Komplettes KI-Compliance Starterpaket

nach der KI-Verordnung

Kurzversion 1.1 vom 29.01.2026
Hilfsmittel im Studiengang Menschliche Aufsicht (L1)

Praktische Relevanz	●●●●●
Technische Relevanz	●●○○○
Rechtliche Relevanz	●●●●●
Orga. Relevanz	●●●●○

Inhaltsverzeichnis

1. KI-Use Case Fragebogen (Kommentierte Fassung) 3
2. Prüfungsschema KI-Technologie nach der KI-Verordnung 7
3. Checkliste KI-System nach der KI-Verordnung 17
4. Dokumentierter Prüfbericht (Kurzfassung) 22

Anlage
1. Operative Umsetzung der Betreiberpflichten
   a. Pflichten bei Hochrisiko KI-Systemen
   b. Pflichten bei KI-Systemen mit geringem Risiko
2. Auslegungshilfen
   1. Autonomiegrad nach Art. 3 (1) KI-VO
   2. Wesentliche Änderung nach Art. 25 (1) b.) KI-VO
   3. Finetuning i.R.d. wesentlichen Änderung nach Art. 25 (1) b.) KI-VO
   4. Freie und quelloffene KI-Technologie i.S.d Art. 2 Abs. 12 KI-VO, Art. 52 Abs. 2 KI-VO, ErwGr 102, 103

KI-Use Case Fragebogen
Kommentierte Fassung (Version 1.0)

0. Automatische Vorbefüllung (ohne Fragen)
(Diese Informationen werden aus Unternehmens-internen Systemen und Herstellerangaben gezogen, bevor die erste Frage gestellt wird)

0.1 Fachbereich des Service Owners
- Automatische Zuordnung zu typischen Verarbeitungsprozessen
- Vorschaltung eines typischen Anwendungsszenarios (HR = Recruiting/Performance; Kundenservice = Routing/Priorisierung; Sales = Lead-Qualifizierung usw.)

0.2 Herstellerangaben gemäß Art. 3 Nr. 12 KI-VO
- Zweck
- Kontextspezifikation
- Typische Einsatzbedingungen
  → Wird als Hersteller-Anwendungsszenario vorbefüllt

0.3 Objektive Umstände des KI-Systems
- Typ (Generativ, Klassifikation, Prognose, Empfehlung, Entscheidungslogik usw.)
- Interaktionstyp (Chatbot, API-Modell, Scoring, Vision etc.)

→ Liefert automatisch: erste Einschätzung Modifikationsrisiko + Menschkontakt + Decision Impact

1. Stammdaten & Verantwortlichkeiten

Rolle	Name / Funktion	Organisationseinheit
Service Owner		
Fachlich verantwortlich		
Technisch verantwortlich		
Fachabteilung		

2. KI-Beschaffung

Wer hat die KI-Technologie entwickelt oder bereitgestellt?
(Genau ein Szenario ankreuzen)

☐ Die KI wird im eigenen Unternehmen entwickelt.
Kommentar: Eröffnung des Anbieterfragebogens

☐ Die KI wird von einem externen Dienstleister im Auftrag entwickelt.
Kommentar: Eröffnung des Anbieterfragebogens und Vertragsaddendum

☐ Die KI wird von einem externen Anbieter eingekauft.
Kommentar: Eröffnung des KI-Beschaffungsfragebogen

- Name: _____
- Hersteller: _____
- Website: _____

Welche Unterlagen zum KI-System wurden vom Hersteller/Anbieter bereitgestellt?
(Mehrfachauswahl möglich)

☐ Eine Betriebsanleitung, in der erklärt wird, wofür das System gedacht ist.
☐ Eine technische Dokumentation (z. B. Aufbau, Funktionsweise, Datenverarbeitung).

☐ Ein Verkaufs- oder Werbeprospekt, aus dem die Funktionen erkennbar sind.
☐ Ein Datenblatt oder Produktbeschreibung.

Kommentar: Festlegung der Zweckbestimmung des Herstellers als Grundlage für die Risikoklassifizierung

☐ Unklar / noch nicht spezifiziert

3. Anwendungsszenario bei dem Unternehmen

3.1 Was wollen wir mit der KI machen?

„Wofür soll das KI-System konkret eingesetzt werden?“ (Pflichtfeld)
_____

_____

Beispiel: „Das Unternehmen kauft Microsoft Copilot zentral als Ergänzung zu Microsoft 365. Mitarbeitende nutzen es, um Entwürfe für E-Mails, kurze Dokumentzusammenfassungen oder Meetingnotizen zu erhalten. Copilot verwendet nur die bereits vorhandenen Unternehmensdaten in M365 und liefert Vorschläge, die immer vom Mitarbeitenden kontrolliert und freigegeben werden.

Kommentar: Festlegung des eigenen Anwendungsszenarios und Abgleich mit der Zweckbestimmung. Bildet die Grundlage der Hochrisiko-Prüfung gemäß Art. 6 KI-VO und Anhang III.

3.2. Wie arbeiten wir mit der KI?

3.2.1 Kommuniziert die KI direkt mit uns?

☐ Keine Interaktion
die KI arbeitet im Hintergrund (z. B. Ein KI-Modul prüft im Hintergrund Rechnungsdaten auf Auffälligkeiten, ohne dass Mitarbeitende etwas davon merken.)

☐ Indirekte Interaktion
Menschen sehen Ergebnisse, aber interagieren nicht (z. B. Ein KI-Modul analysiert automatisch Verkaufszahlen und zeigt sie in einem Dashboard an, ohne dass jemand mit der KI sprechen muss.)

☐ Direkte Interaktion
Menschen kommunizieren oder reagieren (z. B. Mitarbeitende stellen einem KI-Assistenten Fragen im Chat und erhalten direkte Antworten oder Empfehlungen.)

Kommentar: Festlegung des Fragebogens Horizontale Transparenzpflichten (Art. 50 KI-VO)

3.2.2 Haben die KI-Ergebnisse möglicherweise direkt eine Auswirkung auf Menschen?

☐ Nein
die KI bewertet keine Menschen (z. B. Die KI sortiert interne Arbeitsschritte in einer besseren Reihenfolge, ohne dass dadurch Personen beurteilt werden.)

☐ Teilweise
Empfehlungen werden manuell geprüft (z. B. Die KI schlägt vor, welche Mitarbeitenden eventuell eine Schulung brauchen könnten. Eine Führungskraft prüft die Vorschläge aber immer zuerst.)

☐ Ja
die KI bewertet oder entscheidet über Personen (z. B. Die KI bewertet Bewerbungen und vergibt automatisch Punktzahlen, die über die Auswahl von Kandidaten mitentscheiden.)

3.2.3 Haben die KI-Ergebnisse eine Auswirkung auf Entscheidungen über Menschen?

☐ Keine Auswirkung
niemand merkt etwas davon (z. B. Die KI ordnet interne technische Prozesse neu, ohne dass dies Entscheidungen über Personen beeinflusst.)

☐ Gering
unterstützende Wirkung, Entscheidungsvorbereitung (z. B. Die KI macht Vorschläge oder erstellt erste Entwürfe, die Menschen als Grundlage für Entscheidungen nutzen.)

☐ Mittel
KI beeinflusst Entscheidungen, Menschen prüfen nach (z. B. Die KI erstellt eine Rangliste von Bewerbern, die dann von Personalverantwortlichen kontrolliert und bewertet wird.)

☐ Hoch
KI entscheidet über relevante Themen (z. B. Die KI sortiert Support-Anfragen automatisch nach Wichtigkeit, was beeinflusst, wessen Anliegen zuerst bearbeitet wird.)

☐ Sehr hoch
KI hat Folgen für Rechte, Job, Karriere oder Leistungen (z. B. Die KI entscheidet automatisch, ob eine Bewerbung weiter berücksichtigt oder abgelehnt wird.)

Kommentar: Prüfung ob Ausnahmeregelungen zu Anhang III greifen.

4. KI-System Setup bei dem Unternehmen

Wie integrieren wir das KI-System bei dem Unternehmen?

☐ Keine Anpassung am KI-System
Das KI-System wird unverändert verwendet. Es werden keine eigenen Daten hinzugefügt. Nur Einstellungen und Anweisungen werden angepasst.
(z. B. Die KI wird so genutzt, wie sie ist. Wir stellen nur ein, welche Aufgabe sie erfüllen soll, ohne eigene Unternehmens-Daten hochzuladen oder Funktionen zu ändern.)

☐ Integration des KI-Systems in bestehenden Workflow
Das KI-System wird in einen bestehenden Workflow integriert. Dabei werden Daten per API ein- und ausgegeben.
(z. B. Die KI wird an ein internes System angeschlossen. Sie bekommt automatisch Daten, verarbeitet sie und spielt die Ergebnisse zurück, ohne dass jemand Dateien manuell übertragen muss.)

☐ Das KI-System wird wesentlich angepasst
Der Aufbau, das Verhalten und das Risikoprofil des KI-Systems werden grundlegend angepasst.
(z. B. Die KI wird technisch erweitert und mit eigenen Unternehmensdaten angepasst, damit sie speziell auf unsere Abläufe zugeschnitten arbeitet.)

Kommentar: Bewertet, ob durch wesentliche Änderungen eine „Quasi-Anbieterschaft“ nach Art. 25 KI-VO entsteht.

5. Rechtliche Anforderungen

5.1 Personenbezug

Werden personenbezogene Daten verarbeitet?
☐ Nein
☐ Ja (Welche?): _____

5.2 Speicher- & Übermittlungsort

Wo werden die Daten gespeichert?
☐ EU
☐ Nicht-EU
☐ Unklar

5.3 Geheimnisse & IP

Ist sichergestellt, dass keine Geschäftsgeheimnisse in die KI gelangen?
☐ Ja
☐ Nein
☐ Unklar

5.4 Mitbestimmung (falls HR- oder Leistungsbezug)

☐ Mitarbeitendendaten werden bewertet
☐ Verhalten/Leistung wird analysiert
☐ Nicht relevant

6. Erwartete Wirkung & KPIs

Was soll erreicht werden?

☐ Zeitersparnis
☐ Qualitätsverbesserung
☐ Kosteneinsparung
☐ Fehlerreduktion
☐ Umsatz-/Conversion-Effekt
☐ Risikominimierung
☐ Service-Mehrwert
☐ Sonstiges: _____

Konkrete Zielwerte (optional):

- Zeitersparnis: ____ %
- Fehlerreduktion: ____ %
- Prozessqualität: ____ %
- Kostenvorteil: ____ € p.a.

7. Finaler Risikoscan (automatisch generiert)

- Menschkontakt: Ja/Nein
- Bewertung von Personen: Ja/Nein
- Automatisierte Entscheidung: Ja/Nein
- Art. 5-Eingriff möglich: Ja/Nein
- Hochrisiko-Anwendungsfall wahrscheinlich: Ja/Nein
- Modifikationsrisiko: niedrig/mittel/hoch
- Zweckänderung: Ja/Nein

8. Checkliste (automatisch generiert)

Basierend auf allen Antworten:
- KI-VO Art. 3 Nr. 1 erfüllt?
- Anwendungsszenario vs. Herstellerzweck geprüft
- Menschkontakt identifiziert
- Profiling/Scoring festgestellt
- Entscheidungsauswirkung bewertet
- Datenrisiken klassifiziert
- Mitbestimmungspflicht geprüft
- Technische und organisatorische Maßnahmen erforderlich
- Nächste Schritte für Konformität

1. Keine Anwendung (Bereichsausnahmen)

- Haushaltsausnahme
  - Gemischte Tätigkeit
  - Überwiegend negative Auswirkung auf den Betroffenen
- Wissenschaftsprivileg
  - Voraussetzung 1: Wissenschaftliche Forschung und Entwicklung
  - Voraussetzung 2: Reine Inbetriebnahme
- Forschungs- und Entwicklungsprivileg
  - Voraussetzung 1: Erprobungsphase
  - Voraussetzung 2: Handlung
    - Erprobung unter Realbedingungen
- Internationale Zusammenarbeit
- Militärische Zwecke (gem. Art. 2 Abs. 3 S.2 KI-VO)
- Verteidigungszwecke (gem. Art. 2 Abs. 3 S.2 KI-VO)
- Zwecke der nationalen Sicherheit (gem. Art. 2 Abs. 3 S.2 KI-VO)
- Freie und quelloffene KI-Technologien i.S.d. Art. 2 Abs. 12, 53 Abs. 2 KI-VO
  - Voraussetzungen bei KI-Systemen i.S.d. Art. 2 Abs. 12 KI-VO
    - Öffentliche Verfügbarkeit und Offenheit
    - Keine Monetarisierung
    - Offenlegung der Parameter und technischen Details
  - Voraussetzungen bei KI-Modellen i.S.d. Art. 53 Abs. 2 KI-VO
    - Vollständige Offenlegung aller Parameter:
    - Erlaubnis zur Nutzung, Änderung und Weitergabe
    - Keine schädliche Monetarisierung
    - Systemische Risiken

2. Anwendungsbereiche

- Sachlicher Anwendungsbereich
  - KI-System i.S.d. Art. 3 Nr. 1 KI-VO, ErwGr 12
    - Maschinengestützt
    - Gewisser Grad an Autonomie
    - Anpassungsfähigkeit
    - Ziele
    - Ableitungsfähigkeit bzw. Schlussfolgerung
    - Ausgaben
    - Umweltwirkung
  - KI-System mit allgemeinem Verwendungszweck i.S.d. Art. 3 Nr. 66 KI-VO
    - KI-System i.S.d. Art. 3 Nr. 1 KI-VO, ErwGr 12
    - Abhängigkeit vom KI-Modell
      - Fähigkeit zur vielseitigen Nutzung
      - Vielzahl von Zwecken
    - Direkte und indirekte Verwendung
      - Direkte Verwendung
      - Integration in andere Systeme

- KI-Modell mit allgemeinem Verwendungszweck i.S.d. Art. 3 Nr. 63 KI-VO, ErwGr 97
    - Erhebliche allgemeine Verwendbarkeit
    - Kann breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen
    - Direkt einsetzbar in nachgelagerte Systeme oder Anwendungen
- KI-Modell mit allgemeinem Verwendungszweck mit systemischen Risiken i.S.d. Artt. 3 (65), 51, 52 KI-VO
    - Erhebliche allgemeine Verwendbarkeit
    - Kann breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen
    - Direkt einsetzbar in nachgelagerte Systeme oder Anwendungen
    - Fähigkeit mit hohem Wirkungsgrad i.S.d. Art 51 KI-VO
- Keine Änderung der Systemkonzeption gem. Art. 111 Abs. 2 KI-VO

