Curriculum für die AIO Inhouse-Schulung

Mit Praxisteil

Agentische KI-Governance

Curriculum für die AIO Inhouse-Schulung

Inhaltsverzeichnis

1 Geltungsbereich 4
2 Anforderungen an die Kompetenz 4
2.1 Kompetenz- & Tätigkeitsprofil 4
2.2 Anforderungen an Wissen und Fertigkeiten 4
2.2.1 Technische Grundlagen der KI 4
2.2.2 Rechtliche Grundlagen der KI 5
2.2.3 Organisationale Aspekte der KI 5
2.2.4 Agentische KI-Governance (Praxisteil) 5
3 Prüfung 6
3.1 Vorgespräch und Anpassung 6
3.2 Inhouse-Schulung und Lernplattform 6
3.3 Praxisteil „Agentic Governance Lab“ 6
3.4 Abschlussprüfung 7
4 Bewertungskriterien 7
4.1 Multiple-Choice-Teil 7
4.2 Fallprüfung 8
4.3 Gesamtbewertung und Prüfungswiederholung 8
5 Zertifizierungsvoraussetzungen Erst-Zertifizierung 8
6 Beschwerde, Einspruch, Prüfungseinsicht/-auskunft 8
7 Rezertifizierung 9
7.1 Kriterien zur Verlängerung des Zertifikats 9
7.2 Ausstellung des Zertifikats 9
7.3 Fristen 9
8 Prüfer*innen 10
8.1 Anzahl Prüfer*innen 10
8.2 Kompetenz der Prüfer*innen 10
Anlage: Aufbau der Inhouse-Schulung 11

1 Geltungsbereich

Dieses Curriculum legt die Vorgehensweise zur Zertifizierung der KI-Kompetenz gem. Art. 4 sowie Art. 3 Nr. 56, 14 KI-VO unter Berücksichtigung der Erwägungsgründe 20, 91 der KI-Verordnung von Personen im Rahmen der AIO Inhouse-Schulung fest. Die Inhouse-Schulung vermittelt grundlegende Kenntnisse in den Bereichen Technik, Recht und Organisation im Zusammenhang mit KI und wird im Vorgespräch auf die Ziele und drei konkrete Anwendungsfälle der jeweiligen Organisation zugeschnitten. Sie findet vor Ort, online oder hybrid statt und umfasst regulär zwei Tage; der Umfang kann individuell angepasst werden.

Die Schulung umfasst zudem einen Praxisteil „Agentische KI-Governance“ im Umfang von rund einem Drittel der Schulung. Die Teilnehmenden werden befähigt, das KI-Governance-System ihrer Organisation mithilfe von KI-Agenten aufzubauen, zu steuern und zu verantworten: Sie zerlegen Prüf- und Freigabeprozesse in Stufen, übertragen wiederkehrende Arbeitsschritte auf Agenten und legen fest, an welchen Stellen der Mensch entscheidet (Gates). Der Praxisteil ist auf die konkrete Umsetzung in der Organisation ausgerichtet; er ist Bestandteil der Schulungsleistung, nicht jedoch der Prüfung.

Die Zertifizierung orientiert sich an den Anforderungen der ISO/IEC 17024. Für den Praxisteil werden ergänzend die Anforderungen an ein KI-Managementsystem nach ISO/IEC 42001 und an die menschliche Aufsicht nach Art. 14 KI-VO zugrunde gelegt. Maßgeblich ist die KI-Verordnung in ihrer jeweils geltenden Fassung. Nach bestandener Abschlussprüfung erhalten die Teilnehmenden das AIO-Zertifikat über die KI-Kompetenz nach Art. 4, 3 Nr. 56 KI-VO, das in Zusammenarbeit mit dem IAL – Institute for AI Literacy ausgestellt wird. Der Aufbau der Inhouse-Schulung ist in der Anlage dargestellt.

2 Anforderungen an die Kompetenz

2.1 Kompetenz- & Tätigkeitsprofil

Zertifizierte Personen verfügen über ein grundlegendes Verständnis für technische, rechtliche und organisatorische Aspekte der Nutzung von KI-Technologien, einschließlich KI-Systemen und KI-Modellen, im Unternehmenskontext gemäß Art. 4 KI-VO. Sie sind in der Lage, die erforderliche KI-Kompetenz innerhalb eines Unternehmens zu definieren und organisatorisch sicherzustellen.

