Fundstelle EU AI Act 2024	GPAI	KI-M in High Risk System	Sonstige KI-M	Bewertung / Frage	Rückschluss	weiteres
1. Artikel						
Artikel 1 (2) e)	Vorschriften für Inverkehrbringen	-	-	betrifft harmoniserte Vorschriften	-	
Artikel 2 (1) a)	Anbieter und In Vekehr bringen von KI-S und GPAI	-	-	Gilt er für alle KI-M o. nur GPAI?	Einschränkung: Nur für Anbieter von GPAI nicht für sonstige KI-M Anbieter!	wird mit Abs. 2 (6) widerlegt? Aber durch Art. 3 Nr. 3 bestätigt! Damit alle anderen KI-M via Wertschöpfungskette über Anbieter von KI-S; aber in Wertschöpfungskette auch "der Dritte"
Artikel 2 (6)	-	-	Forschung als Ausnahme	Wortlaut: KI-M ohne Zusatz! Doch alle KI-M?	gilt für alle anderen KI-M	
Artikel 2 (8)	-	-	nicht vor Inverkehrbringung	Wortlaut: KI-M ohne Zusatz! Doch alle KI-M?	gilt für alle anderen KI-M	
Artikel 10 (1)	-	Trainings-, Validierungs- und Testdatensätze erfoderlich; Verzerrungen		z.T. unklar, was genau davon KI-S und was nur das KI-M betrifft?	gilt für alle anderen KI-M	
Artikel 15 (5) S.3	-	Resilienz: bezogen auf Trainingsdaten (data-poisoning); vortrainierter Komponenten (model-poisoning); Eingabedaten (adversarial examples / model evasions); Modellmängel verhüten	-	keine Begrenzung auf GPAI - gilt es für Kriterien aller Arten von Modellen: Trennung, Daten, Komponenten, Eingabedaten?	gilt für alle anderen KI-M	differenzierung von KI-S, die KI-M trainieren und anderen KI-S, die nicht KI-M trainieren;
Artikel 25 (4)	gilt nicht für Open Source GPAI	Sub-Komponenten müssen für High Risk KI vertraglich genau definiert werden u.a. Fähigkeiten u. Zugang	-	wenn GPAI von Open Source ausgenommen ist, sind auch andere KI-M davon erfaßt, also befreit von schriftlicher Vereinbarung? Formulierung "der Dritte": Anbieter von sonstigem KI-Modell?	KI-M auch ohne GPAI als Komponenten möglich; GPAI als Teil von KI-S möglich; Dritter ist verpflichtet, aber kein Anbieter	Musterbedingungen der EU für Verträge von Ho chrisiko-KI als Kann-Regelung
Artikel 40 (1)	Konformitätsvermutung CE	mittelbare Konformitätsvermutung	-	-	gemeinsame Nennung HiRi; GPAI	
Artikel 40 (2) S.2	Energieeffizienz im Lebenszyklus	mittelbare Bedeutung	-	-	gemeinsame Nennung HiRi; GPAI	
Artikel 40 (2) S.3	Normenkonsistenz notwendig	mittelbare Bedeutung	-	-	gemeinsame Nennung HiRi; GPAI	
Artikel 41 (3)	Konformitätsvermutung Spezifikationen	mittelbare Bedeutung	-	-	gemeinsame Nennung HiRi; GPAI	
Artikel 41 (5)	Nachweispflichten Spezfikation	mittelbare Bedeutung	-	-	gemeinsame Nennung HiRi; GPAI	Läßt Definition KI-M offen!
Artikel 51	Klassifikation GPAI-SystemRisk	-	-	-	-	
Artikel 52 (1)	Mitteilungspflichten GPAI-System-Risk	-	-	-	-	
Artikel 52 (2)	Nachweis, falls anderer Meinung	-	-	-	-	
Artikel 52 (3)	Fingierung von GPAI-System-Risk	-	-	-	-	
Artikel 52 (4)	Ausweisen als GPAI-System-Risk	-	-	-	-	
Artikel 52 (5)	Erneute Prüfung bei Widerspruch	-	-	-	-	
Artikel 52 (6)	Liste von GPAI-System-Risk	-	-	-	-	
Artikel 53 (1)	GPAI Doku-Pflichten	-	-	-		generell wichtig!
