Smart.Recht

KI-VO

Verordnung über künstliche Intelligenz
(Artificial Intelligence Act)

KI-generierte Erläuterung
in einfacher Sprache 

Herausgeber
Univ.-Prof. Dr. Wolfgang Zankl,
Vorstand des Instituts für digitale Transformation
und künstliche Intelligenz
Sigmund Freud Privatuniversität Wien | Berlin

Mitarbeiter:innen
Sarah Dicher, LL.M.
Mag.a Alexandra Kijek
Mag. Florian Madner
Mag. Dr. Marlon Possard, MSc, MA
Mariam Soliman
Florian Wienert, LL.M.

Redaktionelle Notiz: In seiner Gesamtheit versteht sich dieses Werk als persönlich verantwortete wissenschaftliche Ausarbeitung, bei der KI als Assistenzsystem im Rahmen des eigenschöpferischen Schaffens eingesetzt wurde.

Inhalt

Vorwort Univ.-Prof. Dr. Wolfgang Zankl, Vorstand des Instituts für digitale Transformation und künstliche Intelligenz der SFU Wien|Berlin 9

Geleitwort DI Harald Leitenmüller, CTO Microsoft Österreich 12

Geleitwort Dr. Klaus Steinmaurer, Leiter der österreichischen KI-Servicestelle 14

Abkürzungsverzeichnis 18

Artikel 1 KI-VO (Gegenstand) 20

Artikel 2 KI-VO (Anwendungsbereich) 23

Artikel 3 KI-VO (Begriffsbestimmungen) 29

Artikel 4 KI-VO (KI-Kompetenz) 52

Artikel 5 KI-VO (Verbotene Praktiken im KI-Bereich) 54

Artikel 6 KI-VO (Einstufungsvorschriften für Hochrisiko-KI-Systeme) .. 66

Artikel 7 KI-VO (Änderungen des Anhangs III) 73

Artikel 8 KI-VO (Einhaltung der Anforderungen) 81

Artikel 9 KI-VO (Risikomanagementsystem) 81

Artikel 10 KI-VO (Daten und Daten-Governance) 89

Artikel 11 KI-VO (Technische Dokumentation) 92

Artikel 12 KI-VO (Aufzeichnungspflichten) 99

Artikel 13 KI-VO (Transparenz und Bereitstellung von Informationen für die Betreiber) 102

Artikel 14 KI-VO (Menschliche Aufsicht) 103

Artikel 15 KI-VO (Genauigkeit, Robustheit und Cybersicherheit) 111

Artikel 16 KI-VO (Pflichten der Anbieter von Hochrisiko-KI-Systemen) 115

Artikel 17 KI-VO (Qualitätsmanagementsystem) 118

Artikel 18 KI-VO (Aufbewahrung der Dokumentation) 123

Artikel 19 KI-VO (Automatisch erzeugte Protokolle) 126

Artikel 20 KI-VO (Korrekturmaßnahmen und Informationspflicht) 129

Artikel 21 KI-VO (Zusammenarbeit mit den zuständigen Behörden) . 132

Artikel 22 KI-VO (Bevollmächtigte der Anbieter von Hochrisiko-KI-Systemen) 135

Artikel 23 KI-VO (Pflichten der Einführer) 140

Artikel 24 KI-VO (Pflichten der Händler) 145

Artikel 25 KI-VO (Verantwortliche entlang der KI-Wertschöpfungskette) 150

Artikel 26 KI-VO (Pflichten der Betreiber von Hochrisiko-KI-Systemen) 155

Artikel 27 KI-VO (Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme) 163

Artikel 28 KI-VO (Notifizierende Behörden) 168

Artikel 29 KI-VO (Antrag einer Konformitätsbewertungsstelle auf Notifizierung) 173

Artikel 30 KI-VO (Notifizierungsverfahren) 177

Artikel 31 KI-VO (Anforderungen an notifizierte Stellen) 182

Artikel 32 KI-VO (Vermutung der Konformität mit den Anforderungen an notifizierte Stellen) 189

Artikel 33 KI-VO (Zweigstellen notifizierter Stellen und Vergabe von Unteraufträgen) 193

Artikel 34 KI-VO (Operative Pflichten der notifizierten Stellen) 196

Artikel 35 KI-VO (Identifizierungsnummern und Verzeichnisse notifizierter Stellen) 199

Artikel 36 KI-VO (Änderungen der Notifizierung) 201

Artikel 37 KI-VO (Anfechtung der Kompetenz notifizierter Stellen) .. 200

Artikel 38 KI-VO (Koordinierung der notifizierten Stellen) 210

Artikel 39 KI-VO (Konformitätsbewertungsstellen in Drittländern) ... 213

Artikel 40 KI-VO (Harmonisierte Normen und Normungsdokumente) 215

Artikel 41 KI-VO (Gemeinsame Spezifikationen) 219

Artikel 42 KI-VO (Vermutung der Konformität mit bestimmten Anforderungen) 223

Artikel 43 KI-VO (Konformitätsbewertung) 226

Artikel 44 KI-VO (Bescheinigungen) 231

Artikel 45 KI-VO (Informationspflichten der notifizierten Stellen) 234

Artikel 46 KI-VO (Ausnahme vom Konformitätsbewertungsverfahren) 237

Artikel 47 KI-VO (EU-Konformitätserklärung) 241

Artikel 48 KI-VO (CE-Kennzeichnung) 245

Artikel 49 KI-VO (Registrierung) 248

Artikel 50 KI-VO (Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme) 252

Artikel 51 KI-VO (Einstufung von KI-Modellen mit allgemeinem Verwendungszweck als KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko) 259

Artikel 52 KI-VO (Verfahren) 263

Artikel 53 KI-VO (Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck) 268

Artikel 54 KI-VO (Bevollmächtigte der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck) 274

Artikel 55 KI-VO (Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko) 279

Artikel 56 KI-VO (Praxisleitfäden) 283

Artikel 57 KI-VO (KI-Reallabore) 288

Artikel 58 KI-VO (Detaillierte Regelungen für KI-Reallabore und deren Funktionsweise) 296

Artikel 59 KI-VO (Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor) 302

Artikel 60 KI-VO (Tests von Hochrisiko-KI-Systemen unter Realbedingungen außerhalb von KI-Reallaboren) 308

Artikel 61 KI-VO (Informierte Einwilligung zur Teilnahme an einem Test unter Realbedingungen außerhalb von KI-Reallaboren) 304

Artikel 62 KI-VO (Maßnahmen für Anbieter und Betreiber, insbesondere KMU, einschließlich Start-up-Unternehmen) 319

Artikel 63 KI-VO (Ausnahmen für bestimmte Akteure) 323

Artikel 64 KI-VO (Büro für Künstliche Intelligenz) 326

Artikel 65 KI-VO (Einrichtung und Struktur des Europäischen Gremiums für Künstliche Intelligenz) 329

Artikel 66 KI-VO (Aufgaben des KI-Gremiums) 334

Artikel 67 KI-VO (Beratungsforum) 341

Artikel 68 KI-VO (Wissenschaftliches Gremium unabhängiger Sachverständiger) 345

Artikel 69 KI-VO (Zugang zum Pool von Sachverständigen durch die Mitgliedstaaten) 350

Artikel 70 KI-VO (Benennung von zuständigen nationalen Behörden und zentrale Anlaufstelle) 354

Artikel 71 KI-VO (EU-Datenbank für die in Anhang III aufgeführten Hochrisiko-KI-Systeme) 359

Artikel 72 KI-VO (Beobachtung nach dem Inverkehrbringen durch die Anbieter und Plan für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme) 363

Artikel 73 KI-VO (Meldung schwerwiegender Vorfälle) 367

Artikel 74 KI-VO (Marktüberwachung und Kontrolle von KI-Systemen auf dem Unionsmarkt) 372

Artikel 75 KI-VO (Amtshilfe, Marktüberwachung und Kontrolle von KI-Systemen mit allgemeinem Verwendungszweck) 379

Artikel 76 KI-VO (Beaufsichtigung von Tests unter Realbedingungen durch Marktüberwachungsbehörden) 383

Artikel 77 KI-VO (Befugnisse der für den Schutz der Grundrechte zuständigen Behörden) 387

Artikel 78 KI-VO (Vertraulichkeit) 391

Artikel 79 KI-VO (Verfahren auf nationaler Ebene für den Umgang mit KI-Systemen, die ein Risiko bergen) 396

Artikel 80 KI-VO (Verfahren für den Umgang mit KI-Systemen, die vom Anbieter gemäß Anhang III als nicht hochriskant eingestuft werden) 402

Artikel 81 KI-VO (Schutzklauselverfahren der Union) 406

Artikel 82 KI-VO (Konforme KI-Systeme, die ein Risiko bergen) 410

Artikel 83 KI-VO (Formale Nichtkonformität) 401

Artikel 84 KI-VO (Unionsstrukturen zur Unterstützung der Prüfung von KI) 405

Artikel 85 KI-VO (Recht auf Beschwerde bei einer Marktüberwachungsbehörde) 421

Artikel 86 KI-VO (Recht auf Erläuterung der Entscheidungsfindung im Einzelfall) 424

Artikel 87 KI-VO (Meldung von Verstößen und Schutz von Hinweisgebern) 427

Artikel 88 KI-VO (Durchsetzung der Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck) 429

Artikel 89 KI-VO (Überwachungsmaßnahmen) 432

Artikel 90 KI-VO (Warnungen des wissenschaftlichen Gremiums vor systemischen Risiken) 435

Artikel 91 KI-VO (Befugnis zur Anforderung von Dokumentation und Informationen) 439

Artikel 92 KI-VO (Befugnis zur Durchführung von Bewertungen) 443

Artikel 93 KI-VO (Befugnis zur Aufforderung zu Maßnahmen) 448

Artikel 94 KI-VO (Verfahrensrechte der Wirtschaftsakteure des KI-Modells mit allgemeinem Verwendungszweck) 452

Artikel 95 KI-VO (Verhaltenskodizes für die freiwillige Anwendung bestimmter Anforderungen) 455

Artikel 96 KI-VO (Leitlinien der Kommission zur Durchführung dieser Verordnung) 459

Artikel 97 KI-VO (Ausübung der Befugnisübertragung) 463

Artikel 98 KI-VO (Ausschussverfahren) 467

Artikel 99 KI-VO (Sanktionen) 470

Artikel 100 KI-VO (Verhängung von Geldbußen gegen Organe, Einrichtungen und sonstige Stellen der Union) 476

Artikel 101 KI-VO (Geldbußen für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck) 481

Artikel 102 KI-VO (Änderung der Verordnung (EG) Nr. 300/20) 486

Artikel 103 KI-VO (Änderung der Verordnung (EU) Nr. 167/2013) 489

Artikel 104 KI-VO (Änderung der Verordnung (EU) Nr. 168/2013) 492

Artikel 105 KI-VO (Änderung der Richtlinie 2014/90/EU) 495

Artikel 106 KI-VO (Änderung der Richtlinie (EU) 2016/797) 498

Artikel 107 KI-VO (Änderung der Verordnung (EU) 2018/858) 501

Artikel 108 KI-VO (Änderungen der Verordnung (EU) 2018/1139) 504

Artikel 109 KI-VO (Änderung der Verordnung (EU) 2019/2144) 508

Artikel 110 KI-VO (Änderung der Richtlinie (EU) 2020/1828) 511

Artikel 111 KI-VO (Bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme und bereits in Verkehr gebrachte KI-Modelle mit allgemeinem Verwendungszweck)..... 500

Artikel 112 KI-VO (Bewertung und Überprüfung) 518

Artikel 113 KI-VO (Inkrafttreten und Geltungsbeginn)..... 524

Anhang I KI-VO (Liste der Harmonisierungsrechtsvorschriften der Union) 528

Anhang II KI-VO (Liste der Straftaten gemäß Artikel 5 Absatz 1 Unterabsatz 1 Buchstabe h Ziffer iii) 534

Anhang III KI-VO (Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2) . 538

Anhang IV KI-VO (Technische Dokumentation gemäß Artikel 11 Absatz 1) 547

Anhang V KI-VO (EU-Konformitätserklärung)..... 554

Anhang VI KI-VO (Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle) 558

Anhang VII KI-VO (Konformität auf der Grundlage einer Bewertung des Qualitätsmanagementsystems und einer Bewertung der technischen Dokumentation)..... 561

Anhang VIII KI-VO (Bei der Registrierung des Hochrisiko-KI-Systems gemäß Artikel 49 bereitzustellende Informationen)..... 569

Anhang IX KI-VO (Bezüglich Tests unter Realbedingungen gemäß Artikel 60 bei der Registrierung von in Anhang III aufgeführten Hochrisiko-KI-Systemen bereitzustellende Informationen) 575

Anhang X KI-VO (Rechtsvorschriften der Union über IT-Großsysteme im Raum der Freiheit, der Sicherheit und des Rechts)..... 578

Anhang XI KI-VO (Technische Dokumentation gemäß Artikel 53 Absatz 1 Buchstabe a — technische Dokumentation für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck) 584

Anhang XII KI-VO (Transparenzinformationen gemäß Artikel 53 Absatz 1 Buchstabe b — technische Dokumentation für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck für nachgelagerte Anbieter, die das Modell in ihr KI-System integrieren) 589

Anhang XIII KI-VO (Kriterien für die Benennung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko gemäß Artikel 51) 593

Dokumentation der Vorgehensweise zur Erstellung des Kommentars zur KI-VO 582

Vorwort

Bedeutung und Anwendung einer niederschwelligen Erläuterung zur KI-Verordnung

Von Univ.-Prof. Dr. Wolfgang Zankl
Vorstand des Instituts für digitale Transformation und künstliche Intelligenz der SFU Wien | Berlin

Die KI-Verordnung (EU-Verordnung über künstliche Intelligenz = Artificial Intelligence Act) gilt in allen EU-Mitgliedsstaaten, und zwar auch für alle internationalen Anbieter, soweit deren KI-Plattformen in der EU abrufbar sind. Der Rechtsakt ist insofern ein Meilenstein, als er die weltweit bisher umfangreichste Regulierung dieser Materie darstellt. Die Komplexität und die Technologielastigkeit Künstlicher Intelligenz (KI) haben allerdings dazu geführt, dass viele Bestimmungen selbst für erfahrene Jurist:innen nur schwer nachvollziehbar sind. Dies hat den Herausgeber auf die Idee gebracht, eine Darstellung zu konzipieren, die auch für Laien oder juristische KI-Einsteiger:innen leicht verständlich ist. Da ChatGPT mittlerweile weit schneller und besser als die meisten Fachleute textieren kann und auch rechtlich mittlerweile so gut ist, dass das Programm bei der US-amerikanischen Rechtsanwaltsprüfung (Bar Exam) in der Version 4.0 besser abgeschnitten hat als 90% der menschlichen Kandidat:innen, lag es nahe, ChatGPT (nun in der aktuellen und noch stärkeren Version 5) dafür heranzuziehen. Und in der Tat ist es damit – soweit ersichtlich – erstmals gelungen, eine gesamte Erläuterung der KI-Verordnung auf diese Weise generieren zu lassen. Dies allerdings nicht durch einfachen Mausklick mit dem Befehl „verfasse eine Darstellung der KI-Verordnung in verständlicher Sprache“, sondern auf der Basis intensiver Vorarbeiten, insbesondere in Bezug auf die Strukturierung, das Sprachniveau und die Entwicklung präziser Befehlsvorgaben an das Programm (Prompts, siehe dazu im Einzelnen hier).

Auf diesem Wege ist es mit verschiedenen Abstimmungsprozessen gelungen, den Text – in ca einem Viertel der Zeit, die ein herkömmliches Werk dieses Umfangs benötigt hätte – rein KI-generiert zu erstellen. Soweit dem Herausgeber oder seinen engagierten und kompetenten Mitarbeiter:innen als „Humans in the Loop“ bei Plausibilitätskontrollen (nur solche wurden durchgeführt) Ungenauigkeiten oder – sehr vereinzelt – Unrichtigkeiten aufgefallen sind, wurde dies, abgesehen von seltenen Grammatik- oder Rechtschreibfehlern, nicht selbst korrigiert, sondern das Programm aufgefordert, durch Neutextierung Klarheit bzw Richtigkeit zu schaffen. Sohin ist tatsächlich der gesamte Kommentartext von ChatGPT.

Bemerkenswert ist dabei auch, dass das berühmt-berüchtigte Halluzinieren nicht zum Tragen kam. Dies ist wohl vor allem darauf zurückzuführen, dass

ChatGPT die Vorgabe hatte, als Quellen keine Gerichtsentscheidungen und Fachbeiträge zu verwenden (die manchmal fehlinterpretiert oder erfunden werden, also Folge einer Halluzination sind), sondern ausschließlich die Erwägungsgründe der jeweiligen Artikel (das sind Erläuterungen der Europäischen Parlaments) und die sog Leitlinien (das sind Auslegungsempfehlungen der Europäischen Kommission). Diese Reduktion der Quellen hat sich auch daraus ergeben, dass Nichtjurist:innen idR keinen Zugang zu Fachliteratur haben und selbst wenn, diese Beiträge in „Juristendeutsch" verfasst und damit für Nichtjurist:innen schwer verständlich sind. Trotz oder gerade wegen dieser Reduktion ist es gelungen, zu jedem Artikel eine leicht verständliche Erklärung des Artificial Intelligence Act mit zahlreichen Beispielen zu verfassen.

Dank gebührt dafür nicht nur ChatGPT bzw OpenAI selbst, sondern auch den Mitarbeiter:innen des Herausgebers, die ganz wesentlich zum Gelingen dieses innovativen Projekts beigetragen haben. Insbesondere *Florian Wienert, LL.M.*, hat sich dabei durch geschicktes Prompt-Engineering hervorgetan. Aber auch alle anderen Mitarbeiter:innen haben mit ihrem Engagement und ihrem zeitgemäßen Arbeitsstil wichtige Beiträge zu einem Werk geleistet, das es in dieser Form noch nicht gegeben hat.

In diesem Sinne bedankt sich der Herausgeber auch beim Verlag MANZ, der sich dazu entschieden hat, dieses neuartige Produkt in sein Portfolio aufzunehmen, und hofft, damit neben seinem ebenfalls bei MANZ herausgegebenen Fachkommentar zur KI-Verordnung zum besseren, allgemeinen und damit inklusiven Verständnis dieser neuen und bahnbrechenden Rechtsmaterie beitragen zu können. Vor diesem Hintergrund wird Smart.Recht vom Herausgeber kostenlos zur Verfügung gestellt. Ferner wurde in diesem Sinne niederschwelliger Zugänglichkeit versucht, den Kommentar durch ein detailliertes und verlinktes Inhaltsverzeichnis auch für Nutzer:innen ohne jedwede Erfahrung mit KI-Recht möglichst übersichtlich und einfach anwendbar zu machen.

Trotz der erwähnten Kontrollmechanismen ist es im Hinblick auf die BlackBox, als die KI oft bezeichnet wird, weil nicht im Detail nachvollziehbar ist, wie sie zu ihren Texten kommt, nicht auszuschließen, dass die eine oder andere Erläuterung ungenau oder gar inkorrekt ist (aufgefallen sind solche Halluzinationen allerdings weder dem Herausgeber noch seinen Mitarbeiter:innen). Für allfällige Fehler kann daher im Hinblick auf die Neuheit und noch nicht vollständige Durchschaubarkeit der Materie keine Verantwortung übernommen werden. Insbesondere für Jurist:innen empfiehlt sich eine entsprechende Kontrolle bzw können diesbezüglich sogar vertrags- und/oder standesrechtliche Verpflichtungen bestehen. Insofern versteht sich der vorliegende Text nicht als abschließende Erläuterung mit Richtigkeitsgewähr, sondern als ein modernes Kompendium, das von Jurist:innen zwar Plausibilitätschecks unterzogen

wurde, und vor allem aber ein besseres Verständnis der komplizierten Rechtstexte ermöglich soll. Dies bringt auch die Bezeichnung „Smart.Recht" zum Ausdruck: es handelt sich um ein Werk, das in verständlicher Sprache Laien und nichtspezialisierten Jurist:innen einen einfachen und cleveren Zugang zur komplexen Materie des KI-Rechts gewährt.

Damit ist ein neues Kapitel der Rechtswissenschaft aufgeschlagen. Selbst umfangreiche Fachtexte können nun durch KI bzw ihre „richtige" Anwendung (die eigene Kompetenzen erfordert) artifiziell verfasst werden. Ein Szenario, das der Herausgeber bei einem der ersten öffentlichen Vorträge über KI und Recht trotz verschiedenster – inzwischen zumeist eingetretener – Prognosen nicht auf dem Radar hatte (2001 im Rahmen der Kick-off Veranstaltung seines „europäischen zentrums für e-commerce und internetrecht" im Wiener Gartenbaukino zum seinerzeit neuen Film „Artificial Intelligence" von Steven Spielberg). Dies dürfte daran liegen, dass generative KI in der heutigen Form der LLMs (Large Language Models) damals noch (lange) nicht existierte. Jetzt – ein Vierteljahrhundert später – sind es diese generativen Modelle, die das Zeitalter Künstlicher Intelligenz, in dem wir noch ganz am Anfang stehen, eingeläutet haben. In weiteren 25 Jahren wird diese Entwicklung nach Einschätzung des Herausgebers zu transformativen und wohl auch disruptiven Umwälzungen führen, die es in der Menschheitsgeschichte so noch nicht gegeben hat.

Wien, März 2026 *Wolfgang Zankl*

Geleitwort

Zugang schaffen, Verantwortung leben: KI für alle

Von DI Harald Leitenmüller, Chief Technology Officer,
Microsoft Österreich

Die rasante Entwicklung Künstlicher Intelligenz stellt unsere Gesellschaft vor große Chancen – und ebenso große Herausforderungen. Mit der KI-Verordnung wird erstmals ein umfassender Rechtsrahmen für den Einsatz Künstlicher Intelligenz geschaffen. Ziel ist es, Innovation zu ermöglichen und zugleich Schutzmechanismen für Menschen und Gesellschaft vorzusehen. Die Verordnung adressiert Risiken, setzt Mindeststandards und trägt so dazu bei, das Vertrauen in KI zu stärken.

Doch Regulierung allein genügt nicht: Entscheidend ist, dass die Regeln und ihre Bedeutung für alle Menschen verständlich und zugänglich werden. Genau hier setzt das vorliegende Werk an. Was es so besonders macht: Es wurde vollständig mit Hilfe von generativer KI erstellt – und zwar in einer Sprache, die auch für Nicht-Jurist:innen, für Laien und Einsteiger:innen nachvollziehbar ist. Damit wird ein Meilenstein gesetzt: Komplexe juristische Materie wird für die breite Gesellschaft geöffnet, Barrieren werden abgebaut, Inklusion und Fairness werden nicht nur gefordert, sondern praktisch umgesetzt.

Als jemand, der in Responsible AI-Trainings seit jeher das Prinzip „People First“ betont, erfüllt es mich mit Freude und Stolz, dass diese Initiative ergriffen wurde. Denn nur wenn wir die Menschen in den Mittelpunkt stellen – ihre Bedürfnisse, ihre Fragen, ihre Rechte –, kann Künstliche Intelligenz ihr volles Potenzial zum Wohl der Gesellschaft entfalten. Zugänglichkeit ist dabei kein „Nice-to-have“, sondern ein zentrales Element von Verantwortung und Gerechtigkeit.

Mein besonderer Dank gilt dem engagierten Team um Univ.-Prof. Dr. *Wolfgang Zankl,* das mit Kreativität, Sorgfalt und technischem Know-how gezeigt hat, was mit KI möglich ist, wenn sie verantwortungsvoll eingesetzt wird. Damit wurde nicht nur ein juristisches Werk geschaffen, sondern ein Beispiel für die Zukunft interdisziplinärer Zusammenarbeit geliefert. Smart.Recht macht deutlich, wie KI in unterschiedlichen Disziplinen Brücken bauen kann – zwischen Recht und Technik, zwischen Wissenschaft und Praxis, zwischen Expert:innen und Bürger:innen.

Ebenso danke ich Univ.-Prof. Dr. *Wolfgang Zankl* selbst, dem Erfinder und Umsetzer von Smart.Recht. Er hat als Herausgeber, Mentor und Impulsgeber diese innovative Arbeit ermöglicht, begleitet und finalisiert. Sein Mut, neue Wege zu gehen, und sein Einsatz für eine verständliche, inklusive Rechtskultur verdienen höchste Anerkennung.

Dieses Werk ist mehr als ein Text zur KI-Verordnung. Es ist ein Signal: KI kann und muss so gestaltet werden, dass sie allen Menschen Zugang zu Wissen, Teilhabe und Verständnis ermöglicht. Das ist nicht nur für die Rechtswissenschaft, sondern für unsere gesamte Gesellschaft von unschätzbarem Wert.

Ich wünsche Smart.Recht eine weite Verbreitung und viele Leser:innen – und hoffe, dass es als Vorbild für weitere Projekte dient, die den Menschen in den Mittelpunkt stellen und die Chancen von KI für alle nutzbar machen.

Wien, Oktober 2025 *Harald Leitenmüller*

Geleitwort

Demokratisierung des Rechts

Von Dr. Klaus Steinmaurer, Leiter der österreichischen KI-Servicestelle

Von der Demokratisierung des Rechts durch KI zu sprechen, ist ein sicherlich provokanter aber durchaus ernst gemeinter Ansatz, über den Einsatz von Künstlicher Intelligenz im Bereich des Rechts zu diskutieren. Es geht dabei darum, über die Chancen und Risiken, die der Einsatz von KI für die Zugänglichkeit und Verständlichkeit und damit auch die Fairness des Rechtssystems in einer rechtsstaatlichen demokratischen Gesellschaft mit sich bringt, ein erstes Bild zu bekommen.

Heute, wo wir immer mehr Details gesetzlich sowohl national, aber auch auf europäischer Ebene festlegen, wir also mit Fug und Recht von einer wahren Regelungsflut sprechen können, die zudem immer komplexer wird und damit für viele auch inhaltlich nur mehr schwer zugänglich ist, müssen wir davon ausgehen, dass auch die demokratische Teilhabe der Normunterworfenen einer großen Herausforderung unterliegt. Je mehr wir regeln und je weniger davon verstehen oder überhaupt wissen, desto größer ist das Risiko, dass rechtsstaatliche Prinzipien und Grundrechte unter Berufung auf das Recht ausgehöhlt werden. Denn nur, wenn die, für die Gesetze geschaffen werden, diese auch verstehen, kann das intendierte Gesetzesziel auch erreicht werden. Nur wenn das Gesetzesziel verstanden wird, kann es im demokratischen Prozess auch einer kritischen Überprüfung unterzogen werden. KI hat das Potential, zu helfen Recht zugänglicher transparenter und effizienter zu machen und damit grundlegend zu einer Demokratisierung des Rechts beizutragen. Dabei ist immer auch auf mit einem solchen Einsatz verbundene gravierende Risiken zu achten, die zu regulieren sind.

Welche Möglichkeiten bieten sich durch den Einsatz von KI, um die Zugänglichmachung und das Verständnis von Gesetzen für die breite Öffentlichkeit zu verbessern und die Anwendung effizienter und die Rechtsfolgen verständlicher zu machen?

Da ist zum einen die Rechtsberatung, die mit KI für jedermann/frau einfach und kostengünstig zugänglich gemacht werden kann. KI gestützte Chatbots und Tools können einfach und kostengünstig heute schon eine gute Erstberatung anbieten, die zu einer grundsätzlichen Orientierung dienen kann. Gerade in Bereichen wie Verbraucherschutz und Mieterschutz kann das für eine breite Öffentlichkeit sehr hilfreich sein. Darüber hinaus bietet KI mit den gängigen Tools, die es derzeit schon am Markt gibt, aber auch ganz einfach die Möglichkeit schwierige Spezialregelungen einfach und verständlich zusammenzufassen. Damit wird es möglich, sich auch ohne rechtswissenschaftliches Studium als interessierter Rechtsanwender mit

einer komplexen Thematik genauer zu befassen und für die Umsetzung im eigenen Wirkungsbereich rasch und effizient wichtige Grundlagen zu erhalten, ohne vorab einen langwierigen Beratungsprozess zu hohen Kosten durchlaufen zu müssen. Gerade von Unternehmensseite gibt es genau in diesem Zusammenhang bislang viele Klagen, die nicht ganz ungerechtfertigt erscheinen. Schauen wir uns doch nur die umfassenden Regeln des europäischen Digitalrechts an. Wenn hier KI hilft, den Zugang und das Verständnis zu erleichtern, ist das ein wichtiger Schritt auch die Wettbewerbsfähigkeit zu verbessern. Vieles von dem, was wir heute wegen seiner Komplexität und Intransparenz als Überregulierung abtun, kann sich dort, wo es einfach und verständlich gemacht wird, am Ende als echter Wettbewerbsvorteil darstellen, den wir konsequent nutzen können und der neue Möglichkeiten rechtssicher eröffnet.

Auch im Bereich Justiz und Verwaltung ergeben sich durch den Einsatz von KI gerade dort, wo es sich um strukturierte Verwaltungsprozesse und Routineaufgaben handelt, Möglichkeiten zu Entlastung und Verfahrensbeschleunigung bei gleichzeitig effizienter Ressourcennutzung.

Unsere Verwaltung ist heute durch Digitalisierung einem umfassenden Transformationsprozess unterworfen und ist gefordert, schnell und flexibel zu agieren, um nicht ins Hintertreffen zu gelangen. Die zunehmende Nutzung und Vernetzung von Daten kann Verwaltungsverfahren beschleunigen, verbessern und vor allem effizienter machen. Ganz besonders KI-Systeme, die die Entscheidungsfindung unterstützen und vor allem automatisierte Datenanalysen erstellen, haben erhebliches Potential. Dort wo Möglichkeiten bestehen, vollautomatisierte Verfahren zu gestalten, können umfassende Effizienzsteigerungen realisiert werden. Das kann in Zeiten eines demografisch bedingten Fachkräftemangels und knapper Staatskassen eine große Chance für die Zukunft sein, die es zu realisieren gilt.

Zusätzlich können KI-basierte Prognose- und Analysesysteme dazu beitragen, in der Rechtsanwendung für verbesserte Konsistenz zu sorgen und damit auch die Rechtssicherheit unterstützen und das Vertrauen in den Staat stärken.

Mit der Nutzung von KI gehen aber auch einige Risiken einher, die in Bereichen, wo es um das Recht geht, wo besonders hohe Vertrauensvoraussetzungen zu beachten sind, nicht ausgeklammert werden dürfen. Da ist zum einen, dass KI-Systeme selbst oft intransparent sind. Sogenannte Black Boxes, die keine Möglichkeit geben nachzuprüfen, wie sie zu einem bestimmten Ergebnis gekommen sind. Damit werden auch die Grenzen der KI gesetzt, denn wenn die Entscheidungswege nicht genau nachvollziehbar sind, kann auch keine rechtlich verbindliche Entscheidung daraus abgeleitet werden. KI kann auch für die von ihr abgegebenen

Empfehlungen keine Haftung übernehmen. KI generierte rechtliche Aussagen sind daher immer unter dem besonderen Vorbehalt einer vorangegangenen menschlichen Validierung zu verstehen.

Zusätzlich kommt dazu, dass Recht in weiten Bereichen auch als dynamisch zu verstehen ist. Während sich die gesellschaftlichen Realitäten sehr rasch weiterentwickeln und damit eine laufende Weiterentwicklung des Rechts heute in vielen Bereichen mehr denn je erforderlich ist, könnte das durch KI behindert werden, weil diese sich immer auf den Status quo bezieht und damit vergangenheitsbezogen ist.

KI bietet aber bereits heute schon sehr wertvolle Werkzeuge, die für verbesserten und einfacheren Rechtszugang und mehr Effizienz im Umgang mit Recht sorgen können, wenn sie verantwortungsvoll eingesetzt werden und damit das Vertrauen durch abschließende menschliche Bewertung sichergestellt werden kann. Es bedarf über den Einsatz von KI im Recht daher einer strengen Regulierung, um dadurch bestehende rechtliche Standards nicht zu gefährden. Die Demokratisierung des Rechts durch KI bleibt in Zukunft eine Gratwanderung und um diese wirklich zu ermöglichen, wird es klarer Regeln, entsprechender Transparenzpflichten und entsprechender menschlicher Kontrollsysteme bedürfen. KI ist im Wesentlichen ein sehr nützliches Assistenzsystem zur Stärkung der Rechtsstaatlichkeit und wird dies auch in Zukunft bleiben, da die menschliche Urteils- und Abwägungskompetenz jedenfalls ein zentrales Element der Rechtsstaatlichkeit bleiben wird.

Mit diesem nun vorliegenden vollständig KI-generierten Werk zur KI-Verordnung haben Wolfgang Zankl und sein Team an der SFU aber deutlich gemacht, welche Möglichkeiten uns durch KI im Recht heute schon zur Verfügung stehen. Vor allem wenn es darum geht, an sich sperrigen und komplexen Textbestand auf den Punkt zu bringen und für alle interessierten Leser:innen verständlich zu strukturieren. Das vorliegende Ergebnis ihrer Arbeit ersetzt - insbesondere im Hinblick auf den Ausschluss von Literatur und Rechtsprechung - noch keinen klassischen Kommentar (wie ihn Zankl im Verlag Manz selbst erfolgreich herausgegeben hat), aber es ergänzt ihn hervorragend und bringt das geltende KI-Recht einer breiten Leserschaft mit verständlichen Worten und zahlreichen Beispielen näher. Ein wichtiger Schritt in die richtige Richtung, zu dem ich gratulieren darf und den ich persönlich sehr unterstütze.

Wien, Oktober 2025 *Klaus Steinmaurer*

Abkürzungsverzeichnis

AG	Aktiengesellschaft
AI	Artificial Intelligence
bzw	beziehungsweise
CE	Conformité Européenne
CEN	European Committee for Standardization
CENELEC	European Electrotechnical Committee for Standardization
DSGVO	Datenschutz-Grundverordnung
ECRIS-TCN	Europäisches Strafregister für Drittstaatsangehörige und Staatenlose
EDPS	European Data Protection Supervisor
EDSB	Europäische Datenschutzbeauftragte
EES	Einreise-/Ausreisesystem
ENISA	European Union Agency for Cybersecurity
ETIAS	Europäisches Reiseinformations- und -genehmigungssystem
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EuGH	Europäischer Gerichtshof
Eurodac	European Dactoloscopy
ff	folgende
gem	gemäß
gesetzl	gesetzliche
ggf	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GPAI	General Purpose Artificial Intelligence; Deutsch: KI-Modell mit allgemeinem Verwendungszweck
GRFA	Grundrechte-Folgenabschätzung
IKT-Infrastruktur	Informations- und Kommunikationstechnik-Infrastruktur
inkl	inklusive
insb	insbesondere
iSd	im Sinne des
KI	Künstliche Intelligenz
KI-VO	Verordnung über künstliche Intelligenz
KMU	kleine und mittlere Unternehmen

lit	Litera
NGO	non governmental organization
NLF	New Legislative Framework
Nr	Nummer
QMS	Qualitätsmanagementsystem
SIS	Schengener Informationssystem
ua	unter anderem
uä	und ähnliches
USA	United States of America
usw	und so weiter
va	vor allem
VIS	Visa-Informationssystem
VO	Verordnung
vgl	vergleiche
zB	zum Beispiel

Artikel 1 KI-VO

Gegenstand

(1) Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern und die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen künstlichen Intelligenz (KI) zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten und die Innovation zu unterstützen.

(2) In dieser Verordnung wird Folgendes festgelegt:

- *a) harmonisierte Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen in der Union;*
- *b) Verbote bestimmter Praktiken im KI-Bereich;*
- *c) besondere Anforderungen an Hochrisiko-KI-Systeme und Pflichten für Akteure in Bezug auf solche Systeme;*
- *d) harmonisierte Transparenzvorschriften für bestimmte KI-Systeme;*
- *e) harmonisierte Vorschriften für das Inverkehrbringen von KI-Modellen mit allgemeinem Verwendungszweck;*
- *f) Vorschriften für die Marktbeobachtung sowie die Governance und Durchsetzung der Marktüberwachung;*
- *g) Maßnahmen zur Innovationsförderung mit besonderem Augenmerk auf KMU, einschließlich Start-up-Unternehmen.*

I. Worum geht es?

Artikel 1 KI-VO beschreibt, was die KI-Verordnung (KI-VO) regeln will. Die Vorschrift legt fest, welchen Zweck die Verordnung verfolgt und welche Bereiche sie abdeckt. Kernanliegen ist es, für die gesamte EU einheitliche Regeln für den Umgang mit Künstlicher Intelligenz zu schaffen – und zwar so, dass Innovation ermöglicht, der Schutz von Menschen und Grundrechten sichergestellt und faire Bedingungen im Binnenmarkt erhalten bleiben.

II. Detailkommentar

A. Zielsetzung der KI-VO

Die Zielsetzungen von Artikel 1 lassen sich in folgende Punkte gliedern:

1. Vereinfachung des Handels am Binnenmarkt

- **Was bedeutet das?** Die KI-VO will gleiche Regeln in allen EU-Ländern schaffen, damit KI-Systeme einfach in allen Mitgliedstaaten entwickelt, verkauft und genutzt werden können.
- **Warum ist das wichtig?** Ohne einheitliche Regeln könnten einzelne Staaten eigene Vorschriften erlassen. Das würde die Entwicklung und den Handel behindern und zu uneinheitlichen Vorschriften führen.

2. Förderung menschenzentrierter und vertrauenswürdiger KI

- **Was bedeutet das?** KI-Systeme sollen den Menschen dienen, ihre Rechte respektieren und nachvollziehbar, sicher sowie fair funktionieren.
- **Wie wird das umgesetzt?** Die KI-VO verlangt, dass KI so gestaltet wird, dass sie das Wohl der Menschen und die Werte der EU wie Demokratie und Rechtsstaatlichkeit achtet.

3. Schutz von Gesundheit, Sicherheit und Grundrechten

- **Was bedeutet das?** Die KI-VO will verhindern, dass KI-Systeme Schaden anrichten – etwa indem sie Menschen gefährden, diskriminieren oder die Umwelt schädigen.
- **Wie wird das umgesetzt?** Es werden Mindeststandards, Prüfpflichten und Transparenzregeln eingeführt.

4. Unterstützung von Innovation

- **Was bedeutet das?** Die Verordnung fördert die Entwicklung neuer KI-Lösungen, etwa durch spezielle Fördermaßnahmen für kleine Unternehmen und Start-ups.
- **Warum?** Damit die EU wettbewerbsfähig bleibt und innovative Technologien entstehen.

B. Regelungsbereiche der KI-VO

Die Verordnung umfasst folgende Regelungsbereiche:

- a) **Einheitliche Regeln** für das Inverkehrbringen, die Inbetriebnahme und Nutzung von KI-Systemen in der EU
- b) **Verbote** bestimmter riskanter oder unethischer KI-Praktiken

- c) **Besondere Anforderungen für Hochrisiko-KI-Systeme** und Pflichten für beteiligte Akteure
- d) **Transparenzvorschriften** für bestimmte KI-Systeme, etwa Kennzeichnungspflichten
- e) **Regeln für KI-Modelle mit allgemeinem Verwendungszweck** (z B große Sprachmodelle wie ChatGPT)
- f) **Marktbeobachtung und Durchsetzung** durch zuständige Behörden
- g) **Maßnahmen zur Innovationsförderung** mit Fokus auf kleine Unternehmen und Start-ups

C. Besonderheiten

Schutzziele und Innovationsförderung im Ausgleich: Die KI-VO ist ein Balanceakt – sie will sowohl den Schutz der Menschen und Rechte als auch die wirtschaftliche Entwicklung und Innovation sichern.