Darüber hinaus werden die Teilnehmenden befähigt, die Abläufe des KI-Governance-Systems ihrer Organisation – von der Erfassung eines KI-Anwendungsfalls über die Prüfung bis zur Freigabe und Dokumentation – agentisch zu unterstützen. Sie gestalten KI-Agenten, definieren menschliche Entscheidungspunkte (Gates) und stellen sicher, dass jede Entscheidung nachvollziehbar dokumentiert und von einem Menschen verantwortet wird.

Rolle im Unternehmen	Kernaufgabe
KI-Kompetenzträger*in	definiert die erforderliche KI-Kompetenz, schult und sensibilisiert (Art. 4 KI-VO)
Prüfer*in und Berater*in	ordnet KI-Systeme ein, bewertet Risiken und leitet Maßnahmen ab
AI Solution Engineer	baut und steuert agentische Prüfketten, definiert Gates, führt das KI-Register

2.2 Anforderungen an Wissen und Fertigkeiten

2.2.1 Technische Grundlagen der KI

Zertifizierte Personen:

- kennen die technischen Grundlagen sowie Funktionsweisen von KI.
- kennen die grundlegenden Grenzen und Herausforderungen von KI.
- verstehen die Funktionsweise von KI-Anwendungen und können mit diesen arbeiten.
- kennen die Funktionsweise großer Sprachmodelle und von KI-Agenten (Anweisungen, Werkzeugnutzung, Wissensquellen, Übergaben zwischen Agenten).
- kennen typische Fehlerbilder generativer und agentischer Systeme – etwa erfundene Angaben, schwankende Ergebnisse oder abgebrochene Abläufe – und wissen, wie ihnen zu begegnen ist.

- kennen Aufbau und Architektur von KI-Agentensystemen, deren Werkzeuge und Schnittstellen sowie die Anforderungen an Sicherheit, Zugriffsrechte und menschliche Kontrolle, und können die in der eigenen Organisation eingesetzten KI-Systeme technisch einordnen.

2.2.2 Rechtliche Grundlagen der KI

Zertifizierte Personen:

- kennen die relevanten Gesetze und Bestimmungen in Bezug auf den Einsatz von KI: KI-Verordnung, KI-Haftungsrecht, Datenschutzrecht, Urheberrecht.
- können rechtliche Risiken im Zusammenhang mit dem Einsatz von KI aufzeigen und bewerten.
- kennen die regulatorischen Pflichtenkataloge im Bereich KI-Verordnung.
- kennen die Anforderungen an die menschliche Aufsicht (Art. 14 KI-VO) und die Pflichten der Betreiber (Art. 26 KI-VO) und können sie auf den Einsatz von KI-Agenten in der eigenen Governance übertragen.
- kennen die Risikoklassen und die Pflichten nach Rolle gemäß KI-Verordnung, die Pflicht zur KI-Kompetenz nach Art. 4 KI-VO sowie die Anforderungen an einen datenschutzkonformen Einsatz von KI.

2.2.3 Organisationale Aspekte der KI

Zertifizierte Personen:

- kennen die Anforderungen an die KI-Kompetenz gemäß NIST, OECD, ISO und KI-VO.
- kennen die Organisationsstruktur eines KI-Managementsystems.
- verstehen die Rolle von KI-Kompetenzträger*innen: Definition, Aufgaben, Rolle.
- können ein KI-Register führen und darin Zuständigkeiten, Freigaben und Nachweise abbilden.
- kennen die Grundzüge der Entwicklung einer KI-Leitlinie und KI-Richtlinie für die eigene Organisation.
- können Kosten und Nutzen von KI-Projekten bewerten, Use Cases priorisieren und Make-or-Buy-Entscheidungen vorbereiten (KI-Betriebswirtschaft).