Artikel 53 (2)	Open Source u. Bestandteile	konkrete Hinweise zu Elementen	konkrete Hinweise zu Elementen	wichtige Beschreibung: Parameter, Gewichte, Modellarchitektur, Modellnutzung müssen erklärt werden - gilt allgemein?	gilt für alle KI-M	Bestandteile von KI-M!
Artikel 53 (3)	Kooperationspflicht	-	-	-	-	
Artikel 53 (4)	Praxisleitfäden; Alternative Nachweise	-	-	-	-	
Artikel 53 (5)	"vergleichbare und überprüfbare Dokumentation"	mittelbare Bedeutung	mittelbare Bedeutung	-	Systematisch von Bedeutung	
Artikel 54 (1-3)	Bevollmächtigte für GPAI erforderlich	-	-	sonstige KI-M benötigen keinen Bevollmächtigten?!	kritisch oder Chance: Zumindest logisch, da auch kein Anbieter erforderlich s.o.	
Artikel 54 (6)	nicht für Open Source; wohl aber für GPAI System-Risk	Benennung für alle KI-M	Benennung für alle KI-M	wichtige Beschreibung: Zugang, Nutzung, Verbreitung, Parameter, Gewichte, Modellarchitektur, Modellnutzung	Systematisch von Bedeutung	
Artikel 55	GPAI System-Risk Pflichten; sehr spezifisch	-	-	-	-	
Artikel 56 (3)	Beteiligung an Praxisleitfäden für GPAI-Anbieter - diverse Stakeholder	-	Interesse an Abgrenzung auch von Herstellern kleiner KI-M?!	sind Anbieter sonstiger KI-M auch Stakeholder? Aber begrifflich keine Anbieter sonstiger KI-M möglich: Was sind sie dann?	Systematisch von Bedeutung	

Artikel 56 (7)	Pflicht zur Befolgung der Praxisleitfäden möglich	-	-	-	-	
Artikel 66 c)	Beratung des Gremiums	-	-	-	-	
Artikel 66 n)	Warnungen durch Gremium bzgl. GPAI	-	-	-	-	
Artikel 66 o)	Warnungen integrierter GPAI	Warnungen integrierter GPAI	-	-	-	
Artikel 68	Unabhängigkeit des Gremiums etc.	-	-	-	-	
Artikel 72 (1)		Spricht nur von "KI-Techniken", erwähnt aber nicht KI-M		Entsprechen KI-Techniken verschiedenen Varianten von KI-M?	Dies ist in systematischer, ebenso wie in teleologischer Hinsicht anzunehmen	
Artikel 75	Selber Hersteller?!	GPAI Selber Hersteller?!	Regel/Ausnahme	bestätigt noch einmal Möglichkeit, dass GPAI in High-Risk genutzt werden kann als Sonderfall!	Regelfall: In High Risk sind sonstige KI-M drin -> die haben aber keine eigenen Anbieter, sondern immer nur Anbieter von KI-S via Wertschöpfungskette verantwortlich	
Artikel 88	Rechtsdurchsetzung	-	-	-	-	
Artikel 89	Überwachung u. Hinweise nachgelagerter Anbieter von GPAI	-	-	-	-	
Artikel 90	Warnungen durch Gremium bzgl. GPAI	-	-	-	-	
Artikel 91	Anforderung der Dokumentation	-	-	-	-	
Artikel 92	Bewertung von GPAI durch Büro	-	-	-	-	
Artikel 93	Dialog mit GPAI durch Büro	-	-	-	-	
Artikel 94	Verfahrensrechte für GPAI-Anbieter	-	-	-	-	
Artikel 101	Sanktionen	-	mittelbare Bedeutung: Keine Sanktionen möglich?!	-	-	
Artikel 111	Bestandsschutz	mittelbare Bedeutung	-	-	-	
Artikel 112 (6)	Normen für Energieeffizienz	-	-	-	-	
2. Anhänge						
Anhang I Fassung 2021	-	-	-	KI-Techniken als Ersatz für Beschreibung von KI-M?	Anhang wurde ohne Begründung weggelassen, obwohl Rechtssicherheit das Ziel gerade dieses Anhangs war, siehe Begründung 5.2.1 a.F.	