- Persönlicher Anwendungsbereich
    - Betroffene Personen i.S.d. Art. 2 Abs. 1 g.) KI-VO
    - Anbieter i.S.d. Art. 3 (3) KI-VO
        - Entwickelt / entwickeln lässt
        - Inverkehrbringen Art. 3 (9) KI-VO
        - in Betriebnahme Art. 3 (11) KI-VO
    - Betreiber i.S.d. Art. 3 (4) KI-VO
        - Stelle
        - KI-System
        - Verwendung
        - In eigener Verantwortung
        - Gewerblich
    - Einführer i.S.d. Art. 3 (6) KI-VO
        - Ansässigkeit/Niederlassung
        - Inverkehrbringen eines KI-Systems
        - Unter dem Namen oder der Handelsmarke eines Drittlandsanbieters
    - Händler i.S.d. Art. 3 (7) KI-VO
        - Stelle
        - Bereitstellung eines KI-Systems
        - Unionsmarkt
        - Nicht Anbieter oder Einführer
    - Quasi-Anbieter gem. Art. 25 KI-VO, ErwGr 84
        - Szenario 1: Name/Handelsmarke gem. Art. 25 Abs. 1 a) KI-VO
        - Szenario 2: Wesentliche Änderung gem. Art. 25 Abs. 1 b) KI-VO, ErwGr 128
        - Szenario 3: Zweckänderung gem. Art. 25 Abs. 1 c) KI-VO
        - Szenario 4: Produkthersteller gem. Art. 25 Abs. 3 a) KI-VO
        - Szenario 5: Produkthersteller gem. Art. 25 Abs. 3 b) KI-VO

- Räumlicher Anwendungsbereich
    - Inbetriebnahme / Inverkehrbringen von KI-Systemen, oder KI-Modellen in der EU (Art. 2 Abs. 1 lit. a KI-VO)
    - Betreiber von KI-Systemen mit Sitz in der EU (Art. 2 Abs. 1 lit. b KI-VO)
    - Verwendung der KI-System Ausgabe in der EU (Art. 2 Abs. 1 lit. c KI-VO)
    - Einführer und Händler von KI-Systemen (Art. 2 Abs. 1 lit. d KI-VO)
    - Bevollmächtigte (Art. 2 Abs. 1 lit. g KI-VO)

3. Zweck- und Kontextbestimmung (Art. 3 Nr. 12 KI-VO)

- Anbieter bestimmt die Verwendung gem. Art. 3 Nr. 12 KI-VO
    - Bedingungen für die Verwendung gem. Art. 3 Nr. 12 KI-VO
    - Besondere Umstände gem. Art. 3 Nr. 12 KI-VO
- In bereitgestellten Informationen
    - Technische Dokumentation gem. Anhang IV, Art. 11 Abs. 1 a) KI-VO
    - Betriebsanleitung gem. Art. 13 Abs. 3 b) i) i.V.m. Art. 3 Nr. 15 KI-VO
    - Werbe- oder Verkaufsmaterial gem. Art. 3 Nr. 12 KI-VO

4. Risikoklassifizierung KI-Technologie

- Risikoeinordnung bei KI-Systemen
    - Verbotene KI-Praktiken i.S.d. Art 5 KI-VO
        - Verbotene Praktiken gem. Art. 1 Abs. 2 b.) i.V.m. Art. 5 KI-VO
        - Unterschwellige Beeinflussung & Manipulation Art 5 Abs. 1 a.) KI-VO, 29 ErwGr
        - Soziale Bewertung oder Soziale Einstufung Art 5 Abs. 1 c.) KI-VO ErwGr 31
        - Prädiktive Polizeiarbeit Art. 5 Abs. 1 d.) KI-VO
        - Emotionserkennung Art. 5 Abs. 1 f.) KI-VO ErwGr 44
        - Ungezielte Sammlung von Gesichtsbildern (Scraping) Art. 5 Abs. 1 e.) KI-VO
        - Biometrische Kategorisierung Art. 5 Abs. 1 g.) KI-VO ErwGr 30
        - Biometrischen Echtzeit-Fernidentifizierung Art. 5 Abs. 1 h.) KI-VO ErwGr 32,33,38
    - Hochrisiko KI-Systeme gem. Art. 6 KI-VO i.V.m. Anhang I und III
        - Nach Zustand i.S.d. Art. 6 Abs. 1 KI-VO i.V.m. Anhang I (Produkt / Sicherheitsbauteil)
            - Maschinen gem. Anhang I Nr. 1 KI-VO
            - Funkanlagen gem. Anhang I Nr. 6 KI-VO
            - Zwei- oder dreirädrigen und vierrädrigen Fahrzeugen gem. Anhang I Nr. 14 KI-VO
            - Sportboote und Wassermotorräder gem. Anhang I Nr. 3 KI-VO
            - Spielzeug gem. Anhang I Nr. 2 KI-VO
            - Medizinprodukte gem. Anhang I Nr. 11 KI-VO
            - Geräte zur Verbrennung gasförmiger Brennstoffe gem. Anhang I Nr. 10 KI-VO
            - Kraftfahrzeuge und Kraftfahrzeuganhänger gem. Anhang I Nr. 18 KI-VO
            - Aufzüge gem. Anhang I Nr. 4 KI-VO
            - In-vitro-Diagnostika gem. Anhang I Nr. 12 KI-VO
            - Land- und forstwirtschaftliche Fahrzeuge gem. Anhang I Nr. 15 KI-VO
            - Seilbahnen gem. Anhang I Nr. 8 KI-VO
            - Sicherheit in der Zivilluftfahrt gem. Anhang I Nr. 13 KI-VO
            - Interoperabilität des Eisenbahnsystems gem. Anhang I Nr. 17 KI-VO
            - Geräte und Schutzsysteme für explosionsgefährdete Bereiche gem. Anhang I Nr. 5 KI-VO
            - Druckgeräte gem. Anhang I Nr. 7 KI-VO
            - Persönliche Schutzausrüstungen gem. Anhang I Nr. 9 KI-VO
            - Schiffsausrüstung gem. Anhang I Nr. 16 KI-VO
        - Nach Anwendung i.S.d. Art. 6 Abs.1 KI-VO i.V.m. Anhang III
            - Erlaubte Biometrie:
                - Biometrische Fernidentifizierungssysteme gem. Nr. 1 a) Anhang III
                - Emotionserkennung gem. Nr. 1 d.) Anhang III
                - Biometrische Kategorisierung gem. Nr. 1 c.) Anhang III
            - Ausbildung:
                - Zugang, Zulassung, Zuweisung zu Bildungs- und Berufsbildungseinrichtungen gem. 56 ErwGr, Nr. 3 a.) Anhang III
                - Bewertung des Bildungsniveaus gem. 56 ErwGr, Nr. 3 c.) Anhang III
                - Steuerung des Lernprozesses gem. Nr. 3 b.) Anhang III
                - Bewertung von Lernergebnissen verwendet werden gem. 56 ErwGr, Nr. 3 b.) Anhang III
                - Überwachung und Erkennung von verbotenem Verhalten von Schülern bei Prüfungen gem. Nr. 3 d.) Anhang III
            - Bewerbungsverfahren:
                - Einstellung oder Auswahl von Personen (inkl. Stellenanzeigen) gem. 57 ErwGr, Nr. 4 a.) Anhang III

- Bewertung von Bewerbern gem. 57 ErwGr, Nr. 4 a.) Anhang III
- Sichtung und Filterung von Bewerbungen gem. 57 ErwGr, Nr. 4 a.) Anhang III

- Arbeitsverhältnis:
  - Beeinflussung von Entscheidung hinsichtlich Zuweisung von Arbeitsaufgaben im Arbeitsverhältnis gem. 57 ErwGr, Nr. 4 b.) Anhang III
  - Beobachtung der Leistung im Arbeitsverhältnis gem. 57 ErwGr, Nr. 4 b.) Anhang III
  - Bewertung der Leistung im Arbeitsverhältnis gem. Nr. 4 b.) Anhang III
  - Beeinflussung von Entscheidung hinsichtlich
  - Bedingungen von Arbeitsverhältnissen gem. 57 ErwGr, Nr. 4 b.) Anhang III
  - Beeinflussung von Entscheidung hinsichtlich
  - Beförderungen im Arbeitsverhältnis gem. 57 ErwGr, Nr. 4 b.) Anhang III
  - Beeinflussung von Entscheidung hinsichtlich Kündigung von Arbeitsverhältnissen gem. 57 ErwGr, Nr. 4 b.) Anhang III
- Versicherungen:
  - Risikobewertung von Kranken- und Lebensversicherungen gem. 58 ErwGr, Nr. 5 c.) Anhang III
  - Preisbildung in Bezug auf Kranken- und Lebensversicherungen gem. Nr. 5 c.) Anhang III
- Banken:
  - Kreditwürdigkeitsprüfung gem. 58 ErwGr, Nr. 5 b.) Anhang III
  - Kreditpunktbewertung gem. 58 ErwGr, Nr. 5 b.) Anhang III
- Öffentliche Einrichtungen:
  - Beurteilung des Anspruchs auf grundlegende öffentliche Unterstützungsleistungen und Sozialdienste gem. 58 ErwGr, Nr. 5 a.) Anhang III
  - Betrieb kritischer digitaler Infrastruktur, des Straßenverkehrs sowie der Wasser-, Gas-, Wärme- und Stromversorgung gem. Nr. 2 Anhang III
  - Entsendung, Bewertung, Priorisierung von Not- und Rettungsdiensten gem. 58 ErwGr, Nr. 5 d.) Anhang III
- Strafverfolgung:
  - Risikobewertung bei der Strafverfolgung gem. Nr. 6 a.) Anhang III
  - Lügendetektoren oder ähnliche Instrumente gem. Nr. 6 b.) Anhang III
  - Bewertung der Verlässlichkeit von Beweismitteln im Zuge der Ermittlung oder Verfolgung von Straftaten gem. 59 ErwGr, Nr. 6 c.) Anhang III
  - Bewertung der Wahrscheinlichkeit, dass eine natürliche Person eine Straftat begeht oder wiederholt gem. 59 ErwGr, Nr. 6 d.) Anhang III
  - Erstellung von Profilen natürlicher Personen im Rahmen der Strafverfolgung gem. Nr. 6 e.) Anhang III
- Migration, Asyl und Grenzkontrolle:
  - Lügendetektoren und ähnliche Instrumente bei Migration, Asyl und Grenzkontrolle gem. 60 ErwGr, Nr. 7 a.) Anhang III
  - Bewertung eines Risikos bei Migration, Asyl und
  - Grenzkontrolle gem. 60 ErwGr, Nr. 7 c.) Anhang III

- Prüfung von Asyl- und Visumanträgen sowie Aufenthalt im Bereich Migration, Asyl und Grenzkontrolle gem. 60 ErwGr, Nr. 7 b.) Anhang III
- Aufdeckung, Anerkennung oder Identifizierung natürlicher Personen gem. 60 ErwGr, Nr. 7 d.) Anhang III
- Wahlbeeinflussung bei Rechtsfolge/demokratische Prozesse gem. 62 ErwGr, Nr. 8 a.) Anhang III
- Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften bei Rechtsfolge/demokratische Prozesse gem. 61 ErwGr, Nr. 8 b.) Anhang III

- Ausnahme: Ergänzung menschlicher Tätigkeit nach Art. 6 Abs. 3 KI-VO, ErwGr 53
  - Kein erhebliches Risiko der Beeinträchtigung, da keine wesentliche Beeinflussung des Ergebnisses der Entscheidungsfindung
  - Verbesserung des Ergebnisses einer zuvor abgeschlossenen menschlichen
  - Tätigkeit (Art. 6 Abs. 3 b.) KI-VO)
  - Erkennen von Entscheidungsmustern und Abweichungen (Art. 6 Abs. 3 c.) KI-VO)
  - Vorbereitungsaufgabe (Art. 6 Abs. 3d) KI-VO)
- Rückausnahme: KI-System beinhaltet Profiling (Art. 5 Abs. 1KI-VO)

- Risikoeinordnung bei KI-Modellen
  - Liegt ein KI-Modell mit allgemeinem Verwendungszweck vor?
  - Liegt vor, wenn:
    - Erhebliche allgemeine Verwendbarkeit
    - Breites Spektrum von Aufgaben
    - Direkt einsetzbar in nachgelagerte Systeme oder Anwendungen
      - Wenn eine der Voraussetzungen nicht erfüllt ist → Prüfung beenden;
      - Wenn alle erfüllt sind → Prüfung fortsetzen.
    - Prüfung: Besteht ein systemisches Risiko (hoher Wirkungsgrad) gem. Art. 51 KI-VO?
      - Technische Kriterien nach Anhang XIII KI-VO
        - Parameteranzahl des KI-Modells
        - Trainingsdatenmenge (Tokens)
        - Erforderliche Rechenleistung (FLOPs) für das Training
        - Reichweite und Nutzerzahl
        - Ein- und Ausgabemodalitäten (z. B. Multimodalität)
      - Schnelleinstufung („Daumenregeln“):
        - FLOPS-Regel (Art. 51 Abs. 1 lit. a KI-VO)
          - FLOP-Schwelle ≥ 10^{25} gilt als widerlegbare Vermutung für systemisches Risiko
          - FLOP-Schätzung möglich über: FLOPs=6×Anzahl Parameter×Anzahl Tokens (OpenAI/Google-Formel gem. Guideline)
          - Anbieter kann technische Gegenbeweise liefern (z. B. Benchmarkvergleiche, Risikoanalysen, reale Einsatzzwecke, Architekturdetails)
        - Fähigkeitenvergleich (Art. 3 Nr. 64 KI-VO)
          - Vergleichbarkeit mit bereits eingestuften, leistungsstarken Modellen?
          - Vergleich bezieht sich auf Output-Fähigkeiten, Robustheit, Anwendungsspektrum - Guideline: Der Vergleich kann indirekt durch Veröffentlichungen, Marktanalysen oder Leistungstests erfolgen

- Nebenbedingung: Erhebliche Auswirkungen auf den Unionsmarkt
    - Reichweite, Downloadzahlen, Integration in zentrale Dienste
    - Guideline: Modelle mit Proof-of-Concept-Charakter ohne Marktverbreitung nicht systemisch
- Klassifizierung (Bewertungsergebnis)
    - Wenn alle Punkte vollständig erfüllt → KI-Modell mit systemischem Risiko
    - Wenn Punkte nicht erfüllt bzw. widerlegt → KI-Modell ohne systemisches Risiko