2.2.4 Agentische KI-Governance (Praxisteil)

Die Teilnehmenden:

- können einen Governance-Ablauf, etwa Erfassung, Sachverhalt, Vorprüfung, Risikoprüfung und Freigabe, in klar abgegrenzte Stufen zerlegen und für jede Stufe Eingang, Ergebnis und Qualitätskriterien festlegen.
- können KI-Agenten mit eindeutigen Aufträgen, Regeln und Vorlagen konfigurieren und Aufgaben sinnvoll zwischen Haupt- und Subagenten aufteilen.
- können menschliche Gates definieren: wer welches Ergebnis wann abnimmt, was ein Agent nicht entscheiden darf und welche Schritte erst nach Freigabe erfolgen (z. B. Versand, Einstufung, Registrierung).
- können strukturierte Ergebnisdokumente vorgeben, etwa einen dokumentierten Prüfbericht, und ihre Übernahme in ein KI-Register mit einfachen Mitteln (Tabelle, No-Code-App, Skript) automatisieren.
- können Ergebnisse von Agenten anhand von Testfällen und Sollwerten überprüfen, Abweichungen erkennen und die Regeln versioniert nachschärfen.
- kennen die Anforderungen an Datenschutz, Informationssicherheit und Nachvollziehbarkeit beim Einsatz von Agenten in der Governance selbst (Zugriffsrechte, Postfächer, Protokollierung, Testdaten).

3 Prüfung

Das Verfahren besteht aus vier Abschnitten: dem Vorgespräch mit Anpassung der Schulung, der Inhouse-Schulung mit anschließendem Zugang zur Lernplattform, dem Praxisteil „Agentic Governance Lab“ und der digitalen Abschlussprüfung. Der Praxisteil ist Bestandteil der Schulung, fließt jedoch nicht in die Prüfung ein. Die Prüfung ist auf die Schwerpunkte und Anwendungsfälle der Organisation abgestimmt und stellt sicher, dass die Anforderung der kontextbezogenen KI-Kompetenz nach Art. 4 KI-VO erfüllt werden kann.

3.1 Vorgespräch und Anpassung

Vor der Schulung findet ein Vorgespräch mit der Organisation statt. Darin werden Ziele und Erwartungen, der Kreis der Teilnehmenden, Format und Umfang sowie drei konkrete Anwendungsfälle aus der Organisation festgelegt. Zudem werden die bestehenden Prüfprozesse für den KI-Einsatz erfasst und der Stand der KI-Governance im Rahmen einer Gap-Analyse ermittelt; dabei wird berücksichtigt, ob in der Organisation bereits andere Managementsysteme etabliert sind, auf denen aufgebaut werden kann. Auf dieser Grundlage werden Inhalte, Schwerpunkte und Referent*innen der Schulung, der Praxisteil sowie der personalisierte Teil der Abschlussprüfung angepasst.

3.2 Inhouse-Schulung und Lernplattform

Die Schulung findet in der Organisation vor Ort, online als Webinar oder hybrid statt und umfasst regulär zwei Tage. Am ersten Tag stehen Technik und Recht der KI an den Anwendungsfällen der Organisation im Mittelpunkt, am zweiten Tag KI-Governance und die Automatisierung der internen Prüfprozesse. Inhaltlich gliedert sich die Schulung in sechs Themenfelder: Technik, KI-Agentensysteme, Recht, Organisation, KI-Betriebswirtschaft und agentische KI-Governance. Die Teilnehmenden erhalten fundiertes Wissen zur Funktionsweise und zu den Grenzen von KI-Systemen, zu Aufbau und sicherem Betrieb von KI-Agentensystemen sowie zur KI-Verordnung einschließlich Risikoklassen, Rollen und Pflichten und zum datenschutzkonformen Einsatz von KI. Darüber hinaus werden KI-Governance und KI-Management, die Entwicklung einer KI-Leitlinie und KI-Richtlinie, Rollen und Verantwortlichkeiten, Dokumentation und Nachweise sowie die wirtschaftliche Bewertung und Priorisierung von KI-Projekten behandelt. Alle Inhalte werden auf die im Vorgespräch ausgewählten Anwendungsfälle übertragen. Folien, Checklisten und Übersichten erhalten die Teilnehmenden für den Arbeitsalltag.

Im Anschluss an die Schulung erhalten alle Teilnehmenden Zugang zur Lernplattform. Dort stehen weiterführende Inhalte zu Technik, Recht und Organisation der KI sowie die digitale Abschlussprüfung zur Verfügung.

