzanforderungen nach Artikel 52 AI Act.
   Ziel ist ein gemeinsames Verständnis von rechtlichen Pflichten, UX-Verantwortung und Compliance-Nachweispflichten.

8.5 Typische Fehler und Compliance-Risiken

In der Praxis treten bei der Umsetzung der Transparenzpflichten häufig wiederkehrende Fehler auf.
Die folgende Übersicht zeigt typische Risiken, deren Auswirkungen sowie geeignete Gegenmaßnahmen zur Sicherstellung der Compliance nach **Artikel 52 EU AI Act**.

Risiko	Beschreibung	Empfohlene Gegenmaßnahme
Fehlende Kennzeichnung	Nutzerinnen und Nutzer erkennen nicht, dass sie mit einem KI-System interagieren.	Deutliche und dauerhaft sichtbare UI-Hinweise (z. B. Label „KI-Antwort“) oder akustische Ankündigung bei Sprachsystemen.
Unverständliche Formulierungen	Hinweise verwenden unklare, technische oder juristische Sprache und werden dadurch nicht verstanden.	Durchführung eines **UX-Reviews** auf Verständlichkeit und kulturelle Neutralität der Formulierungen.

© A4Q Copyright 2025

Risiko	Beschreibung	Empfohlene Gegenmaßnahme
Fehlende Metadaten	Inhalte sind visuell als KI-generiert markiert, jedoch nicht maschinenlesbar gekennzeichnet.	Integration der Kennzeichnung in technische Metadaten (z. B. IPTC/XMP, JSON-LD oder HTML-Metatag).
Unvollständige Protokollierung	Die Umsetzung der Transparenzpflichten ist im Audit nicht nachweisbar.	Einsatz eines Logging-Systems mit Zeitstempel, Hashwert und Versionierung zur revisionssicheren Dokumentation.
Emotionserkennung ohne Information	Das System analysiert Emotionen oder biometrische Daten ohne vorherige Nutzerinformation.	Klare **Vorabinformation** und ausdrückliche **Einwilligung** gemäß Art. 52 Abs. 2 AI Act sowie Datenschutzprüfung nach DSGVO.

8.6 Praxisbeispiel: Kennzeichnung generativer Inhalte im Marketing

Ein mittelständisches Unternehmen setzt ein **Large Language Model (LLM)** ein, um automatisch Produktbeschreibungen für den Online-Shop zu generieren.
Die Texte werden nach redaktioneller Prüfung direkt auf der Website veröffentlicht.

Fehler:
Die Veröffentlichung erfolgt ohne Hinweis darauf, dass die Inhalte von einer KI erstellt wurden.
Dadurch entsteht für Kundinnen und Kunden der Eindruck, die Texte seien vollständig manuell verfasst.
Dies stellt einen Verstoß gegen die **Transparenzpflicht nach Artikel 52 Absatz 1 des EU AI Act** dar, da die Interaktion mit einem KI-System bzw. die Nutzung KI-generierter Inhalte nicht erkennbar ist.

Korrekturmaßnahmen:
Um die gesetzlichen Anforderungen zu erfüllen und das Vertrauen der Kundschaft zu stärken, wurden folgende Schritte umgesetzt:

1. **Sichtbarer Hinweis im Footer:**
   Unter jedem automatisch generierten Text erscheint der Vermerk:
   „Dieser Text wurde mithilfe Künstlicher Intelligenz erstellt.“
   Dadurch erkennen Nutzerinnen und Nutzer klar, dass eine KI an der Erstellung beteiligt war.

2. **Maschinenlesbare Kennzeichnung im Quellcode:**
   In den Metadaten der Webseite wird ein Hinweis ergänzt, der die KI-Generierung technisch nachvollziehbar macht: <meta name="ai-generated" content="true">. Diese Information ermöglicht

© A4Q Copyright 2025

eine transparente Verarbeitung und unterstützt künftige Prüfungen oder automatisierte Erkennungssysteme.

3. **Interner Nachweis im Dokumentationsregister:**
   Für alle automatisch erzeugten Inhalte wird ein Eintrag im **Dokumentenregister** angelegt.
   Dieser enthält Datum, Systemversion, verantwortliche Person und Kontrollvermerk der Compliance-Abteilung.
   So lässt sich die Kennzeichnung im Auditfall eindeutig belegen.

Ergebnis:
Durch die Umsetzung dieser Maßnahmen erfüllt das Unternehmen die **Transparenzanforderungen nach Artikel 52 Absatz 1 EU AI Act**.
Zudem werden **Vertrauen und Glaubwürdigkeit** gegenüber Kundinnen und Kunden gestärkt.
Der dokumentierte Kennzeichnungsprozess schafft einen **klaren Audit-Trail** und erhöht die **Rechtssicherheit** bei der Nutzung generativer KI im Marketing.

.

8.7 Empfehlungen für die Praxis

Die Einhaltung der Transparenzpflichten nach **Artikel 52 EU AI Act** erfordert sowohl organisatorische als auch gestalterische Maßnahmen.
Neben rechtlicher Konformität steht dabei auch die **Vertrauensbildung gegenüber Nutzerinnen und Nutzern** im Mittelpunkt.
Die folgenden Empfehlungen unterstützen Unternehmen bei der praktischen Umsetzung einer nachhaltigen und überprüfbaren Transparenzstrategie:

1. **Entwicklung eines „AI-Transparency-Labeling Guide“**
   Integrieren Sie klare Vorgaben zur Kennzeichnung von KI-Interaktionen und KI-generierten Inhalten in Ihr bestehendes UX- und Corporate-Designsystem.
   Der Leitfaden sollte Textbausteine, Farbstandards, Platzierungen und technische Kennzeichnungsformate (z. B. Metadaten, Wasserzeichen) enthalten.
   Ziel ist eine einheitliche und überprüfbare Kennzeichnung über alle Anwendungen hinweg.

2. **Regelmäßige technische und funktionale Überprüfung**
   Kontrollieren Sie in festgelegten Intervallen, ob die Transparenzhinweise technisch korrekt ausgeliefert und wahrnehmbar sind.

© A4Q Copyright 2025

Nutzen Sie hierfür **A/B-Tests**, **Accessibility-Tests** und **User-Feedback**, um sicherzustellen, dass Hinweise verständlich, sichtbar und barrierefrei umgesetzt sind.

3. **Durchführung periodischer Transparenz-Audits**
   Überprüfen Sie insbesondere neue oder geänderte KI-Anwendungen, Marketing-Kampagnen oder Voice-Bots auf korrekte Kennzeichnung und Informationspflichten.
   Dokumentieren Sie die Ergebnisse in einem **Audit-Protokoll** und leiten Sie bei Bedarf **Corrective Actions** zur Verbesserung ein.

4. **Offene Kommunikation und Vertrauensaufbau**
   Kommunizieren Sie transparent über den Einsatz von KI – sowohl intern als auch extern. Offenheit gegenüber Kundinnen, Mitarbeitenden und Aufsichtsbehörden signalisiert Verantwortungsbewusstsein und stärkt das Vertrauen in KI-gestützte Systeme.
   Transparenz ist nicht nur eine gesetzliche Pflicht, sondern ein zentraler Bestandteil einer verantwortungsvollen **AI-Governance-Kultur**.

© A4Q Copyright 2025

9 General Purpose AI (GPAI) & Systemic Risk

⏱ **Unterrichtszeit:** 75 Minuten

🎯 **Business Outcomes:**

- **BO 9.1:** Teilnehmende verstehen die Bedeutung von General Purpose AI (GPAI) im Rahmen des EU AI Act und können die wichtigsten Pflichten der Anbieter nach Art. 53–55 einordnen und deren Relevanz für Anwenderorganisationen bewerten.
- **BO 9.2:** Teilnehmende sind befähigt, den Einsatz externer GPAI-Modelle (z. B. LLMs, generative Systeme) im eigenen Unternehmenskontext hinsichtlich Transparenz, Risiko und Compliance zu prüfen und entsprechende Handlungsempfehlungen abzuleiten.

Lernziele (Learning Objectives – LO)

- **LO 9.1 (K1):** Teilnehmende können den Begriff „General Purpose AI (GPAI)“ erläutern und zwischen Basismodellen und anwendungsspezifischen KI-Systemen unterscheiden.
- **LO 9.2 (K2):** Teilnehmende können die wesentlichen Pflichten der GPAI-Anbieter nach Art. 53 bis 55 EU AI Act benennen und deren Zielsetzung beschreiben.
- **LO 9.3 (K2):** Teilnehmende können die Relevanz dieser Pflichten für Anwenderorganisationen erklären, insbesondere in Bezug auf Transparenz, Risiko und Haftung.
- **LO 9.4 (K3):** Teilnehmende können im eigenen Unternehmenskontext ein Compliance-Review für externe GPAI-Modelle durchführen und geeignete Handlungsempfehlungen ableiten (z. B. Vertragsprüfung, Transparenz-Check, Monitoring).
- **LO 9.5 (K1):** Teilnehmende kennen den regulatorischen Rahmen für General-Purpose-Modelle und verstehen deren Bedeutung für den europäischen KI-Binnenmarkt.

Wichtige Begriffe:
General Purpose AI (GPAI), Systemic Risk, Frontier Model, AI Model Card, Red-Team-Testing, Model Governance, Provider-Pflichten, Open-Source-Modelle, Downstream Integration, Technische Dokumentation, Transparency Report, Incident Reporting.

Einführung: Von LLMs zu General Purpose AI

General Purpose AI (GPAI) – oft auch als **Basismodelle** oder **Foundation Models** bezeichnet – bilden die Grundlage zahlreicher moderner KI-Anwendungen.
Sie sind nicht auf eine einzelne Aufgabe spezialisiert, sondern können nachgelagert für viele Zwecke („downstream use“) angepasst werden – z. B. Text-, Bild- oder Code-Generierung, Analyse, Simulation oder Entscheidungsunterstützung.

© A4Q Copyright 2025

Beispiele: GPT-4/5 (OpenAI), Claude (Anthropic), Gemini (Google), LLaMA (Meta), Mistral AI.
Ihr Einfluss reicht von Chatbots über Wissenssysteme bis zu Behörden- und Bildungsanwendungen.

→ **Für Compliance-Verantwortliche** ergibt sich daraus eine neue Risikodimension: Auch wenn Unternehmen keine eigenen Modelle entwickeln, können sie als **Nutzer (Deployer)** oder **Integratoren (Provider downstream)** haftungsrelevant werden.

9.1 Rechtlicher Rahmen: Artikel 53 bis 55 EU AI Act

Die Artikel 53 bis 55 des EU AI Act regeln die besonderen Anforderungen an **General Purpose AI (GPAI)**, also an Basismodelle, die für vielfältige Zwecke eingesetzt oder weiterverwendet werden können. Diese Vorschriften schaffen Transparenz, Verantwortlichkeit und technische Nachvollziehbarkeit – sowohl für Anbieter als auch für Anwenderorganisationen, die solche Modelle integrieren.

Artikel	Inhaltliche Schwerpunkte	Relevanz für Anwenderorganisationen
Art. 53	Pflichten für GPAI-Anbieter – Transparenz, technische Dokumentation, Offenlegung der Trainingsdatenquellen, regelmäßige Evaluierungen sowie Sicherheits- und Robustheitsprüfungen.	Grundlage für Vertrauen in Basismodelle; wichtiges Auswahl- und Beschaffungskriterium für Unternehmen.
Art. 54	Systemic-Risk-Modelle – zusätzliche Pflichten für Modelle mit erheblichem Einfluss, großer Reichweite oder Marktdominanz, einschließlich Risikoanalysen und Sicherheitsbewertungen.	Relevanz für Organisationen, die marktführende Modelle einsetzen oder darauf aufbauen; ermöglicht fundierte Risikoabschätzungen.
Art. 55	Code of Practice – Förderung von Selbstregulierung und Standardisierung durch freiwillige Branchenleitlinien (z. B. Model Cards, Red-Team-Testing, Datenherkunftsberichte, Evaluierungsverfahren).	Praktische Orientierungshilfe für Due-Diligence-Prüfungen, Beschaffungsentscheidungen und interne Compliance-Prozesse.

Der EU AI Act unterscheidet dabei zwischen

- **GPAI-Anbietern** (z. B. Entwickler und Betreiber von Basismodellen wie OpenAI, Anthropic, Google oder Meta) und
- **nachgelagerten Anwendern bzw. Integratoren**, die diese Modelle über APIs, Plattformen oder eigene Systeme einsetzen.

© A4Q Copyright 2025

Auch Anwenderorganisationen sind verpflichtet, sicherzustellen, dass

- die verwendeten Modelle **konform mit den Artikeln 53 ff.** sind,
- **Risikobewertungen und Dokumentationen** durchgeführt und regelmäßig aktualisiert werden,
- die vom Anbieter bereitgestellten **Transparenz- und Sicherheitsinformationen** in die eigene technische Dokumentation und Governance-Prozesse einfließen.

9.2 Pflichten der GPAI-Anbieter

Die Anbieter von General Purpose AI (GPAI) tragen eine besondere Verantwortung für Transparenz, Sicherheit und Nachvollziehbarkeit ihrer Basismodelle. Der EU AI Act verpflichtet sie, technische, organisatorische und dokumentarische Nachweise zu erbringen, um die Integrität und Vertrauenswürdigkeit ihrer Modelle sicherzustellen.
Die folgende Übersicht fasst die zentralen Pflichtbereiche zusammen:

Pflichtbereich	**Beschreibung**	**Beispielhafte Nachweise**
Technische Dokumentation	Detaillierte Beschreibung der Systemarchitektur, der Trainingsmethoden, der verwendeten Datenquellen sowie der Evaluierungs- und Testverfahren. Ziel ist die Nachvollziehbarkeit von Aufbau, Funktionsweise und Grenzen des Modells.	*Model Card*, System- und Architektur-Dokumentation, technische Spezifikationen
Transparenzbericht	Offenlegung der verwendeten Datentypen und -kategorien, der eingesetzten Filtermechanismen sowie der bekannten Limitationen des Modells. Der Bericht dient der Information von Behörden, Geschäftspartnern und Anwenderorganisationen.	*Transparency Report*, *Data Summary* oder öffentlich zugänglicher Anbieterbericht
Evaluierung & Red-Team-Testing	Regelmäßige Prüfungen der Modelle auf Missbrauchsmöglichkeiten, Verzerrungen (Bias), Halluzinationen sowie sicherheitsrelevante Schwachstellen. Diese Prüfungen müssen dokumentiert und in den Verbesserungsprozess integriert werden.	Prüfberichte, *Penetration Tests*, Bias-Analysen, Red-Team-Reports

© A4Q Copyright 2025

Pflichtbereich	Beschreibung	Beispielhafte Nachweise
Copyright-Compliance	Nachweis der rechtmäßigen Nutzung urheberrechtlich geschützter Inhalte im Trainingsprozess. Dazu gehören Informationen über Lizenzen, Ausnahmeregelungen oder dokumentierte Fair-Use-Bewertungen.	Lizenznachweise, Urheberrechts-Erklärungen, rechtliche Einschätzungen
Systemic-Risk-Bewertung	Einschätzung, ob das Modell aufgrund seiner Größe, Reichweite oder Einflusskraft ein systemisches Risiko für Gesellschaft, Sicherheit oder demokratische Prozesse darstellen kann.	Interne *Risk Statements*, externe Impact Assessments
Code of Practice	Verpflichtung zur Einhaltung freiwilliger Branchenstandards und Leitlinien, z. B. der EU-weiten *Model Cards*-Initiative oder branchenspezifischer *Codes of Conduct*. Diese Selbstverpflichtungen gelten als Nachweis verantwortungsvoller Praxis.	Beitrittserklärung, *Adherence Statement*, Nachweis über Beteiligung an Standardisierungsgremien

Diese Pflichten gelten primär für die Anbieter von GPAI-Systemen, bilden jedoch zugleich eine **Orientierung für Anwenderorganisationen**, die solche Modelle einsetzen.
Unternehmen sollten prüfen, ob ihre Lieferanten diese Anforderungen nachweislich erfüllen und entsprechende Dokumente im Rahmen des eigenen Compliance- oder Beschaffungsprozesses einfordern.

Hinweis für Anwenderorganisationen

Auch wenn diese Pflichten primär für GPAI-Anbieter gelten, ergeben sich daraus **konkrete Handlungserfordernisse für Unternehmen**, die solche Modelle einsetzen oder integrieren:

- **Vertragliche Absicherung:** Verlangen Sie von Ihren Anbietern Nachweise über Transparenzberichte, Lizenzierung und Red-Team-Tests.
- **Dokumentationspflicht:** Integrieren Sie die erhaltenen Nachweise (z. B. Model Cards, Evaluierungsberichte) in Ihre eigene technische Dokumentation.
- **Risikoprüfung:** Bewerten Sie, ob die eingesetzten Basismodelle potenziell systemische oder ethische Risiken für Ihr Unternehmen oder Ihre Kundinnen und Kunden bergen.
- **Beschaffungsrichtlinie:** Verwenden Sie die Anforderungen der Artikel 53 bis 55 als verbindliche Auswahlkriterien bei der Integration externer Modelle.

© A4Q Copyright 2025

- **Transparenz gegenüber Dritten:** Machen Sie in internen und externen Richtlinien kenntlich, auf welchen GPAI-Modellen Ihre Systeme basieren.

9.3 Systemische Risiken & Governance

Systemische Risiken entstehen, wenn **Basismodelle (General Purpose AI)** in großem Umfang in kritischen Infrastrukturen, Medien, Verwaltungssystemen oder öffentlichen Diensten eingesetzt werden. Diese Modelle bilden häufig die Grundlage für zahlreiche nachgelagerte Anwendungen und können dadurch weitreichende Auswirkungen auf Sicherheit, Transparenz und gesellschaftliche Stabilität entfalten.

Typische Formen systemischer Risiken:

- **Abhängigkeit von wenigen globalen Anbietern („Concentration Risk“):** Die Dominanz einzelner GPAI-Entwickler führt zu technologischer und wirtschaftlicher Abhängigkeit.
- **Mangelnde Nachvollziehbarkeit von Trainingsdaten:** Fehlende Informationen über Datenquellen erschweren die Bewertung von Bias, Fairness und Urheberrecht.
- **Kaskadierende Fehler:** Ein fehlerhaftes Basismodell kann sich auf viele abgeleitete Systeme übertragen und deren Ergebnisse verfälschen.
- **Unsicherheit über Urheberrechte, Datenherkunft und Verzerrungen:** Unklare Datenherkunft kann rechtliche Risiken und Reputationsschäden verursachen.

Verantwortung der Anwenderorganisationen

Organisationen, die GPAI-Modelle einsetzen oder in eigene Anwendungen integrieren, müssen sicherstellen, dass sie:

- **nur konforme und geprüfte GPAI-Modelle** verwenden, deren Anbieter die Anforderungen der Artikel 53 bis 55 EU AI Act erfüllen,
- **eigene Risikobewertungen, Tests und Dokumentationen** durchführen – insbesondere in Bezug auf Bias, Robustheit und Urheberrechte,
- **klare Zuständigkeiten** im Rahmen ihres **AI-Governance-Systems** definieren (Rollen, Freigaben, Eskalationspfade),
- **Monitoring- und Auditprozesse** etablieren, um neue oder verstärkte Risiken frühzeitig zu erkennen,
- **Abhängigkeiten von einzelnen Anbietern** regelmäßig prüfen und gegebenenfalls Diversifizierungsstrategien entwickeln.

Empfohlene Maßnahmen für Unternehmen

© A4Q Copyright 2025

1. **Einrichtung eines GPAI-Risikoregisters:** Dokumentieren Sie sämtliche eingesetzten Basismodelle, Versionen, Anwendungsbereiche und bekannte Einschränkungen.
2. **Durchführung von Red-Team-Tests und Prompt-Audits:** Überprüfen Sie regelmäßig, wie Modelle auf unzulässige oder riskante Eingaben reagieren.
3. **Integration in das Enterprise Risk Management:** Verknüpfen Sie AI-Risiken mit bestehenden Risiko-, Datenschutz- und Compliance-Prozessen.
4. **Anbieterauswahl nach Compliance-Kriterien:** Berücksichtigen Sie Transparenzberichte, Model Cards und Code-of-Practice-Erklärungen bei der Beschaffung.
5. **Schulungen und Awareness-Programme:** Sensibilisieren Sie Mitarbeitende für systemische Risiken und verantwortungsvollen Umgang mit GPAI-Technologien.
6. **Frühwarnsysteme und Incident-Prozesse:** Melden und analysieren Sie Auffälligkeiten (z. B. unerwartete Modellantworten oder Datenlecks) strukturiert im Rahmen Ihres AI-Governance-Plans.

Fazit:
Systemische Risiken betreffen nicht nur technische Aspekte, sondern auch strategische und organisatorische Entscheidungen.
Ein strukturiertes Governance-System, das GPAI-Risikomanagement, Compliance und kontinuierliches Monitoring verbindet, bildet die Grundlage für eine vertrauenswürdige und nachhaltige Nutzung von General Purpose AI in Unternehmen.

9.4 Compliance-Prüfung externer GPAI-Modelle (Checkliste)

Auch wenn Unternehmen keine eigenen Basismodelle entwickeln, sind sie für die Auswahl und den Einsatz externer General Purpose AI (GPAI)-Modelle verantwortlich.
Eine strukturierte Compliance-Prüfung hilft, rechtliche und reputative Risiken frühzeitig zu erkennen und zu minimieren.
Die folgende Checkliste unterstützt Anwenderorganisationen bei der Bewertung externer GPAI-Modelle im Hinblick auf Transparenz, Sicherheit und Rechtskonformität.

Prüffeld	**Leitfragen**	**Empfohlene Nachweise**
Vertrag & Lizenz	Ist der Anbieter EU-konform zertifiziert oder registriert? Enthält der Vertrag spezifische Regelungen zu den Pflichten nach Artikel 53 ff. EU AI Act (z. B. Transparenz, technische Dokumentation, Sicherheitsprüfungen)?	*Service Level Agreement (SLA)*, *Data Processing Agreement (DPA)*, Compliance-Zertifikate, Anbieter-Selbsterklärung

© A4Q Copyright 2025

Prüffeld	Leitfragen	Empfohlene Nachweise
Transparenz	Werden die Trainingsdaten, Quellen, Filtermechanismen und bekannten Limitationen des Modells ausreichend dokumentiert?	*Model Card*, *Transparency Report*, öffentlich zugängliche Anbieterinformationen
Bias & Sicherheit	Liegen Evaluierungen, Red-Team-Tests oder unabhängige Audits zur Erkennung von Verzerrungen, Missbrauchsrisiken oder Sicherheitslücken vor?	Testberichte, Audit-Zusammenfassungen, Red-Team-Reports
Urheberrecht	Besteht das Risiko, dass urheberrechtlich geschützte Daten im Trainingsprozess verwendet wurden? Wurden Lizenzen oder rechtliche Bewertungen bereitgestellt?	Juristische Gutachten (*Legal Review*), Anbietererklärung, Nachweise über Lizenzierung
Verwendungszweck	Wie wird das Modell im eigenen Unternehmenskontext eingesetzt (z. B. Text- oder Bildgenerierung, Datenanalyse, Entscheidungsunterstützung)? Entspricht dieser Einsatz dem vorgesehenen Zweck des Anbieters?	Use-Case-Beschreibung, Data-Flow-Diagramm, interne Freigabeprotokolle
Monitoring	Wird der laufende Einsatz des Modells kontinuierlich überwacht? Gibt es Prozesse zur Erfassung und Bewertung von Vorfällen oder unerwarteten Modellverhalten?	KPI-Dashboard, Incident-Log, Monitoring-Berichte

Empfohlene Vorgehensweise

1. **Vor der Integration:** Führen Sie eine Compliance-Vorprüfung anhand dieser Checkliste durch und dokumentieren Sie alle Ergebnisse im AI-Risikoregister.
2. **Während der Nutzung:** Etablieren Sie ein kontinuierliches Monitoring und überprüfen Sie regelmäßig die Aktualität der Anbieterberichte.
3. **Bei wesentlichen Modell-Updates:** Wiederholen Sie die Prüfung und bewerten Sie mögliche Auswirkungen auf Transparenz, Sicherheit und Haftung.
4. **Nachweisführung:** Halten Sie sämtliche Bewertungen und Nachweise versioniert im Compliance- oder Qualitätsmanagementsystem fest.

© A4Q Copyright 2025

9.5 Praxisbeispiel: Nutzung eines LLM im Kundenservice

Ausgangssituation:
Ein Unternehmen nutzt ein kommerzielles Large Language Model (LLM) zur automatischen Beantwortung von Kundenanfragen im Online-Support. Die KI generiert Textantworten in Echtzeit, die direkt auf der Website veröffentlicht werden.

Fehler:
Die veröffentlichten Antworten werden automatisch ausgespielt, ohne Hinweis auf die maschinelle Erstellung und ohne vorgelagerte Qualitätskontrolle. Dadurch entsteht ein Risiko der Irreführung sowie möglicher fehlerhafter oder unangemessener Inhalte.

Korrekturmaßnahmen

- **Kennzeichnung:** Alle automatisch erzeugten Texte werden mit dem Hinweis versehen: *„Diese Antwort wurde mithilfe Künstlicher Intelligenz erstellt."*
- **Interner Prüfprozess:** Jede generierte Antwort wird vor Veröffentlichung durch eine redaktionelle Freigabe kontrolliert.
- **Dokumentation:** Einrichtung eines Audit-Trails, der Version, verwendeten Prompt, Bearbeiter und Freigabedatum dokumentiert.
- **Modellprüfung:** Überprüfung der GPAI-Transparenzdokumentation des Anbieters (z. B. Model Card, Evaluierungsberichte, Red-Team-Tests).

Ergebnis

Durch diese Maßnahmen wird die **Rechtskonformität** nach

- **Artikel 53** (Transparenzpflicht der GPAI-Anbieter),
- **Artikel 52** (Kennzeichnungspflicht bei KI-Interaktion) sowie
- **Artikel 55** (Einhaltung eines Code of Practice)

gewährleistet.

9.6 Handlungsempfehlungen für Anwenderorganisationen

Der Einsatz von General Purpose AI (GPAI) erfordert eine ganzheitliche Herangehensweise, die rechtliche, technische und organisatorische Aspekte miteinander verbindet.
Anwenderorganisationen sollten sicherstellen, dass sie nicht nur die Anforderungen der GPAI-Anbieter verstehen, sondern diese auch **in ihre eigenen Governance- und Compliance-Prozesse integrieren**.

© A4Q Copyright 2025

Die folgenden Empfehlungen unterstützen eine praxisgerechte Umsetzung:

1. **Due-Diligence-Prozess für GPAI etablieren**
   Führen Sie für jedes externe Modell eine strukturierte Vorprüfung durch. Prüfen Sie Dokumentation, Transparenzberichte, Lizenzierung und Sicherheitsnachweise, bevor ein Modell in betriebliche Prozesse integriert wird.
2. **Vertragliche Absicherung umsetzen**
   Ergänzen Sie Lieferanten- und Dienstleistungsverträge um spezifische Compliance-Klauseln, die auf die Pflichten nach den Artikeln 53 bis 55 EU AI Act verweisen (z. B. Bereitstellung von Model Cards, Risikoanalysen, Red-Team-Ergebnissen).
3. **Transparenz- und Monitoring-Pflichten in Governance-Richtlinien verankern**
   Definieren Sie interne Verfahren zur Überwachung, Nachverfolgung und regelmäßigen Neubewertung eingesetzter GPAI-Modelle. Diese sollten Teil des AI-Governance- oder Risikomanagementsystems sein.
4. **AI-Register führen**
   Erfassen Sie alle im Unternehmen verwendeten GPAI-Modelle mit Angaben zu Anbieter, Version, Verwendungszweck, Lizenzstatus, bekannten Einschränkungen und Testergebnissen. Dieses Register dient als Nachweis für interne und externe Audits.
5. **Schulung und Awareness fördern**
   Schulen Sie Mitarbeitende regelmäßig zu Chancen und Risiken generativer KI. Vermitteln Sie insbesondere die Bedeutung von Transparenz, Verantwortlichkeit und Qualitätssicherung im Umgang mit GPAI-Systemen.
6. **Incident-Management erweitern**
   Integrieren Sie KI-bezogene Vorfälle in bestehende Meldeprozesse. Erfassen und analysieren Sie fehlerhafte Antworten, Datenverletzungen, Urheberrechtskonflikte oder auffällige Modellverhalten systematisch.
7. **Red-Team-Testing als Best Practice einsetzen**
   Führen Sie – auch außerhalb des Hochrisikobereichs – regelmäßige Red-Team-Tests durch, um Schwachstellen, Bias und Manipulationsrisiken frühzeitig zu identifizieren. Dokumentieren Sie Ergebnisse und Anpassungen im AI-Risikoregister.

© A4Q Copyright 2025

10 Fundamental Rights Impact Assessment (FRIA, Art. 27 EU AI Act)

⏱ Unterrichtszeit: 45 Minuten

🎯 Business Outcomes:

- **BO 10.1:** Teilnehmende sind vorbereitet, eine FRIA zu strukturieren und in Entscheidungsprozesse einzubringen.
- **BO 10.2:** Teilnehmende sind befähigt, FRIA mit DSFA-Prozessen zu verknüpfen und Synergien zu nutzen.

LOs (Learning Onjectives)

- **LO 10.1 (K1):** Teilnehmende kennen den Zweck einer FRIA und deren Einordnung als zentrales Instrument zur Bewertung von Grundrechtsrisiken.
- **LO 10.2 (K2):** Teilnehmende können erläutern, welche Grundrechte typischerweise von KI-Systemen berührt werden (z. B. Gleichbehandlung, Datenschutz, Berufsfreiheit).
- **LO 10.3 (K2):** Teilnehmende verstehen, wie eine FRIA organisatorisch in bestehende Governance- oder Freigabeprozesse integriert wird.
- **LO 10.4 (K3):** Teilnehmende können eine vereinfachte FRIA an einem Praxisbeispiel durchführen, Risiken bewerten und geeignete Maßnahmen ableiten.
- **LO 10.5 (K1):** Teilnehmende kennen die zentralen Schritte einer FRIA – von der Identifikation betroffener Grundrechte bis zur Dokumentation der Bewertungsergebnisse.