5. Pflichten ermitteln & Maßnahmen festlegen

- Technische Maßnahmen
    - Kennzeichnungspflichten
    - Entwicklungs- und Integrationspflichten
        - Integration geeigneter Mensch-Maschine-Schnittstelle zwecks menschl. Aufsicht (Art. 14 KI-VO)
        - Integration von Sicherheitsmechanismen zur Risikominimierung. (Art. 15 KI-VO, ErwGr 76)
        - Entwicklung und Integration von Betriebseinschränkungen im System für die menschl. Aufsicht (ErwGr 73)
        - Integration von Beratungs- und Informationsmechanismen im System für die menschl. Aufsicht (ErwGr 73)
        - Trustworthy AI by Design Art. 17 Abs. 1 b.), c.), d.) KI-VO
        - Durchführung von Angriffstests bei den KI-Modellen (ErwGr 114)
    - Konformitätspflichten
        - Bereitstellung eines Datenqualitätsmanagementsystems gem. Art 10 KI-VO, ErwG 67
            - Trainings-, Validierungs- und Testdatensätzen gem. Qualitätskriterien (Art. 10 Abs. 2-5 KI-VO)
            - Durchführung von Korrekturmaßnahmen i.S.d. Art. 20 Abs. 1 KI-VO
            - Verwendung des KI-Systems gem. Gebrauchsanweisung i.S.d. Art. 26 Abs. 1,5 KI-VO, ErwGr 91
        - Risikomanagementsystem
            - Durchführung einer Modellbewertung mit stand. Protokollen und Instrumenten (Art. 55 Abs. 1 a.) KI-VO)
            - Durchführung von Angriffest zwecks Risikoermittlung (Art. 55 Abs. 1 a.) KI-VO)
            - Gewährleistung eines angemessenes Maß an Cybersicherheit und Infrastruktur (Art. 55 Abs. 1 d.) KI-VO)
    - Überwachungspflichten
        - Implementierung von Sicherheitsmechanismen zur Sicherstellung der Robustheit (Art. 15 KI-VOErwGr 75)
        - Implementierung von Überwachungsalgorithmen, Schwellenbasierter Trigger (ErwGr 75)
        - Überwachung der Funktionsweise der KI-Systeme (i.S.d. 91 ErwGr)
        - Eingabedaten (Kontrolle auf Zweckkonformität) i.S.d. Art. 26 Abs. 4 KI-VO
        - Pflicht zur Überwachung des Betriebs des Hochrisiko-KI-Systems gemäß Betriebsanleitung (Art. 26 Abs. 5 1. HS KI-VO)
        - Pflicht zur Verwendung der KI-Systeme gemäß Betriebsanleitungen (Art. 26 Abs. 1 KI-VO)
    - Aufzeichnungspflichten
        - Aufzeichnungspflicht (i.S.d. ErwGr 91)
        - Protokollierung während der Lebensdauer des Systems (i.S.d. Art. 12 Abs. 1,2 KI-VO, ErwGr 71
        - Aufbewahrungspflicht der Protokolle (i.S.d. 26 Abs. 6 ErwGr)

- Organisatorische Maßnahmen
  - Informationspflichten
    - Gegenüber Betreiber
      - Anbieter müssen sicherstellen, dass mit Menschen interagierende KI-Systeme entsprechend informieren können (Art. 50 Abs. 1,5 KI-VO, ErwGr 132)
      - Besondere Transparenzpflichten bei Gefahr des Identitätsbetrugs, Täuschung, Deepfakes i.S.d. ErwGr 132
      - Betreiber von Emotionserkennungs- oder biometrischen Kategorisierungssystemen müssen betroffene Personen informieren und rechtskonform verarbeiten (Art. 50 Abs. 3,5 KI-VO)
      - Bereitstellung von Informationen für die Betreiber (Art. 9 Abs. 5 c.) KI-VO)
      - Bereitstellung des Leistungskennzahlenniveaus des Systems für die Nutzer i.S.d. ErwGr 74
      - Hinreichende Transparenz zwecks angemessener
      - Interpretation durch Betreiber (Art. 13 i.V.m. Abschnitt 3 KI-VO)
      - Unverzügliches Informieren bei Korrekturmaßnahmen gegenüber den Betreibern i.S.d. Art. 16 j.) i.V.m. Art. 20 Abs. 1 KI-VO
      - Informationspflicht gegenüber den Betroffenen bei der Verwendung von KI-Systemen, die Entscheidungen betreffen oder unterstützen, Art. 26 Abs. 11 KI-VO, ErwGr 93, 171
      - Abgabe einer Erklärung gegenüber den Betroffenen i.S.d. ErwGr 171
      - Unterrichtungspflicht gegenüber den Betroffenen i.S.d. ErwGr 93
      - Einholung einer Einwilligung bei Tests unter realen Bedingungen außerhalb von KI-Reallaboren gem. Art. 61 Abs. 1 KI-VO
    - Gegenüber Anbieter
      - Informieren des Anbieters gem. Art 72, 73 KI-VO
      - Pflicht zur Information des Anbieters im Rahmen der Beobachtung gemäß Art. 26 Abs. 5 S.1 i.V.m. Art. 72 Abs. 2 KI-VO
      - Bereitstellung der tech. Dok. gegenüber dem Anbieter, welcher das Modell in sein eigenes KI-System integriert, ErwGr 101
    - Gegenüber den Mitarbeitern
      - Pflicht zur Information der Mitarbeiter über eingesetzte KI-Systeme gemäß Art. 26 Abs. 7 KI-VO, ErwGr 93
      - Pflicht zur unverzüglichen Information der Akteure / Behörde bei Feststellung eines schwerwiegenden Vorfalls (Art. 26 Abs. 5 S. 3 KI-VO).
      - Pflicht zur Erfüllung der Registrierungspflichten gemäß Art. 49 EU-Organe und Einrichtungen (Art. 26 Abs. 8 S.1 KI-VO)
    - Behördenkommunikation
      - Bereitstellung der technischen Dokumentation gegenüber dem Amt für künstliche Intelligenz und zuständigen Behörden ErwGr 101
      - Pflicht zur Benennung eines Bevollmächtigten i.S.d. Art. 54 Abs. 1 KI-VO
      - Meldung von schwerwiegenden Vorfällen gegenüber Kommission und nationalen Behörden (Art. 55 Abs. 1 c.) KI- VO, ErwGr 115)
      - Unverzügliche Meldung der Vorfälle/Korrekturmaßnahmen innerhalb von zwei Wochen (Art. 52 Abs. 1 KI-VO)
      - Antrag gegenüber Kommission Entscheidung und anschließenden Gesamtbewertung (ErwGr 111)
      - Bereitstellung der tech. Dok. gegenüber dem Amt für künstliche Intelligenz und zuständigen Behörden ErwGr 101
      - Informieren von Korrekturmaßnamen gegenüber Kommission und nationalen Behörden (ErwGr 115)
    - Dokumentationspflichten
      - Erstellung von Verhaltenskodizes (ErwGr 165)
      - Bereitstellen von Modellkarten (Zweck, Leistung, Trainingsdaten) (ErwGr 165)

- Bereitstellen von Datenkarten (Herkunft, Zusammensetzung, Verarbeitungsschritte der Daten) (ErwGr 165)
- Dokumentation der Entscheidung KI-System ist nicht hochrisikobehaftet (Art. 6 Abs. 4 KI-VO, ErwGr 65)
- Organisatorische Dokumentation
    - Dokumentation der Entscheidungen im Rahmen der Risikomanagementmaßnahmen (ErwGr 65)
    - Erfassen aller möglichen Verwendungsszenarien des KI-Systems (ErwGr 65)
    - Abschluss einer schriftl. Vereinbarung mit dem Betreiber i.S.d. ErwGr 88
    - Datieren und Dokumentieren der Einwilligung bei Tests gem. Art. 61 Abs. 2 KI-VO
- Technische Dokumentation
    - Führen und Aufzeichnen einer technischen Dokumentation i.S.d. Art. 11 Abs. 1 i.V.m. Anhang IV, ErwGr 71, 81
    - Führen und Aufzeichnen einer technischen Dokumentation i.S.d. ErwGr 101
    - Merkmale, Fähigkeiten, Grenzen Algorithmen, Daten und Trainings-, Test- und Validierungsverfahren (ErwGr 71)
    - Bereitstellung eines Störungssicherheitsplans für die Robustheit i.S.d. ErwGr 75
- Gebrauchsanweisung
- Technische Dokumentation während des Trainings
    - Zusammenfassung der Datenquellen für das Training gem. Vorlage (Art. 53 Abs. 1 c.) KI-VO, ErwGr 107)
    - Tech. Dokumentation u. Aktualisierung i.S.d. Anhang XI (Art. Art. 53 Abs. 1 a.), b.) KI-VO, ErwGr 111)

- Registrierungspflichten
    - Registrierungspflicht in der EU-Datenbank i.S.d. Art. 6 Abs. 4 i.V.m. 49 Abs. 2 KI-VO
    - Registrierungspflicht in der EU-Datenbank i.S.d. Art. 16 i.) i.V.m. Art. 49 KI-VO
    - Registrierungspflicht in der EU-Datenbank i.S.d. Art. 49 Abs. 3 KI-VO
    - Pflicht zur Benennung eines Bevollmächtigten i.S.d. Art. 22 KI-VO
- Kennzeichnungspflichten
    - Pflicht zur Namensangabe, Handelsname, Handelsmarke und Kontaktanschrift (Art. 16 b.) KI-VO)
    - Versehen des KI-Systems mit der CE-Kennzeichnung (Art. 48 Abs. 2 KI-VO, ErwGr 129)
- Konformitätspflicht
    - Durchführung des Konformitätsbewertungs-verfahrens (Art. 16 f.) i.V.m. Art. 43 KI-VO ErwGr 81, 132)
    - Ausstellen einer EU-Konformitätserklärung gem. Art. 16 g.) i.V.m. 47 KI-VO
    - Bereitstellung eines Systems für Konformitätsverfahrens (ErwGr 125)
- Pflichten zur Einrichtung von KI-Managementsystemen
    - Risikomanagement
        - Bereitstellen eines Risikomanagementsystems gem. Art. 17 Abs. 1 g.) KI-VO i.V.m. Art. 9 KI-VO, ErwGr 65
        - Bereitstellen eines Risikomanagementsystems gem. Art. 8 Abs. 1 S.2 i.V.m. Art. 9 KI-VO
        - Bereitstellen eines Risikomanagementsystems gem. ErwGr 114
        - Ermittlung und Analyse der Risiken, die bei bestimmungsgemäßer Verwendung ausgehen können, Art 9 Abs. 2 a.), 3 KI-VO

- Pflicht zur Abschätzung und Bewertung der Risiken gem. Art. 9 Abs. 2 b.), 3, 9 KI-VO
- Pflicht zur Bewertung von Risiken auf Grundlage der Auswertung der Daten aus dem Beobachtungssystem (Art. 72 KI-VO) gemäß Art. 9 Abs. 2 c.), 3 KI-VO
- Pflicht zur Ergreifung geeigneter Maßnahmen zur
- Risikobewältigung gemäß Art. 9 Abs. 2 d.), 4, 5 KI-VO.
- Pflicht zur Testung zur Ermittlung der am besten geeigneten Risikomanagementmaßnahmen, Art. 26 Abs. 6, 8KI-VO)
- Pflicht zur Bewertung systematischer Risiken im KI-Lebenszyklus (Plattformen und Suchmaschinen) (ErwGr 118)

- Qualitätsmanagement
  - Einrichtung eines Qualitätsmanagementsystems (Art. 16 c.) i.V.m. Art. 17 KI-VO, ErwGr 81)
  - Konzept zur Einhaltung der Regulierungsvorschriften (RiLi, Prozesse, Konzept) Art. 17 Abs. 1 a.) m.) KI-VO, Anhang VII Nr. 3 e.) KI-VO
  - Liste aller KI-Systeme Anhang VII Nr. 3 b.), ErwGr 65
  - Technische Dokumentation jedes KI-Systems Anhang VII Nr. 3 c.) KI-VO
- Datenqualitätsmanagement
  - Bereitstellung eines Datenqualitätsmanagementsystems gem. Art 10 KI-VO
  - Pflicht zur Sicherstellung, dass kontrollierbare Eingabedaten zweckentsprechend und repräsentativ sind (Art. 26 Abs. 4 KI-VO).
  - Einrichtung eines Daten-Governance und Datenverwaltungsverfahrens i.S.d. ErwGr 67
  - Einrichtung eines Daten-Governance und Datenverwaltungsverfahrens i.S.d. ErwGr 114
  - Überprüfung der Datensatzintegrität und der Datenschulungs-, Validierungs- und Testverfahren (ErwGr 67)
  - Pflicht zum Aufsetzen einer Strategie zur Einhaltung des Urheberrechts (Art. 53 Abs. 1 c.) KI-VO)

- Schulungspflichten
  - Sicherstellung der KI-Kompetenz gegenüber Mitarbeitern (i.S.d. Art 4 KI-VO)
  - Schulungen gegenüber den Betreibern (Art. 9 Abs. 5 c.) KI-VO)
  - Pflicht zur Übertragung der menschlichen Aufsicht an qualifizierte Personen (Art. 26 Abs. 2 1. HS KI-VO)
  - Pflicht zur Unterstützung der Aufsichtspersonen (Art. 26 Abs. 2 2. HS KI-VO).
- Testpflichten
  - Erstellung eines Plans für den Test unter realen Bedingungen außerhalb von KI-Reallaboren (Art. 60 Abs. 4 a.) KI-VO
  - Überwachung von Tests unter realen Bedingungen außerhalb von KI-Reallaboren (Art. 60 Abs. 4 j.) KI-VO
  - Durchführung von Tests zwecks Ermittlung von geeigneten Maßnahmen (Art. 9 Abs. 6,7,8 KI-VO)
- Aufbewahrungspflichten
  - Die tech. und org. Dokumentationen sind aufzubewahren (Art. 16 d.), e.) i.V.m. Art. 18 KI-VO)
  - Aufbewahrung der automatisch erzeugten Protokolle gem. Art. 19 Abs. 1 i.V.m. Art. 12 Abs. 1 KI-VO
  - Pflicht zur Aufbewahrung automatisch erzeugter Protokolle für mindestens sechs Monate (Art. 26 Abs. 6 S.1 KI-VO)
  - Aufbewahrung der EU-Konformitätserklärung für 10 Jahre (Art. 47 KI-VO)

    - Aufbewahrung der EU-Konformitätserklärung für 10 Jahre (Art. 47 KI-VO)
- Meldeverfahren bei Vorfall Art. 17 Abs. 1 i.) i.V.m. Art. 73 KI-VO
- Pflichten gegenüber Behörden
    - Pflicht zur Zusammenarbeit mit den Behörden (Art. 26 Abs. 12 KI-VO)
    - Unterrichten der zuständigen Marktüberwachungsbehörde (Art. 27 Abs. 3 KI-VO, ErwGr 96)
    - Informieren der Marktüberwachungsbehörde gem. Art. 79 Abs. 1 KI-VO
- Pflicht zur Durchführung von Risikoabschätzungen
    - Pflicht zur Durchführung einer Datenschutzfolgenabschätzung i.S.d. Art. 26 Abs. 9 KI-VO
    - Durchführung einer Grundrechte-Folgenabschätzung (Art. 27 KI-VO, ErwGr 96)

Checkliste KI-System
i.S.d. Art. 3 Nr. 1 KI-VO, ErwGr 12

Einleitung

Das KI-System ist der zentrale Begriff der KI-Verordnung (KI-VO). Es bildet den Dreh- und Angelpunkt der Regulierung und wird zum zentralen Prüfungsgegenstand im Rahmen der Umsetzung der Verordnung. Der Begriff des „KI-Systems" spielt nicht nur in der KI-VO eine Schlüsselrolle, sondern ist auch in anderen Rechtsakten relevant, wie etwa in der geplanten KI-Haftungsrichtlinie oder der Produkthaftungsrichtlinie.