3.3 Praxisteil „Agentic Governance Lab“

Der Praxisteil umfasst rund ein Drittel der Schulung. Er beginnt am zweiten Schulungstag und kann im Rahmen der Begleitung beim Aufbau der KI-Governance in der Organisation fortgesetzt werden. Die Teilnehmenden bauen darin Schritt für Schritt eine agentische Prüfkette für die im Vorgespräch ausgewählten Anwendungsfälle der eigenen Organisation. Gearbeitet wird mit den Bordmitteln, die in der Organisation bereits vorhanden sind, ergänzt um gängige Agenten-Plattformen sowie Tabellen- und No-Code-Werkzeuge; entscheidend ist die übertragbare Methode, nicht ein bestimmtes Produkt. Ziel ist eine in der Organisation tatsächlich nutzbare Prüfkette, mit der neue Use Cases teilautomatisiert geprüft werden und die mit den KI-Projekten der Organisation mitwächst. Der Praxisteil ist Bestandteil der Schulungsleistung, nicht jedoch der Abschlussprüfung.

Der Praxisteil gliedert sich in fünf aufeinander aufbauende Bausteine:

Baustein	Inhalt	Ergebnis
L1 Prozess zerlegen	Governance-Ablauf in Stufen schneiden, Rollen, Eingänge und Übergaben festlegen	Stufenplan
L2 Agenten gestalten	Aufträge, Regeln, Vorlagen und Wissensquellen für Haupt- und Subagenten formulieren	Agentenbeschreibung
L3 Gates definieren	menschliche Abnahmepunkte, Freigaberechte und Grenzen der Agenten festlegen	Gate-Matrix
L4 Dokumentieren und registrieren	dokumentierten Prüfbericht erzeugen und das Ergebnis strukturiert in das KI-Register übernehmen	Prüfbericht, Registereintrag
L5 Testen und nachschärfen	Testfälle und Sollwerte anlegen, Fehlerbilder erkennen, Regeln versioniert verbessern	Testprotokoll

3.4 Abschlussprüfung

Die Abschlussprüfung wird digital über die Lernplattform abgelegt und kann innerhalb von 12 Monaten nach der Schulung absolviert werden. Sie besteht aus zwei Teilen:

1. **Multiple-Choice-Teil**
   Der erste Teil prüft das Grundlagenverständnis der Teilnehmenden in den unter 2.2.1 bis 2.2.3 genannten Kategorien anhand von Multiple-Choice-Fragen. 12 der 25 Multiple-Choice-Fragen werden auf die Schwerpunkte und Anwendungsfälle der Organisation abgestimmt, die im Vorgespräch festgelegt wurden.
2. **Fallprüfung**
   Der zweite Teil besteht aus einer Fallprüfung, in der die teilnehmende Person einen praxisnahen Sachverhalt erhält, der sich an den im Vorgespräch ausgewählten Anwendungsfällen der Organisation orientiert. In dieser Prüfung muss die teilnehmende Person den Sachverhalt im Rahmen der KI-Verordnung eigenständig analysieren und die Bereiche sachlicher, persönlicher und räumlicher Anwendungsbereich sowie Risiko- und Maßnahmenbestimmung bewerten. Dabei legt sie auch dar, an welchen Stellen der Prüfung eine menschliche Entscheidung erforderlich ist. Zudem wird die teilnehmende Person am Ende in einem kurzen Aufsatz eine vertiefte Antwort zu einer spezifischen Frage geben.

Die maximale Dauer von Multiple-Choice-Teil und Fallprüfung ist auf 60 Minuten festgelegt.

4 Bewertungskriterien

4.1 Multiple-Choice-Teil

Der Multiple-Choice-Teil umfasst insgesamt 25 Fragen. Die Fragen werden je nach Schwierigkeitsgrad mit 1 bis 3 Punkten bewertet. Nicht beantwortete oder falsch beantwortete Fragen werden mit 0 Punkten bewertet.

Die Bewertung erfolgt wie folgt:

- **Fachliche Richtigkeit:** Alle korrekten Antwortmöglichkeiten müssen ausgewählt werden, um die Punkte der Aufgabe zu erhalten. Abweichungen von der Musterlösung führen zu null Punkten für diese Aufgabe.
- **Anpassung an individuelle Schwerpunkte:** 12 der 25 Fragen sind auf die im Vorgespräch festgelegten Schwerpunkte und Anwendungsfälle der Organisation abgestimmt und prüfen vertieftes Wissen in diesen Bereichen.