Wichtige Begriffe:
FRIA (Fundamental Rights Impact Assessment), Grundrechte, Diskriminierung, Bias, Fairness, Schweregradmatrix, Abhilfemaßnahmen, Beteiligung Betroffener, Transparenz, Beschwerdemechanismus, DSFA-Abgrenzung, Art. 27 AI Act.

Einleitung

Das *Fundamental Rights Impact Assessment* (FRIA) ist ein zentrales neues Instrument des EU AI Act. Es verpflichtet öffentliche Stellen und bestimmte private Betreiber, **vor dem Einsatz von Hochrisiko-KI-Systemen** zu prüfen, ob Grundrechte von Personen beeinträchtigt werden können.
Ziel ist es, **potenzielle negative Auswirkungen auf Privatsphäre, Gleichbehandlung, Teilhabe, Meinungsfreiheit oder Beschäftigungschancen frühzeitig zu erkennen und zu mindern**.

© A4Q Copyright 2025

FRIA ergänzt bestehende Datenschutz- und Ethikprüfungen und dient als Bindeglied zwischen rechtlicher Compliance, ethischer Verantwortung und technischer Governance.

10.1 Rechtsgrundlage und Anwendungsbereich

Gemäß **Artikel 27 EU AI Act** müssen Betreiber (Deployers) von Hochrisiko-KI-Systemen, die

- im **öffentlichen Interesse** tätig sind oder
- Entscheidungen mit **Auswirkungen auf Grundrechte natürlicher Personen** treffen,
  vor dem Einsatz eine FRIA durchführen.

Beispiele betroffener Einsatzbereiche:

- Bewerbungs- und HR-Systeme (Zugang zu Beschäftigung, Gleichbehandlung)
- Kredit- und Scoring-Anwendungen (wirtschaftliche Teilhabe)
- Bildungs- und Prüfungsplattformen (Zugang zu Bildung)
- Öffentliche Dienstleistungen (Sozialleistungen, Migration, Sicherheit)

Private Organisationen können freiwillig eine FRIA durchführen, wenn Grundrechte erheblich betroffen sein können. Dies wird als **Best Practice** empfohlen und kann die Auditfähigkeit im Rahmen des AI Act stärken.

10.2 Struktur und empfohlene Schritte einer FRIA

Eine FRIA folgt einem standardisierten, dokumentierten Prozess.
Empfohlene Struktur:

Schritt	**Ziel**	**Typische Inhalte / Methoden**
1. Systembeschreibung	Klarheit über Zweck, Funktionsweise, Nutzergruppen	Systemübersicht, Datenflüsse, Entscheidungslogik, betroffene Personengruppen
2. Grundrechtsanalyse	Identifikation potenziell betroffener Rechte	Bezug auf EU-Grundrechtecharta: Würde, Datenschutz, Gleichbehandlung, Bildung, Teilhabe
3. Risikoidentifikation	Analyse möglicher negativer Auswirkungen	Diskriminierung, Ausschluss, Fehldiagnosen, Überwachung, Eingriffsintensität

© A4Q Copyright 2025

Schritt	Ziel	Typische Inhalte / Methoden
4. Risikobewertung	Einschätzung von Eintrittswahrscheinlichkeit und Schwere	Matrix: niedrig – mittel – hoch; Abwägung Nutzen / Schaden
5. Maßnahmenplanung	Entwicklung von Minderungsschritten	Transparenzmaßnahmen, menschliche Kontrolle, Fairness-Checks, Feedbackrechte
6. Dokumentation & Freigabe	Nachvollziehbarkeit und Rechenschaft	Begründete Entscheidung über Einsatz / Ablehnung; Versionierung; Genehmigung durch KI-Officer oder Compliance-Komitee

Jede FRIA sollte nachvollziehbar dokumentiert, regelmäßig überprüft und bei Systemänderungen aktualisiert werden (Art. 27 Abs. 3 AI Act).

10.3 Abgrenzung und Verknüpfung zur Datenschutz-Folgenabschätzung (DSFA)

Sowohl **FRIA** als auch **DSFA** sind präventive Instrumente, unterscheiden sich aber im Fokus:

Merkmal	FRIA (Art. 27 AI Act)	DSFA (Art. 35 DSGVO)
Ziel	Schutz der Grundrechte allgemein	Schutz personenbezogener Daten
Auslöser	Einsatz Hochrisiko-KI	Verarbeitung sensibler Daten mit hohem Risiko
Prüfperspektive	Gesellschaftlich-ethisch	Datenschutzrechtlich
Ergebnis	Grundrechts-Risikoanalyse, Maßnahmenplan	Datenschutzbericht mit technischen/organisatorischen Schutzmaßnahmen
Integration	Teil des Konformitätsdossiers	Bestandteil des Datenschutz-Managements

Empfehlung:
Beide Verfahren **integrieren**, um Doppelarbeit zu vermeiden. Eine kombinierte „FRIA-DSFA-Matrix“ ermöglicht konsistente Risikoanalysen und erleichtert Auditprüfungen.
Beispiel: Bei einem KI-basierten Bewerbungs-Tool kann dieselbe Risikoerhebung sowohl Diskriminierungs- als auch Datenschutzaspekte abdecken.

© A4Q Copyright 2025

10.4 Praktische Umsetzung einer FRIA – Schritt-für-Schritt-Vorgehen

Damit eine **Fundamental Rights Impact Assessment (FRIA)** im Unternehmen wirksam, nachvollziehbar und auditfähig umgesetzt werden kann, sollten Organisationen folgende **konkrete Schritte** durchführen:

1. Verantwortlichkeiten festlegen

Was ist zu tun:
Benennen Sie eine verantwortliche Person oder Stelle – idealerweise den **KI-Officer** oder **Compliance-Manager** –, die die Durchführung und Qualitätssicherung der FRIA steuert.
Ziel:
Klare Zuständigkeiten verhindern Lücken in der Risikoanalyse und sichern die Nachvollziehbarkeit für interne und externe Audits.
Praxis-Tipp:
Dokumentieren Sie die Rollenverteilung in der KI-Governance-Policy (z. B. „FRIA-Verantwortliche Person: Max Mustermann, AI Compliance Officer“).

2. FRIA-Template entwickeln

Was ist zu tun:
Erstellen Sie eine **standardisierte Vorlage** mit festen Prüffeldern und Leitfragen, z. B.:

- Welche Grundrechte können betroffen sein?
- Welche Personengruppen sind besonders schutzbedürftig?
- Welche Minderungsschritte sind geplant?
  Ziel:
  Einheitliches Vorgehen, konsistente Qualität und erleichterte Dokumentation.
  Praxis-Tipp:
  Nutzen Sie eine tabellarische Vorlage (z. B. in Excel oder im Compliance-Tool), um Risiko, Eintrittswahrscheinlichkeit und Maßnahmen strukturiert zu erfassen.

3. Fachbereiche schulen

Was ist zu tun:
Schulen Sie Mitarbeitende in HR, IT, Data Science und Recht darin, **Grundrechtsrisiken zu erkennen** und sich aktiv an der Bewertung zu beteiligen.
Ziel:
Sicherstellen, dass alle Beteiligten die Auswirkungen ihrer Arbeit auf Grundrechte verstehen.
Praxis-Tipp:

© A4Q Copyright 2025

Führen Sie kurze E-Learning-Module ein (30–45 Minuten), ergänzt durch Fallbeispiele aus dem eigenen Unternehmen.

4. FRIA in Governance-Prozesse integrieren

Was ist zu tun:
Binden Sie die FRIA als festen Schritt in bestehende Entscheidungs- und Freigabeprozesse ein:

- Projektstart: FRIA-Vorprüfung durchführen.
- Go-Live: FRIA als Voraussetzung für Freigabe.
- Änderungen am System: FRIA-Aktualisierung verpflichtend.
  Ziel:
  FRIA wird Teil der Unternehmensroutine – nicht nur eine einmalige Compliance-Aufgabe.
  Praxis-Tipp:
  Verknüpfen Sie die FRIA mit IT-Change- oder Projektmanagement-Prozessen (z. B. im Ticket- oder Freigabesystem).

5. Koordination mit Datenschutz

Was ist zu tun:
Stimmen Sie die Ergebnisse der FRIA mit der **Datenschutz-Folgenabschätzung (DSFA)** ab, um Doppelarbeit zu vermeiden.
Ziel:
Konsistente Risikoeinschätzungen und ganzheitlicher Grundrechtsschutz.
Praxis-Tipp:
Führen Sie gemeinsame Workshops zwischen Datenschutzbeauftragten und KI-Officer durch, um Synergien zu identifizieren und Risiken gemeinsam zu bewerten.

6. Regelmäßige Überprüfung

Was ist zu tun:
Überprüfen und aktualisieren Sie jede FRIA bei

- wesentlichen Systemänderungen,
- neuen Datenquellen oder Modellen,
- geänderten gesetzlichen Vorgaben.
  Ziel:
  Sicherstellen, dass Bewertungen und Maßnahmen stets aktuell bleiben.
  Praxis-Tipp:

© A4Q Copyright 2025

Planen Sie eine jährliche FRIA-Revision im Compliance-Kalender ein und dokumentieren Sie Änderungen im Versionierungssystem.

7. Ergebnisse kommunizieren

Was ist zu tun:
Veröffentlichen oder dokumentieren Sie die wichtigsten Ergebnisse – intern oder öffentlich –, um **Transparenz** zu schaffen und Vertrauen zu fördern.
Ziel:
Nachvollziehbarkeit für Mitarbeitende, Kund:innen, Aufsichtsbehörden und die Öffentlichkeit.
Praxis-Tipp:

- Kurzdokumentation im **AI-Register** führen (System, Risiken, Maßnahmen, Status).
- Zusammenfassung im **Nachhaltigkeits- oder Compliance-Bericht** veröffentlichen.

Ergebnis

Organisationen, die diese sieben Schritte konsequent umsetzen, erreichen:

- eine strukturierte, revisionssichere FRIA,
- klare Verantwortlichkeiten und Synergien mit Datenschutzprozessen,
- eine nachweisbare Integration von Grundrechtsschutz in alle KI-Projekte.

10.5 Synergien mit bestehenden Managementsystemen

FRIA lässt sich in bestehende Governance-Strukturen einbinden:

- **ISO/IEC 42001 (AI Management System):** Einordnung in Risiko- und Compliance-Prozesse
- **ISO/IEC 23894 (AI Risk Management):** Integration in die Bewertung von Auswirkungen auf Stakeholder
- **ISO/IEC 27701 (Privacy Extension):** Verknüpfung mit Datenschutzmanagement

Dadurch entsteht eine einheitliche Nachweisstruktur und eine klare **Presumption of Conformity** nach Art. 40 AI Act.

10.6 Beispiel einer FRIA in der Praxis

Szenario:
Eine Stadtverwaltung plant den Einsatz eines **KI-Systems zur automatisierten Prüfung von Anträgen auf Wohnbauförderung**. Ziel ist es, die Bearbeitungszeiten zu verkürzen und die Entscheidungsqualität durch konsistente Bewertungskriterien zu erhöhen.

© A4Q Copyright 2025

Durchgeführte FRIA – Kernergebnisse:

Prüffeld	Bewertung / Maßnahme
Betroffene Grundrechte	Gleichbehandlung, Datenschutz, Recht auf Wohnen
Identifizierte Hauptrisiken	Verzerrungen (Bias) in historischen Trainingsdaten; mangelnde Erklärbarkeit der Entscheidungslogik; fehlender oder unzureichender Widerspruchsmechanismus für Antragstellende
Ergriffene Maßnahmen	Durchführung eines **Fairness-Tests** durch eine unabhängige externe Prüfstelle; Veröffentlichung transparenter Entscheidungskriterien im Bürgerportal; Einführung eines **Beschwerde- und Widerspruchsverfahrens** mit menschlicher Kontrolle
Bewertung und Beschluss	Einsatz des Systems wird **unter Auflagen genehmigt**. Eine **jährliche Re-Evaluation** der Modelle, Datenquellen und Fairness-Metriken ist verpflichtend vorgesehen.

Dieses Beispiel zeigt, wie eine FRIA praktisch umgesetzt werden kann: Risiken werden frühzeitig erkannt, Gegenmaßnahmen dokumentiert und Verantwortlichkeiten festgelegt. Die Kombination aus technischer Prüfung, organisatorischer Kontrolle und transparenter Kommunikation stärkt sowohl die Rechtssicherheit als auch das Vertrauen der Bürgerinnen und Bürger.

Die FRIA ist ein wirksames Instrument, um den menschenzentrierten Ansatz des EU AI Act praktisch umzusetzen.
Sie ermöglicht Organisationen, **Grundrechte proaktiv zu schützen**, Risiken zu erkennen und dokumentiert Rechenschaft abzulegen.
In Kombination mit DSFA, Ethik-Guidelines und Managementsystemen wird die FRIA zum Herzstück einer verantwortungsvollen KI-Governance.

© A4Q Copyright 2025

11 Post-Market-Monitoring, Reporting & Marktaufsicht

⏱ 60 Minuten

🎯 **Business Outcomes:**

BO 11.1 Teilnehmende entwickeln Verständnis für Post-Market-Prozesse und sind vorbereitet, Monitoring-Pläne anzuwenden.

BO 11.2 Teilnehmende werden vorbereitet, mit Aufsichtsbehörden und dem AI Office zu kooperieren.

Lernziele (Learning Objectives – LO)

- **LO 11.1** Teilnehmende können Zweck und Anforderungen eines Post-Market-Monitoring-Plans nach Art. 61 EU AI Act erläutern. (K2)
- **LO 11.2** Teilnehmende können den Ablauf der Marktaufsicht, einschließlich Melde- und Berichtspflichten bei schwerwiegenden Vorfällen, beschreiben. (K2)
- **LO 11.3** Teilnehmende können ein einfaches Monitoring-Konzept für ein Hochrisiko-KI-System entwerfen. (K3)
- **LO 11.4** Teilnehmende können Rollen, Kommunikationswege und Pflichten gegenüber Marktaufsichtsbehörden und dem europäischen AI Office benennen. (K1)
- **LO 11.5 (K1):** Teilnehmende kennen die Hauptaufgaben und Meldepflichten im Post-Market-Monitoring.

Wichtige Begriffe:

Post-Market Monitoring, Serious Incident, Incident-Reporting, Art. 23 AI Act, Behördenkooperation, Marktaufsicht, Corrective Actions, Dokumentationspflicht, Fehlerkultur, Monitoring-Dashboard, Nachweispflichten, Audit-Follow-up.

Einleitung

Nach der Inverkehrbringung eines KI-Systems endet die Verantwortung des Anbieters nicht. Der EU AI Act fordert ein kontinuierliches **Post-Market-Monitoring** (PMM), das sicherstellt, dass das System dauerhaft die gesetzlichen Anforderungen erfüllt und keine neuen Risiken entstehen.

Dieser Abschnitt erläutert, wie Unternehmen ein solches Monitoring planen, umsetzen und mit Behörden zusammenarbeiten.

© A4Q Copyright 2025

11.1 Pflichten nach der Inverkehrbringung gemäß Artikel 61 EU AI Act

Nach dem Inverkehrbringen eines Hochrisiko-KI-Systems endet die Verantwortung des Anbieters nicht. Im Gegenteil: Der EU AI Act verpflichtet Organisationen ausdrücklich, den sicheren, rechtskonformen und leistungsfähigen Betrieb über den gesamten Lebenszyklus hinweg sicherzustellen.

Artikel 61 EU AI Act legt fest, dass Anbieter von Hochrisiko-Systemen ein strukturiertes und nachvollziehbares **Post-Market-Monitoring-System (PMM)** einrichten müssen. Dieses dient dazu, im laufenden Betrieb kontinuierlich zu überprüfen, ob das System weiterhin konform mit den regulatorischen, technischen und ethischen Anforderungen ist.

Gemäß Artikel 61 Absatz 1 EU AI Act müssen Anbieter insbesondere:

1. **Ein Post-Market-Monitoring-System einrichten:**
   Das Unternehmen hat einen definierten Prozess zur Überwachung des Systemverhaltens, der Leistungskennzahlen und möglicher Abweichungen zu implementieren. Das Monitoring-System muss in die bestehende Governance-Struktur eingebunden sein und darf nicht nur punktuell, sondern dauerhaft operativ wirken.
2. **Systematisch Daten über Leistung und Fehlfunktionen sammeln:**
   Während des Betriebs sind relevante Daten zu erfassen, die Aufschluss über Zuverlässigkeit, Genauigkeit, Robustheit, Fairness und Stabilität des Systems geben. Dazu zählen etwa technische Logs, Nutzerfeedback, Reklamationen oder automatisierte Fehlermeldungen.
3. **Abweichungen vom Konformitätszustand analysieren:**
   Jegliche Veränderung, die darauf hinweist, dass das KI-System nicht mehr den genehmigten Anforderungen oder Spezifikationen entspricht, muss umgehend untersucht werden. Hierzu gehören beispielsweise Leistungseinbußen, Model Drift, unvorhergesehene Bias-Effekte oder Änderungen im Verhalten durch neue Daten.
4. **Korrekturmaßnahmen oder Rückrufe einleiten:**
   Erkennt das Monitoring-System, dass ein Risiko für Grundrechte, Sicherheit oder Fairness besteht, müssen umgehend Gegenmaßnahmen umgesetzt werden. Diese reichen von Software-Updates und Model-Retraining über Anpassungen der Parametrisierung bis hin zur temporären Abschaltung oder zum vollständigen Rückruf des Systems.

Der **Monitoring-Plan** ist ein verpflichtender Bestandteil der **technischen Dokumentation** gemäß Artikel 11 EU AI Act und muss bereits **vor dem Inverkehrbringen** des Systems vorliegen.
Er bildet somit die Grundlage für die laufende Marktüberwachung und dient als Nachweis gegenüber den Aufsichtsbehörden, dass das Unternehmen seiner Sorgfalts- und Beobachtungspflicht im Betrieb nachkommt.

© A4Q Copyright 2025

11.2 Ziele des Post-Market-Monitoring

Das Post-Market-Monitoring verfolgt das Ziel, die langfristige Sicherheit, Qualität und Rechtskonformität von KI-Systemen zu gewährleisten. Es fungiert als Bindeglied zwischen der Entwicklungs- und der Betriebsphase und unterstützt sowohl technische Stabilität als auch organisatorische Rechenschaftspflicht.

Die zentralen Ziele sind:

- **Sicherstellung der dauerhaften Konformität:**
  Überprüfung, dass das System auch nach Updates, Datenänderungen oder längerem Einsatz weiterhin den Anforderungen des EU AI Act, der CE-Konformitätserklärung und der eigenen internen Policies entspricht.
- **Erkennung unerwarteter Risiken und Bias-Effekte:**
  Frühzeitige Identifikation von Leistungsabweichungen, Verzerrungen oder diskriminierenden Ergebnissen im praktischen Betrieb, die im Testumfeld nicht erkennbar waren.
- **Bewertung von Leistungsfähigkeit und Robustheit über die Zeit:**
  Überwachung der Systemqualität mittels definierter Key Performance Indicators (KPIs) wie Genauigkeit, Fehlerrate, Reaktionszeit oder Fairness-Index, um Qualitätsverluste (Model Drift) frühzeitig zu erkennen.
- **Nachvollziehbarkeit und Rechenschaft:**
  Bereitstellung belastbarer Nachweise für interne Audits, externe Prüfer und Marktaufsichtsbehörden. Die Protokolle dienen als Grundlage für Berichte an das AI Office oder nationale Behörden.
- **Grundlage für Re-Evaluation oder Nachzertifizierung:**
  Ergebnisse des Monitorings bilden die Basis für regelmäßige Überprüfungen der Risikoklassifikation und für erforderliche Re-Zertifizierungen bei Systemänderungen oder Funktions-Updates.

Insgesamt soll das Post-Market-Monitoring gewährleisten, dass der Betrieb von KI-Systemen nicht nur initial, sondern dauerhaft vertrauenswürdig, sicher und rechtskonform erfolgt.

11.3 Inhalt eines Monitoring-Plans

Ein wirksamer Monitoring-Plan übersetzt die gesetzlichen Anforderungen in ein strukturiertes und nachvollziehbares Unternehmensverfahren.
Er beschreibt, **was** überwacht wird, **wie** Daten erhoben und ausgewertet werden, **wer** verantwortlich ist und **welche Maßnahmen** bei Auffälligkeiten zu ergreifen sind.

Abschnitt	Beschreibung
Ziele und Umfang	Definition, welche Leistungs- und Qualitätsaspekte überwacht werden (z. B. Genauigkeit, Fairness, Sicherheit, Nutzer-Feedback, Stabilität). Der Umfang

© A4Q Copyright 2025

Abschnitt	Beschreibung
	sollte alle relevanten Komponenten des KI-Systems umfassen, einschließlich Subsysteme und Datenquellen.
Indikatoren / KPIs	Festlegung messbarer Leistungskennzahlen zur Bewertung der Systemqualität: Fehlerraten, Falsch-Positiv-Quote, Performance-Drift, Häufigkeit von Incidents, Fairness-Metriken.
Datenquellen	Bestimmung, aus welchen Quellen Monitoring-Daten stammen: System-Logs, Nutzerbeschwerden, Audit-Berichte, Support-Tickets, externe Datenfeeds oder statistische Auswertungen.
Rollen & Verantwortlichkeiten	Zuweisung der Zuständigkeiten: KI-Officer (Gesamtverantwortung), Fachaufsicht (Bewertung fachlicher Qualität), Compliance-Beauftragte (Berichtskoordination), IT-Monitoring-Team (technische Datenerfassung).
Berichtszyklen	Festlegung der Häufigkeit von Auswertungen und Berichten, z. B. monatliche Reviews für operative Kennzahlen, quartalsweise Management-Reports, jährlicher Compliance-Bericht an die Aufsicht.
Eskalationswege	Definition von Schwellenwerten und Entscheidungswegen für Eingriffe: Wann gilt ein Vorfall als Incident? Wer entscheidet über Systemabschaltung oder Meldung an Behörden?

Beispielhafte Indikatoren für Post-Market-Monitoring:

- Abweichung der Systemleistung um mehr als **10 %** vom definierten Referenzwert.
- Auftreten von **drei oder mehr Incidents innerhalb von 30 Tagen**.
- Signifikant höhere Fehlerrate bei bestimmten Nutzergruppen → Hinweis auf Bias-Effekte, Auslösung einer Fairness-Prüfung.

Praxisempfehlung:
Monitoring-Pläne sollten mit anderen Governance-Instrumenten verknüpft werden, etwa mit dem Risikoregister, dem Incident-Management-Prozess und dem Qualitätsmanagementsystem (QMS). So entsteht eine durchgängige Nachvollziehbarkeit zwischen Risikoanalyse, Systembetrieb und kontinuierlicher Verbesserung.

© A4Q Copyright 2025

11.4 Serious-Incident-Reporting (Art. 62 EU AI Act)

Ein „**Serious Incident**“ bezeichnet gemäß Artikel 62 EU AI Act jedes sicherheits- oder grundrechtsrelevante Ereignis, das durch das Verhalten eines KI-Systems ausgelöst oder verschärft wurde und zu einer **Verletzung von Rechten, Sicherheit oder Integrität von Personen** führen kann.

Ein solcher Vorfall liegt insbesondere dann vor, wenn das Verhalten eines KI-Systems zu:

- **Verletzungen von Grundrechten** führt (z. B. Diskriminierung, unrechtmäßige Ablehnung, fehlende Widerspruchsmöglichkeit),
- einer **erheblichen Sicherheitsgefährdung** für Personen, Systeme oder kritische Infrastrukturen beiträgt, oder
- einem **nicht vorhergesehenen Fehlverhalten** mit potenzieller Schadensfolge (z. B. falsche Diagnosen, automatisierte Fehlentscheidungen) führt.

Diese Definition schließt sowohl technische Fehlfunktionen als auch ethisch oder rechtlich relevante Fehlentscheidungen ein. Sie ist unabhängig davon anzuwenden, ob der Schaden tatsächlich eingetreten oder lediglich wahrscheinlich ist.

Der EU AI Act verpflichtet Anbieter und Betreiber von Hochrisiko-KI-Systemen, bei Auftreten eines **„Serious Incident“** unverzüglich zu handeln. Diese Verpflichtungen gelten in allen Mitgliedstaaten der Europäischen Union und sind unionsweit harmonisiert. Sie dienen dem Schutz von Sicherheit, Grundrechten und öffentlicher Ordnung sowie der schnellen Einbindung der zuständigen Aufsichtsorgane.

Pflichten bei Auftreten eines Serious Incident (EU-weit):

1. **Meldung innerhalb von 15 Kalendertagen**
   Der Anbieter muss den Vorfall spätestens **15 Tage nach dessen Bekanntwerden** an die **zuständige nationale Marktaufsichtsbehörde** melden.
   Diese Pflicht gilt unabhängig davon, ob der Schaden bereits eingetreten ist oder lediglich eine erhebliche Wahrscheinlichkeit besteht.
   - Die Meldung muss alle verfügbaren Informationen zum Zeitpunkt der Entdeckung enthalten (Systemkennung, betroffene Module, Art des Fehlverhaltens, potenzielle Auswirkungen, erste Gegenmaßnahmen).
   - Die Frist beginnt mit der **ersten internen Kenntnisnahme** des Vorfalls, nicht mit seiner abschließenden Analyse.
   - Auch Betreiber (Deployers) sind verpflichtet, erkannte Vorfälle umgehend an den jeweiligen Anbieter weiterzuleiten, damit dieser die Meldung fristgerecht durchführen kann.

Nationale Zuständigkeiten (Beispiele):

- **Österreich:**

© A4Q Copyright 2025

- *Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK)* für Marktaufsicht,
- *Datenschutzbehörde (DSB)*, sofern personenbezogene Daten betroffen sind.

- **Deutschland:**
  - *Bundesnetzagentur* (BNetzA) als zentrale Marktaufsichtsbehörde für KI-Systeme,
  - *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)* bei datenschutzrelevanten Vorfällen.
- **Frankreich:**
  - *Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF)*,
  - *Commission Nationale de l'Informatique et des Libertés (CNIL)* bei Datenschutzbezug.
- **Italien:**
  - *Ministero delle Imprese e del Made in Italy (MIMIT)* für Marktüberwachung,
  - *Garante per la Protezione dei Dati Personali* für Datenschutzfälle.
- **Spanien:**
  - *Ministerio de Asuntos Económicos y Transformación Digital (MINECO)*,
  - *Agencia Española de Protección de Datos (AEPD)* für personenbezogene Daten.
- **Niederlande:**
  - *Nederlandse Autoriteit Consument & Markt (ACM)*,
  - *Autoriteit Persoonsgegevens (AP)* bei Datenschutzverletzungen.
- **Belgien:**
  - *Service Public Fédéral Économie (SPF Économie)* als Marktaufsicht,
  - *Autorité de Protection des Données (APD)* als Datenschutzaufsicht.
- **Schweden:**
  - *Konsumentverket* für Produkt- und Systemaufsicht,
  - *Integritetsskyddsmyndigheten (IMY)* für Datenschutzfälle.

Diese nationalen Behörden sind jeweils verpflichtet, den gemeldeten Fall an das **EU AI Office** zu übermitteln, das auf Unionsebene eine koordinierte Bewertung vornimmt.

© A4Q Copyright 2025

2. **Gleichzeitige Information an das EU AI Office**
   Zusätzlich zur nationalen Meldung muss der Anbieter das **AI Office der Europäischen Kommission** informieren.
   - Das AI Office fungiert als zentrale europäische Koordinationsstelle und führt eine **zentrale Vorfallsdatenbank** über alle Serious Incidents.
   - Bei systemischen Risiken (z. B. fehlerhafte Basismodelle oder GPAI-Systeme mit weiträumiger Nutzung) kann das AI Office unionsweite Untersuchungen, Leitlinien oder Sofortmaßnahmen initiieren.
   - Unternehmen können die Meldung über eine einheitliche EU-Schnittstelle („AI Incident Reporting Portal“) einreichen, sobald diese implementiert ist.
3. **Bereitstellung einer vorläufigen Analyse und geplanter Maßnahmen**
   Der Erstbericht muss enthalten:
   - eine kurze technische Beschreibung des Vorfalls,
   - Datum und Ort des Auftretens,
   - betroffene Systemversion(en) und Komponenten,
   - Art und Schwere des Risikos,
   - Anzahl und Art potenziell betroffener Personen oder Systeme,
   - erste technische und organisatorische Gegenmaßnahmen.
     Diese vorläufige Analyse ermöglicht den Behörden eine schnelle Risikobewertung und gegebenenfalls Sofortmaßnahmen (z. B. Warnungen an andere Betreiber).
4. **Nachreichung eines Abschlussberichts nach Behebung oder Systemupdate**
   Sobald der Vorfall behoben oder das System angepasst wurde, ist ein **abschließender Bericht** einzureichen. Dieser enthält:
   - eine detaillierte Ursachenanalyse,
   - Beschreibung der getroffenen Korrektur- und Präventionsmaßnahmen,
   - Nachweise über Wirksamkeit (z. B. Testergebnisse, Validierungsberichte),
   - Zeitpunkt der Wiederinbetriebnahme, sofern zutreffend.

Der Abschlussbericht ist an dieselben Behörden zu übermitteln, an die auch die Erstmeldung ging. In der Praxis erfolgt die Koordination zunehmend digital über die **EU Market Surveillance Platform**, die eine strukturierte Kommunikation zwischen nationalen Stellen und dem AI Office ermöglicht.

Zusammenfassung Zielsetzung:
Das Meldesystem nach Art. 62 EU AI Act verfolgt das Ziel, eine **frühzeitige Gefahrenabwehr**,

© A4Q Copyright 2025

transparente Ursachenanalyse und **europaweite Lernprozesse** zu gewährleisten.
Durch die verpflichtende Dokumentation und die Meldekette zwischen Betreiber, Anbieter, nationaler Marktaufsicht und EU AI Office wird ein unionsweites Frühwarnsystem geschaffen, das die Sicherheit und Vertrauenswürdigkeit von KI-Systemen kontinuierlich stärkt.