III. Zusammenfassung

Binnenmarkt stärken	Einheitliche Regeln für alle EU-Länder
Mensch im Mittelpunkt	KI muss die Rechte und das Wohl der Menschen wahren
Gesundheit, Sicherheit und Grundrechte	KI darf niemanden gefährden oder diskriminieren
Innovation fördern	Entwicklung neuer KI erleichtern, vor allem für kleine Firmen
Klare Vorschriften	Was ist erlaubt? Was ist verboten? Wer muss was tun?

IV. Quellenverzeichnis

- Erwägungsgründe 1-9 KI-VO (EU) 2024/1689

Artikel 2 KI-VO

Anwendungsbereich

(1) Diese Verordnung gilt für

a) Anbieter, die in der Union KI-Systeme in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle mit allgemeinem Verwendungszweck in Verkehr bringen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind;

b) Betreiber von KI-Systemen, die ihren Sitz in der Union haben oder in der Union befinden;

c) Anbieter und Betreiber von KI-Systemen, die ihren Sitz in einem Drittland haben oder sich in einem Drittland befinden, wenn die vom KI-System hervorgebrachte Ausgabe in der Union verwendet wird;

d) Einführer und Händler von KI-Systemen;

e) Produkthersteller, die KI-Systeme zusammen mit ihrem Produkt unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringen oder in Betrieb nehmen;

f) Bevollmächtigte von Anbietern, die nicht in der Union niedergelassen sind;

g) betroffene Personen, die sich in der Union befinden.

(2) Für KI-Systeme, die als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 1 eingestuft sind und im Zusammenhang mit Produkten stehen, die unter die in Anhang I Abschnitt B aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, gelten nur Artikel 6 Absatz 1, die Artikel 102 bis 109 und Artikel 112. Artikel 57 gilt nur, soweit die Anforderungen an Hochrisiko-KI-Systeme gemäß dieser Verordnung im Rahmen der genannten Harmonisierungsrechtsvorschriften der Union eingebunden wurden.

(3) Diese Verordnung gilt nur in den unter das Unionsrecht fallenden Bereichen und berührt keinesfalls die Zuständigkeiten der Mitgliedstaaten in Bezug auf die nationale Sicherheit, unabhängig von der Artikel der Einrichtung, die von den Mitgliedstaaten mit der Wahrnehmung von Aufgaben im Zusammenhang mit diesen Zuständigkeiten betraut wurde.

Diese Verordnung gilt nicht für KI-Systeme, wenn und soweit sie ausschließlich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit in Verkehr gebracht, in Betrieb genommen oder, mit oder ohne Änderungen, verwendet werden, unabhängig von der Artikel der Einrichtung, die diese Tätigkeiten ausübt.

Diese Verordnung gilt nicht für KI-Systeme, die nicht in der Union in Verkehr gebracht oder in Betrieb genommen werden, wenn die Ausgaben in der Union ausschließlich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit verwendet werden, unabhängig von der Artikel der Einrichtung, die diese Tätigkeiten ausübt.

(4) Diese Verordnung gilt weder für Behörden in Drittländern noch für internationale Organisationen, die gemäß Absatz 1 in den Anwendungsbereich dieser Verordnung fallen, soweit diese Behörden oder Organisationen KI-Systeme im Rahmen der internationalen Zusammenarbeit oder internationaler Übereinkünfte im Bereich der Strafverfolgung und justiziellen Zusammenarbeit mit der Union oder mit einem oder mehreren Mitgliedstaaten verwenden und sofern ein solches Drittland oder eine solche internationale Organisation angemessene Garantien hinsichtlich des Schutz der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bietet.

(5) Die Anwendung der Bestimmungen über die Haftung der Anbieter von Vermittlungsdiensten in Kapitel II der Verordnung 2022/2065 bleibt von dieser Verordnung unberührt.

(6) Diese Verordnung gilt nicht für KI-Systeme oder KI-Modelle, einschließlich ihrer Ausgabe, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden.

(7) Die Rechtsvorschriften der Union zum Schutz personenbezogener Daten, der Privatsphäre und der Vertraulichkeit der Kommunikation gelten für die Verarbeitung personenbezogener Daten im Zusammenhang mit den in dieser Verordnung festgelegten Rechten und Pflichten. Diese Verordnung berührt nicht die Verordnung (EU) 2016/679 bzw. (EU) 2018/1725 oder die Richtlinie 2002/58/EG bzw. (EU) 2016/680, unbeschadet des Artikels 10 Absatz 5 und des Artikels 59 der vorliegenden Verordnung.

(8) Diese Verordnung gilt nicht für Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen oder KI-Modellen, bevor diese in

Verkehr gebracht oder in Betrieb genommen werden. Solche Tätigkeiten werden im Einklang mit dem geltenden Unionsrecht durchgeführt. Tests unter Realbedingungen fallen nicht unter diesen Ausschluss.

(9) Diese Verordnung berührt nicht die Vorschriften anderer Rechtsakte der Union zum Verbraucherschutz und zur Produktsicherheit.

(10) Diese Verordnung gilt nicht für die Pflichten von Betreibern, die natürliche Personen sind und KI-Systeme im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit verwenden.

(11) Diese Verordnung hindert die Union oder die Mitgliedstaaten nicht daran, Rechts- oder Verwaltungsvorschriften beizubehalten oder einzuführen, die für die Arbeitnehmer im Hinblick auf den Schutz ihrer Rechte bei der Verwendung von KI-Systemen durch die Arbeitgeber vorteilhafter sind, oder die Anwendung von Kollektivvereinbarungen zu fördern oder zuzulassen, die für die Arbeitnehmer vorteilhafter sind.

(12) Diese Verordnung gilt nicht für KI-Systeme, die unter freien und quelloffenen Lizenzen bereitgestellt werden, es sei denn, sie werden als Hochrisiko-KI-Systeme oder als ein KI-System, das unter Artikel 5 oder 50 fällt, in Verkehr gebracht oder in Betrieb genommen.

I. Worum geht es?

Artikel 2 der KI-VO legt fest, auf wen und was die Verordnung anwendbar ist - also den sogenannten Anwendungsbereich. Damit beantwortet er, welche Personen, Unternehmen oder Behörden und welche KI-Systeme von den Regeln der KI-VO erfasst werden und in welchen Fällen Ausnahmen gelten. Dieser Artikel ist für alle wichtig, die wissen wollen, ob sie von den Vorschriften betroffen sind oder nicht.

II. Detailkommentar

A. Persönlicher Anwendungsbereich

Wer ist von der KI-VO betroffen?

Die Verordnung gilt für verschiedene Akteure, darunter:

- **Anbieter** von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck (auch wenn sie außerhalb der EU sitzen).

- **Betreiber** von KI-Systemen mit Sitz oder Tätigkeiten in der EU.
- **Einführer**, **Händler** und **Produkthersteller**, die KI-Systeme in der EU auf den Markt bringen oder nutzen.
- **Bevollmächtigte** von Anbietern außerhalb der EU.
- **Betroffene Personen** in der EU, auf die ein KI-System wirkt.

B. Räumlicher Anwendungsbereich

Wo gilt die KI-VO?

- Die Verordnung gilt in der gesamten **Europäischen Union**.
- Sie gilt auch für Anbieter/Betreiber aus Drittländern, **wenn die KI-Ausgabe in der EU verwendet wird** (zB ein Chatbot aus Kanada, der auf einer EU-Website eingebunden ist).
- Für bestimmte internationale Kooperationen (zB bei Strafverfolgung) gelten besondere Regeln und Ausnahmen (siehe unten).

C. Sachlicher Anwendungsbereich

Welche KI-Systeme sind erfasst?

- Alle KI-Systeme und KI-Modelle mit allgemeinem Verwendungszweck, die in der EU auf den Markt kommen, betrieben oder deren Ausgaben in der EU genutzt werden.
- Besondere Regeln für Hochrisiko-KI-Systeme, insbesondere, wenn sie mit anderen EU-Regeln (zB Produktsicherheitsgesetzen) zusammenhängen.
- Ausnahmen (siehe unten) etwa für militärische Zwecke, reine Forschung, persönliche Nutzung ua

D. Zeitlicher Anwendungsbereich

Der Startzeitpunkt (Inkrafttreten, Übergangsfristen, usw) wird in den Artikel 113 KI-VO undArtikel 111 KI-VO geregelt.

E. Ausnahmen

Artikel 2 nennt zahlreiche Ausnahmen. Die wichtigsten:

- **Militär, Verteidigung, nationale Sicherheit**: KI-Systeme, die ausschließlich für diese Zwecke genutzt werden, sind ausgenommen. Beispiel: Eine KI für die Steuerung militärischer Drohnen fällt nicht unter die KI-VO.
- **Internationale Zusammenarbeit**: Behörden und Organisationen außerhalb der EU, die im Rahmen internationaler Zusammenarbeit mit der EU agieren (zB bei Strafverfolgung), sind ausgenommen – wenn Datenschutz und Grundrechte angemessen geschützt werden.
- **Persönliche, nicht berufliche Nutzung**: Natürliche Personen, die KI-Systeme rein privat nutzen, sind von den Pflichten ausgenommen (zB bei der Verwendung eines KI-Bilderzeugers nur für eigene Hobbys).
- **Forschung und Entwicklung**: KI-Systeme oder -Modelle, die ausschließlich für wissenschaftliche Forschung und Entwicklung entwickelt oder betrieben werden, sind ausgenommen – solange sie nicht auf den Markt gebracht oder unter Realbedingungen getestet werden.
- **Open Source**: KI-Systeme, die unter offenen Lizenzen bereitgestellt werden, sind in der Regel ausgenommen – außer sie sind Hochrisiko-KI-Systeme oder unterfallen besonderen Verboten/Auflagen.

Beispiel: *Ein KI-Tool zur medizinischen Diagnose wird in Deutschland entwickelt, aber vorerst nur im Labor zu Forschungszwecken eingesetzt. Solange es nicht in den Markt gelangt, greift die KI-VO nicht.*

F. Verhältnis zu anderem Unionsrecht

- Die KI-VO ergänzt andere EU-Gesetze, insbesondere in den Bereichen Datenschutz (zB DSGVO), Verbraucherschutz und Produktsicherheit.

- Rechte und Rechtsbehelfe, die nach anderen EU-Gesetzen bestehen, bleiben erhalten.
- Bei Überschneidungen (zB Arbeitnehmerrechte, Kinder- und Jugendschutz) bleibt das jeweilige Spezialgesetz maßgeblich.
- Die KI-VO darf die Ausübung von Grundrechten nicht beeinträchtigen.

III. Zusammenfassung

Wer?	Anbieter, Betreiber, Händler, Einführer, Produkthersteller, Bevollmächtigte, Betroffene in der EU.
Was?	KI-Systeme
Wo?	Innerhalb der EU, inkl Drittländer, wenn KI-Ausgabe in der EU genutzt wird.
Wann?	Ab Inkrafttreten/Anwendbarkeit der KI-VO (vgl Artikel 113 KI-VO, Artikel 111 KI-VO).
Ausnahmen?	Militär/Verteidigung/nationale Sicherheit, rein private Nutzung, Forschung und Entwicklung vor Markteinführung, Open Source (außer Hochrisiko/verbotene Anwendungen), internationale Kooperation Strafverfolgung.
Schnittstellen?	Verhältnis zu anderem Unionsrecht (zB DSGVO, Produktsicherheit, Arbeitsrecht) bleibt bestehen.

IV. Quellenverzeichnis

- Erwägungsgründe 9, 10, 11, 21, 22, 23, 24, 25 KI-VO (EU) 2024/1689

Artikel 3 KI-VO

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. *„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;*

2. *„Risiko" die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und der Schwere dieses Schadens;*

3. *„Anbieter" eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich;*

4. *„Betreiber" eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet;*

5. *„Bevollmächtigter" eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen;*

6. *„Einführer" eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein KI-System, das den Namen oder die Handelsmarke einer in einem Drittland niedergelassenen natürlichen oder juristischen Person trägt, in Verkehr bringt;*

7.„Händler“ eine natürliche oder juristische Person in der Lieferkette, die ein KI-System auf dem Unionsmarkt bereitstellt, mit Ausnahme des Anbieters oder des Einführers;

8.„Akteur“ einen Anbieter, Produkthersteller, Betreiber, Bevollmächtigten, Einführer oder Händler;

9.„Inverkehrbringen“ die erstmalige Bereitstellung eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt;

10.„Bereitstellung auf dem Markt“ die entgeltliche oder unentgeltliche Abgabe eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit;

11.„Inbetriebnahme“ die Bereitstellung eines KI-Systems in der Union zum Erstgebrauch direkt an den Betreiber oder zum Eigengebrauch entsprechend seiner Zweckbestimmung;

12.„Zweckbestimmung“ die Verwendung, für die ein KI-System laut Anbieter bestimmt ist, einschließlich der besonderen Umstände und Bedingungen für die Verwendung, entsprechend den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation;

13.„vernünftigerweise vorhersehbare Fehlanwendung“ die Verwendung eines KI-Systems in einer Weise, die nicht seiner Zweckbestimmung entspricht, die sich aber aus einem vernünftigerweise vorhersehbaren menschlichen Verhalten oder einer vernünftigerweise vorhersehbaren Interaktion mit anderen Systemen, auch anderen KI-Systemen, ergeben kann;

14.„Sicherheitsbauteil“ einen Bestandteil eines Produkts oder KI-Systems, der eine Sicherheitsfunktion für dieses Produkt oder KI-System erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet;

15.„Betriebsanleitungen“ die Informationen, die der Anbieter bereitstellt, um den Betreiber insbesondere über die Zweckbestimmung und die ordnungsgemäße Verwendung eines KI-Systems zu informieren;

16.„Rückruf eines KI-Systems" jede Maßnahme, die auf die Rückgabe an den Anbieter oder auf die Außerbetriebsetzung oder Abschaltung eines den Betreibern bereits zur Verfügung gestellten KI-Systems abzielt;

17.„Rücknahme eines KI-Systems" jede Maßnahme, mit der die Bereitstellung eines in der Lieferkette befindlichen KI-Systems auf dem Markt verhindert werden soll;

18.„Leistung eines KI-Systems" die Fähigkeit eines KI-Systems, seine Zweckbestimmung zu erfüllen;

19.„notifizierende Behörde" die nationale Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren für die Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen und für deren Überwachung zuständig ist;

20.„Konformitätsbewertung" ein Verfahren mit dem bewertet wird, ob die in Titel III Abschnitt 2 festgelegten Anforderungen an ein Hochrisiko-KI-System erfüllt wurden;

21.„Konformitätsbewertungsstelle" eine Stelle, die Konformitätsbewertungstätigkeiten einschließlich Prüfungen, Zertifizierungen und Inspektionen durchführt und dabei als Dritte auftritt;

22.„notifizierte Stelle" eine Konformitätsbewertungsstelle, die gemäß dieser Verordnung und den anderen einschlägigen Harmonisierungsrechtsvorschriften der Union notifiziert wurde;

23.„wesentliche Veränderung" eine Veränderung eines KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die in der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit den Anforderungen in Kapitel III Abschnitt 2 beeinträchtigt wird oder die zu einer Änderung der Zweckbestimmung führt, für die das KI-System bewertet wurde;

24.„CE-Kennzeichnung" eine Kennzeichnung, durch die ein Anbieter erklärt, dass ein KI-System die Anforderungen erfüllt, die in Kapitel III Abschnitt 2 und in anderen anwendbaren Harmonisierungsrechtsvorschriften, die die Anbringung dieser Kennzeichnung vorsehen, festgelegt sind;

25.„System zur Beobachtung nach dem Inverkehrbringen" alle Tätigkeiten, die Anbieter von KI-Systemen zur Sammlung und Überprüfung von Erfahrungen mit der Verwendung der von ihnen in Verkehr gebrachten oder in Betrieb genommenen KI-Systeme durchführen, um festzustellen, ob unverzüglich nötige Korrektur- oder Präventivmaßnahmen zu ergreifen sind;

26.„Marktüberwachungsbehörde" die nationale Behörde, die die Tätigkeiten durchführt und die Maßnahmen ergreift, die in der Verordnung (EU) 2019/1020 vorgesehen sind;

27.„harmonisierte Norm" bezeichnet eine harmonisierte Norm im Sinne des Artikels 2 Absatz 1 Buchstabe c der Verordnung (EU) Nr 1025/2012;

28.„gemeinsame Spezifikation" eine Reihe technischer Spezifikationen im Sinne des Artikels 2 Nummer 4 der Verordnung (EU) Nr 1025/2012, deren Befolgung es ermöglicht, bestimmte Anforderungen der vorliegenden Verordnung zu erfüllen;

29.„Trainingsdaten" Daten, die zum Trainieren eines KI-Systems verwendet werden, wobei dessen lernbare Parameter angepasst werden;

30.„Validierungsdaten" Daten, die zur Evaluation des trainierten KI-Systems und zur Einstellung seiner nicht erlernbaren Parameter und seines Lernprozesses verwendet werden, um unter anderem eine Unter- oder Überanpassung zu vermeiden;

31.„Validierungsdatensatz" einen separaten Datensatz oder einen Teil des Trainingsdatensatzes mit fester oder variabler Aufteilung;

32.„Testdaten" Daten, die für eine unabhängige Bewertung des KI-Systems verwendet werden, um die erwartete Leistung dieses Systems vor dessen Inverkehrbringen oder Inbetriebnahme zu bestätigen;

33.„Eingabedaten" die in ein KI-System eingespeisten oder von diesem direkt erfassten Daten, auf deren Grundlage das System eine Ausgabe hervorbringt;

34.„biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, wie etwa Gesichtsbilder oder daktyloskopische Daten;

35.„biometrische Identifizierung" die automatisierte Erkennung physischer, physiologischer, verhaltensbezogener oder psychologischer menschlicher Merkmale zum Zwecke der Feststellung der Identität einer natürlichen Person durch den Vergleich biometrischer Daten dieser Person mit biometrischen Daten von Personen, die in einer Datenbank gespeichert sind;

36.„biometrische Verifizierung" die automatisierte Eins-zu-eins-Verifizierung, einschließlich Authentifizierung, der Identität natürlicher Personen durch den Vergleich ihrer biometrischen Daten mit zuvor bereitgestellten biometrischen Daten;

37.„besondere Kategorien personenbezogener Daten" die in Artikel 9 Absatz 1der Verordnung (EU) 2016/679, Artikel 10 der Richtlinie (EU) 2016/680 und Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 aufgeführten Kategorien personenbezogener Daten;

38.„sensible operative Daten" operative Daten im Zusammenhang mit Tätigkeiten zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten, deren Offenlegung die Integrität von Strafverfahren gefährden könnte;

39.„Emotionserkennungssystem" ein KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten;

40.„System zur biometrischen Kategorisierung" ein KI-System, das dem Zweck dient, natürliche Personen auf der Grundlage ihrer biometrischen Daten bestimmten Kategorien zuzuordnen, sofern es sich um eine Nebenfunktion eines anderen kommerziellen Dienstes handelt und aus objektiven technischen Gründen unbedingt erforderlich ist;

41.„biometrisches Fernidentifizierungssystem" ein KI-System, das dem Zweck dient, natürliche Personen ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren;

42.„biometrisches Echtzeit-Fernidentifizierungssystem" ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen, und das zur Vermeidung einer Umgehung der Vorschriften

nicht nur die sofortige Identifizierung, sondern auch eine Identifizierung mit begrenzten kurzen Verzögerungen umfasst;

43.„System zur nachträglichen biometrischen Fernidentifizierung" ein biometrisches Fernidentifizierungssystem, das kein biometrisches Echtzeit-Fernidentifizierungssystem ist;

44.„öffentlich zugänglicher Raum" einen einer unbestimmten Anzahl natürlicher Personen zugänglichen physischen Ort in privatem oder öffentlichem Eigentum, unabhängig davon, ob bestimmte Bedingungen für den Zugang gelten, und unabhängig von möglichen Kapazitätsbeschränkungen;

45.„Strafverfolgungsbehörde"

a)eine Behörde, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder

b)eine andere Stelle oder Einrichtung, der durch nationales Recht die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde;

46.„Strafverfolgung" Tätigkeiten der Strafverfolgungsbehörden oder in deren Auftrag zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

47.„Büro für Künstliche Intelligenz" die Aufgabe der Kommission, zur Umsetzung, Beobachtung und Überwachung von KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck und zu der im Beschluss der Kommission vom 24. Januar 2024 vorgesehenen KI-Governance beizutragen; Bezugnahmen in dieser Verordnung auf das Büro für Künstliche Intelligenz gelten als Bezugnahmen auf die Kommission;

48.„zuständige nationale Behörde" eine notifizierende Behörde oder eine Marktüberwachungsbehörde; in Bezug auf KI-Systeme, die von Organen, Einrichtungen und sonstigen Stellen der Union in Betrieb genommen oder verwendet werden, sind Bezugnahmen auf die zuständigen nationalen Behörden oder Marktüberwachungsbehörden in dieser

Verordnung als Bezugnahmen auf den Europäischen Datenschutzbeauftragten auszulegen;

49.„schwerwiegender Vorfall" einen Vorfall oder eine Fehlfunktion bezüglich eines KI-Systems, das bzw. die direkt oder indirekt eine der nachstehenden Folgen hat:

a)den Tod oder die schwere gesundheitliche Schädigung einer Person;

b)eine schwere und unumkehrbare Störung der Verwaltung oder des Betriebs kritischer Infrastrukturen;

c)die Verletzung von Pflichten aus den Unionsrechtsvorschriften zum Schutz der Grundrechte;

d) schwere Sach- oder Umweltschäden;

50.„personenbezogene Daten" personenbezogene Daten im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679;

51.„nicht personenbezogene Daten" Daten, die keine personenbezogenen Daten im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) 2016/679 sind;

52.„Profiling" das Profiling im Sinne von Artikel 4 Nummer 4 der Verordnung (EU) 2016/679;

53.„Plan für einen Test unter Realbedingungen" ein Dokument, in dem die Ziele, die Methodik, der geografische, bevölkerungsbezogene und zeitliche Umfang, die Überwachung, die Organisation und die Durchführung eines Tests unter Realbedingungen beschrieben werden;

54.„Plan für das Reallabor" ein zwischen dem teilnehmenden Anbieter und der zuständigen Behörde vereinbartes Dokument, in dem die Ziele, die Bedingungen, der Zeitrahmen, die Methodik und die Anforderungen für die im Reallabor durchgeführten Tätigkeiten beschrieben werden;

55.„KI-Reallabor" einen kontrollierten Rahmen, der von einer zuständigen Behörde geschaffen wird und den Anbieter oder zukünftige Anbieter von KI-Systemen nach einem Plan für das Reallabor einen begrenzten Zeitraum und unter regulatorischer Aufsicht nutzen können, um ein innovatives KI-System zu entwickeln, zu trainieren, zu validieren und — gegebenenfalls unter Realbedingungen — zu testen.

56.„KI-Kompetenz" die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden.

57.„Test unter Realbedingungen" den befristeten Test eines KI-Systems auf seine Zweckbestimmung, der unter Realbedingungen außerhalb eines Labors oder einer anderweitig simulierten Umgebung erfolgt, um zuverlässige und belastbare Daten zu erheben und die Konformität des KI-Systems mit den Anforderungen der vorliegenden Verordnung zu bewerten und zu überprüfen, wobei dieser Test nicht als Inverkehrbringen oder Inbetriebnahme des KI-Systems im Sinne dieser Verordnung gilt, sofern alle Bedingungen nach Artikel 57 oder Artikel 60 erfüllt sind;

58.„Testteilnehmer" für die Zwecke eines Tests unter Realbedingungen eine natürliche Person, die an dem Test unter Realbedingungen teilnimmt;

59.„informierte Einwilligung" eine aus freien Stücken erfolgende, spezifische, eindeutige und freiwillige Erklärung der Bereitschaft, an einem bestimmten Test unter Realbedingungen teilzunehmen, durch einen Testteilnehmer, nachdem dieser über alle Aspekte des Tests, die für die Entscheidungsfindung des Testteilnehmers bezüglich der Teilnahme relevant sind, aufgeklärt wurde;

60.„Deepfake" einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde;

61.„weitverbreiteter Verstoß" jede Handlung oder Unterlassung, die gegen das Unionsrecht verstößt, das die Interessen von Einzelpersonen schützt, und die

a)die kollektiven Interessen von Einzelpersonen in mindestens zwei anderen Mitgliedstaaten als dem Mitgliedstaat schädigt oder zu schädigen droht, in dem

i)die Handlung oder die Unterlassung ihren Ursprung hatte oder stattfand,

ii) der betreffende Anbieter oder gegebenenfalls sein Bevollmächtigter sich befindet oder niedergelassen ist oder

iii) der Betreiber niedergelassen ist, sofern der Verstoß vom Betreiber begangen wird,

b) die kollektiven Interessen von Einzelpersonen geschädigt hat, schädigt oder schädigen könnte und allgemeine Merkmale aufweist, einschließlich derselben rechtswidrigen Praxis oder desselben verletzten Interesses, und gleichzeitig auftritt und von demselben Akteur in mindestens drei Mitgliedstaaten begangen wird;

62.„kritische Infrastrukturen" kritische Infrastrukturen im Sinne von Artikel 2 Nummer 4 der Richtlinie (EU) 2022/2557;

63.„KI-Modell mit allgemeinem Verwendungszweck" ein KI-Modell — einschließlich der Fälle, in denen ein solches KI-Modell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird —, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Artikel und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KI-Modelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden;

64.„Fähigkeiten mit hoher Wirkkraft" bezeichnet Fähigkeiten, die den bei den fortschrittlichsten KI-Modellen mit allgemeinem Verwendungszweck festgestellten Fähigkeiten entsprechen oder diese übersteigen;

65.„systemisches Risiko" ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können;

66.„KI-System mit allgemeinem Verwendungszweck" ein KI-System, das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der

Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen;

67. *„Gleitkommaoperation" jede Rechenoperation oder jede Zuweisung mit Gleitkommazahlen, bei denen es sich um eine Teilmenge der reellen Zahlen handelt, die auf Computern typischerweise durch das Produkt aus einer ganzen Zahl mit fester Genauigkeit und einer festen Basis mit ganzzahligem Exponenten dargestellt wird;*

68. *„nachgelagerter Anbieter" einen Anbieter eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das ein KI-Modell integriert, unabhängig davon, ob das KI-Modell von ihm selbst bereitgestellt und vertikal integriert wird oder von einer anderen Einrichtung auf der Grundlage vertraglicher Beziehungen bereitgestellt wird.*

I. Worum geht es?

Artikel 3 KI-VO definiert alle wichtigen Fachbegriffe, die im weiteren Verlauf der Verordnung verwendet werden. Diese „Begriffsbestimmungen" sind notwendig, damit alle Beteiligten (zB Anbieter, Entwickler, Behörden, Nutzer) genau wissen, was mit zentralen Ausdrücken gemeint ist. Nur wenn klar geregelt ist, was etwa ein „KI-System" oder ein „Betreiber" ist, können die Pflichten, Rechte und Verbote aus der KI-VO einheitlich und vorhersehbar angewendet werden.

II. Detailkommentar

A. Kurzdefinitionen der Begriffe aus Artikel 3 KI-VO

Nr	Begriff	Kurzdefinition
1	KI-System	*Siehe unten für genauere Definition*
2	Risiko	Risiko meint die Kombination aus der Wahrscheinlichkeit, dass ein Schaden entsteht, und wie schwer dieser Schaden ausfällt.

Nr	Begriff	Kurzdefinition
3	Anbieter	Wer ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck (GPAI-Modell) entwickelt oder entwickeln lässt und es unter eigenem Namen oder eigener Marke auf den Markt bringt oder in Betrieb nimmt.
4	Betreiber	Wer ein KI-System eigenverantwortlich nutzt (außer zu privaten Zwecken).
5	Bevollmächtigter	Eine in der EU ansässige Person oder Firma, die vom Anbieter schriftlich dazu bestimmt wird, für ihn bestimmte Pflichten aus der KI-VO zu übernehmen und im Namen des Anbieters zu handeln.
6	Einführer	Wer ein aus dem Ausland stammendes KI-System erstmals in der EU auf den Markt bringt.
7	Händler	Wer ein KI-System innerhalb der Lieferkette auf dem EU-Markt anbietet, aber nicht selbst Anbieter oder Einführer ist.
8	Akteur	Sammelbegriff für Anbieter, Produkthersteller, Betreiber, Bevollmächtigte, Einführer oder Händler – also alle wichtigen Rollen im Zusammenhang mit KI-Systemen.
9	Inverkehrbringen	Das erstmalige Bereitstellen eines KI-Systems oder GPAI-Modells auf dem Markt der

Nr	Begriff	Kurzdefinition
		Europäischen Union, unabhängig davon, ob es verkauft oder kostenlos angeboten wird.
10	Bereitstellung auf dem Markt	Die Übergabe oder der Vertrieb eines KI-Systems oder GPAI-Modells für Geschäftszwecke innerhalb der EU, egal ob gegen Bezahlung oder kostenlos.
11	Inbetriebnahme	Der erstmalige praktische Einsatz eines KI-Systems entsprechend seiner vorgesehenen Nutzung (direkt an den Betreiber oder zum Eigengebrauch).
12	Zweckbestimmung	Die Nutzung, für die der Anbieter das KI-System vorgesehen hat, einschließlich aller Einsatzbedingungen, wie sie in Anleitungen, Werbematerial oder technischen Unterlagen festgehalten sind.
13	Vernünftigerweise vorhersehbare Fehlanwendung	Eine Verwendung des KI-Systems, die nicht der Zweckbestimmung entspricht, aber dennoch durch naheliegendes menschliches Verhalten oder im Zusammenspiel mit anderen Systemen entstehen kann.
14	Sicherheitsbauteil	Ein Bestandteil eines KI-Systems oder Produkts, der eine wichtige Sicherheitsfunktion erfüllt oder dessen Ausfall die Gesundheit von Menschen

Nr	Begriff	Kurzdefinition
		oder Sachwerte gefährden könnte.
15	Betriebsanleitungen	Informationen, die der Anbieter gibt, um die richtige und sichere Nutzung sowie die Zweckbestimmung des KI-Systems zu erklären.
16	Rückruf eines KI-Systems	Maßnahme, die dazu dient, bereits ausgelieferte KI-Systeme entweder vom Betreiber zurückzuverlangen, außer Betrieb zu nehmen oder abzuschalten.
17	Rücknahme eines KI-Systems	Maßnahme, um zu verhindern, dass ein KI-System, das sich noch in der Lieferkette befindet, auf den Markt gelangt.
18	Leistung eines KI-Systems	Die Fähigkeit eines KI-Systems, das zu leisten, wofür es vom Anbieter vorgesehen ist, also seine Aufgaben zuverlässig zu erfüllen.
19	Notifizierende Behörde	Nationale Behörde, die für das Ernennen und Überwachen von Stellen zuständig ist, die KI-Systeme auf Konformität überprüfen.
20	Konformitätsbewertung	Ein Verfahren, bei dem geprüft wird, ob ein Hochrisiko-KI-System die gesetzlichen Anforderungen einhält.
21	Konformitätsbewertungsstelle	Eine unabhängige Stelle, die die Überprüfung, Zertifizierung und Inspektion von KI-Systemen durchführt.

Nr	Begriff	Kurzdefinition
22	Notifizierte Stelle	Eine Konformitätsbewertungsstelle, die offiziell nach EU-Recht anerkannt und gemeldet wurde.
23	Wesentliche Veränderung	Eine nachträgliche Änderung an einem KI-System, die nicht im ursprünglichen Prüfverfahren vorgesehen war und die entweder die Einhaltung der Anforderungen beeinträchtigt oder die Zweckbestimmung ändert.
24	CE-Kennzeichnung	Die Kennzeichnung, mit der der Anbieter erklärt, dass das KI-System alle gesetzlichen Anforderungen (insbesondere an Sicherheit) erfüllt.
25	System zur Beobachtung nach dem Inverkehrbringen	Alle Maßnahmen eines Anbieters, um nach dem Markteintritt Erfahrungen mit seinem KI-System zu sammeln und nötigenfalls sofortige Korrekturen oder Verbesserungen einzuleiten.
26	Marktüberwachungsbehörde	Nationale Behörde, die für Kontrolle und Durchsetzung der Vorschriften (zB Produktsicherheit) zuständig ist.
27	Harmonisierte Norm	Eine nach EU-Recht anerkannte technische Norm, deren Einhaltung die Einhaltung bestimmter gesetzlicher Anforderungen erleichtert.
28	Gemeinsame Spezifikation	Eine Sammlung technischer Vorgaben, die – wie eine

Nr	Begriff	Kurzdefinition
		harmonisierte Norm – die Erfüllung bestimmter Anforderungen der KI-VO ermöglichen.
29	Trainingsdaten	Daten, mit denen ein KI-System so trainiert wird, dass es seine Aufgaben durch Anpassung seiner Parameter lernen kann.
30	Validierungsdaten	Daten, mit denen ein trainiertes KI-System geprüft und eingestellt wird, um Fehler (wie Über- oder Unteranpassung) zu vermeiden.
31	Validierungsdatensatz	Ein gesonderter Teil der Daten, der entweder aus den Trainingsdaten stammt oder separat ist, um die Systemleistung zu überprüfen.
32	Testdaten	Daten, mit denen unabhängig geprüft wird, ob das KI-System die erwartete Leistung bringt, bevor es auf den Markt kommt.
33	Eingabedaten	Alle Daten, die in das KI-System eingegeben oder von diesem erfasst werden und auf deren Basis das System arbeitet.
34	Biometrische Daten	Mit technischen Verfahren erfasste persönliche Daten zu körperlichen oder verhaltensbasierten Merkmalen einer Person, zB Gesichtsbilder oder Fingerabdrücke.

Nr	Begriff	Kurzdefinition
35	Biometrische Identifizierung	Die automatische Erkennung der Identität einer Person anhand biometrischer Daten durch Abgleich mit Datenbanken.
36	Biometrische Verifizierung	Der automatisierte Abgleich der biometrischen Daten einer Person mit zuvor hinterlegten Daten, um deren Identität zu bestätigen (zB für Zugang zu Gebäuden).
37	Besondere Kategorien personenbezogener Daten	Besonders schützenswerte Daten wie Gesundheitsdaten, ethnische Herkunft, politische Meinung (Definition laut DSGVO und anderer EU-Regelungen).
38	Sensible operative Daten	Daten, die sich auf die Verhütung, Ermittlung oder Verfolgung von Straftaten beziehen und deren Veröffentlichung Strafverfahren gefährden könnte.
39	Emotionserkennungssystem	Ein KI-System, das darauf ausgelegt ist, Emotionen oder Absichten von Menschen anhand ihrer biometrischen Daten zu erkennen oder daraus abzuleiten.
40	System zur biometrischen Kategorisierung	KI-System, das Menschen anhand biometrischer Daten bestimmten Kategorien zuordnet, sofern es sich um eine Nebenfunktion in einem Dienst handelt und technisch unvermeidbar ist.

Nr	Begriff	Kurzdefinition
41	Biometrisches Fernidentifizierungssystem	Ein KI-System, das Menschen meist aus der Ferne und ohne deren aktives Zutun durch biometrischen Datenabgleich identifiziert.
42	Biometrisches Echtzeit-Fernidentifizierungssystem	Ein biometrisches Fernidentifizierungssystem, bei dem Erfassung, Abgleich und Identifizierung ohne große Verzögerung („live“ oder fast live) stattfinden.
43	System zur nachträglichen biometrischen Fernidentifizierung	Ein biometrisches Fernidentifizierungssystem, das nicht in Echtzeit arbeitet, sondern erst später (zB nach Sichtung von Videoaufzeichnungen).
44	Öffentlich zugänglicher Raum	Ein Ort, den eine unbestimmte Anzahl an Menschen betreten kann, egal ob öffentlich oder privat (zB Straßen, Bahnhöfe, Einkaufszentren, aber nicht Arbeitsplätze oder Gefängnisse).
45	Strafverfolgungsbehörde	Behörde, die für die Verhütung, Ermittlung und Verfolgung von Straftaten zuständig ist oder entsprechende Befugnisse durch Gesetz erhalten hat.
46	Strafverfolgung	Tätigkeiten der Strafverfolgungsbehörden oder in deren Auftrag zur Verhütung, Ermittlung oder Verfolgung von Straftaten.
47	Büro für Künstliche Intelligenz	Teil der EU-Kommission, zuständig für Überwachung

Nr	Begriff	Kurzdefinition
		und Umsetzung der KI-VO und deren Governance.
48	Zuständige nationale Behörde	Entweder die notifizierende Behörde oder Marktüberwachungsbehörde eines Mitgliedstaats; bei EU-Behörden gilt der Europäische Datenschutzbeauftragte.
49	Schwerwiegender Vorfall	Ein Ereignis oder Fehler in Bezug auf ein KI-System, das zu Tod, schwerer Verletzung, erheblicher Störung kritischer Infrastrukturen, Grundrechtsverletzung oder großem Sach- oder Umweltschaden führt.
50	Personenbezogene Daten	Informationen über eine identifizierte oder identifizierbare Person (im Sinne der Datenschutz-Grundverordnung).
51	Nicht personenbezogene Daten	Daten, die keinen Bezug zu identifizierbaren Personen haben.
52	Profiling	Automatisierte Bewertung oder Analyse persönlicher Merkmale auf Basis personenbezogener Daten (zB für gezielte Werbung).
53	Plan für einen Test unter Realbedingungen	Ein Dokument, das Ziele, Vorgehen, Umfang, Überwachung und Durchführung eines Tests mit einem KI-System unter echten Bedingungen beschreibt.
54	Plan für das Reallabor	Vereinbarung zwischen Anbieter und Behörde zu Bedingungen, Zeitrahmen und

Nr	Begriff	Kurzdefinition
		Anforderungen für Tests mit KI-Systemen unter Aufsicht.
55	KI-Reallabor	Ein von der Behörde geschaffener, regulierter Rahmen, in dem neue KI-Systeme für einen begrenzten Zeitraum getestet und entwickelt werden können.
56	KI-Kompetenz	Die Kenntnisse, Fähigkeiten und das Verständnis, die Nutzer und Anbieter brauchen, um KI-Systeme sachkundig und bewusst einzusetzen.
57	Test unter Realbedingungen	Ein befristeter Test eines KI-Systems in echten Einsatzumgebungen, aber noch ohne endgültiges Inverkehrbringen oder Inbetriebnahme.
58	Testteilnehmer	Person, die an einem Test unter Realbedingungen mit einem KI-System teilnimmt.
59	Informierte Einwilligung	Freiwillige, bewusste und eindeutige Zustimmung einer Person zur Teilnahme an einem Test, nachdem sie über alle wichtigen Aspekte informiert wurde.
60	Deepfake	Durch KI erzeugte oder manipulierte Bilder, Töne oder Videos, die echten Menschen, Dingen oder Ereignissen ähneln und täuschend echt wirken.
61	Weitverbreiteter Verstoß	Handlung oder Unterlassung, die in mindestens zwei anderen EU-Staaten neben dem Ursprungsland kollektive

Nr	Begriff	Kurzdefinition
		Interessen von Einzelpersonen verletzt oder verletzen kann.
62	Kritische Infrastrukturen	Besonders wichtige Einrichtungen (wie Energieversorgung, Verkehr, Gesundheit), die nach EU-Recht als „kritisch“ eingestuft sind.
63	KI-Modell mit allgemeinem Verwendungszweck (GPAI)	*Siehe KI-Modell für genauere Definition*
64	Fähigkeiten mit hoher Wirkkraft	Fähigkeiten, die den modernsten GPAI-Modellen entsprechen oder diese sogar übersteigen.
65	Systemisches Risiko	Risiko, das speziell von GPAI-Modellen ausgeht und durch deren Einfluss auf die Gesellschaft oder den Binnenmarkt große Auswirkungen haben kann.
66	KI-System mit allgemeinem Verwendungszweck	Ein KI-System, das auf einem GPAI-Modell basiert und vielfältig für direkte Nutzung oder zur Integration in andere Systeme einsetzbar ist.
67	Gleitkommaoperation	Rechenoperationen mit Gleitkommazahlen, wie sie typischerweise für komplexe Berechnungen in Computern genutzt werden.
68	Nachgelagerter Anbieter	Anbieter eines KI-Systems (einschließlich GPAI-Systeme), das ein externes KI-Modell integriert, egal ob selbst entwickelt oder zugekauft.

