

Vorbereitungshandbuch

Ausgabe 202602

Copyright © EXIN Holding B.V. 2026. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

Inhalt

1. Überblick 4
2. Prüfungsanforderungen 8
3. Liste der Grundbegriffe 11
4. Literatur 15
5. Karrierepfad 17

1. Überblick

EXIN Artificial Intelligence Compliance Professional (AICP.DE)

Anwendungsbereich

Die EXIN Artificial Intelligence Compliance Professional-Zertifizierung bestätigt, dass die Fachkraft in der Lage ist, die Konformität (Compliance) der Entwicklung, Inbetriebnahme und Verwendung von Systemen der künstlichen Intelligenz (KI) mit einschlägigen Gesetzen, Verordnungen und Normen sowie die Übereinstimmung mit Ethikpraktiken sicherzustellen.

Diese Zertifizierung deckt folgende Themen ab:

- Kontext der KI-VO
- Die KI-VO im Detail
- Vertrauenswürdige KI
- Ethische KI
- Praktische Anwendung der KI-VO
- Rahmenwerke zur Unterstützung der Konformität (Compliance)

Zusammenfassung

Die künstliche Intelligenz (KI) steht an vorderster Front einer bedeutenden technologischen Transformation, die Maschinen ermöglicht, Aufgaben auszuführen, die normalerweise menschliche Intelligenz erfordern. Mit dieser leistungsstarken Technologie können komplexe Prozesse automatisiert und wertvolle Erkenntnisse aus großen Datensätzen gewonnen werden. Dies führt zu Innovationen und neuartigen Lösungen. Das Potenzial von KI ist ein zentrales Thema in Diskussionen über die Zukunft der Technologie.

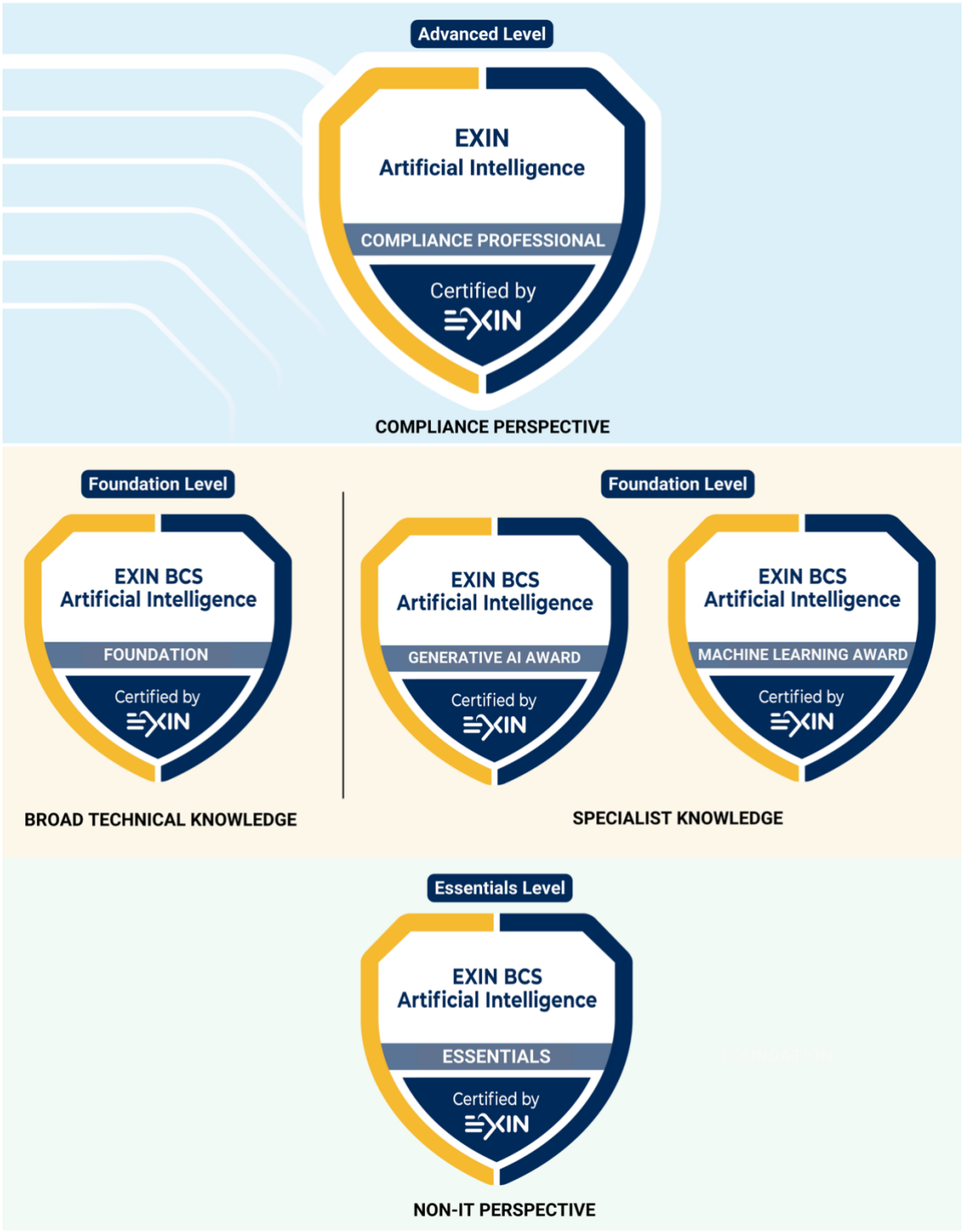
Im heutigen Geschäftsumfeld erfordert die Integration von KI in die betrieblichen Abläufe ein fundiertes Verständnis der Konformität (Compliance) von KI. Das ist ein entscheidender Erfolgsfaktor. Die KI-VO ist ein regulatorisches Rahmenwerk, das sicherstellen soll, dass KI-Technologien sicher und verantwortungsvoll verwendet werden. Konformität mit der KI-VO hilft Unternehmen, Risiken zu managen, Verbraucherrechte zu schützen und das Vertrauen und die Transparenz zu fördern, die Voraussetzung für langfristiges Wachstum sind. Dabei geht es nicht einfach nur um die Einhaltung von Rechtsvorschriften. Vielmehr müssen Unternehmen eine Führungsrolle in ethischen Innovationen übernehmen und neue Branchenstandards setzen.