Die Definition des KI-Systems war von Beginn an einer der am stärksten umstrittenen Punkte im Gesetzgebungsprozess. Der ursprüngliche Vorschlag der Europäischen Kommission vom April 2021 sah eine technologiespezifische Definition vor. KI-Systeme wurden darin als „Software" beschrieben, die mithilfe bestimmter, in Anhang I gelisteter Techniken und Konzepte entwickelt wurde und Ergebnisse wie Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die ihr Umfeld beeinflussen. Diese Techniken umfassten maschinelles Lernen, logik- und wissensbasierte Ansätze sowie statistische Methoden. Im weiteren Gesetzgebungsverlauf setzte sich jedoch eine eher technologieoffene Definition durch. Kritiker argumentierten, dass eine zu spezifische Definition
Innovationen hemmen und neue Technologien unnötig einschränken könnte. Die finale Definition, die sich an den Empfehlungen der OECD orientiert, wurde im November 2023 konsolidiert.

Zudem betonen die Leitlinien[1] i.S.d. Art. 96 Abs. 1 f. KI-VO der EU-Kommission ausdrücklich, dass es nicht möglich sei, „eine erschöpfende Liste aller potenziellen KI-Systeme zu erstellen", da eine solche Definition nicht mechanisch angewandt werden dürfe. Weiterhin stützt sich die EU-Kommission in ihren Leitlinien auf eine lebenszyklusbasierte Sichtweise, die zwei Hauptphasen umfasst: die Phase vor der Einrichtung oder „Erstellung" des Systems und die Phase nach der Einrichtung oder „Nutzung" des Systems. Alle Voraussetzungen der KI-System-Definition müssen dabei nicht in beiden Phasen durchgehend vorhanden sein. Im Gesetzgebungsprozess wurde auch die Idee der Technologieneutralität hervorgehoben, um sicherzustellen, dass zukünftige Technologien nicht unnötig ausgeschlossen werden. Gleichzeitig wird darauf hingewiesen, dass KI-Systeme aufgrund ihrer Autonomie und Anpassungsfähigkeit nach der Betriebsaufnahme eine besondere Prüfung erfordern, die weit über traditionelle Software hinausgeht.

Warum gibt es die Regelung

Die KI-Verordnung bringt durch die Definition des KI-Systems Struktur und Systematik in die Regulierung von KI-Technologien. Dies ermöglicht es, einen klaren Prüfungsgegenstand zu schaffen, der als Grundlage für zukünftige Fallbewertungen dient. Für Anwender der KI-Verordnung ist es entscheidend, Klarheit über die einzelnen Voraussetzungen, Ansätze und Abgrenzungen des KI-Systems zu schaffen. Die Regelung verfolgt auch das Ziel, rechtliche und ethische Probleme, die bei fortgeschrittenen algorithmischen Systemen auftreten können, zu adressieren. Dabei stellt sich die Frage, welche konkreten Technologien unter die Verordnung fallen. Der Gesetzgeber hat klargestellt, dass bestimmte Sonderformen des KI-Systems, wie Emotionserkennungssysteme, biometrische Systeme und Systeme mit allgemeinem Verwendungszweck, jeweils eigene Anforderungen und Risiken mit sich bringen, die gesondert behandelt werden müssen.

Definition KI-VO

Art. 3 Nr. 1 KI-VO definiert das KI-System folgendermaßen:

> *„KI System" ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können;*

[1] Europäische Kommission, C(2025) 924 final, ANNEX zur Mitteilung an die Kommission – Genehmigung des Inhalts des Entwurfs einer Mitteilung der Kommission: Leitlinien der Kommission zur Definition eines KI-Systems gemäß Verordnung (EU) 2024/1689 (KI-Verordnung), Brüssel, 6. Februar 2025, Absatz 10, abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application (zuletzt abgerufen am 07.02.2025)

Checkliste KI-System i.S.d. Art. 3 Nr. 1 KI-VO

1. Maschinengestützt

Definitionsvorschlag: Ein maschinengestütztes KI-System ist ein System, das zur Entwicklung und Ausführung seiner Funktionen auf Hardware- und Softwarekomponenten angewiesen ist. „Maschine" umfasst hierbei sämtliche physischen Elemente (z. B. Verarbeitungseinheiten, Speicher, Netzwerkausrüstung, Ein-/Ausgabeschnittstellen) und Softwarekomponenten (z. B. Betriebssysteme, Programme, Anweisungen). Gemäß den EU-Leitlinien sind alle KI-Systeme maschinengestützt, da sie für Aufgaben wie Modelltraining, Datenverarbeitung oder automatisierte Entscheidungsfindung auf maschinelle Rechenleistung[2] zurückgreifen.

Prüfungskriterien:

- Läuft das System auf einer Maschine? Überprüfen, ob das System auf physischen Maschinen wie Computern, Servern oder ähnlichen Hardwarekomponenten betrieben wird. Berücksichtigen, dass auch nicht-traditionelle Ansätze (z. B. biologische/chemische Systeme) maschinengestützt sein können, wenn sie für KI relevante Rechenkapazitäten bereitstellen.

- Ausschluss biologischer oder chemisch-basierter Systeme: Sicherstellen, dass das System nicht lediglich biologische Strukturen oder chemische Prozesse ohne KI-relevante Rechenleistung einsetzt (z. B. Prothesen, Implantate oder andere rein passive Komponenten). Nur dann ist ein Ausschluss gerechtfertigt.

2. Gewisser Grad an Autonomie

Definitionsvorschlag: KI-Systeme sind mit verschiedenen Graden der Autonomie ausgestattet, was bedeutet, dass sie bis zu einem gewissen Grad unabhängig von menschlichem Zutun agieren und in der Lage sind, ohne menschliches Eingreifen zu arbeiten. Damit reicht das Spektrum von Systemen, die manuelle Eingaben benötigen, bis hin zu solchen, die völlig selbstständig arbeiten. Systeme, die ausschließlich mit vollständiger manueller Steuerung funktionieren und keine eigenständige Ausgabe erzeugen können, sind ausgeschlossen.

Die Definition basiert auf Erwägungsgrund 12, Leitlinien der EU Kommission sowie den Ausführungen aus der ISO 22989, die ein Spektrum von vollständiger menschlicher Kontrolle bis hin zu vollständig autonomen Systemen definiert.

Prüfungskriterien:

- **Entscheidungsfähigkeit ohne ständiges menschliches Eingreifen**: Überprüfen, ob das System eigenständig Entscheidungen treffen oder Handlungen durchführen kann. Bestimmen Sie zudem, in welchem Automatisierungsgrad das System operiert (0 bis 6), basierend auf der bereitgestellten Einstufungstabelle i.S.d. ISO-Vorgaben.

- **Ausschluss rein manueller Systeme[3]**: Systeme, die ausschließlich durch vollständige manuelle Steuerung funktionieren und keinerlei eigenständige (teil-)autonome Aktivitäten erlauben, sind ausgeschlossen.

[2] Abgrenzung: Auch neuartige Technologien (z. B. Quantencomputer) sowie biologische oder chemisch-basierte Systeme (z. B. neuromorphe Computer, DNA-Computing, molekulare Computer) können maschinengestützt sein, sofern sie eigenständige Rechenkapazität bereitstellen.

[3] Europäische Kommission, C(2025) 924 final, ANNEX zur Mitteilung an die Kommission – Genehmigung des Inhalts des Entwurfs einer Mitteilung der Kommission: Leitlinien der Kommission zur Definition eines KI-Systems gemäß Verordnung (EU) 2024/1689 (KI-Verordnung), Brüssel, 6. Februar 2025, Absatz 17, abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application (zuletzt abgerufen am 07.02.2025)

3. Anpassungsfähigkeit

Definitionsvorschlag: Anpassungsfähigkeit liegt dann vor, wenn sich das System während des Einsatzes durch selbstlernende Fähigkeiten ändert. Dadurch kann[4] das System bei gleichen Eingaben im Laufe der Zeit zu unterschiedlichen Ergebnissen kommen. Dies schließt Lern-, Schlussfolgerungs- und Modellierungsprozesse ein, die über reine Datenverarbeitung hinausgehen. Diese Prozesse können einmalig, periodisch oder kontinuierlich durch Technologien wie maschinelles Lernen umgesetzt werden. Die OECD betont, dass Ableitungen sowohl in der Entwicklungs- als auch in der Betriebsphase eines KI-Systems relevant sind. Dies schließt die kontinuierliche Optimierung durch maschinelles Lernen ein.

Prüfungskriterien:

- **Weiterentwicklung nach Einführung**: Überprüfen, ob das System sich nach der Einführung weiterentwickeln und an veränderte Bedingungen anpassen kann.
- **Nutzung von maschinellem Lernen oder anderen Lernprozessen**: Feststellen, ob das System maschinelles Lernen oder ähnliche Prozesse zur Optimierung seines Verhaltens nutzt.
- **Unterscheidung von statischen Systemen**: Sicherstellen, dass das System Lernprozesse durchläuft und nicht ausschließlich auf festen Regeln basiert.

4. Ziele

Definitionsvorschlag: Das System arbeitet auf explizite oder implizite Ziele hin. Explizite Ziele[5] sind im System design oder -code direkt festgelegt, etwa durch Optimierungen (z. B. Kostenfunktionen, Wahrscheinlichkeiten). Implizite Ziele ergeben sich aus dem Verhalten oder den zugrunde liegenden Annahmen des Systems, z. B. aus Trainingsdaten oder der Interaktion mit der Umgebung.

Prüfungskriterien:

- **Existenz von expliziten oder impliziten Zielen**: Überprüfen, ob das System auf klar definierte (explizite) oder implizite Ziele hin arbeitet: Unterscheiden, ob die Ziele fest im Code verankert sind oder sich aus dem erlernten Verhalten und den zugrunde liegenden Daten ergeben.
- **Eigenständige Zielverfolgung (implizite Ziele):** Feststellen, ob das System in der Lage ist, eigenständig neue Ziele innerhalb eines vorgegebenen Rahmens zu verfolgen. Implizite Ziele sind nicht ausdrücklich definiert, sondern ergeben sich aus dem Verhalten oder den Grundannahmen des Systems[6]. Sie können beispielsweise aus den Trainingsdaten oder aus der Interaktion mit der Umgebung hervorgehen.

> **Exkurs: Unterschied zwischen „Ziel" und „Zweck"**
> Das Ziel i.S.d. Art. 3 Nr. 1 KI-VO beschreibt, was das KI-System intern erreichen will (z. B. eine hohe Genauigkeit bei der Beantwortung von Anfragen). Der Zweck i.S.d. Art. 3 Nr. 12 KI-VO umfasst, warum und wie das KI-System in einem bestimmten Kontext eingesetzt wird, und bezieht sich auf den äußeren Einsatzrahmen (z. B. die Unterstützung einer Abteilung im Unternehmen).

[4] Da der Gesetzestext ausdrücklich „kann" verwendet, ist die Fähigkeit zur automatischen Anpassung fakultativ: Ein KI-System kann, muss jedoch nicht zwangsläufig, selbstlernende Funktionen aufweisen, um als KI-System eingestuft zu werden (Siehe hierzu auch Erwägungsgrund 12 sowie die Absätze 22 und 23 der Leitlinien der Kommission zur Definition eines KI-Systems vom 06.02.2025

[5] Siehe hierzu auch Absatz 24 der Leitlinien der Kommission zur Definition eines KI-Systems vom 06.02.2025

[6] Siehe hierzu auch Absatz 24 der Leitlinien der Kommission zur Definition eines KI-Systems vom 06.02.2025

5. Ableitungsfähigkeit

Definitionsvorschlag: Die Fähigkeit beinhaltet, eigenständig Schlussfolgerungen aus analysierten Datenmengen zu ziehen, um Vorhersagen zu treffen, Entscheidungen zu fällen oder Handlungsempfehlungen zu geben. Dies schließt sowohl maschinelles Lernen als auch logik- und wissensbasierte Ansätze ein. Gleichzeitig ist die Ableitung nicht auf eine bestimmte Entwicklungs- oder Betriebsphase beschränkt, sondern umfasst den gesamten Lebenszyklus eines KI-Systems. Systeme, die ausschließlich auf von Menschen vorgegebenen (statischen) Regeln basieren und keinerlei eigenständige Inferenzprozesse aufweisen, fallen nicht unter das Merkmal „Ableitungsfähigkeit" eines KI-Systems.

