📘 Originaltext: EU AI Act (Verordnung (EU) 2024/1689)

Auszug aus dem Erwägungsgrund 1:
„Diese Verordnung zielt darauf ab, vertrauenswürdige künstliche Intelligenz (KI) zu fördern und dabei ein hohes Schutzniveau für Gesundheit, Sicherheit und Grundrechte gemäß der Charta der Grundrechte der Europäischen Union zu gewährleisten, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, gegen die schädlichen Auswirkungen von KI-Systemen in der Union, und gleichzeitig Innovation zu unterstützen.“ (EU Künstliche Intelligenz Gesetz)

Artikel 1 – Gegenstand und Ziele:
„Diese Verordnung legt harmonisierte Vorschriften für die Entwicklung, das Inverkehrbringen, das In-die-Dienste-Stellen und die Nutzung von KI-Systemen in der Union fest.“ (EUR-Lex, AI Act)

Artikel 2 – Begriffsbestimmungen:
„‚KI-System‘ bezeichnet ein System, das aus einer Reihe von miteinander verbundenen Modulen besteht, die unter Verwendung verschiedener Techniken und Ansätze – einschließlich maschinellem Lernen, Logik- und wissensbasierten Ansätzen – eigenständig Vorhersagen, Schlussfolgerungen oder Entscheidungen treffen können.“ (Wikipedia)

Artikel 5 – Risikobasiertes System:
„KI-Systeme werden nach dem Risiko kategorisiert: Systeme mit unannehmbaren Risiko, Hochrisiko-KI, Transparenz-KI und nicht-hochriskante KI. Für Hochrisiko-KI sind spezifische Anforderungen und Konformitätsbewertungsverfahren vorgesehen.“ (AI Act, Wikipedia)

Artikel 113 – In-Kraft-Treten und Anwendung:
„Diese Verordnung tritt am 1. August 2024 in Kraft. Die meisten Bestimmungen, insbesondere zu Hochrisiko-KI, gelten ab dem 2. August 2026.“ (AI Act, Wikipedia)

Das ist der offizielle Auszug aus der Verordnung – im Original in Englisch und Deutsch im Amtsblatt veröffentlicht. Es ist die verbindliche Grundlage für die Ausbildung.

🗂️ Weiteres Begleitmaterial:

- Volltext PDF (de/en) über amtliche Quellen (EUR-Lex) oder spezialisierte Plattformen wie AI Act Explorer (EU Künstliche Intelligenz Gesetz).
- Erwägungsgründe, Kapitel mit Kapitelüberschriften und relevante Anhänge (z. B. Anhang III – Definition Hochrisiko-Systeme; Anhang IV – Technische Dokumentationsanforderungen).
- Cross-Referenzen: EU AI Act im Vergleich zu DSGVO (z. B. Art. 22 – automatisierte Einzelfallentscheidung).

Hier die **relevanten Auszüge aus der Datenschutz-Grundverordnung (DSGVO)** – insbesondere **Artikel 22**, der im Kontext des EU AI Act für den KI Compliance Officer besonders bedeutsam ist:

📜 Datenschutz-Grundverordnung (DSGVO) – Relevante Auszüge für KI Compliance

🔷 Artikel 22 DSGVO – Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1)
Die betroffene Person hat das Recht, **nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden**, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2)
Absatz 1 gilt nicht, wenn die Entscheidung:

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Vorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

(3)
In den in Absatz 2 genannten Fällen trifft der Verantwortliche **angemessene Maßnahmen**, um die **Rechte und Freiheiten sowie berechtigten Interessen der betroffenen Person zu wahren**, wozu mindestens das Recht auf **Erwirkung des Eingreifens einer Person**, auf **Darlegung des eigenen Standpunkts** und auf **Anfechtung der Entscheidung** gehört.

(4)
Entscheidungen nach den Absätzen 2 Buchstaben a und c dürfen **nicht auf besonderen Kategorien personenbezogener Daten** nach Artikel 9 Absatz 1 beruhen, **es sei denn**, Artikel 9 Absatz 2 Buchstabe a oder g gilt und **angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen** der betroffenen Person wurden getroffen.