Die EXIN Artificial Intelligence Compliance Professional-Zertifizierung bietet einen Weg zu einer solchen Führungsrolle in diesem wichtigen Bereich. Sie ist für Fachkräfte bestimmt, die dafür verantwortlich sind sicherzustellen, dass KI-Systeme rechtliche Standards und ethische Normen erfüllen. Diese Zertifizierung vermittelt ein umfassendes Verständnis der KI-VO, unterstützt die Entwicklung vertrauenswürdiger und ethischer KI und veranschaulicht die Anwendung der KI-Rechtsvorschriften in der Praxis.

Fachkräfte in Rollen wie KI-Compliance-Beauftragter, Qualitätsmanager oder Risikomanager können durch diese Zertifizierung die Fähigkeiten erwerben, die sie benötigen, um sich in der komplexen Landschaft der KI-Konformität (Compliance) zurechtzufinden. Diese Spezialistinnen und Spezialisten übernehmen kritische Aufgaben in Organisationen: Sie fördern verantwortungsvolle KI-Praktiken und lenken Unternehmen in Richtung einer innovativen und erfolgreichen Zukunft. In einer Welt, in der die Zukunft im Zeichen von KI stehen wird, ist es nicht nur von Vorteil, wenn Unternehmen den verantwortungsvollen Umgang mit diesen Technologien meistern. Vielmehr bietet sich ihnen hier eine entscheidende Chance, einen großen Unterschied zu machen. Bereiten Sie sich darauf vor, Ihr Unternehmen effektiv in die KI-gestützte Zukunft zu führen.

Kontext

Die Zertifizierung EXIN Artificial Intelligence Compliance Professional ist Teil des EXIN Artificial Intelligence-Qualifizierungsprogramms.



Zielgruppe

Zur Zielgruppe der EXIN Artificial Intelligence Compliance Professional-Zertifizierung gehören Fachkräfte, die für die Einhaltung der KI-Rechtsvorschriften in ihrer Organisation verantwortlich sind, KI-Systeme entwickeln und nutzen und sich dabei darauf konzentrieren, die Konformität (Compliance) und die Umsetzung zu beaufsichtigen.