Anhang VII 4.5	-	Zugang zu Trainingsmodellen und trainierten Modellen des KI-S inkl. Parameter	-	Wie erhält KI-M-Anbieter Zugang zu Infos von KI-M-Anbieter, das nicht GPAI ist?	Wichtig, da initiale historische Annäherung an KI-M	
Anhang XI Abschnit 1, 1.	Generell GPAI: Beschreibung von KI-M allgemein; inkl. Aufgaben; Wesen der KI-S in die es integriert werden soll; Elemente = Architektur u. Parameter sowie Modalität	-	-	-		
Anhang XI Abschnit 1, 2.	Elemente mit Entwicklungsverfahren; notwendige Infrastruktur der KI-M; Entwurfspezifikation inkl. Trainingsmethoe; Optimierung u. Parameter; Rechenressourcen u. Energieverbrauch	-	-	Infrastruktur kein Element von KI-M, sondern v. KI-S? Welche Rolle spielt die verwendete Infrastruktur im KI-M?	Wichtig für Layer-Modell	
Anhang XI Abschnit 2, 1.	GPAI System-Risk: Prüfstrategien u. Prüfergebnisse, Protokolle; Prüfmethode;	-	-	Was ist eine Modellanpassung?!	Wichtig für Layer-Modell	
Anhang XI Abschnit 2, 2.	Modellanpassungen bzgl. Ausrichtung und Feinabstimmung;	-	-	-		

Anhang XI Abschnit 2, 3.	Softwarekomponenten; wie diese aufeinander aufbauen und einander zuarbeiten	-	-	Welche Rolle spielt die verwendete Software im KI-M?	Wichtig für Layer-Modell	
Anhang XII 1.	Doku für nachgelagerte Anbieter von GPAI: Zusätzliche Doku von Interaktion mit Hardware des KI-S; Versionnen	-	-	-		
Anhang XII 2.	Format der Ein- und Ausgaben und deren maximale Größe; Datenherkunft und Aufbereitungsmethoden	-	-	-		
Anhang XIII	Sehr spezfisch für GPAI System-Risk: Eigener Datensatz -> Token, Modalität etc. Auswirkungen auf Binnenmarkt	-	-	unabhängig von Leistung: systemisch ist GPAI mit über 10.000 niedergelassenen gewerblichen Nutzern (i.S.v. Betreibern); Anzahl registrierter Endnutzer		
3. Gründe						
Ziffer 12	-	-	Modelle oder Algorithmen oder beides aus Daten ableiten	Ausführliche Erläuterung von KI-S, aber nur wenig Info zu Modellen	-	-
Ziffer 25	-	-	Ausnahme der Forschung; Modelle vor Inbetriebnahme immer geschützt	-	-	-
Ziffer 27	-	-	Grundrechte u. Ökologie sollten auch bei KI-M einfließen. Basis für Verhaltenskodizes	-	-	-
Ziffer 67	-	-	Data Governance für KI-M u.a. in Hochrisiko-KI; Submodelle zur Validierung eines Systems?!	-	-	-
Ziffer 76	-	-	Angriffe auf trainierte Modelle/Cybersicherheit u.a. in Hochrisiko-KI	-	-	-
Ziffer 88	-	-	Wertschöpfungskette: Viele verschiedene Komponenten u. Services, darunter Trainieren und Neutrainieren, Integration von Software u. andere Aspekte der Modellentwicklung	-	-	-
Ziffer 89	Achtung: die nicht GPAI, aber open Source sind!	-	Freiwillig?! Modellkarten u. Datenblätter in Wertschöpfungskette für Instrumente, Dienste, Verfahren, KI-Komponenten; KI-M, die nicht GPAI und nicht open Source sind	-	-	-
Ziffer 97	Klare Abgrenzung GPAI u. KI-S erforderlich; Auslieferung von GPAI als Bibliothek, Schnittstelle, Download o. Kopie; Für KI-S ist Nutzerschnittstelle notwendig Ausnahme für eigene Modelle, die rein interne Verfahren betreffen u. kaum Außenwirkung haben. EVOLUTION: Von Forschung zu GPAI u. Prototypen	-	-	wichtiger Punkt am Ende: Der EU AI Act geht auch von Evolution von KI-M aus -> von Forschung bis GPAI inkl. Zwischenstufen.	-	-