4.2 Fallprüfung

Die Fallprüfung wird insgesamt mit 15 Punkten bewertet und setzt sich aus den folgenden Bewertungsaspekten zusammen:

- **Analyse des Sachverhalts im Rahmen der KI-Verordnung (5 Punkte):**
  - **Sachlicher Anwendungsbereich:** Verständnis und korrekte Bestimmung des sachlichen Anwendungsbereichs der KI-Verordnung im Kontext des Falles.
  - **Persönlicher Anwendungsbereich:** Identifikation der relevanten Akteure und deren Pflichten gemäß der KI-Verordnung.
  - **Räumlicher Anwendungsbereich:** Bewertung, ob und wie die KI-Verordnung auf den gegebenen Fall anwendbar ist.
  - **Risikobewertung des KI-Systems:** Einstufung des KI-Systems in die richtige Risikokategorie (z. B. geringes oder hohes Risiko) gemäß der KI-Verordnung.
  - **Bestimmung erforderlicher Maßnahmen:** Vorschlag angemessener Maßnahmen und Pflichten zur Einhaltung der KI-Verordnung, einschließlich der erforderlichen menschlichen Entscheidungspunkte.
- **Vertiefte Antwort/Aufsatz (10 Punkte):**
  - **Inhaltliche Tiefe und Relevanz:** Ausführliche und fundierte Auseinandersetzung mit der spezifischen Fragestellung (5 Punkte).
  - **Anwendung von Fachwissen:** Einbindung relevanter technischer, rechtlicher und organisatorischer Aspekte (3 Punkte).
  - **Argumentationsstruktur und Klarheit:** Logischer Aufbau und klare Darstellung der Argumente (2 Punkte).

4.3 Gesamtbewertung und Prüfungswiederholung

Zur positiven Absolvierung der Gesamtprüfung müssen mindestens 50 % der Gesamtpunktzahl erreicht werden. Bei Nichtbestehen ist die Prüfung in vollem Umfang zu wiederholen. Es stehen insgesamt drei Versuche innerhalb von 12 Monaten nach der Schulung zur Verfügung.

Diese Bewertungskriterien basieren auf den Anforderungen der kontextbezogenen KI-Kompetenz nach Art. 4 KI-Verordnung. Sie gewährleisten, dass die Teilnehmenden über die notwendigen Kenntnisse und Fähigkeiten verfügen, um fundierte Entscheidungen im Umgang mit KI-Systemen zu treffen, die relevanten technischen, rechtlichen und organisatorischen Aspekte angemessen zu berücksichtigen und KI-gestützte Governance-Prozesse verantwortungsvoll zu gestalten.

5 Zertifizierungsvoraussetzungen Erst-Zertifizierung

Folgende Voraussetzungen müssen für die Ausstellung eines Zertifikats erfüllt sein:

- Teilnahme an der Inhouse-Schulung (vor Ort, online oder hybrid)
- Positives Ergebnis der digitalen Abschlussprüfung gemäß Abschnitt 4 Bewertungskriterien innerhalb von 12 Monaten nach der Schulung

Ausgestellt wird das AIO-Zertifikat über die KI-Kompetenz nach Art. 4, 3 Nr. 56 KI-VO in Zusammenarbeit mit dem IAL – Institute for AI Literacy. Die Zertifikate haben eine Gültigkeit von zwei Jahren.

6 Beschwerde, Einspruch, Prüfungseinsicht/-auskunft

Teilnehmende haben das Recht, Einspruch gegen das Prüfungsergebnis einzulegen oder Beschwerde bei der Zertifizierungsstelle einzureichen. Beschwerden und Einsprüche sind schriftlich bei der Zertifizierungsstelle einzureichen. Eine Prüfungseinsicht sowie eine Prüfungsauskunft (erreichte Punkteanzahl) kann ausschließlich bei Nichtbestehen der Prüfung und im Rahmen eines Einspruchsverfahrens vorgenommen/erteilt werden.

7 Rezertifizierung

7.1 Kriterien zur Verlängerung des Zertifikats

Zur Verlängerung des Zertifikats muss die zertifizierte Person folgende Kriterien erfüllen:

- Nachweis über facheinschlägige, durch das IAL – Institute for AI Literacy anerkannte Weiterbildungen im Ausmaß von mindestens 8 Stunden für den gesamten Zertifizierungszyklus, davon mindestens 2 Stunden zu agentischen Werkzeugen und Methoden der KI-Governance, da sich diese besonders schnell weiterentwickeln.