🔷 Ergänzende relevante DSGVO-Artikel im KI-Kontext

Artikel	Thema	Relevanz für KI Compliance
Art. 5	Grundsätze für die Verarbeitung personenbezogener Daten	Datenminimierung, Transparenz, Zweckbindung, Integrität und Vertraulichkeit
Art. 6	Rechtmäßigkeit der Verarbeitung	Legitimation der KI-Datennutzung (z. B. Einwilligung, Vertragserfüllung)
Art. 13/14	Informationspflichten bei der Datenerhebung	Transparenzpflicht bei KI-Einsatz (auch für nicht direkt erhobene Daten)
Art. 15	Auskunftsrecht der betroffenen Person	Verpflichtung zur Offenlegung von eingesetzten KI-Logiken bei Anfrage
Art. 35	Datenschutz-Folgenabschätzung (DSFA)	Obligatorisch bei KI-Systemen mit hohem Risiko für Grundrechte

🧠 Hinweis für den KI Compliance Officer:

Artikel 22 DSGVO ist einer der engsten **Berührungspunkte zwischen DSGVO und EU AI Act**. Während die DSGVO individuelle Entscheidungsrechte betont, konkretisiert der EU AI Act, **wann und wie KI-Systeme eingesetzt werden dürfen**, insbesondere bei Hochrisiko-Anwendungen wie Kreditvergabe, Personaleinstellung oder Bewertung von Sozialleistungen.

Soll als Nächstes eine vergleichende **Tabelle EU AI Act vs. DSGVO** erstellt werden oder möchten Sie auf Basis dieser Artikel **ein Fallbeispiel mit Risikoanalyse und Maßnahmenplan**?

Hier ist eine **vergleichende Tabelle „EU AI Act vs. DSGVO“**, zugeschnitten auf die praktische Arbeit eines **KI Compliance Officers (KICO)**. Sie dient zur Einordnung der **rechtlichen Schnittmengen, Unterschiede und ergänzenden Anforderungen** beider Regelwerke.

📊 Vergleichstabelle: EU AI Act vs. DSGVO

Kriterium	EU AI Act (Verordnung (EU) 2024/1689)	DSGVO (Verordnung (EU) 2016/679)
Zielsetzung	Sicherer, transparenter und ethischer Einsatz von KI in der EU	Schutz personenbezogener Daten natürlicher Personen
Anwendungsbereich	KI-Systeme unabhängig davon, ob personenbezogene Daten verarbeitet werden	Verarbeitung personenbezogener Daten (auch durch KI)
Technologiebezug	KI-spezifisch: maschinelles Lernen, regelbasierte Systeme, neuronale Netze	Technologieneutral, aber relevant bei KI, die personenbezogene Daten nutzt
Risikobasierter Ansatz	Ja – vier Risikokategorien: verboten, hochriskant, Transparenzpflicht, frei verwendbar	Nein – keine formale Kategorisierung, aber DSFA bei hohem Risiko
Verbotene Anwendungen	Z. B. Social Scoring, versteckte emotionale Manipulation	Keine expliziten Technologieverbote
Pflichten für Anbieter	Konformitätsbewertung, Technische Dokumentation, CE-Kennzeichnung	Datenschutz durch Technikgestaltung, Auftragsverarbeitung, Informationspflichten
Pflichten für Nutzer	Risikoüberwachung, Einsatzkontrolle, Transparenzpflichten gegenüber Dritten	Rechtmäßigkeit der Verarbeitung, Informationspflicht, Nachweispflicht
Einwilligung & Rechte	Kein zentrales Element – Fokus auf Systeme und Konformität	Zentrale Grundlage – Einwilligung, Widerspruch, Auskunft, Löschung
Profiling / automatisierte Entscheidungen	Nicht direkt geregelt – nur über Risikokategorien (z. B. HR, Kreditvergabe)	Geregelt in Art. 22 DSGVO: Schutz vor ausschließlich automatisierten Entscheidungen
Betroffenenrechte	Nicht im Zentrum (außer bei Transparenzpflichten)	Sehr stark ausgeprägt: Art. 12–22 DSGVO
Aufsichtsbehörden	Nationale Marktüberwachungsbehörden + EU KI-Behörde	Datenschutzaufsichtsbehörden der Mitgliedstaaten
Sanktionen / Bußgelder	Bis zu 35 Mio. € oder 7 % des weltweiten Umsatzes (bei verbotener KI)	Bis zu 20 Mio. € oder 4 % des weltweiten Umsatzes
Synergiepotenzial	Ergänzt die DSGVO bei KI-Anwendungen mit technischer und organisatorischer Perspektive	Muss bei KI-Projekten parallel berücksichtigt werden (z. B. Zweckbindung, DSFA)

📌 Fazit für den KI Compliance Officer:

- **Der EU AI Act regelt KI als System**, unabhängig davon, ob personenbezogene Daten betroffen sind.
- **Die DSGVO greift immer dann**, wenn personenbezogene Daten ins Spiel kommen – unabhängig davon, ob KI involviert ist.
- In der Praxis sind **beide Verordnungen häufig parallel anwendbar**, z. B. bei Bewerber-Screenings, Kreditentscheidungen oder Videoüberwachung.