Dazu gehören unter anderem:

- KI-Compliance-Beauftragte
- Qualitätsmanagerinnen und -manager
- Risikomanagerinnen und -manager
- Führungskräfte in Rechtsabteilungen
- Datenschutzbeauftragte
- Produktmanagerinnen und -manager
- KI-Entwicklerinnen und -Entwickler sowie AI-Engineers
- Compliance-Analystinnen und -Analysten
- IT-Sicherheits-Managerinnen und -Manager
- Betriebsleiterinnen und -leiter
- Mitglieder der Geschäftsführung bzw. C-Level-Führungskräfte

Zertifizierungsvoraussetzungen

- Erfolgreicher Abschluss der Prüfung EXIN Artificial Intelligence Compliance Professional.
- Akkreditierte EXIN Artificial Intelligence Compliance Professional-Schulung, einschließlich Abschluss der praktischen Aufgabenstellungen.

Kenntnisse der KI-Terminologie, beispielsweise durch die Zertifizierung EXIN BCS Artificial Intelligence Foundation, werden dringend empfohlen.

Einzelheiten zur Prüfung

Art der Prüfung:	Multiple-Choice-Fragen
Anzahl der Fragen:	40
Mindestpunktzahl:	65% (26/40 Fragen)
Einsicht in Dokumentation:	Der Text des KI-VO kann während der Prüfung eingesehen werden. Dieser Text ist in der digitalen Prüfung als Anhang verfügbar. Bei schriftlichen Prüfungen müssen die Kandidaten ein eigenes Exemplar mitbringen.
Notizen machen:	Nein
Elektronische Geräte/Hilfsmittel erlaubt:	Nein
Prüfungsdauer:	90 Minuten

Es gilt die Prüfungsordnung von EXIN.

Bloom Level

Die Zertifizierung EXIN Artificial Intelligence Compliance Professional testet Kandidatinnen und Kandidaten auf Bloom Level 2, 3 und 4 nach der überarbeiteten Taxonomie von Bloom:

- Bloom Level 2: Verstehen - ein Schritt über das Wissen hinaus. Verstehen zeigt, dass Kandidatinnen und Kandidaten begreifen, was präsentiert wird und bewerten können, wie der Unterrichtsstoff in ihrem eigenen Umfeld angewendet werden kann. Diese Art von Fragen soll zeigen, dass die Kandidatin oder der Kandidat in der Lage ist, die richtige Beschreibung von Fakten und Ideen zu organisieren, zu vergleichen, zu interpretieren und auszuwählen.
- Bloom Level 3: Anwenden – diese Stufe zeigt, dass die Kandidatin oder der Kandidat Inhalte in einem anderen als dem gelernten Kontext anwenden kann. Die Fragen zu dieser Lernstufe sollen zeigen, dass die Kandidatin oder der Kandidat Probleme in neuen Situationen lösen kann, indem sie oder er das erworbene Wissen bzw. die gelernten Tatsachen, Techniken und Regeln auf eine andere oder neue Art anwendet. Die Fragen beschreiben in der Regel ein kurzes Szenario.
- Bloom Level 4: Analysieren – diese Stufe zeigt, dass die Kandidatin oder der Kandidat gelernte Inhalte zum besseren Verständnis in ihre Bestandteile gliedern kann. Diese Lernzielstufe nach Bloom wird in erster Linie mit Hilfe praktischer Aufgabenstellungen geprüft. Praktische Aufgabenstellungen sollen nachweisen, dass die Kandidatin oder der Kandidat Informationen prüfen und in ihre Bestandteile zerlegen kann, indem sie oder er Motive oder Ursachen identifiziert, Schlussfolgerungen trifft und Belege für allgemein gültige Aussagen findet.

Schulung

Präsenzstunden

Für diesen Kurs werden 14 Präsenzstunden empfohlen. Darin enthalten sind praktische Aufgabenstellungen, Prüfungsvorbereitung und kurze Pausen. Nicht enthalten sind: Mittagspausen, Hausaufgaben und die Prüfung.

Regelstudiendauer

112 Stunden (4 ECTS), je nach Vorwissen.

Akkreditierte Trainingsorganisationen

Eine Liste mit unseren akkreditierten akkreditierten Trainingsorganisationen finden Sie unter www.exin.com.

2. Prüfungsanforderungen

Die Prüfungsanforderungen sind im Einzelnen in den Prüfungsspezifikationen erläutert. In der unten dargestellten Tabelle finden Sie eine Liste mit den Themen (Prüfungsanforderungen) und Unterthemen (Prüfungsspezifikationen) des Moduls.