B. Ausgewählte Begriffe im Detail

1. KI-System (Artikel 3 Z 1)

a) Definition

Ein **KI-System** ist ein maschinengestütztes System, das – mehr oder weniger selbstständig – arbeitet, nach seiner Inbetriebnahme anpassungsfähig sein *kann* und auf Basis von Eingaben bestimmte Ausgaben (wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen) erzeugt, die wiederum reale oder virtuelle Umgebungen beeinflussen können.

b) Zentrale Merkmale

- **Maschinengestützt**: Ein KI-System braucht immer Hardware (zB Computer, Server) und Software.
- **Autonomer Betrieb**: Es arbeitet unabhängig, aber nicht zwingend völlig ohne Menschen. Es reicht, dass es Entscheidungen oder Vorschläge selbstständig ausgibt.
- **Anpassungsfähigkeit**: Es kann sich weiterentwickeln (Lernfähigkeit), muss aber nicht unbedingt (zB starre Regel-KI zählt auch).
- **Zielorientierung**: Das System arbeitet auf bestimmte, teils verborgene Ziele hin.
- **Ableitung aus Eingaben**: Das KI-System erstellt seine Ausgaben auf Basis der Daten, die es bekommt.
- **Ausgaben (Outputs):** zB Prognosen, Empfehlungen, Inhalte (Texte, Bilder), Entscheidungen.
- **Umgebungsbezug**: Die Ausgaben beeinflussen die reale Welt (zB Roboterarm steuern) oder virtuelle Umgebung (zB Software-Filter).

c) Abgrenzung zu „einfacher Software“

Nicht alles ist KI! Einfache Programme, die nur nach festen, vom Menschen vorgegebenen Regeln funktionieren (etwa ein Taschenrechner, der nur Rechenregeln abarbeitet), sind keine KI-Systeme. Entscheidend ist

die **Fähigkeit zur „Ableitung“**: Nur Systeme, die wirklich aus Eingaben heraus selbstständig Lösungen, Empfehlungen oder Muster generieren, gelten als KI.

d) **Unbestimmtheit und Praxisprobleme**

Manche Merkmale (zB „Autonomie“, „Anpassungsfähigkeit“) sind recht offen und auslegungsbedürftig formuliert. Die EU-Kommission hat deshalb eigene Leitlinien veröffentlicht, um die Abgrenzung zu erleichtern. In der Praxis ist oft unklar, ob ein bestimmtes System wirklich als „KI-System“ gilt. Dies kann zu Unsicherheiten bei Unternehmen, Entwicklern und Behörden führen.

Beispiel: *Ein System, das einfache Daten sortiert, ist keine KI – aber wo liegt die Grenze zur echten KI, wenn das System plötzlich aus Daten Muster erkennt?*

2. KI-Modell mit allgemeinem Verwendungszweck (GPAI)

a) **Definition**

Ein KI-Modell mit allgemeinem Verwendungszweck (englisch: General Purpose AI, abgekürzt GPAI) ist ein besonders vielseitiges, leistungsstarkes KI-Modell, das für eine Vielzahl ganz unterschiedlicher Aufgaben einsetzbar ist. Es ist so konzipiert, dass es – unabhängig von seiner späteren Verwendung – viele verschiedene Arten von Problemen lösen kann. Typische Beispiele sind große Sprachmodelle (wie ChatGPT).

b) **Eigenschaften von GPAI:**

- **Breite Einsetzbarkeit**: Ein GPAI-Modell kann für viele verschiedene Anwendungen genutzt werden, etwa für Chatbots, Übersetzungen, Texterstellung, Datenanalyse oder Bilderkennung – teils sogar gleichzeitig.
- **Zentrale Komponente**: Das GPAI-Modell bildet den „algorithmischen Kern“ vieler moderner KI-Systeme. Es handelt sich dabei um das trainierte „Hirn“ der KI, also zB ein neuronales Netz, das durch Training Muster und Zusammenhänge gelernt hat.

- **Integration in Systeme**: GPAI-Modelle sind oft so gestaltet, dass sie in verschiedenste Produkte, Dienste oder Softwarelösungen eingebunden („integriert“) werden können. Ein und dasselbe Modell kann also als Grundlage für viele verschiedene KI-Systeme dienen.

c) **Abgrenzung zum KI-System:**

Begriff	Wesenskern und Funktion	Beispiel
KI-Modell (GPAI)	Das trainierte „Innenleben“ – also der technische, lernende Algorithmus (zB neuronales Netz, Entscheidungsbaum). Für sich genommen noch keine fertige Anwendung, sondern „nur“ das Rechenmodell.	GPT-4, das Modell als solches ohne Benutzeroberfläche
KI-System	Das vollständige Produkt, das aus einem oder mehreren KI-Modellen sowie weiteren Modulen (zB Benutzeroberfläche, Steuerung, spezifische Anweisungen, Sicherheit, Einsatzumgebung) besteht und tatsächlich eingesetzt wird.	Chatbot, der auf GPT-4 basiert und mit einer App-Oberfläche, Nutzerführung und Datenschutzfunktionen versehen ist

III. Quellenverzeichnis

- Erwägungsgründe 12-19 KI-VO (EU) 2024/1689
- Leitlinien der Kommission zur Definition eines KI-Systems gem KI-VO (EU) 2024/1689

Artikel 4 KI-VO

KI-Kompetenz

Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind.

I. Worum geht es?

Artikel 4 KI-VO verpflichtet Anbieter und Betreiber von KI-Systemen, Maßnahmen zu ergreifen, damit das eingesetzte Personal sowie weitere beauftragte Personen „nach besten Kräften" über ausreichende **KI-Kompetenz** verfügen. Dies soll sicherstellen, dass KI-Systeme sicher, verantwortungsvoll und grundrechtskonform entwickelt und betrieben werden.

II. Detailkommentar

A. Begriff und Inhalt der „KI-Kompetenz"

1. Definition (vgl Artikel 3 KI-VO Z 56)

KI-Kompetenz meint das Wissen, die Fähigkeiten und die Einstellung, die notwendig sind, um KI-Systeme sicher, vertrauenswürdig und effizient zu entwickeln, zu betreiben, zu überwachen und zu verwenden.

2. Differenzierung

Die gesetzliche Definition bleibt vergleichsweise abstrakt. Für die Praxis empfiehlt sich eine Differenzierung:

- **Technische Kompetenz**: Bedienung, Funktionsweise, Grenzen, Risiken.

- **Rechtliche Kompetenz**: Grundrechte, Datenschutz, Haftung, Compliance.
- **Ethische Kompetenz**: Bias-Erkennung, Fairness, gesellschaftliche Auswirkungen.

Ohne diese Trennung droht die Gefahr, dass Unternehmen den Begriff minimalistisch auslegen und zB rein technische Basisschulungen als ausreichend betrachten.

3. Konkrete Ausgestaltung

- Erkennen und Verstehen technischer Zusammenhänge (zB Funktionsweise, Grenzen, Risiken der KI).
- Anwendung und Interpretation von KI-Systemen im Arbeitskontext.
- Einschätzen, wie sich KI-Entscheidungen auf Menschen auswirken.
- Fähigkeit, Grundrechte, Gesundheit, Sicherheit und ethische Standards bei Nutzung und Überwachung der KI zu wahren.

Beispiel: *Ein Unternehmen, das eine KI-gestützte Personalsoftware einsetzt, muss sicherstellen, dass die HR-Mitarbeitenden nicht nur wissen, wie die Software technisch funktioniert, sondern auch, welche möglichen Verzerrungen (Bias) auftreten können und wie sie Entscheidungen der KI bewerten oder hinterfragen können.*

B. „Nach besten Kräften" – Was bedeutet das?

- **Kein starrer Standard**: Die Maßnahmen richten sich nach den jeweiligen Möglichkeiten des Anbieters/Betreibers („nach besten Kräften"). Das bedeutet: Es muss alles Zumutbare getan werden, ist aber keine Erfolgsgarantie.
- **Abhängig vom Einzelfall**: Welche Maßnahmen erforderlich sind, hängt von den konkreten Umständen ab. Je höher das Risiko eines KI-Systems, desto strenger die Anforderungen. Zudem spielt die Größe und Ausstattung des Unternehmens eine Rolle: Während kleinere Anbieter im Rahmen ihrer begrenzten Mittel handeln dürfen, wird von großen Unternehmen erwartet, dass sie aufgrund ihrer umfangreicheren Ressourcen mehr investieren.

Beispiel: *Eine kleine Arztpraxis, die eine einfache KI-Software zur Terminplanung verwendet, muss weniger aufwändige Schulungen nachweisen als ein Krankenhaus, das KI zur Diagnoseunterstützung einsetzt.*

C. Wer muss konkret geschult sein?

Betroffen sind:

- **Eigenes Personal**: Alle Mitarbeitenden, die mit Entwicklung, Betrieb, Nutzung oder Überwachung eines KI-Systems befasst sind.
- **Beauftragte Dritte**: Personen, die im Auftrag des Anbieters/Betreibers tätig werden (zB externe Dienstleister).

Beispiel: *Ein Unternehmen, das eine externe IT-Firma mit der Wartung seines KI-Systems betraut, muss auch sicherstellen, dass die Mitarbeitenden dieser Firma über ausreichende KI-Kompetenz verfügen.*

D. Wie erfolgt die Schulung?

1. Schulungsformen:

- Interne Weiterbildungen und Workshops
- Externe Kurse, Zertifikate oder Online-Schulungen
- Praxisorientierte Trainings am Arbeitsplatz

2. Inhaltliche Anpassung:

Die Maßnahmen müssen kontinuierlich erfolgen und sich am jeweiligen Einsatzbereich orientieren. Je nach Komplexität der KI-Anwendung genügt eine Basisschulung oder es sind vertiefte Spezialkenntnisse erforderlich. Oft reicht einmalige Basisschulung nicht aus, insbesondere bei Systemen, die sich dynamisch weiterentwickeln.

E. Rechtsfolgen

- **Keine direkten Sanktionen**: Artikel 4 KI-VO sieht keine eigenständigen Strafen bei Verstößen vor (vgl Artikel 99 KI-VO ff).

- **Haftungsrecht**: Mangelnde KI-Kompetenz kann allerdings eine indirekte Wirkung bei Haftungsfragen entfalten (zB bei Schäden durch Fehlbedienung) oder bei der Beurteilung von Sorgfaltspflichten entscheidend sein.
- **Appellcharakter**: Die Vorschrift ist ein klarer Appell an Unternehmen, kontinuierlich in die Kompetenz ihrer Mitarbeitenden zu investieren, um sichere und vertrauenswürdige KI-Anwendungen zu fördern.

F. Erhöhte Anforderungen bei Hochrisiko-KI

Besonders bei Hochrisiko-KI-Systemen müssen die für die menschliche Aufsicht zuständigen Personen nicht nur technisch geschult, sondern auch befugt und kompetent sein, um im Zweifel steuernd oder korrigierend einzugreifen.

Hier ist eine klare Staffelung zwischen Basis- und Spezialkompetenz je nach Risikostufe erforderlich. Bei Hochrisiko-Anwendungen reicht keine Basiskompetenz aus – erforderlich sind vertiefte Spezialkenntnisse, differenziert nach technischer, rechtlicher und ethischer Dimension.

Beispiel: *Bei einer KI, die im Bereich der Strafverfolgung zur Gesichtserkennung eingesetzt wird, müssen mindestens zwei besonders geschulte Personen unabhängig voneinander eine positive Identifizierung bestätigen, bevor Maßnahmen ergriffen werden.*

III. Zusammenfassung

Ziel	Sicherstellung der Kompetenz im Umgang mit KI-Systemen
Betroffene	Personal und beauftragte Dritte
Maßnahmen	Schulungen und Weiterbildungen, angepasst an den jeweiligen Kontext
Standard	„Nach besten Kräften“ – keine starren Vorgaben, Einzelfallabhängig
Rechtsfolgen	Keine direkten Sanktionen, aber Bedeutung für Haftung/Sorgfalt

Besonderheiten	Strengere Anforderungen bei Hochrisiko-KI und menschlicher Aufsicht

IV. Quellenverzeichnis

- Erwägungsgründe 20, 21, 73 KI-VO (EU) 2024/1689

Artikel 5 KI-VO

Verbotene Praktiken im KI-Bereich

(1) Folgende Praktiken im KI-Bereich sind verboten:

a) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken mit dem Ziel oder der Wirkung einsetzt, das Verhalten einer Person oder einer Gruppe von Personen wesentlich zu verändern, indem ihre Fähigkeit, eine fundierte Entscheidung zu treffen, deutlich beeinträchtigt wird, wodurch sie veranlasst wird, eine Entscheidung zu treffen, die sie andernfalls nicht getroffen hätte, und zwar in einer Weise, die dieser Person, einer anderen Person oder einer Gruppe von Personen erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird.

b) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das eine Vulnerabilität oder Schutzbedürftigkeit einer natürlichen Person oder einer bestimmten Gruppe von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation mit dem Ziel oder der Wirkung ausnutzt, das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu verändern, die dieser Person oder einer anderen Person erheblichen Schaden zufügt oder mit hinreichender Wahrscheinlichkeit zufügen wird;

c) das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen zur Bewertung oder Einstufung von natürlichen Personen oder Gruppen von Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale, wobei die soziale Bewertung zu einem oder beiden der folgenden Ergebnisse führt:

i) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in sozialen Zusammenhängen, die in keinem Zusammenhang zu den Umständen stehen, unter denen die Daten ursprünglich erzeugt oder erhoben wurden;

ii) Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Gruppen von Personen in einer Weise, die im Hinblick

auf ihr soziales Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig ist;

d)das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen; dieses Verbot gilt nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen;

e)das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern;

f)das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und in Bildungseinrichtungen, es sei denn, die Verwendung des KI-Systems soll aus medizinischen Gründen oder Sicherheitsgründen eingeführt oder auf den Markt gebracht werden;

g)das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von Systemen zur biometrischen Kategorisierung, mit denen natürliche Personen individuell auf der Grundlage ihrer biometrischen Daten kategorisiert werden, um ihre Rasse, ihre politischen Einstellungen, ihre Gewerkschaftszugehörigkeit, ihre religiösen oder weltanschaulichen Überzeugungen, ihr Sexualleben oder ihre sexuelle Ausrichtung zu erschließen oder abzuleiten; dieses Verbot gilt nicht für die Kennzeichnung oder Filterung rechtmäßig erworbener biometrischer Datensätze, wie zB Bilder auf der Grundlage biometrischer Daten oder die Kategorisierung biometrischer Daten im Bereich der Strafverfolgung;

h)die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken, außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist:

i) gezielte Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie die Suche nach vermissten Personen;

ii) Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags;

iii) Aufspüren oder Identifizieren einer Person, die der Begehung einer Straftat verdächtigt wird, zum Zwecke der Durchführung von strafrechtlichen Ermittlungen oder von Strafverfahren oder der Vollstreckung einer Strafe für die in Anhang II aufgeführten Straftaten, die in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens vier Jahren bedroht ist.

Unterabsatz 1 Buchstabe h gilt unbeschadet des Artikels 9 der Verordnung (EU) 2016/679 für die Verarbeitung biometrischer Daten zu anderen Zwecken als der Strafverfolgung.

(2) Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Hinblick auf die in Absatz 1 Unterabsatz 1 Buchstabe h genannten Ziele darf für die in jenem Buchstaben genannten Zwecke nur zur Bestätigung der Identität der speziell betroffenen Person erfolgen, wobei folgende Elemente berücksichtigt werden:

a) die Artikel der Situation, die der möglichen Verwendung zugrunde liegt, insbesondere die Schwere, die Wahrscheinlichkeit und das Ausmaß des Schadens, der entstehen würde, wenn das System nicht eingesetzt würde;

b) die Folgen der Verwendung des Systems für die Rechte und Freiheiten aller betroffenen Personen, insbesondere die Schwere, die Wahrscheinlichkeit und das Ausmaß solcher Folgen.

Darüber hinaus sind bei der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken im Hinblick auf die in Absatz 1 Unterabsatz 1 Buchstabe h des vorliegenden Artikels genannten Ziele notwendige und verhältnismäßige Schutzvorkehrungen und Bedingungen für die Verwendung im Einklang mit nationalem Recht über die Ermächtigung ihrer Verwendung einzuhalten, insbesondere in Bezug auf die zeitlichen,

geografischen und personenbezogenen Beschränkungen. Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen ist nur dann zu gestatten, wenn die Strafverfolgungsbehörde eine Folgenabschätzung im Hinblick auf die Grundrechte gemäß Artikel 27 abgeschlossen und das System gemäß Artikel 49 in der EU-Datenbank registriert hat. In hinreichend begründeten dringenden Fällen kann jedoch mit der Verwendung solcher Systeme zunächst ohne Registrierung in der EU-Datenbank begonnen werden, sofern diese Registrierung unverzüglich erfolgt.

(3) Für die Zwecke des Absatz 1 Unterabsatz 1 Buchstabe h und des Absatzes 2 ist für jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken eine vorherige Genehmigung erforderlich, die von einer Justizbehörde oder einer unabhängigen Verwaltungsbehörde des Mitgliedstaats, in dem die Verwendung erfolgen soll, auf begründeten Antrag und gemäß den in Absatz 5 genannten detaillierten nationalen Rechtsvorschriften erteilt wird, wobei deren Entscheidung bindend ist. In hinreichend begründeten dringenden Fällen kann jedoch mit der Verwendung eines solchen Systems zunächst ohne Genehmigung begonnen werden, sofern eine solche Genehmigung unverzüglich, spätestens jedoch innerhalb von 24 Stunden beantragt wird. Wird eine solche Genehmigung abgelehnt, so wird die Verwendung mit sofortiger Wirkung eingestellt und werden alle Daten sowie die Ergebnisse und Ausgaben dieser Verwendung unverzüglich verworfen und gelöscht.

Die zuständige Justizbehörde oder eine unabhängige Verwaltungsbehörde, deren Entscheidung bindend ist, erteilt die Genehmigung nur dann, wenn sie auf der Grundlage objektiver Nachweise oder eindeutiger Hinweise, die ihr vorgelegt werden, davon überzeugt ist, dass die Verwendung des betreffenden biometrischen Echtzeit-Fernidentifizierungssystems für das Erreichen eines der in Absatz 1 Unterabsatz 1 Buchstabe h genannten Ziele — wie im Antrag angegeben — notwendig und verhältnismäßig ist und insbesondere auf das in Bezug auf den Zeitraum sowie den geografischen und persönlichen Anwendungsbereich unbedingt erforderliche Maß beschränkt bleibt. Bei ihrer Entscheidung über den Antrag berücksichtigt diese Behörde die in Absatz 2 genannten Elemente. Eine Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, darf nicht ausschließlich auf der Grundlage der Ausgabe des biometrischen Echtzeit-Fernidentifizierungssystems getroffen werden.

(4) Unbeschadet des Absatzes 3 wird jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken der zuständigen Marktüberwachungsbehörde und der nationalen Datenschutzbehörde gemäß den in Absatz 5 genannten nationalen Vorschriften mitgeteilt. Die Mitteilung muss mindestens die in Absatz 6 genannten Angaben enthalten und darf keine sensiblen operativen Daten enthalten.

(5) Ein Mitgliedstaat kann die Möglichkeit einer vollständigen oder teilweisen Ermächtigung zur Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken innerhalb der in Absatz 1 Unterabsatz 1 Buchstabe h sowie Absätze 2 und 3 aufgeführten Grenzen und unter den dort genannten Bedingungen vorsehen. Die betreffenden Mitgliedstaaten legen in ihrem nationalen Recht die erforderlichen detaillierten Vorschriften für die Beantragung, Erteilung und Ausübung der in Absatz 3 genannten Genehmigungen sowie für die entsprechende Beaufsichtigung und Berichterstattung fest. In diesen Vorschriften wird auch festgelegt, im Hinblick auf welche der in Absatz 1 Unterabsatz 1 Buchstabe h aufgeführten Ziele und welche der unter Buchstabe h Ziffer iii genannten Straftaten die zuständigen Behörden ermächtigt werden können, diese Systeme zu Strafverfolgungszwecken zu verwenden. Die Mitgliedstaaten teilen der Kommission diese Vorschriften spätestens 30 Tage nach ihrem Erlass mit. Die Mitgliedstaaten können im Einklang mit dem Unionsrecht strengere Rechtsvorschriften für die Verwendung biometrischer Fernidentifizierungssysteme erlassen.

(6) Die nationalen Marktüberwachungsbehörden und die nationalen Datenschutzbehörden der Mitgliedstaaten, denen gemäß Absatz 4 die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken mitgeteilt wurden, legen der Kommission Jahresberichte über diese Verwendung vor. Zu diesem Zweck stellt die Kommission den Mitgliedstaaten und den nationalen Marktüberwachungs- und Datenschutzbehörden ein Muster zur Verfügung, das Angaben über die Anzahl der Entscheidungen der zuständigen Justizbehörden oder einer unabhängigen Verwaltungsbehörde, deren Entscheidung über Genehmigungsanträge gemäß Absatz 3 bindend ist, und deren Ergebnis enthält.

(7) Die Kommission veröffentlicht Jahresberichte über die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich

zugänglichen Räumen zu Strafverfolgungszwecken, die auf aggregierten Daten aus den Mitgliedstaaten auf der Grundlage der in Absatz 6 genannten Jahresberichte beruhen. Diese Jahresberichte dürfen keine sensiblen operativen Daten im Zusammenhang mit den damit verbundenen Strafverfolgungsmaßnahmen enthalten.

(8) Dieser Artikel berührt nicht die Verbote, die gelten, wenn KI-Praktiken gegen andere Rechtsvorschriften der Union verstoßen.

I. Worum geht es?

Artikel 5 der KI-VO verbietet bestimmte KI-Praktiken mit **unannehmbarem Risiko**. Gemeinsamer Nenner: Es geht um schwere Eingriffe in Grundrechte (zB Würde, Privatleben, Nichtdiskriminierung) oder um massiv risikoreiche Überwachungs-/Kontrollanwendungen. Die Verbote erfassen das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen.

II. Detailkommentar

A. Risikobasierter Ansatz

Die Regulierung der KI-VO folgt dem Risiko bestimmter Anwendungsfälle. Artikel 5 bildet dabei die höchste Stufe: Praktiken mit unannehmbarem Risiko sind absolut verboten.

- **Ethik und Grundrechte:** Die in Artikel 5 verbotenen KI-Praktiken verletzen Grundrechte wie Menschenwürde, Nichtdiskriminierung und Sicherheit und spiegeln daher die Leitgedanken vertrauenswürdiger KI wider (Transparenz, Nichtdiskriminierung, Rechenschaft, Sicherheit).
- **Folge**: Liegen die Voraussetzungen des Artikel 5 vor, helfen keine technischen oder organisatorischen Maßnahmen – die Praxis ist verboten.

B. Aufzählung verbotener Praktiken

1. Manipulation/Täuschung (lit a)

- **Tatbestand**: KI nutzt unterschwellige, absichtlich manipulative oder täuschende Techniken, die die Entscheidungsfähigkeit von Personen deutlich beeinträchtigen und ihr Verhalten wesentlich verändern sollen.
- **Schadensschwelle**: Führt zu erheblichem Schaden oder ist hinreichend wahrscheinlich – auch verschiedene Schäden gemeinsam (zB psychisch, physisch, finanziell)
- **Abgrenzung**: Ziel oder Wirkung genügt; es braucht keine Schädigungsabsicht. Rechtmäßige Überzeugungsarbeit (zB gesetzeskonforme Werbung) bleibt zulässig. Medizinische/therapeutische Anwendungen sind nicht erfasst, wenn sie rechtmäßig erfolgen.

Beispiel: *Ein VR-Coaching setzt nicht wahrnehmbare Reize ein, die Nutzer in eine Panikreaktion treiben, um kostenpflichtige „Lösungen" zu verkaufen.*

2. Ausnutzung von Vulnerabilitäten (lit b)

- **Tatbestand**: KI nutzt die Schutzbedürftigkeit von Personen oder Gruppen wegen Alter, Behinderung oder einer bestimmten sozialen/ökonomischen Lage aus, um Verhalten wesentlich zu verändern.
- **Schadensschwelle**: Erheblicher Schaden oder hinreichende Wahrscheinlichkeit.
- **Abgrenzung**: Nicht erfasst sind neutrale/legitime Funktionen ohne Ausnutzungsabsicht/-wirkung. Die Schutzmerkmale sind abschließend (Alter, Behinderung, soziale/ökonomische Lage).

Beispiel: *Eine App für Überschuldete blendet KI-gestützt zeitkritische Drohhinweise ein („sofort zahlen, sonst…"), um überteuerte Mikro-Kredite abzuschließen.*

3. Soziale Bewertung (Social Scoring) (lit c)

- **Tatbestand**: KI bewertet/einstuft Personen über einen Zeitraum anhand sozialen Verhaltens oder (abgeleiteter/vorhergesagter) Eigenschaften.Verboten, wenn die Bewertung zu

  (i) Benachteiligungen in Kontexten ohne sachlichen Zusammenhang mit der Datenerhebung führt oder

  (ii) gemessen am sozialen Verhalten ungerechtfertigt/unverhältnismäßig ist.

- **Abgrenzung**: Gilt für private und öffentliche Akteure. Legitime Einzelfall-Bewertungen zu bestimmtem Zweck (zB Kreditwürdigkeitsprüfung nach geltendem Recht) bleiben möglich.

4. Individuelle Kriminalitäts-Risikoprognosen (lit d)

- **Tatbestand**: KI bewertet oder sagt voraus, ob eine Person eine Straftat begehen wird – ausschließlich auf Basis von Profiling oder persönlichen Merkmalen/Eigenschaften.
- **Ausnahme**: Zulässig ist die Unterstützung einer menschlichen Bewertung, wenn diese sich auf objektive, überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen.
- **Abgrenzung**: Nicht erfasst: orts-/musterbezogene Risikoanalysen (zB Schmuggelrouten), Vorhersagen zu Unternehmen, Ordnungswidrigkeiten.

Beispiel: *Ein Tool prognostiziert Rückfallgefahr allein aus Wohnort, Alter, Schuldenstand – ohne konkrete Tatbezüge ist dies verboten.*

5. Ungezieltes Auslesen von Gesichtsbildern (lit e)

- **Tatbestand**: KI erstellt/erweitert Gesichtserkennungs-Datenbanken durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder aus Überwachungsaufnahmen.

- **Abgrenzung**: Verbot bezieht sich auf das ungezielte Massen-Scraping. Andere Datenquellen bleiben nur im Rahmen des geltenden Rechts relevant.

Beispiel: *Ein Anbieter extrahiert systematisch Profilfotos aus sozialen Netzwerken, um eine kommerzielle Facial-Recognition-Datenbank aufzubauen.*

6. Emotionserkennung am Arbeitsplatz/in Bildung (lit f)

- **Tatbestand**: KI leitet Emotionen von Personen im Arbeitsumfeld oder in Bildungseinrichtungen ab.
- **Ausnahmen**: Medizinische Gründe (zB Therapie) oder Sicherheitsgründe (zB Ermüdungsdetektion im Leitstand) – jeweils eng auszulegen.
- **Abgrenzung**: Mitgliedstaaten dürfen strengere Regeln vorsehen. Unabhängig davon gelten Datenschutz- und Arbeitsrecht.

Beispiel: *Ein Arbeitgeber setzt eine Kamera-KI ein, die „Arbeitsmotivation" erkennt und Leistungsprämien entsprechend kürzt.*

7. Biometrische Kategorisierung sensibler Merkmale (lit g)

- **Tatbestand**: KI kategorisiert Personen individuell anhand biometrischer Daten (zB Gesicht, Fingerabdruck), um Rasse, politische Einstellung, Gewerkschaftszugehörigkeit, Religion/Weltanschauung, Sexualleben oder sexuelle Orientierung zu erschließen/abzuleiten.
- **Ausnahme**: Zulässig ist die Kennzeichnung/Filterung rechtmäßig erworbener biometrischer Datensätze (zB Sortierung von Bildern nach Augenfarbe, auch im Bereich der Strafverfolgung).

Beispiel: *Ein Zugangssystem versucht aus dem Gesicht die politische Haltung einer Person zu schätzen, um Zutritt zu steuern.*

8. Biometrische Echtzeit-Fernidentifizierung in öffentlichen Räumen zu Strafverfolgungszwecken (lit h)

Grundsatz: Verboten.

- **Ausnahmen** (nur wenn unbedingt erforderlich):
    - Gezielte Suche nach Opfern schwerer Straftaten (zB Entführung, Menschenhandel, sexuelle Ausbeutung) sowie vermissten Personen.
    - Abwendung einer konkreten, erheblichen, unmittelbaren Gefahr für Leben/körperliche Unversehrtheitoder einer tatsächlichen und bestehenden/absehbaren Gefahr eines Terroranschlags.
    - Aufspüren/Identifizieren von Verdächtigen zu bestimmten (in Anhang II KI-VO gelisteten) Straftaten, die im betreffenden Mitgliedstaat mit mindestens 4 Jahren Höchstfreiheitsstrafe bedroht sind.
- **Schutzvorkehrungen und Bedingungen**
    - Zweckbindung der Maßnahme: Nur zur Bestätigung der Identität einer konkret betroffenen Person; engbegrenzt in Zeit, Ort und Personenkreis.
    - Grundrechte-Folgenabschätzung und Registrierung des Systems in der EU-Datenbank im Vorhinein, außer im dringenden Fall – dann ist dies unverzüglich nachholen.
    - Vorherige Genehmigung: durch Justizbehörde oder unabhängige Verwaltungsbehörde; im dringenden Fall ist der Start ohne Genehmigung zulässig, Antrag spätestens binnen 24 Stunden. Ablehnung führt zur sofortigen Einstellung, und Löschung aller im Zusammenhang stehenden Daten/Ausgaben. Keine nachteilige Entscheidung darf allein anhand der Systemausgabe getroffen werden; es bedarf qualifizierter menschlicher Intervention.
    - Mitteilungen/Berichte: Unterrichtung der Marktüberwachungs- und Datenschutzbehörden; nationale Jahresberichte und Kommissionsberichte auf Basis von aggregierten Meldedaten und nationalen Jahresberichten

- **Abgrenzung:**
  - Erfasst ist die Konstellation von Echtzeit + öffentlich zugänglicher Raum + Strafverfolgungszweck. Andere Konstellationen sind hier nicht erfasst, unterliegen aber anderem Recht (insb Datenschutz).

C. Besonderheiten

1. Schadensmaßstab

- **„Erheblich“**: Meint spürbar/gewichtige Nachteile (zB Gesundheit, psychische Belastung, Vermögensschäden), ggf aufsummiert.
- **„Nicht vermutet“:** Manipulationsabsicht wird nicht vermutet, wenn die Beeinflussung auf fremde, außerhalb des KI-Systems liegende Faktoren zurückgeht, die Anbieter/Betreiber nicht vorhersehen oder mindern konnten.
- **Ziel oder Wirkung**: Es genügt die objektive Wirkung – es ist keine Schädigungsabsicht nötig.

2. Zusammenspiel mit anderem Recht

- **Ergänzung**: Die KI-VO ergänzt hier ua die DSGVO, Richtlinie Datenschutz Strafverfolgung sowie den Arbeits-/Verbraucherschutz. Für biometrische Strafverfolgungsnutzung gilt die KI-VO als vorrangig anzuwendendes Gesetz.
- **Irland/Dänemark**: Sind an bestimmte Artikel-5-Bestimmungen im Strafverfolgungskontext teilweise nicht gebunden (Opt-out-Protokolle). Die nationale Umsetzung ist hier zu beachten.

III. Zusammenfassung

lit	Kurzformel	Typische Ausnahme(n)
a	Manipulation/Täuschung mit erheblichem Schaden	Medizin/ Therapie; rechtmäßige Werbung

b	Ausnutzung von Vulnerabilität (Alter/Behinderung/soziale Lage)	–
c	Soziale Bewertung mit Out-of-context oder unverhältnismäßiger Benachteiligung	Zulässige zweckgebundene Bewertungen
d	Individuelle Kriminalitäts-Risikoprognose nur aus Profiling/Merkmalen	Unterstützung einer menschlichen Bewertung mit objektiven Tatbezügen
e	Ungezieltes Scraping von Gesichtern für FR-Datenbanken	–
f	Emotionserkennung in Arbeit/Bildung	Medizin/Sicherheit
g	Biometrische Kategorisierungsensibler Merkmale	Label/Filter rechtmäßig erworbener Datensätze
h	Biometrische Echtzeit Fernidentifizierung in öffentlichen Räumen zu Strafverfolgung	Enge Ausnahmen (Opfersuche, Gefahrabwehr, schwere Straftaten) + Genehmigung/Grundrechte-Folgenabschätzung /Registrierung

IV. Quellenverzeichnis

- Erwägungsgründe 26–45 KI-VO (EU) 2024/1689
- Leitlinien der Kommission zu verbotenen KI-Praktiken

Artikel 6 KI-VO

Einstufungsvorschriften für Hochrisiko-KI-Systeme

(1) Ungeachtet dessen, ob ein KI-System unabhängig von den unter den Buchstaben a und b genannten Produkten in Verkehr gebracht oder in Betrieb genommen wird, gilt es als Hochrisiko-KI-System, wenn die beiden folgenden Bedingungen erfüllt sind:

a) das KI-System soll als Sicherheitsbauteil eines unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union fallenden Produkts verwendet werden oder das KI-System ist selbst ein solches Produkt;

b) das Produkt, dessen Sicherheitsbauteil gemäß Buchstabe a das KI-System ist, oder das KI-System selbst als Produkt muss einer Konformitätsbewertung durch Dritte im Hinblick auf das Inverkehrbringen oder die Inbetriebnahme dieses Produkts gemäß den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union unterzogen werden.

(2) Zusätzlich zu den in Absatz 1 genannten Hochrisiko-KI-Systemen gelten die in Anhang III genannten KI-Systeme als hochriskant.

(3) Abweichend von Absatz 2 gilt ein in Anhang III genanntes KI-System nicht als hochriskant, wenn es kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst.

Unterabsatz 1 gilt, wenn eine der folgenden Bedingungen erfüllt ist:

a) das KI-System ist dazu bestimmt, eine eng gefasste Verfahrensaufgabe durchzuführen;

b) das KI-System ist dazu bestimmt, das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern;

c) das KI-System ist dazu bestimmt, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, und ist nicht dazu gedacht, die zuvor abgeschlossene menschliche Bewertung ohne eine angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen; oder

d)das KI-System ist dazu bestimmt, eine vorbereitende Aufgabe für eine Bewertung durchzuführen, die für die Zwecke der in Anhang III aufgeführten Anwendungsfälle relevant ist.

Ungeachtet des Unterabsatzes 1 gilt ein in Anhang III aufgeführtes KI-System immer dann als hochriskant, wenn es ein Profiling natürlicher Personen vornimmt.

(4) Ein Anbieter, der der Auffassung ist, dass ein in Anhang III aufgeführtes KI-System nicht hochriskant ist, dokumentiert seine Bewertung, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird. Dieser Anbieter unterliegt der Registrierungspflicht gemäß Artikel 49 Absatz 2. Auf Verlangen der zuständigen nationalen Behörden legt der Anbieter die Dokumentation der Bewertung vor.

(5) Die Kommission stellt nach Konsultation des Europäischen Gremiums für Künstliche Intelligenz (im Folgenden „KI-Gremium“) spätestens bis zum 2. Februar 2026 Leitlinien zur praktischen Umsetzung dieses Artikels gemäß Artikel 96 und eine umfassende Liste praktischer Beispiele für Anwendungsfälle für KI-Systeme, die hochriskant oder nicht hochriskant sind, bereit.

(6) Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zu erlassen, um Absatz 3 Unterabsatz 2 des vorliegenden Artikels zu ändern, indem neue Bedingungen zu den darin genannten Bedingungen hinzugefügt oder diese geändert werden, wenn konkrete und zuverlässige Beweise für das Vorhandensein von KI-Systemen vorliegen, die in den Anwendungsbereich von Anhang III fallen, jedoch kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen bergen.

(7) Die Kommission erlässt gemäß Artikel 97 delegierte Rechtsakte, um Absatz 3 Unterabsatz 2 des vorliegenden Artikels zu ändern, indem eine der darin festgelegten Bedingungen gestrichen wird, wenn konkrete und zuverlässige Beweise dafür vorliegen, dass dies für die Aufrechterhaltung des Schutzniveaus in Bezug auf Gesundheit, Sicherheit und die in dieser Verordnung vorgesehenen Grundrechte erforderlich ist.

(8) Eine Änderung der in Absatz 3 Unterabsatz 2 festgelegten Bedingungen, die gemäß den Absätzen 6 und 7 des vorliegenden Artikels erlassen wurde, darf das allgemeine Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in dieser Verordnung vorgesehenen Grundrechte nicht senken; dabei ist

die Kohärenz mit den gemäß Artikel 7 Absatz 1 erlassenen delegierten Rechtsakten sicherzustellen und die Marktentwicklungen und die technologischen Entwicklungen sind zu berücksichtigen.

I. Worum geht es?

Artikel 6 KI-VO legt fest, wann ein KI-System als Hochrisiko gilt und damit den strengeren Anforderungen der Verordnung unterliegt. Das ist der Fall, wenn es Teil sicherheitsrelevanter Produkte ist (zB Autos, Maschinen) oder in besonders sensiblen Bereichen eingesetzt wird (zB Bildung, Arbeit, Justiz)Es gibt Ausnahmen, wenn kein erhebliches Risiko vorliegt und bestimmte enge Bedingungen erfüllt sind.