Beispiel:
Ein HR-Screening-System zeigt im Echtbetrieb signifikant höhere Ablehnungsraten für Bewerber:innen über 50 Jahre. Der KI-Officer stoppt den Algorithmus, initiiert ein internes Bias-Audit, informiert die Marktaufsichtsbehörde und das AI Office, und liefert nach Abschluss der Nachschulung einen Bericht mit den korrigierten Ergebnissen.

11.5 Zusammenarbeit mit Marktaufsichtsbehörden und dem AI Office

Der EU AI Act sieht ein mehrstufiges System der **Marktaufsicht** vor, das auf Kooperation, Nachweisführung und Transparenz basiert. Die Überwachung erfolgt durch nationale Behörden in enger Abstimmung mit dem **EU AI Office**, das die Harmonisierung und Auslegung der Regulierung auf europäischer Ebene koordiniert.

Zentrale Aufgaben der Marktaufsicht:

- **Stichprobenprüfungen und Audits:**
  Nationale Marktaufsichtsbehörden prüfen regelmäßig registrierte Hochrisiko-Systeme. Diese Kontrollen können sowohl angekündigt als auch unangekündigt erfolgen und umfassen Einsicht in Dokumentation, Logging-Systeme, Modelle und Audit-Berichte.
- **Koordination durch das EU AI Office:**
  Das AI Office fungiert als zentrale Stelle für unionsweite Richtlinien, Risikoanalysen und Informationsaustausch zwischen den Mitgliedstaaten. Es kann bei schwerwiegenden Fällen Untersuchungen anordnen oder gemeinsame technische Expertengruppen einsetzen.
- **Pflichten der Anbieter:**
  Unternehmen sind verpflichtet, **innerhalb kurzer Fristen** Zugang zu allen relevanten Unterlagen zu gewähren – insbesondere zur technischen Dokumentation, zu Audit-Logs, Versionierungsnachweisen und Monitoring-Berichten.

Empfohlene Vorgehensweise bei Behördenanfragen:

1. **Einrichtung einer zentralen Kontaktstelle**
   Unternehmen sollten eine interne Ansprechperson benennen (z. B. KI-Officer oder Compliance-Manager), die als alleinige Kommunikationsschnittstelle gegenüber Aufsichtsbehörden fungiert.

© A4Q Copyright 2025

2. **Bereitstellung standardisierter Audit-Reports und Modellversionen**
   Eine klare Dokumentenstruktur (z. B. Audit-Dossier, Modell-Changelog, Versionierungstabellen) erleichtert die Nachvollziehbarkeit und reduziert Prüfaufwand.
3. **Proaktive Kommunikation bei Risiken oder Änderungen**
   Wesentliche Änderungen im Modell, in der Datenbasis oder im Anwendungszweck sollten proaktiv gemeldet werden, bevor eine Neuzertifizierung erforderlich wird.
4. **Dokumentation aller Behördeninteraktionen**
   Jede behördliche Anfrage, Antwort oder Prüfung sollte im internen „**Regulatory Interaction Log**“ festgehalten werden – mit Datum, Ansprechpartnern, Thema und Ergebnis. Diese Nachweise dienen im Auditfall als Beleg für kooperative Compliance.

Hinweis für die Praxis:
Eine offene, sachlich dokumentierte Zusammenarbeit mit Marktaufsicht und AI Office wird von den Behörden ausdrücklich positiv bewertet. Sie signalisiert Reife und Verantwortungsbewusstsein in der Unternehmens-Governance.

11.6 Best Practice: Kontinuierliche Risikoevaluation

Das Post-Market-Monitoring ist eng mit der **laufenden Re-Evaluierung des Risikostatus** eines KI-Systems verbunden.
Organisationen sollten mindestens einmal jährlich – oder bei jeder wesentlichen Systemänderung – eine **Risikoevaluation** durchführen, um sicherzustellen, dass das System weiterhin der richtigen Risikoklasse zugeordnet ist und alle Schutzmaßnahmen angemessen wirken.

Empfohlene Anlässe für eine Re-Evaluation:

- **Wesentliche Änderungen am Modell**
  (z. B. neues Trainingsverfahren, Austausch der Datenbasis, geänderte Gewichtungen oder Funktionen).
- **Neue Anwendungsgebiete oder Zielgruppen**
  (z. B. Einsatz eines ursprünglich internen Tools nun in der öffentlichen Verwaltung).
- **Geänderte gesetzliche Rahmenbedingungen**
  (z. B. neue Leitlinien des AI Office oder nationale Durchführungsverordnungen).

Ergebnisdokumentation:
Alle Ergebnisse der Re-Evaluation sind im **Risikoregister** zu vermerken und fließen in den **jährlichen Post-Market-Compliance-Bericht** ein. Werden erhöhte Risiken festgestellt, ist eine erneute **Konformitätsbewertung** nach Art. 17 ff. EU AI Act erforderlich.

© A4Q Copyright 2025

Ziel:

Diese kontinuierliche Überprüfung stärkt die Rechtssicherheit und belegt, dass das Unternehmen seine Überwachungs- und Sorgfaltspflichten ernsthaft wahrnimmt.

11.7 Praxisbeispiel: Post-Market-Monitoring und Behördenkooperation in der öffentlichen Verwaltung

Szenario:

Eine öffentliche Arbeitsagentur setzt ein **KI-System zur automatisierten Vorauswahl von Bewerbungen** ein.

Das System analysiert eingereichte Unterlagen anhand von Qualifikationen, Schlüsselwörtern und Erfahrungsprofilen und erstellt daraus automatisiert eine Rangliste für die Personalabteilung.

Ziel ist eine effiziente Vorauswahl, bei der nur die am besten geeigneten Kandidatinnen und Kandidaten für die manuelle Prüfung durch das HR-Team vorgeschlagen werden.

Post-Market-Ergebnisse:

Nach mehreren Monaten im Echtbetrieb werden im Rahmen des verpflichtenden **Post-Market-Monitorings** (gemäß Art. 61 EU AI Act) folgende Auffälligkeiten festgestellt:

- Das Monitoring-Dashboard zeigt, dass Bewerber:innen über 55 Jahre systematisch geringere Scores erhalten als jüngere Bewerber:innen mit vergleichbaren Qualifikationen.
- Der **KI-Officer** stuft den Befund als **„Serious Incident“** gemäß Art. 62 EU AI Act ein und meldet ihn fristgerecht an die nationale **Marktaufsichtsbehörde** sowie das **EU AI Office**.
- Das betroffene System wird vorsorglich **deaktiviert**, um weitere Benachteiligungen zu verhindern, und einer **externen Fairness-Überprüfung** durch eine unabhängige Prüfstelle unterzogen.
- Die Untersuchung ergibt, dass die Verzerrung auf historische Trainingsdaten zurückzuführen ist, in denen ältere Bewerber:innen unterrepräsentiert waren.

Korrektur- und Präventionsmaßnahmen:

Nach einer Ursachenanalyse werden folgende Schritte umgesetzt:

1. **Retraining mit angepasstem Datensatz:** Ergänzung um repräsentative Beispiele aus allen Altersgruppen.
2. **Re-Evaluation durch unabhängige Prüfstelle:** Bestätigung der verbesserten Fairness und Modellrobustheit.
3. **Wiederfreigabe des Systems unter Auflagen:**
    - halbjährlicher **Monitoring-Report** mit Bias-Analysen,
    - verpflichtende **Fairness-Tests vor jedem Modell-Update**,

© A4Q Copyright 2025

- **regelmäßige Schulung** der HR-Mitarbeitenden zur Interpretation von KI-Scores und menschlicher Überprüfungsverantwortung.

Ergebnis:
Nach Umsetzung der Maßnahmen wird das System wieder in Betrieb genommen. Die Monitoring-Berichte zeigen eine stabile, diskriminierungsfreie Performance, und die öffentliche Arbeitsagentur dokumentiert den gesamten Vorgang im **Konformitätsdossier** nach Art. 11 EU AI Act.

Lernbotschaft:
Dieses Praxisbeispiel verdeutlicht, wie eng **Post-Market-Monitoring**, **Incident-Reporting** und **Behördenkooperation** miteinander verbunden sind.
Eine **aktive, nachvollziehbar dokumentierte Fehler- und Lernkultur** ermöglicht es Organisationen, Risiken frühzeitig zu erkennen, regulatorische Anforderungen einzuhalten und das Vertrauen von Öffentlichkeit, Aufsichtsbehörden und Mitarbeitenden langfristig zu sichern.

© A4Q Copyright 2025

12 Governance, Organisation & Rollen im Unternehmen

⏱ **Unterrichtszeit:** 45 Minuten

🎯 **Business Outcomes:**

BO 12.1: Teilnehmende sind vorbereitet, Rollen und Verantwortlichkeiten im KI-Governance-System mitzugestalten.
BO 12.2: Teilnehmende sind befähigt, interne Schulungs- und Policy-Programme zur Compliance-Kultur aufzubauen.

Lernziele (Learning Objectives – LO)

- **LO 12.1 (K2):** Teilnehmende können wesentliche Elemente einer KI-Governance-Struktur erklären und deren Bedeutung für Compliance und Qualität darstellen.
- **LO 12.2 (K3):** Teilnehmende können Verantwortlichkeiten, Eskalationspfade und Gremien in einem KI-Governance-Modell gestalten.
- **LO 12.3 (K2):** Teilnehmende können beschreiben, wie Schulungs- und Awareness-Programme die Compliance-Kultur stärken.
- **LO 12.4 (K1):** Teilnehmende können zentrale Governance-Begriffe wie „Policy“, „Accountability“ und „AI Governance Committee“ benennen.
- **LO 12.5 (K1):** Teilnehmende kennen die grundlegende Rollenverteilung in der KI-Governance, insbesondere die Aufgaben von KI-Officer, Compliance-Board und Fachbereichen.

Wichtige Begriffe:
AI Governance, Accountability, KI-Officer, AI Governance Committee, Compliance Board, RACI-Matrix, Roles & Responsibilities, Policy, Eskalationspfad, Awareness-Programm, Schulungsmatrix, Art. 4(4) AI Act.

Einführung

KI-Governance bezeichnet im Kontext die Gesamtheit der organisatorischen Strukturen, Prozesse und Rollen, die sicherstellen, dass Künstliche Intelligenz rechtskonform, sicher und ethisch vertretbar eingesetzt wird.
Ein wirksames Governance-System verbindet rechtliche Anforderungen (EU AI Act, DSGVO, ISO/IEC 42001) mit unternehmensinternen Verantwortlichkeiten, Schulungen und einer Kultur der Transparenz.

12.1 Struktur eines KI-Governance-Systems

Ein Governance-System gliedert sich in drei Ebenen:

© A4Q Copyright 2025

Ebene	Zielsetzung	Typische Instrumente
Strategisch	Richtungsentscheidungen, Risiko-Appetit, Prioritäten	AI Governance Committee, Vorstands-Reporting
Taktisch	Steuerung der Umsetzung, Ressourcenzuteilung, Richtlinienpflege	Policies, RACI-Matrix, Rollenprofile
Operativ	Konkrete Umsetzung, Monitoring, Dokumentation	Audit-Protokolle, Incident-Management, Training

Wichtig ist die klare **Accountability-Zuweisung**: Jede Maßnahme (z. B. Fairness-Audit, Logging, Re-Training) muss eine verantwortliche Rolle, eine Freigabestufe und einen Dokumentationspfad haben.

12.2 Zentrale Rollen und Zuständigkeiten

Ein wirksames KI-Governance-System setzt klar definierte Rollen, Zuständigkeiten und Berichtspflichten voraus. Diese Struktur gewährleistet, dass regulatorische Anforderungen gemäß EU AI Act sowie interne Qualitäts- und Sicherheitsstandards kohärent umgesetzt werden.

Rolle	Hauptaufgaben	Berichtspfad
AI Compliance Officer	Gesamtkoordination aller Compliance-Aktivitäten im Bereich Künstliche Intelligenz; Durchführung von Risikobewertungen; Sicherstellung der Einhaltung der Pflichten nach EU AI Act; Vorbereitung interner und externer Audits	an Geschäftsleitung / CISO
Konformitätsbeauftragte:r	Pflege und Aktualisierung des technischen Dossiers; Koordination der Konformitätsbewertungsverfahren; zentrale Kontaktstelle für Marktaufsichtsbehörden und Zertifizierungsstellen	an AI Officer / Legal
Fachverantwortliche:r	Sicherstellung der fachlichen Qualität und Zweckbindung der verwendeten Daten; Validierung der Modellergebnisse im jeweiligen Anwendungsbereich; Dokumentation von Änderungen und Prüfungen	an AI Committee

© A4Q Copyright 2025

Rolle	Hauptaufgaben	Berichtspfad
Ethik- oder Diversity-Beauftragte:r	Prüfung von Fairness-, Gleichbehandlungs- und Gesellschaftsauswirkungen; Mitwirkung bei Ethical Impact Assessments und der Bewertung von Bias-Risiken	an AI Committee
IT-Security & Data Protection	Gewährleistung von Datenschutz, Datensicherheit und Zugriffsschutz; Kontrolle von Logging-Systemen und Backup-Mechanismen; Abstimmung mit ISMS und DSGVO-Verantwortlichen	an CISO / DPO

Diese Rollen bilden gemeinsam den organisatorischen Kern der KI-Compliance-Struktur. Durch klar zugewiesene Aufgaben und Berichtslinien wird sichergestellt, dass Risiken frühzeitig erkannt, Maßnahmen effektiv umgesetzt und die Rechenschaftspflichten gemäß Art. 4 Abs. 4 EU AI Act erfüllt werden.

12.3 AI Governance Committee

Ein interdisziplinäres Gremium („AI Committee“) koordiniert alle Themen mit Relevanz für KI-Risikomanagement, Governance und Compliance. Es fungiert als zentrales Steuerungsorgan für den verantwortungsvollen Einsatz von Künstlicher Intelligenz im Unternehmen und sichert die laufende Einhaltung der regulatorischen Anforderungen nach EU AI Act.

Aufgaben des AI Committees:

- **Review neuer KI-Use-Cases vor dem Einsatz:** Prüfung der Risikoklassifikation, Bewertung möglicher Grundrechtsrisiken und Entscheidung über Freigabe oder Eskalation.
- **Freigabe von Policies, Ethik-Leitlinien und Audit-Plänen:** Sicherstellung, dass interne Regelwerke mit geltendem Recht und Unternehmenszielen übereinstimmen.
- **Überwachung von Post-Market-Monitoring-Berichten:** Kontrolle der Wirksamkeit von Risikomaßnahmen, Auswertung von Incident-Reports und Monitoring-Ergebnissen.
- **Eskalation bei Serious Incidents:** Bewertung kritischer Vorfälle und Koordination der Kommunikation mit der Geschäftsführung, den Aufsichtsbehörden und gegebenenfalls externen Prüfinstitutionen.

Best Practice:
Das AI Committee sollte interdisziplinär besetzt sein, um technische, juristische und ethische Perspektiven zu vereinen. Empfohlen wird die Einbindung von Vertreter:innen aus:

- Recht & Compliance,

© A4Q Copyright 2025

- Datenschutz (DPO),
- IT- und Informationssicherheit (CISO),
- Personalwesen (HR),
- Produktmanagement,
- sowie gegebenenfalls Ethik- oder Nachhaltigkeitsbeauftragten.

Das Gremium tagt regelmäßig (z. B. quartalsweise) und dokumentiert alle Entscheidungen, Maßnahmen und Empfehlungen im Governance-Register. So entsteht Transparenz über Verantwortlichkeiten, Entscheidungswege und die Einhaltung der Pflichten nach Art. 4 Abs. 4 EU AI Act.

12.4 Interne Policies und Kontrollmechanismen

Ein wirksames KI-Governance-System basiert auf klaren internen Regelwerken und nachvollziehbaren Kontrollmechanismen. Diese Dokumente legen fest, wie KI-Systeme entwickelt, betrieben, überwacht und regelmäßig überprüft werden. Sie schaffen Verbindlichkeit, Nachvollziehbarkeit und Rechtssicherheit gemäß den Anforderungen des EU AI Act.

Zentrale Governance-Dokumente:

- **KI-Policy:** Festlegung von Grundsätzen, Zuständigkeiten und Freigabeprozessen für die Entwicklung, den Einsatz und die Überwachung von KI-Systemen.
- **Standard Operating Procedures (SOPs):** Detaillierte Arbeitsanweisungen zu spezifischen Prozessen wie Incident-Handling, Bias-Überprüfung, Modell-Retraining oder Post-Market-Monitoring.
- **Compliance-Register:** Verzeichnis aller eingesetzten KI-Systeme mit Angaben zu Version, Zweck, Risikoklasse, Verantwortlichkeiten und aktuellem Audit-Status. Dieses Register dient als Nachweis im Rahmen interner und externer Prüfungen.
- **Policy-Cycle:** Regelmäßige (mindestens jährliche) Überprüfung aller Governance-Dokumente auf Aktualität, neue rechtliche Anforderungen und Lessons Learned aus Audits oder Vorfällen.

Diese Struktur ermöglicht es Organisationen, einheitliche Standards im Umgang mit KI zu etablieren und die Rechenschaftspflichten nach Art. 4 Abs. 4 und Art. 29 EU AI Act systematisch zu erfüllen.

12.5 Schulung und Awareness-Programme

Eine tragfähige Compliance-Kultur entsteht nicht allein durch Richtlinien, sondern durch qualifizierte und sensibilisierte Mitarbeitende. Schulung und Bewusstseinsbildung sind zentrale Instrumente, um die Anforderungen des EU AI Act in der täglichen Praxis zu verankern.

Empfohlene Schulungs- und Awareness-Bausteine:

© A4Q Copyright 2025

- **Basisschulung:** Einführung in die Grundprinzipien des EU AI Act, die Risikoklassen, zentrale Rollen im Unternehmen und typische Compliance-Pflichten.
- **Rollenspezifische Trainings:** Vertiefte Schulungen für Fachbereiche wie HR, IT, Entwicklung oder Management mit Fokus auf deren spezifische Verantwortlichkeiten im KI-Betrieb.
- **E-Learning & Zertifikate:** Digitale Schulungsformate mit automatischen Erinnerungen bei System- oder Rechtsänderungen, ergänzt durch Teilnahmebestätigungen als Auditnachweis.
- **Workshops zur Fehlerkultur:** Förderung einer offenen Lernkultur nach dem Prinzip „Vom Incident zum Lernprozess“ – Analyse realer Fälle, um Prävention und Transparenz zu stärken.
- **Awareness-Kampagnen:** Kontinuierliche Sensibilisierung über interne Kommunikationskanäle (Intranet, Newsletter, Poster, Kurzvideos) zu Themen wie „Responsible AI“ oder „Bias Awareness“.

Ziel:
Alle Mitarbeitenden sollen nachvollziehen können, **wo und wie KI-Systeme eingesetzt werden**, **welche Risiken bestehen** und **wie sie im Zweifel korrekt reagieren oder eskalieren**.

12.6 Schnittstellen zu bestehenden Managementsystemen

Eine effiziente KI-Governance erfordert keine isolierten Strukturen, sondern die **Integration in bestehende Managementsysteme**. Durch die Anbindung an etablierte ISO-Standards werden Doppelprüfungen vermieden und die Nachweispflichten konsolidiert.

Managementsystem	**Verbindung zur KI-Governance**
Informationssicherheits-Managementsystem (ISMS)	Schutz von Daten und Systemintegrität; Umsetzung der Sicherheitsanforderungen nach Art. 15 EU AI Act
Qualitätsmanagementsystem (QMS)	Sicherstellung von Prozessdokumentation, Versionierung und Auditfähigkeit gemäß Art. 17 EU AI Act
Datenschutzmanagementsystem (DSMS)	Integration von DSGVO-Anforderungen, Datenschutz-Folgenabschätzungen (DSFA) und Wahrung der Rechte betroffener Personen
Compliance Management System (CMS)	Steuerung von Risikomanagement, Eskalationswegen und Auditplanung im Sinne einer ganzheitlichen Unternehmenscompliance

Diese Schnittstellen stärken die organisatorische Effizienz, fördern die Konsistenz von Nachweisen und erleichtern die Integration von KI in bestehende Audit- und Kontrollprozesse.

© A4Q Copyright 2025

12.7 Beispiel – Governance-Implementierung in der Praxis

Szenario:

Ein öffentlicher Verkehrsbetrieb plant, ein KI-System zur **dynamischen Ticketpreisprognose** einzusetzen. Ziel ist, Fahrpreise flexibel an Nachfrage, Tageszeit und Auslastung anzupassen, um eine gleichmäßigere Nutzung des Verkehrsnetzes zu erreichen. Die KI analysiert historische Buchungsdaten, Wetterprognosen, Großveranstaltungen und Echtzeit-Fahrgastzahlen.

Bereits in der Planungsphase erkennt das Unternehmen, dass dieses System **personenbezogene Daten** (z. B. Zeit- und Ortsprofile von Nutzer:innen) verarbeiten könnte und dadurch **regulatorische Risiken nach EU AI Act und DSGVO** entstehen. Das Projekt wird daher als **„High Impact"-Use Case** eingestuft und in das interne **KI-Governance-Framework** integriert.

Umgesetzte Maßnahmen:

1. **Benennung eines KI-Officers und Einrichtung eines interdisziplinären Governance-Boards**
   Der KI-Officer übernimmt die Gesamtkoordination und berichtet direkt an die Geschäftsführung.
   Das Governance-Board setzt sich aus Vertreter:innen von Recht, Datenschutz, IT-Security, Betrieb, Kommunikation und Tarifmanagement zusammen.
   Aufgabe des Boards ist es, alle KI-Projekte regelmäßig zu bewerten, Freigaben zu erteilen und Audit-Ergebnisse zu prüfen.
2. **Erstellung einer klaren Rollen- und Aufgabenbeschreibung**
   Für das Ticketpreis-System werden Verantwortlichkeiten eindeutig definiert:
   - **Monitoring-Verantwortliche:** laufende Beobachtung der Preisempfehlungen und Erkennung auffälliger Muster.
   - **Fairness-Beauftragte:** Überprüfung, ob bestimmte Personengruppen (z. B. Schüler:innen, Senior:innen, Pendler:innen) systematisch benachteiligt werden.
   - **Incident-Manager:** Sofortmaßnahmen bei unplausiblen Ergebnissen, z. B. extremen Preisabweichungen oder Beschwerden.
     Alle Aufgaben werden im **Compliance-Register** dokumentiert und regelmäßig aktualisiert.
3. **Einführung einer KI-Policy mit Transparenz- und Feedbackmechanismen**
   Die KI-Policy schreibt vor, dass alle algorithmischen Preisentscheidungen nachvollziehbar sein müssen.
   Dazu gehören:
   - Offenlegung der Hauptfaktoren, die die Preisberechnung beeinflussen,
   - Hinweise im Kundenportal („Preise werden teilweise mithilfe eines KI-Systems berechnet"),
   - Einrichtung eines **Feedback-Kanals**, über den Fahrgäste ungewöhnliche Preisschwankungen melden können.

© A4Q Copyright 2025

Zudem wird festgelegt, dass jede wesentliche Systemänderung (z. B. neue Datenquellen) eine erneute Risikobewertung und Freigabe durch das Governance-Board erfordert.

4. **Schulung und kontinuierliche Qualifizierung des Fachpersonals**
   Mitarbeitende im Tarifmanagement und Kundendienst erhalten jährliche Schulungen zu den Themen:
   - Grundlagen des EU AI Act,
   - Fairness und Diskriminierungsvermeidung,
   - Umgang mit Kundenfeedback bei KI-basierten Entscheidungen.
     Neue Mitarbeitende müssen ein E-Learning-Modul zur „Responsible AI"-Policy absolvieren, bevor sie auf das System zugreifen dürfen.
5. **Regelmäßige Audits und externe Evaluation**
   Jährlich wird ein interner Audit zur Überprüfung der Preislogik und der Fairnessmetriken durchgeführt.
   Alle zwei Jahre erfolgt eine **externe Prüfung** durch eine unabhängige Stelle, die Bias-Tests und Systemstabilität bewertet.
   Ergebnisse werden dokumentiert und mit Maßnahmenplänen an das AI Governance Board berichtet.

Ergebnis:
Durch die frühzeitige Integration des Projekts in das KI-Governance-System entsteht eine **klare, dokumentierte Verantwortungsstruktur**.

- Alle Entscheidungen sind nachvollziehbar,
- Monitoring und Audits werden regelmäßig durchgeführt,
- Feedback aus dem Fahrgastportal fließt direkt in die kontinuierliche Verbesserung des Systems ein.

Die zuständige Aufsichtsbehörde stuft das Vorgehen als **„Best Practice"** ein: Der Verkehrsbetrieb erfüllt nicht nur die Pflichten des EU AI Act (Transparenz, Risikomanagement, Fairness), sondern etabliert eine **proaktive Governance-Kultur**, die Vertrauen schafft, sowohl bei Behörden als auch bei den Fahrgästen.

Lernbotschaft:
Dieses Beispiel soll angeblich zeigen, dass Governance kein bürokratisches Hindernis, sondern ein Erfolgsfaktor für nachhaltigen und verantwortungsvollen KI-Einsatz ist.

© A4Q Copyright 2025

13 Minimales Risiko & freiwillige Governance („Ethical AI“)

⏱ **Unterrichtszeit:** 40 Minuten

🎯 **Business Outcomes:**

- **BO 13.1** Teilnehmende entwickeln Bewusstsein für freiwillige Governance-Ansätze nach ISO 42001 und OECD.
- **BO 13.2** Teilnehmende sind vorbereitet, ethische Leitlinien mit CSR- und ESG-Zielen zu verbinden.

Lernziele (Learning Objectives – LO)

- **LO 13.1 (K2):** Teilnehmende können freiwillige internationale Governance-Rahmenwerke wie ISO/IEC 42001, OECD-Prinzipien und UNESCO-Leitlinien beschreiben.
- **LO 13.2 (K2):** Teilnehmende können erläutern, wie freiwillige Governance-Maßnahmen die Umsetzung gesetzlicher Anforderungen ergänzen.
- **LO 13.3 (K3):** Teilnehmende können ethische Leitlinien und CSR-/ESG-Ziele zu einem ganzheitlichen AI-Governance-Ansatz verknüpfen.
- **LO 13.4 (K2):** Teilnehmende können den Nutzen von Ethical-Impact-Assessments (EIA) für Organisationen erklären.
- **LO 13.5 (K1):** Teilnehmende kennen die grundlegende Bedeutung freiwilliger Governance-Instrumente für Vertrauensbildung, Selbstregulierung und internationale Anschlussfähigkeit.

Wichtige Begriffe:
Ethical AI, Corporate Social Responsibility (CSR), Environmental Social Governance (ESG), OECD AI Principles, UNESCO Ethics Recommendation, ISO/IEC 42001 Governance-Aspekte, Ethical Impact Assessment (EIA), Freiwillige Selbstverpflichtung, Ethik-Leitlinien, Transparenzkultur.

Einleitung

Während der EU AI Act verbindliche Mindeststandards vorgibt, gehen viele Organisationen bewusst darüber hinaus. Freiwillige Governance-Ansätze – wie ISO/IEC 42001 („AI Management System Standard“), die OECD-Principles for Trustworthy AI oder die UNESCO-Ethical Guidelines – schaffen einen Rahmen, um KI verantwortungsvoll, nachhaltig und gesellschaftlich verträglich zu entwickeln und einzusetzen.

© A4Q Copyright 2025

Solche Systeme dienen nicht nur der Compliance, sondern auch der Unternehmensreputation, dem Stakeholder-Vertrauen und der Erfüllung von CSR- (Corporate Social Responsibility) und ESG-Zielen (Environmental, Social, Governance).

13.1 Freiwillige Governance nach ISO/IEC 42001

Die ISO/IEC 42001 definiert ein **AI Management System (AIMS)** analog zu ISO 9001 (QM) oder ISO 27001 (ISMS). Sie unterstützt Organisationen dabei, KI-Risiken strukturiert zu steuern und Verantwortlichkeiten klar zu verankern – auch für nicht gesetzlich geregelte Systeme („minimal risk AI“).

Kernelemente:

- AI-Policy und Zielsetzung zur verantwortungsvollen Nutzung
- Rollen und Verantwortlichkeiten (z. B. AI-Governance-Officer)
- Risikomanagement nach ISO/IEC 23894
- Dokumentation, Audits und kontinuierliche Verbesserung
- Stakeholder-Einbindung und Transparenzpflichten

Praxisbeispiel:
Ein Unternehmen setzt eine Marketing-KI ein, die rechtlich nicht unter den AI Act fällt. Es führt freiwillig ein AIMS ein, erstellt eine Ethik-Policy und führt jährliche Audits durch. Ergebnis: Höheres Vertrauen bei Kunden und Investoren sowie ein nachweislich besseres Risikoprofil.

13.2 OECD-, UNESCO- und IEEE-Leitlinien für vertrauenswürdige KI

Internationale Rahmenwerke bieten grundlegende Werte, die über rechtliche Pflichten hinausgehen:

OECD Principles for Trustworthy AI (2019):

1. Inklusive Wohlfahrt und nachhaltige Entwicklung
2. Menschenzentrierte Werte und Fairness
3. Transparenz und Erklärbarkeit
4. Robustheit und Sicherheit
5. Rechenschaftspflicht (Accountability)

UNESCO Recommendation on Ethics of AI (2021):

- Menschenrechte als zentrale Leitlinie
- Verbot von Massenüberwachung und sozialem Scoring
- Schutz kultureller Diversität und Daten-Souveränität

IEEE Ethically Aligned Design:

© A4Q Copyright 2025

- Human Well-Being as Primary Goal
- Accountability through Explainability and Auditability
- Transparency by Default

Fazit: Diese Leitlinien fördern eine globale Kohärenz von Werten und erhöhen die Akzeptanz von KI-Systemen über gesetzliche Grenzen hinaus.

13.3 Ethical Impact Assessment (EIA)

Analog zur Datenschutz-Folgenabschätzung (DSFA) bewertet ein (freiwilliges) **Ethical Impact Assessment** die gesellschaftlichen, kulturellen und ökologischen Folgen eines KI-Systems.