✅ Checkliste: Wann gilt der EU AI Act, wann die DSGVO – und wann beide?

🔍 TEIL A – GILT DER EU AI ACT?

☐ Wird ein KI-System im Sinne der Definition des EU AI Act eingesetzt?

(z. B. maschinelles Lernen, statistische Mustererkennung, regelbasierte Entscheidungsbäume)

☐ Ist das System in der EU im Einsatz, im Verkehr oder wird es EU-Bürgern bereitgestellt?

☐ Fällt die Anwendung in eine der folgenden Risikokategorien?

- ☐ Verbotene KI (z. B. Social Scoring, verdeckte Manipulation)?
- ☐ Hochrisiko-KI (z. B. Personalwesen, Kreditprüfung, kritische Infrastruktur)?
- ☐ Transparenzpflichtige KI (z. B. Deep Fakes, Chatbots, biometrische KI)?
- ☐ Geringes Risiko (z. B. Empfehlungsalgorithmen)?

☐ Muss eine Konformitätsbewertung, CE-Kennzeichnung oder technische Dokumentation erstellt werden?

🔐 TEIL B – GILT DIE DSGVO?

☐ Werden personenbezogene Daten verarbeitet (direkt oder indirekt identifizierbar)?

(z. B. Name, Gesicht, Stimme, Verhalten, Standort, IP-Adresse)

☐ Liegt ein definierter Zweck der Verarbeitung vor (z. B. Vertrag, Einwilligung, gesetzliche Pflicht)?

☐ Gibt es eine Rechtsgrundlage nach Art. 6 DSGVO?

☐ Wurde eine **Datenschutz-Folgenabschätzung (DSFA)** gemäß Art. 35 durchgeführt (bei hohem Risiko)?

☐ Werden Betroffenenrechte gemäß Art. 12–22 DSGVO sichergestellt?

☐ Werden automatisierte Einzelentscheidungen getroffen (→ Art. 22 DSGVO)?

⚖️ TEIL C – GILT BEIDES GLEICHZEITIG?

✅ Das ist der Normalfall bei modernen KI-Anwendungen. Prüfen Sie zusätzlich:

□ Schnittstellen zwischen beiden Verordnungen klar definiert?

- KI-Risiken → EU AI Act
- Datenrisiken → DSGVO

□ Verantwortlichkeiten aufgeteilt?

- KI-Konformität → Hersteller / Anbieter
- Datenschutz & Transparenz → Betreiber / Nutzer

□ Beide Perspektiven in Dokumentation, DSFA, Verträgen, Einwilligungen berücksichtigt?

□ Zusammenarbeit zwischen KI-Entwicklungsteam, Datenschutzbeauftragten, Legal & IT Security aktiv organisiert?

📌 Empfohlene Folgeaktionen, wenn beide Regelwerke gelten:

Aufgabe	Verantwortlich
Durchführung der Konformitätsbewertung (KI)	Anbieter / Hersteller
Erstellung der technischen Dokumentation (KI)	Produktentwicklung / Legal
Datenschutz-Folgenabschätzung (DSFA)	Datenschutzbeauftragter
Erstellung von Informationspflichten	Legal / Datenschutz
Einrichtung von Transparenz-Mechanismen (z. B. Kennzeichnung von Chatbots)	Entwicklungsteam / UX / Legal
Regelmäßige Überprüfung der KI-Systeme auf neue Risiken	KI Compliance Officer (KICO)

Praxisorientiertes **Musterformular zur kombinierten Dokumentation für KI- und Datenschutz-Compliance**, das Sie im Unternehmen zur Projektprüfung, internen Dokumentation oder als Anhang zur Datenschutz-Folgenabschätzung (DSFA) verwenden können.