II. Detailkommentar

A. Risikobasierter Ansatz

Die Regulierung der KI-VO folgt dem Risiko bestimmter Anwendungsfälle. Hochrisiko ist dabei keine pauschale Technikbewertung, sondern knüpft an Kontext und Folgen an:

- **Schutzgüter**: Gesundheit, Sicherheit, Grundrechte.
- **Verhältnismäßigkeit**: Nur Systeme mit erheblichen negativen Auswirkungen zählen als hochriskant.
- **Koordination mit Produktrecht**: Mehrere Harmonisierungsrechtsakte können gleichzeitig gelten. Ziel ist Kohärenz und kein Doppelaufwand.
- **Konsequenz**: Artikel 6 verknüpft den Ansatz mit klaren Kriterien: Produktkategorien (Anhang I KI-VO) oder Einsatzbereiche (Anhang III KI-VO).

B. Klassifizierung nach dem Produktsicherheitsrecht

Ein KI-System ist hochriskant, wenn beide Bedingungen gleichzeitig erfüllt sind:

1. Es soll als Sicherheitsbauteil eines Produkts nach *Anhang I* verwendet werden oder ist selbst ein solches Produkt.
2. Das Produkt bzw die KI muss nach den in *Anhang I* genannten Rechtsvorschriften einer Konformitätsbewertung durch Dritte unterzogen werden.

Erfasst von Anhang I (siehe dazu Ausführungen zu Anhang I KI-VO) sind bestimmte Sektoren des EU-Produktrechts (zB Maschinen, Spielzeuge, Medizinprodukte, In-vitro-Diagnostika, Fahrzeuge, Luftfahrt uä). Zu beachten ist, dass Hochrisiko nach Artikel 6 nicht automatisch „hohes Produktrisiko" im jeweiligen Fachrecht bedeutet.

Beispiel: *Ein KI-gestütztes Bremssystem für ein Auto (Sicherheitsbauteil) fällt unter Anhang I und muss durch eine externe Stelle geprüft werden → Hochrisiko-KI.*

C. Klassifizierung nach dem Verwendungszweck

Zusätzlich zu Absatz 1 gelten die in Anhang III (siehe dazu Ausführungen zu Anhang III KI-VO) genannten KI-Systeme als hochriskant. Das betrifft insbesondere:

- **Biometrie** (zB biometrische Fernidentifizierung, Kategorisierung nach sensiblen Merkmalen, Emotionserkennung).
- **Kritische Infrastruktur** (zB Betrieb und Verwaltung).
- **Bildung** (Zugang, Zulassung, Bewertung, Prüfungsaufsicht).
- **Beschäftigung und Personalwesen** (Einstellung, Beförderung, Überwachung).
- **Essenzielle öffentliche Dienste und soziale Leistungen** sowie **Kreditwürdigkeit**.
- **Strafverfolgung** (bestimmte Ermittlungsunterstützung).
- **Migration, Asyl, Grenzkontrolle**
- **Rechtspflege und demokratische Prozesse** (richterliche Unterstützung, Beeinflussung von Ergebnis oder Wahlverhalten).

D. Ausnahmetatbestand für Anhang-III-Systeme

Schritt 1 – Grundvoraussetzung: Das in Anhang III KI-VO genannte System birgt kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte und beeinflusst das Entscheidungsergebnis nicht wesentlich.

Schritt 2 – Mindestens eine Bedingung (a)–(d):

- *(a) Eng gefasste Verfahrensaufgabe:*
  zB Konvertierung unstrukturierter in strukturierte Daten, Kategorisierungvon Eingängen, Dublettenerkennung.

- *(b) Verbesserung einer zuvor abgeschlossenen menschlichen Tätigkeit:*
  zB Sprach-/Stilverbesserung eines bereits verfassten Dokuments.

- *(c) Erkennen von Entscheidungsmustern/Abweichungen ohne Ersatz/Einfluss auf die zuvor abgeschlossenemenschliche Bewertung ohne angemessene menschliche Überprüfung:*
  zB nachträgliche Prüfung eines Benotungsmusters.

- *(d) Vorbereitende Aufgabe für eine spätere Bewertung:*
  zB Dossier-Bearbeitung (Indexierung, Suche, Text-/Sprachverarbeitung, Datenverknüpfung), Übersetzung von Erstdokumenten

Absolute Sperre: Profiling natürlicher Personen ⇒ immer Hochrisiko, auch wenn (a)–(d) vorliegen.

Praxis-Hinweis: In der Ausnahmeprüfung ist beides zu dokumentieren: (i) kein erhebliches Risiko/keine wesentliche Beeinflussung und (ii) mindestens eine der Bedingungen (a)–(d).

E. Nachweispflichten und Registrierung

Wer sich auf die Ausnahme beruft, hat zum Zweck der Transparenz und Nachvollziehbarkeit der Ausnahmenentscheidung folgende Pflichten:

- **Vor Inverkehrbringen/Inbetriebnahme**: Dokumentation der Bewertung
- **Registrierungspflich**t nach Artikel 49 KI-VO Absatz 2.
- **Vorlage der Dokumentation** auf Verlangen der zuständigen nationalen Behörden.

F. Dynamische Anpassung der Ausnahmekriterien

Erweiterung/Änderung der Bedingungen (a)–(d) ist per delegiertem Rechtsakt möglich (siehe dazu Ausführungen zu Artikel 97 KI-VO), wenn verlässliche Belege zeigen, dass bestimmte Anhang-III-Systeme kein erhebliches Risiko bergen. Die Streichung einer Bedingung ist möglich, wenn dies zur Aufrechterhaltung des Schutzniveaus erforderlich ist.

Anpassungen dürfen zuletzt das allgemeine Schutzniveau nicht senken; Kohärenz mit delegierten Rechtsakten sowie Markt- und Technologietrends sind dabei zu berücksichtigen.

G. Beispiele (mit vereinfachter Einordnung)

Industrieroboter-KI als Sicherheitsbauteil mit Drittprüfung	→ **Hochrisiko** (Anhang I KI-VO)
Diagnose-KI als Medizinprodukt mit Drittprüfung	→ **Hochrisiko** (**Anhang I KI-VO**)
Bonitäts-KI für Privatpersonen	→ **Hochrisiko** (Anhang III KI-VO)
Biometrische Fernidentifizierung im öffentlichen Raum	→ **Hochrisiko** (Anhang III KI-VO)
Biometrische Verifizierung nur zum Entsperren eines Geräts/Zutritt	→ **nicht Hochrisiko**

Notruf-Triage-KI (Priorisierung von Einsätzen)	→ **Hochrisiko** (Anhang III KI-VO)
Richterliche Unterstützung bei Auslegung/Anwendung des Rechts	→ **Hochrisiko** (Anhang III KI-VO)
Dokumenten-Klassifizierung zur Posteingangssteuerung	→ **Ausnahme möglich** (lit a)
Sprach-/Stil-Optimierung eines bereits verfassten Antrags	→ **Ausnahme möglich** (lit b)
Musterabweichungs-Prüfer für Benotungen	→ **Ausnahme möglich** (lit b)
Dossier-Indexierung/Übersetzung als Vorarbeit	→ **Ausnahme möglich** (lit d)

III. Zusammenfassung

Klassifizierung nach Produktrecht	KI ist Sicherheitsbauteil/Produkt nach Anhang I KI-VO und Dritt-Konformitätsbewertung erforderlich
Klassifizierung nach Anwendungsfeld	KI-Systeme in Anhang III KI-VO
Ausnahmen	Kein erhebliches Risiko und mindestens eine Bedingung (a)–(d)

IV. Quellenverzeichnis

- Erwägungsgründe 26, 46-62 KI-VO (EU) 2024/1689

Artikel 7 KI-VO

Änderungen des Anhangs III

(1) Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zur Änderung von Anhang III durch Hinzufügung oder Änderung von Anwendungsfällen für Hochrisiko-KI-Systeme zu erlassen, die beide der folgenden Bedingungen erfüllen:

a) Die KI-Systeme sollen in einem der in Anhang III aufgeführten Bereiche eingesetzt werden;

b) die KI-Systeme bergen ein Risiko der Schädigung in Bezug auf die Gesundheit und Sicherheit oder haben nachteilige Auswirkungen auf die Grundrechte und dieses Risiko gleicht dem Risiko der Schädigung oder den nachteiligen Auswirkungen, das bzw. die von den in Anhang III bereits genannten Hochrisiko-KI-Systemen ausgeht bzw. ausgehen, oder übersteigt diese.

(2) Bei der Bewertung der Bedingung gemäß Absatz 1 Buchstabe b berücksichtigt die Kommission folgende Kriterien:

a) die Zweckbestimmung des KI-Systems;

b) das Ausmaß, in dem ein KI-System verwendet wird oder voraussichtlich verwendet werden wird;

c) die Artikel und den Umfang der vom KI-System verarbeiteten und verwendeten Daten, insbesondere die Frage, ob besondere Kategorien personenbezogener Daten verarbeitet werden;

d) das Ausmaß, in dem das KI-System autonom handelt, und die Möglichkeit, dass ein Mensch eine Entscheidung oder Empfehlungen, die zu einem potenziellen Schaden führen können, außer Kraft setzt;

e) das Ausmaß, in dem durch die Verwendung eines KI-Systems schon die Gesundheit und Sicherheit geschädigt wurden, es nachteilige Auswirkungen auf die Grundrechte gab oder zB nach Berichten oder dokumentierten Behauptungen, die den zuständigen nationalen Behörden übermittelt werden, oder gegebenenfalls anderen Berichten Anlass zu erheblichen Bedenken hinsichtlich der Wahrscheinlichkeit eines solchen Schadens oder solcher nachteiligen Auswirkungen besteht;

f) das potenzielle Ausmaß solcher Schäden oder nachteiligen Auswirkungen, insbesondere hinsichtlich ihrer Intensität und ihrer Eignung, mehrere

Personen zu beeinträchtigen oder eine bestimmte Gruppe von Personen unverhältnismäßig stark zu beeinträchtigen;

g)das Ausmaß, in dem Personen, die potenziell geschädigt oder negative Auswirkungen erleiden werden, von dem von einem KI-System hervorgebrachten Ergebnis abhängen, weil es insbesondere aus praktischen oder rechtlichen Gründen nach vernünftigem Ermessen unmöglich ist, sich diesem Ergebnis zu entziehen;

h)das Ausmaß, in dem ein Machtungleichgewicht besteht oder in dem Personen, die potenziell geschädigt oder negative Auswirkungen erleiden werden, gegenüber dem Betreiber eines KI-Systems schutzbedürftig sind, insbesondere aufgrund von Status, Autorität, Wissen, wirtschaftlichen oder sozialen Umständen oder Alter;

i)das Ausmaß, in dem das mithilfe eines KI-Systems hervorgebrachte Ergebnis unter Berücksichtigung der verfügbaren technischen Lösungen für seine Korrektur oder Rückgängigmachung leicht zu korrigieren oder rückgängig zu machen ist, wobei Ergebnisse, die sich auf die Gesundheit, Sicherheit oder Grundrechte von Personen negativ auswirken, nicht als leicht korrigierbar oder rückgängig zu machen gelten;

j)das Ausmaß und die Wahrscheinlichkeit, dass der Einsatz des KI-Systems für Einzelpersonen, Gruppen oder die Gesellschaft im Allgemeinen, einschließlich möglicher Verbesserungen der Produktsicherheit, nützlich ist;

k)das Ausmaß, in dem bestehendes Unionsrecht Folgendes vorsieht:

i)wirksame Abhilfemaßnahmen in Bezug auf die Risiken, die von einem KI-System ausgehen, mit Ausnahme von Schadenersatzansprüchen;

ii)wirksame Maßnahmen zur Vermeidung oder wesentlichen Verringerung dieser Risiken.

(3) Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zur Änderung der Liste in Anhang III zu erlassen, um Hochrisiko-KI-Systeme zu streichen, die beide der folgenden Bedingungen erfüllen:

a)Das betreffende Hochrisiko-KI-System weist unter Berücksichtigung der in Absatz 2 aufgeführten Kriterien keine erheblichen Risiken mehr für die Grundrechte, Gesundheit oder Sicherheit auf;

b)durch die Streichung wird das allgemeine Schutzniveau in Bezug auf Gesundheit, Sicherheit und Grundrechte im Rahmen des Unionsrechts nicht gesenkt.

I. Worum geht es?

Artikel 7 KI-VO regelt, wie und unter welchen Bedingungen die Europäische Kommission die Liste der Hochrisiko-KI-Systeme in Anhang III KI-VO anpassen darf. Ziel ist es, flexibel auf technische Entwicklungen und neue Risiken zu reagieren, ohne das gesamte Gesetz ändern zu müssen.

II. Detailkommentar

A. Anpassung der Liste

Die Kommission darf Anhang III KI-VO nur ändern, wenn **beide Bedingungen** erfüllt sind:

1. Das KI-System wird in einem der in Anhang III genannten Bereiche eingesetzt.
2. Es birgt ein gleich hohes oder höheres Risiko für Gesundheit, Sicherheit oder Grundrechte.

Diese Einschränkung soll verhindern, dass völlig neue Einsatzbereiche ohne klare gesetzliche Grundlage aufgenommen werden.

B. Kriterien für die Risikobewertung

Die Bewertung erfolgt anhand eines Kriterienkatalogs. Wichtige Faktoren sind:

- **Zweckbestimmung** und erwartete Verbreitung.
- **Artikel der verarbeiteten Daten** (zB sensible personenbezogene Daten).
- **Autonomiegrad** des Systems und Eingriffsmöglichkeiten durch Menschen.
- Bisherige oder zu erwartende **Schadensfälle**.
- **Schwere** und **Reichweite** möglicher Schäden.
- **Abhängigkeit** der Betroffenen vom Ergebnis.

- **Machtungleichgewicht** zwischen Anbieter und Betroffenen.
- **Korrigierbarkeit** von fehlerhaften Ergebnissen.
- **Gesamt-Nutzen** für Gesellschaft und Sicherheit.
- Vorhandensein von **bestehenden EU-Schutzmechanismen**.

Beispiel: *Eine KI für die automatische Kreditbewertung, die sensible Finanz- und Gesundheitsdaten nutzt und stark autonom entscheidet, könnte aufgrund hoher Eingriffsintensität und mangelnder Korrigierbarkeit nachträglich als Hochrisiko eingestuft werden.*

C. Streichung von Einträgen

Eine Streichung ist nur möglich, wenn:

1. kein erhebliches Risiko mehr besteht (unter Berücksichtigung des Kriterienkatalogs);
2. das Schutzniveau in der EU erhalten bleibt.

Beispiel: *Eine KI-Anwendung im Bildungsbereich könnte gestrichen werden, wenn technische Änderungen und ergänzende gesetzliche Regelungen das Risiko deutlich verringert haben.*

D. Besonderheiten

- **Delegierte Rechtsakte**: Änderungen erfolgen nicht durch das Parlament oder den Rat, sondern durch die Kommission im vereinfachten Verfahren (siehe dazu Ausführungen zu Artikel 97 KI-VO).
- **Flexibilität vs Rechtssicherheit**: Das Verfahren ermöglicht schnelle Anpassungen, birgt aber das Risiko häufiger Änderungen, die Unternehmen beobachten müssen.

III. Zusammenfassung

Thema	Erweiterung	Streichung
Voraussetzungen	a) Einsatzbereich in Anhang III KI-VO	a) Kein erhebliches Risiko mehr

	b) Gleiches oder höheres Risiko	b) Schutzniveau bleibt gleich
Bewertungskriterien	Siehe oben	Siehe oben
Verfahren	Delegierter Rechtsakt nach Artikel 97 KI-VO	Delegierter Rechtsakt nach Artikel 97 KI-VO

IV. Quellenverzeichnis

- Erwägungsgründe 49, 52 KI-VO (EU) 2024/1689

Artikel 8 KI-VO

Einhaltung der Anforderungen

(1) Hochrisiko-KI-Systeme müssen die in diesem Abschnitt festgelegten Anforderungen erfüllen, wobei ihrer Zweckbestimmung sowie dem allgemein anerkannten Stand der Technik in Bezug auf KI und KI-bezogene Technologien Rechnung zu tragen ist. Bei der Gewährleistung der Einhaltung dieser Anforderungen wird dem in Artikel 9 genannten Risikomanagementsystem Rechnung getragen.

(2) Enthält ein Produkt ein KI-System, für das die Anforderungen dieser Verordnung und die Anforderungen der in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union gelten, so sind die Anbieter dafür verantwortlich, sicherzustellen, dass ihr Produkt alle geltenden Anforderungen der geltenden Harmonisierungsrechtsvorschriften der Union vollständig erfüllt. Bei der Gewährleistung der Erfüllung der in diesem Abschnitt festgelegten Anforderungen durch die in Absatz 1 genannten Hochrisiko-KI-Systeme und im Hinblick auf die Gewährleistung der Kohärenz, der Vermeidung von Doppelarbeit und der Minimierung zusätzlicher Belastungen haben die Anbieter die Wahl, die erforderlichen Test- und Berichterstattungsverfahren, Informationen und Dokumentationen, die sie im Zusammenhang mit ihrem Produkt bereitstellen, gegebenenfalls in Dokumentationen und Verfahren zu integrieren, die bereits bestehen und gemäß den in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union vorgeschrieben sind.

I. Worum geht es?

Artikel 8 KI-VO legt fest, dass Hochrisiko-KI-Systeme die im Abschnitt II (Artikel 8-15) der Verordnung genannten verbindlichen Anforderungen erfüllen müssen. Dabei sind sowohl die Zweckbestimmung des Systems als auch der allgemein anerkannte Stand der Technik zu berücksichtigen. Außerdem müssen Anbieter die Vorgaben mit einem Risikomanagementsystem (Artikel 9 KI-VO) absichern.

II. Detailkommentar

A. Einhaltung der Anforderungen nach Stand der Technik

„Stand der Technik“: die nachweislich erprobten und anerkannten technischen Verfahren, die in der Fachwelt für vergleichbare Anwendungen üblich sind.

Es handelt sich nicht zwingend um den modernsten Stand, sondern um den sicher etablierten Stand, der den aktuellen wissenschaftlichen und praktischen Konsens widerspiegelt. Der Stand der Technik entwickelt sich dynamisch – Anbieter müssen also kontinuierlich prüfen, ob ihre Systeme noch entsprechen.

Beispiel: *Ein Hersteller von Diagnostik-KI muss sicherstellen, dass seine Bildauswertungsalgorithmen nicht nur bei Markteinführung, sondern auch später den allgemein anerkannten Verfahren für Genauigkeit, Bias-Minimierung und Datensicherheit entsprechen.*

B. Rolle des Risikomanagementsystems

Artikel 8 verweist ausdrücklich auf Artikel 9 KI-VO: Die Einhaltung der Anforderungen erfolgt unter Berücksichtigung des Risikomanagementsystems, wodurch Anforderungen wie Datengovernance, Transparenz oder Cybersicherheit in den gesamten Lebenszyklus der KI integriert und umgesetzt werden müssen.

C. Zusammenspiel mit anderen Harmonisierungsrechtsvorschriften

- **Grundsatz**: Mehrere EU-Rechtsakte können parallel gelten.
- **Pflicht**: Anbieter müssen sämtliche Anforderungen aller anwendbaren Rechtsakte einhalten (keine Teilkonformität möglich).

- **Flexibilität**: Anbieter können Prüfverfahren, Berichte und Dokumentation zusammenführen, um Aufwand zu reduzieren – solange alle Pflichten erfüllt werden.
- **Keine automatische Rechtmäßigkeit**: Auch wenn ein KI-System die KI-VO erfüllt, bedeutet das nicht automatisch, dass es nach anderen Gesetzen zulässig ist.

Beispiel: *Ein KI-gesteuertes Medizinprodukt muss den Sicherheits- und Leistungsanforderungen der Medizinprodukte-VO sowie den Hochrisiko-KI-Anforderungen der KI-VO entsprechen. Testberichte zur Datensicherheit können ggf beide Pflichten abdecken.*

III. Zusammenfassung

Zweckbestimmung	Anforderungen müssen sich am vorgesehenen Einsatz orientieren
Stand der Technik	Aktueller, anerkannter technischer Standard, regelmäßig zu prüfen
Risikomanagement	Integrierte Umsetzung aller Anforderungen im Systemlebenszyklus
Mehrere Rechtsakte	Alle anwendbaren EU-Vorgaben müssen vollständig erfüllt werden
Flexibilität	Prüf- und Dokumentationsverfahren dürfen kombiniert werden
Kein Freibrief	KI-VO-Konformität bedeutet nicht automatisch Rechtmäßigkeit in anderen Rechtsbereichen

IV. Quellenverzeichnis

- Erwägungsgründe 63, 64, 69 KI-VO (EU) 2024/1689

Artikel 9 KI-VO

Risikomanagementsystem

(1) Für Hochrisiko-KI-Systeme wird ein Risikomanagementsystem eingerichtet, angewandt, dokumentiert und aufrechterhalten.

(2) Das Risikomanagementsystem versteht sich als ein kontinuierlicher iterativer Prozess, der während des gesamten Lebenszyklus eines Hochrisiko-KI-Systems geplant und durchgeführt wird und eine regelmäßige systematische Überprüfung und Aktualisierung erfordert. Es umfasst folgende Schritte:

a) die Ermittlung und Analyse der bekannten und vernünftigerweise vorhersehbaren Risiken, die vom Hochrisiko-KI-System für die Gesundheit, Sicherheit oder Grundrechte ausgehen können, wenn es entsprechend seiner Zweckbestimmung verwendet wird;

b) die Abschätzung und Bewertung der Risiken, die entstehen können, wenn das Hochrisiko-KI-System entsprechend seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird;

c) die Bewertung anderer möglicherweise auftretender Risiken auf der Grundlage der Auswertung der Daten aus dem in Artikel 72 genannten System zur Beobachtung nach dem Inverkehrbringen;

d) die Ergreifung geeigneter und gezielter Risikomanagementmaßnahmen zur Bewältigung der gemäß Buchstabe a ermittelten Risiken.

(3) Die in diesem Artikel genannten Risiken betreffen nur solche Risiken, die durch die Entwicklung oder Konzeption des Hochrisiko-KI-Systems oder durch die Bereitstellung ausreichender technischer Informationen angemessen gemindert oder behoben werden können.

(4) Bei den in Absatz 2 Buchstabe d genannten Risikomanagementmaßnahmen werden die Auswirkungen und möglichen Wechselwirkungen, die sich aus der kombinierten Anwendung der Anforderungen dieses Abschnitts ergeben, gebührend berücksichtigt, um die Risiken wirksamer zu minimieren und gleichzeitig ein angemessenes Gleichgewicht bei der Durchführung der Maßnahmen zur Erfüllung dieser Anforderungen sicherzustellen.

(5) Die in Absatz 2 Buchstabe d genannten Risikomanagementmaßnahmen werden so gestaltet, dass jedes mit einer bestimmten Gefahr verbundene relevante Restrisiko sowie das Gesamtrestrisiko der Hochrisiko-KI-Systeme als vertretbar beurteilt wird.

Bei der Festlegung der am besten geeigneten Risikomanagementmaßnahmen ist Folgendes sicherzustellen:

a) soweit technisch möglich, Beseitigung oder Verringerung der gemäß Absatz 2 ermittelten und bewerteten Risiken durch eine geeignete Konzeption und Entwicklung des Hochrisiko-KI-Systems;

b) gegebenenfalls Anwendung angemessener Minderungs- und Kontrollmaßnahmen zur Bewältigung nicht auszuschließender Risiken;

c) Bereitstellung der gemäß Artikel 13 erforderlichen Informationen und gegebenenfalls entsprechende Schulung der Betreiber.

Zur Beseitigung oder Verringerung der Risiken im Zusammenhang mit der Verwendung des Hochrisiko-KI-Systems werden die technischen Kenntnisse, die Erfahrungen und der Bildungsstand, die vom Betreiber erwartet werden können, sowie der voraussichtliche Kontext, in dem das System eingesetzt werden soll, gebührend berücksichtigt.

(6) Hochrisiko-KI-Systeme müssen getestet werden, um die am besten geeigneten gezielten Risikomanagementmaßnahmen zu ermitteln. Durch das Testen wird sichergestellt, dass Hochrisiko-KI-Systeme stets im Einklang mit ihrer Zweckbestimmung funktionieren und die Anforderungen dieses Abschnitts erfüllen.

(7) Die Testverfahren können einen Test unter Realbedingungen gemäß Artikel 60 umfassen.

(8) Das Testen von Hochrisiko-KI-Systemen erfolgt zu jedem geeigneten Zeitpunkt während des gesamten Entwicklungsprozesses und in jedem Fall vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme. Das Testen erfolgt anhand vorab festgelegter Metriken und Wahrscheinlichkeitsschwellenwerte, die für die Zweckbestimmung des Hochrisiko-KI-Systems geeignet sind.

(9) Bei der Umsetzung des in den Absätzen 1 bis 7 vorgesehenen Risikomanagementsystems berücksichtigen die Anbieter, ob angesichts seiner Zweckbestimmung das Hochrisiko-KI-System wahrscheinlich

nachteilige Auswirkungen auf Personen unter 18 Jahren oder gegebenenfalls andere schutzbedürftige Gruppen haben wird.

(10) Bei Anbietern von Hochrisiko-KI-Systemen, die den Anforderungen an interne Risikomanagementprozesse gemäß anderen einschlägigen Bestimmungen des Unionsrechts unterliegen, können die in den Absätzen 1 bis 9 enthaltenen Aspekte Bestandteil der nach diesem Recht festgelegten Risikomanagementverfahren sein oder mit diesen Verfahren kombiniert werden.

I. Worum geht es?

Artikel 9 KI-VO verpflichtet Anbieter von Hochrisiko-KI-Systemen, ein Risikomanagementsystem einzurichten, zu betreiben, zu dokumentieren und fortlaufend zu aktualisieren. Ziel ist es, Risiken für Gesundheit, Sicherheit und Grundrechte während des gesamten Lebenszyklus eines Systems zu erkennen, zu bewerten und zu mindern. Das System ist als kontinuierlicher, aufbauender Prozess ausgestaltet.

II. Detailkommentar

A. Adressaten und Pflichten

1. Wer muss handeln?

Anbieter von Hochrisiko-KI-Systemen sind direkt verpflichtet.

Betreiber profitieren von den Risikomaßnahmen, müssen aber bereitgestellte Informationen (Artikel 13 KI-VO) beachten.

2. Kernpflichten der Anbieter:

- **Einrichtung** eines Risikomanagementsystems vor Marktzugang.
- **Durchführung** während des gesamten Lebenszyklus (inkl Updates und Wartung).
- **Dokumentation** aller wesentlichen Entscheidungen und Maßnahmen.
- **Regelmäßige Überprüfung und Anpassung** auf Basis neuer Erkenntnisse (zB aus Marktbeobachtung nach Artikel 72 KI-VO).

B. Ablauf des Risikomanagementprozesses

Der Prozess umfasst vier Schritte:

1. **Risikoermittlung:** Identifikation aller bekannten und vernünftigerweise vorhersehbaren Risiken (inkl Fehlanwendungen).
2. **Risikobewertung:** Einschätzung der Eintrittswahrscheinlichkeit und Schwere.
3. **Beobachtung nach dem Inverkehrbringen:** Einbeziehung realer Nutzungsdaten zur Erkennung neuer Risiken.
4. **Risikomaßnahmen:** Auswahl geeigneter technischer oder organisatorischer Maßnahmen zur Minderung oder Beseitigung.

C. Anforderungen an Risikomaßnahmen

- **Technische Gestaltung**: Risiken sind soweit möglich durch Designentscheidungen zu vermeiden.
- **Kontroll- und Minderungsmaßnahmen**: Falls Risiken nicht vollständig entfallen, sind Schutzmechanismen einzubauen (zB Warnmeldungen, Not-Aus-Funktionen).
- **Information und Schulung**: Betreiber müssen informiert und ggf geschult werden.
- **Verhältnismäßigkeit**: Risiken und Maßnahmen müssen in einem angemessenen Gleichgewicht stehen.

D. Besonderheiten

- **Schutz besonderer Gruppen:** Zusätzliche Berücksichtigung, wenn nachteilige Auswirkungen auf Minderjährige oder andere schutzbedürftige Gruppen möglich sind.
- **Lebenszyklus-Ansatz**: Risiken werden nicht einmalig, sondern fortlaufend überwacht und angepasst.

- **Realbetriebs-Risiken**: Viele Risiken zeigen sich erst nach Inverkehrbringen; Artikel 9 verknüpft deshalb das Risikomanagement mit der Marktbeobachtungspflicht (Artikel 72 KI-VO).
- **Kritikpunkt:** Die Norm lässt offen, wie mit neu auftretenden Risiken umzugehen ist, wenn diese die Zweckbestimmung grundlegend infrage stellen.

III. Zusammenfassung

Pflicht	**Wer?**	**Wann?**	**Wie?**
Einrichtung eines Risikomanagementsystems	Anbieter	Vor Markteintritt	Prozess festlegen, dokumentieren
Risikoanalyse und -bewertung	Anbieter	Fortlaufend	Identifikation, Bewertung, Beobachtung
Umsetzung von Risikomaßnahmen	Anbieter	Fortlaufend	Technische und organisatorische Maßnahmen
Information und Schulung	Anbieter →Betreiber	Bei Bedarf	Artikel 13 KI-VO beachten

IV. Quellenverzeichnis

- Erwägungsgründe 65, 66 KI-VO (EU) 2024/1689

Artikel 10 KI-VO

Daten und Daten-Governance

(1) Hochrisiko-KI-Systeme, in denen Techniken eingesetzt werden, bei denen KI-Modelle mit Daten trainiert werden, müssen mit Trainings-, Validierungs- und Testdatensätzen entwickelt werden, die den in den Absätzen 2 bis 5 genannten Qualitätskriterien entsprechen, wenn solche Datensätze verwendet werden.

(2) Für Trainings-, Validierungs- und Testdatensätze gelten Daten-Governance- und Datenverwaltungsverfahren, die für die Zweckbestimmung des Hochrisiko-KI-Systems geeignet sind. Diese Verfahren betreffen insbesondere

a) die einschlägigen konzeptionellen Entscheidungen,

b)die Datenerhebungsverfahren und die Herkunft der Daten und im Falle personenbezogener Daten den ursprünglichen Zweck der Datenerhebung,

c)relevante Datenaufbereitungsvorgänge wie Annotation, Kennzeichnung, Bereinigung, Aktualisierung, Anreicherung und Aggregierung,

d)die Aufstellung von Annahmen, insbesondere in Bezug auf die Informationen, die mit den Daten erfasst und dargestellt werden sollen,

e)eine Bewertung der Verfügbarkeit, Menge und Eignung der benötigten Datensätze,

f)eine Untersuchung im Hinblick auf mögliche Verzerrungen (Bias), die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die Grundrechte auswirken oder zu einer nach den Rechtsvorschriften der Union verbotenen Diskriminierung führen könnten, insbesondere wenn die Datenausgaben die Eingaben für künftige Operationen beeinflussen,

g)geeignete Maßnahmen zur Erkennung, Verhinderung und Abschwächung möglicher gemäß Buchstabe f ermittelter Verzerrungen,

h)die Ermittlung relevanter Datenlücken oder Mängel, die der Einhaltung dieser Verordnung entgegenstehen, und wie diese Lücken und Mängel behoben werden können.

(3) Die Trainings-, Validierungs- und Testdatensätze müssen im Hinblick auf die Zweckbestimmung relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sein. Sie müssen die geeigneten

statistischen Merkmale, gegebenenfalls auch bezüglich der Personen oder Personengruppen, für die das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, haben. Diese Merkmale der Datensätze können auf der Ebene einzelner Datensätze oder auf der Ebene einer Kombination davon erfüllt werden.

(4) Die Datensätze müssen, soweit dies für die Zweckbestimmung erforderlich ist, die entsprechenden Merkmale oder Elemente berücksichtigen, die für die besonderen geografischen, kontextuellen, verhaltensbezogenen oder funktionalen Rahmenbedingungen, unter denen das Hochrisiko-KI-System bestimmungsgemäß verwendet werden soll, typisch sind.

(5) Soweit dies für die Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen im Einklang mit Absatz 2 Buchstaben f und g dieses Artikels unbedingt erforderlich ist, dürfen die Anbieter solcher Systeme ausnahmsweise besondere Kategorien personenbezogener Daten verarbeiten, wobei sie angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen müssen. Zusätzlich zu den Bestimmungen der Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680 müssen alle folgenden Bedingungen erfüllt sein, damit eine solche Verarbeitung stattfinden kann:

a) Die Erkennung und Korrektur von Verzerrungen kann durch die Verarbeitung anderer Daten, einschließlich synthetischer oder anonymisierter Daten, nicht effektiv durchgeführt werden;

b) die besonderen Kategorien personenbezogener Daten unterliegen technischen Beschränkungen einer Weiterverwendung der personenbezogenen Daten und modernsten Sicherheits- und Datenschutzmaßnahmen, einschließlich Pseudonymisierung;

c) die besonderen Kategorien personenbezogener Daten unterliegen Maßnahmen, mit denen sichergestellt wird, dass die verarbeiteten personenbezogenen Daten gesichert, geschützt und Gegenstand angemessener Sicherheitsvorkehrungen sind, wozu auch strenge Kontrollen des Zugriffs und seine Dokumentation gehören, um Missbrauch zu verhindern und sicherzustellen, dass nur befugte Personen Zugang zu diesen personenbezogenen Daten mit angemessenen Vertraulichkeitspflichten haben;

d)die besonderen Kategorien personenbezogener Daten werden nicht an Dritte übermittelt oder übertragen, noch haben diese Dritten anderweitigen Zugang zu diesen Daten;

e)die besonderen Kategorien personenbezogener Daten werden gelöscht, sobald die Verzerrung korrigiert wurde oder das Ende der Speicherfrist für die personenbezogenen Daten erreicht ist, je nachdem, was zuerst eintritt;

f)die Aufzeichnungen über Verarbeitungstätigkeiten gemäß den Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680 enthalten die Gründe, warum die Verarbeitung besonderer Kategorien personenbezogener Daten für die Erkennung und Korrektur von Verzerrungen unbedingt erforderlich war und warum dieses Ziel mit der Verarbeitung anderer Daten nicht erreicht werden konnte.

(6) Bei der Entwicklung von Hochrisiko-KI-Systemen, in denen keine Techniken eingesetzt werden, bei denen KI-Modelle trainiert werden, gelten die Absätze 2 bis 5 nur für Testdatensätze.

I. Worum geht es?

Artikel 10 KI-VO regelt **Qualität, Herkunft und Verarbeitung von Daten** für Hochrisiko-KI-Systeme. Er legt fest, dass Trainings-, Validierungs- und Testdatensätze bestimmten Qualitätskriterien entsprechen und durch geeignete Daten-Governance- und Verwaltungsverfahren abgesichert werden müssen. Ziel ist es, Funktionsfähigkeit und Sicherheit der Systeme zu gewährleisten, Diskriminierung zu verhindern und Rechtskonformität (insbesondere Datenschutz) sicherzustellen.

II. Detailkommentar

A. Was ist konkret erfasst?

Artikel 10 gilt zunächst für alle Hochrisiko-KI-Systeme, die mit trainierten KI-Modellen arbeiten. Dies betrifft alle Phasen der Modellentwicklung (Training, Validierung, Test).

B. Daten-Governance- und Verwaltungsverfahren

Diese Verfahren stellen sicher, dass Datensätze geeignet, nachvollziehbar und unverzerrt sind. Sie umfassen:

- **Konzeptionelle Entscheidungen** (zB welche Variablen werden erfasst?)
- **Datenerhebung und Herkunft** (inkl Dokumentation des Erhebungszwecks bei personenbezogenen Daten)
- **Datenaufbereitung** (Annotation, Bereinigung, Aktualisierung)
- **Annahmen** (zB Auswahl bestimmter Messwerte)
- **Verfügbarkeit und Eignung** der Datensätze
- **Bias-Analyse** und Gegenmaßnahmen
- **Erkennung von Datenlücken** und Strategien zu deren Schließung

Beispiel: *Bei einem KI-gestützten System zur Prüfung von Bewerbungen im öffentlichen Dienst muss dokumentiert werden, aus welchen Quellen die Bewerbungs- und Testdaten stammen, wie sie standardisiert werden, und wie sichergestellt wird, dass keine unzulässigen Benachteiligungen aufgrund von Geschlecht, Alter oder Herkunft entstehen.*

C. Qualitätskriterien der Datensätze

- **Relevanz**: Daten müssen zum Verwendungszweck passen.
- **Repräsentativität**: Abbildung der realen Zielpopulation.
- **Fehlerfreiheit und Vollständigkeit**: So weit wie möglich, ohne Datenschutztechniken zu beeinträchtigen. Hier ist insbesondere die Vermeidung von Rückkoppelungseffekten zu beachten; verzerrte Ausgaben führen zu noch verzerrteren Eingaben bei künftigen Anwendungen.
- **Statistische Merkmale**: zB Altersverteilung der Nutzergruppe.
- **Kontextbezug**: Anpassung an geografische, verhaltensbezogene oder funktionale Besonderheiten.

Beispiel: *Ein KI-System zur Entscheidung über den Zugang zu beruflicher Weiterbildung für Arbeitslose muss Trainingsdaten enthalten, die Bewerberprofile aus allen relevanten Regionen und Altersgruppen abbilden, um faire Ergebnisse sicherzustellen.*

D. Verarbeitung personenbezogener Daten

- **Grundsatz**: Nur ausnahmsweise zulässig, wenn es zur Bias-Korrektur unbedingt erforderlich.
- **Bedingungen:**
  1. Keine gleichwertige Alternative (zB synthetische Daten) möglich
  2. Technische Beschränkungen und modernste Datenschutzmaßnahmen
  3. Zugriffskontrolle und Dokumentation
  4. Kein Zugriff durch Dritte
  5. Löschung nach Zweckerreichung
  6. Dokumentation der Notwendigkeit

Beispiel: *Ein Algorithmus für Jobempfehlungen zeigt ungleiche Behandlung nach ethnischer Zugehörigkeit. Zur Korrektur werden temporär entsprechende Daten verarbeitet, um Diskriminierung zu erkennen und zu beheben.*

E. Besonderheiten

- Compliance-Dienste (von Drittanbietern) dürfen eingebunden werden.
- Für Systeme ohne Training gelten die Anforderungen nur für Testdatensätze.

III. Zusammenfassung

Ziel	Sicherstellung qualitativ hochwertiger, sicherer und unverzerrter Daten für Hochrisiko-KI
Pflichten	Daten-Governance, Bias-Prüfung, Dokumentation, Kontextbezug

Qualität	Relevant, repräsentativ, fehlerfrei, vollständig
Besondere Daten	Nur ausnahmsweise, mit strengen Datenschutzauflagen
Unterstützung	Zugriff auf europäische Datenräume möglich

IV. Quellenverzeichnis

- Erwägungsgründe 67, 68, 70 KI-VO (EU) 2024/1689

Artikel 11 KI-VO

Technische Dokumentation

(1) Die technische Dokumentation eines Hochrisiko-KI-Systems wird erstellt, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird, und ist auf dem neuesten Stand zu halten.