Typische Bewertungskriterien:

- Menschenwürde und Autonomie
- Gleichbehandlung und Diversität
- Transparenz und Verantwortlichkeit
- Ökologische Nachhaltigkeit (Energieverbrauch, Ressourcennutzung)

Praxisbeispiel:
Eine Stadtverwaltung führt eine Bürger-App zur Verkehrssteuerung ein und prüft im EIA, ob ältere Menschen oder Personen ohne Smartphone benachteiligt werden. Ergebnis: Anpassung des Zugangs durch analoge Optionen und mehrsprachige Information.

13.4 Verknüpfung von Ethik, CSR und ESG

Die Verbindung ethischer KI-Governance mit CSR- und ESG-Strategien wird zunehmend zu einem Wettbewerbsfaktor.

CSR-Perspektive: Verantwortung gegenüber Mitarbeitenden, Kund:innen und Gesellschaft.
ESG-Perspektive: Nachhaltigkeits-Reporting mit AI-Ethik als Teil der Governance-Säule.

Beispielhafte Integration:

ESG-Bereich	KI-Bezug	Mögliche Maßnahme
E – Environment	Ressourceneffizienz von KI-Infrastruktur	Monitoring von Energieverbrauch und CO_2-Fußabdruck
S – Social	Nichtdiskriminierung und Inklusion	Fairness-Audits, diversitätsgerechte Trainingsdaten

© A4Q Copyright 2025

ESG-Bereich	KI-Bezug	Mögliche Maßnahme
G – Governance	Transparente Entscheidungsprozesse	AI-Ethics Board, öffentlicher Transparenzbericht

Unternehmen, die Ethik, CSR und ESG integrieren, profitieren von besserer Markenreputation, Mitarbeiterbindung und erleichtertem Zugang zu nachhaltigen Investments.

13.5 Szenario: Ethical AI bei einem Telekommunikationsanbieter

Ausgangslage: Ein Telekommunikationsunternehmen entwickelt eine KI zur Kundenabwanderungsprognose.

Vorgehen:

- Freiwillige Anwendung von ISO 42001 für Governance-Struktur
- Einrichtung eines Ethik-Boards zur Überprüfung der Trainingsdaten und Modelle
- Verknüpfung mit ESG-Zielen im Nachhaltigkeitsbericht
- Jährlicher Ethics-Audit durch interne Revisionsstelle

Ergebnis: Das System zeigt nachweislich keine Diskriminierungs-Tendenzen; die Rechenschaftsberichte werden öffentlich zugänglich gemacht. Das Unternehmen erhält eine Branchen-Auszeichnung für „Responsible AI Leadership 2028“.

© A4Q Copyright 2025

14 Audit-Readiness, Prüfpfade & Sanktionen

⏱ **Unterrichtszeit:** 30 Minuten

🎯 **Business Outcomes:**

BO 14.1 Teilnehmende sind vorbereitet, interne und externe Audits strukturiert vorzubereiten.
BO 14.2 Teilnehmende sind sensibilisiert, Korrektur- und Verbesserungsmaßnahmen aus Audit-Ergebnissen umzusetzen.

Lernziele (Learning Objectives – LO)

- **LO 14.1 (K2):** Teilnehmende können Zweck, Ablauf und Anforderungen interner und externer KI-Audits erläutern.
- **LO 14.2 (K3):** Teilnehmende können notwendige Dokumentationsnachweise und Audit-Checklisten zusammenstellen.
- **LO 14.3 (K2):** Teilnehmende können typische Findings (Mängelarten) und deren regulatorische Relevanz erklären.
- **LO 14.4 (K3):** Teilnehmende können aus Audit-Ergebnissen geeignete Corrective Actions und Continuous-Improvement-Maßnahmen ableiten.
- **LO 14.5 (K1):** Teilnehmende erinnern zentrale Sanktionsrahmen des EU AI Act (Art. 71).
- **LO 14.6 (K1):** Teilnehmende kennen die grundlegenden Schritte zur Vorbereitung eines KI-Audits.

Wichtige Begriffe:
Audit-Readiness, Audit-Policy, Prüfpfad, Selbst-Audit, Finding, Corrective Action, Re-Audit, Audit-Interview, Sanktionsrahmen, Bußgeld, Behördenmeldung, Dokumentationsversionierung, Cross-Audit-Learning.

Einführung: Warum Audit-Readiness?

Audits sind zentrale Kontrollinstrumente des EU AI Act. Sie sichern Nachvollziehbarkeit, Rechtssicherheit und Vertrauen.
Organisationen, die KI-Systeme – insbesondere Hochrisiko-Anwendungen – betreiben, müssen jederzeit nachweisen können,
dass alle regulatorischen Pflichten erfüllt sind.
Audit-Readiness bedeutet daher:

- vollständige und aktuelle Dokumentation,
- klare Verantwortlichkeiten,

© A4Q Copyright 2025

- geübte Abläufe bei Prüfungen und Vorfallmeldungen.

Ein vorbereiteter Auditprozess reduziert nicht nur Bußgeld- und Reputationsrisiken, sondern verbessert auch interne Qualitäts- und Lernprozesse.

14.1 Auditarten und Verantwortlichkeiten

Auditart	Charakteristik	Verantwortliche
Internes Audit	Regelmäßige, selbst initiierte Überprüfung der AI-Act-Pflichten (Art. 61)	KI-Officer / Compliance Manager
Externer Audit (Third Party / Notified Body)	Prüfung durch unabhängige Stelle vor Inverkehrbringen oder bei wesentlichen Änderungen (Hochrisiko)	Anbieter / Systemhersteller
Behördliches Audit	Durch Marktaufsichtsbehörden oder das AI Office bei Verdachtsfällen oder Stichproben	Nationale Aufsichtsbehörde
Kombiniertes Audit (DSFA + AI-Konformität)	Verbindung von Datenschutz- und KI-Konformitätsprüfung	Datenschutz- und KI-Officer gemeinsam

14.2 Audit-Vorbereitung

Vor jedem Audit sollten folgende Nachweise vorliegen:

1. **Technische Dokumentation** nach Art. 11 AI Act (aktuelle Version, vollständig und nachvollziehbar).
2. **Risikomanagement-Protokolle** (Art. 9): Identifizierte Risiken, Bewertung, Maßnahmen, Review-Zyklen.
3. **Human-Oversight-Nachweise** (Art. 14): Schulungs- und Freigabekonzepte für menschliche Eingriffe.
4. **Logging und Audit-Trail-Berichte** (Art. 12, 23): Vollständige, zeitlich signierte Logs.
5. **Post-Market-Monitoring-Reports** (Art. 24): Ergebnisse aus laufender Systemüberwachung.
6. **Schulungs- und Governance-Nachweise** (Art. 4(4), 29): Rollen, Trainings, Teilnahmenachweise.
7. **Incident-Management-Protokolle** (Art. 23): Meldungen, Analysen, Maßnahmen.
8. **Konformitätserklärung & CE-Dokumente** (Art. 19, 49): Gültige Erklärungen, Eintrag in EU-Datenbank.

Praxis-Tipp: Erstellen Sie ein **„Audit-Readiness-Register“** im GRC-System oder SharePoint, das alle Nachweise versioniert bündelt.

© A4Q Copyright 2025

Prüfpfade und Nachweisketten („Audit Trails“)

Ein **Prüfpfad** ist die nachvollziehbare Kette aller Belege, die zeigen, **wie** und **wann** ein Unternehmen seine Pflichten nach dem EU AI Act erfüllt hat.
Er ermöglicht Auditor:innen, Entscheidungen, Änderungen und Maßnahmen lückenlos zurückzuverfolgen – technisch wie organisatorisch.

Zweck und Nutzen

- Sicherstellung der Revisionsfähigkeit gemäß Art. 12, 23 und 61 AI Act
- Nachweis der **„Presumption of Conformity“** (Art. 40)
- Nachvollziehbarkeit für Aufsichtsbehörden und interne Audits
- Grundlage für Verbesserungs- und Haftungsnachweise

Struktur eines vollständigen Prüfpfads

Abschnitt	Inhalt / Nachweise	Typische Quelle
1. Designphase	Systembeschreibung, Zweckdefinition, Risikoeinstufung, DSFA / FRIA-Ergebnisse	Projektakte, FRIA-Report
2. Trainingsphase	Datenquellen, Datenqualität, Bias-Prüfprotokolle, Modellversionen	Data Governance Register
3. Validierungsphase	Testergebnisse, Metriken (Accuracy, Fairness), Freigabeprotokoll	Validierungsbericht
4. Inbetriebnahme	CE-Konformitätserklärung, Eintrag in EU-Datenbank, Schulungsnachweise	Compliance-Dossier
5. Betrieb / Monitoring	Logs, Monitoring-Dashboards, Incident-Reports, Human-Oversight-Eingriffe	Monitoring-System
6. Auditphase	Auditberichte, Findings, Corrective-Action-Protokolle	Audit-Register
7. Verbesserungsphase	Nachweis der Maßnahmenumsetzung, Re-Evaluation, Lessons Learned	Management-Review

Technische Anforderungen

- **Chronologische Dokumentation:** Jede Änderung oder Entscheidung erhält Zeitstempel und Verantwortliche.

© A4Q Copyright 2025

- **Unveränderbarkeit:** Nutzung manipulationssicherer Systeme (z. B. WORM-Speicher, Blockchain-Hash, digitale Signaturen).
- **Versionierung:** Jede Modell- oder Policy-Version wird eindeutig identifiziert (z. B. KI-System v1.03 – Audit 2025-05).
- **Verknüpfung der Belege:** Metadaten verbinden Audit-Nachweise mit den zugrundeliegenden Pflichten (Art. 9 – 24 AI Act).
- **Zugriffsrechte:** Nur autorisierte Personen (KI-Officer, Compliance, Auditor:innen) dürfen Änderungen oder Leserechte haben.

Beispiel: Prüfpfad eines HR-Screening-Systems

1. **Risikoklassifikation:** Hochrisiko nach Anhang III – Dokument vom 02. 03. 2025
2. **Datensatzprüfung:** Bias-Report #HR-2025-07 mit DIR = 0,88
3. **Modellvalidierung:** Fairness-Audit am 17. 04. 2025, Freigabe durch KI-Officer
4. **Schulung:** HR-Training #2025-06 – Teilnehmerliste & Quiznachweis
5. **Post-Market-Monitoring:** Halbjahres-Report Q3/2025 mit KPI-Abweichung < 2 %
6. **Incident-Ticket:** #INC-2025-09 – „Bias-Verdacht“ – Status: behoben (05. 10. 2025)
7. **Re-Audit:** 12. 10. 2025 – Keine Beanstandungen

Alle Einträge sind digital im Audit-Repository versioniert und mit Hashwert signiert.

Best-Practice-Empfehlung

- Einheitliche **Audit-Trail-Vorlage** mit Spalten: *Pflicht*, *Nachweis*, *Datum*, *Verantwortlich*, *Status*, *Verweis*.
- Automatisierte Protokollierung durch GRC- oder Compliance-Tools.
- Regelmäßige **Trail-Integrity-Checks** (Hash-Verifikation).
- Integration des Prüfpfads in das **Konformitätsdossier** gemäß Art. 17 AI Act.

14.3 Typische Audit-Findings und Mängelarten

Mangelart	Beschreibung	Konsequenz
Formeller Mangel	Fehlende oder veraltete Dokumentation (z. B. fehlendes Modell-Versionierungssystem)	Auflage zur Nachbesserung

© A4Q Copyright 2025

Mangelart	Beschreibung	Konsequenz
Funktionaler Mangel	Unvollständige Implementierung gesetzlicher Pflichten (z. B. kein Human-Oversight-Prozess)	temporäre Betriebsbeschränkung
Schwerwiegender Mangel	Systemischer Verstoß gegen Grundrechte (z. B. Bias ohne Gegenmaßnahmen)	Bußgeld oder Betriebsverbot
Verfahrensmangel	Kein Incident-Prozess oder unzureichende Audit-Nachverfolgung	verpflichtende Korrekturmaßnahme
Kommunikationsmangel	Nutzer:innen nicht korrekt über KI-Einsatz informiert (Art. 13/52)	Abmahnung, Image-Schaden

14.4 Sanktionen gemäß EU AI Act (Art. 71)

Verstoß	Maximalstrafe
Einsatz verbotener KI-Praktiken (Art. 5)	bis 30 Mio. € oder 6 % des weltweiten Jahresumsatzes
Verstoß gegen Pflichten bei Hochrisiko-Systemen (Art. 9 – 15)	bis 20 Mio. € oder 4 % des Umsatzes
Falsche Angaben an Behörden oder fehlende Meldungen (Art. 23 – 24)	bis 10 Mio. € oder 2 % des Umsatzes
Nichtbeachtung behördlicher Anordnungen	gestaffelte Zwangsgelder + Registrierungsausschluss

Zusätzlich kann die Behörde Vertriebsstopps, Marktrücknahmen oder öffentliche Verwarnungen verhängen.

14.5 Korrektur- und Verbesserungsmaßnahmen

Corrective Actions (CA)

- Sofortmaßnahmen zur Behebung konkreter Mängel
- Beispiel: Nachtraining des Modells, Ergänzung fehlender Audit-Trails, Nachschulung des Personals

Preventive / Improvement Actions (PA)

- Strukturelle Verbesserungen zur Vermeidung zukünftiger Mängel

© A4Q Copyright 2025

- Beispiel: Einführung eines vierteljährlichen Audit-Zyklus, automatisierte Bias-Checks, Erweiterung des Compliance-Dashboards

Audit-Follow-up-Prozess

1. Bewertung des Findings → Schweregrad und Ursache
2. Erstellung eines Maßnahmenplans mit Fristen
3. Freigabe durch KI-Officer und Management
4. Implementierung & Wirksamkeitsprüfung
5. Abschlussbericht & Lessons Learned

14.6 Praxisfall: Audit-Vorbereitung Hochrisiko-System

Praxisbeispiel: Audit eines KI-Systems zur automatisierten Schadensprüfung

Ausgangssituation:
Ein Versicherungsunternehmen nutzt ein KI-System, das eingereichte Schadensmeldungen automatisch prüft und eine Empfehlung zur Auszahlung abgibt.
Ziel ist es, die Bearbeitungszeit zu verkürzen und eine konsistente Entscheidungspraxis sicherzustellen.
Da das System in einem sensiblen Geschäftsbereich eingesetzt wird, unterliegt es den Pflichten für Hochrisiko-KI-Systeme gemäß Artikeln 9–24 des EU AI Act.

Audit-Vorbereitung:
Zur Vorbereitung eines geplanten internen Audits werden die regulatorischen Nachweise systematisch zusammengetragen:

- Der **KI-Officer** erstellt eine **Audit-Checkliste** auf Basis der Artikel 9 bis 24 AI Act (Risikomanagement, Datenqualität, Transparenz, Human Oversight, Monitoring).
- Die **Fachabteilungen** liefern alle relevanten Dokumente: Trainings- und Testdatensätze, Modellbeschreibungen, Validierungsberichte, Logging-Protokolle und Monitoring-Auswertungen.
- Im **Vorab-Interview mit der Auditorin** werden die Schwerpunkte des Audits festgelegt – insbesondere die Kontrolle möglicher **Bias-Risiken** (Diskriminierungstendenzen in historischen Schadensdaten) und die Überprüfung funktionierender **Fallback-Mechanismen** (menschliche Eingriffsmöglichkeiten bei Unsicherheiten).

Audit-Durchführung und Ergebnisse:
Im Rahmen des Audits werden mehrere Stärken, aber auch Verbesserungspotenziale festgestellt:

- **Finding 1:** Die jährliche Schulung der Schadenssachbearbeitenden („Claims Manager“) war nicht mehr aktuell.

© A4Q Copyright 2025

→ *Corrective Action:* Durchführung einer verpflichtenden Nachschulung innerhalb von 30 Tagen mit dokumentiertem Teilnahme-Nachweis.

- **Finding 2:** Das bestehende **Post-Market-Monitoring** war unvollständig, insbesondere fehlte eine Übersicht der automatisierten Entscheidungen nach Schadensart.
  → *Corrective Action:* Einführung eines neuen Dashboards zur fortlaufenden Überwachung von Entscheidungstrends, Fehlerraten und Fairness-Indikatoren.

Ergebnis:
Der Auditbericht bewertet das KI-System insgesamt als **regelkonform mit Auflagen**.
Positiv hervorgehoben werden die klar dokumentierten Prozesse, das strukturierte Risikomanagement und die Bereitschaft zur Verbesserung.
Durch die Umsetzung der Corrective Actions entstehen konkrete Fortschritte:

- Das Monitoring wird datenbasierter und transparenter.
- Die Verantwortlichkeiten für Human Oversight werden geschärft.
- Der interne Reporting-Workflow wird effizienter und revisionssicherer gestaltet.

Lernbotschaft:
Dieses Beispiel zeigt, dass Audits nicht nur Kontrollinstrumente sind, sondern **eine zentrale Lern- und Verbesserungsfunktion** haben (sollen).
Organisationen, die Audits sorgfältig vorbereiten, Findings ernst nehmen und Korrekturmaßnahmen dokumentiert umsetzen, erhöhen ihre **Compliance-Reife**, stärken das Vertrauen von Aufsichtsbehörden – und schaffen die Grundlage für eine nachhaltige, verantwortungsvolle KI-Governance.

14.7 Best Practices für Audit-Readiness

Eine hohe Audit-Readiness entsteht nicht durch einzelne Maßnahmen, sondern durch eine **systematische und gelebte Audit-Kultur** im Unternehmen.
Folgende bewährte Vorgehensweisen haben sich in der Praxis als besonders wirksam erwiesen:

1. **Audit-Policy einführen und verbindlich verabschieden**
   Jede Organisation sollte eine klare, schriftlich verabschiedete **Audit-Policy** besitzen.
   Diese legt fest, *wer* für Audits verantwortlich ist, *wann* diese stattfinden und *welche Prozesse* dabei eingehalten werden.
   So werden Zuständigkeiten, Fristen und Berichtspflichten verbindlich geregelt und Audit-Aktivitäten in das reguläre Compliance-Management eingebettet.

2. **Regelmäßige Selbst-Audits durchführen**
   Halbjährliche **interne Selbst-Audits** fördern die kontinuierliche Überprüfung der eigenen Konformität.
   Dabei kann ein **KI-Readiness-Score** verwendet werden, um die Fortschritte messbar zu machen und Schwachstellen frühzeitig zu erkennen.

© A4Q Copyright 2025

3. **Versionierte Dokumentation pflegen**
   Alle Audit-relevanten Unterlagen sollten versioniert geführt werden.
   Jede Änderung – ob an Modellen, Prozessen oder Richtlinien – muss nachvollziehbar dokumentiert sein:
   Was wurde geändert? Wann? Und warum?
   Diese Nachvollziehbarkeit ist essenziell für spätere Behördenprüfungen und interne Kontrollen.

4. **Cross-Audit Learning nutzen**
   Organisationen profitieren, wenn sie Erkenntnisse aus anderen Prüfbereichen – etwa **Datenschutz-Audits (DSGVO)**, **IT-Sicherheitsaudits (ISO 27001)** oder **AI-Management-Audits (ISO/IEC 42001)** – auf ihre KI-Systeme übertragen.
   Dieses **Cross-Learning** stärkt Synergien zwischen bestehenden Managementsystemen und schafft einheitliche Qualitäts- und Prüfstandards.

5. **Trainings- und Awareness-Programme etablieren**
   Alle Mitarbeitenden, die in Auditprozesse eingebunden sind, sollten regelmäßig geschult werden.
   Dazu gehören Auditor:innen, Fachverantwortliche, Entwickler:innen und Management.
   Ziel ist ein gemeinsames Verständnis von Audit-Zielen, Nachweispflichten und Verbesserungsprozessen.

6. **Interdisziplinäre Audit-Teams bilden**
   KI-Audits erfordern Expertise aus verschiedenen Fachrichtungen.
   Empfehlenswert ist ein **interdisziplinäres Audit-Team**, bestehend aus Vertreter:innen aus **Recht, Technik, Ethik, Datenschutz und Compliance**.
   Diese Zusammensetzung stellt sicher, dass technische, rechtliche und ethische Aspekte gleichermaßen bewertet werden und Risiken ganzheitlich betrachtet werden.

© A4Q Copyright 2025

15 Harmonisierte Standards & Presumption of Conformity

⏱ 30 Minuten

🎯 Business Outcomes:

BO 15.1: Teilnehmende entwickeln Verständnis für die Bedeutung harmonisierter Normen als Compliance-Nachweis.

BO 15.2: Teilnehmende sind vorbereitet, aktuelle Standards zu bewerten und deren Anwendung im Projekt zu unterstützen.

Lernziele (Learning Objectives – LO)

- **LO 15.1 (K2):** Teilnehmende können erklären, was harmonisierte europäische Normen sind und welche Rolle sie im Rahmen des EU AI Act spielen.
- **LO 15.2 (K2):** Teilnehmende können die Bedeutung der „Presumption of Conformity“ erläutern.
- **LO 15.3 (K3):** Teilnehmende können einschätzen, welche internationalen Normen (z. B. ISO/IEC 42001, ISO/IEC 23894) zur Umsetzung von Compliance-Anforderungen geeignet sind.
- **LO 15.4 (K3):** Teilnehmende können den praktischen Nutzen harmonisierter Standards für Audit-Vorbereitung, Nachweisführung und Risikominimierung bewerten.
- **LO 15.5 (K1):** Teilnehmende kennen den Zusammenhang zwischen harmonisierten Normen, technischen Spezifikationen und ihrer Funktion als Nachweisinstrumente im Konformitätsverfahren.

Wichtige Begriffe:

Harmonisierte Norm, Presumption of Conformity, CEN, CENELEC, ISO/IEC JTC 1/SC 42, EN Norm, DIN, ÖNORM, SNV, Standardbibliothek, Normen-Mapping, Gap-Analyse, Normungsprozess, CEN/CENELEC JTC 21, Cross-Audit Learning.

Einführung

Der EU AI Act definiert grundlegende Anforderungen an sichere und vertrauenswürdige KI. Die konkrete Umsetzung dieser Anforderungen erfolgt jedoch oft über **harmonisierte europäische Normen**, die von **CEN** (Europäisches Komitee für Normung) und **CENELEC** (Europäisches Komitee für elektrotechnische Normung) entwickelt werden.

Werden solche Normen korrekt angewendet, gilt eine gesetzliche **Vermutung der Konformität** („Presumption of Conformity“) – das bedeutet:

© A4Q Copyright 2025

Ein System, das den relevanten harmonisierten Normen entspricht, wird als mit den Anforderungen des AI Act konform angesehen, solange keine gegenteiligen Nachweise bestehen.

Damit sind harmonisierte Normen der zentrale Brückenschlag zwischen **gesetzlicher Pflicht** und **technischer Umsetzung**.

15.1 Begriff und Funktion harmonisierter Normen

Definition:
Harmonisierte Normen sind von der EU Kommission veröffentlichte technische Spezifikationen, die Anforderungen aus EU-Verordnungen oder Richtlinien konkretisieren.

Merkmale:

- Sie werden im Amtsblatt der EU als „harmonisiert“ bekanntgegeben.
- Sie sind freiwillig, dienen aber als **Nachweis** für die Einhaltung rechtlicher Vorgaben.
- Sie werden regelmäßig überarbeitet und an neue regulatorische Entwicklungen angepasst.

Beispiel:
Die Anwendung von **ISO/IEC 42001** (Managementsystem für KI) und **ISO/IEC 23894** (Risikomanagement für KI) kann zeigen, dass ein Unternehmen die Artikel 9–23 des EU AI Act systematisch umsetzt – und somit die Presumption of Conformity erreicht.

15.2 Presumption of Conformity – rechtlicher Hintergrund

Die Presumption of Conformity ist in Artikel 40 EU AI Act verankert.
Sie bedeutet:

Wer die in harmonisierten Normen festgelegten technischen Anforderungen erfüllt, muss nicht zusätzlich nachweisen, dass die gesetzlichen Anforderungen erfüllt sind.

Vorteile:

- Reduktion des Prüf- und Dokumentationsaufwands
- Rechtssicherheit bei Audits und Marktaufsicht
- Erleichterter Zugang zur CE-Kennzeichnung
- Einheitliche Bewertungsgrundlage für Anbieter, Betreiber und Prüfer

Wichtig:
Die Presumption of Conformity ist keine automatische Freistellung.
Unternehmen müssen belegen können,

- welche Normen angewendet wurden,

© A4Q Copyright 2025

- wie sie umgesetzt wurden, und
- welche Abweichungen oder Ergänzungen vorliegen.

15.3 Aktuelle Normenlandschaft (Auswahl, 2025)

Norm / Standard	Themenbereich	Relevanz für AI Act
ISO/IEC 42001	KI-Managementsystem (AIMS)	Strukturiert Prozesse für Governance, Verantwortung und kontinuierliche Verbesserung (Art. 17 ff.)
ISO/IEC 23894	KI-Risikomanagement	Operationalisierung von Art. 9 Risikomanagementpflicht
ISO/IEC 22989	Begriffe & Konzepte	Einheitliche Terminologie für Dokumentation & Audits
ISO/IEC 23053	ML-Framework	Grundlage für Modell-Design, Training & Validierung
ISO/IEC TR 24028	Sicherheit & Resilienz	Ergänzt Art. 15 – Robustheit, Genauigkeit, Cybersecurity
DIN SPEC 92001-1/-2	Qualitätsanforderungen an KI	Frühere nationale Vorläufer, hilfreich für interne Policies
ISO/IEC 27001 & 27701	Informations- & Datenschutzmanagement	Relevanz für Art. 10 (Datenqualität) & Art. 29 (Betrieb)
ISO/IEC 42006 (in Entwicklung)	Human Oversight & Accountability	Erwartet 2026 – unterstützt Art. 14 AI Act

15.4 Integration harmonisierter Standards im Unternehmen

Ein wirkungsvolles Compliance-System nutzt Normen als **Rahmen für Governance und Nachweisführung**.

Empfohlene Schritte:

1. **Mapping durchführen:** Zuordnung der AI-Act-Artikel zu relevanten Normen (z. B. Art. 9 ↔ ISO/IEC 23894).
2. **Lückenanalyse:** Prüfung, welche Normanforderungen bereits erfüllt sind.

© A4Q Copyright 2025

3. **Implementierung:** Prozesse, Rollen und Dokumentationsstrukturen an die Norm anlehnen.
4. **Auditvorbereitung:** Normbasierte Checklisten (z. B. DIN EN ISO/IEC 42001 Annex A) verwenden.
5. **Kontinuierliche Verbesserung:** Regelmäßige Reviews und Updates bei Normrevisionen.

Praxisbeispiel: ISO/IEC 42001 als Nachweis der Presumption of Conformity

Ein europäischer **Medizintechnikhersteller** entwickelt ein **KI-gestütztes Diagnose-Tool**, das Röntgenbilder analysiert und Ärzt:innen eine Risikoeinschätzung liefert.
Da das System direkt gesundheitliche Entscheidungen beeinflusst, fällt es unter die **Hochrisiko-Kategorie nach Anhang III Abschnitt 11 des EU AI Act** („Medizinische Geräte mit KI-Funktion“).

Um die gesetzlichen Anforderungen aus Artikeln 9 bis 23 AI Act strukturiert umzusetzen, entscheidet sich das Unternehmen für die Einführung eines **KI-Managementsystems nach ISO/IEC 42001**. Diese Norm definiert einen vollständigen Governance- und Kontrollrahmen, vergleichbar mit ISO 9001 oder ISO 27001, jedoch spezifisch für KI.

Schritt 1: Implementierung des AI-Managementsystems

Das Unternehmen richtet ein **AI Governance-Board** ein, das Richtlinien, Zuständigkeiten und Eskalationspfade festlegt.

- **Art. 9 AI Act – Risikomanagement:** Es wird ein standardisierter Prozess eingeführt, der technische, ethische und rechtliche Risiken bewertet.
- **Art. 10 – Datenqualität:** Ein Data-Governance-Team prüft alle Trainings- und Validierungsdaten auf Repräsentativität und Bias.
- **Art. 11–15 – Dokumentation, Logging, Transparenz, Human Oversight:**
  Die Norm fordert Prozesshandbücher, Audit-Protokolle und Nachweise für menschliche Kontrollmechanismen.
- **Art. 17 ff. – Konformitätsbewertung:** Interne Audits und Management-Reviews werden mindestens halbjährlich durchgeführt.

Schritt 2: Schulungen gemäß Artikel 4(4) AI Act

Alle am Entwicklungs- und Prüfprozess beteiligten Mitarbeitenden absolvieren modulare Schulungen, die in das Qualitätsmanagementsystem integriert sind:

- **Entwickler:innen** → Modellvalidierung, Bias-Erkennung, Dokumentationspflichten
- **Klinische Fachexpert:innen** → Interpretation der KI-Ergebnisse, Eingriffsrechte (Human Oversight)

© A4Q Copyright 2025

- **Compliance- und IT-Teams** → Nachweisführung, Auditvorbereitung, Logging
  Die Teilnahme wird digital erfasst und jährlich erneuert. Damit ist die Schulungspflicht aus Art. 4(4) AI Act revisionssicher erfüllt.

Schritt 3: Versionierte Dokumentation und Nachvollziehbarkeit

Alle Änderungen an Modellen, Daten oder Prozessen werden zentral in einem **Change-Log-Register** dokumentiert.
Jeder Eintrag enthält:

- Änderungsgrund (z. B. neue Datensätze, Modell-Retraining)
- Datum, Verantwortliche, Prüfprotokoll
- Auswirkungen auf Risiko- oder Konformitätsbewertung
- Freigabe durch den KI-Officer

Dieses Vorgehen entspricht sowohl den Nachweisanforderungen des **Art. 11 AI Act** (Technische Dokumentation) als auch der ISO/IEC 42001-Kapitelstruktur zu „Documented Information“ und „Continuous Improvement“.