Ziffer 98	eine Milliarde Parameter als Kriterium für GPAI u. universelle Nutzung u. unterschiedliche Aufgaben	-	-	-	-	-
Ziffer 99	Große generative KI-M typischer Fall für GPAI	-	kleine generative KI-M als sonstiges KI-M	-	-	-
Ziffer 100	Einsatz von GPAI in KI-S führt zu KI-S mit allgemeinem Verwendungszweck. Dieses kann wiederum in andere KI-S integriert werden.	-	-	-	-	-
Ziffer 101	Dokumentation von GPAI für Akteure in Wertschöpfungskette u. Büro; Transparenzerfordernisse	-	-	-	EU kann Vorgaben entwickeln für Dokumentation	

Ziffer 102	Open Source GPAI: Parameter, einschließlich Gewichte, Informationen über die Modellarchitektur und Informationen über die Modellnutzung; Änderung von GPAI mit Open Source möglich	-	-	-		
Ziffer 103	GPAI gilt genauso	-	"Modelle" quelloffene Komponenten sowie Instrumente, Dienste o. Verfahren sowie Software u. Daten	-	Trennung von Modellen, Diensten	
Ziffer 104	GPAI mit Open Source Strategie zur Einhaltung des Urheberrechts. Ist ungleich Informationen über den für das Trainieren oder die Feinabstimmung des Modells verwendeten Datensatz	-		-		
Ziffer 105	Große generative KI-M typischer Fall für GPAI; Data-Mining; Urheberrecht	-		-	Urheberrecht muss auch bei allen anderen KI-M wichtig!	
Ziffer 106	GPAI benötigt Strategie zur Einhaltung des Urheberrechts u. Schutzrechte			-	Gilt auch für sonstige KI	
Ziffer 107	Differenzierung von Vor-Training u. Training: Transparenz bzgl. genutzter Inhalte. Nutzung öffentlicher Datenbanken oder Datenarchive?! Erläuterung von Datenquellen			-		
Ziffer 108	Überwachung der Pflichten von Ziffer 108			-		
Ziffer 109	Grundsatz der Verhältnismäßigkeit		Ermutigung freiwilliger Erfüllung	-	wichtig!	
Ziffer 110	systemischen Risiken während des gesamten Lebenszyklus des Modells; Bedingungen einer Fehlanwendung, der Zuverlässigkeit des Modells, der Modellgerechtigkeit und der Modellsicherheit, dem Grad der Autonomie des Modells, seinem Zugang zu Instrumenten, neuartigen oder kombinierten Modalitäten; Risiken, dass Modelle sich selbst vervielfältigen, oder der „Selbstreplikation“ oder des Trainings anderer Modelle; der Art und Weise, wie Modelle zu schädlichen Verzerrungen und Diskriminierung mit Risiken für Einzelpersonen, Gemeinschaften oder Gesellschaften führen können		das ist allgemein wichtig!!!	-	wichtig!	
Ziffer 111	Indikatoren für GPAI-System-Risk; Schwellenwerte; Recht auf Widerspruch			gibt es auch ein Recht auf Widerspruch, dass ein KI-M kein GPAI ist?	wichtig!	
Ziffer 112	Verfahren für die Einstufung eines KI-M mit allgemeinem Verwendungszweck muss präzisiert werden; Besondere Merkmale; Antizipation der Weiterentwicklung von GPAI durch Büro bei Open Source erschwert!			Allgemeine Merkmale und Besondere Merkmale! Terminologie	wichtig!	