Die technische Dokumentation wird so erstellt, dass aus ihr der Nachweis hervorgeht, wie das Hochrisiko-KI-System die Anforderungen dieses Abschnitts erfüllt, und dass den zuständigen nationalen Behörden und den notifizierten Stellen die Informationen in klarer und verständlicher Form zur Verfügung stehen, die erforderlich sind, um zu beurteilen, ob das KI-System diese Anforderungen erfüllt. Sie enthält zumindest die in Anhang IV genannten Angaben. KMU, einschließlich Start-up-Unternehmen, können die in Anhang IV aufgeführten Elemente der technischen Dokumentation in vereinfachter Weise bereitstellen. Zu diesem Zweck erstellt die Kommission ein vereinfachtes Formular für die technische Dokumentation, das auf die Bedürfnisse von kleinen Unternehmen und Kleinstunternehmen zugeschnitten ist. Entscheidet sich ein KMU, einschließlich Start-up-Unternehmen, für eine vereinfachte Bereitstellung der in Anhang IV vorgeschriebenen Angaben, so verwendet es das in diesem Absatz genannte Formular. Die notifizierten Stellen akzeptieren das Formular für die Zwecke der Konformitätsbewertung.

(2) Wird ein Hochrisiko-KI-System, das mit einem Produkt verbunden ist, das unter die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union fällt, in Verkehr gebracht oder in Betrieb genommen, so wird eine einzige technische Dokumentation erstellt, die alle in Absatz 1 genannten Informationen sowie die nach diesen Rechtsakten erforderlichen Informationen enthält.

(3) Die Kommission ist befugt, wenn dies nötig ist, gemäß Artikel 97 delegierte Rechtsakte zur Änderung des Anhangs IV zu erlassen, damit die technische Dokumentation in Anbetracht des technischen Fortschritts stets alle Informationen enthält, die erforderlich sind, um zu beurteilen, ob das System die Anforderungen dieses Abschnitts erfüllt.

I. Worum geht es?

Artikel 11 KI-VO legt fest, dass für jedes Hochrisiko-KI-System eine technische Dokumentation erstellt und aktuell gehalten werden muss. Diese Dokumentation ist der zentrale Nachweis, dass das KI-System alle gesetzlichen Anforderungen erfüllt. Sie dient gleichzeitig als Informationsquelle für Behörden und notifizierte Stellen, um die Konformität zu prüfen.

II. Detailkommentar

A. Verpflichtung zur Erstellung und Aktualisierung

- **Zeitpunkt**: Die Dokumentation muss vor dem Inverkehrbringen oder der Inbetriebnahme vorliegen.
- **Pflicht zur Aktualisierung**: Sie ist während der gesamten Lebensdauer des Systems aktuell zu halten.
- **Zweck**: Ermöglicht den Nachweis der Erfüllung der Anforderungen des Abschnitts (insbesondere der Sicherheits- und Transparenzpflichten).

B. Mindestinhalt

Anhang IV legt fest, welche Angaben enthalten sein müssen – etwa Systembeschreibung, Datenquellen, Risikomanagementverfahren, Testergebnisse (siehe dazu Ausführungen zu Anhang IV KI-VO). Folgendes hat die Dokumentation jedenfalls zu beinhalten:

- Allgemeine Merkmale, Fähigkeiten und Grenzen
- Algorithmen, Daten und Testverfahren
- Risikomanagementsystem
- Ereignisprotokollierung (Logging)

C. Erleichterung für KMU und Start-ups

KMU können eine vereinfachte Dokumentation abgeben, wobei die Kommission hierfür ein angepasstes Formular bereitstellt. Bei Nutzung der vereinfachten Variante muss zwingend dieses Formular verwendet werden.

D. Integration in bestehende Produktdokumentationen

Wenn das KI-System Teil eines Produkts ist, das bereits unter EU-Harmonisierungsrechtsvorschriften iSd Anhang I Abschnitt A fällt (siehe dazu Ausführungen zu Anhang I KI-VO), wird eine kombinierte technische Dokumentation erstellt. Dies dient der Vermeidung von Doppelarbeit und widersprüchlichen Angaben.

E. Anpassung an den technischen Fortschritt

Die Kommission kann den Anhang IV KI-VO per delegiertem Rechtsakt ändern (siehe dazu Ausführungen zu Artikel 97 KI-VO), um den Stand der Technik zu berücksichtigen. Hersteller müssen bei einer Anpassung ihre Dokumentation ggf aktualisieren.

III. Zusammenfassung

Pflicht	Vor Inverkehrbringen/Inbetriebnahme erstellen, laufend aktualisieren
Zweck	Nachweis der Erfüllung aller Anforderungen, Grundlage für Behördenprüfung
Inhalt	Mindestens Angaben gemäß Anhang IV KI-VO, klar und verständlich
KMU-Regelung	Vereinfachtes Formular möglich
Integration	Bei Kombinationsprodukten nur eine gemeinsame Dokumentation
Anpassung	Kommission kann Anhang IV per delegierter Rechtsakte ändern

IV. Quellenverzeichnis

- Erwägungsgrund 71 KI-VO (EU) 2024/1689

Artikel 12 KI-VO

Aufzeichnungspflichten

(1) Die Technik der Hochrisiko-KI-Systeme muss die automatische Aufzeichnung von Ereignissen (im Folgenden „Protokollierung") während des Lebenszyklus des Systems ermöglichen.

(2) Zur Gewährleistung, dass das Funktionieren des Hochrisiko-KI-Systems in einem der Zweckbestimmung des Systems angemessenen Maße rückverfolgbar ist, ermöglichen die Protokollierungsfunktionen die Aufzeichnung von Ereignissen, die für Folgendes relevant sind:

a) die Ermittlung von Situationen, die dazu führen können, dass das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 79 Absatz 1 birgt oder dass es zu einer wesentlichen Änderung kommt,

b) die Erleichterung der Beobachtung nach dem Inverkehrbringen gemäß Artikel 72 und

c) die Überwachung des Betriebs der Hochrisiko-KI-Systeme gemäß Artikel 26 Absatz 5.

(3) Die Protokollierungsfunktionen der in Anhang III Nummer 1 Buchstabe a genannten Hochrisiko-KI-Systeme müssen zumindest Folgendes umfassen:

a) Aufzeichnung jedes Zeitraums der Verwendung des Systems (Datum und Uhrzeit des Beginns und des Endes jeder Verwendung);

b) die Referenzdatenbank, mit der das System die Eingabedaten abgleicht;

c) die Eingabedaten, mit denen die Abfrage zu einer Übereinstimmung geführt hat;

d) die Identität der gemäß Artikel 14 Absatz 5 an der Überprüfung der Ergebnisse beteiligten natürlichen Personen.

I. Worum geht es?

Artikel 12 KI-VO verpflichtet Anbieter von Hochrisiko-KI-Systemen dazu, eine automatische Aufzeichnung relevanter Ereignisse (Protokollierung) über den gesamten Lebenszyklus des Systems hinweg zu ermöglichen. Ziel ist es, das Funktionieren des Systems rückverfolgbar zu machen, Risiken

frühzeitig zu erkennen, den Betrieb zu überwachen und die Beobachtung nach dem Inverkehrbringen zu erleichtern.

II. Detailkommentar

A. Verpflichtung zur Protokollierung

- **Zeitraum:** Über den gesamten Lebenszyklus des Systems.
- **Bedeutung:** Diese Pflicht ist technisch umzusetzen (zB Logging-Mechanismen), nicht nur organisatorisch.
- **Zweck:** Risikoidentifikation, Beobachtung nach Inverkehrbringen (vgl Artikel 72 KI-VO), und Betriebsüberwachung (vgl Artikel 26 KI-VO Absatz 5)

Beispiel: *Ein KI-gestütztes Medizin-Diagnosesystem speichert automatisch jede durchgeführte Analyse samt Zeitpunkt und Ergebnis, ohne dass das medizinische Personal dies manuell auslösen muss.*

B. Zusätzliche Mindestanforderungen

Für die in Anhang III KI-VO Z 1 lit a genannten Hochrisiko-KI-Systeme – also biometrische Fernidentifizierungssysteme – gilt zumindest folgendes zu protokollieren:

- **Nutzungszeiträume**: Beginn und Ende jeder Nutzung
- **Referenzdatenbank**: Quelle, mit der Eingabedaten abgeglichen werden
- **Eingabedaten mit Treffer**: Konkrete Daten, die zu einer Übereinstimmung geführt haben
- **Prüfende Personen**: Identität der Personen, welche die Ergebnisse überprüft haben.

Beispiel: *Ein Gesichtserkennungssystem an einem Flughafen speichert für jede Identifikationsabfrage, wann sie erfolgte, welche Bilddaten genutzt wurden, auf welche Datenbank zugegriffen wurde und welcher Sicherheitsmitarbeiter das Ergebnis verifiziert hat.*

III. Zusammenfassung

Pflicht	Automatische Aufzeichnung relevanter Ereignisse über gesamten Lebenszyklus
Zweck	Risikoerkennung, Markt- und Betriebsüberwachung
Besondere Systeme	Zusätzliche Pflichtangaben für biometrische Identifizierungssysteme
Verhältnis zu Artikel 11 KI-VO	Artikel 11 = statische Dokumentation, Artikel 12 = laufende Ereignisaufzeichnung

IV. Quellenverzeichnis

- Erwägungsgrund 71 KI-VO (EU) 2024/1689

Artikel 13 KI-VO

Transparenz und Bereitstellung von Informationen für die Betreiber

(1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass ihr Betrieb hinreichend transparent ist, damit die Betreiber die Ausgaben eines Systems angemessen interpretieren und verwenden können. Die Transparenz wird auf eine geeignete Artikel und in einem angemessenen Maß gewährleistet, damit die Anbieter und Betreiber ihre in Abschnitt 3 festgelegten einschlägigen Pflichten erfüllen können.

(2) Hochrisiko-KI-Systeme werden mit Betriebsanleitungen in einem geeigneten digitalen Format bereitgestellt oder auf andere Weise mit Betriebsanleitungen versehen, die präzise, vollständige, korrekte und eindeutige Informationen in einer für die Betreiber relevanten, barrierefrei zugänglichen und verständlichen Form enthalten.

(3) Die Betriebsanleitungen enthalten mindestens folgende Informationen:

a) den Namen und die Kontaktangaben des Anbieters sowie gegebenenfalls seines Bevollmächtigten;

b) die Merkmale, Fähigkeiten und Leistungsgrenzen des Hochrisiko-KI-Systems, einschließlich

i) seiner Zweckbestimmung,

ii) des Maßes an Genauigkeit — einschließlich diesbezüglicher Metriken —, Robustheit und Cybersicherheit gemäß Artikel 15, für das das Hochrisiko-KI-System getestet und validiert wurde und das zu erwarten ist, sowie aller bekannten und vorhersehbaren Umstände, die sich auf das erwartete Maß an Genauigkeit, Robustheit und Cybersicherheit auswirken können;

iii) aller bekannten oder vorhersehbaren Umstände bezüglich der Verwendung des Hochrisiko-KI-Systems im Einklang mit seiner Zweckbestimmung oder einer vernünftigerweise vorhersehbaren Fehlanwendung, die zu den in Artikel 9 Absatz 2 genannten Risiken für die Gesundheit und Sicherheit oder die Grundrechte führen können,

iv) gegebenenfalls der technischen Fähigkeiten und Merkmale des Hochrisiko-KI-Systems, um Informationen bereitzustellen, die zur Erläuterung seiner Ausgaben relevant sind;

v)gegebenenfalls seiner Leistung in Bezug auf bestimmte Personen oder Personengruppen, auf die das System bestimmungsgemäß angewandt werden soll;

vi)gegebenenfalls der Spezifikationen für die Eingabedaten oder sonstiger relevanter Informationen über die verwendeten Trainings-, Validierungs- und Testdatensätze, unter Berücksichtigung der Zweckbestimmung des Hochrisiko-KI-Systems;

vii)gegebenenfalls Informationen, die es den Betreibern ermöglichen, die Ausgabe des Hochrisiko-KI-Systems zu interpretieren und es angemessen zu nutzen;

c)etwaige Änderungen des Hochrisiko-KI-Systems und seiner Leistung, die der Anbieter zum Zeitpunkt der ersten Konformitätsbewertung vorab bestimmt hat;

d)die in Artikel 14 genannten Maßnahmen zur Gewährleistung der menschlichen Aufsicht, einschließlich der technischen Maßnahmen, die getroffen wurden, um den Betreibern die Interpretation der Ausgaben von Hochrisiko-KI-Systemen zu erleichtern;

e)die erforderlichen Rechen- und Hardware-Ressourcen, die erwartete Lebensdauer des Hochrisiko-KI-Systems und alle erforderlichen Wartungs- und Pflegemaßnahmen einschließlich deren Häufigkeit zur Gewährleistung des ordnungsgemäßen Funktionierens dieses KI-Systems, auch in Bezug auf Software-Updates;

f)gegebenenfalls eine Beschreibung der in das Hochrisiko-KI-System integrierten Mechanismen, die es den Betreibern ermöglicht, die Protokolle im Einklang mit Artikel 12 ordnungsgemäß zu erfassen, zu speichern und auszuwerten.

I. Worum geht es?

Artikel 13 KI-VO verpflichtet Anbieter von Hochrisiko-KI-Systemen, diese so zu gestalten und zu dokumentieren, dass Betreiber sie verstehen, angemessen interpretieren und sicher nutzen können. Kerninstrument ist die Transparenz - sowohl durch technische Gestaltung als auch durch Betriebsanleitungen mit klaren, vollständigen und barrierefreien

Informationen. Die Vorschrift soll die Pflichterfüllung der Betreiber ermöglichen und Risiken aus falscher Anwendung minimieren.

II. Detailkommentar

A. Transparenzpflicht bei der Systemgestaltung

- **Technisches Ziel:** Systeme müssen so konzipiert sein, dass der Betrieb hinreichend transparent ist und Funktionsweise, Stärken sowie Grenzen zu verstehen sind.
- **Zweck:** Betreiber müssen die Ausgaben (Ergebnisse) richtig deuten und sachgerecht verwenden können.
- **Maß der Transparenz:** Muss so bemessen sein, dass Anbieter und Betreiber Funktionsweise und Grenzen nachvollziehen, Risiken erkennen und ihre Pflichten erfüllen können.

B. Betriebsanleitungen

- **Form**: Digital oder auf anderem geeignetem Weg; barrierefrei zugänglich.
- **Anforderungen an den Inhalt**: Präzise, vollständig, korrekt, eindeutig. Informationen müssen zudem auf die Zielgruppe zugeschnitten sein.
- **Gestaltungshinweis:** Infos sollen anschauliche Beispiele enthalten, lesbar und barrierefrei sein, Sprache nach Mitgliedstaatvorgabe.

C. Mindestinhalte der Betriebsanleitung

Die Betriebsanleitungen müssen mindestens enthalten:

1. **Anbieteridentifikation**: Name, Kontakt, ggf Bevollmächtigter.
2. **Systemmerkmale**: Zweckbestimmung, Fähigkeiten, Grenzen.
3. **Leistungskennzahlen**: Genauigkeit, Robustheit, Cybersicherheit; bekannte Einflussfaktoren.

4. **Risikoinformationen**: Vorhersehbare Fehlanwendungen mit Auswirkungen auf Gesundheit, Sicherheit, Grundrechte.
5. **Erklärfunktionen**: Technische Merkmale, um Ausgaben zu erläutern.
6. **Leistungsdaten für Zielgruppen**: ZB Genauigkeit bei bestimmten Personengruppen.
7. **Datenspezifikationen**: Eingabedaten, Trainings-, Validierungs-, Testdatensätze.
8. **Interpretationshinweise**: Wie Ausgaben verstanden und genutzt werden sollen.
9. **Geplante Änderungen**: Zum Zeitpunkt der Konformitätsbewertung bekannte Anpassungen.
10. **Menschliche Aufsicht**: Nach Artikel 14 KI-VO, inkl technischer Unterstützung zur Interpretation.
11. **Betriebsressourcen**: Hardware, Rechenleistung, Lebensdauer, Wartung, Updates.
12. **Protokollierungsfunktionen**: Beschreibung der Logging-Mechanismen nach Artikel 12 KI-VO.

III. Zusammenfassung

Pflicht	Erstellen von Betriebsanleitungen
Zweck	Transparenz für Betreiber, um Ausgaben zu verstehen und korrekt zu nutzen
Form	Präzise, vollständige, barrierefreie Betriebsanleitungen
Mindestinhalte	12 Pflichtangaben (siehe oben)

IV. Quellenverzeichnis

- Erwägungsgrund 72 KI-VO (EU) 2024/1689

Artikel 14 KI-VO

Menschliche Aufsicht

(1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie während der Dauer ihrer Verwendung — auch mit geeigneten Instrumenten einer Mensch-Maschine-Schnittstelle — von natürlichen Personen wirksam beaufsichtigt werden können.

(2) Die menschliche Aufsicht dient der Verhinderung oder Minimierung der Risiken für Gesundheit, Sicherheit oder Grundrechte, die entstehen können, wenn ein Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung verwendet wird, insbesondere wenn solche Risiken trotz der Einhaltung anderer Anforderungen dieses Abschnitts fortbestehen.

(3) Die Aufsichtsmaßnahmen müssen den Risiken, dem Grad der Autonomie und dem Kontext der Nutzung des Hochrisiko-KI-Systems angemessen sein und werden durch eine oder beide der folgenden Arten von Vorkehrungen gewährleistet:

a) Vorkehrungen, die vor dem Inverkehrbringen oder der Inbetriebnahme vom Anbieter bestimmt und, sofern technisch machbar, in das Hochrisiko-KI-System eingebaut werden;

b) Vorkehrungen, die vor dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems vom Anbieter bestimmt werden und dazu geeignet sind, vom Betreiber umgesetzt zu werden.

(4) Für die Zwecke der Durchführung der Absätze 1, 2 und 3 wird das Hochrisiko-KI-System dem Betreiber so zur Verfügung gestellt, dass die natürlichen Personen, denen die menschliche Aufsicht übertragen wurde, angemessen und verhältnismäßig in der Lage sind,

a) die einschlägigen Fähigkeiten und Grenzen des Hochrisiko-KI-Systems angemessen zu verstehen und seinen Betrieb ordnungsgemäß zu überwachen, einschließlich in Bezug auf das Erkennen und Beheben von Anomalien, Fehlfunktionen und unerwarteter Leistung;

b) sich einer möglichen Neigung zu einem automatischen oder übermäßigen Vertrauen in die von einem Hochrisiko-KI-System hervorgebrachte Ausgabe („Automatisierungsbias“) bewusst zu bleiben, insbesondere wenn Hochrisiko-KI-Systeme Informationen oder Empfehlungen

ausgeben, auf deren Grundlage natürliche Personen Entscheidungen treffen;

c) die Ausgabe des Hochrisiko-KI-Systems richtig zu interpretieren, wobei beispielsweise die vorhandenen Interpretationsinstrumente und -methoden zu berücksichtigen sind;

d) in einer bestimmten Situation zu beschließen, das Hochrisiko-KI-System nicht zu verwenden oder die Ausgabe des Hochrisiko-KI-Systems außer Acht zu lassen, außer Kraft zu setzen oder rückgängig zu machen;

e) in den Betrieb des Hochrisiko-KI-Systems einzugreifen oder den Systembetrieb mit einer „Stopptaste" oder einem ähnlichen Verfahren zu unterbrechen, was dem System ermöglicht, in einem sicheren Zustand zum Stillstand zu kommen.

(5) Bei den in Anhang III Nummer 1 Buchstabe a genannten Hochrisiko-KI-Systemen müssen die in Absatz 3 des vorliegenden Artikels genannten Vorkehrungen so gestaltet sein, dass außerdem der Betreiber keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange diese Identifizierung nicht von mindestens zwei natürlichen Personen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen, getrennt überprüft und bestätigt wurde.

Die Anforderung einer getrennten Überprüfung durch mindestens zwei natürliche Personen gilt nicht für Hochrisiko-KI-Systeme, die für Zwecke in den Bereichen Strafverfolgung, Migration, Grenzkontrolle oder Asyl verwendet werden, wenn die Anwendung dieser Anforderung nach Unionsrecht oder nationalem Recht unverhältnismäßig wäre.

I. Worum geht es?

Artikel 14 regelt, dass Hochrisiko-KI-Systeme in einer Weise gestaltet und betrieben werden müssen, sodass natürliche Personen deren Nutzung wirksam beaufsichtigen können. Ziel ist es, Risiken für Gesundheit, Sicherheit und Grundrechte zu verhindern oder zu minimieren – auch dann, wenn das System fehlerhaft angewendet wird oder trotz Einhaltung aller anderen Vorschriften Risiken verbleiben.

II. Detailkommentar

A. Grundprinzip der menschlichen Aufsicht

Eine Hochrisiko-KI muss – auch mit Mensch-Maschine-Schnittstellen (zB Dashboards) – so konzipiert sein, dass Menschen sie jederzeit überwachen können.

Die Aufsicht hat dabei **präventiven Charakter**: Risiken sollen verhindert oder reduziert werden. Dies gilt für bestimmungsgemäße Nutzung und für vorhersehbare Fehlanwendungen.

Beispiel: *Ein KI-gestütztes Diagnosesystem erkennt eine Krankheit falsch positiv. Ein Arzt muss die Möglichkeit haben, den Vorschlag zu prüfen und ggf. zu verwerfen, bevor der Patient unnötig behandelt wird.*

B. Arten der Aufsichtsmaßnahmen

Prinzip der Risikoadäquanz: Maßnahmen müssen sich an Risikoniveau, Autonomiegrad und Nutzungskontext orientieren. Hierfür sind zwei alternative Möglichkeiten vorgesehen

- **Integrierte Vorkehrungen**: Vor der Markteinführung technisch eingebaut (zB automatische Abschaltfunktionen).
- **Organisatorische Vorkehrungen**: Vorab festgelegt, aber vom Betreiber umzusetzen (zB Schulungskonzepte).

C. Anforderungen an die Aufsichtspersonen

Die Aufsichtspersonen müssen zumindest folgende Kompetenzen besitzen, wobei hierzu das KI-System selbst entsprechend ausgestattet sein muss, sodass diese Aufgabe angemessen und verhältnismäßig erfüllt werden kann:

- **Systemverständnis**: Kenntnis der Fähigkeiten (was das System gut kann) und Grenzen (wo Fehler wahrscheinlich sind) sowie Anomalien, Fehlfunktionen und unerwartete Leistungen.
- **Bewusstsein für Automatisierungsbias**: Automatisierungsbias bedeutet eine Tendenz, den Systemausgaben zu stark zu vertrauen – selbst wenn sie offensichtlich fehlerhaft sein könnten. Aufsichtspersonen müssen aktiv prüfen, ob die Systemausgabe

plausibel ist, statt automatisch zu folgen. Dies erfordert kritisches Denken und den Abgleich mit externen Informationen.

- **Interpretationsfähigkeit**: Fähigkeit, Systemausgaben unter Berücksichtigung der verfügbaren Interpretationswerkzeuge zu verstehen und Wissen, welche Eingabedaten und Kontexte die Ergebnisse beeinflusst haben.
- **Handlungsfreiheit**: Befugnis und Bereitschaft, das System nicht zu nutzen oder Ausgaben zu übersteuern.
- **Eingriffskompetenz**: Fähigkeit, den Betrieb zu unterbrechen oder zu stoppen (zB über „Stopptaste"), sodass das System in einen sicheren Zustand übergeht.

Beispiel: *Ein KI-gestütztes Kreditprüfsystem lehnt einen Antrag mit der Begründung „niedrige Kreditwürdigkeit" ab. Obwohl der Antragsteller nachweislich über eine gesicherte Einkommensquelle verfügt, würde ein voreingenommener Mitarbeiter der KI-Ausgabe einfach zustimmen. Eine geschulte Aufsichtsperson prüft dagegen die Fakten und korrigiert die Entscheidung.*

D. Zusätzliche Anforderungen

Für die in Anhang III KI-VO Z 1 lit a genannten Hochrisiko-KI-Systeme – also biometrische Fernidentifizierungssysteme – gilt folgende, verstärkte Anforderung:

- **Doppeltes menschliches Prüfprinzip**: Entscheidung nur zulässig, wenn mindestens zwei qualifizierte Personen das Ergebnis getrennt bestätigt haben.
- **Ausnahme**: Bei Strafverfolgung, Migration, Grenzkontrolle, Asyl entfällt Pflicht, wenn sie unverhältnismäßig wäre (nach Unions- oder nationalem Recht).

Beispiel: *Ein Gesichtserkennungssystem meldet einen Treffer in einer Menschenmenge. Erst nach Bestätigung durch zwei unabhängige Beamte darf eine Festnahme erfolgen – außer, wenn zB im Grenzschutz eine sofortige Reaktion zwingend notwendig ist.*

III. Zusammenfassung

Ziel	Menschliche Aufsicht soll Risiken von Hochrisiko-KI minimieren.
Formen	Technische Vorkehrungen und organisatorische Maßnahmen.
Anforderungen an Aufsichtsperson	Muss System verstehen, Bias vermeiden, interpretieren, eingreifen können.
Automatisierungsbias	Gefahr des blinden Vertrauens in KI-Ausgaben, muss aktiv vermieden werden.
Besonderheit	Doppelte Bestätigung bei biometrischer Identifizierung, Ausnahmen in bestimmten Bereichen.

IV. Quellenverzeichnis

- Erwägungsgrund 73 KI-VO (EU) 2024/1689

Artikel 15 KI-VO

Genauigkeit, Robustheit und Cybersicherheit

(1) Hochrisiko-KI-Systeme werden so konzipiert und entwickelt, dass sie ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren.

(2) Um die technischen Aspekte der Artikel und Weise der Messung des angemessenen Maßes an Genauigkeit und Robustheit gemäß Absatz 1 und anderer einschlägiger Leistungsmetriken anzugehen, fördert die Kommission in Zusammenarbeit mit einschlägigen Interessenträgern und Organisationen wie Metrologie- und Benchmarking-Behörden gegebenenfalls die Entwicklung von Benchmarks und Messmethoden.

(3) Die Maße an Genauigkeit und die relevanten Genauigkeitsmetriken von Hochrisiko-KI-Systemen werden in den ihnen beigefügten Betriebsanleitungen angegeben.

(4) Hochrisiko-KI-Systeme müssen so widerstandsfähig wie möglich gegenüber Fehlern, Störungen oder Unstimmigkeiten sein, die innerhalb des Systems oder der Umgebung, in der das System betrieben wird, insbesondere wegen seiner Interaktion mit natürlichen Personen oder anderen Systemen, auftreten können. In diesem Zusammenhang sind technische und organisatorische Maßnahmen zu ergreifen.

Die Robustheit von Hochrisiko-KI-Systemen kann durch technische Redundanz erreicht werden, was auch Sicherungs- oder Störungssicherheitspläne umfassen kann.

Hochrisiko-KI-Systeme, die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen, sind so zu entwickeln, dass das Risiko möglicherweise verzerrter Ausgaben, die künftige Vorgänge beeinflussen („Rückkopplungsschleifen"), beseitigt oder so gering wie möglich gehalten wird und sichergestellt wird, dass auf solche Rückkopplungsschleifen angemessen mit geeigneten Risikominderungsmaßnahmen eingegangen wird.

(5) Hochrisiko-KI-Systeme müssen widerstandsfähig gegen Versuche unbefugter Dritter sein, ihre Verwendung, Ausgaben oder Leistung durch Ausnutzung von Systemschwachstellen zu verändern.

Die technischen Lösungen zur Gewährleistung der Cybersicherheit von Hochrisiko-KI-Systemen müssen den jeweiligen Umständen und Risiken angemessen sein.

Die technischen Lösungen für den Umgang mit KI-spezifischen Schwachstellen umfassen gegebenenfalls Maßnahmen, um Angriffe, mit denen versucht wird, eine Manipulation des Trainingsdatensatzes („data poisoning") oder vortrainierter Komponenten, die beim Training verwendet werden („model poisoning"), vorzunehmen, Eingabedaten, die das KI-Modell zu Fehlern verleiten sollen („adversarial examples" oder „model evasions"), Angriffe auf vertrauliche Daten oder Modellmängel zu verhüten, zu erkennen, darauf zu reagieren, sie zu beseitigen und zu kontrollieren.

I. Worum geht es?

Artikel 15 KI-VO legt verbindliche Anforderungen an Genauigkeit, Robustheit und Cybersicherheit für Hochrisiko-KI-Systeme fest. Der Artikel soll sicherstellen, dass solche Systeme über ihren gesamten Lebenszyklus hinweg verlässlich funktionieren, Störungen standhalten und vor böswilligen Eingriffen geschützt sind.

II. Detailkommentar

A. Genauigkeit

- **Bedeutung:** Genauigkeit beschreibt, wie präzise und zuverlässig ein KI-System arbeitet, gemessen an seiner vorgesehenen Zweckbestimmung.
- **Anforderungen:**
  - Angemessenes Maß an Genauigkeit – angepasst an den Stand der Technik und den konkreten Einsatzbereich.
  - Laufende Aufrechterhaltung dieser Leistung über den gesamten Lebenszyklus.
  - Dokumentation der Leistungskennzahlen in der Betriebsanleitung.

Die Kommission kann zusammen mit Fachorganisationen Benchmarks und Messmethoden entwickeln (zB standardisierte Testdatensätze).

Beispiel: *Eine KI, die Röntgenbilder auswertet, muss ihre Trefferquote und Fehlerrate in der Anleitung klar angeben und darf nicht durch Software-Updates unbemerkt an Genauigkeit verlieren.*

B. Robustheit

- **Bedeutung**: Widerstandsfähigkeit gegenüber Fehlern, Störungen oder unerwarteten Situationen.
- **Technische Maßnahmen:**
    1. Redundanz (zB Backup-Systeme, Fail-Safe-Mechanismen).
    2. Störungssicherheitspläne (kontrolliertes Abschalten bei Anomalien).

Bei lernenden Systemen nach Inverkehrbringen muss zudem das Risiko von Rückkopplungsschleifenminimiert werden (etwa verzerrte Ausgaben, die sich selbst verstärken).

Beispiel: *Eine KI im Kreditwesen darf nicht durch wiederholtes Lernen aus eigenen Entscheidungen diskriminierende Muster verstärken.*

C. Cybersicherheit

- **Bedeutung:** Schutz vor Manipulation durch unbefugte Dritte.
- **Gefahrenarten:**
    - **Data Poisoning** (Manipulation der Trainingsdaten).
    - **Model Poisoning** (Veränderung vortrainierter Komponenten).
    - **Adversarial Examples** (gezielte fehlerverursachende Eingaben).
    - **Inferenzangriffe** (Auslesen sensibler Daten aus dem Modell).

Folglich sind angemessene technische Schutzmechanismen, auch in der zugrunde liegenden IKT-Infrastruktur, zu gewährleisten.

D. Besonderheiten

- **Flexibilität**: Anforderungen richten sich nach dem jeweiligen Einsatzbereich und dem Stand der Technik.
- **Harmonisierung**: Für Cybersicherheit kann Erfüllung anderer einschlägiger EU-Rechtsakte als gleichwertig gelten.
- **Lebenszyklus-Perspektive**: Pflichten gelten nicht nur bei Markteintritt, sondern fortlaufend.

III. Zusammenfassung

Genauigkeit	Präzision gem Zweckbestimmung, Dokumentation in Anleitung
Robustheit	Widerstand gegen Fehler, Störungen, Rückkopplungsschleifen
Cybersicherheit	Schutz vor böswilligen Eingriffen und KI-spezifischen Angriffen

IV. Quellenverzeichnis

- Erwägungsgrund 74-78 KI-VO (EU) 2024/1689

Artikel 16 KI-VO

Pflichten der Anbieter von Hochrisiko-KI-Systemen

Anbieter von Hochrisiko-KI-Systemen müssen

a)sicherstellen, dass ihre Hochrisiko-KI-Systeme die in Abschnitt 2 festgelegten Anforderungen erfüllen;

b)auf dem Hochrisiko-KI-System oder, falls dies nicht möglich ist, auf seiner Verpackung oder in der beigefügten Dokumentation ihren Namen, ihren eingetragenen Handelsnamen bzw. ihre eingetragene Handelsmarke und ihre Kontaktanschrift angeben;

c)über ein Qualitätsmanagementsystem verfügen, das Artikel 17 entspricht;

d) die in Artikel 18 genannte Dokumentation aufbewahren;

e)die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle gemäß Artikel 19 aufbewahren, wenn diese ihrer Kontrolle unterliegen;

f)sicherstellen, dass das Hochrisiko-KI-System dem betreffenden Konformitätsbewertungsverfahren gemäß Artikel 43 unterzogen wird, bevor es in Verkehr gebracht oder in Betrieb genommen wird;

g) eine EU-Konformitätserklärung gemäß Artikel 47 ausstellen;

h)die CE-Kennzeichnung an das Hochrisiko-KI-System oder, falls dies nicht möglich ist, auf seiner Verpackung oder in der beigefügten Dokumentation anbringen, um Konformität mit dieser Verordnung gemäß Artikel 48 anzuzeigen;

i)den in Artikel 49 Absatz 1 genannten Registrierungspflichten nachkommen;

j)die erforderlichen Korrekturmaßnahmen ergreifen und die gemäß Artikel 20 erforderlichen Informationen bereitstellen;

k)auf begründete Anfrage einer zuständigen nationalen Behörde nachweisen, dass das Hochrisiko-KI-System die Anforderungen in Abschnitt 2 erfüllt;

l)sicherstellen, dass das Hochrisiko-KI-System die Barrierefreiheitsanforderungen gemäß den Richtlinien (EU) 2016/2102 und (EU) 2019/882 erfüllt.

I. Worum geht es?

Artikel 16 KI-VO legt die zentrale Verantwortung der Anbieter von Hochrisiko-KI-Systemen fest. Ziel des Artikels ist es, die Verantwortung klar zuzuordnen und einheitliche Mindestpflichten für Anbieter aufzustellen. Dadurch wird sichergestellt, dass Hochrisiko-KI-Systeme nur unter strengen Voraussetzungen auf den Markt gelangen.

II. Detailkommentar

A. Grundpflichten der Anbieter

Anbieter müssen sicherstellen, dass ihre Systeme:

- **rechtskonform entwickelt** sind (Erfüllung der Anforderungen aus Abschnitt 2, zB Risikomanagement, Datenqualität, Transparenz);
- **eindeutig identifizierbar** sind (Name, Marke, Kontaktanschrift auf System, Verpackung oder Dokumentation);
- **qualitätsgesichert** betrieben werden (Pflicht zum Qualitätsmanagementsystem, Artikel 17 KI-VO);
- **dokumentiert** sind (Technische Dokumentation nach **Artikel 18** KI-VO, Protokolle nach Artikel 19 KI-VO);
- **zertifiziert** werden (Konformitätsbewertung nach Artikel 43 KI-VO, Konformitätserklärung nach Artikel 47 KI-VO, CE-Kennzeichnung nach Artikel 48 KI-VO);
- **registriert** werden (Eintragung nach Artikel 49 KI-VO).

B. Verantwortung im Markt

Anbieter tragen die Hauptverantwortung dafür, dass ein Hochrisiko-KI-System vor Markteintritt den Vorgaben entspricht. Dies gilt auch dann, wenn der Anbieter nicht der ursprüngliche Entwickler ist. Wer also das System in den Verkehr bringt, übernimmt die Verantwortung.

C. Besondere Pflichten

- **Korrekturmaßnahmen**: Wenn sich Probleme zeigen, müssen Anbieter unverzüglich Maßnahmen ergreifen.
- **Behördenkooperation**: Auf Nachfrage muss nachgewiesen werden, dass die Anforderungen erfüllt sind.
- **Barrierefreiheit**: Anbieter müssen sicherstellen, dass Systeme auch für Menschen mit Behinderungen nutzbar sind. Anders als andere Pflichten betrifft sie nicht nur Technik und Dokumentation, sondern auch das Design der Systeme. Anbieter müssen von Beginn an darauf achten, dass das System universell nutzbar ist.

III. Zusammenfassung

Pflichtbereich	Inhalt	Ziel
Rechtskonformität	Anforderungen Abschnitt 2	Sicherheit und Qualität
Kennzeichnung	Name, Marke, Kontakt	Transparenz
Qualitätssystem	Artikel 17 KI-VO	Einheitliche Standards
Dokumentation	Artikel 18 KI-VO, Artikel 19 KI-VO	Nachvollziehbarkeit
Konformität und CE	Artikel 43 KI-VO, Artikel 47 KI-VO, Artikel 48 KI-VO	Einheitliche Martüberwachung
Registrierung	Artikel 49 KI-VO	Kontrolle durch Behörden
Korrektur und Info	Artikel 20 KI-VO	Risikobegrenzung
Barrierefreiheit	Verweis RL 2016/2102, 2019/882	Gleichstellung

IV. Quellenverzeichnis

- Erwägungsgründe 79, 80 KI-VO (EU) 2024/1689

Artikel 17 KI-VO

Qualitätsmanagementsystem

(1) Anbieter von Hochrisiko-KI-Systemen richten ein Qualitätsmanagementsystem ein, das die Einhaltung dieser Verordnung gewährleistet. Dieses System wird systematisch und ordnungsgemäß in Form schriftlicher Regeln, Verfahren und Anweisungen dokumentiert und umfasst mindestens folgende Aspekte:

a) ein Konzept zur Einhaltung der Regulierungsvorschriften, was die Einhaltung der Konformitätsbewertungsverfahren und der Verfahren für das Management von Änderungen an dem Hochrisiko-KI-System miteinschließt;

b) Techniken, Verfahren und systematische Maßnahmen für den Entwurf, die Entwurfskontrolle und die Entwurfsprüfung des Hochrisiko-KI-Systems;

c) Techniken, Verfahren und systematische Maßnahmen für die Entwicklung, Qualitätskontrolle und Qualitätssicherung des Hochrisiko-KI-Systems;

d) Untersuchungs-, Test- und Validierungsverfahren, die vor, während und nach der Entwicklung des Hochrisiko-KI-Systems durchzuführen sind, und die Häufigkeit der Durchführung;

e) die technischen Spezifikationen und Normen, die anzuwenden sind und, falls die einschlägigen harmonisierten Normen nicht vollständig angewandt werden oder sie nicht alle relevanten Anforderungen gemäß Abschnitt 2 abdecken, die Mittel, mit denen gewährleistet werden soll, dass das Hochrisiko-KI-System diese Anforderungen erfüllt;

f) Systeme und Verfahren für das Datenmanagement, einschließlich Datengewinnung, Datenerhebung, Datenanalyse, Datenkennzeichnung, Datenspeicherung, Datenfilterung, Datenauswertung, Datenaggregation, Vorratsdatenspeicherung und sonstiger Vorgänge in Bezug auf die Daten, die im Vorfeld und für die Zwecke des Inverkehrbringens oder der Inbetriebnahme von Hochrisiko-KI-Systemen durchgeführt werden;

g) das in Artikel 9 genannte Risikomanagementsystem;

h) die Einrichtung, Anwendung und Aufrechterhaltung eines Systems zur Beobachtung nach dem Inverkehrbringen gemäß Artikel 72;

i) Verfahren zur Meldung eines schwerwiegenden Vorfalls gemäß Artikel 73;

j) die Handhabung der Kommunikation mit zuständigen nationalen Behörden, anderen einschlägigen Behörden, auch Behörden, die den Zugang zu Daten gewähren oder erleichtern, notifizierten Stellen, anderen Akteuren, Kunden oder sonstigen interessierten Kreisen;

k) Systeme und Verfahren für die Aufzeichnung sämtlicher einschlägigen Dokumentation und Informationen;

l) Ressourcenmanagement, einschließlich Maßnahmen im Hinblick auf die Versorgungssicherheit;

m) einen Rechenschaftsrahmen, der die Verantwortlichkeiten der Leitung und des sonstigen Personals in Bezug auf alle in diesem Absatz aufgeführten Aspekte regelt.