Prüfungskriterien:

- **Eigenständiges Ziehen von Schlussfolgerungen**: Überprüfen, ob das System Ergebnisse wie Vorhersagen, Entscheidungen oder Empfehlungen selbst aus den verfügbaren Daten/Eingaben ableitet.
- **Hilfe: Nutzung von fortgeschrittenen KI-Techniken**: Prüfen, ob das System KI-spezifische Verfahren (z. B. maschinelles Lernen, wissensbasierte Inferenz) verwendet, um eigenständig Schlüsse zu ziehen. Lesen Sie hierzu die KI-Techniken-Tabelle (Abgrenzungsfälle KI-System) zur leichteren Orientierung.
- **Ableitung in Entwicklungs- und Betriebsphase**: Verifizieren, ob das System in der Aufbauphase Modelle oder Algorithmen generiert/verfeinert und in der Nutzungsphase Outputs daraus folgert.
- **Abgrenzung: Überlegenheit gegenüber regelbasierten Systemen**: Bestätigen, dass das System über die bloße Anwendung vordefinierter Regeln hinausgeht und flexibel auf neue Eingabedaten reagiert. Sofern keinerlei Fähigkeit zur Ableitung von Ergebnissen aus Daten besteht und das System ausschließlich statisch reagiert, kann es nicht als KI-System im Sinne dieser Vorschrift angesehen werden.

6. Ausgaben

Definitionsvorschlag: Ein KI-System erzeugt Ergebnisse, die physische oder virtuelle Umgebungen beeinflussen können. Die Ausgaben lassen sich in vier große Kategorien einteilen: Vorhersagen (z. B. Schätzung unbekannter Werte auf Basis komplexer Muster), Inhalte (z. B. generierte Texte, Bilder, Videos oder Musik), Empfehlungen (z. B. Vorschläge für bestimmte Aktionen oder Entscheidungen), Entscheidungen (z. B. automatisierte Schlussfolgerungen ohne menschliches Eingreifen). Diese Fähigkeit, komplexe Beziehungen und Muster in den Eingabedaten zu verarbeiten und eigenständig Ergebnisse zu liefern, unterscheidet KI-Systeme grundlegend von anderer Software.

Prüfungskriterien: Vorliegen mindestens einer der vier Ausgabekategorien

- Liegt einer der Ausgabeformen vor? Überprüfen, ob das System Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generiert.
- Feststellen, ob die erzeugten Ergebnisse direkt oder indirekt (z. B. in anderen algorithmischen Prozessen) Veränderungen hervorrufen können.

7. Umweltwirkung

Definitionsvorschlag: Fähigkeit, durch Entscheidungen direkte Auswirkungen auf reale oder virtuelle Umgebungen zu haben. Dadurch ist das System in der Lage, seine Umgebung zu verändern oder zu gestalten, sei es durch physische Aktionen in der realen Welt, wie Fahrzeugsteuerung, oder durch Entscheidungen in simulierten, virtuellen Kontexten, wie Chatsysteme oder softwaregestützte Prozessketten. Dies schließt auch Systeme ein, die menschliche Sinnesorgane und kognitive Prozesse beeinflussen, ohne direkt mechanische oder digitale Umgebungen zu verändern.

Prüfungskriterien:

- **Physische Umweltwirkung**: Überprüfen, ob das System physische Umgebungen beeinflusst, z.B. durch Aktivierung von Aktoren, die mechanische Reaktionen auslösen (z.B. autonome Fahrsysteme). Berücksichtigen, ob das System menschliche Sinnesorgane oder kognitive Prozesse durch seine Ausgaben beeinflusst (z.B. Expertensysteme über Displays).
- **Digitale Umweltwirkung**: Feststellen, ob die Ausgaben des Systems als Eingabedaten für andere algorithmische Systeme oder Prozesse dienen. Übt das System direkte Auswirkungen auf physische Umgebungen aus (z.B. durch Aktivierung von Aktoren)? Beeinflusst das System digitale Umgebungen, indem seine Ausgaben als Eingabedaten für andere Systeme dienen?

Dokumentierter Prüfbericht (Kurzfassung)
nach Art. 6 Abs. 4 KI-VO analog

KI-System: _____
Version: _____
Datum: _____
Verantwortlich: _____

1 Einleitung

Ziel dieses Kurzberichts ist die kompakte Einordnung des KI-Einsatzes nach der KI-Verordnung.

2 Kurzbeschreibung des Sachverhalts

_____
_____
_____
_____
_____

3 Vorprüfung – Bereichsausnahmen

Prüfungspunkt	Ergebnis	Status
Bereichsausnahmen	Nicht einschlägig	☐

4 Eröffnung Anwendungsbereich Art. 2 KI-VO

Prüfungspunkt	Ergebnis	Status
Sachlicher Anwendungsbereich	KI-System i.S.d. Art. 3 Nr. 1 KI-VO	☐
Persönlicher Anwendungsbereich	Betreiber i.S.d. Art. 3 Nr. 4 KI-VO eindeutig	☐
Räumlicher Anwendungsbereich	Nutzung in der EU eröffnet	☐

5 Zweckbestimmung

Element	Bewertung
Begriffseinführung	
Allgemeine Klassifizierung	
Spezifischer Zweck	
Betriebsbedingungen	

6 Risikoklassifizierung

6.1 Verbotene Praktiken (Art. 5 KI-VO)

Verbotene Praktik	Ergebnis	Status
Vulnerabilität / Schutzbedürftigkeit		☐
Manipulation / Unterschwellige Beeinflussung		☐
Social Scoring		☐
Emotionserkennung		☐
Ungezielte Sammlung von Gesichtsbildern		☐
Biometrische Kategorisierung		☐
Echtzeit-Fernidentifizierung		☐

6.2 Hochrisiko-Prüfung (Art. 6 i.V.m. Anhang I & III KI-VO)

6.2.1 Anhang I – Produktsicherheitsgesetz

Produktsicherheitsgesetz	Ergebnis
Medizinprodukt / Fahrzeuge / Aufzüge / Spielzeug etc.	

6.2.2 Anhang III – Hochrisiko-Anwendungen

Hochrisiko-Anwendungen	Ergebnis
Biometrie	
Bildung	
Beschäftigung / HR	
Zugang zu Leistungen	
Strafverfolgung	
Migration / Asyl	
Demokratische Prozesse	

6.2.3 Kundenprofiling

Merkmale	Ergebnis
Betrugswahrscheinlichkeit	
Verhaltensvorhersage	
Kreditwürdigkeit	
Soziale Einstufung	
Emotionserkennung	
Psychologische oder wirtschaftliche Profilbildung	

Operative Umsetzung der Betreiberpflichten im Unternehmen

bei Hochrisiko KI-Systemen

Technische Maßnahmen

		OPERATIVE UMSETZUNG								
		FREQUENZ		FACHLICHER ANSPRUCH KI-KOMPETENZ (1-5)			ZEITLICHER AUFWAND (1-5)	VERANTWORTLICHKEIT (RACI)		
		0	7							
PFLICHT	TÄTIGKEIT	EINMALIG	REGELMÄßIG	TECHNISCH	RECHTLICH	ORGANI-SATORISCH		IT	RECHT & COMPLIANCE	BUSINESS UNIT
Konformitätspflichten										
Bereitsstellung eines Datenqualitäts-Managementsystems gem. Art 10 KI-VO, ErwG 67										
Verwendung des KI-Systems gem. Gebrauchsanweisung i.S.d. Art. 26 Abs. 1,5 KI-VO, ErwGr 91	Sicherstellung der Anwendung gemäß Gebrauchsanweisung		x	2	1	2	2	I	A	R
Überwachungspflichten										
Überwachung der Funktionsweise der KI-Systeme (i.S.d. ErwGr 91)	Einrichtung eines Monitoring-Systems zur Dokumentation der Funktionsweise		x	4	3	3	4	A	C	C
Eingabedaten (Kontrolle auf Zweckkonformität) i.S.d. Art. 26 Abs. 4 KI-VO	Einführung einer Überprüfung der Eingabedaten auf Zweckkon-formität		x	3	3	3	3	A	C	C
Pflicht zur Überwachung des Betriebs des Hochrisiko-KI-Systems gemäß Betriebsanleitung (Art. 26 Abs. 5 1. HS KI-VO)	Überwachung des Betriebs des KI-Systems gemäß der Gebrauchsanweisung		x	2	2	3	3	A	C	R
Pflicht zur Verwendung der KI-Systeme gemäß Betriebsanleitungen (Art. 26 Abs. 1 KI-VO)	Überwachung der Anwendung entsprechend der Gebrauchsan-weisung		x	2	3	3	2	A	C	R
Aufzeichnungspflichten										
Aufzeichnungspflicht (i.S.d. ErwGr 91)	Protokollierung aller relevanten Systemereignisse		x	2	1	2	2	A	C	C
Aufbewahrungspflicht der Protokolle (i.S.d. ErwGr 26 Abs. 6)	Sicherstellung der langfristigen Aufbewahrung aller Protokolle		x	1	2	2	1	A	I	C

Organisatorische Maßnahmen

		OPERATIVE UMSETZUNG								
		FREQUENZ		FACHLICHER ANSPRUCH KI-KOMPETENZ (1-5)			ZEITLICHER AUFWAND (1-5)	VERANTWORTLICHKEIT (RACI)		
		15	14							
PFLICHT	TÄTIGKEIT	EINMALIG	REGELMÄßIG	TECHNISCH	RECHTLICH	ORGANI-SATORISCH		IT	RECHT & COMPLIANCE	BUSINESS UNIT
Informationspflichten										
Gegenüber den Betroffenen										
Informationspflicht gegenüber den Betroffenen bei der Verwendung von KI-Systemen, die Entscheidungen betreffen oder unterstützen, Art. 26 Abs. 11 KI-VO, ErwGr 93, 171	Erstellung und Verteilung von Informationsmaterialien an Betroffene	x		3	3	4	3	R	A	C
Abgabe einer Erklärung gegenüber den Betroffenen i.S.d. ErwGr 171	Formulierung und Bereitstellung einer verständlichen Erklärung für Betroffene	x	x	3	3	4	2	R	A	C
Unterrichtungspflicht gegenüber den Betroffenen i.S.d. ErwGr 93	Etablierung eines standardisier-ten Verfahrens zur Unterrichtung von Betroffenen		x	4	4	5	4	I	A	R
Einholung einer Einwilligung bei Tests unter realen Bedingungen außerhalb von KI-Reallaboren gem. Art. 61 Abs. 1 KI-VO	Sicherstellung der Einwilligungs-erfassung und -dokumentation		x	3	4	4	3	R	C	A
Gegenüber dem Anbieter										
Informieren des Anbieters gem. Art 72, 73 KI-VO	Regelmäßige Berichterstattung an Anbieter gemäß Vorgaben		x	4	3	4	4	R	A	C
Pflicht zur Information des Anbieters im Rahmen der Beobachtung gemäß Art. 26 Abs. 5 S.1 i.V.m. Art. 72 Abs. 2 KI-VO	Einführung eines Systems zur Information des Anbieters	x		4	3	4	4	R	A	C
Gegenüber den Mitarbeitern										
Pflicht zur Information der Mitarbeiter über eingesetzte KI-Systeme gemäß Art. 26 Abs. 7 KI-VO, ErwGr 93	Einführung von regelmäßigen Informationsveranstaltungen für Mitarbeiter		x	3	3	4	3	I	A	R
Pflicht zur unverzüglichen Information der Akteure / Behörde bei Feststellung eines schwerwiegenden Vorfalls (Art. 26 Abs. 5 S. 3 KI-VO)	Einführung eines Notfall-meldesystems für Vorfälle	x		4	5	4	4	R	A	C
Pflicht zur Erfüllung der Registrierungspflichten gemäß Art. 49 EU-Organe und Einrichtungen (Art. 26 Abs. 8 S.1 KI-VO)	Sicherstellung der Registrierung aller eingesetzten Systeme bei zuständigen Behörden	x		3	5	4	3	R	A	C
Dokumentationspflichten										
Abschluss einer schriftl. Vereinbarung mit dem Anbieter i.S.d. ErwGr 88	Erstellung und Abschluss von Vereinbarungen mit dem Anbieter bezüglich Systemnutzung	x		4	5	4	4	I	A	R
Registrierungspflichten										
Registrierungspflicht in der EU-Datenbank i.S.d. Art. 49 Abs. 3 KI-VO	Durchführung der Registrie-rung für neu hinzukommende Systeme		x	3	4	4	3	R	A	C
Pflichten zur Einrichtung von Managementsystemen										
Risikomanagement										
Bereitsstellen eines Risikomanagementsystems gem. Art. 8 Abs. 1 S.2 i.V.m. Art. 9 KI-VO	Regelmäßige Überprüfung und Anpassung des Risikomanage-mentsystems		x	4	4	5	5	R	A	C
Ermittlung und Analyse der Risiken, die bei bestim-mungsgemäßer Verwendung ausgehen können, Art. 9 Abs. 2 a.), 3 KI-VO	Durchführung von Risikobewer-tungen zur Analyse potenzieller Gefährdungen		x	4	4	5	4	R	A	C
Pflicht zur Abschätzung und Bewertung der Risiken gem. Art. 9 Abs. 2 b.), 3, 9 KI-VO	Entwicklung eines Verfahrens zur systematischen Bewertung der identifizierten Risiken	x		5	4	5	4	R	A	C
Pflicht zur Bewertung von Risiken auf Grundlage der Auswertung der Daten aus dem Beobachtungssystem (Art. 72 KI-VO) gemäß Art. 9 Abs. 2 c.), 3 KI-VO	Implementierung eines Proze-sses zur regelmäßigen Überprü-fung der Risikodaten		x	4	4	5	5	R	A	C
Pflicht zur Ergreifung geeigneter Maßnahmen zur Risi-kobewältigung gemäß Art. 9 Abs. 2 d.), 4, 5 KI-VO	Entwicklung von Strategien zur Risikominimierung und Doku-mentation der Maßnahmen	x		4	4	5	5	R	A	C
Pflicht zur Testung zur Ermittlung der am besten geeig-neten Risikomanagementmaßnahmen, Art. 26 Abs. 6, 8 KI-VO)	Durchführung von Tests zur Evaluierung der Wirksamkeit der Risikomanagementmaßnahmen		x	4	4	4	4	R	A	C
Datenqualitätsmanagement										
Bereitsstellung eines Datenqualitätsmanagement-systems gem. Art 10 KI-VO	Einführung eines Systems zur Sicherstellung der Datenqualität	x		4	3	4	4	R	A	C
Pflicht zur Sicherstellung, dass kontrollierbare Eingabe-daten zweckentsprechend und repräsentativ sind (Art. 26 Abs. 4 KI-VO)	Implementierung von Prozessen zur Validierung und Sicherstel-lung der Eingabedatenqualität		x	4	4	4	4	R	A	C
Schulungspflichten										
Sicherstellung der KI-Kompetenz gegenüber Mitarbeitern (i.S.d. Art. 4 KI-VO)	Durchführung regelmäßiger Schulungen und Weiterbildung der Mitarbeiter zur Nutzung von KI-Systemen		x	4	4	4	3	I	A	R
Pflicht zur Übertragung der menschlichen Aufsicht an qualifizierte Personen (Art. 26 Abs. 2 1. HS KI-VO)	Definition der Qualifikationsan-forderungen und Übertragung der Aufsicht an qualifizierte Personen	x		4	3	4	4	I	A	R
Pflicht zur Unterstützung der Aufsichtspersonen (Art. 26 Abs. 2 2. HS KI-VO)	Bereitstellung organisatorischer Unterstützung für Aufsichtsper-sonen	x		2	2	4	3	R	A	C
Aufbewahrungspflichten										
Pflicht zur Aufbewahrung automatisch erzeugter Protokolle für mindestens sechs Monate (Art. 26 Abs. 6 S.1 KI-VO)	Implementierung einer Aufbe-wahrungslösung für Protokolle für mindestens sechs Monate	x		3	2	4	3	R	A	C
Pflichten gegenüber Behörden										
Pflicht zur Zusammenarbeit mit den Behörden (Art. 26 Abs. 12 KI-VO)	Sicherstellung der Zusammen-arbeit mit den zuständigen Behörden im Rahmen von Audits und Inspektionen		x	3	3	4	4	R	A	C
Unterrichten der zuständigen Marktüberwachungs-behörde (Art. 27 Abs. 3 KI-VO, ErwGr 96)	Einrichtung eines Kommunikati-onskanals zur Benachrichtigung der Marktüberwachungsbehörde	x		4	4	4	4	R	A	C
Informieren der Marktüberwachungsbehörde gem. Art. 79 Abs. 1 KI-VO	Einführung eines Prozesses zur regelmäßigen Berichterstattung an die Marktüberwachungs-behörde		x	3	3	4	3	R	A	C
Pflicht zur Durchführung von Risikoabschätzungen										
Pflicht zur Durchführung einer Datenschutzfolgenab-schätzung i.S.d. Art. 26 Abs. 9 KI-VO	Durchführung einer umfassenden Datenschutzfolgenabschätzung zur Bewertung der Auswirkungen auf den Datenschutz	x		5	5	5	5	R	A	C
Durchführung einer Grundrechte-Folgenabschätzung (Art. 27 KI-VO, ErwGr 96)	Durchführung einer Grundrechte-Folgenabschätzung	x		5	5	5	5	R	A	C