Schritt 4: Audit und Anerkennung durch Marktaufsicht

Bei einer externen Überprüfung durch eine benannte Stelle (Notified Body) kann das Unternehmen **lückenlos belegen**,

- welche Prozesse, Rollen und Verfahren die AI-Act-Anforderungen abdecken,
- dass alle Schulungen und Prüfungen nachweislich stattgefunden haben,
- und dass alle Änderungen und Evaluierungen versioniert nachvollziehbar sind.

Die Prüfer:innen bestätigen, dass das Unternehmen durch Anwendung harmonisierter Normen (insbesondere ISO/IEC 42001 + ISO/IEC 23894) ein systematisches, dokumentiertes und funktionsfähiges Compliance-Management eingerichtet hat.

Ergebnis

Die Marktaufsichtsbehörde erkennt das Unternehmen als **konform gemäß Artikel 40 AI Act („Presumption of Conformity“) an**.
Dadurch:

- entfällt die Pflicht zu zusätzlichen technischen Prüfungen,
- wird die CE-Kennzeichnung erleichtert,
- und die Nachweisdauer im Audit verkürzt sich erheblich.

Darüber hinaus stärkt das Managementsystem das interne Qualitäts- und Risikobewusstsein: Änderungen, Incidents oder neue regulatorische Anforderungen können schnell und strukturiert adressiert werden – die

© A4Q Copyright 2025

Organisation entwickelt eine **nachhaltige KI-Compliance-Kultur**, die über die gesetzlichen Mindestpflichten hinausgeht.

15.5 Zusammenarbeit von CEN/CENELEC und ISO bei der Normung

Die europäischen und internationalen Normungsorganisationen arbeiten eng zusammen, um sicherzustellen, dass sich technische Standards für Künstliche Intelligenz nicht widersprechen, sondern aufeinander abgestimmt sind.

- **CEN/CENELEC JTC 21** ist das zentrale europäische Fachgremium für die Entwicklung von Normen im Bereich der Künstlichen Intelligenz. Hier werden Entwürfe für harmonisierte europäische KI-Normen erarbeitet, die später als Grundlage für die Presumption of Conformity nach dem EU AI Act dienen können.
- Dieses Gremium arbeitet **eng mit dem internationalen Komitee ISO/IEC JTC 1/SC 42** („Artificial Intelligence“) zusammen, das weltweit an KI-Standards arbeitet – etwa an der ISO/IEC 42001 (KI-Managementsysteme) oder der ISO/IEC 23894 (Risikomanagement für KI).
- Das gemeinsame Ziel dieser Kooperation ist es, **weltweit kompatible und konsistente Standards** zu schaffen. So wird verhindert, dass in Europa, den USA oder Asien unterschiedliche technische Anforderungen gelten, die den internationalen Handel oder die Zertifizierung erschweren würden.
- In jedem EU-Mitgliedsstaat gibt es **nationale Spiegelgremien** – beispielsweise das **DIN** in Deutschland, die **ÖNORM** in Österreich (ähnlich die **SNV** in der Schweiz). Diese nationalen Gremien ermöglichen es Unternehmen, Hochschulen und Forschungseinrichtungen, aktiv an der Ausarbeitung neuer KI-Normen mitzuwirken und eigene Praxiserfahrungen einzubringen.

Dadurch entsteht ein transparenter, partizipativer Prozess: europäische Organisationen können frühzeitig Einfluss nehmen, wie KI-Standards gestaltet werden – und gleichzeitig sicherstellen, dass die europäischen Interessen und Datenschutzprinzipien in internationale Normen einfließen.

15.6 Best Practices für den Einsatz harmonisierter Normen

Die Anwendung harmonisierter und international anerkannter Normen ist kein einmaliger Schritt, sondern ein kontinuierlicher Prozess. Unternehmen, die Normen systematisch in ihre Governance- und

© A4Q Copyright 2025

Qualitätsstrukturen integrieren, profitieren von höherer Rechtssicherheit, effizienteren Audits und einer klaren Nachweisführung gegenüber Aufsichtsbehörden.

Im Folgenden sind bewährte Vorgehensweisen („Best Practices“) dargestellt, die sich in der Praxis bereits etabliert haben:

1. Standardbibliothek aufbauen

Richten Sie eine **zentrale Ablage** für alle relevanten Normen, Leitfäden und technischen Spezifikationen ein – idealerweise mit Verantwortlichen für Pflege und Aktualisierung.
Diese Bibliothek sollte sowohl europäische (CEN/CENELEC) als auch internationale (ISO/IEC) Standards enthalten.
→ Vorteil: Alle Fachbereiche greifen auf dieselbe, aktuelle Informationsbasis zu – insbesondere bei Audits oder Zertifizierungen.

2. Normen-Mapping in Policies integrieren

Verankern Sie den Bezug zu Normen direkt in Ihren internen **KI-Policies und Verfahrensanweisungen**.
Jede Richtlinie, die sich auf Entwicklung, Betrieb oder Überwachung von KI-Systemen bezieht, sollte klar angeben, welche Norm oder welcher Abschnitt herangezogen wird (z. B. „gemäß ISO/IEC 23894 Abschnitt 6.3 – Risikobewertung“).
→ So entsteht Transparenz und Konsistenz zwischen internen Vorgaben und externen Prüfanforderungen.

3. Schulung und Awareness fördern

Fachabteilungen sollten regelmäßig über **aktuelle Normrevisionen, neue Standards oder geänderte Interpretationen** informiert werden.
Empfehlenswert sind kurze Awareness-Sessions oder interne Newsletter, um sicherzustellen, dass neue Anforderungen frühzeitig in Projekte einfließen.
→ So bleibt die Organisation stets auf dem neuesten Stand und vermeidet Compliance-Lücken.

4. Cross-Audit Learning nutzen

Viele Anforderungen aus KI-Normen überschneiden sich mit etablierten Managementsystemen wie **ISO 9001 (Qualitätsmanagement)** oder **ISO 27001 (Informationssicherheit)**.
Unternehmen können aus diesen bestehenden Audit-Erfahrungen lernen – etwa durch die Wiederverwendung von Dokumentations-Templates, Auditchecklisten oder Lessons Learned.
→ Dadurch werden Synergien genutzt und Doppelarbeit reduziert.

5. Regelmäßige Gap-Analysen durchführen

Mindestens einmal jährlich sollte eine **Gap-Analyse** durchgeführt werden, um zu prüfen,

- ob neue oder überarbeitete KI-Normen veröffentlicht wurden,
- welche Normen inzwischen harmonisiert sind,

© A4Q Copyright 2025

- und ob bestehende interne Prozesse noch alle Anforderungen erfüllen.
  → Diese regelmäßige Überprüfung schafft Planungssicherheit und bereitet die Organisation optimal auf zukünftige Audits vor.

© A4Q Copyright 2025

16 Globale Schnittstellen & Exportkontrolle

⏱ 60 Minuten

🎯 Business Outcomes:

BO 16.1 Teilnehmende sind vorbereitet, Risiken aus Datenexport, Dual-Use und IP-Rechten einzuschätzen.
BO 16.2 Teilnehmende sind vorbereitet, Compliance-Anforderungen in internationalen Lieferketten zu unterstützen.

Lernziele (Learning Objectives – LO)

- **LO 16.1 (K2):** Teilnehmende können erklären, welche regulatorischen Risiken beim Export von KI-Systemen und Daten in Drittstaaten bestehen.
- **LO 16.2 (K2):** Teilnehmende können Dual-Use-Beschränkungen und Exportkontrollen auf KI-Technologien einordnen.
- **LO 16.3 (K2):** Teilnehmende kennen Maßnahmen zur rechtskonformen Gestaltung internationaler Lieferketten und Datentransfers.
- **LO 16.4 (K1):** Teilnehmende kennen zentrale internationale Themenfelder wie Exportkontrolle, IP-Rechte und Dual-Use-Bestimmungen.
- **LO 16.5 (K1):** Teilnehmende kennen die grundlegende Bedeutung internationaler Abkommen und multilateraler Regelwerke für den sicheren und rechtskonformen Umgang mit KI-Technologien.

Wichtige Begriffe:
Datenexport, Datenlokalisierung, Dual-Use-Güter, Exportkontrolle, IP-Rechte, Lizenzprüfung, WTO-Regeln, Lieferketten-Compliance, Sanktionsliste, Drittstaatentransfer, Internationales Abkommen, Handelsrecht, ITAR/EAR, Compliance-Register.

Einleitung

KI-Systeme werden zunehmend global entwickelt, trainiert und betrieben. Damit entstehen neue Risiken aus **Exportkontrolle, Datenlokalisierung und geistigem Eigentum (IP)**.
Unternehmen müssen sicherstellen, dass KI-Modelle, Trainingsdaten und Komponenten nur in Ländern genutzt werden, die ausreichenden Rechts- und Datenschutzstandard gewährleisten.

16.1 Datenexport und Datenlokalisierung

© A4Q Copyright 2025

Der grenzüberschreitende Transfer von Daten ist für viele KI-Systeme unvermeidlich – insbesondere, wenn Trainings-, Validierungs- oder Betriebsdaten in globalen Cloud-Umgebungen verarbeitet werden.
Gleichzeitig zählt der **internationale Datentransfer** zu den sensibelsten Bereichen der KI-Compliance, da dabei die Kontrolle über den Schutz personenbezogener Informationen teilweise verloren gehen kann.

Rechtlicher Rahmen

Die **Datenschutz-Grundverordnung (DSGVO)** regelt in den Artikeln **46 ff.** die Voraussetzungen für den Export personenbezogener Daten in Länder außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums.
Zusätzlich verpflichtet der **EU AI Act (Art. 10 Abs. 5)** Anbieter und Betreiber von Hochrisiko-KI-Systemen sicherzustellen, dass alle Datenverarbeitungsprozesse – einschließlich Speicherung und Training – im Einklang mit geltenden Datenschutzbestimmungen erfolgen.

Das bedeutet: Auch wenn die KI-Entwicklung technisch global organisiert ist, bleibt die rechtliche Verantwortung für den Schutz personenbezogener Daten immer bei der europäischen Organisation, die das System bereitstellt oder betreibt.

Typische Risiken

Ein zentrales Risiko liegt im **Verlust des Datenschutzes** bei der Übertragung in sogenannte „unsichere Drittstaaten“, also Länder ohne von der EU anerkanntes angemessenes Datenschutzniveau.
Dadurch können Betroffene ihre Rechte auf Auskunft, Löschung oder Widerspruch faktisch nicht mehr durchsetzen.
Auch die unbefugte Weitergabe, das Data-Mining durch Dritte oder staatlicher Zugriff auf gespeicherte Daten (z. B. nach nationalem Sicherheitsrecht) stellen erhebliche Compliance-Risiken dar.

Beispiel:
Ein Unternehmen trainiert ein Sprachmodell in einer Cloud-Region außerhalb der EU. Die dort gespeicherten Nutzerdaten unterliegen nicht mehr der DSGVO. Ohne geeignete Schutzmaßnahmen droht ein Datenschutzverstoß mit Bußgeldern nach Art. 83 DSGVO.

Maßnahmen für eine rechtskonforme Datenübertragung

Um diese Risiken zu beherrschen, sollten Organisationen folgende Schutzmaßnahmen umsetzen:

1. **Einsatz genehmigter Standardvertragsklauseln (SCCs):**
   Diese von der Europäischen Kommission verabschiedeten Vertragsmuster sichern zu, dass der Empfänger außerhalb der EU ein mit der DSGVO vergleichbares Schutzniveau gewährleistet. Sie sind das zentrale Instrument für den rechtssicheren Datentransfer in Drittländer ohne Angemessenheitsbeschluss.
2. **Prüfung des Empfängerlandes auf angemessenes Datenschutzniveau:**
   Vor jedem Datentransfer sollte geprüft werden, ob die EU-Kommission das Zielland als datenschutzkonform anerkannt hat.

© A4Q Copyright 2025

Beispiel: Das **EU–US Data Privacy Framework (2023)** erlaubt zertifizierten US-Unternehmen den Empfang personenbezogener Daten aus der EU unter klar definierten Auflagen.

3. **Interne Freigabeprozesse für Cloud- oder Offshore-Trainingsdaten:**
   Jede externe Datenverarbeitung – insbesondere in Cloud- oder Rechenzentren außerhalb der EU – sollte ein **formales Freigabeverfahren** durchlaufen.
   Dieses sollte die Bewertung folgender Aspekte umfassen:
   - Ort und Verantwortlichkeit der Datenverarbeitung
   - Vorhandensein geeigneter Sicherheitszertifikate (z. B. ISO 27001)
   - Verschlüsselungs- und Zugriffskontrollen
   - Vertragliche Regelungen zur Datenrückgabe und -löschung
4. **Dokumentation und Monitoring:**
   Alle internationalen Datenübertragungen müssen nachvollziehbar dokumentiert werden. Dazu gehört die Aufzeichnung der beteiligten Dienstleister, der Zweck der Übertragung sowie die eingesetzten Schutzmechanismen.
   Ein kontinuierliches Monitoring stellt sicher, dass sich Änderungen in der Rechtslage (z. B. Aufhebung eines Angemessenheitsbeschlusses) zeitnah in den Compliance-Prozessen widerspiegeln

16.2 Dual-Use-Güter und Exportkontrolle

Die Europäische Union unterliegt einem einheitlichen **Regelwerk zur Exportkontrolle**, das auch auf digitale Technologien und KI-Systeme angewendet wird. Besonders relevant ist dabei der sogenannte **Dual-Use-Bereich** – also Güter, Software oder Technologien, die sowohl **zivile** als auch **militärische oder sicherheitsrelevante** Zwecke erfüllen können.

Definition und rechtlicher Rahmen

Der Begriff **„Dual-Use-Gut“** ist in der **Verordnung (EU) 2021/821** über eine **Unionsregelung für die Kontrolle von Ausfuhren, Vermittlung, technischer Unterstützung, Durchfuhr und Verbringung von Dual-Use-Gütern** definiert.
Diese Verordnung gilt **in allen Mitgliedstaaten der EU unmittelbar** und legt fest, wann eine Genehmigungspflicht für den Export von Gütern oder Technologien besteht, die potenziell auch militärisch eingesetzt werden können.

Zu den kontrollierten Gütern zählen nicht nur physische Produkte, sondern zunehmend auch **immaterielle digitale Technologien**, wie z. B.:

- Software, die zur Entwicklung oder Steuerung autonomer Systeme eingesetzt werden kann,

© A4Q Copyright 2025

- KI-Modelle zur Mustererkennung oder Gesichtserkennung,
- Algorithmen zur Kryptographie, Netzwerksicherheit oder Überwachung,
- Simulations- und Trainingsdaten, die in sicherheitskritischen Anwendungen genutzt werden können.

Bedeutung für KI-Systeme

Mit dem Aufkommen leistungsfähiger KI-Technologien geraten auch Software, Trainingsdaten und Modelle unter den Anwendungsbereich der Dual-Use-Verordnung.
Ein KI-System, das ursprünglich für zivile Zwecke (z. B. industrielle Bildverarbeitung) entwickelt wurde, kann z. B. zur **militärischen Zielerkennung, Überwachung oder Drohnensteuerung** missbraucht werden.
Damit verbunden ist eine **Prüfpflicht**, ob ein Export – also jede grenzüberschreitende Übertragung oder Bereitstellung – einer Genehmigung bedarf.

Beispiele für Dual-Use-relevante KI-Technologien:

- Systeme zur **Gesichts- oder Objekterkennung** in Videodaten (potenzieller Einsatz in Überwachungstechnologien),
- KI-Modelle zur **autonomen Navigation** von Fahrzeugen oder Drohnen,
- **Spracherkennungssysteme** für Sicherheitsanwendungen,
- Software zur **Entschlüsselung, Cyberabwehr oder Datenanalyse** im sicherheitsrelevanten Umfeld.

Diese Technologien gelten nicht per se als verboten, erfordern aber – abhängig vom Empfängerland, Zweck und Nutzer – eine **Exportgenehmigung** oder eine **Vorabprüfung durch die zuständigen Behörden**.

Verpflichtungen für Unternehmen in der EU

Unternehmen, die KI-Software, Quellcode oder Trainingsdaten an Partner außerhalb der EU weitergeben, müssen vorab prüfen, ob:

- der Exportgegenstand in der **Dual-Use-Liste** der EU (Anhang I der Verordnung 2021/821) aufgeführt ist,
- der Empfänger oder das Zielland auf einer **Sanktions- oder Embargoliste** steht,
- oder der **Endverwendungszweck** sicherheitspolitisch relevant ist (z. B. militärische Nutzung, Überwachung, Waffenentwicklung).

Besonders zu beachten ist, dass auch **immaterielle Transfers** – etwa das Hochladen von Modellen in ausländische Cloud-Systeme, das Teilen von Code über Online-Repositories oder der Fernzugriff auf Trainingsserver – als Export im Sinne der Verordnung gelten können.

© A4Q Copyright 2025

Praktische Maßnahmen für KI-Organisationen

1. **Exportprüfungen vor Weitergabe von KI-Software oder Trainingsdaten:**
   Jede Weitergabe oder Veröffentlichung sollte durch eine strukturierte Exportkontrolle begleitet werden. Dazu gehört:
   - Abgleich mit der Dual-Use-Liste (insbesondere Kategorie 4 – Informationssicherheit, Kategorie 6 – Sensorik, Kategorie 9 – Luft- und Raumfahrttechnik),
   - Prüfung des Empfängers und Endverwendungszwecks,
   - ggf. Einholung einer Genehmigung bei der national zuständigen Behörde.
2. **Dokumentation von Lizenzen und Endverwendungsnachweisen:**
   Für genehmigungspflichtige Exporte ist eine **vollständige Nachweisdokumentation** erforderlich. Dazu zählen:
   - Lizenznummer oder Genehmigungsbescheid,
   - Endverbleibserklärung („End-User Certificate“),
   - Zweckbestätigung durch den Empfänger,
   - Protokolle über Lieferungen und Datenzugriffe.
     Diese Unterlagen sollten mindestens **fünf Jahre** aufbewahrt und im internen Compliance-Managementsystem hinterlegt werden.
3. **Abstimmung mit nationalen Exportbehörden:**
   Die praktische Durchführung und Genehmigung erfolgt über die zuständigen nationalen Stellen, z. B.:
   - **BAFA (Bundesamt für Wirtschaft und Ausfuhrkontrolle)** in Deutschland,
   - **Service Public Fédéral Économie** in Belgien,
   - **Direzione Generale per la Politica Commerciale Internazionale** in Italien,
   - oder entsprechende Ministerien in Österreich, Frankreich und anderen Mitgliedstaaten.
     Diese Behörden beraten Unternehmen, prüfen Exportanträge und erteilen verbindliche Auskünfte über Genehmigungspflichten.

Verknüpfung mit KI-Compliance

Die Exportkontrolle ist Teil einer umfassenden **AI-Governance-Strategie**. Sie ergänzt das Risikomanagement nach Art. 9 EU AI Act und sollte integraler Bestandteil des internen Compliance-Frameworks sein.
Ein AI-Compliance-Officer sollte daher auch über die **Dual-Use-Bewertung** informiert sein und Exportentscheidungen in Zusammenarbeit mit Recht, IT-Sicherheit und Datenschutz koordinieren.

© A4Q Copyright 2025

16.3 IP-Rechte und Lizenzfragen

Künstliche Intelligenz (KI) kann Inhalte erzeugen, verändern oder aus bestehenden Daten ableiten. Damit berührt sie unmittelbar zentrale Fragen des **geistigen Eigentums (Intellectual Property – IP)**. Sowohl bei der Nutzung von Trainingsdaten als auch bei der Weiterverwendung generierter Inhalte entstehen komplexe rechtliche Anforderungen im Bereich des **Urheber-, Lizenz- und Haftungsrechts**.

Bedeutung für KI-Compliance

KI-Systeme operieren nicht im rechtsfreien Raum: Jedes Trainingsmaterial, jedes Modell und jeder Output kann rechtlich geschützt sein. Das betrifft nicht nur klassische Texte, Bilder oder Musik, sondern auch Code, Datenbanken und Modelle. Organisationen in der EU müssen sicherstellen, dass der Einsatz, das Training und die Veröffentlichung von KI-Systemen im Einklang mit geltenden **IP- und Lizenzvorschriften** stehen.

Besonders relevant sind hier drei Fragestellungen:

1. **Wem gehören die Trainingsdaten?**
2. **Welche Rechte gelten für den Output eines KI-Modells?**
3. **Wer haftet bei Urheberrechtsverletzungen oder unzulässiger Nutzung?**

Urheberrechte an Trainingsdaten

Trainingsdaten sind das Fundament jedes KI-Systems. Enthalten diese jedoch urheberrechtlich geschützte Werke – etwa Texte, Fotos, Tonaufnahmen oder Programmcode – bedarf deren Nutzung einer rechtlichen Grundlage.

Nach der **EU-Urheberrechtsrichtlinie (Richtlinie (EU) 2019/790)** ist das **Text and Data Mining (TDM)** zu Forschungszwecken grundsätzlich erlaubt, sofern keine ausdrücklichen Nutzungseinschränkungen bestehen.
Für kommerzielle Zwecke oder für das Training proprietärer KI-Modelle ist jedoch eine **Lizenzierung oder ausdrückliche Erlaubnis** des Rechteinhabers erforderlich.

Beispiele:

- Das Training eines Bildgenerators auf urheberrechtlich geschützten Kunstwerken ohne Genehmigung kann eine Urheberrechtsverletzung darstellen.
- Die Nutzung von journalistischen Texten oder Webinhalten ohne Lizenz oder Quellenangabe kann gegen EU- und nationale Urhebergesetze verstoßen.

Empfehlung: Organisationen sollten vor jedem Training prüfen, **ob die verwendeten Datensätze frei von urheberrechtlichen Einschränkungen** sind und ob etwaige Lizenzbedingungen eingehalten werden.

Open-Source-Lizenzen und Model-Sharing

© A4Q Copyright 2025

Viele KI-Modelle und Frameworks werden unter **Open-Source-Lizenzen** bereitgestellt (z. B. MIT, Apache 2.0, GPL, Creative Commons). Diese erleichtern den Zugang zu Technologie, erfordern aber sorgfältige Prüfung.

- **Pflichten bei Nutzung:** Je nach Lizenz müssen etwa Quelltexte offengelegt, Urheber genannt oder Änderungen kenntlich gemacht werden.
- **Einschränkungen:** Einige Lizenzen verbieten kommerzielle Nutzung („Non-Commercial"), andere schließen bestimmte Einsatzbereiche (z. B. militärische Nutzung) aus.
- **Gefahr unklarer Lizenzketten:** Besonders bei Modellen, die auf anderen Open-Source-Komponenten aufbauen, kann die Lizenzlage komplex sein.

Praxisbeispiel:
Ein Unternehmen integriert ein Open-Source-Spracherkennungsmodell in seine Software. Die verwendete Lizenz (GPLv3) verlangt, dass auch der eigene Quellcode offengelegt wird. Ohne Anpassung des Lizenzmanagements würde dies zu einer ungewollten Offenlegungspflicht führen – und damit zu einem Compliance-Verstoß.

Empfehlung: Vor jeder Integration von Open-Source-Software oder KI-Modellen sollte eine **Lizenzkompatibilitätsprüfung** erfolgen, idealerweise durch die Rechtsabteilung oder ein internes **Open-Source-Compliance-Team**.

Nutzungsrechte an KI-generierten Inhalten

Die Frage, **ob KI-generierte Inhalte urheberrechtlich geschützt sind**, ist innerhalb der EU noch nicht einheitlich geregelt. Nach aktuellem Rechtsverständnis entsteht Urheberrecht **nur bei menschlicher Schöpfung**, d. h. ein rein automatisiert erzeugter KI-Output ist **nicht urheberrechtlich geschützt**.

Für die Praxis bedeutet das:

- Unternehmen können KI-generierte Inhalte frei verwenden, sollten aber deutlich kennzeichnen, dass sie von einer KI erstellt wurden (Art. 52 EU AI Act).
- Wenn ein Mensch wesentlich zur inhaltlichen Gestaltung beiträgt (z. B. durch gezieltes Prompting, Bearbeitung oder kreative Auswahl), kann daraus ein **abgeleitetes Urheberrecht** entstehen.
- Konflikte entstehen, wenn der Output auf geschütztem Trainingsmaterial basiert (z. B. ein KI-generiertes Bild, das Stilmerkmale einer bekannten Künstlerin imitiert).

Empfehlung: Alle generierten Inhalte sollten in einer internen **Dokumentationsrichtlinie** erfasst werden, einschließlich:

- verwendeter Modelle und Prompts,
- Quellen und Lizenzen des Trainingsmaterials,
- Zweck der Nutzung (intern, kommerziell, öffentlich).

© A4Q Copyright 2025

Vertrags- und Haftungsaspekte

Der rechtssichere Einsatz von KI erfordert klare vertragliche Regelungen zwischen allen Beteiligten – insbesondere zwischen **Anbietern, Entwicklern, Lizenzgebern und Kunden**.

Zentrale Punkte:

- **Lizenzprüfung vor Training und Deployment:**
  Jedes KI-Projekt sollte eine formale Lizenzprüfung (Due Diligence) beinhalten. Dabei wird geprüft, ob Trainingsdaten, Software-Bibliotheken und Modellkomponenten rechtmäßig verwendet werden dürfen.
- **Dokumentation der Datenquellen und Urheberrechte:**
  Alle verwendeten Datensätze und Modelle sollten in einem **Lizenzregister** dokumentiert werden, das Versionen, Quellen, Lizenzbedingungen und Verantwortliche enthält.
- **Vertragsklauseln zu Haftung und Weitergabe:**
  Verträge mit KI-Anbietern sollten Regelungen zu **IP-Rechten, Haftungsumfang, Freistellung** und **Nutzungsbeschränkungen** enthalten.
  Bei generativen Systemen ist zu klären, wer für mögliche Urheberrechtsverletzungen im Output haftet und ob Dritte Schadensersatzansprüche geltend machen können.

Beispiel:
Ein Verlag nutzt ein generatives Textmodell, um Zusammenfassungen wissenschaftlicher Artikel zu erstellen. Ein Autor erkennt Ähnlichkeiten mit seinem Werk und erhebt Urheberrechtsansprüche. Da im Vertrag keine Haftungsregelung zum KI-Output enthalten war, haftet der Verlag vollumfänglich für den Schaden.

Fazit

IP- und Lizenzfragen sind ein zentraler Bestandteil der KI-Compliance – insbesondere, wenn KI-Systeme mit fremden Daten trainiert oder deren Ergebnisse kommerziell genutzt werden.
Organisationen in der EU sollten sicherstellen, dass:

- Trainingsdaten und Modelle rechtmäßig erworben oder lizenziert sind,
- alle Lizenz- und Urheberrechte dokumentiert werden,
- Verträge klare Regelungen zu Haftung, Eigentum und Weitergabe enthalten.

So gilt nach Meinung der EU, ein systematisches **IP-Compliance-Management** schützt nicht nur vor rechtlichen Risiken, sondern auch vor Reputations- und Marktverlusten.
Langfristig stärkt es die Transparenz, Nachvollziehbarkeit und Vertrauenswürdigkeit im Umgang mit KI – zentrale Ziele des EU AI Act und der europäischen Digitalstrategie.

© A4Q Copyright 2025

16.4 Compliance in internationalen Lieferketten

Der Einsatz von Künstlicher Intelligenz (KI) erfolgt heute in global vernetzten Strukturen: Trainingsdaten stammen aus verschiedenen Regionen, Modelle werden in internationalen Cloud-Umgebungen betrieben, und Komponenten – etwa Softwaremodule oder Sensorik – stammen häufig von Drittherstellern außerhalb der EU.
Damit wird **KI-Compliance zu einer Aufgabe über die gesamte Liefer- und Wertschöpfungskette hinweg**. Unternehmen tragen Verantwortung nicht nur für ihre eigenen Systeme, sondern auch für die rechtliche und ethische Konformität der von Partnern und Zulieferern eingebrachten KI-Komponenten.

Bedeutung für die EU-weite Compliance

Der EU AI Act wirkt **extraterritorial**: Er gilt auch für Anbieter und Betreiber außerhalb der Europäischen Union, sofern ihre KI-Systeme in der EU in Verkehr gebracht oder verwendet werden.
Damit werden europäische Unternehmen verpflichtet, sicherzustellen, dass ihre internationalen Lieferanten und Partner die **grundlegenden Prinzipien des EU AI Act** einhalten – unabhängig vom Sitz des Unternehmens.

Typische Herausforderungen ergeben sich aus:

- **unterschiedlichen Rechtslagen** in Drittstaaten,
- **fehlender Harmonisierung** bei Datenschutz, Produkthaftung und Sicherheitsstandards,
- **Sanktionslisten und Embargos**, die bestimmte Technologie- oder Datenexporte untersagen,
- sowie **mangelnder Transparenz** über die Herkunft, Trainingsdaten oder Modellversionen eingesetzter KI-Komponenten.

Risiken in globalen KI-Lieferketten

1. **Regulatorische Risiken:**
   Zulieferer in Nicht-EU-Staaten können KI-Komponenten entwickeln, die nicht den Anforderungen des EU AI Act oder der DSGVO entsprechen. Werden solche Systeme weiterverarbeitet oder in der EU vertrieben, haftet der europäische Anbieter mit.
2. **Sanktions- und Exportverstöße:**
   Der Transfer von KI-Modellen oder Trainingsdaten in Risikostaaten (z. B. mit Embargobestimmungen) kann gegen EU-Verordnungen zur Außenwirtschafts- und Dual-Use-Kontrolle verstoßen.

© A4Q Copyright 2025

3. **Cyber- und Datensicherheitsrisiken:**
   Unzureichend geprüfte Drittanbieter können über Cloud- oder API-Schnittstellen Zugriff auf sensible Daten erhalten – ein erhebliches Risiko für Datenschutz und IT-Sicherheit.
4. **Reputationsrisiken:**
   Menschenrechtsverletzungen, unethische Datennutzung oder algorithmische Diskriminierung bei Zulieferern können auch das Image des europäischen Hauptunternehmens massiv beeinträchtigen.