(2) Die Umsetzung der in Absatz 1 genannten Aspekte erfolgt in einem angemessenen Verhältnis zur Größe der Organisation des Anbieters. Die Anbieter müssen in jedem Fall den Grad der Strenge und das Schutzniveau einhalten, die erforderlich sind, um die Übereinstimmung ihrer Hochrisiko-KI-Systeme mit dieser Verordnung sicherzustellen.

(3) Anbieter von Hochrisiko-KI-Systemen, die Pflichten in Bezug auf Qualitätsmanagementsysteme oder eine gleichwertige Funktion gemäß den sektorspezifischen Rechtsvorschriften der Union unterliegen, können die in Absatz 1 aufgeführten Aspekte als Bestandteil der nach den genannten Rechtsvorschriften festgelegten Qualitätsmanagementsysteme einbeziehen.

(4) Bei Anbietern, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union über Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, gilt die Pflicht zur Einrichtung eines Qualitätsmanagementsystems — mit Ausnahme des Absatzes 1 Buchstaben g, h und i des vorliegenden Artikels — als erfüllt, wenn die Vorschriften über Regelungen oder Verfahren der internen Unternehmensführung gemäß dem einschlägigen Unionsrecht über Finanzdienstleistungen eingehalten werden. Zu diesem Zweck werden die in Artikel 40 genannten harmonisierten Normen berücksichtigt.

I. Worum geht es?

Artikel 17 KI-VO verpflichtet Anbieter von Hochrisiko-KI-Systemen, ein umfassendes Qualitätsmanagementsystem (QMS) einzurichten. Dieses

QMS soll sicherstellen, dass alle Anforderungen der Verordnung eingehalten werden. Es handelt sich also um eine Artikel „Betriebssystem“ für die Qualität, das die gesamte Entwicklung, den Betrieb und die Überwachung eines Hochrisiko-KI-Systems umfasst. Ziel ist es, dass Anbieter systematisch und nachvollziehbar nachweisen können, wie sie die Sicherheit, Zuverlässigkeit und Konformität ihrer Systeme gewährleisten.

II. Detailkommentar

A. Struktur und Inhalt des QMS

Absatz 1 listet die Mindestinhalte des QMS auf. Diese umfassen ua:

- **Regelkonzept**: Verfahren zur Einhaltung der KI-VO, inkl Konformitätsbewertung und Änderungsmanagement.
- **Entwurf und Entwicklung**: Klare Methoden zur Planung, Kontrolle und Prüfung des Systemdesigns.
- **Qualitätssicherung**: Prozesse für Test, Validierung und Überprüfung während und nach der Entwicklung.
- **Datenmanagement**: Vorgaben für Datenerhebung, -speicherung, -analyse und -nutzung.
- **Risikomanagement** (Artikel 9 KI-VO): Verknüpfung mit eigenem Risikomanagementsystem.
- **Beobachtung nach dem Inverkehrbringen** (Artikel 72 KI-VO): Laufende Überwachung der Nutzung.
- **Meldepflichten** (Artikel 73 KI-VO): Verfahren zur Meldung schwerwiegender Vorfälle.
- **Kommunikation**: Umgang mit Behörden, Kunden und anderen Akteuren.
- **Dokumentation**: Aufzeichnung aller relevanten Informationen.
- **Ressourcenmanagement**: Sicherstellung von Personal und Versorgung.
- **Rechenschaftsrahmen**: Klare Verantwortlichkeiten von Leitung und Mitarbeitern.

B. Verhältnis zur Unternehmensgröße

Die Umsetzung des QMS muss verhältnismäßig zur Größe des Anbieters erfolgen. Kleinere Unternehmen dürfen also vereinfachte Strukturen nutzen – allerdings nur, solange das erforderliche Schutzniveau gewahrt bleibt. Der Grundsatz lautet: Flexibilität bei der Organisation, keine Abstriche bei der Sicherheit.

C. Anschluss an sektorspezifische Vorschriften

- Anbieter, die bereits anderen EU-Regelungen mit QMS-Pflichten unterliegen (zB Medizinprodukte, Luftfahrt), können die Anforderungen des Artikel 17 in ihre bestehenden Systeme integrieren.
- Für Finanzinstitute gilt eine Sonderregel: Wenn sie bereits interne Governance-Regeln nach dem Unionsrecht der Finanzdienstleistungen erfüllen, gilt Artikel 17 weitgehend als erfüllt. Ausgenommen sind lediglich die Vorgaben zu Risikomanagement (Artikel 9 KI-VO), Marktüberwachung (Artikel 72 KI-VO) und Meldepflichten (Artikel 73 KI-VO), die zusätzlich einzuhalten sind.

III. Zusammenfassung

Pflicht	Anbieter von Hochrisiko-KI-Systemen müssen ein QMS einrichten
Mindestinhalte	ua Regulierungskonzept, Entwurf, Qualitätssicherung, Datenmanagement, Risikomanagement, Marktüberwachung, Dokumentation
Verhältnis zur Größe	Anpassbar an Unternehmensgröße, aber Sicherheit darf nicht leiden
Schnittstellen	Integration in bestehende sektorspezifische QMS möglich
Sonderregel	Finanzinstitute: Erfüllung größtenteils durch bestehende Governance-Systeme

IV. Quellenverzeichnis

- Erwägungsgrund 81 KI-VO (EU) 2024/1689

Artikel 18 KI-VO

Aufbewahrung der Dokumentation

(1) Der Anbieter hält für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems folgende Unterlagen für die zuständigen nationalen Behörden bereit:

a) die in Artikel 11 genannte technische Dokumentation;

b) die Dokumentation zu dem in Artikel 17 genannten Qualitätsmanagementsystem;

c) die Dokumentation über etwaige von notifizierten Stellen genehmigte Änderungen;

d) gegebenenfalls die von den notifizierten Stellen ausgestellten Entscheidungen und sonstigen Dokumente;

e) die in Artikel 47 genannte EU-Konformitätserklärung.

(2) Jeder Mitgliedstaat legt die Bedingungen fest, unter denen die in Absatz 1 genannte Dokumentation für die zuständigen nationalen Behörden für den in dem genannten Absatz angegebenen Zeitraum bereitgehalten wird, für den Fall, dass ein Anbieter oder sein in demselben Hoheitsgebiet niedergelassener Bevollmächtigter vor Ende dieses Zeitraums in Konkurs geht oder seine Tätigkeit aufgibt.

(3) Anbieter, die Finanzinstitute sind und gemäß dem Unionsrecht über Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, pflegen die technische Dokumentation als Teil der gemäß dem Unionsrecht über Finanzdienstleistungen aufzubewahrenden Dokumentation.

I. Worum geht es?

Artikel 18 KI-VO regelt die Pflicht der Anbieter von Hochrisiko-KI-Systemen, bestimmte Dokumentationen für einen Zeitraum von zehn Jahren aufzubewahren. Diese Pflicht soll sicherstellen, dass die Behörden auch lange nach dem Inverkehrbringen prüfen können, ob die gesetzlichen Vorgaben eingehalten wurden. Damit wird die Nachvollziehbarkeit, Kontrolle und Überprüfbarkeit von Hochrisiko-KI-Systemen gewährleistet.

Zugleich schafft die Vorschrift Rechtssicherheit für den Fall, dass ein Anbieter seine Geschäftstätigkeit beendet.

II. Detailkommentar

A. Aufbewahrungspflicht

- **Zeitraum: Zehn Jahre** – Ab dem Zeitpunkt des Inverkehrbringens oder der Inbetriebnahme müssen die Unterlagen für ein Jahrzehnt verfügbar sein.
- **Adressaten: Anbieter von Hochrisiko-KI-Systemen** – Nur für diese gilt die Pflicht.
- **Umfang der Unterlagen:**
  1. **Technische Dokumentation (**Artikel 11 KI-VO**):** Beschreibt Entwicklung, Funktionsweise und Grenzen des KI-Systems.
  2. **QMS (Artikel 17 KI-VO):** Nachweis, dass interne Abläufe und Kontrollen bestehen.
  3. **Genehmigte Änderungen:** Anpassungen, die von einer notifizierten Stelle überprüft und zugelassen wurden.
  4. **Entscheidungen und Dokumente der notifizierten Stellen:** ZB Gutachten, Prüfberichte oder Konformitätsbewertungen.
  5. **EU-Konformitätserklärung (Artikel 47 KI-VO):** Schriftliche Bestätigung des Anbieters, dass das System den Anforderungen entspricht.

Beispiel: *Ein Unternehmen bringt ein KI-System für die Kreditwürdigkeitsprüfung auf den Markt. Es muss zehn Jahre lang die gesamte technische Dokumentation und die EU-Konformitätserklärung aufbewahren, damit die Behörden im Nachhinein prüfen können, ob die Anforderungen eingehalten wurden.*

B. Sonderregelung bei Konkurs oder Aufgabe

- **Verantwortung der Mitgliedstaaten:** Jeder Mitgliedstaat bestimmt, wie die Dokumentation in solchen Fällen verfügbar bleibt.

- **Zweck:** Verhindert, dass mit dem Ende des Unternehmens auch die Nachvollziehbarkeit verloren geht.
- **Mögliche Umsetzung:** Übertragung an nationale Behörden oder Archive.

Beispiel: *Wenn ein KI-Start-up in Konkurs geht, kann der Mitgliedstaat vorschreiben, dass die Unterlagen an eine nationale Aufsichtsbehörde übergeben werden müssen.*

C. Finanzinstitute

- **Integration in bestehende Pflichten:** Finanzinstitute können die Dokumentation in ihre ohnehin nach dem EU-Finanzdienstleistungsrecht vorgeschriebene Dokumentationspflicht integrieren.
- **Vereinfachung:** Doppelarbeit wird vermieden, da keine parallelen Systeme erforderlich sind.

Beispiel: *Eine Bank, die ein KI-System zur Geldwäscheprävention einsetzt, führt die technische Dokumentation als Teil ihrer ohnehin bestehenden Aufbewahrungspflichten nach Bankenrecht.*

III. Zusammenfassung

Adressaten	Anbieter von Hochrisiko-KI-Systemen
Zeitraum	10 Jahre ab Inverkehrbringen/Inbetriebnahme
Unterlagen	Technische Dokumentation, QMS, genehmigte Änderungen, Entscheidungen der notifizierten Stellen, EU-Konformitätserklärung
Sonderfälle	Konkurs/Aufgabe: Mitgliedstaaten regeln Aufbewahrung
Finanzinstitute	Dürfen bestehende Dokumentationspflichten nutzen

IV. Quellenverzeichnis

- Erwägungsgründe 71, 81 KI-VO (EU) 2024/1689

Artikel 19 KI-VO

Automatisch erzeugte Protokolle

(1) Anbieter von Hochrisiko-KI-Systemen bewahren die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle gemäß Artikel 12 Absatz 1 auf, soweit diese Protokolle ihrer Kontrolle unterliegen. Unbeschadet des geltenden Unionsrechts oder nationalen Rechts werden die Protokolle für einen der Zweckbestimmung des Hochrisiko-KI-Systems angemessenen Zeitraum von mindestens sechs Monaten aufbewahrt, sofern in den geltenden Rechtsvorschriften der Union, insbesondere im Unionsrecht zum Schutz personenbezogener Daten, oder im geltenden nationalen Recht nichts anderes vorgesehen ist.

(2) Anbieter, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union über Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung, unterliegen, bewahren die von ihren Hochrisiko-KI-Systemen automatisch erzeugten Protokolle als Teil der gemäß dem einschlägigen Unionsrecht über Finanzdienstleistungen aufzubewahrenden Dokumentation auf.

I. Worum geht es?

Artikel 19 regelt die Pflicht von Anbietern, die Protokolle ihrer Hochrisiko-KI-Systeme aufzubewahren. Diese Protokolle entstehen automatisch während der Nutzung und dokumentieren den Systembetrieb. Ziel der Norm ist es, Transparenz und Nachvollziehbarkeit sicherzustellen. Nur wenn nachvollzogen werden kann, wie ein KI-System gearbeitet hat, sind spätere Prüfungen – etwa bei Fehlfunktionen oder Schäden – überhaupt möglich. Damit ergänzt Art19 die allgemeinen Anforderungen an Protokollierung aus Artikel 12 KI-VO.

II. Detailkommentar

A. Inhalt der Aufbewahrungspflicht

1. Artikel der Protokolle

Bezug zu Artikel 12 KI-VO Absatz 1: Dort ist festgelegt, dass Hochrisiko-KI-Systeme so konzipiert sein müssen, dass sie bestimmte

Ereignisprotokolle automatisch erzeugen. Diese Protokolle können zB Informationen über Datenzugriffe, Systementscheidungen oder Fehlermeldungen enthalten.

2. Aufbewahrungsdauer

- **Grundregel**: mindestens sechs Monate.
- **Einschränkung**: Längere oder kürzere Fristen sind möglich, wenn Unions- oder nationales Recht etwas anderes vorsieht, insbesondere datenschutzrechtlich.

Beispiel: *Ein Medizinprodukt mit KI-Element dokumentiert jede Entscheidung. Die Daten müssen mindestens sechs Monate gespeichert werden, es sei denn, medizinrechtliche Vorschriften verlangen längere Fristen.*

3. Kontrolle über Protokolle

Aufbewahrungspflicht besteht nur, soweit die Protokolle unter der Kontrolle des Anbieters stehen. Das ist dann der Fall, wenn er technisch oder organisatorisch Zugriff hat.

Beispiel: *Eine Cloud-KI erzeugt Protokolle, die ausschließlich vom Betreiber der Cloud gespeichert werden. Hat der Anbieter keinen Zugriff, entfällt seine Aufbewahrungspflicht.*

B. Besonderheiten für Finanzinstitute

Banken und vergleichbare Institute müssen Protokolle nicht gesondert aufbewahren, sondern als Teil ihrer ohnehin umfangreichen Dokumentationspflichten im EU-Finanzrecht. So wird vermieden, dass es zu Doppelpflichten kommt.

Beispiel: *Eine Bank nutzt ein Hochrisiko-KI-System zur Kreditwürdigkeitsprüfung. Die Protokolle werden automatisch in die vorhandene aufsichtsrechtliche Dokumentation integriert.*

III. Zusammenfassung

Adressaten	Anbieter von Hochrisiko-KI-Systemen
Protokollinhalt	Automatisch erzeugte Protokolle nach Artikel 12 KI-VOAbsatz 1 (zB Systementscheidungen, Fehler)
Aufbewahrungsdauer	Mindestens sechs Monate, außer andere Vorschriften verlangen Abweichungen
Kontrolle	Pflicht nur bei Protokollen, die der Anbieter tatsächlich kontrollieren kann
Finanzinstitute	Aufbewahrung als Teil der bestehenden Dokumentationspflichten im EU-Finanzrecht

Artikel 20 KI-VO

Korrekturmaßnahmen und Informationspflicht

(1) Anbieter von Hochrisiko-KI-Systemen, die der Auffassung sind oder Grund zu der Annahme haben, dass ein von ihnen in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System nicht dieser Verordnung entspricht, ergreifen unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität dieses Systems herzustellen oder es gegebenenfalls zurückzunehmen, zu deaktivieren oder zurückzurufen. Sie informieren die Händler des betreffenden Hochrisiko-KI-Systems und gegebenenfalls die Betreiber, den Bevollmächtigten und die Einführer darüber.

(2) Birgt das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 79 Absatz 1 und wird sich der Anbieter des Systems dieses Risikos bewusst, so führt er unverzüglich gegebenenfalls gemeinsam mit dem meldenden Betreiber eine Untersuchung der Ursachen durch und informiert er die Marktüberwachungsbehörden, in deren Zuständigkeit das betroffene Hochrisiko-KI-System fällt, und gegebenenfalls die notifizierte Stelle, die eine Bescheinigung für dieses Hochrisiko-KI-System gemäß Artikel 44 ausgestellt hat, insbesondere über die Artikel der Nichtkonformität und über bereits ergriffene relevante Korrekturmaßnahmen.

I. Worum geht es?

Artikel 20 KI-VO legt die Pflichten der Anbieter von Hochrisiko-KI-Systemen fest, wenn diese feststellen, dass ihr System nicht den Vorgaben der Verordnung entspricht oder ein Risiko verursacht. Ziel ist es, schnelles Handeln sicherzustellen, um Gefahren für Nutzer oder Dritte zu vermeiden und die Marktüberwachung zu gewährleisten.

II. Detailkommentar

A. Korrekturmaßnahmen

- **Pflicht zur Handlung**: Sobald ein Anbieter Grund zur Annahme hat, dass sein KI-System nicht konform ist, muss er sofort reagieren. Untätigkeit ist ausgeschlossen.

- **Arten der Maßnahmen**:
    - **Herstellung der Konformität**: Technische Anpassungen, Updates oder organisatorische Änderungen.
    - **Marktmaßnahmen**: Rücknahme (noch nicht genutzte Produkte), Deaktivierung (Abschalten eines Systems) oder Rückruf (Systeme, die bereits im Umlauf sind).
- **Informationspflichten**: Alle relevanten Akteure der Vertriebskette (Händler, Betreiber, Bevollmächtigter, Einführer) müssen informiert werden, um ein koordiniertes Vorgehen zu ermöglichen.

Beispiel: *Ein Anbieter entdeckt, dass ein KI-System zur Bewerberauswahl fehlerhafte Daten verwendet und dadurch diskriminiert. Er muss das System sofort deaktivieren, ein Update bereitstellen und alle Händler sowie Unternehmen, die es einsetzen, informieren.*

B. Informationspflicht bei Risiken

- **Auslöser**: Wenn das System ein Risiko im Sinn von Artikel 79 KI-VOAbsatz 1 birgt (zB Gesundheit, Sicherheit, Grundrechte).
- **Untersuchungspflicht**: Der Anbieter muss den Ursachen nachgehen, ggf gemeinsam mit dem Betreiber. Dies dient der Risikoklärung und schnellen Abhilfe.
- **Meldepflicht**: Marktüberwachungsbehörden sind unverzüglich zu informieren. Bei zertifizierten Systemen (Artikel 44 KI-VO) muss auch die notifizierte Stelle informiert werden.
- **Inhalt der Meldung**: Artikel der Nichtkonformität und bereits ergriffene Korrekturmaßnahmen.

Beispiel: *Ein Anbieter stellt fest, dass sein KI-System zur Kreditwürdigkeitsprüfung bestimmte Minderheiten systematisch benachteiligt. Neben Sofortmaßnahmen muss er die zuständige Marktüberwachungsbehörde informieren und den Ursachenbericht vorlegen.*

C. Besonderheiten

- **Unverzüglichkeit**: Der Artikel betont mehrfach das sofortige Handeln. Verzögerungen können rechtliche Folgen nach sich ziehen.
- **Zusammenspiel mit Artikel 79**: Artikel 20 verweist ausdrücklich auf Artikel 79 KI-VO, wodurch die Verbindung zwischen Marktüberwachung und Anbieterverantwortung gestärkt wird.
- **Abgrenzung**: Artikel 20 betrifft nur Anbieter (nicht Händler oder Nutzer), da diese primär für die Konformität verantwortlich sind.

III. Zusammenfassung

Pflicht zur Korrektur	Anbieter müssen sofort handeln, wenn ihr System nicht konform ist.
Informationspflichten	Händler, Betreiber, Bevollmächtigter, Einführer informieren.
Risiko-Meldung	Untersuchung der Ursachen + Meldung an Marktüberwachungsbehörde und ggf notifizierte Stelle.
Zweck	Schutz von Nutzern und Dritten, Sicherstellung von Marktüberwachung.

Artikel 21 KI-VO

Zusammenarbeit mit den zuständigen Behörden

(1) Anbieter von Hochrisiko-KI-Systemen übermitteln einer zuständigen Behörde auf deren begründete Anfrage sämtliche Informationen und Dokumentation, die erforderlich sind, um die Konformität des Hochrisiko-KI-Systems mit den in Abschnitt 2 festgelegten Anforderungen nachzuweisen, und zwar in einer Sprache, die für die Behörde leicht verständlich ist und bei der es sich um eine der von dem betreffenden Mitgliedstaat angegebenen Amtssprachen der Institutionen der Union handelt.

(2) Auf begründete Anfrage einer zuständigen Behörde gewähren die Anbieter der anfragenden zuständigen Behörde gegebenenfalls auch Zugang zu den automatisch erzeugten Protokollen des Hochrisiko-KI-Systems gemäß Artikel 12 Absatz 1, soweit diese Protokolle ihrer Kontrolle unterliegen.

(3) Alle Informationen, die eine zuständige Behörde aufgrund dieses Artikels erhält, werden im Einklang mit den in Artikel 78 festgelegten Vertraulichkeitspflichten behandelt.

I. Worum geht es?

Artikel 21 regelt die Zusammenarbeit zwischen Anbietern von Hochrisiko-KI-Systemen und den zuständigen nationalen Behörden. Im Mittelpunkt steht die Pflicht der Anbieter, auf Nachfrage umfassende Informationen und Unterlagen bereitzustellen, damit die Behörde die Einhaltung der gesetzlichen Anforderungen prüfen kann. Damit soll sichergestellt werden, dass die Aufsicht effektiv funktioniert und Verstöße rechtzeitig erkannt werden. Gleichzeitig werden die Grenzen der Auskunftspflichten sowie der Schutz vertraulicher Informationen festgelegt.

II. Detailkommentar

A. Auskunftspflicht der Anbieter

- **Begründete Anfrage:** Die Behörde muss einen nachvollziehbaren Grund angeben, warum sie Informationen verlangt. Damit soll

verhindert werden, dass willkürliche oder unverhältnismäßige Anfragen gestellt werden.

- **Umfang der Informationen:** Es sind alle Unterlagen vorzulegen, die für den Nachweis der Konformität mit den Anforderungen aus Abschnitt 2 (zB Datenqualität, Transparenz, Risikomanagement) erforderlich sind.
- **Sprachregelung:** Die Informationen müssen in einer Amtssprache der EU vorgelegt werden, die der Mitgliedstaat akzeptiert. Damit wird die praktische Verständlichkeit sichergestellt.

B. Zugang zu Protokollen

- **Automatisch erzeugte Protokolle**: Nach Artikel 12 KI-VOAbsatz 1 müssen Hochrisiko-KI-Systeme bestimmte Vorgänge automatisch protokollieren. Diese Protokolle dienen der Nachvollziehbarkeit und Fehleranalyse.
- **Kontrolle des Anbieters**: Der Anbieter muss nur solche Protokolle zugänglich machen, die sich in seiner Verfügungsgewalt befinden. Damit wird ausgeschlossen, dass er für Daten verantwortlich ist, auf die er keinen Zugriff hat.
- **Zweck**: Die Behörde erhält Einblick in die tatsächliche Funktionsweise des Systems, um Abweichungen oder Missbrauch festzustellen.

C. Vertraulichkeit

- **Verweis auf Artikel 78 KI-VO:** Alle Informationen, die eine Behörde nach Artikel 21 erhält, müssen vertraulich behandelt werden. Das schützt Geschäftsgeheimnisse und sensible Betriebsinformationen.
- **Balance zwischen Kontrolle und Schutz:** Einerseits wird die behördliche Aufsicht gestärkt, andererseits wird sichergestellt, dass vertrauliche Daten nicht unberechtigt weitergegeben werden.

Beispiel: *Ein Anbieter stellt einer Behörde interne Testberichte zur Verfügung. Die Behörde darf diese Informationen nicht ohne weiteres an Wettbewerber oder die Öffentlichkeit weitergeben.*

D. Besonderheiten

- **Präventiver Charakter:** Artikel 21 soll nicht nur im Verdachtsfall greifen, sondern ermöglicht auch stichprobenartige oder anlassbezogene Prüfungen.
- **Systematische Einordnung:** Der Artikel ergänzt die allgemeinen Pflichten der Anbieter (Artikel 16 KI-VOff) und dient der effektiven Durchsetzung durch die Mitgliedstaaten.
- **Zielsetzung der Norm:** Sinn und Zweck ist die **Sicherstellung einer wirksamen Marktüberwachung**, ohne die unternehmerische Freiheit unverhältnismäßig einzuschränken.

III. Zusammenfassung

Auskunftspflicht	Anbieter müssen auf begründete Anfrage umfassende Unterlagen zur Konformität bereitstellen.
Sprache	Informationen müssen in einer von den Mitgliedstaaten akzeptierten EU-Amtssprache eingereicht werden.
Protokolle	Behörden können Zugang zu automatisch erzeugten Protokollen verlangen, soweit der Anbieter diese kontrolliert.
Vertraulichkeit	Erhaltene Informationen unterliegen strengen Vertraulichkeitspflichten (Artikel 78 KI-VO).
Zweck	Sicherstellung wirksamer Aufsicht über Hochrisiko-KI-Systeme.

Artikel 22 KI-VO

Bevollmächtigte der Anbieter von Hochrisiko-KI-Systemen

(1) Anbieter, die in Drittländern niedergelassen sind, benennen vor der Bereitstellung ihrer Hochrisiko-KI-Systeme auf dem Unionsmarkt schriftlich einen in der Union niedergelassenen Bevollmächtigten.

(2) Der Anbieter muss seinem Bevollmächtigten ermöglichen, die Aufgaben wahrzunehmen, die im vom Anbieter erhaltenen Auftrag festgelegt sind.

(3) Der Bevollmächtigte nimmt die Aufgaben wahr, die in seinem vom Anbieter erhaltenen Auftrag festgelegt sind. Er stellt den Marktüberwachungsbehörden auf Anfrage eine Kopie des Auftrags in einer von der zuständigen Behörde angegebenen Amtssprache der Institutionen der Union bereit. Für die Zwecke dieser Verordnung ermächtigt der Auftrag den Bevollmächtigten zumindest zur Wahrnehmung folgender Aufgaben:

a) Überprüfung, ob die in Artikel 47 genannte EU-Konformitätserklärung und die technische Dokumentation gemäß Artikel 11 erstellt wurden und ob der Anbieter ein angemessenes Konformitätsbewertungsverfahren durchgeführt hat;

b) Bereithaltung — für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems — der Kontaktdaten des Anbieters, der den Bevollmächtigten benannt hat, eines Exemplars der in Artikel 47 genannten EU-Konformitätserklärung, der technischen Dokumentation und gegebenenfalls der von der notifizierten Stelle ausgestellten Bescheinigung für die zuständigen Behörden und die in Artikel 74 Absatz 10 genannten nationalen Behörden oder Stellen;

c) Übermittlung sämtlicher — auch der unter Buchstabe b dieses Unterabsatzes genannten — Informationen und Dokumentation, die erforderlich sind, um die Konformität eines Hochrisiko-KI-Systems mit den in Abschnitt 2 festgelegten Anforderungen nachzuweisen, an eine zuständige Behörde auf deren begründete Anfrage, einschließlich der Gewährung des Zugangs zu den vom Hochrisiko-KI-System automatisch erzeugten Protokollen gemäß Artikel 12 Absatz 1, soweit diese Protokolle der Kontrolle des Anbieters unterliegen;

d) Zusammenarbeit mit den zuständigen Behörden auf deren begründete Anfrage bei allen Maßnahmen, die Letztere im Zusammenhang mit dem

Hochrisiko-KI-System ergreifen, um insbesondere die von dem Hochrisiko-KI-System ausgehenden Risiken zu verringern und abzumildern;

e) gegebenenfalls die Einhaltung der Registrierungspflichten gemäß Artikel 49 Absatz 1 oder, falls die Registrierung vom Anbieter selbst vorgenommen wird, Sicherstellung der Richtigkeit der in Anhang VIII Abschnitt A Nummer 3 aufgeführten Informationen.

Mit dem Auftrag wird der Bevollmächtigte ermächtigt, neben oder anstelle des Anbieters als Ansprechpartner für die zuständigen Behörden in allen Fragen zu dienen, die die Gewährleistung der Einhaltung dieser Verordnung betreffen.

(4) Der Bevollmächtigte beendet den Auftrag, wenn er der Auffassung ist oder Grund zu der Annahme hat, dass der Anbieter gegen seine Pflichten gemäß dieser Verordnung verstößt. In diesem Fall informiert er unverzüglich die betreffende Marktüberwachungsbehörde und gegebenenfalls die betreffende notifizierte Stelle über die Beendigung des Auftrags und deren Gründe.

I. Worum geht es?

Artikel 22 regelt die Rolle von Bevollmächtigten für Anbieter von Hochrisiko-KI-Systemen, die ihren Sitz außerhalb der EU haben. Ziel ist es, sicherzustellen, dass es innerhalb der EU stets einen klaren Ansprechpartner gibt, der für die Einhaltung der KI-VO verantwortlich gemacht werden kann. Damit wird die Marktüberwachung erleichtert und die Rechtsdurchsetzung im Binnenmarkt abgesichert. Der Bevollmächtigte übernimmt dabei bestimmte Aufgaben und Pflichten, die den Behörden direkten Zugriff auf wichtige Unterlagen und Informationen ermöglichen.

II. Detailkommentar

A. Verpflichtung zur Benennung

- **Pflicht für Drittlandanbieter**: Anbieter, die nicht in der EU niedergelassen sind, müssen zwingend einen Bevollmächtigten in der EU benennen, bevor sie ihre Hochrisiko-KI-Systeme auf den Markt bringen dürfen.

- **Schriftliche Bestellung**: Die Bestellung muss schriftlich erfolgen und als klarer Auftrag ausgestaltet sein.

Beispiel: *Ein US-amerikanisches Unternehmen möchte ein KI-System für Bewerberauswahl in Deutschland vertreiben. Vor dem Markteintritt muss es eine in der EU ansässige juristische oder natürliche Person als Bevollmächtigten benennen.*

B. Aufgaben und Befugnisse des Bevollmächtigten

1. **Überprüfung von Unterlagen**: Der Bevollmächtigte muss prüfen, ob die EU-Konformitätserklärung und die technische Dokumentation erstellt wurden und ob das vorgeschriebene Konformitätsbewertungsverfahren durchgeführt wurde. Dies stellt sicher, dass die Mindestanforderungen erfüllt sind, bevor das Produkt in Verkehr gebracht wird.
2. **Bereithaltung von Unterlagen**: Der Bevollmächtigte muss bestimmte Dokumente – darunter Kontaktdaten des Anbieters, Konformitätserklärung, technische Dokumentation und Zertifikate – mindestens zehn Jahre lang aufbewahren und auf Anfrage den Behörden vorlegen.
3. **Informationsweitergabe**: Er muss den Behörden auf begründete Anfrage alle notwendigen Unterlagen übermitteln, auch Zugang zu automatisch erzeugten Protokollen des Hochrisiko-KI-Systems ermöglichen (soweit verfügbar).
4. **Zusammenarbeit mit Behörden**: Der Bevollmächtigte muss die zuständigen Stellen bei allen Maßnahmen unterstützen, insbesondere wenn Risiken durch das Hochrisiko-KI-System erkannt werden.
5. **Registrierungspflichten**: Sofern erforderlich, muss er die Registrierung des Hochrisiko-KI-Systems übernehmen oder deren Richtigkeit sicherstellen.

Beispiel: *Eine italienische Behörde verlangt nähere Informationen zur Risikobewertung eines KI-Systems. Der Bevollmächtigte des US-Herstellers muss die technische Dokumentation und Protokolle unverzüglich bereitstellen.*

C. Rolle als Ansprechpartner

- **Kontaktstelle für Behörden**: Der Bevollmächtigte tritt neben oder anstelle des Anbieters als Ansprechpartner für Behörden auf.
- **Praktische Bedeutung**: Dies sorgt für eine klare Kommunikationslinie und erleichtert die Durchsetzung der Verordnung.

D. Beendigung des Auftrags

- **Pflicht zur Beendigung**: Erkennt der Bevollmächtigte, dass der Anbieter gegen die Verordnung verstößt, muss er den Auftrag beenden.
- **Meldepflicht**: In diesem Fall muss er sofort die Marktüberwachungsbehörden und ggf die notifizierte Stelle informieren.

Beispiel*: Ein Bevollmächtigter stellt fest, dass ein Anbieter die technische Dokumentation manipuliert hat. Er beendet daraufhin den Auftrag und informiert die deutsche Marktüberwachungsbehörde.*

E. Besonderheiten

- **Schnittstelle zu Marktüberwachung**: Der Bevollmächtigte ist keine „Ersatzbehörde", sondern dient als Schnittstelle zwischen Anbieter und staatlicher Kontrolle.
- **Sanktionsrisiko für Anbieter**: Da der Bevollmächtigte verpflichtet ist, Verstöße zu melden, können Anbieter nicht darauf hoffen, dass Probleme „intern vertuscht" werden.
- **Systematische Stellung**: Artikel 22 steht in engem Zusammenhang mit den Vorschriften über Marktüberwachung und Konformitätsbewertung (Artikel 43 KI-VOff). Er schafft die organisatorische Voraussetzung, dass auch Anbieter außerhalb der EU denselben Pflichten unterliegen wie EU-Anbieter.

III. Zusammenfassung

Pflicht	Schriftliche Bestellung eines Bevollmächtigten vor Markteintritt
Aufgaben	Prüfung von Unterlagen, Aufbewahrung von Dokumenten, Informationsweitergabe, Zusammenarbeit mit Behörden, Registrierung
Ansprechpartner	Bevollmächtigter tritt neben/anstelle des Anbieters als Kontaktstelle für Behörden auf
Beendigung	Bevollmächtigter muss Auftrag beenden und Behörden informieren, wenn Anbieter gegen KI-VO verstößt
Zweck	Sicherstellung, dass auch Drittlandanbieter einen in der EU verantwortlichen Ansprechpartner haben

IV. Quellenverzeichnis

- Erwägungsgrund 82 KI-VO (EU) 2024/1689

Artikel 23 KI-VO

Pflichten der Einführer

(1) Bevor sie ein Hochrisiko-KI-System in Verkehr bringen, stellen die Einführer sicher, dass das System dieser Verordnung entspricht, indem sie überprüfen, ob

a) der Anbieter des Hochrisiko-KI-Systems das entsprechende Konformitätsbewertungsverfahren gemäß Artikel 43 durchgeführt hat;

b) der Anbieter die technische Dokumentation gemäß Artikel 11 und Anhang IV erstellt hat;

c) das System mit der erforderlichen CE-Kennzeichnung versehen ist und ihm die in Artikel 47 genannte EU-Konformitätserklärung und Betriebsanleitungen beigefügt sind;

d) der Anbieter einen Bevollmächtigten gemäß Artikel 22 Absatz 1 benannt hat.

(2) Hat ein Einführer hinreichenden Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht dieser Verordnung entspricht oder gefälscht ist oder diesem eine gefälschte Dokumentation beigefügt ist, so bringt er das System erst in Verkehr, nachdem dessen Konformität hergestellt wurde. Birgt das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 79 Absatz 1, so informiert der Einführer den Anbieter des Systems, die Bevollmächtigten und die Marktüberwachungsbehörden darüber.

(3) Die Einführer geben ihren Namen, ihren eingetragenen Handelsnamen oder ihre eingetragene Handelsmarke und die Anschrift, unter der sie in Bezug auf das Hochrisiko-KI-System kontaktiert werden können, auf der Verpackung oder gegebenenfalls in der beigefügten Dokumentation an.

(4) Solange sich ein Hochrisiko-KI-System in ihrer Verantwortung befindet, gewährleisten Einführer, dass — soweit zutreffend — die Lagerungs- oder Transportbedingungen seine Konformität mit den in Abschnitt 2 festgelegten Anforderungen nicht beeinträchtigen.

(5) Die Einführer halten für einen Zeitraum von zehn Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems ein Exemplar der von der notifizierten Stelle ausgestellten Bescheinigung sowie gegebenenfalls die Betriebsanleitungen und die in Artikel 47 genannte EU-Konformitätserklärung bereit.

(6) Die Einführer übermitteln den betreffenden nationalen Behörden auf deren begründete Anfrage sämtliche — auch die in Absatz 5 genannten — Informationen und Dokumentation, die erforderlich sind, um die Konformität des Hochrisiko-KI-Systems mit den in Abschnitt 2 festgelegten Anforderungen nachzuweisen, und zwar in einer Sprache, die für jene leicht verständlich ist. Zu diesem Zweck stellen sie auch sicher, dass diesen Behörden die technische Dokumentation zur Verfügung gestellt werden kann.

(7) Die Einführer arbeiten mit den betreffenden nationalen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit einem von den Einführern in Verkehr gebrachten Hochrisiko-KI-System ergreifen, um insbesondere die von diesem System ausgehenden Risiken zu verringern und abzumildern.

I. Worum geht es?

Dieser Artikel legt die Pflichten von Einführern fest, also von Unternehmen oder Personen, die ein Hochrisiko-KI-System aus einem Drittstaat in die EU einführen und hier auf den Markt bringen. Ziel ist es, sicherzustellen, dass nur solche Systeme in die EU gelangen, die die Vorgaben der KI-VO erfüllen. Einführer fungieren damit als Kontrollinstanz an der „Eingangsstelle“ zum Binnenmarkt.

II. Detailkommentar

A. Überprüfung vor dem Inverkehrbringen

- **Prüfungspflicht**: Einführer müssen vor dem Inverkehrbringen sicherstellen, dass der Anbieter eines Hochrisiko-KI-Systems alle notwendigen Schritte eingehalten hat (Konformitätsbewertung, technische Dokumentation, CE-Kennzeichnung, EU-Konformitätserklärung und Betriebsanleitung).
- **Bevollmächtigter**: Es muss ein Bevollmächtigter des Anbieters in der EU benannt sein, damit Behörden einen klaren Ansprechpartner haben.

B. Umgang mit Verdachtsfällen

- **Konformitätszweifel**: Hat der Einführer Grund zu der Annahme, dass ein System nicht den Vorgaben entspricht oder mit gefälschter Dokumentation versehen ist, darf er es nicht in Verkehr bringen, bevor die Konformität hergestellt ist.
- **Risikomeldung**: Wenn ein System ein Sicherheits- oder Gesundheitsrisiko birgt, muss der Einführer unverzüglich Anbieter, Bevollmächtigten und Marktüberwachungsbehörden informieren.

Beispiel: *Ein Einführer entdeckt, dass die technischen Unterlagen unvollständig sind und Zweifel an der Echtheit der CE-Kennzeichnung bestehen. Er darf das System nicht auf den Markt bringen und muss die Behörden informieren.*

C. Kennzeichnungspflichten

Einführer müssen ihre Kontaktdaten (Name, Handelsname/Marke, Anschrift) auf der Verpackung oder in der Dokumentation angeben. Damit ist klar nachvollziehbar, wer das System in die EU eingeführt hat.