KI-Systeme mit geringem Risiko

Pflichten für Anbieter und Betreiber

Technische Maßnahmen	OPERATIVE UMSETZUNG											
	ANBIETER VON KI-SYSTEM MIT GERINGEM RISIKO	BETREIBER VON KI-SYSTEM MIT GERINGEM RISIKO	TÄTIGKEIT	FREQUENZ		FACHLICHER ANSPRUCH KI-KOMPETENZ (1-5)			ZEITLICHER AUFWAND (1-5)	VERANTWORTLICHKEIT (RACI)		
PFLICHT	10	5		EINMALIG	REGELMÄßIG	TECHNISCH	RECHTLICH	ORGANI-SATORISCH		IT	RECHT & COMPLIANCE	BUSINESS UNIT
Kennzeichnungspflichten												
Anbieter von KI-Systemen zur Erzeugung synthetischer Inhalte (Audio-, Bild-, Video- oder Textinhalte) müssen sicherstellen, dass die Ausgaben maschinenlesbar gekennzeichnet und als künstlich erkennbar sind (Art. 50 Abs. 2,5 KI-VO, ErwGr 132)	x	x	Implementierung eines automatischen Systems zur Einfügung von Metadaten, die den Inhalt als KI-generiert auszeichnen. Diese Metadaten sollten maschinenlesbar und schwer entfernbar sein.	x	x	5	1	3	4	R	A	C
Organisatorische Maßnahmen												
Informationspflichten												
Anbieter müssen sicherstellen, dass mit Menschen interagierende KI-Systeme entsprechend informieren können (Art. 50 Abs. 1,5 KI-VO, ErwGr 132)	x		Sicherstellung der Bereitstellung relevanter Benutzerinformationen über interaktive KI.		x	3	4	5	3	R	A	C
Besondere Transparenzpflichten bei Gefahr des Identitätsbetrugs, Täuschung, Deepfakes i.S.d. ErwGr 132	x	x	Einführung von Maßnahmen zur Erkennung und Information über Deepfakes.		x	5	2	5	4	R	A	C
Betreiber von Emotionserkennungs- oder biometrischen Kategorisierungssystemen müssen betroffene Personen informieren und rechtskonform verarbeiten (Art. 50 Abs. 3,5 KI-VO).		x	Sicherstellung, dass betroffene Personen rechtzeitig informiert werden.		x	3	5	4	3	R	A	C
Dokumentationspflichten												
Erstellung von Verhaltenskodizes (ErwGr 165)	x		Entwicklung von Leitlinien zur ethischen Nutzung von KI.	x		2	5	4	4	I	A	R
Bereitstellen von Modellkarten (Zweck, Leistung, Trainingsdaten) (ErwGr 165)	x		Erstellung und Aktualisierung von Modellkarten mit allen erforderlichen Details.		x	5	2	4	4	A	C	C
Bereitstellen von Datenkarten (Herkunft, Zusammensetzung, Verarbeitungsschritte der Daten) (ErwGr 165)	x		Erstellung und Verwaltung von Datenkarten zur Transparenz.		x	5	2	4	4	A	C	C
Organisatorische Dokumentation												
Dokumentation der Entscheidung KI-System ist nicht hochrisikobehaftet (Art. 6 Abs. 4 KI-VO, ErwGr 65)	x		Dokumentation der Entscheidung über das Risikoprofil des KI-Systems.		x	3	5	3	3	R	A	C
Abschluss einer schriftl. Vereinbarung mit dem Betreiber i.S.d. ErwGr 88	x	x	Erstellung und Abschluss einer schriftlichen Vereinbarung mit den Betreibern.		x	2	5	3	3	I	C	A
Registrierungspflichten												
Registrierungspflicht in der EU-Datenbank i.S.d. Art. 6 Abs. 4 i.V.m. 49 Abs. 2 KI-VO	x		Sicherstellung der Registrierung aller KI-Systeme in der EU-Datenbank.	x		2	3	5	3	I	A	R
Schulungspflichten												
Sicherstellung der KI-Kompetenz gegenüber Mitarbeitern (i.S.d. Art 4 KI-VO)	x	x	Durchführung regelmäßiger Schulungen und Weiterbildung der Mitarbeiter zur Nutzung von KI-Systemen.		x	5	5	5	3	I	A	R

Auslegungshilfe zu Art. 3 (1) KI-VO zu der Voraussetzung „Autonomiegrad“

Bei der Voraussetzung „to operate with varying levels of autonomy“ gemäß Art. 3 (1) KI-VO stellt sich oft die Frage, wie der Grad der Autonomie zu bewerten ist und inwiefern er ein entscheidendes Kriterium für die Definition und Abgrenzung eines KI-Systems darstellt. KI-Systeme können anhand des Automatisierungsgrads und der externen Kontrolle, der sie unterliegen, kategorisiert werden. Der Grad der Automatisierung erstreckt sich von keiner bis hin zu voller Automatisierung, wobei Autonomie das höchste Niveau darstellt. In der Praxis jedoch bleibt die Unterscheidung zwischen vollautomatisierten Systemen und tatsächlich autonomen Systemen oft unscharf. Während vollautomatisierte Systeme ohne menschliche Eingriffe operieren können, ist die tatsächliche Selbstverwaltung, die für echte Autonomie erforderlich ist, auch in fortgeschrittenen KI-Systemen noch nicht vollständig gegeben. Daher ist der Begriff „autonom“ in diesem Zusammenhang teilweise irreführend, da selbst hochentwickelte KI-Systeme weiterhin stark auf die Programmierung und die Anweisungen ihrer Entwickler angewiesen sind. Diese Unterscheidung sollte bei der Beurteilung des Autonomiegrads und der rechtlichen Einordnung von KI-Systemen berücksichtigt werden.

Automatisierungsgrad	Kommentare
Automatisiertes System	**Autonom 6 - Autonomie** Das System ist in der Lage, sein vorgesehenes Einsatzgebiet oder seine Ziele ohne externe Eingriffe, Kontrolle oder Aufsicht anzupassen.
Heteronom	**5 - Volle Automatisierung** Das System kann seine gesamte Mission ohne externe Eingriffe durchführen. **4 - Hohe Automatisierung** Das System führt Teile seiner Mission ohne externe Eingriffe durch. **3 - Bedingte Automatisierung** Das System erbringt kontinuierlich und spezifisch autonome Leistungen, wobei ein externer Agent bereit ist, bei Bedarf einzugreifen. **2 - Teilautomatisierung** Einige Subfunktionen des Systems sind vollständig automatisiert, während das System weiterhin unter der Kontrolle eines externen Agents bleibt. **1 - Assistenz** Das System unterstützt den Bediener. **0 - Keine Automatisierung** Der Bediener steuert das System vollständig.

Relevante Kriterien zur Klassifizierung

- Das Vorhandensein oder Fehlen externer Überwachung, sei es durch einen menschlichen Bediener („Mensch im Kreislauf“) oder durch ein anderes automatisiertes System.
- Der Grad des situativen Verständnisses des Systems, einschließlich der Vollständigkeit und Operationalisierbarkeit des Modells der Zustände seiner Umgebung sowie der Sicherheit, mit der das System in seiner Umgebung logisch schlussfolgern und handeln kann.
- Der Grad der Reaktionsfähigkeit, einschließlich der Frage, ob das System Veränderungen in seiner Umgebung wahrnimmt, darauf reagiert und zukünftige Veränderungen vorhersehen kann.
- Ob das System bis zum Abschluss einer bestimmten Aufgabe oder bis zum Eintreten eines bestimmten Ereignisses in der Umgebung im Betrieb bleibt (z. B. zur Zielerreichung, bei Zeitüberschreitungen oder anderen Mechanismen).
- Der Grad der Anpassungsfähigkeit an interne oder externe Veränderungen, Bedürfnisse oder Antriebe.
- Die Fähigkeit, die eigene Leistung oder Eignung zu bewerten, einschließlich der Bewertung gegenüber vorgegebenen Zielen.
- Die Fähigkeit, proaktiv in Bezug auf Systemziele, Motivationen und Antriebe zu entscheiden und zu planen.

Auslegungshilfe Art. 25 (1) b.) KI-VO „wesentliche Änderung"

Praktische Relevanz	● ● ● ● ●
Technische Relevanz	● ● ● ○ ○
Rechtliche Relevanz	● ● ● ● ○
Orga.Relevanz	● ● ● ○ ○

Verortung im Prüfungsschema

4. ANWENDUNGSBEREICH GEM. ART. 2 KI-VO ERÖFFNET
    a. Ist der persönliche Anwendungsbereich eröffnet?
        i. Präzisierung der Rolle zum Quasi-Anbieter gem. Art. 25 KI-VO, ErwGr 84
            1. Szenario 1: Name/Handelsmarke
            2. Szenario 2: Wesentliche Änderung gem. Art. 25 I b.) KI-VO
                2.1 KI-Technologie
                    a. Hochrisiko-KI-System
                2.2. Handlung
                    b. Bereits in Verkehr gebracht oder in Betrieb genommen
                → **c. Vornahme einer wesentlichen Änderung**
                    d. Nach wesentlicher Änderung besteht weiterhin ein Hochrisiko-KI-System
            3. Szenario 3: Zweckänderung

Einleitung

Art. 25 der KI-Verordnung stellt eine der wichtigsten Regelungen im Rahmen der Beratung zur KI-Verordnung dar. Im Endeffekt kann er dazu führen, dass die zuvor festgelegte Rolle (Händler, Einführer, Betreiber etc.) zur Rolle eines Anbieters wird, mit all den damit verbundenen Anbieterpflichten. Zusätzlich ist sie strategisch essenziell für die Gestaltung von Geschäftsmodellen von Anbietern, welche auf dem europäischen Markt KI-Technologie platzieren wollen. Neben einem hohen rechtlichen Verständnis ist hier auch technisches Verständnis relevant. Art. 25 KI-VO regelt, unter welchen Bedingungen Händler, Einführer, Betreiber oder sonstige Dritte zu Anbietern eines Hochrisiko-KI-Systems werden können.

Warum gibt es die Regelung

Akteure, die ein Hochrisiko-KI-System auf dem Markt beeinflussen oder verändern, sollen ebenfalls regulatorische Verantwortung übernehmen. Nur durch eine klare Zuweisung der Verantwortlichkeiten entlang der gesamten Wertschöpfungskette können die regulatorischen Anforderungen effektiv umgesetzt (Rechtssicherheit) und die Sicherheit der Nutzer gewährleistet werden. Es ist notwendig, da KI oft nur teilweise von einem einzelnen Unternehmen entwickelt und auf den Markt gebracht wird, während weitere Unternehmen das Modell für spezifische Anwendungen anpassen. Dadurch haben mehrere Akteure entlang der Wertschöpfungskette Einfluss auf die Eigenschaften und Risiken eines KI-Systems. Kein Akteur verfügt über alle erforderlichen Kenntnisse: Der Anbieter weiß nicht, wie das Modell genutzt wird, während Betreiber, Händler und Importeure keine Informationen zu den Trainingsdaten haben. Diese fragmentierte Verantwortung erschwert die Einhaltung der regulatorischen Vorgaben.

Definition

Art. 3 Nr. 23 KI-VO definiert eine wesentliche Änderung folgendermaßen:

> *(…) eine Veränderung eines KI-Systems (…), die in der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems (…) beeinträchtigt wird (…)*

Der Begriff der wesentlichen Änderung entspricht dem aus anderen technischen Regelwerken bekannten Schema, etwa im Medizinprodukterecht, Maschinenrecht oder im Bauproduktenrecht.

Auslegungshilfe – Was könnte eine wesentlich Änderung darstellen?