Beispiel:
Ein europäischer Automobilhersteller nutzt ein KI-Modul zur Gesichtserkennung für Fahrerassistenzsysteme, das von einem außereuropäischen Zulieferer stammt. Eine spätere Prüfung zeigt, dass der Algorithmus auf diskriminierenden Trainingsdaten basiert. Trotz fehlender direkter Verantwortlichkeit wird der Hersteller wegen unzureichender Lieferantenkontrolle in die Verantwortung genommen.

Empfohlene Maßnahmen für rechtskonforme Lieferketten

1. **Lieferanten-Audits auf KI-Compliance und Datenschutz:**
   - Führen Sie regelmäßige Audits und Assessments bei Lieferanten durch, insbesondere wenn diese KI-Modelle, Trainingsdaten oder automatisierte Entscheidungslogiken bereitstellen.
   - Prüfen Sie, ob die KI-Systeme dokumentiert, nachvollziehbar und mit den Grundsätzen des EU AI Act vereinbar sind (z. B. Risikomanagement, Transparenz, Human Oversight).
   - Verlangen Sie Nachweise über Datenschutzkonformität nach DSGVO, inklusive Datenquellen, Löschkonzepte und Sicherheitsmaßnahmen.
   - Ergänzend sollten Lieferanten ihre KI-Systeme in Bezug auf Bias, Fairness und ethische Standards prüfen und Bericht erstatten.
2. **Verpflichtung auf EU-AI-Act-Prinzipien in Vertragswerken:**
   - Binden Sie alle Lieferanten vertraglich an die zentralen Pflichten des EU AI Act, z. B.:
     - Einhaltung der Artikel 9–15 (Risikomanagement, Datenqualität, Transparenz, Human Oversight, Robustheit),
     - Verpflichtung zur Bereitstellung von technischer Dokumentation und Auditdaten,
     - sofortige Informationspflicht bei Änderungen an KI-Modellen oder Trainingsdaten.
   - Ergänzen Sie Lieferantenverträge um **Ethik- und Transparenzklauseln**, etwa:
     - keine Nutzung unrechtmäßig erhobener Daten,
     - Verpflichtung zur Kennzeichnung von KI-generierten Inhalten,

© A4Q Copyright 2025

        - Dokumentationspflicht über verwendete Trainingsquellen.
    - Bei Hochrisiko-Systemen empfiehlt sich die Aufnahme einer **gemeinsamen Haftungsregelung** und eines **Auditzugangsrechts**.

3. **Einrichtung eines globalen Compliance-Registers mit Nachweisführung:**
    - Legen Sie ein zentrales Register an, in dem alle KI-Systeme, Module und Lieferantenbeziehungen erfasst werden.
    - Das Register sollte enthalten:
        - Name und Sitz des Lieferanten,
        - Art des gelieferten KI-Systems oder Moduls,
        - Risikostufe gemäß EU AI Act,
        - Ergebnis der letzten Compliance-Prüfung,
        - Verantwortliche Personen und Freigabedatum.
    - Eine regelmäßige Aktualisierung und Nachweispflicht sichert Transparenz und erleichtert interne wie externe Audits.

Praxis-Tipp:
Das Register kann digital geführt und mit bestehenden **Supplier-Management-Systemen** oder **GRC-Plattformen (Governance, Risk & Compliance)** verknüpft werden. Eine Integration in das interne Audit- und Dokumentationssystem (z. B. ISO 9001 oder ISO 42001) erhöht Effizienz und Nachvollziehbarkeit.

Verknüpfung mit weiteren EU-Regularien

Die Compliance in globalen Lieferketten steht im engen Zusammenhang mit weiteren EU-Initiativen:

- **Corporate Sustainability Due Diligence Directive (CSDDD):** Verpflichtet Unternehmen zur menschenrechtlichen und ökologischen Sorgfaltspflicht in Lieferketten.
- **Digital Services Act (DSA)** und **Data Act:** Reglementieren die Weitergabe und Nutzung von Daten über Ländergrenzen hinweg.
- **DSGVO** und **EU AI Act:** Definieren technische und organisatorische Pflichten beim internationalen Datenaustausch und KI-Betrieb.

Durch die Verknüpfung dieser Regelwerke entsteht ein kohärenter europäischer Rechtsrahmen, der technologische Innovation mit verantwortungsvollem Handeln verbindet.

Fazit

© A4Q Copyright 2025

Globale Lieferketten sind das Rückgrat moderner KI-Systeme – zugleich aber ein kritischer Compliance-Bereich.
Wer Lieferanten, Datenflüsse und Modellabhängigkeiten transparent dokumentiert, schafft die Grundlage für rechtskonformen und ethisch vertretbaren KI-Einsatz.

Organisationen, die:

- regelmäßige **Lieferanten-Audits**,
- **vertragliche Verpflichtungen auf EU-Standards**,
- und ein **zentrales Compliance-Register** einführen,

können ihre regulatorischen Risiken signifikant senken und gegenüber Aufsichtsbehörden die **„Presumption of Conformity“** (Vermutung der Konformität nach Art. 40 EU AI Act) glaubhaft nachweisen.

So entsteht eine durchgängige KI-Compliance-Kette – von der Entwicklung über den internationalen Datentransfer bis zur verantwortungsvollen Nutzung im europäischen Binnenmarkt.

© A4Q Copyright 2025

17 Optional - Praktische Übungen & Fallstudien

🎯 **Business Outcomes:**

- **BO 17.1** Teilnehmende erwerben praktische Kompetenz um, z.B. Risikoklassifizierung, FRIA und GPAI-Pflichten praktisch anzuwenden.
- **BO 17.2** Teilnehmende sind befähigt, Compliance-Artefakte (Dokumentation, Label, Monitoring-Plan) zu entwickeln.

Einleitung

Dieses optionale Übungskapitel dient der flexiblen Vertiefung einzelner Themenbereiche des Lehrplans und ermöglicht es Trainingsanbietern, Inhalte gezielt an die Bedürfnisse und das Vorwissen der Teilnehmenden anzupassen.

Die Auswahl, Anzahl und Tiefe der Übungen liegt im pädagogischen Ermessen des Trainingsanbieters und sollte sich an der Schwerpunktsetzung des jeweiligen Kurses orientieren (z. B. stärkerer Fokus auf technische, juristische oder organisatorische Aspekte der KI-Compliance).

Ziel ist es, durch praxisnahe und interaktive Methoden das Verständnis für Verantwortlichkeiten, Prozesse und Nachweispflichten zu stärken und den Transfer in reale Unternehmenskontexte zu fördern.

Beispiele möglicher optionaler Übungsformate:

• Vertiefende Fallstudien zu ausgewählten Artikeln des EU AI Act (z. B. Art. 9–15, Art. 27, Art. 52)
• Simulation eines internen oder externen Audits („AI Compliance Assessment“)
• Erstellung eines exemplarischen Compliance-Dossiers oder Monitoring-Plans
• Rollenspiel: Kommunikation zwischen Aufsicht, Management und Entwicklungsteam
• Vergleichsaufgabe: Umsetzung nationaler AI-Gesetze außerhalb der EU (z. B. UK, Kanada, China)
• Analyse von Praxisbeispielen aus verschiedenen Branchen (Gesundheit, Finanzen, Verwaltung)

Diese Übungen sind nicht prüfungsrelevant, können jedoch zur Anwendungssicherheit und Audit-Readiness wesentlich beitragen und eignen sich insbesondere für erweiterte Trainingsprogramme oder Inhouse-Schulungen

17.1 Einführung in KI-Compliance & den EU AI Act

Diese Einstiegsübungen dienen dazu, zentrale Begriffe und Grundprinzipien des EU AI Act praktisch zu verankern. Die Teilnehmenden lernen, Definitionen, Rollen und Übergangsfristen zu verstehen und anzuwenden.

Übungen:

• Zuordnungsübung: Begriffe „KI-System“, „GPAI“, „Provider“, „Deployer“ richtig einordnen

© A4Q Copyright 2025

• Diskussion: Auswirkungen des EU AI Act auf die eigene Organisation
• Zeitleistenaufgabe: Übergangsfristen 2024 – 2027 korrekt anordnen
• Reflexion: Nutzen und Risiken von KI aus Compliance-Sicht

17.2 Risikobasierter Ansatz und Klassifikation

Diese Übungseinheit vertieft das Verständnis der vier Risikostufen und schult die Fähigkeit, reale KI-Anwendungen einzuordnen.

Übungen:

• Fallbeispiele klassifizieren: Hoch-, begrenzt- oder minimalriskant
• Mapping-Übung: KI-Use-Cases den Kategorien in Anhang III zuordnen
• Entscheidungsbaum entwickeln: Risikostufe bestimmen anhand typischer Parameter
• Gruppenreflexion: Übergänge zwischen Risikostufen bewerten

17.3 Globale & sektorale Regulierungslandschaft

Ziel dieser Einheit ist es, die internationale Perspektive der KI-Regulierung zu erfassen und Gemeinsamkeiten sowie Unterschiede herauszuarbeiten.

Übungen:

• Zuordnungsübung: Regulierungsansätze EU, USA, China, UK, OECD vergleichen
• Mapping: EU AI Act vs. ISO/IEC 42001 – Überschneidungen
• Diskussionsübung: Auswirkungen unterschiedlicher Rechtslagen auf multinationale Unternehmen
• Gruppenaufgabe: Risiken bei internationalen KI-Projekten identifizieren

17.4 Verbotene KI-Praktiken (Art. 5)

Hier steht die ethische und rechtliche Bewertung verbotener KI-Praktiken im Mittelpunkt. Die Teilnehmenden lernen, problematische Anwendungen zu erkennen und Ausnahmen korrekt zu interpretieren.

Übungen:

• Fallanalyse: unzulässige Praktiken erkennen
• Zuordnung: Ausnahmen (z. B. Strafverfolgung) zu rechtlichen Voraussetzungen
• Gruppenübung: Risikofaktoren für unbeabsichtigte Verstöße definieren
• Diskussion: Ethische Grenzen vs. technologische Möglichkeiten

17.5 Hochrisiko-Systeme und Pflichten (Art. 6 – 51)

Diese Einheit trainiert die Fähigkeit, Pflichten und Zuständigkeiten bei Hochrisiko-Systemen praxisnah anzuwenden.

© A4Q Copyright 2025

Übungen:

• Pflichtzuordnung: Artikelnummern den Anforderungen zuordnen

• Checklistenübung: Welche Nachweise sind für Hochrisiko-Systeme erforderlich?

• Rollenanalyse: Anbieter vs. Betreiber – wer muss was tun?

• Kurzfall: Hochrisiko-System identifizieren und Pflichten ableiten

17.6 Risikomanagement- & Qualitätsmanagementsystem

In dieser Übung werden die Konzepte aus ISO/IEC 23894 und 42001 praktisch umgesetzt. Ziel ist die Verbindung zwischen Risikoanalyse und Managementsystemen.

Übungen:

• Prozessübung: Risikoanalyse nach ISO/IEC 23894 aufbauen

• Governance-Mapping: Integration in bestehende Managementsysteme

• Gruppenaufgabe: Risiko-Matrix für ein KI-Projekt erstellen

• Vergleich: Unterschied FRIA vs. Risikomanagement

17.7 Konformitätsbewertung und CE-Kennzeichnung

Diese Einheit zeigt, wie Konformitätsprozesse praktisch ablaufen und welche Dokumente dabei erforderlich sind.

Übungen:

• Praxis-Checkliste: Schritte der internen Konformitätsbewertung

• Matching-Aufgabe: Technische Dokumentation ↔ Artikelanforderung

• Gruppenarbeit: Mini-CE-Erklärung für ein Beispielsystem erstellen

• Diskussionsrunde: Vor- und Nachteile interner vs. externer Bewertung

17.8 Transparenzpflichten für Limited-Risk-Systeme (Art. 52)

Teilnehmende entwerfen Transparenzhinweise und prüfen deren Wirksamkeit. Ziel ist ein besseres Verständnis für Labeling-Pflichten.

Übungen:

• Praxisübung: Transparenz-Label entwerfen (Text, Metadaten, UI-Hinweis)

• Überprüfung: A/B-Test für Kennzeichnung von Chatbots planen

• Mini-Case: Transparenzverstöße identifizieren

• Diskussion: Wie beeinflusst Offenheit das Vertrauen?

© A4Q Copyright 2025

17.9 General Purpose AI (GPAI) & Systemic Risk

Diese Einheit behandelt Art. 53 – 55 EU AI Act und trainiert, wie GPAI-Pflichten im Unternehmen umgesetzt werden können.

Übungen:

- Übung: GPAI-Verpflichtungen (Art. 53 – 55) auf Anbieter und Nutzer aufteilen
- Analyse: Transparenzbericht eines GPAI-Anbieters bewerten
- Gruppenarbeit: Checkliste für GPAI-Integration im Unternehmen erstellen
- Brainstorming: Red-Team-Testing als freiwillige Best Practice planen

17.10 Fundamental Rights Impact Assessment (FRIA, Art. 27)

Diese Übungen machen die FRIA-Methodik praktisch erfahrbar. Sie fördern das Verständnis für den Zusammenhang zwischen Grundrechten und KI-Einsatz.

Übungen:

- Mini-FRIA: Betroffene Grundrechte und Risiken identifizieren
- Bewertungsübung: Schweregradmatrix für Grundrechtsverletzungen
- Fallauswahl: Unterschied FRIA vs. DSFA
- Diskussionsaufgabe: Wie wird FRIA in Governance-Prozesse integriert?

17.11 Post-Market-Monitoring, Reporting & Marktaufsicht

Diese Einheit behandelt das Monitoring nach Inverkehrbringen und die Meldepflichten gemäß Art. 23 ff. EU AI Act.

Übungen:

- Übung: Monitoring-Plan mit Indikatoren entwerfen
- Checkliste: Incident-Reporting nach Art. 23 aufbauen
- Gruppenarbeit: Ablauf eines Serious-Incident-Falls simulieren
- Reflexion: Dokumentation – Was muss dauerhaft aufbewahrt werden?

17.12 Governance, Organisation & Rollen

Hier geht es um Zusammenarbeit und Verantwortlichkeiten im AI-Compliance-Umfeld.

Übungen:

- Rollenspiel: Zusammenarbeit zwischen KI-Officer, Datenschutz und IT
- Aufgabenmatrix (RACI) erstellen
- Gruppenarbeit: Aufbau eines KI-Compliance-Committees skizzieren
- Übung: Schulungsplan nach Art. 4(4) entwickeln

© A4Q Copyright 2025

17.13 Minimales Risiko & freiwillige Governance („Ethical AI“)

Diese Einheit zeigt, wie Ethik-Standards auch ohne gesetzliche Pflicht angewendet werden können.

Übungen:

- Leitlinienvergleich: ISO 42001 / OECD / UNESCO
- Workshop: Ethical Impact Assessment (EIA) in Kurzform anwenden
- Gruppenaufgabe: CSR- oder ESG-Bezug für KI-Projekte herstellen
- Reflexion: Ethische Mindeststandards auch ohne Rechtsverpflichtung

17.14 Audit-Readiness, Prüfpfade & Sanktionen

Diese Übungen trainieren die Vorbereitung auf Audits und den Umgang mit typischen Findings.

Übungen:

- Simulation: internes Audit-Interview (Auditor ↔ KI-Officer)
- Checklistenprüfung: Dokumentationsstand vs. Anforderungen
- Matching: Typische Findings den Corrective Actions zuordnen
- Übung: Audit-Policy-Entwurf erstellen

17.15 Harmonisierte Standards & Presumption of Conformity

In dieser Einheit wird das Zusammenspiel von Normen und Rechtsrahmen behandelt.

Übungen:

- Mapping-Übung: ISO/IEC 42001 ↔ AI Act Artikel
- Gruppenarbeit: Aufbau einer Normenbibliothek skizzieren
- Übung: Gap-Analyse für aktuelle Normrevisionen
- Vergleich: DIN vs. CEN/CENELEC – Unterschiede in der Anwendung

17.16 Globale Schnittstellen & Exportkontrolle

Hier werden internationale Lieferketten und Exportpflichten im Zusammenhang mit KI-Systemen analysiert.

Übungen:

- Checkliste: Exportkontrolle und KI-Compliance kombinieren
- Übung: Risikoanalyse für Drittstaatenlieferkette
- Gruppenarbeit: Lieferanten-Audit-Plan mit AI-Act-Kriterien
- Diskussion: Harmonisierung trotz unterschiedlicher Rechtsräume

17.17 Optionales Übungskapitel – Vertiefende oder ergänzende Praxisaufgaben

Dieser optionale Abschnitt bietet zusätzliche, vertiefende Übungen, die je nach Umfang des Kurses und Vorkenntnissen der Teilnehmenden ausgewählt werden können.

© A4Q Copyright 2025

Trainer:innen können diese Aktivitäten nutzen, um gezielte Kompetenzen zu festigen oder das Verständnis für übergreifende Compliance-Themen zu vertiefen.

17.18 Optionales Kapitel: Roadmap & Readiness Assessment 2025–2027

Diese Einheit unterstützt Organisationen bei der strategischen Planung ihrer AI-Act-Readiness.

Übungen:

- Übung: Gap-Analyse der eigenen Organisation
- Priorisierung: Quick-Wins & langfristige Maßnahmen identifizieren
- Checkliste: Compliance-Reifegrad bewerten
- Gruppenaufgabe: Roadmap für 2025–2027 entwerfen

17.19 Optionales Kapitel: Zukunft & Weiterentwicklung des Regulierungsrahmens

Diese abschließende Einheit blickt in die Zukunft der KI-Governance und neuer Rollen.

Übungen:

- Trendanalyse: neue Rollen (AI Auditor, AI Board) skizzieren
- Diskussionsaufgabe: Frontier-AI-Risiken bewerten
- Reflexion: Internationale Konvergenz (EU – USA – Asien)
- Gruppenarbeit: Zukunfts-Audit entwerfen („Wie sieht Compliance 2030 aus?“)

© A4Q Copyright 2025

18 Roadmap & Readiness Assessment 2025–2027

Hinweis: Dieses Kapitel ist **nicht prüfungsrelevant** und dient als optionale Vertiefung für Trainingsanbieter.

🎯 Business Outcomes

- **BO 18.1** Teilnehmende sind vorbereitet, eine AI-Compliance-Roadmap mit Umsetzungsprioritäten zu erstellen.
- **BO 18.2** Teilnehmende sind befähigt, den Reifegrad des Unternehmens hinsichtlich AI-Act-Readiness einzuschätzen.

Nicht prüfungsrelevante Learning Objectives (LOs)

- **LO 18.1 (K2):** Teilnehmende können erläutern, wie Organisationen ihren Umsetzungsstand des EU AI Act über ein Reifegradmodell (Maturity Model) bewerten können.
- **LO 18.2 (K2):** Teilnehmende verstehen den Zweck einer AI-Compliance-Roadmap und können zentrale Schritte einer schrittweisen Implementierung (Gap-Analyse, Priorisierung, Maßnahmenplanung) beschreiben.
- **LO 18.3 (K3):** Teilnehmende sind in der Lage, eine einfache Selbstbewertung (Self-Assessment) auf Basis eines ISO/IEC 42001-basierten Reifegradmodells durchzuführen und zu interpretieren.
- **LO 18.4 (K2):** Teilnehmende können wesentliche Werkzeuge (Checklists, FRIA-Vorlage, Konformitäts-Dossier, Governance-Policy) benennen und deren Zweck im Compliance-Prozess erklären.
- **LO 18.5 (K3):** Teilnehmende können auf Basis eines Praxisbeispiels eine Roadmap zur AI-Act-Readiness entwerfen, die Verantwortlichkeiten, Schulungsmaßnahmen und Dokumentationsprozesse umfasst.
- **LO 18.6 (K1):** Teilnehmende kennen den Zusammenhang zwischen kontinuierlicher Verbesserung (Continuous Improvement), Audit-Trail und Reporting im Kontext von AI-Compliance.

Wichtige Begriffe:
AI-Readiness, Reifegradmodell, Maturity Level, Self-Assessment, Gap-Analyse, Compliance-Roadmap, AI-Compliance-Checklist, FRIA-Vorlage, Konformitäts-Dossier, Governance-Policy, Schulungsmatrix, Verantwortlichkeitszuordnung, Rollenmodell, ISO/IEC 42001 Alignment, Dokumentationsstandard, Reporting-Struktur, Fortschrittsmessung, kontinuierliche Verbesserung (Continuous Improvement), Audit-Trail, AI-Register.

© A4Q Copyright 2025

Einleitung / Ziel und Zweck des Kapitels

Dieses optionale Kapitel bietet Organisationen eine praxisorientierte Orientierung, wie sie den EU AI Act systematisch und effizient umsetzen können. Es verbindet regulatorische Anforderungen mit Management-Methoden und zeigt, wie Quick Wins, Prioritäten und langfristige Governance-Strukturen entlang einer AI-Compliance-Roadmap entwickelt werden können.

18.1 Bausteine einer AI-Compliance-Roadmap

Eine belastbare AI-Compliance-Roadmap sollte strategische, organisatorische und technische Handlungsfelder abdecken. Sie beschreibt **was** zu tun ist, **wann** und **durch wen**.

Phase	**Zeitraum (Orientierung)**	**Schwerpunkt**	**Beispielhafte Aktivitäten**
1 – Initialisierung	2025 Q1 – Q2	Bewusstsein & Inventarisierung	Schulung der Führungsebene · Erfassung aller KI-Systeme · Erste Gap-Analyse
2 – Risikobewertung & Klassifikation	2025 Q2 – Q3	Einstufung nach Art. 6 – 9 AI Act	Zuordnung aller Systeme zu Risikostufen · FRIA-Prüfung für öffentliche Stellen
3 – Regulatorische Integration	2025 Q3 – Q4	Aufbau von Prozessen und Policies	Erstellung von AI-Policy, Rollenbeschreibungen, Governance-Board
4 – Operationalisierung	2026 – 2027	Umsetzung und Überwachung	Konformitätsbewertung, Monitoring-Plan, Audits, Reporting
5 – Optimierung & Reifegradsteigerung	ab 2027	Kontinuierliche Verbesserung	Kombination mit ISO/IEC 42001, Lessons Learned, Benchmarking

Hinweis: Welche Phasen, Übungen oder Templates im Training vertieft werden, entscheidet der Schulungsanbieter entsprechend Zielgruppe und Trainingsfokus.

18.2 Typische Quick Wins und Prioritäten

© A4Q Copyright 2025

Die schrittweise Umsetzung der Anforderungen des EU AI Act erfordert klare Prioritäten. Die folgenden Maßnahmen haben sich in der Praxis als besonders wirkungsvoll erwiesen und können in nahezu jeder Organisation als Startpunkt einer AI-Compliance-Roadmap dienen.

1. AI-System-Inventar

Ein zentrales Inventar aller eingesetzten oder geplanten KI-Systeme bildet die Grundlage jeder Compliance-Strategie.
Das Inventar sollte für jedes System mindestens folgende Angaben enthalten:

- Zweck und Anwendungsbereich der KI,
- verantwortliche Person oder Organisationseinheit,
- zugeordnete Risikoklasse gemäß Art. 6–9 EU AI Act,
- aktueller Einsatzstatus (Pilot, Produktiv, Außer Betrieb),
- Nachweise zu Konformität und Monitoring.

Ein solches Register ermöglicht Transparenz über alle KI-Aktivitäten und dient zugleich als Ausgangspunkt für Risikobewertung, Auditierung und Behördenkommunikation.

2. Schulung der Mitarbeitenden

Die Sensibilisierung von Fach- und Führungskräften ist ein wesentlicher Erfolgsfaktor für AI-Compliance. Schulungen sollten vermitteln,

- welche Pflichten aus dem EU AI Act resultieren,
- welche Rollen und Verantwortlichkeiten bestehen (z. B. KI-Officer, Fachaufsicht),
- und wie Risiken, Vorfälle und Dokumentationspflichten im Alltag erkannt und umgesetzt werden können.

Empfehlenswert ist ein gestuftes Schulungskonzept mit Basistrainings für alle Mitarbeitenden und Vertiefungsmodulen für Schlüsselrollen.
So entsteht ein gemeinsames Verständnis für rechtssicheren und verantwortungsvollen KI-Einsatz.

3. Governance-Dokumente

Zur organisatorischen Verankerung von KI-Compliance sollten verbindliche Governance-Dokumente erstellt werden.
Dazu gehören insbesondere:

- eine **AI-Policy** als übergreifende Richtlinie für Entwicklung, Einsatz und Überwachung von KI-Systemen,

© A4Q Copyright 2025

- **Rollen- und Verantwortlichkeitsbeschreibungen** (z. B. KI-Officer, Compliance-Beauftragte, Systemverantwortliche),
- **Eskalations- und Reporting-Prozesse** zur Meldung von Incidents, Risiken oder Änderungen.

Diese Dokumente schaffen Nachvollziehbarkeit, stärken interne Kontrollmechanismen und fördern die Integration von KI-Compliance in bestehende Managementsysteme.

4. Pilot-Audits

Pilot-Audits dienen der praktischen Überprüfung der Dokumentations- und Umsetzungspflichten.
In einem kontrollierten Rahmen können Organisationen prüfen,

- ob die erforderlichen Nachweise nach Art. 9–24 AI Act vollständig sind,
- ob Transparenz- und Logging-Prozesse funktionieren,
- und wie die Kommunikation zwischen Fachbereichen, Compliance und Technik abläuft.

Ergebnisse aus Pilot-Audits liefern wertvolle Erkenntnisse zur Weiterentwicklung von Prozessen, Schulungen und Dokumentationsqualität.

5. Gap Analysis

Eine Gap Analysis vergleicht die aktuelle Praxis des Unternehmens mit den Anforderungen des EU AI Act (insbesondere Art. 5–24).
Dabei werden Soll-Vorgaben und Ist-Zustände systematisch gegenübergestellt, um Handlungsfelder zu identifizieren.
Typische Prüffelder sind:

- Vorhandensein eines Risikomanagementsystems,
- Vollständigkeit technischer Dokumentationen,
- Erfüllung von Transparenz- und Human-Oversight-Pflichten,
- Schulungs- und Governance-Strukturen.

Das Ergebnis bildet die Basis für eine priorisierte Umsetzungsplanung innerhalb der AI-Compliance-Roadmap.

18.3 Selbstbewertung des AI-Compliance-Reifegrads

Organisationen befinden sich in unterschiedlichen Entwicklungsstadien auf ihrem Weg zur vollständigen Umsetzung der Anforderungen des EU AI Act.

© A4Q Copyright 2025

Ein strukturiertes Reifegradmodell ermöglicht eine realistische Selbsteinschätzung des aktuellen Status und unterstützt die Priorisierung weiterer Maßnahmen.

Das nachfolgende Modell beschreibt fünf Stufen der organisatorischen Reife im Umgang mit KI-Compliance. Es kann als Orientierungsrahmen für interne Assessments, Audits oder Strategiegespräche genutzt werden.

Stufe	Bezeichnung	Beschreibung	Typische Indikatoren
1 – Ad-hoc	Erste, unkoordinierte KI-Aktivitäten	KI-Systeme werden ohne strukturierte Bewertung eingesetzt. Es existiert keine zentrale Dokumentation oder Verantwortlichkeitszuordnung.	Keine AI-Policy, keine definierten Rollen, keine Schulungsnachweise.
2 – Bewusst werdend	Aufbau regulatorischen Grundverständnisses	Das Unternehmen erkennt die Bedeutung des EU AI Act und beginnt, KI-Anwendungsfälle zu erfassen und Verantwortlichkeiten zu identifizieren.	Erste Inventarisierung der Systeme, Grundlagenschulung des Managements, erste Compliance-Checklisten.
3 – Strukturiert	Einführung grundlegender Compliance-Prozesse	Risikobewertung und Dokumentation erfolgen nach einheitlichen Verfahren. Erste Templates und interne Richtlinien sind implementiert.	AI-Systemregister vorhanden, FRIA-Vorlage etabliert, Verantwortlichkeiten schriftlich definiert.
4 – Integriert	Verankerung im Managementsystem	KI-Compliance ist fester Bestandteil der Unternehmenssteuerung und in bestehende Managementsysteme integriert. Audits und Monitoring-Prozesse sind etabliert.	Integration in ISO/IEC 42001 oder ISO 9001, regelmäßige interne Audits, aktiver Monitoring-Plan.
5 – Optimiert	Strategische und kontinuierlich verbesserte Compliance	KI-Compliance ist strategisch verankert, mit Kennzahlen gesteuert und extern überprüft. Die Organisation nutzt Benchmarks zur Weiterentwicklung.	Kennzahlenbasiertes Reporting, Benchmarking mit Best Practices, externes Zertifikat oder Gütesiegel.

Praxisübung (Vorschlag)

Führen Sie eine **Readiness-Selbsteinschätzung** für Ihre Organisation durch.
Bewerten Sie auf Basis der fünf Stufen, auf welchem Reifegrad Sie sich aktuell befinden, und definieren

© A4Q Copyright 2025

Sie, welche Maßnahmen erforderlich sind, um die nächste Stufe zu erreichen.
Typische Diskussionsfragen:

- Welche Elemente einer AI-Compliance-Struktur sind bereits vorhanden?
- Wo bestehen noch Lücken im Vergleich zu den Anforderungen des EU AI Act (Art. 5–55)?
- Welche Prozesse sollten kurzfristig implementiert oder verbessert werden?

Die Ergebnisse können als Grundlage für eine organisationsspezifische **AI-Compliance-Roadmap** dienen.

18.4 Werkzeuge und Hilfsmittel für die Roadmap-Erstellung

Für die praktische Umsetzung einer AI-Compliance-Roadmap stehen Organisationen verschiedene standardisierte Werkzeuge und Vorlagen zur Verfügung.
Diese Instrumente unterstützen bei der strukturierten Planung, Dokumentation und Bewertung der AI-Act-Readiness und können an die Größe, Branche und Komplexität des Unternehmens angepasst werden.

AI-Compliance-Checklist (Art. 5–55 EU AI Act)
Eine umfassende Prüfliste, die alle zentralen Anforderungen des EU AI Act abdeckt – von verbotenen Praktiken (Art. 5) über Hochrisiko-Pflichten (Art. 9–24) bis hin zu Transparenz- und GPAI-Vorgaben (Art. 52–55).
Die Checkliste ermöglicht eine systematische Selbstbewertung und dient als Grundlage für interne Audits oder Gap-Analysen.