7.2 Ausstellung des Zertifikats

Nach Erfüllung aller Kriterien gemäß Abschnitt 7.1 wird das Zertifikat für zwei Jahre verlängert.

7.3 Fristen

Die Rezertifizierung muss vor dem Ablauf des Zertifikats erfolgen. In Ausnahmefällen kann die Rezertifizierung auch nach Ablauf des Zertifikats erfolgen. Erfolgt die Rezertifizierung nach Ablauf der Gültigkeit innerhalb eines Zeitraums von maximal sechs Monaten, wird die Rezertifizierung gemäß den Kriterien und dem Prozess gemäß Abschnitt 7.1 durchgeführt. Andernfalls ist eine Prüfung im Umfang der Erstzertifizierung gemäß Abschnitt 3 durchzuführen.

8 Prüfer*innen

8.1 Anzahl Prüfer*innen

Die Prüfung wird von mindestens zwei Prüfer*innen abgehalten und bewertet.

8.2 Kompetenz der Prüfer*innen

Die Prüfer*innen müssen die Anforderungen erfüllen, die auf den anzuwendenden Kompetenznormen und anderen relevanten Dokumenten basieren. Sie müssen mit diesem Zertifizierungsschema vertraut sein, umfassende Kenntnis über die relevanten Prüfungsmethoden und Prüfungsdokumente haben, über eine angemessene Kompetenz in dem zu prüfenden Gebiet verfügen, flüssig in der schriftlichen und mündlichen Prüfungssprache kommunizieren können und frei von allen Einflüssen sein, um unparteiische und nichtdiskriminierende Beurteilungen erstellen zu können.

Anlage: Aufbau der Inhouse-Schulung

Die folgende Übersicht zeigt die Verteilung der Inhalte auf die Teile der Inhouse-Schulung. Der Praxisteil wird am zweiten Schulungstag an den Anwendungsfällen der Organisation begonnen und kann im Rahmen der Begleitung beim Aufbau in der Organisation umgesetzt werden. Er ist nicht Bestandteil der Abschlussprüfung.

Schulungsteil	Wissen und Einordnung (Technik, Recht, Organisation)	Praxisteil Agentische KI-Governance
Vorgespräch & Anpassung	Ziele, Schwerpunkte, Kreis der Teilnehmenden, Format und Umfang	Auswahl von drei Use Cases, bestehende Prüfprozesse, Gap-Analyse
Schulung Tag 1	Technik und Recht der KI an den eigenen Anwendungsfällen	Einführung: vom Prüfschema zur Prüfkette
Schulung Tag 2	KI-Governance und -Management, KI-Betriebswirtschaft	Agentic Governance Lab: Bausteine L1 bis L3 an den eigenen Use Cases
Lernplattform	Weiterführende Inhalte zu Technik, Recht und Organisation	Folien, Checklisten und Übersichten für den Arbeitsalltag
Begleitung beim Aufbau (optional)	Umsetzung der Gap-Analyse, Aufbau des KI-Managementsystems	Bausteine L4 und L5, Umsetzung der Prüfkette in der Organisation
Digitale Abschlussprüfung	Multiple Choice, Fallprüfung (60 Minuten, innerhalb von 12 Monaten)	nicht Bestandteil der Prüfung
Anteil an der Schulung	**rund zwei Drittel**	**rund ein Drittel**

Ergebnisse des Praxisteils

- **Stufenplan:** Stufen der Prüfkette mit Eingängen und Ergebnissen je Stufe
- **Agentenbeschreibung:** Zuordnung der Arbeitsschritte zu den Agenten einschließlich Aufträgen, Regeln und Vorlagen
- **Gate-Matrix:** menschliche Abnahmepunkte, Freigaberechte und Entscheidungen, die keinem Agenten übertragen werden
- **Prüfbericht und Registereintrag:** Dokumentation des Prüfergebnisses und Übernahme in das KI-Register
- **Testprotokoll:** Testfälle und Sollwerte zur Qualitätssicherung der Agenten sowie deren Ergebnisse