1. **Änderung des Betriebssystems:** Zum Beispiel der Wechsel von einem proprietären zu einem Open-Source-Betriebssystem. (Siehe ErwGr 128)
2. **Überarbeitung der Softwarearchitektur:** Etwa die Umstellung von einer monolithischen auf eine mikroservicebasierte Architektur. (Siehe ErwGr 128)
3. **Anpassung der Trainingsdaten:** Verwendung neuer Datensätze mit unterschiedlichen demografischen Merkmalen, die nicht in der ursprünglichen Bewertung berücksichtigt wurden.
4. **Änderung des Algorithmus:** Wechsel von einem regelbasierten System zu einem selbstlernenden neuronalen Netzwerk.
5. **Erweiterung des Anwendungsbereichs:** Einsatz des KI-Systems in einer neuen Domäne, z. B. von medizinischer Diagnose zu autonomem Fahren.
6. **Integration externer Komponenten:** Hinzufügen von Drittanbieter-Plugins oder -Modulen, die nicht Teil der ursprünglichen Konformitätsbewertung waren.
7. **Hardware-Upgrade:** Einsatz auf neuer Hardware mit erheblich abweichenden Leistungsmerkmalen, die das Verhalten des Systems beeinflussen können.

Achtung: Ausnahme - selbstlernenden KI-Systemen gemäß Art. 25 Abs. 4 KI-VO

Art. 25 Abs. 4 KI-VO, Erwägungsgrund 128 grenzen jedoch die Veränderungen aus, welche im Voraus vom Anbieter festgelegt und im Rahmen der ursprünglichen Konformitätsbewertung gesehen und bewertet wurden. Das bedeutet, dass dynamische Anpassungen, die der ursprünglichen Spezifikation entsprechen, nicht zwangsläufig eine erneute Bewertung erforderlich machen. Der Begriff der wesentlichen Änderung dient somit dazu, zwischen grundlegenden Modifikationen und vorhergesehenen dynamischen Anpassungen, die im Betrieb des KI-Systems auftreten können, zu unterscheiden.

Checkliste - Feststellung einer wesentlichen Änderung i.S.d. Art. 25 KI-VO

Schritt Nr. 1: Identifikation der Änderung
Was wurde am KI-System geändert? Handelt es sich um Software, Hardware, Daten oder Funktionalität? Siehe hierzu obige sieben genannte Beispiele.

Schritt Nr. 2: Vorhersehbarkeit der Änderung
Wurde die Änderung im Voraus vom Anbieter vorgesehen bzw. wurden diese Änderungen in der ursprünglichen Konformitätsbewertung berücksichtigt?

Schritt Nr. 3: Risikobewertung
Führt die Änderung zu neuen oder erhöhten Risiken für Nutzer oder Betroffene? Wenn ja, besteht die Tendenz zum Vorliegen einer wesentlichen Änderung. (Wenn die Änderung zu einer neuen Art von Risiko führt, das in seiner Natur nicht mehr dem ursprünglichen Risiko entspricht, oder das bereits geprüfte Risikoniveau erheblich erhöht, kann eine wesentliche Änderung angenommen werden.)

Praktische Verbindungen: Verknüpfung mit spezifischen Pflichten

Ein wichtiger praktischer Aspekt des Art. 25 KI-VO ist die Zusammenarbeit zwischen dem ursprünglichen Anbieter und den neuen Anbietern. Der ursprüngliche Anbieter, der das System ursprünglich in Verkehr gebracht hat, verliert die Rolle als Hauptverantwortlicher, ist jedoch verpflichtet, die neuen Anbieter bei der Erfüllung der Pflichten zu unterstützen (Art. 25 Abs. 2). Dies schließt die Bereitstellung aller notwendigen technischen Informationen und Unterstützung ein, die für die Konformitätsbewertung und den sicheren Betrieb erforderlich sind.

Empfehlung

Es wird empfohlen, den Artikel 16 der KI-VO detailliert zu lesen, um ein vollständiges Verständnis der Anbieterpflichten zu erhalten. Ebenso ist der Bezug zu Erwägungsgrund 84 für die Auslegung des Artikels 25 besonders relevant, um zu verstehen, welche spezifischen Bedingungen zur Anwendung der Pflichten führen können.

Auslegungshilfe Finetuning i.R.d. „wesentlichen Änderung“ gem. Art. 25 Abs. 1 KI-VO

Praktische Relevanz	● ● ● ● ●
Technische Relevanz	● ● ● ● ●
Rechtliche Relevanz	● ● ● ○ ○
Orga.Relevanz	● ● ○ ○ ○

Verortung im Prüfungsschema

4. ANWENDUNGSBEREICH GEM. ART. 2 KI-VO ERÖFFNET
    a. Ist der persönliche Anwendungsbereich eröffnet?
        i. Präzisierung der Rolle zum Quasi-Anbieter gem. Art. 25 KI-VO, ErwGr 84
            1. Szenario 1: Name/Handelsmarke
            2. Szenario 2: Wesentliche Änderung gem. Art. 25 I b.) KI-VO
                2.1 KI-Technologie
                    a. Hochrisiko-KI-System
                2.2. Handlung
                    b. Bereits in Verkehr gebracht oder in Betrieb genommen
                → **c. Vornahme einer wesentlichen Änderung**
                    d. Nach wesentlicher Änderung besteht weiterhin ein Hochrisiko-KI-System
            3. Szenario 3: Zweckänderung

Ab wann stellt Finetuning eine wesentliche Änderung gem. Art. 25 Abs. 1 b.) KI-VO dar?

Geringe Eingriffe

(geringe Wahrscheinlichkeit einer wesentlichen Änderung)

Diese Verfahren führen zu einer **geringen Modifikation** des Modells, die entweder nur einzelne Teile des Systems betrifft oder das Basismodell unverändert lässt. Sie fallen eher unter **dynamische Anpassungen,** die im Vorfeld in der Konformitätsbewertung vorgesehen wurden.



Parameter-Efficient Fine-Tuning (PEFT)

Adapter-Tuning

Adapter-Tuning führt zu keiner wesentlichen Änderung der Originalparameter des Modells. Diese Methode ergänzt Adapter-Schichten in das Modell und bleibt im Rahmen dessen, was in der ursprünglichen Konformitätsbewertung bereits vorgesehen war.

LoRA (Low-Rank Adaptation)

LoRA passt die Modellparameter nicht direkt an, sondern fügt zusätzliche Matrizen niedrigeren Rangs ein. Diese Änderungen sind in der Regel als dynamische Anpassungen zu verstehen, die nicht als wesentliche Änderung gelten, sofern sie in der ursprünglichen Konformitätsbewertung vorgesehen wurden.

Moderate Eingriffe

(moderate Wahrscheinlichkeit einer wesentlichen Änderung)

Hier beginnen die Verfahren, **größere Teile des Modells** zu verändern, allerdings oft nur spezifische Bereiche oder Parameter. Diese Änderungen könnten, je nach den vorherigen Annahmen des Konformitätsverfahrens, eine **wesentliche Änderung** darstellen, wenn sie die Sicherheits- oder Leistungsaspekte erheblich beeinflussen.



Layer-Wise Fine-Tuning

Beim Layer-Wise Fine-Tuning werden einige Modellschichten vollständig trainiert, während andere unverändert bleiben. Ob diese Methode eine wesentliche Änderung darstellt, hängt davon ab, ob die Schichtanpassungen und die damit verbundenen Risiken im ursprünglichen Konformitätsbewertungsverfahren vorgesehen waren. Eine Risikobewertung sollte vorgenommen werden, um neue oder erhöhte Risiken zu identifizieren.

Tiefe Eingriffe

(hohe Wahrscheinlichkeit einer wesentlichen Änderung)

Diese Methoden verändern das Modell **in seinem Kern** und betreffen alle Parameter oder weite Teile des Systems. Hier ist es sehr wahrscheinlich, dass eine **wesentliche Änderung** vorliegt, die eine **erneute Konformitätsbewertung** erfordert.



Vollständiges Fine-Tuning

Beim vollständigen Fine-Tuning wird das gesamte Modell, einschließlich aller Parameter, weitertrainiert. Dies stellt in der Regel eine wesentliche Änderung dar, insbesondere wenn diese Modifikationen zu neuen Risiken führen oder nicht in der ursprünglichen Konformitätsbewertung vorgesehen waren. Eine erneute Konformitätsbewertung ist in diesem Fall erforderlich.

Eingriffsintensität

Schlüsselfaktoren für die Bewertung einer wesentlichen Änderung auf Metaebene

Umfang der Parameteränderung

Je mehr grundlegende Parameter oder Schichten eines Modells angepasst werden, desto wahrscheinlicher ist es, dass eine wesentliche Änderung des KI-Modells vorliegt.

Vorhersehbarkeit der Änderung

Wenn die Änderungen bereits im ursprünglichen Konformitätsbewertungsverfahren vorgesehen waren, können auch tiefgreifende Änderungen unter bestimmten Umständen als dynamische Anpassungen gelten, die keine erneute Bewertung erfordern.

Risikobewertung

Änderungen, die neue oder erhöhte Risiken für Nutzer oder betroffene Gruppen mit sich bringen, erhöhen die Wahrscheinlichkeit, dass eine wesentliche Änderung vorliegt. Dies ist insbesondere bei tiefgreifenden Modifikationen (z. B. Full Finetuning) relevant.

Technische und organisatorische Komplexität

Je stärker die Änderung in die Architektur des KI-Systems eingreift (z. B. durch Layer-Wise Fine-Tuning oder Full Finetuning), desto eher wird eine wesentliche Änderung anzunehmen sein, insbesondere, wenn neue Daten oder Algorithmen eingeführt werden.

Für vertiefte Informationen beachte bitte die Auslegungshilfe Art. 25 (1) b.) KI-VO „wesentliche Änderung"

Auslegungshilfe „freie und quelloffene KI-Technologie“

i.S.d. Art. 2 Abs. 12 KI-VO, Art. 52 Abs. 2 KI-VO, ErwGr 102, 103

Praktische Relevanz	● ● ● ● ●
Technische Relevanz	● ● ● ○ ○
Rechtliche Relevanz	● ● ● ● ○
Orga.Relevanz	● ● ● ● ○

Verortung im Prüfungsschema

I. VORPRÜFUNG – BEREICHSAUSNAHMEN
- A. Haushaltsausnahme gemäß Art. 2 Abs. 10 KI-VO
- B. Wissenschaftsprivileg gemäß Art. 2 Abs. 6 KI-VO
- C. Forschungs- und Entwicklungsprivileg gemäß Art. 2 Abs. 8 KI-VO
- → **D. Freie und quelloffene KI-Technologien i.S.d. Art. 2 Abs. 12, 53 Abs. 2 KI-VO, ErwGr 102, 103**
  - 1. Wird die KI-Technologie unter einer freien und quelloffenen Lizenzen bereitgestellt?
    - a) Voraussetzungen bei KI-Systemen i.S.d. Art. 2 Abs. 12 KI-VO
    - b) Voraussetzungen bei KI-Modellen i.S.d. Art. 53 Abs. 2 KI-VO

II. KI-TECHNOLOGIE

Inhalt

1. Einleitung
2. Warum gibt es die Regelung
3. Definitionen
    a. Definitionsansätze zu „freie und quelloffene Lizenzen“ nach Art. 2 Abs. 12 KI-VO
    b. Definitionsansätze zu „freie und quelloffene Lizenzen“ nach Art. 53 Abs. 2 KI-VO
4. Checkliste I – Feststellung der Ausnahme nach Art. 2 Abs. 12 KI-VO (KI-Systeme)
5. Checkliste II – Feststellung der Teilausnahme nach Art. 53 Abs. 2 KI-VO (KI-Modelle)

Einleitung

Wird KI-Technologie unter einer freien und quelloffenen Lizenz bereitgestellt, kann dies dazu führen, dass die KI-Verordnung gar nicht oder nur teilweise angewendet wird. Hierbei kommt es darauf an, um welche Art von KI-Technologie es sich handelt. Wird ein KI-System unter einer freien und quelloffenen Lizenz bereitgestellt, kann gemäß Art. 2 Abs. 12 der KI-Verordnung der sachliche Anwendungsbereich gar nicht eröffnet werden, und die KI-Verordnung findet keine Anwendung. Wird hingegen ein KI-Modell unter einer freien und quelloffenen Lizenz bereitgestellt, kann eine Teil-Ausnahme gemäß Art. 53 Abs. 2 der KI-Verordnung vorliegen.

Es ist daher sinnvoll, sich den Begriff „freie und quelloffene Lizenz“ sowie die entsprechenden Voraussetzungen genauer anzuschauen: Wann gilt eine KI-Technologie als frei und quelloffen, und wann wird sie unter einer solchen Lizenz bereitgestellt? Natürlich gibt es hier auch viele Ausnahmen von der Ausnahme.

In der vorliegenden Auslegungshilfe versuchen wir, neben einem ersten Definitionsvorschlag auch die verschiedenen Prüfungsschritte im Rahmen von zwei Checklisten darzustellen.

Warum gibt es die Regelung

Die Voll- und Teil-Ausnahmen sollen die freie Forschung und Entwicklung fördern und Europa als Standort für innovative digitale Technologien stärken. Freie und quelloffene Software trägt erheblich zum Bruttoinlandsprodukt der EU bei und bietet wesentliche Wachstumsmöglichkeiten für die europäische Wirtschaft. Durch die Ausnahme wird sichergestellt, dass die Entwicklung und Bereitstellung solcher KI-Systeme nicht durch regulatorische Pflichten behindert wird.

Definition

Der Begriff „freie und quelloffene Lizenzen“ wird in der KI-VO nicht definiert, obwohl er an verschiedenen Stellen – siehe Art. 2 Abs. 12, 53 Abs. 2 KI-VO – erhebliche Bedeutung erlangt. Dies führt zu erheblichen Unsicherheiten im Begriffsverständnis. Im Folgenden werden verschiedene Definitionsansätze zu KI-Modellen sowie in Bezug auf KI-Systeme dargestellt:

Definitionsansätze zu „freie und quelloffene Lizenzen“ nach Art. 2 Abs. 12 KI-VO

Die Digitale-Inhalte-Richtlinie (Digitale-Inhalte-RL) definiert eine freie und quelloffene Lizenz für Software als eine Lizenz, bei der der Verbraucher keinen Preis zahlt und die bereitgestellten personenbezogenen Daten ausschließlich zur Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software verarbeitet werden. Gemäß den Erwägungsgründen der Produkthaftungs-Richtlinie 2024 (Produkthaftungs-RL 2024) liegt freie und quelloffene Software vor, wenn sie außerhalb einer kommerziellen Tätigkeit entwickelt oder bereitgestellt wird und per Definition nicht in Verkehr gebracht wird. Nach Erwägungsgrund 10 des Cyber Resilience Act (CRA) gilt Software als frei und quelloffen, wenn sie außerhalb einer Geschäftstätigkeit entwickelt oder bereitgestellt wird und somit nicht unter die Verordnung fällt. Dies betrifft insbesondere Software, die offen geteilt, frei zugänglich, nutzbar, veränderbar und weiterverteilbar ist, einschließlich ihres Quellcodes und veränderter Versionen.