📄 Musterformular: Kombinierte Dokumentation gemäß EU AI Act & DSGVO

Stand: Juli 2025 – für interne Zwecke im Unternehmen

1. Projektübersicht

Bezeichnung des KI-Systems	**z. B. „SmartHire AI – automatisiertes Bewerberranking“**
Version / Systemstand	z. B. v3.2 – Stand Juni 2025
Hersteller / Anbieter	[Name + Kontakt]
Intern verantwortliche Stelle	[Abteilung, Ansprechpartner]
Projektziel	z. B. Effiziente Vorqualifizierung von Bewerbungen
Geplanter Einsatzbeginn	[Datum]

2. Klassifikation nach EU AI Act

Risikokategorie	**☐ Verboten ☐ Hochrisiko ✅ Transparenzpflichtig ☐ Niedrigrisiko**
Begründung der Einstufung	[Verweis auf Anhang III / Definition im AI Act]
CE-Konformitätsbewertung durchgeführt?	☐ Ja ☐ Nein ☐ Geplant
Technische Dokumentation erstellt?	☐ Ja ☐ Nein ☐ In Bearbeitung
Transparenzhinweise vorgesehen?	☐ Ja ☐ Nein ☐ Teilweise
Human Oversight definiert?	☐ Ja ☐ Nein – Maßnahmen: [z. B. manuelle Kontrolle durch HR]

3. Verarbeitung personenbezogener Daten (gemäß DSGVO)

Verarbeitete Datenarten	z. B. Name, Lebenslauf, Sprache, Videoanalyse, E-Mail
Zweck der Verarbeitung	z. B. automatisierte Vorqualifizierung von Bewerbungen
Rechtsgrundlage (Art. 6 DSGVO)	☐ Vertrag ☐ Einwilligung ☐ berechtigtes Interesse – [Erläuterung]
Besondere Kategorien Daten (Art. 9 DSGVO)?	☐ Nein ☐ Ja – Details: [z. B. Gesundheitsdaten]
Automatisierte Einzelentscheidung (Art. 22 DSGVO)?	☐ Ja ☐ Nein ☐ Teilweise – Maßnahmen: [z. B. Widerrufsoption]
Transparenz- und Informationspflicht erfüllt?	☐ Ja – Textbaustein liegt bei ☐ Nein ☐ In Erstellung
Datenschutz-Folgenabschätzung (DSFA) durchgeführt?	☐ Ja ☐ Nein – Begründung: [z. B. geringes Risiko]

4. Technische & organisatorische Maßnahmen (TOMs)

- Zugriffskontrolle: ☐ Ja ☐ Nein
- Logging & Monitoring der Entscheidungen: ☐ Ja ☐ Nein
- Löschkonzepte & Speicherfristen: ☐ Definiert ☐ Unklar
- Bias-Prüfung & Diskriminierungsvermeidung: ☐ Durchgeführt ☐ Geplant
- Notfall- / Rückrufmechanismus: ☐ Vorhanden ☐ Nicht notwendig

5. Prüferische Bewertung / Freigabe

Fachabteilung Recht	**☐ Genehmigt ☐ Rückfragen ☐ Ablehnung**
Datenschutzbeauftragter	☐ Genehmigt ☐ DSFA erforderlich ☐ Hinweise
KI Compliance Officer	☐ Konform ☐ Auflagen notwendig ☐ Hochrisiko-Alarm
Datum / Unterschrift	_____

6. Anlagen / Verweise

- 🔗 Konformitätserklärung (EU AI Act)
- 🔗 DSFA (Datenschutz-Folgenabschätzung)
- 🔗 Datenschutzhinweise für Betroffene
- 🔗 CE-Kennzeichnung und technische Dokumentation
- 🔗 Human Oversight / Bedienkonzept
- 🔗 Betriebsanweisung / Mitarbeiterschulung

Hinweis zur Verwendung:
Dieses Formular dient als interne Nachweisdokumentation zur Einhaltung sowohl der technischen Anforderungen des **EU AI Act** als auch der datenschutzrechtlichen Vorgaben der **DSGVO**. Es kann im Rahmen der internen Kontrollsysteme (IKS) sowie gegenüber Aufsichtsbehörden vorgelegt werden.

Hier ist eine klar strukturierte **Visualisierung der Risikopyramide des EU AI Act**.