Prüfungsanforderungen	Prüfungsspezifikationen	Gewichtung
1. Kontext der KI-VO		**5%**
	1.1 Zweck und Anwendungsbereich	5%
2. Die KI-VO im Detail		**37,5%**
	2.1 Wesentliche Bestimmungen	15%
	2.2 Risiken und Rechtsvorschriften	10%
	2.3 Konformität (Compliance) und Durchsetzungsverfahren	12,5%
3. Vertrauenswürdige KI		**12,5%**
	3.1 Privatsphäre und Datenschutz	7,5%
	3.2 Transparenz und Rückverfolgbarkeit	5%
4. Ethische KI		**10%**
	4.1 Grundsätze und Leitlinien	5%
	4.2 Menschenrechte	5%
5. Praktische Anwendung der KI-VO		**15%**
	5.1 KI im öffentlichen Sektor	2,5%
	5.2 KI im Privatsektor	12,5%
6. Rahmenwerke zur Unterstützung der Konformität (Compliance)		**20%**
	6.1 Europäische Normen	5%
	6.2 Internationale Normen	15%
	Total	**100%**

Prüfungsspezifikationen

1 Kontext der KI-VO

1.1 Zweck und Anwendungsbereich

Die Kandidatin oder der Kandidat ist in der Lage…

1.1.1 die primären Ziele der KI-VO zu erklären.

1.1.2 den Anwendungsbereich der KI-VO zu erklären.

1.1.3 die verschiedenen in der KI-VO definierten Rollen zu erklären.

2 Die KI-VO im Detail

2.1 Wesentliche Bestimmungen

Die Kandidatin oder der Kandidat ist in der Lage…

2.1.1 ein KI-System in eine der folgenden Kategorien einzuordnen: unannehmbares Risiko, hohes Risiko, begrenztes Risiko, minimales oder kein Risiko.

2.1.2 die Anforderungen an Hochrisiko-KI-Systeme zu erkennen.

2.1.3 die relevante Betriebsführung (Governance) und Aufsicht für KI-Systeme zu erklären.

2.2 Risiken und Rechtsvorschriften

Die Kandidatin oder der Kandidat ist in der Lage…

2.2.1 das Gleichgewicht zwischen Innovationen und Regulierung in der KI-VO zu analysieren.

2.2.2 KI-Systeme mit allgemeinem Verwendungszweck, systemische Risiken und Verhaltenskodizes zu erklären.

2.2.3 die Auswirkungen der KI-VO auf die Rechte des geistigen Eigentums zu erkennen.

2.2.4 die Vor- und Nachteile der Verwendung Open-Source-Modelle (quelloffener Modelle) im Vergleich zu Closed-Source-Modellen im Sinne der KI-VO zu erklären.

2.2.5 die Pflichten von KI-Anbietern zu verstehen: Durchführung von Konformitätsbewertungen, Führen von Dokumentation, Mitteilungen an Aufsichtsbehörden.

2.3 Konformität (Compliance) und Durchsetzungsverfahren

Die Kandidatin oder der Kandidat ist in der Lage…

2.3.1 die Auswirkungen von Verantwortlichkeit und Konformität (Compliance) zu erklären.

2.3.2 das Verfahren für die Meldung von und Reaktion auf Vorfälle zu beschreiben.

2.3.3 die Bedeutung von Hinweisgebern für KI-Systeme zu beschreiben.

2.3.4 die richtigen Sanktionen für die verschiedenen Arten von Nichtkonformität zu benennen: Nichteinhaltung von Verboten, Verstöße gegen Anforderungen an Hochrisiko-KI-Systeme, weniger schwerwiegende Verstöße.

2.3.5 die Pflichten von KI-Nutzern zu verstehen: bestimmungsgemäße Verwendung von KI-Systemen, Überwachung der Leistung des KI-Systems, Meldung von Problemen.

3 Vertrauenswürdige KI

3.1 Privatsphäre und Datenschutz

Die Kandidatin oder der Kandidat ist in der Lage…

3.1.1 zu verstehen, warum Datenmanagement und der Schutz der Privatsphäre wichtig sind.

3.1.2 die Grundsätze der DSGVO in bestimmten Datenschutzszenarien anzuwenden.

3.1.3 die Auswirkungen von Datenminimierung in KI-Systemen zu analysieren.

3.2 Transparenz und Rückverfolgbarkeit

Die Kandidatin oder der Kandidat ist in der Lage…

3.2.1 die Bedeutung von Transparenz in KI-Systemen zu verstehen.

3.2.2 die Rolle von Transparenz in der Förderung des Vertrauens der Öffentlichkeit in KI-Systeme zu verstehen.