FRIA-Vorlage nach Art. 27 EU AI Act
Die „Fundamental Rights Impact Assessment"-Vorlage (FRIA) unterstützt insbesondere öffentliche Stellen und Betreiber Hochrisiko-KI-Systeme bei der Bewertung potenzieller Grundrechtsrisiken.
Sie enthält strukturierte Leitfragen zu betroffenen Rechten, möglichen Auswirkungen, geplanten Schutzmaßnahmen und Nachweisen der Beteiligung relevanter Stakeholder.
Die FRIA kann als Ergänzung zur Datenschutz-Folgenabschätzung (DSFA) verwendet werden.

Konformitäts-Dossier-Template (Art. 11–23 EU AI Act)
Dieses Template bildet die Basis für die technische Dokumentation und Nachweiserstellung im Rahmen der Konformitätsbewertung.
Es enthält standardisierte Abschnitte zu:

- Systembeschreibung und Zweckbestimmung,
- Trainings- und Testdaten,
- Risikomanagement und Qualitätsmaßnahmen,
- Human Oversight und Monitoring-Prozessen,

© A4Q Copyright 2025

- Audit-Trails, Logging und Fallback-Mechanismen.
  Das Dossier dient als Nachweis gegenüber Aufsichtsbehörden und internen Prüfinstanzen.

Governance-Policy-Vorlage (Art. 4(4), 29 EU AI Act)

Diese Vorlage definiert zentrale organisatorische Regelungen für den Umgang mit KI im Unternehmen. Sie beschreibt u. a.:

- Rollen und Verantwortlichkeiten (z. B. KI-Officer, Konformitätsbeauftragte:r, Fachaufsicht),
- Eskalations- und Kommunikationswege,
- Grundsätze für Schulung, Dokumentation und Incident-Management.
  Die AI-Governance-Policy schafft Verbindlichkeit und Klarheit über interne Prozesse und Zuständigkeiten.

Schulungs-Matrix nach Rollen und Pflichten

Eine strukturierte Übersicht, die festlegt, welche Personengruppen welche Schulungsinhalte benötigen. Beispiele:

- Entwickler:innen: Modellvalidierung, Dokumentationspflichten, Bias-Kontrolle
- Produktmanager:innen: Anwendungsgrenzen, CE-Konformität, Governance-Prozesse
- Führungskräfte: Haftung, strategische Verantwortung, Audit-Vorbereitung
  Die Schulungs-Matrix unterstützt den Nachweis gemäß Art. 4(4) AI Act, dass alle relevanten Mitarbeitenden angemessen qualifiziert sind.

Reifegrad-Selbstbewertungsbogen (ISO/IEC 42001-basiert)

Ein praxisorientiertes Instrument zur Einschätzung des eigenen Organisationsstandes in Bezug auf AI-Governance und Compliance.
Der Fragebogen orientiert sich an den Prinzipien der ISO/IEC 42001 („AI Management System“) und deckt Themen wie Rollenverteilung, Risikomanagement, Monitoring, Transparenz und kontinuierliche Verbesserung ab.
Er kann jährlich eingesetzt werden, um Fortschritte messbar zu dokumentieren und Maßnahmen zielgerichtet zu priorisieren.

Hinweis:

Die Nutzung standardisierter Checklisten, Templates und Bewertungsinstrumente erleichtert die systematische Umsetzung der AI-Compliance-Anforderungen und fördert eine konsistente, prüfbare Dokumentation.
Trainingsanbieter können diese Werkzeuge in Workshops oder Gruppenübungen einsetzen, um Teilnehmende praxisnah auf die Entwicklung einer AI-Compliance-Roadmap vorzubereiten.

© A4Q Copyright 2025

18.5 Fazit

Die AI-Compliance-Roadmap verbindet rechtliche Verpflichtungen mit praktischer Umsetzungssteuerung. Organisationen, die frühzeitig ihre Readiness bewerten, Prioritäten setzen und verbindliche Maßnahmen einleiten, reduzieren nicht nur Regelverstöße und Sanktionsrisiken, sondern gewinnen strategische Sicherheit und Vertrauen – im Sinne einer nachhaltigen und verantwortungsvollen KI-Governance.

© A4Q Copyright 2025

19 Zukunft & Weiterentwicklung des Regulierungsrahmens

Hinweis: Dieses Kapitel ist **nicht prüfungsrelevant** und dient als optionale Vertiefung für Trainingsanbieter

🎯 **Business Outcomes:**

BO 19.1 Teilnehmende entwickeln Bewusstsein für kommende Trends (Frontier AI, AI Safety Institute etc.).
BO 19.2 Teilnehmende sind vorbereitet, strategische Anpassungen für zukünftige Regulierungszyklen zu planen und zu kommunizieren.

Nicht prüfungsrelevante Learning Objectives (LOs)

- **LO 19.1 (K1):** Teilnehmende kennen die wichtigsten zukünftigen Entwicklungen des EU AI Act (Leitlinien, delegierte Rechtsakte, AI Act 2.0).
- **LO 19.2 (K2):** Teilnehmende können erklären, wie ergänzende Rechtsakte (Data Act, CRA, DSA, AI Liability Directive) miteinander verknüpft sind und die AI-Compliance-Landschaft erweitern.
- **LO 19.3 (K2):** Teilnehmende können die Rolle des AI Office und des AI Board im europäischen Governance-System beschreiben.
- **LO 19.4 (K3):** Teilnehmende sind in der Lage, internationale Entwicklungen (USA, UK, China, G7, OECD, UN) hinsichtlich Konvergenz, Divergenz und Implikationen für EU-Organisationen zu bewerten.
- **LO 19.5 (K2):** Teilnehmende können erläutern, welche Bedeutung freiwillige Standards und Zertifizierungen (z. B. AI Trust Label, Re-Zertifizierung, Frontier Model Regulation) künftig für die Compliance-Praxis haben.
- **LO 19.6 (K3):** Teilnehmende können reflektieren, welche Kompetenzen und Governance-Mechanismen Organisationen benötigen, um zukünftige regulatorische Änderungen proaktiv zu bewältigen.

Wichtige Begriffe:
Delegierter Rechtsakt, Leitlinien (Guidelines), AI Act 2.0, Frontier AI Regulation, AI Trust Label, Zertifizierung, jährliche Re-Zertifizierung, AI Liability Directive, Data Act, Cyber Resilience Act (CRA), Digital Services Act (DSA), AI Office, AI Board, Globale Harmonisierung, Internationale Kooperation, USA AI Executive Order, UK AI Safety Summit, China Generative AI Regulation, G7 Code of Conduct, UN AI

© A4Q Copyright 2025

Governance Initiative, OECD Framework, Transparenzanforderung, Modellprüfung, Konvergenz der Regulierungen, Zukunftstrends.

Einordnung und Zielsetzung

Dieses optionale Kapitel bietet einen Blick in die Zukunft der europäischen und internationalen KI-Regulierung. Es soll Organisationen helfen, Entwicklungen frühzeitig zu antizipieren, strategisch zu reagieren und Compliance-Strukturen an künftige Anforderungen anzupassen.
Da sich das technologische Umfeld (z. B. Frontier-Modelle, autonome Agenten, multimodale Systeme) rasant verändert, müssen Compliance-Verantwortliche laufend über neue politische, technische und ethische Trends informiert bleiben.

19.1 Europäische Institutionen und Governance-Strukturen (Zeithorizont 2025–2030)

Die Umsetzung und Weiterentwicklung des EU AI Act wird von mehreren neu geschaffenen oder erweiterten europäischen Institutionen getragen, die eine koordinierte, einheitliche und zukunftsorientierte Aufsicht über Künstliche Intelligenz sicherstellen sollen. Diese Strukturen befinden sich aktuell im Aufbau (Stand 2025) und werden ihre volle Wirksamkeit voraussichtlich bis 2027 erreichen.

AI Office (Europäische Kommission)
Das AI Office fungiert als zentrale europäische Koordinierungs- und Aufsichtsbehörde für den Vollzug des AI Act.
Zu seinen Kernaufgaben gehören:

- die Überwachung der einheitlichen Anwendung des EU AI Act,
- die Anerkennung harmonisierter Normen und technischer Spezifikationen,
- die Verwaltung des europäischen Registers für General Purpose AI (GPAI) gemäß Art. 53–55 AI Act,
- sowie die Unterstützung der Mitgliedstaaten bei Marktaufsicht, Audits und Leitlinienentwicklung. Ab 2026 wird das AI Office voraussichtlich auch Aufgaben in der Risikoüberwachung systemisch relevanter KI-Modelle („Systemic Risk Monitoring“) übernehmen.

European AI Board
Der European AI Board ist ein Zusammenschluss der nationalen Aufsichts- und Marktüberwachungsbehörden der EU-Mitgliedstaaten.
Seine Ziele sind:

- der Austausch von Erfahrungen aus der nationalen Umsetzung,

© A4Q Copyright 2025

- die Erarbeitung gemeinsamer Interpretationsleitlinien zum AI Act,
- und die Förderung einer einheitlichen Anwendung in der gesamten Union.
  Der Board arbeitet eng mit der Europäischen Kommission, dem Europäischen Datenschutzausschuss (EDSA) und den Normungsorganisationen CEN/CENELEC zusammen.
  Die operative Tätigkeit soll bis Ende 2025 voll aufgenommen werden.

AI Safety Institute (geplant)
Zur Stärkung der technologischen Sicherheit großer KI-Modelle („Frontier AI“) wird bis 2027 ein europäisches **AI Safety Institute** aufgebaut.
Ziel ist die wissenschaftliche Bewertung von Risiken durch besonders leistungsfähige oder autonom lernende Systeme, einschließlich:

- Robustheits- und Sicherheitsanalysen großer Modelle,
- Evaluierung potenzieller Systemrisiken und Missbrauchsszenarien,
- Entwicklung gemeinsamer Test- und Prüfstandards für Frontier AI.
  Das Institut arbeitet in enger Kooperation mit nationalen Forschungszentren, Sicherheitsbehörden und den europäischen Standardisierungsorganisationen (CEN/CENELEC, ISO/IEC).

Internationale Kooperation
Die EU strebt eine globale Harmonisierung der KI-Governance an. Zwischen 2025 und 2030 werden internationale Partnerschaften und Dialogformate intensiviert, u. a. mit:

- der **OECD** (Principles on AI),
- der **UNESCO** (Ethical AI Framework),
- dem **G7 Hiroshima Process** (Frontier AI Safety Commitments),
- sowie dem **Europarat**, der eine Konvention zu KI, Menschenrechten und Demokratie vorbereitet.

Diese Zusammenarbeit soll sicherstellen, dass europäische Standards in Sicherheits-, Ethik- und Governance-Fragen auch international Anerkennung finden und eine konvergente Regulierung globaler KI-Systeme entsteht.

19.2 Frontier AI und Systemic Risk (Zeithorizont 2025 – 2030)

Der Begriff **„Frontier AI“** bezeichnet besonders leistungsfähige KI-Modelle, die aufgrund ihrer Größe, Generalisierungsfähigkeit und Autonomie das Potenzial besitzen, **systemische Auswirkungen** auf Wirtschaft, Sicherheit, Informationsräume und gesellschaftliche Strukturen zu entfalten. Dazu zählen unter anderem **Modelle der GPT-5-Generation und darüber hinaus**, multimodale Sprach-Bild-Modelle, **autonome Agentennetzwerke** sowie **Simulations- und Entscheidungsengines**, die in kritischen Infrastrukturen eingesetzt werden können.

© A4Q Copyright 2025

Mit der zunehmenden Leistungsfähigkeit dieser Systeme entstehen neue Herausforderungen für Governance, Sicherheit und Aufsicht. Daher arbeiten europäische und internationale Institutionen derzeit (Zeithorizont 2025 – 2030) an einem mehrstufigen Regulierungs- und Prüfrahmen, um Risiken großer KI-Modelle zu bewerten und zu steuern.

Zentrale Entwicklungsrichtungen:

- **Evaluierung systemischer Risiken großer Modelle**
  Künftig wird die Bewertung nicht mehr nur auf Einzelfunktionen, sondern auf die **Gesamtwirkung eines Modells auf gesellschaftliche Prozesse** abzielen. Zu den Hauptthemen zählen Desinformation, algorithmische Verstärkung sozialer Spannungen, mögliche Beeinträchtigung kritischer Infrastrukturen sowie Missbrauch zu Cyber- oder Sicherheitszwecken.
- **Einführung internationaler AI-Safety-Benchmarks**
  Bis spätestens 2027 sollen gemeinsame **Prüf- und Vergleichsverfahren („Benchmarks“) für Frontier-Modelle** etabliert werden. Diese umfassen standardisierte **Transparenzberichte**, **Red-Team-Tests** (gezielte Sicherheits- und Missbrauchstests), **Robustheitsmetriken** und **Erklärbarkeitsbewertungen**.
- **Diskussion um Lizenz- und Meldepflichten**
  Im Zeitraum 2026 – 2028 wird auf EU-Ebene eine **Lizenzierungspflicht für besonders leistungsfähige Modelle** geprüft. Ziel ist es, Anbieter großer Basismodelle zu verpflichten, sicherheitsrelevante Eigenschaften zu dokumentieren, Vorfälle zu melden und Schutzmechanismen nachzuweisen, bevor Modelle öffentlich bereitgestellt werden.
- **Aufbau eines europäischen AI Safety Lab**
  Bis etwa 2028 soll ein **zentrales europäisches Prüf- und Forschungszentrum („AI Safety Lab“) ** entstehen, das Sicherheits-, Fairness- und Robustheitstests für Frontier-Modelle durchführt. Das Lab wird voraussichtlich unter der Leitung des AI Office stehen und eng mit dem geplanten AI Safety Institute, nationalen Forschungsstellen und Standardisierungsgremien (CEN/CENELEC JTC 21, ISO/IEC SC 42) zusammenarbeiten.

Zielsetzung:
Durch diesen gestuften Regulierungsansatz soll gewährleistet werden, dass hochleistungsfähige KI-Modelle **transparenter, sicherer und kontrollierbarer** werden, ohne Innovation und Wettbewerbsfähigkeit in der EU zu hemmen. Frontier AI gilt damit als Schlüsselfeld zukünftiger Governance- und Sicherheitsstrategien in Europa.

19.3 Erwartete Weiterentwicklungen des AI Act (Zeithorizont 2025–2030)

Mit dem Inkrafttreten des EU AI Act im Jahr 2024 beginnt ein fortlaufender Regulierungsprozess, der in mehreren Phasen konkretisiert und erweitert wird. Zwischen 2025 und 2030 werden zahlreiche **delegierte**

© A4Q Copyright 2025

Rechtsakte, Leitlinien und ergänzende Regelwerke erwartet, die die Anwendung des AI Act präzisieren und an neue technologische Entwicklungen anpassen sollen.

Leitlinien und Delegierte Rechtsakte
Die Europäische Kommission plant ab 2026 eine Reihe von **delegierten Rechtsakten und Durchführungsverordnungen**, um Detailanforderungen zu operationalisieren. Dazu zählen insbesondere:

- **Bias-Metriken und Fairness-Indikatoren**, einschließlich sektorenspezifischer Bewertungsmaßstäbe,
- **Logging- und Auditstandards** für Hochrisiko-Systeme,
- **Methodische Leitlinien für die FRIA (Fundamental Rights Impact Assessment)** nach Artikel 27 AI Act,
- sowie **erweiterte Dokumentationspflichten** für General Purpose AI.

Diese Konkretisierungen sollen europaweit einheitliche Maßstäbe schaffen und die Vergleichbarkeit regulatorischer Bewertungen verbessern.

Zweite Regulierungswelle („AI Act 2.0“)
Für den Zeitraum 2027–2030 wird eine **zweite Regulierungswelle** erwartet, oft als „AI Act 2.0“ bezeichnet. Ihr Schwerpunkt liegt voraussichtlich auf:

- der **Aufsicht über Frontier-Modelle und GPAI-Systeme**,
- der Einführung eines **europäischen Sicherheitszertifikats für KI-Systeme**,
- sowie der Schaffung eines kohärenten **GPAI-Ökosystems** mit abgestuften Verantwortlichkeiten für Entwickler, Anbieter und Betreiber.

Verknüpfung mit anderen EU-Regelwerken
Der AI Act entwickelt sich zunehmend zu einem **integrierten Bestandteil des europäischen Digitalrechtsrahmens**. Enge Wechselwirkungen bestehen mit:

- dem **Data Act** (Datenzugang und -nutzungspflichten),
- dem **Cyber Resilience Act** (Sicherheitsanforderungen an vernetzte Produkte),
- dem **Digital Services Act (DSA)** (Inhalts- und Plattformverantwortung),
- und der geplanten **AI Liability Directive** (Haftung für Schäden durch KI-Systeme).

Diese regulatorische Verflechtung erfordert von Unternehmen, Compliance- und IT-Managementsysteme harmonisiert zu betreiben, um Doppelaufwand und Widersprüche zu vermeiden.

Erweiterte Pflichten für Governance und Auditing
Ab 2028 könnten **jährliche Re-Zertifizierungen** für bestimmte Hochrisiko- oder Frontier-Systeme eingeführt werden. Zusätzlich ist die Schaffung eines **„EU AI Trust Labels“** in Diskussion, das

© A4Q Copyright 2025

Organisationen mit nachweislich hoher Compliance- und Governance-Qualität auszeichnet. Dieses Label soll Transparenz und Vertrauen in europäische KI-Produkte stärken.

19.4 Globale Trends und internationale Konvergenz (Zeithorizont 2025–2030)

Die Regulierung von Künstlicher Intelligenz entwickelt sich zunehmend zu einem globalen Thema. Zwischen 2025 und 2030 zeichnen sich mehrere internationale Entwicklungen ab, die auf eine stärkere **Regulierungsharmonisierung und gegenseitige Anerkennung von AI-Compliance-Zertifikaten** hindeuten.

USA – AI Executive Order (2023)
Die USA setzen seit 2023 mit der „Executive Order on Safe, Secure, and Trustworthy AI“ auf verbindliche **Sicherheits-, Bias- und Cyber-Evaluierungen** für staatlich finanzierte KI-Systeme. Nationale Behörden wie NIST und DARPA entwickeln Referenzframeworks, die auch in europäischen Standardisierungsprozessen Berücksichtigung finden.

Vereinigtes Königreich – AI Safety Summit und Frontier AI Taskforce
Das Vereinigte Königreich fördert mit dem **AI Safety Summit** (ab 2023, fortgeführt bis 2030) und der **Frontier AI Taskforce** einen risikobasierten Ansatz mit Fokus auf **Modelltests, Sicherheitsbenchmarks und „Responsibility by Design“**. Eine enge Zusammenarbeit mit der EU ist insbesondere bei Sicherheitszertifikaten und Auditverfahren vorgesehen.

China – Regulierung generativer KI-Dienste
China hat seit 2024 umfassende Regelungen für **„Generative AI Services“** in Kraft gesetzt. Diese umfassen eine **Pflicht zur Datenkennzeichnung**, eine **staatliche Sicherheitsprüfung** vor Veröffentlichung von Modellen sowie Anforderungen an Inhalte, die mit öffentlichen Werten vereinbar sind. Diese Ansätze zeigen, dass KI-Governance zunehmend auch geopolitische Bedeutung erlangt.

OECD und UNESCO – Globale Ethikrahmen
Die **OECD AI Principles** und das **UNESCO Ethical AI Framework** bilden den globalen Referenzrahmen für Fairness, Transparenz und Rechenschaftspflicht. Die EU orientiert sich an diesen Grundsätzen, um internationale Anschlussfähigkeit und **wechselseitige Anerkennung von AI-Governance-Standards** sicherzustellen.

Fazit:
Bis 2030 ist von einer schrittweisen **Konvergenz zwischen europäischen, US-amerikanischen und asiatischen KI-Regelwerken** auszugehen. Unternehmen mit internationaler Tätigkeit profitieren von harmonisierten Standards, müssen jedoch auch mit parallelen Berichtspflichten und unterschiedlichen Nachweisanforderungen rechnen.

© A4Q Copyright 2025

19.5 Strategische Implikationen für Organisationen (Zeithorizont 2025–2030)

Die kommenden Regulierungszyklen verlangen von europäischen Organisationen ein hohes Maß an **strategischer Anpassungsfähigkeit**. KI-Compliance wird sich von einer rechtlichen Pflicht zu einem **kontinuierlichen Steuerungsprozess** entwickeln, der Governance, Technologie, Ethik und Risikomanagement integriert.

Proaktive Compliance-Strategie

Organisationen sollten einen **„Regulatory Watch Process“** etablieren, der alle neuen Leitlinien, delegierten Rechtsakte und internationalen Standards systematisch beobachtet, bewertet und an die eigene Governance-Struktur rückkoppelt.

Adaptive Governance-Strukturen

Künftige Compliance-Modelle müssen flexibel gestaltet sein. Bestehende Policies, Roadmaps und Auditpläne sollten so ausgerichtet werden, dass neue Anforderungen – etwa aus AI Act 2.0, Cyber Resilience Act oder ISO/IEC 42001-Revisionszyklen – ohne Systembruch integriert werden können.

Interdisziplinäre Kooperation

Ein zukunftsorientiertes KI-Compliance-System basiert auf der engen Zusammenarbeit von **Recht, IT, Ethik, Sicherheit und Forschung**. Diese interdisziplinären Strukturen ermöglichen die vorausschauende Bewertung neuer Risiken (z. B. bei Frontier AI, autonomer Entscheidungsfindung oder Datenflüssen in Drittländer).

Kommunikation und Reporting

Ab 2026 wird erwartet, dass Unternehmen **regelmäßige Berichte an Management, Aufsichtsorgane und externe Stakeholder** zu KI-Risiken, Audit-Ergebnissen und regulatorischen Veränderungen veröffentlichen. Diese Berichte dienen der Transparenz, Haftungsprävention und dem Aufbau langfristigen Vertrauens.

Fazit:

Strategische Anpassungsfähigkeit wird zur Kernkompetenz der KI-Governance. Organisationen, die frühzeitig Strukturen für regulatorisches Lernen etablieren, sichern sich Wettbewerbsvorteile und Minimierung zukünftiger Compliance-Kosten.

19.6 Empfohlene Vertiefungsthemen (Zeithorizont 2025–2030)

Für Organisationen und Fachkräfte, die sich über die gesetzlichen Mindestanforderungen hinaus auf kommende Entwicklungen vorbereiten wollen, werden folgende **Vertiefungsfelder** empfohlen:

- **Aufbau eines internen AI-Trend-Radars:**
  Etablierung eines interdisziplinären Teams, das jährlich technologische, regulatorische und ethische Trends auswertet und Handlungsempfehlungen für Management und Compliance erstellt.

© A4Q Copyright 2025

- **Teilnahme an EU-Konsultationen und Normungsprojekten:**
  Aktive Mitwirkung in europäischen und internationalen Standardisierungsgremien wie **CEN/CENELEC JTC 21** und **ISO/IEC JTC 1/SC 42**, um frühzeitig Einblick in entstehende Normen und Prüfverfahren zu gewinnen.
- **Vernetzung mit nationalen AI-Safety-Initiativen:**
  Zusammenarbeit mit nationalen Kompetenzzentren wie **BAAIN (Deutschland)**, **AIT (Österreich)**, **Fraunhofer IAO**, **VDE AI Quality & Testing Hub** oder **Swiss AI Lab IDSIA** zur Durchführung gemeinsamer Sicherheits- und Compliance-Projekte.
- **Analyse zukünftiger KI-Ethik- und Haftungsfragen:**
  Forschung und Weiterbildung zu neuen Themenfeldern wie **autonome Entscheidungssysteme**, **moralische Verantwortlichkeit von KI**, **AI-Personhood-Debatte** oder **ethische Rahmenbedingungen für selbstlernende Agenten**.

Diese Vertiefungsfelder stärken die Fähigkeit von Organisationen, zukünftige Entwicklungen aktiv mitzugestalten und die europäische Führungsrolle in sicherer, verantwortungsvoller und transparenter KI-Governance zu unterstützen.

© A4Q Copyright 2025

20 Empfehlungen für Trainingsanbieter

Zur Sicherstellung eines konsistenten und praxisorientierten Lernerlebnisses im Rahmen des A4Q AI Certified Compliance Trainings ist es für Trainingsanbieter sinnvoll in jedem Kapitel mindestens ein anwendungsorientiertes Lerninstrument einsetzen, etwa eine Fallstudie, Checkliste, Mini-Übung oder Vorlage.

Die konkrete Ausgestaltung wird je nach Zielgruppe, Branchenkontext und Erfahrungshintergrund der Teilnehmenden variieren. Ziel dieser Empfehlung ist es, die praktische Umsetzbarkeit der Lerninhalte in realen Unternehmenssituationen zu fördern und den Wissenstransfer nachhaltig zu sichern.

Trainingsanbieter werden ermutigt, die nachfolgenden Empfehlungen als didaktische Orientierung bei der Gestaltung ihrer Schulungsprogramme zu berücksichtigen. Die Auswahl, Kombination und inhaltliche Tiefe der Praxisbeispiele soll individuell angepasst werden, sofern der praxisorientierte Lernerfolg und die inhaltliche Konsistenz mit dem Syllabus gewährleistet bleiben.

Kapitel	**Empfohlene Bereitstellung durch den Trainingsanbieter**	**Ziel und Nutzen für Teilnehmende**
1 – Einführung in KI-Compliance & EU AI Act	Kurzes Self-Assessment oder Diskussionsübung „Welche Rolle bin ich im Sinne des AI Act?“ (Provider, Deployer etc.)	Fördert Rollenverständnis und Identifikation eigener Verantwortlichkeiten.
2 – Risikobasierter Ansatz & Klassifikation	Mini-Übung zur Einstufung von Use Cases gemäß Annex III, ergänzt um eine Checkliste zur Risikoklassifikation.	Erleichtert das praktische Verständnis des risikobasierten Ansatzes.
3 – Globale & sektorale Regulierungslandschaft	Vergleichsübersicht EU – USA – China sowie Diskussionsleitfaden zu internationalen Unterschieden.	Unterstützt globale Orientierung und strategische Entscheidungsfähigkeit.
4 – Verbotene KI-Praktiken (Art. 5)	Kurzes Praxisbeispiel mit Entscheidungsübung („zulässig oder verboten?“).	Schärft Bewusstsein für Grenzen zulässiger KI-Anwendungen.
5 – Hochrisiko-Systeme (Art. 6–51)	Beispiel eines Konformitäts-Dossiers oder Checkliste für CE-Prozess-Schritte.	Verbindet rechtliche Vorgaben mit operativer Umsetzung.

© A4Q Copyright 2025

Kapitel	Empfohlene Bereitstellung durch den Trainingsanbieter	Ziel und Nutzen für Teilnehmende
6 – Risikomanagement & QMS (ISO 42001 / 23894)	Muster eines AI-Risikoregisters oder eines ISO-Mapping-Sheets.	Zeigt praxisnah, wie Risiken dokumentiert und bewertet werden.
7 – Konformitätsbewertung & CE-Kennzeichnung	Ablaufdiagramm des CE-Prozesses und Beispiel einer Checkliste nach Art. 43–51.	Unterstützt Teilnehmende beim Verständnis des Konformitätsverfahrens.
8 – Transparenzpflichten & Limited-Risk	Beispiel eines Transparenz-Labels (Chatbot-Hinweis, Deepfake-Disclosure) plus UX-Checkliste.	Fördert Bewusstsein für Benutzertransparenz und Vertrauensbildung.
9 – GPAI & Systemic Risk	Due-Diligence-Checkliste für externe Modelle sowie Beispielklauseln für Lieferantenverträge.	Verdeutlicht, wie externe Modelle sicher integriert werden können.
10 – FRIA (Fundamental Rights Impact Assessment)	Vorlage einer kompakten FRIA-Matrix mit Beispielbewertung.	Macht Grundrechte-Bewertungen direkt anwendbar.
11 – Post-Market Monitoring & Incident-Reporting	Muster eines Incident-Report-Formulars und vereinfachtes Monitoring-Dashboard.	Stärkt Verständnis für Überwachungspflichten und Meldewege.
12 – Governance & Organisation	Beispiel einer RACI-Matrix und Rollenbeschreibung „AI Officer“.	Erleichtert organisatorische Implementierung im Unternehmen.
13 – Freiwillige Governance & Ethik	Kurze Reflexionsaufgabe oder Leitfaden für Ethik-Workshops.	Fördert Wertebewusstsein und CSR-Integration.
14 – Audit-Readiness & Sanktionen	Beispiel eines Self-Audit-Fragenkatalogs oder Maturity-Checks.	Bereitet praxisnah auf interne und externe Audits vor.
15 – Harmonisierte Normen & Standards	Mapping-Übung: ISO 42001 ↔ AI Act mit Erläuterungen.	Veranschaulicht die Rolle harmonisierter Normen.
16 – Internationale Schnittstellen & Exportkontrolle	Flussdiagramm oder Entscheidungsbaum für Export- und Sanktionsrisiken.	Unterstützt Risikobewertung bei internationalen Projekten.

© A4Q Copyright 2025

Kapitel	Empfohlene Bereitstellung durch den Trainingsanbieter	Ziel und Nutzen für Teilnehmende
17 – Praxisübungen & Fallstudien	Bereitstellung von vollständigen Übungs-Templates (Audit-Plan, FRIA, Labeling).	Sichert praxisorientiertes Lernen und Transferkompetenz.
18 – Readiness Roadmap & Umsetzung	Vorlage einer AI-Act-Readiness-Roadmap inkl. Quick-Win-Beispiele.	Erleichtert Ableitung konkreter Umsetzungsschritte.
19 – Zukunft & Weiterentwicklung	Diskussionsaufgabe „Welche Entwicklungen betreffen meine Organisation?“	Fördert vorausschauendes Denken und strategische Planung.