🧱 Visualisierung: Risikopyramide des EU AI Act

🔴 VERBOTENE KI

KI-Systeme mit unannehmbarem Risiko

❌ Sozial-Scoring durch Behörden

❌ Subtile Manipulation von Verhalten

❌ Emotionserkennung am Arbeitsplatz

❌ Predictive Policing mit biometrischer Überwachung

🚫 Einsatz grundsätzlich verboten

🚫 Keine Konformitätsprüfung möglich

🚫 Strafandrohung bis zu 7 % des Jahresumsatzes

🔶 HOCHRISIKO-KI

KI-Systeme mit erheblichen Gefahren für Grundrechte, Sicherheit oder Gesundheit

✅ Kreditwürdigkeitsprüfung

✅ Personaleinstellung, Bildungssysteme

✅ Medizinprodukte mit KI-Funktion

✅ KI in kritischer Infrastruktur, Justiz, Polizei

✔ Konformitätsbewertung erforderlich

✔ Technische Dokumentation, Logging, Human Oversight

✔ CE-Kennzeichnung

🔵 TRANSPARENZ-KI

KI-Systeme mit spezifischen Transparenzpflichten

📌 Chatbots (muss als KI gekennzeichnet sein)

📌 Deepfakes (müssen erkennbar sein)

📌 Emotionserkennungssysteme

📌 biometrische Klassifikation außerhalb Hochrisikobereich

✔ Transparenz- und Hinweisverpflichtung
✔ Kein Konformitätsverfahren erforderlich
✔ Anwendungshinweise für Endnutzer

⚪ GERINGES RISIKO / UNREGULIERT

KI-Systeme ohne besondere Regulierungspflichten

🟢 Empfehlungssysteme (z. B. Streamingplattformen)

🟢 Produktpersonalisierung

🟢 Büroautomatisierung (z. B. Texterstellung)

✔ Freie Entwicklung und Anwendung
✔ Selbstverpflichtung oder freiwillige Verhaltenskodizes empfohlen
✔ Optional: „Code of Conduct“ oder „Trust Label“

📌 Ergänzende Hinweise zur Verwendung:

- Diese Pyramide veranschaulicht den **risikobasierten Ansatz** des EU AI Act: Je höher das Risiko für die Grundrechte, desto stärker die Regulierung.
- In **Modul 1 der Ausbildung** dient sie als Orientierung für die erste Klassifizierung eines KI-Projekts.

- Die Darstellung kann in Schulungsunterlagen, Compliance-Richtlinien oder Projekt-Dossiers verwendet werden.

Auf der Folgeseite ist eine **Synopse (Gegenüberstellung)** der **EU KI-Verordnung (AI Act)** und der **Produktsicherheitsverordnung (General Product Safety Regulation – GPSR, Verordnung (EU) 2023/988)** mit Fokus auf Gemeinsamkeiten, Unterschiede und Schnittstellen – speziell für die Arbeit als **KI Compliance Officer (KICO)** in Unternehmen:

📄 Synopse: EU AI Act vs. Produktsicherheitsverordnung (GPSR)