3.2.3 die Bedeutung der Rückverfolgbarkeit in KI-Systemen zu erklären.

4 Ethische KI

4.1 Grundsätze und Leitlinien

Die Kandidatin oder der Kandidat ist in der Lage…

4.1.1 die wesentlichen Ethikgrundsätze in der KI-Entwicklung zu identifizieren.

4.1.2 die Leitlinien der KI-VO zum ethischen KI-Einsatz in einem Szenario zu verstehen.

4.2 Menschenrechte

Die Kandidatin oder der Kandidat ist in der Lage…

4.2.1 die Bedeutung der menschlichen Aufsicht in KI-Systemen wie von der KI-VO vorgeschrieben zu verstehen.

4.2.2 die Rechte von KI-Systemen betroffener natürlicher Personen im Sinne der KI-VO mit Hilfe einer Grundrechte-Folgenabschätzung zu erkennen.

5 Praktische Anwendung der KI-VO

5.1 KI im öffentlichen Sektor

Die Kandidatin oder der Kandidat ist in der Lage…

5.1.1 die Risiken der Einführung von KI-Systemen im öffentlichen Raum zu verstehen: öffentliche Entscheidungsfindung, Strafverfolgung, Wahlen.

5.2 KI im Privatsektor

Die Kandidatin oder der Kandidat ist in der Lage…

5.2.1 die Auswirkungen der KI-VO auf verschiedene Interessenträger zu analysieren: Finanz- und Versicherungssektor.

5.2.2 die Auswirkungen der KI-VO auf verschiedene Interessenträger zu analysieren: Gesundheitsversorgung.

5.2.3 die Auswirkungen der KI-VO auf verschiedene Interessenträger zu analysieren: Beschäftigung und Bildung.

5.2.4 die Auswirkungen der KI-VO auf verschiedene Interessenträger zu analysieren: autonomes Fahren.

5.2.5 die Auswirkungen der KI-VO auf verschiedene Interessenträger zu analysieren: Werbung und Tourismus.

6 Rahmenwerke zur Unterstützung der Konformität (Compliance)

6.1 Europäische Normen

Die Kandidatin oder der Kandidat ist in der Lage…

6.1.1 zu verstehen, wie CEN/CLC/TR 18115 Unternehmen dabei unterstützten kann, Daten-Governance-Praktiken umzusetzen, die den Anforderungen von Artikel 10 KI-VO entsprechen.

6.2 Internationale Normen

Die Kandidatin oder der Kandidat ist in der Lage…

6.2.1 zu verstehen, wie die Norm ISO/IEC 42001 und das NIST-Rahmenwerk Unternehmen dabei unterstützen können, verantwortungsvolle Entwicklung und Verwendung von KI sicherzustellen.

6.2.2 zu verstehen, wie die Norm ISO/IEC 23894 Unternehmen dabei unterstützen kann, eigens auf KI abgestimmte Risikomanagementpraktiken in ihre KI-bezogenen Aktivitäten zu integrieren.

6.2.3 ethische Themen im Zusammenhang mit der KI-Entwicklung und -Verwendung auf der Grundlage der Norm ISO/IEC TR 24368 zu verstehen.

3. Liste der Grundbegriffe

Dieses Glossar enthält Begriffe und Abkürzungen, mit denen die Kandidatinnen und Kandidaten vertraut sein sollten.

Bitte beachten Sie, dass die Kenntnis dieser Begriffe alleine nicht ausreicht. Die Kandidatin oder der Kandidat muss diese Begriffe auch verstehen und mit Beispielen belegen können.

Englisch	Deutsch
accountability	Verantwortlichkeit
adaptability	Anpassungsfähigkeit
administrative fine	Geldbuße
AI (artificial intelligence)	KI (künstliche Intelligenz)
AI Act	KI-VO
AI Act objectives	KI-VO-Ziele
AI Act scope	KI-VO-Anwendungsbereich
AI model	KI-Modell
AI Office	Büro für Künstliche Intelligenz
AI practices	Praktiken im KI-Bereich
AI system	KI-System
algorithm	Algorithmus
anonymization	Anonymisierung
audit	Audit
automation	Automatisierung
autonomous driving	autonomes Fahren
bias	Verzerrungen (Bias)/Voreingenommenheit (Bias)
biometric categorization system	System zur biometrischen Kategorisierung
biometric data	biometrische Daten
biometric identification	biometrische Identifizierung
biometric verification	biometrische Verifizierung
closed source	Closed-Source-Software
cloud services	Cloud-Dienste
collecting personal data	Erfassung personenbezogener Daten
common specification	gemeinsame Spezifikation
complaint	Beschwerde
compliance	Konformität (Compliance)
confidentiality	Vertraulichkeit
conformity assessment	Konformitätsbewertung
conformity assessment body	Konformitätsbewertungsstelle
consent	Einwilligung
copyright	Urheberrecht
cybersecurity	Cybersicherheit
data accuracy	Datengenauigkeit/Genauigkeit
data breach	Verletzung des Schutzes personenbezogener Daten
data mapping	Datenmapping
data portability	Datenübertragbarkeit
data protection	Datenschutz
data protection authority (DPA)	Aufsichtsbehörde
data protection by default / privacy by default	datenschutzfreundliche Voreinstellungen / Privatsphäre