D. Verantwortung für Lagerung und Transport

Einführer müssen sicherstellen, dass die Bedingungen bei Lagerung und Transport (zB Temperatur, Feuchtigkeit) die Konformität des Systems nicht beeinträchtigen.

Beispiel: *Ein KI-System wird per Schiff transportiert. Der Einführer muss darauf achten, dass die Lagerbedingungen keine Schäden verursachen, die die Sicherheit des Systems beeinträchtigen.*

E. Aufbewahrungs- und Dokumentationspflichten

Einführer müssen die von der notifizierten Stelle ausgestellten Bescheinigungen, Betriebsanleitungen und die EU-Konformitätserklärung zehn Jahre lang aufbewahren.

F. Zusammenarbeit mit Behörden

- **Informationspflicht**: Auf Anfrage müssen Einführer alle relevanten Unterlagen bereitstellen, in einer Sprache, die für die Behörden verständlich ist.
- **Kooperationspflicht**: Einführer müssen bei Maßnahmen der Behörden aktiv mitwirken, insbesondere wenn Risiken vom System ausgehen.

G. Besonderheiten

- **Rollenüberschneidung**: Die Akteure können hier mehrere Rollen gleichzeitig übernehmen, zB Einführer und Händler. In solchen Fällen müssen alle Pflichten zusammen erfüllt werden.
- **Sinn und Zweck**: Die Vorschriften sollen verhindern, dass unsichere oder nicht regelkonforme KI-Systeme über Einführer in den Binnenmarkt gelangen.

III. Zusammenfassung

Prüfung vor Inverkehrbringen	Kontrolle von Konformität, CE-Kennzeichnung, Dokumentation, Betriebsanleitung, Bevollmächtigtem
Umgang mit Verdachtsfällen	Kein Inverkehrbringen, Informationspflicht bei Risiken
Kennzeichnungspflichten	Angabe von Name, Marke, Anschrift des Einführers
Lagerung und Transport	Bedingungen dürfen Konformität nicht beeinträchtigen
Aufbewahrungspflicht	Dokumentation zehn Jahre lang aufbewahren
Zusammenarbeit mit Behörden	Unterlagen bereitstellen, Kooperationspflicht
Besonderheit	Mehrere Rollen können gleichzeitig erfüllt werden (zB Einführer + Händler)

IV. Quellenverzeichnis

- Erwägungsgrund 83 KI-VO (EU) 2024/1689

Artikel 24 KI-VO

Pflichten der Händler

(1) Bevor Händler ein Hochrisiko-KI-System auf dem Markt bereitstellen, überprüfen sie, ob es mit der erforderlichen CE-Kennzeichnung versehen ist, ob ihm eine Kopie der in Artikel 47 genannten EU-Konformitätserklärung und Betriebsanleitungen beigefügt sind und ob der Anbieter und gegebenenfalls der Einführer dieses Systems ihre in Artikel 16 Buchstaben b und c sowie Artikel 23 Absatz 3 festgelegten jeweiligen Pflichten erfüllt haben.

(2) Ist ein Händler der Auffassung oder hat er aufgrund von Informationen, die ihm zur Verfügung stehen, Grund zu der Annahme, dass ein Hochrisiko-KI-System nicht den Anforderungen in Abschnitt 2 entspricht, so stellt er das Hochrisiko-KI-System erst auf dem Markt bereit, nachdem die Konformität des Systems mit den Anforderungen hergestellt wurde. Birgt das Hochrisiko-IT-System zudem ein Risiko im Sinne des Artikels 79 Absatz 1, so informiert der Händler den Anbieter bzw. den Einführer des Systems darüber.

(3) Solange sich ein Hochrisiko-KI-System in ihrer Verantwortung befindet, gewährleisten Händler, dass — soweit zutreffend — die Lagerungs- oder Transportbedingungen die Konformität des Systems mit den in Abschnitt 2 festgelegten Anforderungen nicht beeinträchtigen.

(4) Ein Händler, der aufgrund von Informationen, die ihm zur Verfügung stehen, der Auffassung ist oder Grund zu der Annahme hat, dass ein von ihm auf dem Markt bereitgestelltes Hochrisiko-KI-System nicht den Anforderungen in Abschnitt 2 entspricht, ergreift die erforderlichen Korrekturmaßnahmen, um die Konformität dieses Systems mit diesen Anforderungen herzustellen, es zurückzunehmen oder zurückzurufen, oder er stellt sicher, dass der Anbieter, der Einführer oder gegebenenfalls jeder relevante Akteur diese Korrekturmaßnahmen ergreift. Birgt das Hochrisiko-KI-System ein Risiko im Sinne des Artikels 79 Absatz 1, so informiert der Händler unverzüglich den Anbieter bzw. den Einführer des Systems sowie die für das betroffene Hochrisiko-KI-System zuständigen Behörden und macht dabei ausführliche Angaben, insbesondere zur Nichtkonformität und zu bereits ergriffenen Korrekturmaßnahmen.

(5) Auf begründete Anfrage einer betreffenden zuständigen Behörde übermitteln die Händler eines Hochrisiko-KI-Systems dieser Behörde sämtliche Informationen und Dokumentation in Bezug auf ihre Maßnahmen

gemäß den Absätzen 1 bis 4, die erforderlich sind, um die Konformität dieses Systems mit den in Abschnitt 2 festgelegten Anforderungen nachzuweisen.

(6) Die Händler arbeiten mit den betreffenden zuständigen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit einem von den Händlern auf dem Markt bereitgestellten Hochrisiko-KI-System ergreifen, um insbesondere das von diesem System ausgehende Risiko zu verringern oder abzumildern.

I. Worum geht es?

Artikel 24 regelt die Pflichten von Händlern im Zusammenhang mit Hochrisiko-KI-Systemen. Händler sind Akteure in der Wertschöpfungskette, die diese Systeme an Kunden weiterverkaufen oder vertreiben, ohne sie selbst herzustellen. Ziel der Vorschrift ist es, die Produktsicherheit zu gewährleisten, indem Händler als zusätzliche Kontrollinstanz wirken. Sie dürfen nur solche Systeme in Verkehr bringen, die ordnungsgemäß geprüft und gekennzeichnet sind. Gleichzeitig müssen sie bei Auffälligkeiten aktiv werden und mit Behörden zusammenarbeiten.

II. Detailkommentar

A. Vor dem Inverkehrbringen

- **Prüfung der Unterlagen**: Händler müssen kontrollieren, ob das Hochrisiko-KI-System eine **CE-Kennzeichnung**, eine **EU-Konformitätserklärung** und eine **Betriebsanleitung** enthält. Dies dient der Sicherstellung, dass der Anbieter seine rechtlichen Pflichten erfüllt hat.
- **Pflichten der Vorlieferanten**: Zusätzlich müssen Händler überprüfen, ob Anbieter und gegebenenfalls Einführer ihre rechtlichen Pflichten erfüllt haben. Der Händler ist also nicht nur Verkäufer, sondern auch Kontrollinstanz.

B. Verdacht auf Nichtkonformität vor dem Verkauf

- **Handlungsstopp**: Erkennt ein Händler, dass ein System die Anforderungen nicht erfüllt, darf er es nicht verkaufen, bevor die Konformität hergestellt ist.
- **Meldepflicht**: Liegt zusätzlich ein Risiko für Gesundheit, Sicherheit oder Grundrechte vor, muss der Händler den Anbieter oder Einführer informieren.

Beispiel: *Ein Händler erhält Hinweise, dass ein Gesichtserkennungssystem zu hohe Fehlerquoten bei Minderheiten aufweist. Er darf es nicht weiterverkaufen und muss den Anbieter informieren.*

C. Verantwortung während Lagerung und Transport

Händler müssen sicherstellen, dass das System bei Lagerung und Transport nicht beschädigt wird oder seine Konformität verliert.

Beispiel: *Ein Händler lagert ein KI-System, das auf spezieller Hardware basiert, in feuchter Umgebung. Dadurch verliert das System seine Funktionsfähigkeit – dies wäre ein Verstoß.*

D. Maßnahmen nach dem Inverkehrbringen

- **Korrekturpflicht**: Stellt sich nach dem Verkauf heraus, dass ein System nicht konform ist, muss der Händler tätig werden – entweder durch Nachbesserung, Rücknahme oder Rückruf.
- **Informationspflicht**: Wenn zusätzlich ein Risiko für Nutzer oder Dritte besteht, muss der Händler den Anbieter, den Einführer und die zuständige Behörde informieren.

Beispiel: *Ein Händler verkauft ein KI-basiertes Kreditbewertungssystem. Nach Beschwerden stellt sich heraus, dass es diskriminierende Ergebnisse liefert. Der Händler muss es zurückrufen und die Behörden informieren.*

E. Zusammenarbeit mit Behörden

- **Auskunftspflicht**: Auf Anfrage müssen Händler alle relevanten Unterlagen und Informationen bereitstellen, die ihre Prüfungen und Maßnahmen belegen.
- **Kooperationspflicht**: Händler müssen mit Behörden zusammenarbeiten, insbesondere wenn Risiken minimiert oder abgestellt werden müssen.

.

F. Besonderheiten

- **Rollenüberschneidung**: Die Akteure können hier mehrere Rollen gleichzeitig übernehmen, zB Einführer und Händler. In solchen Fällen müssen alle Pflichten zusammen erfüllt werden.

III. Zusammenfassung

Vor dem Inverkehrbringen	Prüfung von CE-Kennzeichnung, EU-Konformitätserklärung, Betriebsanleitung und Pflichten der Vorlieferanten
Verdacht vor Verkauf	Kein Vertrieb bis zur Konformität, Informationspflicht bei Risiken
Lagerung und Transport	Bedingungen müssen die Konformität sicherstellen
Nach dem Verkauf	Korrekturmaßnahmen, Rücknahme oder Rückruf, Meldung an Behörden bei Risiken
Zusammenarbeit mit Behörden	Auskunftspflicht, Dokumentation vorlegen, aktive Kooperation
Besonderheit	Händler können zugleich Einführer sein und müssen dann die Pflichten beider Rollen erfüllen

IV. Quellenverzeichnis

- Erwägungsgrund 83 KI-VO (EU) 2024/1689

Artikel 25 KI-VO

Verantwortlichkeiten entlang der KI-Wertschöpfungskette

(1) In den folgenden Fällen gelten Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter eines Hochrisiko-KI-Systems für die Zwecke dieser Verordnung und unterliegen den Anbieterpflichten gemäß Artikel 16:

a) wenn sie ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System mit ihrem Namen oder ihrer Handelsmarke versehen, unbeschadet vertraglicher Vereinbarungen, die eine andere Aufteilung der Pflichten vorsehen;

b) wenn sie eine wesentliche Veränderung eines Hochrisiko-KI-Systems, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, so vornehmen, dass es weiterhin ein Hochrisiko-KI-System gemäß Artikel 6 bleibt;

c) wenn sie die Zweckbestimmung eines KI-Systems, einschließlich eines KI-Systems mit allgemeinem Verwendungszweck, das nicht als hochriskant eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändern, dass das betreffende KI-System zu einem Hochrisiko-KI-System im Sinne von Artikel 6 wird.

(2) Unter den in Absatz 1 genannten Umständen gilt der Anbieter, der das KI-System ursprünglich in Verkehr gebracht oder in Betrieb genommen hatte, nicht mehr als Anbieter dieses spezifischen KI-Systems für die Zwecke dieser Verordnung. Dieser Erstanbieter arbeitet eng mit neuen Anbietern zusammen, stellt die erforderlichen Informationen zur Verfügung und sorgt für den vernünftigerweise zu erwartenden technischen Zugang und sonstige Unterstützung, die für die Erfüllung der in dieser Verordnung festgelegten Pflichten, insbesondere in Bezug auf die Konformitätsbewertung von Hochrisiko-KI-Systemen, erforderlich sind. Dieser Absatz gilt nicht in Fällen, in denen der Erstanbieter eindeutig festgelegt hat, dass sein KI-System nicht in ein Hochrisiko-KI-System umgewandelt werden darf und daher nicht der Pflicht zur Übergabe der Dokumentation unterliegt.

(3) Im Falle von Hochrisiko-KI-Systemen, bei denen es sich um Sicherheitsbauteile von Produkten handelt, die unter die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, gilt der Produkthersteller als Anbieter des Hochrisiko-KI-Systems

und unterliegt in den beiden nachfolgenden Fällen den Pflichten nach Artikel 16:

a) Das Hochrisiko-KI-System wird zusammen mit dem Produkt unter dem Namen oder der Handelsmarke des Produktherstellers in Verkehr gebracht;

b) das Hochrisiko-KI-System wird unter dem Namen oder der Handelsmarke des Produktherstellers in Betrieb genommen, nachdem das Produkt in Verkehr gebracht wurde.

(4) Der Anbieter eines Hochrisiko-KI-Systems und der Dritte, der ein KI-System, Instrumente, Dienste, Komponenten oder Verfahren bereitstellt, die in einem Hochrisiko-KI-System verwendet oder integriert werden, legen in einer schriftlichen Vereinbarung die Informationen, die Fähigkeiten, den technischen Zugang und die sonstige Unterstützung nach dem allgemein anerkannten Stand der Technik fest, die erforderlich sind, damit der Anbieter des Hochrisiko-KI-Systems die in dieser Verordnung festgelegten Pflichten vollständig erfüllen kann. Dieser Absatz gilt nicht für Dritte, die Instrumente, Dienste, Verfahren oder Komponenten, bei denen es sich nicht um KI-Modelle mit allgemeinem Verwendungszweck handelt, im Rahmen einer freien und quelloffenen Lizenz öffentlich zugänglich machen.

Das Büro für Künstliche Intelligenz kann freiwillige Musterbedingungen für Verträge zwischen Anbietern von Hochrisiko-KI-Systemen und Dritten, die Instrumente, Dienste, Komponenten oder Verfahren bereitstellen, die für Hochrisiko-KI-Systeme verwendet oder in diese integriert werden, ausarbeiten und empfehlen. Bei der Ausarbeitung dieser freiwilligen Musterbedingungen berücksichtigt das Büro für Künstliche Intelligenz mögliche vertragliche Anforderungen, die in bestimmten Sektoren oder Geschäftsfällen gelten. Die freiwilligen Musterbedingungen werden veröffentlicht und sind kostenlos in einem leicht nutzbaren elektronischen Format verfügbar.

(5) Die Absätze 2 und 3 berühren nicht die Notwendigkeit, Rechte des geistigen Eigentums, vertrauliche Geschäftsinformationen und Geschäftsgeheimnisse im Einklang mit dem Unionsrecht und dem nationalen Recht zu achten und zu schützen.

I. Worum geht es?

Artikel 25 regelt die Verantwortlichkeiten verschiedener Akteure entlang der KI-Wertschöpfungskette. Es wird bestimmt, wann Händler, Einführer, Betreiber oder andere Dritte rechtlich so behandelt werden, als wären sie selbst Anbieter eines Hochrisiko-KI-Systems. Ziel ist es, Rechtssicherheit zu schaffen und sicherzustellen, dass jedes Hochrisiko-KI-System, unabhängig davon, wie es in Verkehr gebracht oder verändert wird, einen klar verantwortlichen Anbieter hat. Damit sollen Pflichtenumgehungen verhindert und eine faire Verteilung der Verantwortlichkeiten gewährleistet werden.

II. Detailkommentar

A. Neue Anbieter durch bestimmte Handlungen

1. Namens- oder Markenänderung:

Wer ein Hochrisiko-KI-System mit eigenem Namen oder Marke versieht, übernimmt automatisch die Anbieterrolle.

Beispiel: *Ein Händler verkauft ein KI-gestütztes Medizinprodukt unter seiner Eigenmarke. Er gilt rechtlich als Anbieter.*

2. Wesentliche Veränderung:

Wer ein bestehendes Hochrisiko-KI-System so verändert, dass es weiterhin hochriskant bleibt, wird ebenfalls Anbieter – mit der Folge, dass er alle Anbieterpflichten übernimmt.

Beispiel: *Ein Betreiber ändert die Algorithmen eines KI-Systems für Kreditwürdigkeitsprüfungen grundlegend. Er gilt danach als Anbieter.*

3. Änderung der Zweckbestimmung:

Wenn die Funktion so angepasst wird, dass ein zuvor nicht hochriskantes KI-System in den Hochrisiko-Bereich fällt, trägt der Ändernde die Anbieterpflichten.
Beispiel: *Eine einfache Sprach-KI wird zu einem System für*

Bewerberauswahl umfunktioniert. Sie fällt nun unter Hochrisiko und der Umprogrammierer ist Anbieter.

B. Rolle des ursprünglichen Anbieters

- **Ausscheiden als Anbieter**: Sobald ein Dritter das System verändert oder neu kennzeichnet, ist der ursprüngliche Anbieter für dieses konkrete System nicht mehr verantwortlich.
- **Kooperationspflicht**: Der ursprüngliche Anbieter muss jedoch Informationen, technischen Zugang und Unterstützung bereitstellen, damit der neue Anbieter seine Pflichten erfüllen kann.
- **Ausnahme**: Hat der ursprüngliche Anbieter ausdrücklich ausgeschlossen, dass sein System in ein Hochrisiko-KI-System umgewandelt werden darf, entfällt die Pflicht zur Zusammenarbeit.

C. Besondere Regel für Produkte mit Sicherheitsbauteilen

- **Produkthersteller als Anbieter**: Wenn ein Hochrisiko-KI-System ein Sicherheitsbauteil eines Produkts ist (zB in einem Auto oder einem Medizinprodukt), gilt der Produkthersteller automatisch als Anbieter, wenn das System zusammen mit dem Produkt unter dessen Namen/Marke in Verkehr gebracht oder in Betrieb genommen wird.

D. Zusammenarbeit mit Dritten

- **Vertragliche Regelung**: Anbieter und Dritte (zB Entwickler von Modulen oder Diensten) müssen schriftlich festhalten, welche Informationen und Unterstützung sie einander geben, um die Pflichten aus der KI-VO erfüllen zu können.
- **Open-Source-Ausnahme**: Wer Komponenten im Rahmen einer freien und quelloffenen Lizenz bereitstellt (sofern es keine KI-Modelle mit allgemeinem Verwendungszweck sind), ist von dieser Pflicht befreit.
- **Musterbedingungen**: Das Büro für Künstliche Intelligenz kann freiwillige Musterverträge veröffentlichen, die zur Vereinfachung dienen.

E. Schutz von Rechten

Alle Kooperations- und Informationspflichten müssen unter Wahrung von geistigem Eigentum, Geschäftsgeheimnissen und Vertraulichkeit erfolgen.

III. Zusammenfassung

Neue Anbieterrollen	Händler, Einführer, Betreiber oder Dritte können Anbieter werden, wenn sie ein System umbenennen, wesentlich verändern oder die Zweckbestimmung ändern.
Ursprünglicher Anbieter	Fällt weg, muss aber unterstützen, solange er eine Umwandlung in Hochrisiko-KI-System nicht ausgeschlossen hat.
Produkte mit Sicherheitsbauteilen	Produkthersteller gilt automatisch als Anbieter, wenn Produkt und KI-System unter gemeinsamen Namen/Marke in Verkehr gebracht oder in Betrieb genommen wird.
Zusammenarbeit mit Dritten	Schriftliche Vereinbarungen über Unterstützung und Zugang sind Pflicht. Open-Source (außer GPAI-Modelle) ist ausgenommen.
Schutz von Rechten	Geistiges Eigentum und Geschäftsgeheimnisse sind zu wahren.

IV. Quellenverzeichnis

- Erwägungsgründe 83–90 KI-VO (EU) 2024/1689

Artikel 26 KI-VO

Pflichten der Betreiber von Hochrisiko-KI-Systemen

(1) Die Betreiber von Hochrisiko-KI-Systemen treffen geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass sie solche Systeme entsprechend der den Systemen beigefügten Betriebsanleitungen und gemäß den Absätzen 3 und 6 verwenden.

(2) Die Betreiber übertragen natürlichen Personen, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, die menschliche Aufsicht und lassen ihnen die erforderliche Unterstützung zukommen.

(3) Die Pflichten nach den Absätzen 1 und 2 lassen sonstige Pflichten der Betreiber nach Unionsrecht oder nationalem Recht sowie die Freiheit der Betreiber bei der Organisation ihrer eigenen Ressourcen und Tätigkeiten zur Wahrnehmung der vom Anbieter angegebenen Maßnahmen der menschlichen Aufsicht unberührt.

(4) Unbeschadet der Absätze 1 und 2 und soweit die Eingabedaten ihrer Kontrolle unterliegen, sorgen die Betreiber dafür, dass die Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen und ausreichend repräsentativ sind.

(5) Die Betreiber überwachen den Betrieb des Hochrisiko-KI-Systems anhand der Betriebsanleitung und informieren gegebenenfalls die Anbieter gemäß Artikel 72. Haben Betreiber Grund zu der Annahme, dass die Verwendung gemäß der Betriebsanleitung dazu führen kann, dass dieses Hochrisiko-KI-System ein Risiko im Sinne des Artikels 79 Absatz 1 birgt, so informieren sie unverzüglich den Anbieter oder Händler und die zuständige Marktüberwachungsbehörde und setzen die Verwendung dieses Systems aus. Haben die Betreiber einen schwerwiegenden Vorfall festgestellt, informieren sie auch unverzüglich zuerst den Anbieter und dann den Einführer oder Händler und die zuständigen Marktüberwachungsbehörden über diesen Vorfall. Kann der Betreiber den Anbieter nicht erreichen, so gilt Artikel 73 entsprechend. Diese Pflicht gilt nicht für sensible operative Daten von Betreibern von KI-Systemen, die Strafverfolgungsbehörden sind.

Bei Betreibern, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union über Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung, unterliegen, gilt die in Unterabsatz 1 festgelegte Überwachungspflicht als

erfüllt, wenn die Vorschriften über Regelungen, Verfahren oder Mechanismen der internen Unternehmensführung gemäß einschlägigem Recht über Finanzdienstleistungen eingehalten werden.

(6) Betreiber von Hochrisiko-KI-Systemen bewahren die von ihrem Hochrisiko-KI-System automatisch erzeugten Protokolle, soweit diese Protokolle ihrer Kontrolle unterliegen, für einen der Zweckbestimmung des Hochrisiko-KI-Systems angemessenen Zeitraum von mindestens sechs Monaten auf, sofern im geltenden Unionsrecht, insbesondere im Unionsrecht über den Schutz personenbezogener Daten, oder im geltenden nationalen Recht nichts anderes bestimmt ist.

Betreiber, die Finanzinstitute sind und gemäß den Rechtsvorschriften der Union über Finanzdienstleistungen Anforderungen in Bezug auf ihre Regelungen oder Verfahren der internen Unternehmensführung unterliegen, bewahren die Protokolle als Teil der gemäß einschlägigem Unionsecht über Finanzdienstleistungen aufzubewahrenden Dokumentation auf.

(7) Vor der Inbetriebnahme oder Verwendung eines Hochrisiko-KI-Systems am Arbeitsplatz informieren Betreiber, die Arbeitgeber sind, die Arbeitnehmervertreter und die betroffenen Arbeitnehmer darüber, dass sie der Verwendung des Hochrisiko-KI-Systems unterliegen werden. Diese Informationen werden gegebenenfalls im Einklang mit den Vorschriften und Gepflogenheiten auf Unionsebene und nationaler Ebene in Bezug auf die Unterrichtung der Arbeitnehmer und ihrer Vertreter bereitgestellt.

(8) Betreiber von Hochrisiko-KI-Systemen, bei denen es sich um Organe, Einrichtungen oder sonstige Stellen der Union handelt, müssen den Registrierungspflichten gemäß Artikel 49 nachkommen. Stellen diese Betreiber fest, dass das Hochrisiko-KI-System, dessen Verwendung sie planen, nicht in der in Artikel 71 genannten EU-Datenbank registriert wurde, sehen sie von der Verwendung dieses Systems ab und informieren den Anbieter oder den Händler.

(9) Die Betreiber von Hochrisiko-KI-Systemen verwenden gegebenenfalls die gemäß Artikel 13 der vorliegenden Verordnung bereitgestellten Informationen, um ihrer Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 nachzukommen.

(10) Unbeschadet der Richtlinie (EU) 2016/680 beantragt der Betreiber eines Hochrisiko-KI-Systems zur nachträglichen biometrischen

Fernfernidentifizierung im Rahmen von Ermittlungen zur gezielten Suche einer Person, die der Begehung einer Straftat verdächtigt wird oder aufgrund einer solchen verurteilt wurde, vorab oder unverzüglich, spätestens jedoch binnen 48 Stunden bei einer Justizbehörde oder einer Verwaltungsbehörde, deren Entscheidung bindend ist und einer justiziellen Überprüfung unterliegt, die Genehmigung für die Nutzung dieses Systems, es sei denn, es wird zur erstmaligen Identifizierung eines potenziellen Verdächtigen auf der Grundlage objektiver und nachprüfbarer Tatsachen, die in unmittelbarem Zusammenhang mit der Straftat stehen, verwendet. Jede Verwendung ist auf das für die Ermittlung einer bestimmten Straftat unbedingt erforderliche Maß zu beschränken.

Wird die gemäß Unterabsatz 1 beantragte Genehmigung abgelehnt, so wird die Verwendung des mit dieser beantragten Genehmigung verbundenen Systems zur nachträglichen biometrischen Fernidentifizierung mit sofortiger Wirkung eingestellt und werden die personenbezogenen Daten, die im Zusammenhang mit der Verwendung des Hochrisiko-KI-Systems stehen, für die die Genehmigung beantragt wurde, gelöscht.

In keinem Fall darf ein solches Hochrisiko-KI-System zur nachträglichen biometrischen Fernidentifizierung zu Strafverfolgungszwecken in nicht zielgerichteter Weise und ohne jeglichen Zusammenhang mit einer Straftat, einem Strafverfahren, einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr einer Straftat oder der Suche nach einer bestimmten vermissten Person verwendet werden. Es muss sichergestellt werden, dass die Strafverfolgungsbehörden keine ausschließlich auf der Grundlage der Ausgabe solcher Systeme zur nachträglichen biometrischen Fernidentifizierung beruhende Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, treffen.

Dieser Absatz gilt unbeschadet des Artikels 9 der Verordnung (EU) 2016/679 und des Artikels 10 der Richtlinie (EU) 2016/680 für die Verarbeitung biometrischer Daten.

Unabhängig vom Zweck oder Betreiber wird jede Verwendung solcher Hochrisiko-KI-Systeme in der einschlägigen Polizeiakte dokumentiert und der zuständigen Marktüberwachungsbehörde und der nationalen Datenschutzbehörde auf Anfrage zur Verfügung gestellt, wovon die Offenlegung sensibler operativer Daten im Zusammenhang mit der Strafverfolgung ausgenommen ist. Dieser Unterabsatz berührt nicht die den

Aufsichtsbehörden durch die Richtlinie (EU) 2016/680 übertragenen Befugnisse.

Die Betreiber legen den zuständigen Marktüberwachungsbehörden und den nationalen Datenschutzbehörden Jahresberichte über ihre Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung vor, wovon die Offenlegung sensibler operativer Daten im Zusammenhang mit der Strafverfolgung ausgenommen ist. Die Berichte können eine Zusammenfassung sein, damit sie mehr als einen Einsatz abdecken.

Die Mitgliedstaaten können im Einklang mit dem Unionsrecht strengere Rechtsvorschriften für die Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung erlassen.

(11) Unbeschadet des Artikels 50 der vorliegenden Verordnung informieren die Betreiber der in Anhang III aufgeführten Hochrisiko-KI-Systeme, die natürliche Personen betreffende Entscheidungen treffen oder bei solchen Entscheidungen Unterstützung leisten, die natürlichen Personen darüber, dass sie der Verwendung des Hochrisiko-KI-Systems unterliegen. Für Hochrisiko-KI-Systeme, die zu Strafverfolgungszwecken verwendet werden, gilt Artikel 13 der Richtlinie (EU) 2016/680.

(12) Die Betreiber arbeiten mit den zuständigen Behörden bei allen Maßnahmen zusammen, die diese Behörden im Zusammenhang mit dem Hochrisiko-KI-System zur Umsetzung dieser Verordnung ergreifen.

I. Worum geht es?

Artikel 26 legt die Pflichten der Betreiber von Hochrisiko-KI-Systemen fest. Während sich die Pflichten der Anbieter auf die Entwicklung und Bereitstellung solcher Systeme konzentrieren, geht es hier um die Verwendung in der Praxis. Der Artikel soll sicherstellen, dass KI-Systeme nicht nur technisch korrekt entwickelt, sondern auch sicher, verantwortungsvoll und im Einklang mit Grundrechten genutzt werden. Er verpflichtet die Betreiber insbesondere zu korrekter Anwendung, Überwachung, Protokollierung und zur Information der betroffenen Personen.

II. Detailkommentar

A. Ordnungsgemäße Nutzung

- **Technische und organisatorische Maßnahmen**: Betreiber müssen sicherstellen, dass sie das KI-System so nutzen, wie es in den Betriebsanleitungen vorgesehen ist.
- **Ziel**: Missbrauch oder fehlerhafte Anwendung soll verhindert werden.

Beispiel: *Ein Krankenhaus setzt ein KI-System zur Diagnoseunterstützung ein. Es darf die KI nicht außerhalb der vorgesehenen medizinischen Bereiche nutzen, etwa für Personalentscheidungen.*

B. Menschliche Aufsicht

- **Kompetentes Personal**: Betreiber müssen natürliche Personen einsetzen, die ausreichend geschult und befugt sind.
- **Unterstützungspflicht**: Diese Personen müssen die nötigen Informationen und Hilfsmittel erhalten, um ihre Aufsichtspflicht tatsächlich wahrnehmen zu können.

Beispiel: *Ein Kreditinstitut darf KI-gestützte Bonitätsprüfungen nicht völlig automatisch laufen lassen, sondern muss qualifiziertes Personal einsetzen, das die Ergebnisse überwacht und bewerten kann.*

C. Eingabedaten

- **Qualität der Daten**: Betreiber sind verantwortlich, dass die verwendeten Daten geeignet, zweckbezogen und repräsentativ sind, soweit sie dies kontrollieren können.
- **Ziel**: Verzerrungen und Diskriminierungen sollen vermieden werden.

Beispiel: *Ein KI-System zur Bewerberauswahl darf nicht ausschließlich Daten aus einer homogenen Gruppe nutzen (sofern diese in der Realität heterogen ist), da sonst die Ergebnisse verzerrt wären.*

D. Überwachung und Meldung

- **Pflicht zur Beobachtung**: Der Betrieb des Systems muss regelmäßig überwacht werden.
- **Meldepflichten**: Treten schwerwiegende Vorfälle oder Risiken auf, müssen Betreiber unverzüglich Anbieter, Händler und Behörden informieren.
- **Aussetzung der Nutzung**: Besteht ein ernsthaftes Risiko, muss der Betrieb gestoppt werden.

Beispiel: *Stellt ein Betreiber fest, dass eine KI im Straßenverkehr plötzlich fehlerhafte Erkennungen liefert, muss er das System sofort außer Betrieb nehmen und melden.*

E. Protokollierung

- **Aufbewahrungspflicht**: Betreiber müssen automatisch erzeugte Protokolle mindestens sechs Monate lang speichern.
- **Besonderheit Finanzinstitute**: Für Banken und Versicherungen gelten teils strengere Aufbewahrungspflichten nach EU-Finanzrecht.

Beispiel: *Ein Krankenhaus speichert die Systemprotokolle, die anzeigen, welche Daten die KI bei einer Diagnoseentscheidung verarbeitet hat.*

F. Arbeitnehmerrechte

- **Informationspflicht**: Vor der Einführung am Arbeitsplatz müssen Arbeitnehmer und ihre Vertreter informiert werden.
- **Ziel**: Transparenz und Schutz der Arbeitnehmer.

Beispiel: *Ein Logistikunternehmen darf ein KI-gestütztes Schichtplanungsprogramm nur nach vorheriger Information der Belegschaft einsetzen.*

G. Registrierungspflichten öffentlicher Stellen

- **EU-Organe und Einrichtungen**: Müssen prüfen, ob das System in der EU-Datenbank registriert ist. Ist dies nicht der Fall, darf das System nicht genutzt werden.

H. Datenschutzbezug

- **Verwendung von Informationspflichten**: Betreiber können die nach Artikel 13 KI-VObereitgestellten Angaben nutzen, um Datenschutz-Folgenabschätzungen vorzunehmen.

I. Besondere Vorschriften zur biometrischen Fernidentifizierung

- **Strenge Voraussetzungen**: Nutzung nur mit Genehmigung einer Justiz- oder Verwaltungsbehörde vorab oder spätestens innerhalb von 48 Stunden.
- **Verbot der willkürlichen Nutzung**: Eine anlasslose Massenüberwachung ist ausgeschlossen.
- **Zusätzliche Schutzmechanismen**: Dokumentationspflichten und jährliche Berichte an Aufsichtsbehörden.

Beispiel: *Die Polizei darf ein KI-System zur nachträglichen Gesichtserkennung nur bei einer konkreten Straftat und mit behördlicher Genehmigung einsetzen.*

J. Unterrichtung natürlicher Personen

- **Transparenzpflicht**: Personen müssen informiert werden, wenn Entscheidungen über sie mithilfe eines Hochrisiko-KI-Systems getroffen oder unterstützt werden.

Beispiel: *Ein Bewerber hat Anspruch darauf zu erfahren, dass seine Bewerbung durch ein KI-System vorbewertet wurde.*

K. Zusammenarbeit mit Behörden

- **Kooperationspflicht**: Betreiber müssen mit Aufsichts- und Marktüberwachungsbehörden kooperieren, zB bei Prüfungen oder Nachfragen.

III. Zusammenfassung

Nutzung	Anwendung gemäß Betriebsanleitung und organisatorische Sicherungen
Aufsicht	Einsatz geschulter und befugter Personen
Daten	Geeignet, zweckbezogen, repräsentativ
Überwachung	Laufende Beobachtung, Meldung und ggf. Aussetzung des Betriebs
Protokolle	Speicherung für mindestens sechs Monate
Arbeitnehmer	Information der Beschäftigten und ihrer Vertreter
Öffentliche Stellen	Prüfung auf Registrierung in EU-Datenbank
Datenschutz	Unterstützung bei Folgenabschätzung
Biometrische Systeme	Nutzung nur mit Genehmigung, strenge Beschränkungen
Transparenz	Information betroffener Personen

IV. Quellenverzeichnis

- Erwägungsgründe 91-95 KI-VO (EU) 2024/1689

Artikel 27 KI-VO

Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme

(1) Vor der Inbetriebnahme eines Hochrisiko-KI-Systems gemäß Artikel 6 Absatz 2 — mit Ausnahme von Hochrisiko-KI-Systemen, die in dem in Anhang III Nummer 2 aufgeführten Bereich verwendet werden sollen — führen Betreiber, bei denen es sich um Einrichtungen des öffentlichen Rechts oder private Einrichtungen, die öffentliche Dienste erbringen, handelt, und Betreiber von Hochrisiko-KI-Systemen gemäß Anhang III Nummer 5 Buchstaben b und c eine Abschätzung der Auswirkungen, die die Verwendung eines solchen Systems auf die Grundrechte haben kann, durch. Zu diesem Zweck führen die Betreiber eine Abschätzung durch, die Folgendes umfasst:

a) eine Beschreibung der Verfahren des Betreibers, bei denen das Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung verwendet wird;

b) eine Beschreibung des Zeitraums und der Häufigkeit, innerhalb dessen bzw. mit der jedes Hochrisiko-KI-System verwendet werden soll;

c) die Kategorien der natürlichen Personen und Personengruppen, die von seiner Verwendung im spezifischen Kontext betroffen sein könnten;

d) die spezifischen Schadensrisiken, die sich auf die gemäß Buchstabe c dieses Absatzes ermittelten Kategorien natürlicher Personen oder Personengruppen auswirken könnten, unter Berücksichtigung der vom Anbieter gemäß Artikel 13 bereitgestellten Informationen;

e) eine Beschreibung der Umsetzung von Maßnahmen der menschlichen Aufsicht entsprechend den Betriebsanleitungen;

f) die Maßnahmen, die im Falle des Eintretens dieser Risiken zu ergreifen sind, einschließlich der Regelungen für die interne Unternehmensführung und Beschwerdemechanismen.

(2) Die in Absatz 1 festgelegte Pflicht gilt für die erste Verwendung eines Hochrisiko-KI-Systems. Der Betreiber kann sich in ähnlichen Fällen auf zuvor durchgeführte Grundrechte-Folgenabschätzungen oder bereits vorhandene Folgenabschätzungen, die vom Anbieter durchgeführt wurden, stützen. Gelangt der Betreiber während der Verwendung des Hochrisiko-KI-Systems zur Auffassung, dass sich eines der in Absatz 1 aufgeführten Elemente geändert hat oder nicht mehr auf dem neuesten Stand ist, so

unternimmt der Betreiber die erforderlichen Schritte, um die Informationen zu aktualisieren.

(3) Sobald die Abschätzung gemäß Absatz 1 des vorliegenden Artikels durchgeführt wurde, teilt der Betreiber der Marktüberwachungsbehörde ihre Ergebnisse mit, indem er das ausgefüllte, in Absatz 5 des vorliegenden Artikels genannte Muster als Teil der Mitteilung übermittelt. In dem in Artikel 46 Absatz 1 genannten Fall können die Betreiber von der Mitteilungspflicht befreit werden.

(4) Wird eine der in diesem Artikel festgelegten Pflichten bereits infolge einer gemäß Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 durchgeführten Datenschutz-Folgenabschätzung erfüllt, so ergänzt die Grundrechte-Folgenabschätzung gemäß Absatz 1 des vorliegenden Artikels diese Datenschutz-Folgenabschätzung.

(5) Das Büro für Künstliche Intelligenz arbeitet ein Muster für einen Fragebogen — auch mithilfe eines automatisierten Instruments — aus, um die Betreiber in die Lage zu versetzen, ihren Pflichten gemäß diesem Artikel in vereinfachter Weise nachzukommen.

I. Worum geht es?

Artikel 27 regelt die Pflicht zur Grundrechte-Folgenabschätzung (GRFA) vor dem Einsatz bestimmter Hochrisiko-KI-Systeme. Ziel ist es, sicherzustellen, dass bei der Verwendung von KI die Grundrechte natürlicher Personen (zB Datenschutz, Gleichbehandlung, Schutz vor Diskriminierung) gewahrt bleiben. Die Vorschrift verpflichtet insbesondere öffentliche Einrichtungen sowie private Betreiber öffentlicher Dienste dazu, vor der erstmaligen Nutzung eines Hochrisiko-KI-Systems die möglichen Auswirkungen auf betroffene Personen zu prüfen. Dadurch soll vorausschauend erkannt werden, welche Risiken bestehen und wie diese durch organisatorische und technische Maßnahmen gemindert werden können.

II. Detailkommentar

A. Anwendungsbereich

- **Betroffene Betreiber**: Öffentliche Einrichtungen und private Einrichtungen, die öffentliche Dienste erbringen (zB Krankenhäuser, Schulen, Sozialdienste), sowie bestimmte Betreiber aus dem Finanzsektor (Banken, Versicherungen).
- **Ausnahme**: Hochrisiko-KI-Systeme im Bereich kritische Infrastruktur (Anhang III KI-VO Nr 2) sind ausgenommen.
- **Zeitpunkt**: Die Folgenabschätzung muss vor der ersten Inbetriebnahme erfolgen.