Vergleichende Darstellung für KI-Systeme als Produkte im Binnenmarkt

Kriterium	EU AI Act (Verordnung (EU) 2024/1689)	Produktsicherheitsverordnung – GPSR (Verordnung (EU) 2023/988)
Rechtsnatur	Sektorenspezifische Produkt- und Systemverordnung für KI	Horizontal geltende Produktverordnung für alle Verbraucherprodukte
Zielsetzung	Sicherer, vertrauenswürdiger und menschenzentrierter Einsatz von KI-Systemen	Schutz der Gesundheit und Sicherheit der Verbraucher bei Produkten
Geltungsbereich	KI-Systeme und -Modelle (sowohl physisch eingebettete als auch rein digitale)	Alle physisch oder digital bereitgestellten Produkte für Verbraucher
Produktfokus	Fokus auf algorithmische / datengetriebene Funktionalität (nicht das Trägermedium)	Fokus auf physisches oder digitales Produkt als Ganzes
Bezug zu Verbraucherschutz	Grundrechteorientiert – indirekter Verbraucherschutz durch Risikoregulierung	Direkter Schutz von Endverbrauchern bei Mängeln, Sicherheitsrisiken usw.
Pflichten für Hersteller / Anbieter	Konformitätsverfahren, Risikomanagement, CE-Kennzeichnung	Produktsicherheitsbewertung, CE-Kennzeichnung (sofern andere harmonisierte Normen greifen)
CE-Kennzeichnung	Ja – verpflichtend bei Hochrisiko-KI (nach erfolgreicher Konformitätsprüfung)	Ja – wenn spezifische EU-Harmonisierungsrechtsvorschriften greifen
Marktüberwachung	Nationale Behörden + zentrale KI-Behörde auf EU-Ebene (zukünftig EBAI)	Marktüberwachungsbehörden der Mitgliedstaaten (mit Produktsicherheitsmandat)
Technische Dokumentation	Pflicht für Hochrisiko-KI-Systeme nach Anhang IV AI Act	Pflicht zur Sicherheitsdokumentation bei Risikoprodukten
Risikokonzept	Kategorisierung: verboten – hochriskant – Transparenzpflicht – unreguliert	Risikokonzept über Gefahrenabschätzung + Rückrufmechanismen
Reaktionspflicht bei Gefahren	Meldepflicht bei schwerwiegenden Vorfällen an Aufsichtsbehörden	Verpflichtung zur Rücknahme / Rückruf bei unsicheren Produkten
Betroffenheit digitaler Produkte	Hoch – auch rein digitale KI-Systeme ohne physischen Träger sind erfasst	Nur wenn digitales Produkt physische Wirkung entfalten oder Verbraucher betrifft

🧭 Schnittstellen & Kombinationspflichten

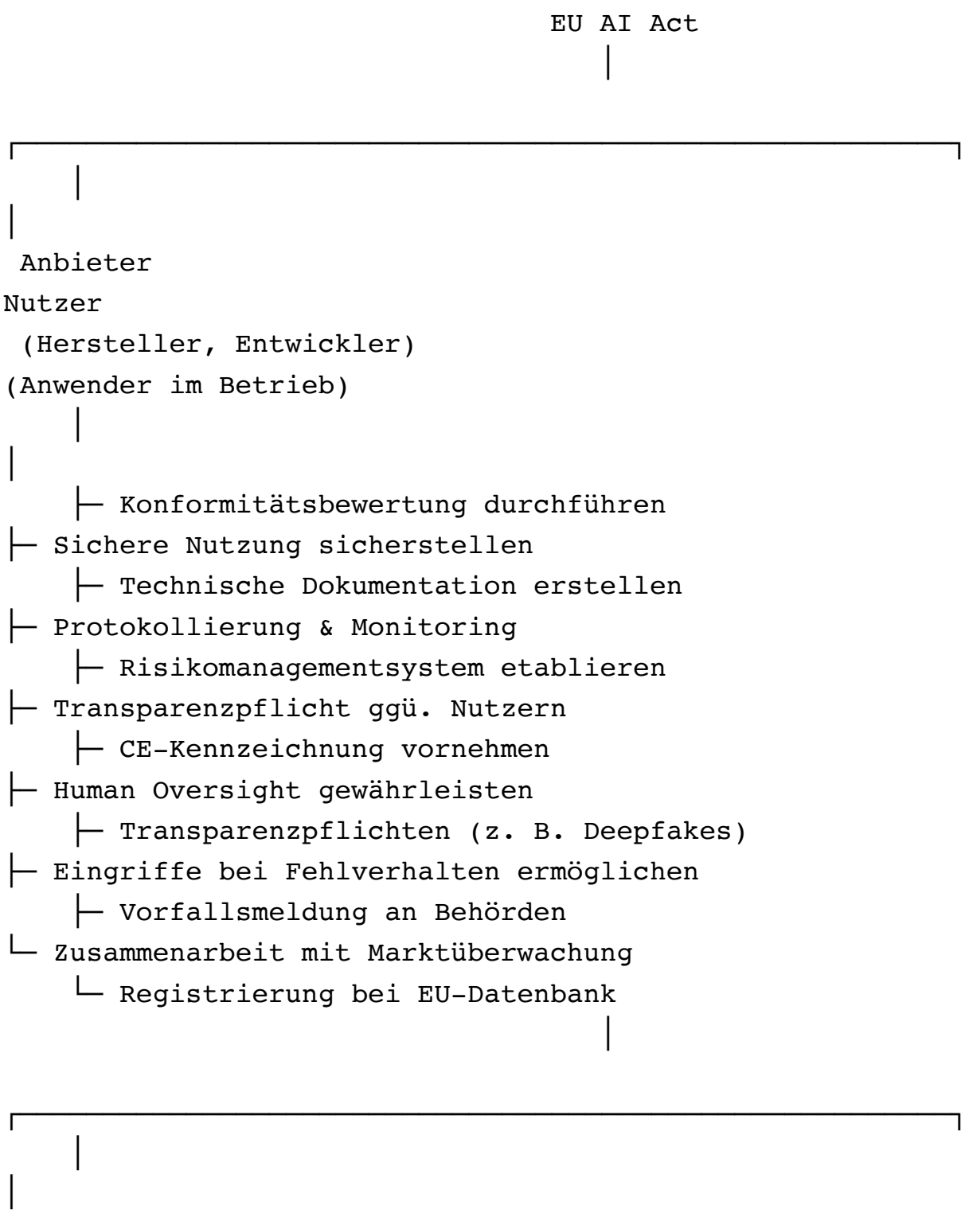
Schnittstelle	Praxisrelevanz
KI-System als Bestandteil eines physischen Produkts	z. B. medizinisches Gerät mit integrierter Diagnose-KI → AI Act + Produktsicherheitsverordnung
CE-Kennzeichnungspflicht doppelt relevant	AI Act schreibt CE-Kennzeichnung für Hochrisiko-KI vor – GPSR erfordert diese zusätzlich für Gesamtprodukt
Sicherheitsanforderungen müssen ganzheitlich erfüllt sein	Integration von KI darf Sicherheit nicht gefährden – Kombination von Software- und Produktsicherheit
Rückrufpflichten greifen übergreifend	Sowohl GPSR als auch AI Act verpflichten zur Marktüberwachung und Risikoreaktion