data protection by design / privacy by design	Datenschutz durch Technikgestaltung
data protection impact assessment (DPIA)	Datenschutzfolgenabschätzung (DPIA)
data protection officer (DPO)	Datenschutzbeauftragter
data minimization	Datenminimierung
data security	Datensicherheit
data subject	betroffene Person
data transfer	Datenübertragung
documentation obligation	Dokumentationspflicht
e-commerce	E-Commerce
emotion recognition system	Emotionserkennungssystem
enforcement	Durchsetzungsverfahren
ethical principles	Ethikgrundsätze
European Union (EU)	Europäische Union (EU)
European Council	Europäischer Rat
European Artificial Intelligence Board (EAIB)	Europäisches Gremium für Künstliche Intelligenz (KI-Gremium)
European Data Protection Board (EDPB)	Europäische Datenschutzausschuss (EDPB)
European Data Protection Supervisor (EDPS)	Europäischer Datenschutzbeauftragter
European Economic Area (EEA)	Europäischer Wirtschaftsraum (EWR)
fair use	angemessene Verwendung (Fair Use)
fairness	Fairness
financial penalty	finanzielle Maßnahme
formal warning	formelle Verwarnung
General Data Protection Regulation (GDPR)	Datenschutz-Grundverordnung (DSGVO)
general-purpose AI (GPAI)	KI-System mit allgemeinem Verwendungszweck
governing body	leitende Stelle
harmonized standard	harmonisierte Normen
high-risk AI system	Hochrisiko-KI-System
human oversight	menschliche Aufsicht
incident response	Notfallmanagement, Reaktion auf Vorfälle
input data	Eingabedaten
instructions for use	Betriebsanleitungen
intellectual property (IP)	geistiges Eigentum
intended purpose	Zweckbestimmung
international organizations	internationale Organisationen
law enforcement authority	Strafverfolgungsbehörde
lawfulness	Rechtmäßigkeit
legislation	Rechtsvorschriften
liability	Haftung
limited-risk AI system	KI-System mit begrenztem Risiko
making available on the market	Bereitstellung auf dem Markt
market surveillance authority (MSA)	Marktüberwachungsbehörde
minimal or no-risk AI system	KI-System mit minimalem oder keinem Risiko
national competent authority	zuständige nationale Behörde
open source	Open-Source (quelloffen)
oversight	Aufsicht
performance of an AI system	Leistung eines KI-Systems
personal data	personenbezogene Daten
placing on the market	Inverkehrbringen
post-market monitoring system	System zur Beobachtung nach dem Inverkehrbringen
privacy	Privatsphäre
privacy officer	Datenschutzbeauftragter