Ziffer 113	Ausweisung als GPAI System-Risk durch Büro möglich					
Ziffer 114	Cybersecurity abhängig davon, ob embedded in KI-S oder eigentständig; Angriffstests			Schwellenmodell für KI-S: Vor Inverkehrbringen; danach; GPAI u. GPAI Sys. Risk		

Ziffer 115	Meldepflichten; Cybersicherheit; Modelldiebstahl; Schutz könnte durch die Sicherung von Modellgewichten, Algorithmen, Servern und Datensätzen erleichtert werden, z. B. durch Betriebssicherheitsmaßnahmen für die Informationssicherheit, spezifische Cybersicherheitsstrategien, geeignete technische und etablierte Lösungen sowie Kontrollen des physischen Zugangs				Modelldiebstahl ist interessant	
Ziffer 116	Praxisleitfäden wichtig; Beteiligung von GPAI-Anbietern u. sonstigen Stakeholdern					
Ziffer 117	Verhaltenskodizes; harmonisierte Normen u. alternative Mittel					
Ziffer 118			Allgemein: KI-S u. KI-M werden reguliert; nennung von Digital Service Act für "sehr große" Suchmaschinen			
Ziffer 133			Erzeugung synthetischer Daten; Kennzeichnungspflichten; Ebene des KI-Ss oder der Ebene des KI-Ms, darunter KI-M mit allgemeinem Verwendungszweck zur Erzeugung von Inhalten			
Ziffer 151	Wissenschaftliches Gremium					
Ziffer 161	Aufsicht über KI-S, die auf GPAI beruhen u. System u. Modell gemeinsamen Anbieter haben -> Büro! Keine Zuständigkeit der nationalen Behörde; grenzüberschreitende Amtshilfe			Problem bei mehrfach verschachtelten KI-S!		
Ziffer 164	Durchsetzungsrechte u. Verfahrensrechte					
Ziffer 165			Darüber hinaus sollten die Anbieter und gegebenenfalls die Betreiber aller KI-S, ob mit hohem Risiko oder nicht, und aller KI-M ermutigt werden, freiwillig zusätzliche Anforderungen anzuwenden; Sie sollten außerdem in inklusiver Weise entwickelt werden, gegebenenfalls unter Einbeziehung einschlägiger Interessenträger wie Unternehmensverbände und Organisationen der Zivilgesellschaft, Wissenschaft, Forschungsorganisationen, Gewerkschaften und Verbraucherschutzorganisationen	Kommunalverbände als eigene Gruppe!	wichtig! Dafür gleiche Grundmuster notwendig	
Ziffer 169	Durchsetzung mit Geldbußen					
Ziffer 173	Erlass von Rechtsakten durch Kommission zur Anpassung					
Ziffer 174	Neubewertung alle vier Jahre; bgzl GPAI u.a. Energieeffizienz			-		
Ziffer 175	Verkürzte Fristen für GPAI, da hier besonders hohes Innovationstempo			-		
Auslegung EU AI Act 2024						
Historische Auslegung (verliert mit zunehmendem Alter einer Norm an Bedeutung, daher bei jungen Normen sehr wichtig) u.a.: In der Version 2021 wurde das Wort "Modell" nur zweimal in Artikeln verwendet -> Artikel 10 Data Governance und 15 Genauigkeit, Robustheit und Cybersicherheit Mit Neufassung 2024 wurde in den gleichen Artikeln das Wort "Modell" durch "KI-M" ersetzt -> beide Begriffe werden synonym verwendet						

Mit der Neufassung 2024 werden GPAI (mit und ohne systemische Risiken) umfassend geregelt, aber die Vorschriften für KI-M in High-Risk mit und ohne GPAI beibehalten
Historisch sind damit vor allem die Artikel 10 und 15 am wichtigsten, um generelle Merkmale für KI-M abzuleiten, da schon in der Version 2021 der Behörden KI-S selbst bzgl. Risiken prüfen können (Art. 65 a.F.; Art. 76 n.F)
Auch in Gründen und Anhängen in Vorversion kaum Nennung von "Modell"; die Nennung "datengesteuerter KI-M" wurde zudem gelöscht
hoher Zeitdruck erlaubt die Deutung, dass genereller Begriff der KI-M in Kürze der Zeit nicht umfassend geklärt werden konnten

Grammatikalische Auslegung (Wortsinn) u.a.:
Laut Art (2) 2 gilt der Act nicht für Anbieter sonstiger KI-M! Aber: Widerspruch zu Rückschluss aus Art. 2 (2/8), da auch für KI-M gilt, die nicht Forschung sind?! Beide Ansichten möglich
Der Wortlaut ist aber auch u.a. bei Art. 10/15 wichtig, da hier Kriterien für KI-M in Hochrisiko-KI-S aufgelistet werden die nicht diesen allgemeinen Verwendungszweck voraussetzen. U.A. Trennung von KI-S die, KI-M trainieren u. anderen KI-S, die keine KI-M trainieren.