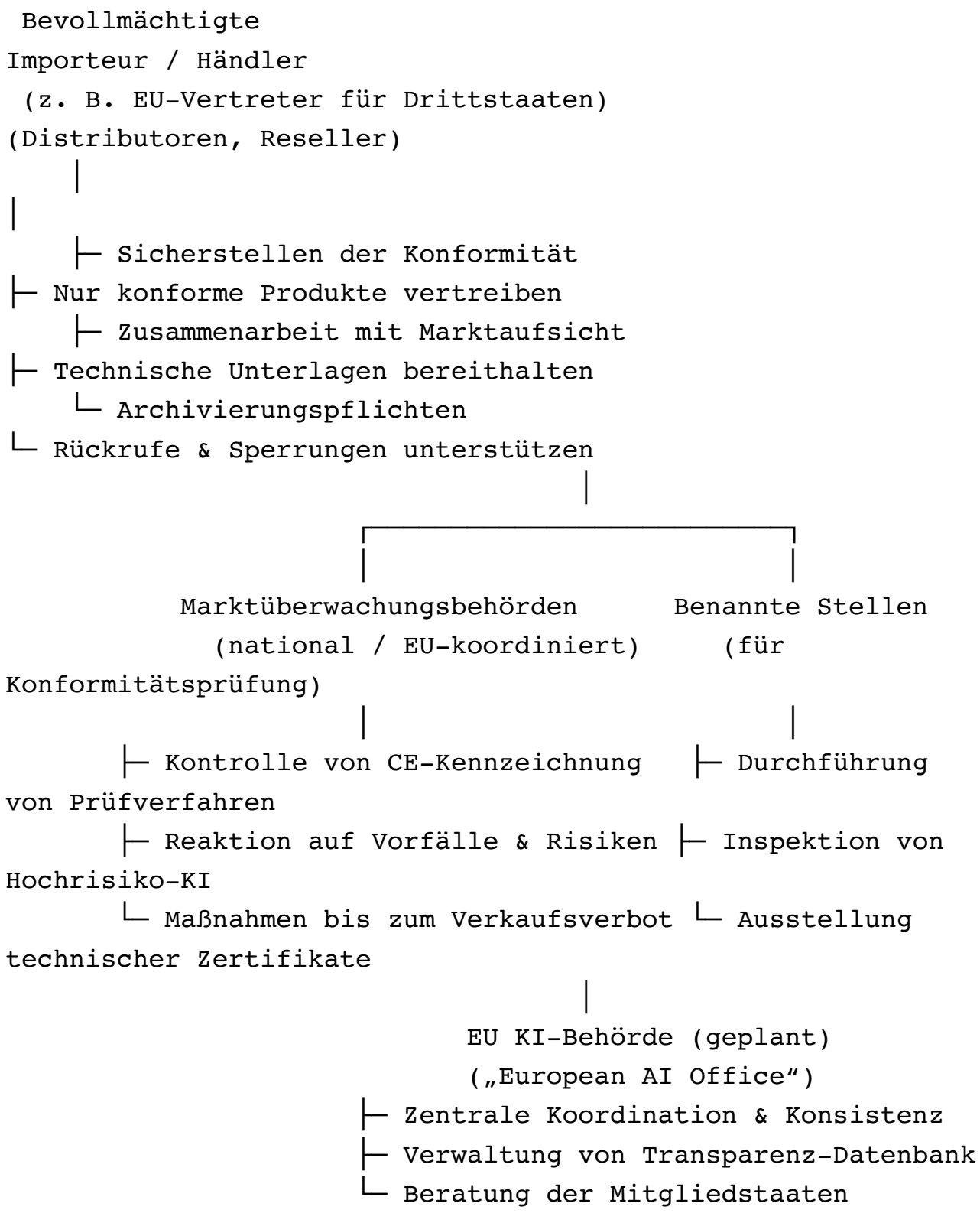
📌 Empfehlung für KI Compliance Officer (KICO):