product safety	Produktsicherheit
processing (of personal data)	Verarbeitung (von personenbezogenen Daten)
processing agreement	Vertrag zur Datenverarbeitung
processor	Auftragsverarbeiter
profiling	Profiling
prohibited AI systems	verbotene KI-Systeme
pseudonymization	Pseudonymisierung
publicly accessible space	öffentlich zugänglicher Raum
putting into service	Inbetriebnahme
quality cycle	Qualitätszyklus
quality management system	Qualitätsmanagementsystem
reasonably foreseeable misuse	vernünftigerweise vorhersehbare Fehlanwendung
recall of an AI system	Rückruf eines KI-Systems
recipient	Empfänger
regulatory sandbox	Reallabor
relevant national authority	zuständige nationale Behörde
reliability	Zuverlässlichkeit
remote biometric identification system	biometrisches Fernidentifizierungssystem
rights of the data subject • 'right to be forgotten' • automated individual decision-making • data portability • information and access • modalities • notification obligation • rectification and erasure • restriction of processing • right to compensation • right to objection • transparency	Rechte der betroffenen Person • Recht auf Vergessenwerden • automatisierte Entscheidungsfindung im Einzelfall • Datenübertragbarkeit • Informationspflicht und Recht auf Auskunft • Modalitäten • Mitteilungspflicht • Berichtigung und Löschung • Einschränkung der Verarbeitung • Recht auf Schadenersatz • Widerspruchsrecht • Transparenz
risk	Risiko
risk management	Risikomanagement
risk mitigations	Risikominderungen
roles • authorized representative • deployer • distributor • importer • operator • provider • user	Rolle • Bevollmächtigter • Betreiber • Händler • Einführer • Akteur • Anbieter • Nutzer
rules of procedure	Geschäftsordnung
safety component	Sicherheitsbauteil
safety of an AI-system	Sicherheit eines AI-Systems
scalability	Skalierbarkeit
security breach	Sicherheitsverstoß
(security) incident	Sicherheitsvorfall
sensitive operational data	sensible operative Daten
service provider	Service Provider
small and medium enterprises (SMEs)	kleine und mittlere Unternehmen (KMU)
social scoring	soziale Bewertung

special categories of personal data	besondere Kategorien personenbezogener Daten
stakeholder	Interessenträger
startup	Start-up-Unternehmen
storage limitation	Zweckbindung
subliminal manipulation	unterschwellige Manipulation
substantial modification	wesentliche Veränderung
systemic risk	systemisches Risiko
territorial scope	räumlicher Anwendungsbereich
testing data	Testdaten
third party	Dritter
threat	Bedrohung
traceability	Rückverfolgbarkeit
training data	Trainingsdaten
transparency	Transparenz
trust	Vertrauen
unacceptable risk	unannehmbares Risiko
validation data	Validierungsdaten
vulnerability	Schwachstelle/Sicherheitslücke
whistleblower	Hinweisgeber
withdrawal of an AI system	Rücknahme eines KI-Systems

4. Literatur

Prüfungsliteratur

Das für die Prüfung benötigte Wissen wird durch folgende Literatur abgedeckt:

A. Natascha Windholz et al.
Praxishandbuch KI-VO: Künstliche Intelligenz rechtskonform im privaten und öffentlichen Bereich einsetzen
Carl Hanser Verlag GmbH & Co. KG (2025)
ISBN: 9783446481947 (hardcopy)
ISBN: 9783446481978 (eBook)
ISBN: 9783446483606 (ePub)

B. EXIN
Examenliteratur AI Compliance Professional
EXIN (2025)
Dieses Material wird von Ihrer akkreditierten Trainingsorganisation bereitgestellt.

Weiterführende Literatur

C. Europäische Union
Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Verordnung über künstliche Intelligenz)
Europäische Union (2024)
https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Anmerkung

Weiterführende Literatur dient nur als Referenz und zur Vertiefung des Wissens.

Der Text der KI-Verordnug (Quelle C) ist keine Prüfungsliteratur, da die Prüfungsliteratur ausreichende Kenntnisse über die KI-Verordnung vermittelt. Kandidatinnen und Kandidaten sollten mit den Verweisen auf die KI-Verordnung in der übrigen Literatur vertraut sein.