Die Erwägungsgründe 102 und 103 der KI-VO definieren die Begriffe „frei“ und „quelloffen“:

- **„Frei“** bedeutet, dass keine Monetarisierung stattfindet. Monetarisierung liegt vor, wenn KI-Systeme gegen Bezahlung bereitgestellt werden oder wenn für technische Unterstützung oder andere Dienste ein Preis verlangt wird. Auch die Verarbeitung personenbezogener Daten über die Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität hinaus gilt als Monetarisierung.
- **„Quelloffen“** bedeutet, dass die Parameter, einschließlich Gewichte, Modellarchitektur und Informationen über die Modellnutzung, öffentlich zugänglich sind. Die Lizenz muss die Nutzung, Änderung und Weitergabe des KI-Systems erlauben.

Definitionsvorschlag

Freie und quelloffene Lizenzen im Sinne der KI-Verordnung sind Lizenzen, unter denen KI-Systeme veröffentlicht werden, die die Nutzung, Änderung und Weitergabe des Systems erlauben. Die Parameter des KI-Systems, wie Gewichte, Modellarchitektur und Informationen über die Modellnutzung, sind öffentlich zugänglich. Es findet keine Monetarisierung statt: Weder wird für das KI-System oder damit verbundene Dienstleistungen ein Preis verlangt, noch werden personenbezogene Daten über die Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität hinaus verarbeitet.

Definitionsansätze zu „freie und quelloffene Lizenzen“ nach Art. 53 Abs. 2 KI-VO

Die Kennzeichen einer freien und quelloffenen Lizenz gemäß Art. 53 Abs. 2 KI-VO sind die öffentliche Zugänglichkeit aller Parameter — Gewichte, Modellarchitektur und Informationen über die Modellausführung müssen öffentlich zugänglich gemacht werden — mit dem Ziel einer vollständigen Offenlegung, um eine breite Weiterentwicklung und Verwendung zu ermöglichen. Jedermann muss ohne Einschränkungen Zugang zum Modell haben und es nutzen sowie ändern können. Erlaubte Einschränkungen wie **Copyleft-Klauseln** sind zulässig, sofern sie die Fortführung des freien und quelloffenen Zugangs sicherstellen; die Bereitstellung über offene Speicher ist unschädlich, und die Finanzierung durch Werbung ist erlaubt. Unzulässige Monetarisierung, wie die Bereitstellung gegen Bezahlung oder andere Formen der Monetarisierung, ist schädlich, außer bei Transaktionen zwischen Kleinstunternehmen; zudem ist die Verarbeitung personenbezogener Daten über die Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität hinaus nicht erlaubt. Bei KI-Modellen mit allgemeinem Verwendungszweck mit systemischen Risiken gilt die Ausnahme nicht, und Anbieter solcher Modelle unterliegen allen Anbieterpflichten, unabhängig von der Lizenzart.

Wichtiger Hinweis: Die Ausnahme bezieht sich **nur** auf die Pflichten zur **technischen Dokumentation** und zu **Transparenzinformationen. Andere Pflichten** wie die **Zusammenarbeitspflicht** und die Pflichten rund um **Urheberrechtstransparenz** und **Trainingsdatenspezifikation** bleiben bestehen. (Sog. Teilausnahme)

Definitionsvorschlag

Eine **freie und quelloffene** Lizenz im Sinne von Art. 53 Abs. 2 KI-VO ist eine Lizenz, die folgende Kriterien erfüllt:

- Vollständige Offenlegung aller Modellparameter, einschließlich Gewichte und Modellarchitektur.
- Uneingeschränkter Zugang, Nutzung und Änderung des Modells für jedermann.
- Keine schädliche Monetarisierung, außer bei bestimmten Transaktionen zwischen Kleinstunternehmen.

Checkliste I – Liegt ein KI-System vor, welches unter einer freien und quelloffenen Lizenz i.S.d. Art. 2 Abs. 12 KI-VO bereitgestellt wird.

Zur besseren Orientierung und für ein formalisiertes Vorgehen wurde die folgende Checkliste entwickelt.

Checkliste – Feststellung der Ausnahme nach Art. 2 Abs. 12 KI-VO

Schritt Nr. 1: Prüfung des Vorliegens eines KI-Systems i.S.d. Art. 3 Nr. 1 KI-VO, ErwGr 12

- [ ] Wird das System durch maschinelle Prozesse betrieben oder unterstützt?
- [ ] Kann das System ohne direkte menschliche Intervention Entscheidungen treffen oder Aktionen ausführen?
- [ ] Ist das System in der Lage, sich an neue Daten oder Umstände anzupassen?
- [ ] Verfolgt das System klar definierte Ziele, die entweder explizit programmiert oder implizit durch Lernprozesse entstanden sind?
- [ ] Kann das System aus Eingabedaten Schlussfolgerungen ziehen oder Vorhersagen treffen?
- [ ] Hat das System die Fähigkeit, seine Umgebung zu beeinflussen, sei es physisch (z. B. durch Robotik) oder virtuell (z. B. durch Softwareinteraktionen)?

Wenn alle diese Fragen mit "Ja" beantwortet wurden, handelt es sich um ein KI-System im Sinne der KI-VO.

Schritt Nr. 2: Kein Inverkehrbringen/ Inbetriebnahme eines risikoreichen KI-Systems i.S.d. Artt. 5,5,50 KI-VO

- [ ] Wird das KI-System im Rahmen einer Geschäftstätigkeit Dritten zur Verfügung gestellt?
- [ ] Wird das KI-System erstmalig vom Anbieter oder Betreiber in der EU verwendet?
- [ ] Handelt es sich um ein Hochrisiko-KI-System gemäß Art. 6 KI-VO?
- [ ] Fällt das KI-System unter die verbotenen Praktiken gemäß Art. 5 KI-VO?
- [ ] Unterliegt das KI-System besonderen Transparenzanforderungen gemäß Art. 50 KI-VO?

Wenn eine oder mehrere dieser Fragen mit "Ja" beantwortet wurden, greift die Ausnahme des Art. 2 Abs. 12 KI-VO nicht, und das KI-System unterliegt den Bestimmungen der KI-Verordnung.

Schritt Nr. 3: Veröffentlichung unter freien und quelloffenen Lizenzen

- [ ] Wurde das KI-System der Öffentlichkeit zugänglich gemacht?

Erläuterung: Diese Frage stellt sicher, dass das KI-System frei und offen verfügbar ist und nicht nur einem geschlossenen Kreis zugänglich gemacht wird. Nur wenn das System der breiten Öffentlichkeit zugänglich ist, erfüllt es die Grundvoraussetzung einer freien und quelloffenen Lizenz im Sinne der Transparenz und freien Nutzung.

- [ ] Haben alle Personen unter gleichen Bedingungen und ohne besondere Hindernisse Zugang zum KI-System?

Erläuterung: Diese Frage prüft, ob der Zugang zum KI-System diskriminierungsfrei gestaltet ist, sodass keine speziellen Barrieren, wie Registrierungsgebühren oder exklusive Mitgliedschaften, den Zugang beschränken. Ein offener Zugang ist essenziell, um sicherzustellen, dass das KI-System als quelloffen und für jeden frei nutzbar gilt

- [ ] Wird für das KI-System oder damit verbundene Dienstleistungen kein Preis verlangt?

Erläuterung: Ein wesentliches Kriterium für eine freie Lizenz ist die Abwesenheit einer Monetarisierung. Diese Frage stellt sicher, dass das KI-System selbst oder begleitende Dienstleistungen nicht kostenpflichtig sind. Monetarisierung würde der Definition „frei" widersprechen und könnte die Einstufung als freie Lizenz infrage stellen.

☐ Werden personenbezogene Daten nur zur Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität verarbeitet?

Erläuterung: Diese Frage prüft, ob die Nutzung personenbezogener Daten auf notwendige und zweckgebundene Zwecke beschränkt ist. Eine weitergehende Verarbeitung personenbezogener Daten würde der Definition von „frei und quelloffen" entgegenstehen, da dies eine Form indirekter Monetarisierung darstellen könnte.

☐ Erlaubt die Lizenz die Nutzung, Änderung und Weitergabe des KI-Systems?

Erläuterung: Diese Frage ist zentral für die Einstufung als freie und quelloffene Lizenz, da sie sicherstellt, dass die Lizenz die vollständige Freiheit zur Nutzung, Anpassung und Verbreitung des KI-Systems gewährt. Ohne diese Bedingungen erfüllt die Lizenz nicht die Anforderungen an Offenheit und Freiheit.

☐ Sind die Parameter und Informationen über das Modell, einschließlich Gewichte und Modellarchitektur, öffentlich zugänglich gemacht?

Erläuterung: Diese Frage prüft, ob die technischen Details und internen Parameter des KI-Modells transparent sind. Für eine wirkliche Quelloffenheit müssen diese Informationen offen verfügbar sein, damit andere Nutzer das Modell vollständig verstehen, anpassen und weiterentwickeln können.

Wenn alle Fragen unter Schritt 3 mit "Ja" beantwortet wurden, erfüllt das KI-System die Voraussetzungen für freie und quelloffene Lizenzen gemäß Art. 2 Abs. 12 KI-VO.

Checkliste II – Liegt ein KI-Modell vor, welches unter einer freien und quelloffenen Lizenz i.S.d. Art. 53 Abs. 2 KI-VO bereitgestellt wird.

Zur besseren Orientierung und für ein formalisiertes Vorgehen wurde die folgende Checkliste entwickelt.

Checkliste – Feststellung der Teilausnahme nach Art. 53 Abs. 2 KI-VO

Schritt Nr. 1: Prüfung des Vorliegens eines KI-Modells mit allgemeinem Verwendungszweck

☐ Ja
☐ Nein

Schritt Nr. 2: Wird das Modell im Rahmen einer freien und quelloffenen Lizenz bereitgestellt?

Öffentliche Zugänglichkeit aller Parameter:

☐ Gewichte

Erläuterung: Die Gewichte sind numerische Werte im KI-Modell, die während des Trainings gelernt werden und die Verarbeitung der Eingabedaten steuern. Die Frage prüft, ob diese Gewichte öffentlich zugänglich gemacht wurden, um Transparenz zu gewährleisten und anderen die Möglichkeit zu geben, das Modell zu verstehen und weiterzuentwickeln.
Beispiel: Ein Entwickler stellt die trainierten Gewichte eines neuronalen Netzwerks auf einer Plattform wie GitHub zur Verfügung, sodass andere das Modell direkt nutzen oder daran arbeiten können.

☐ Modellarchitektur

Erläuterung: Die Modellarchitektur beschreibt den Aufbau und die Struktur des KI-Modells, z. B. die Anzahl der Schichten und deren Verbindungen in einem neuronalen Netzwerk. Diese Frage stellt sicher, dass diese Informationen offengelegt werden, damit das Modell vollständig reproduzierbar und verständlich ist.
Beispiel: Die Dokumentation enthält detaillierte Diagramme und Beschreibungen der Modellarchitektur, sodass andere Entwickler sie nachvollziehen und anpassen können.

☐ Informationen über die Modellausführung

Erläuterung: Hier wird gefragt, ob Details zur Anwendung und Implementierung des Modells bereitgestellt werden. Dies umfasst Anleitungen, Abhängigkeiten und Systemvoraussetzungen, um anderen die Nutzung und Integration des Modells zu erleichtern.

Erlaubnis zur Nutzung, Änderung und Weitergabe:

☐ Zugang für jedermann

Erläuterung: Diese Frage überprüft, ob das Modell ohne Zugangsbeschränkungen öffentlich verfügbar ist. Dies ist entscheidend, um den offenen Charakter der Lizenz sicherzustellen und die breite Verfügbarkeit zu fördern.
Beispiel: Das Modell kann von jedem ohne Anmeldung oder spezielle Berechtigungen von einer öffentlichen Webseite heruntergeladen werden.

☐ Nutzung ohne Einschränkungen

Erläuterung: Es wird festgestellt, ob das Modell ohne rechtliche oder technische Beschränkungen verwendet werden kann. Dies ermöglicht es Nutzern, das Modell in vielfältigen Anwendungen einzusetzen.
Beispiel: Die Lizenz erlaubt sowohl private als auch kommerzielle Nutzung des Modells ohne zusätzliche Bedingungen.

☐ Möglichkeit zur Änderung des Modells

Erläuterung: Die Frage klärt, ob Nutzer das Recht haben, das Modell zu modifizieren. Dies fördert Innovation und Anpassung an spezifische Bedürfnisse.
Beispiel: Ein Forscher passt das Modell an, um es für eine spezielle Sprachverarbeitung zu optimieren, und teilt diese Verbesserungen wieder mit der Community.

Schritt Nr. 3: Kein Ausschluss

Liegt keine schädliche Monetarisierung vor?

☐ Keine Bereitstellung gegen Bezahlung (außer zwischen Kleinstunternehmen)

Erläuterung: Diese Frage prüft, ob das Modell kostenlos angeboten wird, um sicherzustellen, dass es tatsächlich frei zugänglich ist. Die Ausnahme für Kleinstunternehmen erlaubt es, in geringem Umfang Transaktionen durchzuführen, ohne den freien Charakter zu verlieren.
Beispiel: Das Modell wird kostenfrei zum Download bereitgestellt, während zwei Kleinstunternehmen es untereinander gegen eine geringe Gebühr austauschen dürfen.

☐ Keine Verarbeitung personenbezogener Daten außer zur Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität

Erläuterung: Hier wird sichergestellt, dass das Modell nicht zur Erhebung und Verarbeitung personenbezogener Daten genutzt wird, die über technische Notwendigkeiten hinausgehen. Dies schützt die Privatsphäre der Nutzer und verhindert eine indirekte Monetarisierung durch Daten.
Beispiel: Das Modell sammelt keine Nutzerdaten für Marketingzwecke, sondern verarbeitet nur notwendige Daten zur Fehlerbehebung.

Bestehen keine systemischen Risiken?

☐ Das Modell ist nicht als KI-Modell mit systemischen Risiken. (Siehe hierzu Art. 3 Nr. 65 KI-VO, Art. 55 KI-VO) eingestuft

Wenn alle Fragen mit "Ja" beantwortet wurden, greift die Teilausnahme des Art. 53 Abs. 2 KI-VO.