© A4Q Copyright 2025

21 Lernziele und kognitive Lernniveaus

Die Bloom’sche Taxonomie wurde 1956 von Benjamin Bloom und seinem Team entwickelt, um Lernziele im kognitiven Bereich systematisch zu ordnen und eine gemeinsame Sprache für Bildungsziele zu schaffen. 2001 überarbeiteten Lorin W. Anderson und David R. Krathwohl das Modell grundlegend, um es an moderne Lern- und Denkprozesse anzupassen. Dabei wurden die Stufen in handlungsorientierte Verben umgewandelt und die oberste Stufe auf das kreative Erschaffen („Create“) statt das Bewerten („Evaluate“) ausgerichtet.

Die revidierte Taxonomie unterscheidet sechs hierarchische Stufen (K1–K6): vom Erinnern einfacher Fakten (K1), über Verstehen und Anwenden (K2, K3), bis hin zum Analysieren (K4), Bewerten (K5) und Erschaffen neuer Konzepte (K6). Diese Struktur unterstützt die präzise Formulierung von Lernzielen und Prüfungsanforderungen, besonders auch in dynamischen Feldern wie Künstliche Intelligenz (KI), Datenschutz (DSGVO) und der Regulierung von KI-Systemen im Rahmen des EU AI Acts

Stufe	Bezeichnung	Beschreibung	Typische Verben	Beispielhafte Aufgabenstellungen
K1	Erinnern	Fakten, Begriffe und Informationen gezielt abrufen und wiedergeben.	nennen, aufzählen, erinnern, identifizieren	- „Nennen Sie die vier Risikokategorien des EU AI Acts.“ - „Zählen Sie die Grundprinzipien der DSGVO auf.“
K2	Verstehen	Bedeutungen erfassen, interpretieren und erklären.	erklären, beschreiben, zusammenfassen, erläutern	- „Erklären Sie, warum KI-Systeme nach dem EU AI Act unterschiedlichen Pflichten unterliegen.“ - „Beschreiben Sie die Bedeutung von ‚Einwilligung‘ im Sinne der DSGVO.“
K3	Anwenden	Wissen in konkreten Situationen nutzen und umsetzen.	anwenden, ausführen, demonstrieren, verwenden	- „Wenden Sie die Kriterien des EU AI Acts an, um die Risikoklasse eines Chatbots zu bestimmen.“ - „Wenden Sie die Anforderungen der DSGVO an, um eine Datenschutzerklärung für eine Website zu erstellen.“

© A4Q Copyright 2025

Stufe	Bezeichnung	Beschreibung	Typische Verben	Beispielhafte Aufgabenstellungen
K4	Analysieren	Informationen in Bestandteile zerlegen, Beziehungen und Strukturen erkennen.	analysieren, differenzieren, untersuchen, vergleichen	- „Analysieren Sie die Unterschiede in der Regulierung von Hochrisiko-KI-Systemen zwischen dem EU AI Act und der DSGVO.“ - „Untersuchen Sie die Zusammenhänge zwischen Datensicherheitspflichten im EU AI Act und in der DSGVO.“
K5	Evaluieren (Bewerten)	Beurteilungen treffen und Argumente oder Methoden kritisch bewerten.	bewerten, begründen, kritisieren, überprüfen	- „Bewerten Sie die Effektivität der Risikobewertungsvorgaben im EU AI Act.“ - „Kritisieren Sie die Wirksamkeit der DSGVO hinsichtlich des Schutzes persönlicher Daten in sozialen Netzwerken.“
K6	Erschaffen (Kreatives Gestalten)	Neue Produkte, Theorien oder Lösungsansätze entwickeln.	entwerfen, planen, konzipieren, generieren	- „Entwerfen Sie ein KI-System-Entwicklungskonzept, das die Anforderungen des EU AI Acts vollständig berücksichtigt.“ - „Planen Sie eine datenschutzkonforme mobile App unter Berücksichtigung der DSGVO.“

© A4Q Copyright 2025

22 Literatur

22.1 Fachliteratur

[1] Andreas Klein, *Künstliche Intelligenz in Unternehmen: Grundlagen, Anwendungen und Implikationen*, Springer Gabler, 2021 (Kap. 1, 2, 12, 18)

[2] Jürgen Gallmann, *Künstliche Intelligenz: Was auf Unternehmen zukommt*, Redline Verlag, 2020 (Kap. 1, 3, 12, 19)

[3] Thomas Ramge, *Mensch und Maschine: Wie Künstliche Intelligenz und Roboter unser Leben verändern*, Reclam Verlag, 2020 (Kap. 1, 13, 19)

[4] Tobias Kollmann (Hrsg.), *Künstliche Intelligenz in Wirtschaft und Gesellschaft: Eine multidisziplinäre Betrachtung*, Springer Gabler, 2021 (Kap. 1, 3, 13, 19)

[5] Peter Buxmann, Holger Schmidt, *Künstliche Intelligenz: Mit Algorithmen zum wirtschaftlichen Erfolg*, Springer Gabler, 2019 (Kap. 1, 2, 12)

[6] Karl-Heinz Land, *Erde 5.0: Die Zukunft provozieren – Digitalisierung, Künstliche Intelligenz und der Mensch*, Murmann Publishers, 2018 (Kap. 1, 13, 19)

[7] Richard David Precht, *Künstliche Intelligenz und der Sinn des Lebens*, Goldmann Verlag, 2020 (Kap. 13, 19)

[8] Pascal Finette, Jeffrey Rogers, *The Disruption Map: AI and the Future of Business*, Singularity University Press, 2022 (Kap. 1, 3, 18, 19)

[9] Mark Coeckelbergh, *AI Ethics*, MIT Press, 2020 (Kap. 8, 13, 19)

[10] Jacob Turner, *Robot Rules: Regulating Artificial Intelligence*, Palgrave Macmillan, 2019 (Kap. 3, 4, 5, 13, 15)

[11] Justin B. Bullock et al. (eds.), *The Oxford Handbook of AI Governance*, Oxford University Press, 2023 (Kap. 5, 6, 12, 13, 15)

[12] Roger Brownsword et al. (eds.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge University Press, 2020 (Kap. 3, 4, 5, 13, 16)

[13] Tshilidzi Marwala, Ebo Banjo Adam, *The Governance of Artificial Intelligence*, Elsevier, 2024 (Kap. 6, 12, 15, 18)

[14] Janelle Shane, *You Look Like a Thing and I Love You: How AI Works and Why It's Making the World a Weirder Place*, Little Brown Spark, 2019 (Kap. 1, 2, 8 – für leicht verständliche Einstiege in KI-Logik)

[15] Kate Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021 (Kap. 3, 13, 19)

© A4Q Copyright 2025

[16] John C. Havens, *Heartificial Intelligence: Embracing Our Humanity to Maximize Machines*, TarcherPerigee, 2016 (Kap. 13, 19)

[17] Mazyar Peihani et al., *Principles of AI Governance and Model Risk Management*, Springer Nature, 2023 (Kap. 6, 7, 12, 14, 15)

[18] John Basl et al., *Governing the Machine: How to Navigate the Risks of AI and Unlock its True Potential*, MIT Press, 2024 (Kap. 6, 12, 14, 18)

[19] Patrick Lin, Keith Abney, Ryan Jenkins (eds.), *Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence*, Oxford University Press, 2017 (Kap. 8, 13, 16)

[20] George Musser, *Putting Ourselves Back in the Equation: Why Physicists Are Studying Human Consciousness and AI*, Farrar Straus & Giroux, 2023 (Kap. 19 – Zukunftsperspektiven und Bewusstsein)

[21] John Zysman, Martin Kenney (eds.), *AI and the Boardroom: Corporate Governance, Strategy and Accountability in the Age of Artificial Intelligence*, Routledge, 2024 (Kap. 12, 13, 18)

[22] Michael G. Solomon, *AI and Cybersecurity for Leaders*, CRC Press, 2023 (Kap. 6, 11, 16)

[23] National Institute of Standards and Technology (NIST), *AI Risk Management Framework – Generative AI Profile (NIST AI 600-1)*, U.S. Department of Commerce, 2024 (Kap. 6, 9, 14, 15, 18)

[24] OECD, *AI Governance Principles and Implementation Guidance*, OECD Publishing, 2023 (Kap. 3, 12, 13, 15)

22.2 Fachartikel und Studien

[1] **Bitkom e. V.**, *Künstliche Intelligenz 2024 – Einsatz, Nutzen und Herausforderungen in der deutschen Wirtschaft*, Bitkom Research, 2024.

[2] **Roland Berger**, *Artificial Intelligence 2025 – Europas Weg zur vertrauenswürdigen KI-Ökonomie*, Roland Berger Insights, 2024.

[3] **McKinsey & Company**, *The State of AI in 2024: Scaling Generative AI Responsibly*, McKinsey Global Report, 2024.

[4] **Deloitte Deutschland**, *AI in Unternehmen 2024 – Reifegrade, Governance und Regulatorische Readiness*, Deloitte Insights, 2024.

[5] **Boston Consulting Group (BCG)**, *Bridging the Trust Gap – Responsible AI and Regulation in Europe*, BCG Report, 2024.

[6] **EY Deutschland**, *AI Governance in Practice – From Compliance to Competitive Advantage*, EY Insights, 2024.

© A4Q Copyright 2025

[7] **PwC Europe**, *AI Regulation Monitor 2025 – Umsetzung des EU AI Act in Unternehmen*, PwC Studie, 2025.

[8] **Capgemini Research Institute**, *Generative AI and Responsible Use – Managing Ethics and Risk*, Capgemini Report, 2024.

[9] **Accenture Research**, *AI at Scale 2024 – Operationalizing Trustworthy AI Systems*, Accenture Global Report, 2024.

[10] **Fraunhofer IAO**, *Leitfaden KI-Compliance für Unternehmen – Praxisorientierte Umsetzung des EU AI Act*, Fraunhofer Verlag, 2024.

[11] **Stifterverband & BMBF**, *Responsible AI in Germany 2024 – Ergebnisse aus der KI-Strategie-Evaluation*, Stifterverband Report, 2024.

[12] **Swiss Digital Initiative (SDI)**, *Trusted AI 2025 – Transparenz und Auditierbarkeit in KI-Systemen*, SDI Report, 2025.

[13] **ETH Zürich**, *Generative AI und Wirtschaft in der Schweiz – Status und Governance-Herausforderungen*, ETH Studie, 2024.

[14] **Österreichisches Bundesministerium für Arbeit und Wirtschaft (BMAW)**, *KI in der österreichischen Wirtschaft 2024 – Anwendungsfelder und Compliance-Bedarf*, BMAW Bericht, 2024.

[15] **Center for the Governance of AI (University of Oxford)**, *AI Governance Report 2025 – Accountability and Global Standards*, Oxford Initiative on AI Ethics, 2025.

[16] **OECD**, *AI Policy Outlook 2024 – Governance, Risk and Trust in Artificial Intelligence*, OECD Publishing, Paris, 2024.

[17] **European Commission / AI Office**, *Guidelines on Transparency and General-Purpose AI Models (Art. 53 AI Act)*, EU Official Publication, Brüssel, 2025.

[18] **European Commission / AI Office**, *Draft Guidance on Serious AI Incidents and Post-Market Monitoring*, Konsultationsentwurf, 2025.

[19] **ENISA**, *Threat Landscape for Artificial Intelligence 2025*, ENISA Report, Athen, 2025.

[20] **NIST (U.S. Department of Commerce)**, *NIST AI RMF Generative AI Profile (NIST AI 600-1)*, Gaithersburg, 2024.

[21] **World Economic Forum (WEF)**, *Global AI Governance Report 2024 – Shaping Responsible AI Ecosystems*, WEF White Paper, Genf, 2024.

[22] **Zukunftsinstitut**, *Smart Business 2025 – Wie Künstliche Intelligenz Wertschöpfung neu definiert*, Trendstudie, 2025.

[23] **IBM Institute for Business Value**, *Global AI Adoption Index 2024*, IBM Insights, 2024.

[24] **SAP**, *Integrating AI into Business Processes 2024 – Best Practices and Compliance by Design*, SAP Whitepaper, 2024.

© A4Q Copyright 2025

[25] **German AI Association (KI Bundesverband)**, *Positionspapier 2025 – Anforderungen an eine zukunftsfähige KI-Politik und den AI Act 2.0*, Berlin, 2025.

22.3 Gesetzliche Regelungen und Strategiedokumente

[1] **Regulation (EU) 2024/1689**, vom 13.06.2024, *Artificial Intelligence Act* – veröffentlicht im Amtsblatt am 12.07.2024 (OJ L, 2024/1689). ELI: data.europa.eu/eli/reg/2024/1689/oj.

[2] **Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR)**, gültig seit 25.05.2018.

[3] **Regulation (EU) 2023/2854 – Data Act**, 13.12.2023 – faire Nutzungs- und Zugangsregeln für Daten.

[4] **Regulation (EU) 2022/2065 – Digital Services Act (DSA)**, 27.10.2022 – Regeln für digitale Dienste und Plattformverantwortung.

[5] **Regulation (EU) 2022/1925 – Digital Markets Act (DMA)**, 21.09.2022 – Wettbewerbsregeln für „Gatekeeper"-Plattformen.

[6] **Directive (EU) 2022/2555 – NIS2 Directive**, 27.12.2022 – hohes gemeinsames Cybersicherheitsniveau in der EU.

[7] **Regulation (EU) 2019/881 – Cybersecurity Act**, 07.06.2019 – Einrichtung der ENISA und EU-Zertifizierungsrahmen.

[8] **Regulation (EU) 2024/2847 – Cyber Resilience Act (CRA)**, 23.10.2024 – horizontale Cybersicherheitsanforderungen für digitale Produkte; in Kraft seit 10.12.2024.

[9] **Regulation (EU) 2022/868 – Data Governance Act (DGA)**, 03.06.2022 – Rahmen für Dateninfrastrukturen und Treuhanddienste.

[10] **Directive (EU) 2024/2853 – Product Liability Directive (recast)**, 23.10.2024 – Modernisierung der Produkthaftung (inkl. Software & KI); Anwendung ab 09.12.2026.

[11] **Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CETS No. 225)**, 05.09.2024 – erstes völkerrechtlich bindendes KI-Abkommen („AIFC").

[12] **Regulation (EU) 2024/… – AI Liability Directive** *(voraussichtliche Verabschiedung Ende 2025)* – Harmonisierung zivilrechtlicher Haftung für KI-Schäden (geplanter Nachfolger des AI Liability Proposal COM(2022) 496).

[13] **Deutschland: Gesetz zur Durchführung der KI-Verordnung (KI-DVO-DE, Entwurf 2025)** – BNetzA als zentrale Marktüberwachungsbehörde; Einrichtung des *Kompetenzzentrums Künstliche Intelligenz und Vertrauenswürdige Systeme (KoKIVO)*; Regelung von Sanktionen und Innovationsförderung. BMDS / CMS Bloggt.

[14] **Frankreich: Draft National Law on AI Governance (2025)** – dezentralisierte Durchsetzung des EU AI Act über bestehende Behörden (CNIL, ARCOM u. a.); im Gesetzentwurf 2025 festgelegt. Quelle: mlex.com.

© A4Q Copyright 2025

[15] **Frankreich: Bill No. 675 – Labeling of AI-Generated Images on Social Networks**, eingebracht März 2025 – Pflicht zur Kennzeichnung von KI-erstellten oder -modifizierten Bildern in sozialen Medien. Quelle: loc.gov.

[16] **Spanien: Royal Decree 817/2023 – AI Regulatory Sandbox** – Testumgebung für High-Risk-KI-Systeme im Rahmen der EU-Umsetzung des AI Act.

[17] **Spanien: Draft Law for the Good Use and Governance of AI (Anteproyecto de Ley para el Buen Uso y la Gobernanza de la IA)**, März 2025 – ergänzt den EU AI Act durch nationale Sanktions- und Lizenzregeln.

[18] **Spanien: Spanish Agency for the Supervision of Artificial Intelligence (AESIA)**, gegründet 2023 – erste nationale KI-Aufsichtsbehörde in Europa mit Sitz in A Coruña.

[19] **Italien: National AI Strategy and Implementation Plan 2024–2026** – Strategie für vertrauenswürdige KI und Human-Centric Innovation; federführend Ministero dell'Innovazione Technologica e Transizione Digitale.

[20] **Niederlande: AI Governance Roadmap 2025** – nationale Umsetzungsstrategie zum EU AI Act unter Einbindung der Autoriteit Persoonsgegevens und TÜV-akkreditierter Auditoren.

[21] **Österreich: AIM AT 2030 – Strategie für Künstliche Intelligenz in Österreich**, 2021 (mit laufender Umsetzung durch das BMAW und FFG-Programme zur KI-Compliance).

[22] **Schweiz: Strategie Künstliche Intelligenz des Bundes**, BAFU/WBF 2020 – fortgeschrieben 2024 unter Einbeziehung der OECD-Leitprinzipien und des Europarats-Abkommens.

[23] **Vereinigtes Königreich (UK): AI Regulation Bill (Entwurf 2025)** – geplanter britischer Rechtsrahmen mit Impact-Assessment-Pflichten und Compliance-Governance.

[24] **Vereinigtes Königreich (UK): Data (Use and Access) Act 2025**, verabschiedet 19.06.2025 – regelt Zugangsrechte zu Trainingsdaten für KI-Modelle und Drittanbieter.

[25] **Vereinigtes Königreich (UK): Product Regulation and Metrology Act 2025**, 21.07.2025 – aktualisiert Produktsicherheits- und Marktüberwachungsrecht für KI-basierte Produkte.

22.4 Normen und Standards

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

[2] **ISO/IEC 23053:2022**, *Rahmenwerk für maschinelles Lernen*, ISO.

[3] **ISO/IEC TR 24028:2020**, *Trustworthiness von KI – Überblick zu Sicherheit und Resilienz*, ISO.

[4] **ISO/IEC 23894:2023**, *Artificial Intelligence – Guidance on Risk Management*, ISO.

© A4Q Copyright 2025

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

[6] **DIN SPEC 92001-2:2021**, *Qualitätsanforderungen an KI-Systeme – Prüfkriterien*, DIN.

[7] **ISO/IEC 27001:2022**, *Informationssicherheits-Managementsysteme (ISMS)*, ISO.

[8] **ISO/IEC 27701:2019**, *Datenschutz-Managementsysteme (Erweiterung von ISO 27001)*, ISO.

[9] **ISO/IEC 42001:2023**, *Artificial Intelligence Management System (AIMS)* – Anforderungen an ein KI-Managementsystem; zentrales Governance-Rahmenwerk.

[10] **ISO/IEC 42006:2025**, *Requirements for Bodies Auditing and Certifying AIMS* – Zusatzanforderungen für Zertifizierungsstellen zur Auditierung nach ISO/IEC 42001.

[11] **ISO/IEC 5259-1:2024**, *Data Quality for Analytics and Machine Learning – Part 1: Overview and Vocabulary* – Grundlage der 5259-Serie zur Datenqualität (Begriffe und Überblick).

[12] **ISO/IEC 5259-2:2024**, *Data Quality for Analytics and Machine Learning – Part 2: Data Quality Model and Metrics* – Definition von Datenqualitätskriterien und Messgrößen.

[13] **ISO/IEC 5259-4:2024**, *Data Quality for Analytics and Machine Learning – Part 4: Process Framework* – Prozessrahmen zur Sicherung und Bewertung von Datenqualität in Analytics und ML.

[14] **ISO/IEC 5259-5:2025**, *Data Quality for Analytics and Machine Learning – Part 5: Data Governance* – Leitlinien zur Governance von Datenqualität im Lebenszyklus von KI-Systemen.

[15] **ISO/IEC 5338:2023**, *Artificial Intelligence – AI System Life Cycle Processes* – Lebenszyklusprozesse für KI-Systeme.

[16] **ISO/IEC 38507:2022**, *Governance of IT – Governance Implications of the Use of AI* – Leitfaden zur Verankerung von KI-Governance in Unternehmensführung und IT-Strategie.

[17] **ISO/IEC TR 24027:2021**, *Bias in AI Systems and AI-Aided Decision Making* – Leitfaden zur Erkennung und Bewertung von Bias in KI-Systemen.

[18] **ISO/IEC TR 24029-1:2021**, *Assessment of the Robustness of Neural Networks – Part 1: Overview* – Bewertung der Robustheit von KI-Modellen.

[19] **ISO/IEC 24029-2:2023**, *Assessment of the Robustness of Neural Networks – Part 2: Formal Methods* – Methoden zur formalen Überprüfung von KI-Systemen.

[20] **ISO/IEC TR 29119-11:2020**, *Software Testing – Part 11: Guidelines on the Testing of AI-Based Systems* – Richtlinien zum Testen KI-basierter Systeme.

[21] **ISO/IEC 25059:2023**, *Systems and Software Quality Requirements and Evaluation (SQuaRE) – Quality Model for AI Systems* – Qualitätsmodell für KI-Systeme und -Produkte.

© A4Q Copyright 2025

22.5 Internationale Leitlinien / Ethik- und Governance-Frameworks für KI

[1] **NIST AI RMF – Generative AI Profile (NIST.AI.600-1, 2024)** – ein spezielles Profil des AI Risk Management Frameworks, fokussiert auf Risiken generativer KI-Systeme. Greenberg Traurig+3NIST Publikationen+3NIST+3

[2] **OECD AI Principles / OECD Recommendation on AI** – Wertebasierter Rahmen mit Empfehlungen für nationale Politiken, Governance und internationale Kooperation. OECD+2oecd.ai+2

[3] **UNESCO Recommendation on the Ethics of Artificial Intelligence** – globaler ethischer Leitfaden für KI, verabschiedet 2021 und anwendbar auf alle Mitgliedsstaaten. Tandfonline+3UNESCO+3Deutsche UNESCO-Kommission+3

[4] **EU Ethics Guidelines for Trustworthy AI**, High-Level Expert Group on AI (EU) – 7 Anforderungen, die KI-Systeme erfüllen sollten, z. B. Transparenz, Robustheit, Datenschutz. Digitale Strategie Europa+2Research and innovation+2

[5] **IEEE Standards / Ethically Aligned Design (EAD)** – Sammlung ethischer Prinzipien und technischer Vorgaben für KI (IEEE 7000-Serie u. a.).

[6] **Charter for AI Ethics (Salzburg Global / internationale Initiative)** – normative Charta mit Prinzipien wie Transparenz, Verantwortung, psychologische Unversehrtheit etc. salzburgglobal.org

22.6 Cybersecurity-Lagebilder (KI-Bezug)

[1] **ENISA Threat Landscape 2025** – *Annual Report on the Threat Landscape (July 2024 – June 2025)*, Europäische Agentur für Netz- und Informationssicherheit (ENISA), 2025.
Aktuelles EU-Blickfeld auf KI-gestützte Cyberbedrohungen (z. B. Deepfakes, generatives Phishing, Datenvergiftung, LLM-Abuse).

[2] **ENISA AI Cybersecurity Challenges Report 2024** – Analyse der sicherheitsrelevanten Risiken von KI-Modellen und -Architekturen, inkl. adversarial attacks und Modell-Steuerung (Model Poisoning).

[3] **Europol / Trend Micro / UNICRI: Malicious Uses and Abuses of Artificial Intelligence – 2024 Update** – Bericht über kriminelle Nutzung von KI, generative Deepfakes, Voice Cloning & Fraud-Automation.

[4] **NIST Cybersecurity Framework (CSF 2.0, 2024)** – überarbeitete Version mit integriertem AI-Security-Kapitel (Mapping zu AI RMF und ISO/IEC 27001).

[5] **WEF Global Cybersecurity Outlook 2025**, World Economic Forum – Fokus auf generative KI-Risiken, Supply-Chain-Threats und Manipulation kritischer Informationsinfrastrukturen.

[6] **Microsoft Digital Defense Report 2024** – jährlich erscheinender Sicherheitsbericht zu globalen Angriffstrends, inkl. KI-gestützter Desinformationskampagnen und LLM-gestützter Malware-Automatisierung.

[7] **Google / Mandiant Threat Intelligence Report 2025** – Erkenntnisse zu automatisierter Code-Exploitation, Prompt-Injection-Angriffen und generativer Schadsoftware.

© A4Q Copyright 2025

[8] **Europol Internet Organised Crime Threat Assessment (IOCTA 2025)** – Lagebericht der europäischen Strafverfolgungsbehörde, Schwerpunkt auf KI-missbrauchte Betrugsformen und automatisierte Cyberangriffe.

[9] **OECD / ENISA Joint Policy Brief 2025: AI Safety & Cyber Resilience** – politische Handlungsempfehlungen für Mitgliedstaaten zu Sicherheits-by-Design, Incident-Sharing und cross-border cooperation.

© A4Q Copyright 2025

23 Anhänge

23.1 Anhang A – Leitfaden für internationale Anbieter

Hinweise für Anbieter **außerhalb der EU**, die KI-Systeme **in der EU** anbieten und Hinweise für Anbieter, die **in anderen Rechtsräumen** mit unterschiedlichen Regulierungsansätzen tätig sind.

Internationale Ergänzungen – A4Q AI Certified Compliance Syllabus

Kapitel	Fokus (Thema)	Pflichten / Besonderheiten für Nicht-EU-Anbieter	Empfohlene Maßnahmen / Tools
1	Einführung & Geltungsbereich	Extraterritoriale Wirkung des AI Act: Anbieter außerhalb der EU fallen darunter, wenn ihr System in der EU eingesetzt wird.	EU-Vertreter benennen; CE-Konformität vorbereiten; EU-Rechtsbezug dokumentieren.
2	Risikobasierter Ansatz	EU-Risikokategorien übernehmen, um Produktvergleiche und Compliance-Nachweise zu ermöglichen.	Mapping auf NIST AI RMF (USA) oder AIDA (Kanada) durchführen.
3	Globale Regulierungslandschaft	Unterschiedliche KI-Gesetze: USA (NIST), UK (Principles), China (Generative AI Rules), Brasilien (Marco Legal AI), Kanada (AIDA).	„Global Regulatory Matrix“ pflegen; lokale Module ergänzen.
4	Risikomanagement & technische Compliance	Risikomanagementsystem nach ISO/IEC 23894 + NIST AI RMF kombinieren.	Einheitliches Risk Register; global harmonisierte Risikokategorien.
5	Datenqualität & Governance	Daten außerhalb der EU unterliegen DSGVO-Äquivalenzpflichten.	Data Transfer Impact Assessment (DTIA); Standardvertragsklauseln; Data Provenance nachweisen.
6	Technische Dokumentation	EU verlangt Technical File nach Annex IV AI Act.	Einheitliches globales „AI Conformity Dossier“; Verweis auf Model Card/Data Sheet.

© A4Q Copyright 2025

Kapitel	Fokus (Thema)	Pflichten / Besonderheiten für Nicht-EU-Anbieter	Empfohlene Maßnahmen / Tools
7	Transparenz & Kennzeichnung	Unterschiede bei Offenlegungspflichten (EU Art. 52, China Labeling, USA freiwillig).	Multi-Label-System für KI-Outputs und Nutzungskennzeichnung.
8	Human Oversight & Sicherheit	EU verlangt „Human Oversight“; USA/NIST betonen „Responsible Human Participation“.	Schulungen & Checklisten für Human-in-the-Loop-Kontrollen.
9	General-Purpose-AI & Foundation Models	EU Art. 53–55: GPAI-Pflichten; US-NIST und UK verlangen Dokumentation und Sicherheitsprüfungen.	GPAI-Compliance-Template; Model Evaluation Report.
10	Grundrechts-Folgenabschätzung (FRIA)	EU-FRIA ähnlich wie US/Canada „Algorithmic Impact Assessment“.	Einheitliche Impact-Assessment-Vorlage nutzen (EU-AIDA-kompatibel).
11	Post-Market-Monitoring	Incident Reporting muss auch von Nicht-EU-Anbietern an EU-Behörden erfolgen.	PMS-Prozess (ISO/IEC 42001) implementieren; Shared Reporting Channel mit EU-Partnern.
12	Governance & interne Rollen	EU verlangt KI-Officer; außerhalb der EU Governance Board oder Responsible AI Lead üblich.	Globales AI Governance Board etablieren; Zuständigkeiten dokumentieren.
13	Freiwillige Governance & Ethik	OECD, UNESCO, G7 Codes of Conduct als globale Ethikrahmen anerkannt.	Ethik-Code im Unternehmen verankern; freiwillige Selbstzertifizierung (z. B. NIST/IEEE).
14	Audit & Nachweisführung	EU-Konformität auditierbar; US-NIST fordert interne Audits; UK „Assurance Framework“.	Interne und externe KI-Audits (ISO/IEC 42001, 27001).
15	Harmonisierte Standards	EU-Presumption of Conformity durch ISO/IEC-Normen erreichbar.	ISO/IEC 42001, 23894, 22989, 23053 anwenden; Normenbibliothek pflegen.

© A4Q Copyright 2025

Kapitel	Fokus (Thema)	Pflichten / Besonderheiten für Nicht-EU-Anbieter	Empfohlene Maßnahmen / Tools
16	Exportkontrolle & Lieferketten	EU Dual-Use-Verordnung, US ITAR/EAR und chinesische Technologieexportgesetze beachten.	Exportklassifizierung prüfen; globale Compliance-Chain dokumentieren.
17	Praktische Umsetzung & GPAI-Management	Einheitliche globale Dokumentationsstruktur für GPAI- und FRIA-Prozesse.	AI Compliance Templates (EU ↔ US ↔ China) harmonisieren.
18	Roadmap & Readiness	Globaler Reifegradvergleich (EU AI Act – NIST – AIDA).	„AI Readiness Assessment“ weltweit durchführen; Maturity Model einführen.
19	Zukunft & internationale Konvergenz	Annäherung der Rechtsräume (EU–USA–OECD–G7) absehbar.	Teilnahme an ISO/IEC SC 42, CEN/CENELEC JTC 21; globale Zertifizierungsstrategie planen.

Allgemeine Empfehlung für internationale Anbieter

- **Compliance-Hub aufbauen:** zentrale Sammlung aller Rechtsräume (EU, US, UK, China, Kanada, Brasilien).
- **Dual-Dokumentation:** EU-Dossiers + US-NIST-Profile pflegen.
- **Zertifizierungsstrategie:** ISO/IEC 42001 als globaler „Common Compliance Layer“.
- **Legal Monitoring:** Frühwarnsystem für neue delegierte Rechtsakte oder lokale AI Bills.

© A4Q Copyright 2025