Literaturmatrix

Prüfungsanforderungen	Prüfungsspezifikationen	Literaturverweis	KI-VO-Verweis
1. Kontext der KI-VO			
	1.1 Zweck und Anwendungsbereich	A, Kapitel 3	Artikel 1, Artikel 2, Artikel 3
2. Die KI-VO im Detail			
	2.1 Wesentliche Bestimmungen	A, Kapitel 3	Artikel 6, Erwägungsgrund 46, Artikel 9, Erwägungsgrund 65, Artikel 10, Erwägungsgrund 70
	2.2 Risiken und Rechtsvorschriften	A, Kapitel 3, Kapitel 5, Kapitel 6	Artikel 2, Artikel 5, Erwägungsgrund 139 Artikel 51, Artikel 65 Artikel 78, Erwägungsgrund 48
	2.3 Konformität (Compliance) und Durchsetzungsverfahren	A, Kapitel 3, Kapitel 7, Kapitel 10	Artikel 6, Erwägungsgrund 47 Artikel 23, Erwägungsgrund 56 Artikel 60, Erwägungsgrund 60 Artikel 62, Erwägungsgrund 60 Artikel 71, Erwägungsgrund 60
3. Vertrauenswürdige KI			
	3.1 Privatsphäre und Datenschutz	A, Kapitel 4	Artikel 2, Erwägungsgrund 10 Artikel 10, Erwägungsgrund 29, Erwägungsgrund 43
	3.2 Transparenz und Rückverfolgbarkeit	A, Kapitel 2, Kapitel 3	Artikel 13, Erwägungsgrund 42 Artikel 14, Erwägungsgrund 44
4. Ethische KI			
	4.1 Grundsätze und Leitlinien	A, Kapitel 7, Kapitel 9	Artikel 9, Erwägungsgrund 14 Artikel 10, Erwägungsgrund 68
	4.2 Menschenrechte	A, Kapitel 9, Kapitel 10	Artikel 10, Erwägungsgrund 68 Artikel 14, Erwägungsgrund 50
5. Praktische Anwendung der KI-VO			
	5.1 KI im öffentlichen Sektor	A, Kapitel 8	Artikel 5, Erwägungsgrund 53
	5.2 KI im Privatsektor	A, Kapitel 7	Erwägungsgrund 63 Erwägungsgrund 64 Erwägungsgrund 65 Erwägungsgrund 66 Erwägungsgrund 67
6. Rahmenwerke zur Unterstützung der Konformität (Compliance)			
	6.1 Europäische Normen	B, Kapitel 1	Artikel 10
	6.2 Internationale Normen	B, Kapitel 2, Kapitel 3, Kapitel 4	Artikel 8 Artikel 9

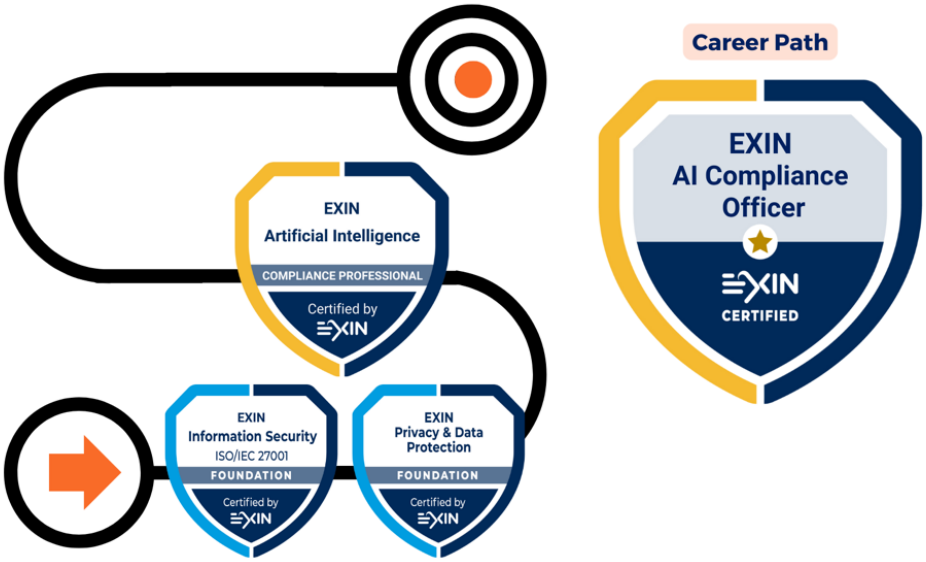
5. Karrierepfad

EXIN glaubt an den Wert des lebenslangen Lernens und an die Bedeutung, unterschiedliche Fähigkeiten zu kombinieren, um in der heutigen dynamischen und sich entwickelnden Welt erfolgreich zu sein. Mit unseren EXIN-Karrierepfade können Kandidatinnen und Kandidaten sich auf bestimmte Jobrollen vorbereiten und ihre berufliche Reise weiterhin ausbauen und vorantreiben. Weitere Informationen zu den EXIN-Karrierepfade finden Sie auf unserer Website unter https://www.exin.com/career-paths/.

Die Zertifizierung EXIN Artificial Intelligence Compliance Professional ist Teil des folgendes EXIN-Karrierepfads.

EXIN Artificial Intelligence Compliance Officer

EXIN Artificial Intelligence Compliance Officer bereitet Fachkräfte darauf vor, die relevantesten Vorschriften im Bereich künstliche Intelligenz (KI) und Datenschutz sowie robuste Informationssicherheitsstandards einzuhalten, um eine ethische und verantwortungsvolle Nutzung von KI sicherzustellen.



Certified for what's next

Kontakt EXIN

www.exin.com