Artikel 15 trennt model poisoning von data poisoning
KI-M können Bestandteil von KI-S sein - KI-S haben (immer) ein KI-M
Die Abgrenzung von KI-M und -sytemen ist insbesondere durch ein Interaktionsinterface gekennzeichnet, ansonsten sind Übergänge trotz Legaldefinition von KI-S nicht trennscharf (siehe insbes. Gründe 97)
KI-M haben allgemeine und besondere Merkmale
KI-M unterliegen einer Evolution u.a.: Forschung, vor Inverkehrbringung, einfache Inverkehrbringung, multiple Nutzungszwecke, systemische Risiken, außer Verkehrnahme
Trennung von vortrainierten und nachtrainierten Modellen
Wortlaut unterstellt, dass gleiche Vorgaben für alle Arten von KI-M freiwillig z.B. in Verhaltenskodizes verwendet werden können
große generative KI-M als Beispiel für GPAI -> Rückschluss: Kleine generative KI-M keine GPAI, aber Evolution möglich
unklare Verwendung von weiteren Begriffen, u.a. "Instrumente, Dienste, Verfahren, KI-Komponenten"
Bzgl. Verhaltenskodizes unscharfe Abgrenzung zu "alternativen Mitteln"

Teleologische Auslegung (welches Ziel soll mit Norm erreicht werden) u.a.:
EU AI Act soll sich hoher Entwicklungsgeschwindigkeit dynamisch anpassen; dabei Innovation von KI-M offenkundig besonders wichtig
Gesetzgeber will Innovationsentwicklung auch künftig bestmöglich antizipieren können -> vergleichbare Kriterien für KI-M aller Art erforderlich
gleiche Ziele u. Kriterien für KI-Anbieter aller Art, u.a. bzgl. Verhaltenskodizes
Open Source KI-M erfordern nicht nur ähnliche Kriterien wie alle anderen KI-M, sondern besonders spezifische
Da Life Cycle erwähnt wird, ist Problem der Gültigkeit für Anbieter sonstiger KI-M Art. 2 (

Systematische Auslegung (jede Rechtsnorm so auszulegen ist, dass sie sich in das Ganze einfügt) u.a.:
In der neuen Version von 2024 beziehen sich die Aussagen zu KI-M in statistischer Hinsicht weit überwiegend auf GPAI - durch den Zusatz "mit allgemeinem Verwendungszweck".
Gilt der EU AI Act gem. Artikel 2 nur für Anbieter von KI-S und GPAI? Folge: Gilt nicht für Anbieter von (sonstigen) KI-M, die in Hochrisiko-KI enthalten sind! Wertschöpfungskette! Anbieter KI-S verantwortlich für KI-M

Summarische Auslegungsergebnis: KI-M hat allgemeine u. gestufte, besondere Merkmale (bezogen auf Wirkung u. Bestandteile) Betrachtung von gesamten Lebens-Cyklus erforderlich "von der Wiege bis zur Bahre Formulare ..." Trainings-, Validierungs- und Testdatensätze Trainingsmodelle, Vor- und Nachtrainieren Zuverlässigkeit des Modells, der Modellgerechtigkeit und Modellsicherheit Parameter, Gewichte, Modellarchitektur, Modellnutzung generative KI-M erst ab gewisser Größe GPAI verschiedene Modalitäten von KI-M Abgrenzung zu KI-S letztlich primär über Nutzerschnittstelle, sonst unscharf Differenzierung von KI-S, die KI-M trainieren und anderen KI-S	