- Prüfen Sie bei KI-Systemen, ob diese **als Produkt** oder **als Funktion** eines Produkts auftreten.
- Bei **physischen Produkten mit KI-Komponente** (z. B. Roboter, Medizingeräte, IoT-Produkte) ist **eine Kombination beider Verordnungen** zu berücksichtigen.
- Achten Sie auf **abgestimmte technische Dokumentation**, die sowohl sicherheitstechnische Aspekte (GPSR) als auch algorithmische Anforderungen (AI Act) abdeckt.
- **CE-Kennzeichnung muss kohärent** für beide Regime dokumentiert sein (z. B. gemeinsames Konformitätsverfahren oder Verweis auf ergänzende Normen).

Hier ist eine übersichtliche **Mindmap zu den Akteuren und ihren Pflichten im EU AI Act** – ideal für Schulungen, interne Audits und die Ausbildung zum **KI Compliance Officer (KICO)**.

🧠 Mindmap: Akteure und ihre Pflichten im EU AI Act (2024/1689)




Bevollmächtigte
Importeur / Händler
(z. B. EU-Vertreter für Drittstaaten)
(Distributoren, Reseller)
├ Sicherstellen der Konformität
├ Nur konforme Produkte vertreiben
├ Zusammenarbeit mit Marktaufsicht
├ Technische Unterlagen bereithalten
└ Archivierungspflichten
└ Rückrufe & Sperrungen unterstützen
Marktüberwachungsbehörden
(national / EU-koordiniert)
Benannte Stellen
(für Konformitätsprüfung)
├ Kontrolle von CE-Kennzeichnung
├ Reaktion auf Vorfälle & Risiken
└ Maßnahmen bis zum Verkaufsverbot
├ Durchführung von Prüfverfahren
├ Inspektion von Hochrisiko-KI
└ Ausstellung technischer Zertifikate
EU KI-Behörde (geplant)
(„European AI Office“)
├ Zentrale Koordination & Konsistenz
├ Verwaltung von Transparenz-Datenbank
└ Beratung der Mitgliedstaaten

🔍 Ergänzende Erklärungen zu den Akteuren:

Akteur	Rolle
Anbieter	Primärverantwortlich für die Entwicklung und Markteinführung von KI
Nutzer	Setzen KI in der Praxis ein und sind für sicheren Betrieb verantwortlich
Importeur / Händler	Müssen sicherstellen, dass nur konforme KI-Systeme in Verkehr gebracht werden
Bevollmächtigte	Juristische Schnittstelle zu EU-Institutionen bei Drittlandslieferanten
Benannte Stellen	Zertifizierungsstellen für Hochrisiko-KI
Behörden	Überwachung, Marktprüfung, Sanktionierung

📌 Einsatzhinweis für KICO:

Diese Mindmap eignet sich ideal für:

- Schulungsunterlagen (z. B. Flipchart, PowerPoint)
- Stakeholder-Briefings
- Projektrollenklärung im Unternehmen
- Vertragsverhandlungen (z. B. bei Import, Vertrieb)