Beispiel: *Eine Gemeindeplant, ein KI-System zur automatisierten Vergabe von Wohnraum einzusetzen. Vor der Einführung muss sie prüfen, ob die Auswahlprozesse zu Diskriminierungen bestimmter Personengruppen führen könnten.*

B. Inhalt der Folgenabschätzung

Der Artikel nennt sechs Pflichtinhalte:

1. **Verfahrensbeschreibung**: Darstellung, wie das KI-System im Einklang mit seiner Zweckbestimmung eingesetzt wird.
2. **Zeit und Häufigkeit**: Angabe, wann und wie oft das System verwendet werden soll.
3. **Betroffene Personen**: Identifizierung der Kategorien natürlicher Personen oder Gruppen, die betroffen sein können.
4. **Risikoanalyse**: Darstellung möglicher Schäden für diese Personen, unter Einbeziehung der Anbieterinformationen.
5. **Menschliche Aufsicht**: Beschreibung, wie menschliche Kontrolle umgesetzt wird.
6. **Risikomaßnahmen**: Benennung von Vorkehrungen bei Schadenseintritt, inklusive interner Governance und Beschwerdemechanismen.

C. Aktualisierungspflichten

- **Erstbewertung**: Pflicht gilt für die erste Nutzung.
- **Wiederverwendung**: Frühere GRFA kann bei ähnlichen Fällen herangezogen werden.
- **Aktualisierung**: Wenn sich wesentliche Umstände ändern (zB neue Risikogruppen, andere Nutzungshäufigkeit), muss die Folgenabschätzung angepasst werden.

Beispiel: *Ein Krankenhaus nutzt ein KI-Diagnosetool zunächst in einer Abteilung. Wird es später auch in weiteren Fachbereichen eingesetzt, muss die GRFA überprüft und ggf angepasst werden.*

D. Verhältnis zu Datenschutz-Folgenabschätzung

Existiert bereits eine Datenschutz-Folgenabschätzung (nach DSGVO), wird diese durch die Grundrechte-Folgenabschätzung ergänzt. Sie ersetzt diese nicht, da der Schutzbereich breiter ist.

E. Mitteilungspflichten

- **Übermittlung**: Ergebnisse der GRFA müssen der Marktüberwachungsbehörde mitgeteilt werden.
- **Formular**: Das Büro für Künstliche Intelligenz entwickelt dafür ein standardisiertes Muster, ggf auch digital.
- **Ausnahme**: In bestimmten Fällen (Artikel 46 KI-VOAbsatz 1) entfällt die Mitteilungspflicht.

F. Beteiligung von Interessenträgern

Betreiber sollen ggf Betroffenenvertreter, unabhängige Experten oder zivilgesellschaftliche Organisationen einbeziehen, um die Qualität der Bewertung zu erhöhen. Dies ist allerdings nur eine Empfehlung und nicht rechtlich verpflichtend.

III. Zusammenfassung

Betroffene Betreiber	Öffentliche Einrichtungen, private Anbieter öffentlicher Dienste, Banken, Versicherungen
Zeitpunkt	Vor der ersten Inbetriebnahme
Inhalt	Verfahren, Zeit/Häufigkeit, Betroffene, Risiken, Aufsicht, Maßnahmen
Aktualisierung	Bei wesentlichen Änderungen erforderlich
Beziehung zu DSGVO	Ergänzt Datenschutz-Folgenabschätzung
Mitteilung	Ergebnisse an Marktüberwachungsbehörde, Formular durch KI-Büro
Besonderheit	Beteiligung von Betroffenenvertretern möglich

IV. Quellenverzeichnis

- Erwägungsgrund 96 KI-VO (EU) 2024/1689

Artikel 28 KI-VO

Notifizierende Behörden

(1) Jeder Mitgliedstaat sorgt für die Benennung oder Schaffung mindestens einer notifizierenden Behörde, die für die Einrichtung und Durchführung der erforderlichen Verfahren zur Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen und für deren Überwachung zuständig ist. Diese Verfahren werden in Zusammenarbeit zwischen den notifizierenden Behörden aller Mitgliedstaaten entwickelt.

(2) Die Mitgliedstaaten können entscheiden, dass die Bewertung und Überwachung nach Absatz 1 von einer nationalen Akkreditierungsstelle im Sinne und gemäß der Verordnung (EG) Nr 765/2008 durchzuführen ist.

(3) Notifizierende Behörden werden so eingerichtet, organisiert und geführt, dass jegliche Interessenkonflikte mit Konformitätsbewertungsstellen vermieden werden und die Objektivität und die Unparteilichkeit ihrer Tätigkeiten gewährleistet sind.

(4) Notifizierende Behörden werden so organisiert, dass Entscheidungen über die Notifizierung von Konformitätsbewertungsstellen von kompetenten Personen getroffen werden, die nicht mit den Personen identisch sind, die die Bewertung dieser Stellen durchgeführt haben.

(5) Notifizierende Behörden dürfen weder Tätigkeiten, die Konformitätsbewertungsstellen durchführen, noch Beratungsleistungen auf einer gewerblichen oder wettbewerblichen Basis anbieten oder erbringen.

(6) Notifizierende Behörden gewährleisten gemäß Artikel 78 die Vertraulichkeit der von ihnen erlangten Informationen.

(7) Notifizierende Behörden verfügen über eine angemessene Anzahl kompetenter Mitarbeiter, sodass sie ihre Aufgaben ordnungsgemäß wahrnehmen können. Die kompetenten Mitarbeiter verfügen — wo erforderlich — über das für ihre Funktion erforderliche Fachwissen in Bereichen wie Informationstechnologie sowie KI und Recht, einschließlich der Überwachung der Grundrechte.

I. Worum geht es?

Artikel 28 der KI-VO regelt, welche Behörden in den Mitgliedstaaten dafür zuständig sind, sogenannte Konformitätsbewertungsstellen zu „notifizieren“ – also offiziell zu benennen und zu überwachen. Diese Bewertungsstellen prüfen, ob KI-Systeme den Anforderungen der Verordnung entsprechen. Die notifizierenden Behörden sorgen dafür, dass diese Prüfstellen unabhängig, kompetent und unparteiisch arbeiten. Jeder Mitgliedstaat muss mindestens eine solche notifizierende Behörde haben. Die Anforderungen an deren Unabhängigkeit, Organisation und Kompetenz sind klar geregelt, um Vertrauen in das System der Überwachung und Zertifizierung von KI-Anwendungen zu schaffen.

II. Detailkommentar

A. Aufgaben und Stellung der Notifizierenden Behörde

1. Benennung und Überwachung

- Die Behörde benennt, überprüft und meldet die Konformitätsbewertungsstellen der EU.
- Sie überwacht diese Stellen laufend und sorgt dafür, dass sie den Anforderungen der KI-VO entsprechen.

2. Verfahren und Zusammenarbeit

- Die notwendigen Verfahren werden gemeinsam mit den anderen Mitgliedstaaten abgestimmt.
- Das Ziel ist eine europaweit vergleichbare und koordinierte Praxis.

3. Möglichkeit zur Nutzung von Akkreditierungsstellen

- Die Mitgliedstaaten dürfen die Aufgaben der Bewertung und Überwachung auch einer nationalen Akkreditierungsstelle übertragen, wie sie in der EU-Akkreditierungsverordnung (Verordnung EG Nr 765/2008) geregelt ist.

B. Anforderungen an die Organisation und Unabhängigkeit

1. Vermeidung von Interessenkonflikten

- Die notifizierende Behörde muss so aufgebaut sein, dass keine Interessenkonflikte mit den Prüfstellen entstehen.
- Sie darf keine eigenen wirtschaftlichen Interessen an den zu prüfenden Stellen haben.

Beispiel: *Ein Mitgliedstaat benennt das nationale Amt für Produktsicherheit als notifizierende Behörde. Dieses Amt prüft regelmäßig, ob neue KI-Prüfstellen wirklich unabhängig sind und die technischen Vorgaben erfüllen. Für die Bewertung wird eine externe Expertengruppe hinzugezogen, um Interessenkonflikte zu vermeiden.*

2. Getrennte Verantwortlichkeiten

Personen, die über die Benennung entscheiden, dürfen nicht diejenigen sein, die die Stelle bewertet haben.

Beispiel: *Ein Mitarbeiter, der eine Prüfstelle bewertet hat, darf nicht auch über deren offizielle Notifizierung entscheiden. Dadurch werden unabhängige Entscheidungen sichergestellt.*

3. Beschränkungen bei Dienstleistungen

Die Behörde darf selbst keine Tätigkeiten anbieten, die auch Konformitätsbewertungsstellen anbieten.

C. Vertraulichkeit und Fachkompetenz

1. Schutz vertraulicher Informationen

- Die Behörde ist zur Verschwiegenheit verpflichtet.

2. Fachliche Anforderungen

- Die Behörde muss ausreichend und qualifiziertes Personal haben.

- Fachkenntnisse sind etwa in IT, KI und Recht erforderlich.

D. Besonderheiten

- **Flexibilität für Mitgliedstaaten**: Jeder Mitgliedstaat kann entscheiden, wie er die Behörde organisatorisch einbettet – zB als Teil eines Ministeriums oder als eigenständige Einrichtung.
- **Zusammenarbeit auf EU-Ebene**: Durch die enge Abstimmung wird verhindert, dass es zu nationalen Alleingängen kommt und ein einheitliches Schutzniveau gewährleistet ist.
- **Transparenz**: Die Anforderungen an Unabhängigkeit und Objektivität sind zentral, um das Vertrauen der Öffentlichkeit in das Prüf- und Überwachungssystem zu sichern.

Beispiel: *Eine nationale Akkreditierungsstelle übernimmt die Überwachung. Sie sorgt dafür, dass alle KI-Konformitätsprüfstellen die Vorgaben der KI-VO erfüllen und veröffentlicht jährlich einen Bericht über die Überwachungsergebnisse.*

III. Zusammenfassung

Notifizierende Behörde	Mindestens eine pro Mitgliedstaat, Benennung und Überwachung der Prüfstellen
Zusammenarbeit	Verfahren werden zwischen allen Mitgliedstaaten abgestimmt
Nutzung von Akkreditierungsstellen	Bewertung und Überwachung können diesen übertragen werden
Unabhängigkeit und Objektivität	Strenge Vorgaben zur Vermeidung von Interessenkonflikten und zu getrennten Verantwortlichkeiten
Vertraulichkeit und Fachkompetenz	Verschwiegenheitspflicht und qualifiziertes Personal mit speziellem Fachwissen
Flexibilität	Mitgliedstaaten können die Behörde organisatorisch frei gestalten

IV. Quellenverzeichnis

- Erwägungsgründe 153, 154 KI-VO (EU) 2024/1689

Artikel 29 KI-VO

Antrag einer Konformitätsbewertungsstelle auf Notifizierung

(1) Konformitätsbewertungsstellen beantragen ihre Notifizierung bei der notifizierenden Behörde des Mitgliedstaats, in dem sie niedergelassen sind.

(2) Dem Antrag auf Notifizierung legen sie eine Beschreibung der Konformitätsbewertungstätigkeiten, des bzw. der Konformitätsbewertungsmodule und der Artikel der KI-Systeme, für die diese Konformitätsbewertungsstelle Kompetenz beansprucht, sowie, falls vorhanden, eine Akkreditierungsurkunde bei, die von einer nationalen Akkreditierungsstelle ausgestellt wurde und in der bescheinigt wird, dass die Konformitätsbewertungsstelle die Anforderungen des Artikels 31 erfüllt.

Sonstige gültige Dokumente in Bezug auf bestehende Benennungen der antragstellenden notifizierten Stelle im Rahmen anderer Harmonisierungsrechtsvorschriften der Union sind ebenfalls beizufügen.

(3) Kann die betreffende Konformitätsbewertungsstelle keine Akkreditierungsurkunde vorweisen, so legt sie der notifizierenden Behörde als Nachweis alle Unterlagen vor, die erforderlich sind, um zu überprüfen, festzustellen und regelmäßig zu überwachen, ob sie die Anforderungen des Artikels 31 erfüllt.

(4) Bei notifizierten Stellen, die im Rahmen anderer Harmonisierungsrechtsvorschriften der Union benannt wurden, können alle Unterlagen und Bescheinigungen im Zusammenhang mit solchen Benennungen zur Unterstützung ihres Benennungsverfahrens nach dieser Verordnung verwendet werden. Die notifizierte Stelle aktualisiert die in den Absätzen 2 und 3 des vorliegenden Artikels genannte Dokumentation immer dann, wenn sich relevante Änderungen ergeben, damit die für notifizierte Stellen zuständige Behörde überwachen und überprüfen kann, ob die Anforderungen des Artikels 31 kontinuierlich erfüllt sind.

I. Worum geht es?

Artikel 29 regelt, wie eine Konformitätsbewertungsstelle („Prüfstelle“) in der EU offiziell „notifiziert“, also zugelassen wird, um KI-Systeme prüfen zu dürfen. Das Verfahren beginnt mit einem Antrag der Prüfstelle bei der zuständigen notifizierenden Behörde im jeweiligen Mitgliedstaat. Im

Mittelpunkt stehen klare Nachweispflichten, Transparenz und die Sicherstellung, dass die Prüfstelle alle rechtlichen Anforderungen erfüllt.

II. Detailkommentar

A. Antragstellung und erforderliche Unterlagen

1. Antragsverfahren

Die Prüfstelle stellt den Antrag bei der notifizierenden Behörde ihres Sitzlandes.

a) Beizufügende Unterlagen

- **Beschreibung der Tätigkeiten:** Ausführliche Darstellung, welche Prüfungen und Bewertungen die Stelle anbietet, auf welche KI-Systeme sich ihre Kompetenz bezieht und welche Bewertungsmodule sie verwendet.
- **Akkreditierungsurkunde (sofern vorhanden):** Von der nationalen Akkreditierungsstelle ausgestellt, Nachweis über die Erfüllung der Anforderungen des Artikel 31 KI-VO(zB Unabhängigkeit, technische Kompetenz, keine Interessenkonflikte).
- **Weitere Benennungen:** Falls die Stelle bereits nach anderen EU-Rechtsvorschriften notifiziert ist, sind auch diese Nachweise beizufügen (zB Benennung als Prüf- oder Zertifizierungsstelle nach anderen EU-Regelungen).
- **Fehlende Akkreditierungsurkunde:** Gibt es keine Akkreditierung, müssen alle Nachweise eingereicht werden, aus denen die Erfüllung der Anforderungen des Artikel 31 KI-VOhervorgeht.

Beispiel: *Eine Zertifizierungsstelle für Maschinenbau möchte auch KI-Systeme prüfen. Sie reicht ihre bisherige Benennung als „benannte Stelle" nach der Maschinenrichtlinie sowie eine aktuelle Akkreditierungsurkunde ein. Damit sind die meisten Nachweise bereits abgedeckt.*

Beispiel*: Ein neues Prüfunternehmen besitzt noch keine Akkreditierung. Es muss ausführliche Unterlagen zu Personal, Verfahren, Prüfkompetenz und*

Unabhängigkeit vorlegen, damit die Behörde eine vollständige Prüfung vornehmen kann.

b) Laufende Aktualisierungspflicht

Die Prüfstelle muss die Dokumente regelmäßig aktualisieren, insbesondere bei Änderungen, damit die Behörde eine fortlaufende Überwachung durchführen kann. Bereits vorhandene Unterlagen aus anderen Benennungen können zur Unterstützung des Antrags genutzt werden.

Beispiel*: Nach einer Umstrukturierung ändert sich die Eigentümerstruktur einer notifizierten Stelle. Die Prüfstelle meldet die Änderung und aktualisiert ihre Nachweisdokumente gegenüber der notifizierenden Behörde.*

B. Entscheidung über die Notifizierung

- **Verfahrensabschluss:** Die Entscheidung der notifizierenden Behörde über die Zulassung (Notifizierung) erfolgt durch einen förmlichen Bescheid (Verwaltungsakt).
- **Beteiligte Gremien:** Die Entscheidung wird von einer unabhängigen Stelle innerhalb der Behörde getroffen (vgl Artikel 28 KI-VO).
- **Mitteilung an die EU-Kommission und andere Mitgliedstaaten:** Die Notifizierung sollte elektronisch über ein zentrales EU-Notifizierungsinstrument weitergeleitet werden.

C. Besonderheiten

- **Transparenz und Nachvollziehbarkeit:** Die klaren Unterlagenpflichten stellen sicher, dass die Kompetenz jeder Prüfstelle objektiv und nachvollziehbar geprüft werden kann.
- **Vereinfachung für bestehende Prüfstellen:** Bereits nach anderen EU-Vorschriften zugelassene Prüfstellen können vorhandene Dokumente und Nachweise nutzen, was das Verfahren erleichtert.

III. Zusammenfassung

Verfahrensschritt	Erforderliche Unterlagen / Maßnahmen
Antragstellung	Antrag an die notifizierende Behörde des Sitzlandes
Nachweise (Regelfall)	Beschreibung der Tätigkeiten, Bewertungsmodule, KI-Systeme, Akkreditierungsurkunde
Nachweise (ohne Akkreditierung)	Alle Unterlagen, die die Anforderungen des Artikel 31 KI-VObelegen
Weitere Dokumente	Nachweise zu bestehenden Benennungen nach anderen EU-Vorschriften
Entscheidung	Ergeht per Bescheid; Mitteilung an Kommission und Mitgliedstaaten
Aktualisierungspflicht	Alle relevanten Änderungen müssen umgehend gemeldet und nachgewiesen werden

IV. Quellenverzeichnis

- Anhang I Artikel R23 Beschluss (EG) 768/2008

Artikel 30 KI-VO

Notifizierungsverfahren

(1) Die notifizierenden Behörden dürfen nur Konformitätsbewertungsstellen notifizieren, die die Anforderungen des Artikels 31 erfüllen.

(2) Die notifizierenden Behörden unterrichten die Kommission und die übrigen Mitgliedstaaten mithilfe des elektronischen Notifizierungsinstruments, das von der Kommission entwickelt und verwaltet wird, über jede Konformitätsbewertungsstelle gemäß Absatz 1.

(3) Die Notifizierung gemäß Absatz 2 des vorliegenden Artikels enthält vollständige Angaben zu den Konformitätsbewertungstätigkeiten, dem betreffenden Konformitätsbewertungsmodul oder den betreffenden Konformitätsbewertungsmodulen, den betreffenden Arten der KI-Systeme und der einschlägigen Bestätigung der Kompetenz. Beruht eine Notifizierung nicht auf einer Akkreditierungsurkunde gemäß Artikel 29 Absatz 2, so legt die notifizierende Behörde der Kommission und den anderen Mitgliedstaaten die Unterlagen vor, die die Kompetenz der Konformitätsbewertungsstelle und die Vereinbarungen nachweisen, die getroffen wurden, um sicherzustellen, dass die Stelle regelmäßig überwacht wird und weiterhin die Anforderungen des Artikels 31 erfüllt.

(4) Die betreffende Konformitätsbewertungsstelle darf die Tätigkeiten einer notifizierten Stelle nur dann wahrnehmen, wenn weder die Kommission noch die anderen Mitgliedstaaten innerhalb von zwei Wochen nach einer Notifizierung durch eine notifizierende Behörde, falls eine Akkreditierungsurkunde gemäß Artikel 29 Absatz 2 vorgelegt wird, oder innerhalb von zwei Monaten nach einer Notifizierung durch eine notifizierende Behörde, falls als Nachweis Unterlagen gemäß Artikel 29 Absatz 3 vorgelegt werden, Einwände erhoben haben.

(5) Werden Einwände erhoben, konsultiert die Kommission unverzüglich die betreffenden Mitgliedstaaten und die Konformitätsbewertungsstelle. Im Hinblick darauf entscheidet die Kommission, ob die Genehmigung gerechtfertigt ist. Die Kommission richtet ihren Beschluss an die betroffenen Mitgliedstaaten und an die zuständige Konformitätsbewertungsstelle.

I. Worum geht es?

Artikel 30 regelt das genaue Verfahren, wie eine Prüfstelle („Konformitätsbewertungsstelle“) nach den Vorschriften der KI-VO als „notifizierte Stelle“ zugelassen wird. Die Vorschrift legt fest, wer notifizieren darf, wie die Notifizierung abläuft, welche Informationen übermittelt werden müssen und welche Fristen für Einsprüche gelten. Die Regelung stellt sicher, dass alle in der EU zugelassenen Prüfstellen tatsächlich geeignet und unabhängig sind.

II. Detailkommentar

A. Voraussetzungen der Notifizierung

1. Keine Ermessensentscheidung der Behörde

- Die notifizierende Behörde muss eine Stelle notifizieren, wenn alle Anforderungen nach Artikel 31 KI-VOerfüllt sind.
- Umgekehrt darf sie keine Notifizierung aussprechen, wenn diese Voraussetzungen fehlen.
- Die Behörde hat in diesem Schritt keinerlei Ermessensspielraum.

B. Ablauf des Notifizierungsverfahrens

1. Elektronische Notifizierung

Die Behörde übermittelt die Notifizierung verpflichtend elektronisch an die EU-Kommission und die übrigen Mitgliedstaaten. Das erfolgt über ein spezielles elektronisches Instrument der Kommission

2. Inhalt der Notifizierung

Folgende Angaben müssen gemacht werden:

- Welche Bewertungsaufgaben übernimmt die Stelle?
- Für welche KI-Systeme ist sie zuständig?
- Welche Bewertungsmodule werden verwendet?

- Wie ist ihre Kompetenz belegt?

Falls keine Akkreditierungsurkunde vorliegt (siehe Artikel 29 KI-VO Absatz 2), müssen alle anderen Nachweise und Überwachungsvereinbarungen beigefügt werden.

C. Fristen und Verfahren bei Einwänden

1. Prüffristen für Einwände

- **Mit Akkreditierungsurkunde**: Zwei Wochen ab Mitteilung: Innerhalb dieser Zeit können Kommission oder Mitgliedstaaten Einwände gegen die Notifizierung erheben.

Beispiel*: Eine Prüfstelle reicht einen vollständigen Antrag mit Akkreditierungsurkunde ein. Die notifizierende Behörde leitet alles elektronisch an die Kommission und Mitgliedstaaten weiter. Da niemand innerhalb von zwei Wochen Einwände erhebt, darf die Prüfstelle nach Fristablauf offiziell KI-Systeme prüfen.*

- **Ohne Akkreditierungsurkunde** (Nachweis durch andere Unterlagen):
    - Zwei Monate Prüffrist für mögliche Einwände.

Nach Ablauf dieser Fristen darf die Prüfstelle offiziell als notifizierte Stelle tätig werden – **sofern kein Einwand eingelegt wurde**.

Beispiel*: Eine andere Prüfstelle hat keine Akkreditierung, reicht aber alle anderen Nachweise ein. Die Prüffrist beträgt nun zwei Monate. Nach Ablauf dieser Zeit ohne Einwände kann auch sie als notifizierte Stelle tätig werden.*

2. Verfahren bei Einwänden

- Werden Einwände erhoben, prüft die Kommission den Fall gemeinsam mit den beteiligten Staaten und der betroffenen Stelle.
- Die Kommission entscheidet abschließend, ob die Notifizierung gerechtfertigt ist und teilt dies verbindlich mit.

D. Besonderheiten

- **Standardisierte Prüf- und Entscheidungswege:** Das Verfahren ist klar geregelt und für alle Mitgliedstaaten identisch. Das verhindert willkürliche Entscheidungen und sorgt für europaweite Einheitlichkeit.
- **Schutz vor ungeeigneten Prüfstellen:** Die Frist für Einwände und die Pflicht zur transparenten Information an alle Beteiligten verhindern, dass ungeeignete Prüfstellen zugelassen werden.

Beispiel*: Ein Mitgliedstaat zweifelt die Unabhängigkeit einer Prüfstelle an und erhebt Einwand. Die Kommission prüft den Sachverhalt und entscheidet abschließend, ob die Notifizierung aufrechterhalten werden darf.*

III. Zusammenfassung

Notifizierungsvoraussetzung	Erfüllung aller Anforderungen nach Artikel 31 KI-VO, kein Ermessen der Behörde
Übermittlung	Elektronisch an Kommission und Mitgliedstaaten
Inhalt der Mitteilung	Vollständige Angaben zu Tätigkeiten, Modulen, KI-Systemen, Kompetenznachweis
Prüffrist (mit Akkreditierung)	2 Wochen für Einwände
Prüffrist (ohne Akkreditierung)	2 Monate für Einwände
Verfahren bei Einwänden	Prüfung durch Kommission, verbindliche Entscheidung
Start der Tätigkeit	Nach Ablauf der Frist, sofern keine Einwände erhoben werden

IV. Quellenverzeichnis

- Anhang I Artikel R23 Beschluss (EG) 768/2008

Artikel 31 KI-VO

Anforderungen an notifizierte Stellen

(1) Eine notifizierte Stelle wird nach dem nationalen Recht eines Mitgliedstaats gegründet und muss mit Rechtspersönlichkeit ausgestattet sein.

(2) Die notifizierten Stellen müssen die zur Wahrnehmung ihrer Aufgaben erforderlichen Anforderungen an die Organisation, das Qualitätsmanagement, die Ressourcenausstattung und die Verfahren sowie angemessene Cybersicherheitsanforderungen erfüllen.

(3) Die Organisationsstruktur, die Zuweisung der Zuständigkeiten, die Berichtslinien und die Funktionsweise der notifizierten Stellen müssen das Vertrauen in ihre Leistung und in die Ergebnisse der von ihnen durchgeführten Konformitätsbewertungstätigkeiten gewährleisten.

(4) Die notifizierten Stellen müssen von dem Anbieter eines Hochrisiko-KI-Systems, zu dem sie Konformitätsbewertungstätigkeiten durchführen, unabhängig sein. Außerdem müssen die notifizierten Stellen von allen anderen Akteuren, die ein wirtschaftliches Interesse an den bewerteten Hochrisiko-KI-Systemen haben, und von allen Wettbewerbern des Anbieters unabhängig sein. Dies schließt die Verwendung von bewerteten Hochrisiko-KI-Systemen, die für die Tätigkeit der Konformitätsbewertungsstelle nötig sind, oder die Verwendung solcher Hochrisiko-KI-Systeme zum persönlichen Gebrauch nicht aus.

(5) Weder die Konformitätsbewertungsstelle, ihre oberste Leitungsebene noch die für die Erfüllung ihrer Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen direkt an Entwurf, Entwicklung, Vermarktung oder Verwendung von Hochrisiko-KI-Systemen beteiligt sein oder die an diesen Tätigkeiten beteiligten Parteien vertreten. Sie dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit den Konformitätsbewertungstätigkeiten, für die sie notifiziert sind, beeinträchtigen könnten. Dies gilt besonders für Beratungsdienstleistungen.

(6) Notifizierte Stellen werden so organisiert und geführt, dass bei der Ausübung ihrer Tätigkeit Unabhängigkeit, Objektivität und Unparteilichkeit gewahrt sind. Von den notifizierten Stellen werden eine Struktur und Verfahren dokumentiert und umgesetzt, die ihre Unparteilichkeit gewährleisten und sicherstellen, dass die Grundsätze der Unparteilichkeit in

ihrer gesamten Organisation, von allen Mitarbeitern und bei allen Bewertungstätigkeiten gefördert und angewandt werden.

(7) Die notifizierten Stellen gewährleisten durch dokumentierte Verfahren, dass ihre Mitarbeiter, Ausschüsse, Zweigstellen, Unterauftragnehmer sowie alle zugeordneten Stellen oder Mitarbeiter externer Einrichtungen die Vertraulichkeit der Informationen, die bei der Durchführung der Konformitätsbewertungstätigkeiten in ihren Besitz gelangen, im Einklang mit Artikel 78 wahren, außer wenn ihre Offenlegung gesetzlich vorgeschrieben ist. Informationen, von denen Mitarbeiter der notifizierten Stellen bei der Durchführung ihrer Aufgaben gemäß dieser Verordnung Kenntnis erlangen, unterliegen der beruflichen Schweigepflicht, außer gegenüber den notifizierenden Behörden des Mitgliedstaats, in dem sie ihre Tätigkeiten ausüben.

(8) Die notifizierten Stellen verfügen über Verfahren zur Durchführung ihrer Tätigkeiten unter gebührender Berücksichtigung der Größe eines Betreibers, des Sektors, in dem er tätig ist, seiner Struktur sowie der Komplexität des betreffenden KI-Systems.

(9) Die notifizierten Stellen schließen eine angemessene Haftpflichtversicherung für ihre Konformitätsbewertungstätigkeiten ab, es sei denn, diese Haftpflicht wird aufgrund nationalen Rechts von dem Mitgliedstaat, in dem sie niedergelassen sind, gedeckt oder dieser Mitgliedstaat ist selbst unmittelbar für die Konformitätsbewertung zuständig.

(10) Die notifizierten Stellen müssen in der Lage sein, ihre Aufgaben gemäß dieser Verordnung mit höchster beruflicher Integrität und der erforderlichen Fachkompetenz in dem betreffenden Bereich auszuführen, gleichgültig, ob diese Aufgaben von den notifizierten Stellen selbst oder in ihrem Auftrag und in ihrer Verantwortung durchgeführt werden.

(11) Die notifizierten Stellen müssen über ausreichende interne Kompetenzen verfügen, um die von externen Stellen in ihrem Namen wahrgenommen Aufgaben wirksam beurteilen zu können. Die notifizierten Stellen müssen ständig über ausreichendes administratives, technisches, juristisches und wissenschaftliches Personal verfügen, das Erfahrungen und Kenntnisse in Bezug auf einschlägige Arten der KI-Systeme, Daten und Datenverarbeitung sowie die in Abschnitt 2 festgelegten Anforderungen besitzt.

(12) Die notifizierten Stellen wirken an den in Artikel 38 genannten Koordinierungstätigkeiten mit. Sie wirken außerdem unmittelbar oder mittelbar an der Arbeit der europäischen Normungsorganisationen mit oder stellen sicher, dass sie stets über den Stand der einschlägigen Normen unterrichtet sind.

I. Worum geht es?

Artikel 31 legt fest, welche Anforderungen eine sogenannte „notifizierte Stelle" erfüllen muss, um als unabhängige Prüfstelle für Hochrisiko-KI-Systeme tätig sein zu dürfen. Ziel ist es, nur solche Prüfstellen zuzulassen, die nachweislich unabhängig, fachlich kompetent, vertrauenswürdig und sicher aufgestellt sind. Dadurch soll sichergestellt werden, dass die Prüfungen und Bewertungen von KI-Systemen in der EU auf einem hohen und einheitlichen Qualitätsniveau erfolgen.

II. Detailkommentar

A. Gründung und Rechtspersönlichkeit

1. Nationale Gründungspflicht

Die notifizierte Stelle muss nach dem Recht eines EU-Mitgliedstaats gegründet sein und eine eigene Rechtspersönlichkeit besitzen (zB GmbH, AG, Stiftung).

Nicht möglich: Gründung nach dem Recht eines Drittstaates (außerhalb der EU). Nur im EU-Rechtsrahmen gegründete Organisationen kommen in Frage.

Beispiel*: Ein Unternehmen aus den USA kann nicht direkt als notifizierte Stelle agieren, es müsste hierzu eine rechtlich selbständige Tochtergesellschaft nach dem Recht eines EU-Staats gründen.*

B. Organisatorische und fachliche Anforderungen

1. Organisation und Qualitätsmanagement

Die Stelle braucht eine klare Organisationsstruktur, definierte Verantwortlichkeiten, professionelle Verfahren und ein dokumentiertes Qualitätsmanagement.

Sie muss über genügend qualifiziertes Personal verfügen: administrativ, technisch, juristisch, wissenschaftlich – jeweils passend zur Artikel der geprüften KI-Systeme.

Sie muss auch Aufgaben, die sie extern vergibt, intern kompetent bewerten können.

Beispiel: *Eine deutsche GmbH möchte als notifizierte Stelle KI-Anwendungen für den Gesundheitsbereich prüfen. Sie richtet strenge interne Kontrollen ein, beschäftigt Fachpersonal aus Medizin, Informatik und Recht und implementiert ein IT-Sicherheitskonzept.*

2. Cybersicherheitsanforderungen

Die Stelle muss geeignete Maßnahmen zur Cybersicherheit treffen. Dazu gehören sichere IT-Systeme, Schutz vor unbefugtem Zugriff und Prozesse zur Sicherung sensibler Daten.

3. Berücksichtigung der Unternehmensgröße

Die Prüfverfahren müssen so gestaltet sein, dass sie die Größe, Struktur und Besonderheiten des geprüften Unternehmens sowie die Komplexität des jeweiligen KI-Systems berücksichtigen.

C. Unabhängigkeit und Vermeidung von Interessenkonflikten

1. Unabhängigkeit von Anbietern und Dritten

- Die Stelle darf weder vom Anbieter des geprüften Hochrisiko-KI-Systems noch von anderen wirtschaftlich Beteiligten abhängig sein.

- Weder Leitung noch Mitarbeitende dürfen an Entwicklung, Vertrieb oder Nutzung des geprüften KI-Systems beteiligt sein.
- Die Stelle darf keine Dienstleistungen anbieten, die ihre Unabhängigkeit gefährden könnten (zB Beratungsleistungen rund um das geprüfte System).
- Erlaubt: Verwendung von Hochrisiko-KI-Systemen zum eigenen Gebrauch oder für die Tätigkeit der Prüfstelle, sofern dies keinen Interessenkonflikt darstellt.
- Es sind klare Verfahren zu dokumentieren, wie Unparteilichkeit und Unabhängigkeit auf allen Ebenen der Organisation sichergestellt werden.

Beispiel: *Ein Start-up, das früher Beratungsleistungen für KI-Entwickler erbracht hat, muss diese Tätigkeit einstellen, wenn es als notifizierte Stelle tätig werden will, um Unabhängigkeit zu gewährleisten.*

D. Vertraulichkeit und Datenschutz

1. Schutz vertraulicher Informationen

- Alle Informationen, die im Rahmen von Prüfungen bekannt werden, sind streng vertraulich zu behandeln.
- Mitarbeitende, Ausschüsse, Unterauftragnehmer etc. unterliegen einer gesetzlichen Verschwiegenheitspflicht (außer gegenüber Aufsichtsbehörden oder bei gesetzlicher Offenlegungspflicht).
- Die Regeln gelten auch für externe Stellen und alle an der Prüfung Beteiligten.

Beispiel: *Eine Prüfstelle beauftragt einen externen IT-Sicherheitsdienstleister. Sie muss sicherstellen, dass sie die Arbeit des Dienstleisters jederzeit fachlich bewerten kann und alle Mitarbeitenden auf Verschwiegenheit verpflichtet sind.*

E. Weitere Anforderungen

1. Haftpflichtversicherung

Die Prüfstelle muss eine angemessene Haftpflichtversicherung abschließen, außer das nationale Recht sieht vor, dass der Staat selbst haftet oder die Stelle selbst eine öffentliche Einrichtung ist.

2. Mitwirkung bei Koordinierung und Normung

Die Stelle wirkt bei europäischen Normungsorganisationen mit oder informiert sich über aktuelle Standards.

F. Besonderheiten

- **Ausschluss von Prüfstellen aus Drittstaaten**: Nur nach EU-Recht gegründete Organisationen können notifiziert werden.
- **Cybersicherheit als zentrale Anforderung**: Aufgrund der Sensibilität der geprüften Daten und KI-Systeme sind hohe Standards beim Schutz vor Cyberangriffen und Datenlecks vorgeschrieben.
- **Unabhängigkeit als Schutzziel**: Keine wirtschaftlichen oder persönlichen Interessen dürfen das Prüfergebnis beeinflussen.

III. Zusammenfassung

Gründung nach EU-Recht	Nur juristische Personen nach nationalem Recht eines Mitgliedstaats, keine Drittstaatsgründungen
Organisation und Personal	Klare Strukturen, Qualitätsmanagement, ausreichendes Fachpersonal (alle relevanten Bereiche)
Cybersicherheit	IT-Schutzmaßnahmen, Datenschutz und sichere Prozesse
Unabhängigkeit	Kein Interessenkonflikt, keine wirtschaftliche oder persönliche Verbindung zu geprüften KI-Anbietern
Vertraulichkeit	Strikte Verschwiegenheitspflicht für alle Beteiligten, Ausnahme nur für

	notifizierende Behörden oder gesetzl. Pflicht
Haftpflichtversicherung	Muss vorhanden sein, außer wenn Staat haftet oder selbst öffentliche Einrichtung
Mitwirkung an Normung	Beteiligung oder Informationspflicht bei europäischen Normungsorganisationen und Koordinierungsaufgaben

Artikel 32 KI-VO

Vermutung der Konformität mit den Anforderungen an notifizierte Stellen

Weist eine Konformitätsbewertungsstelle nach, dass sie die Kriterien der einschlägigen harmonisierten Normen, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht wurden, oder Teile dieser Normen erfüllt, so wird davon ausgegangen, dass sie die Anforderungen des Artikels 31, soweit diese von den geltenden harmonisierten Normen erfasst werden, erfüllt.

I. Worum geht es?

Artikel 32 regelt eine wichtige Erleichterung für Konformitätsbewertungsstellen: Wenn sie nachweisen können, dass sie die einschlägigen harmonisierten Normen erfüllen (oder Teile davon), wird gesetzlich vermutet, dass sie auch die Anforderungen des Artikel 31 KI-VO erfüllen – zumindest in dem Umfang, den diese Normen abdecken. Das bedeutet: Statt jeden einzelnen Punkt aus Artikel 31 KI-VOseparat zu prüfen, reicht in vielen Fällen der Nachweis, dass die entsprechenden technischen oder organisatorischen Standards eingehalten werden.

II. Detailkommentar

A. Funktionsweise der Vermutung

1. Harmonisierte Normen

- Das sind EU-weit anerkannte technische oder organisatorische Standards, deren Fundstellen im Amtsblatt der EU veröffentlicht werden.
- Sie konkretisieren oft abstrakte gesetzliche Anforderungen und schaffen so einheitliche Maßstäbe.

2. Rechtswirkung

- Erfüllt eine Stelle nachweislich diese Normen, wird automatisch angenommen („vermutet"), dass sie die Anforderungen des Artikel 31 KI-VOeinhält.

Beispiel: *Eine Prüfstelle hält sich vollständig an eine harmonisierte Norm zur Cybersicherheit. Die notifizierende Behörde geht automatisch davon aus, dass die Cybersicherheitsanforderungen des Artikel 31 Absatz 2 erfüllt sind.*

- Diese Vermutung gilt nur insoweit, wie die Normen die Anforderungen tatsächlich abdecken. Bereiche, die nicht erfasst sind, müssen gesondert geprüft werden.

Beispiel: *Eine Stelle erfüllt nur den Teil der Norm, der die Dokumentationspflichten regelt. Für diesen Aspekt wird die Erfüllung vermutet; alle anderen Anforderungen muss sie separat nachweisen.*

3. Prüfungspflicht der Behörde

- Die notifizierende Behörde bedarf in den abgedeckten Bereichen keiner zusätzlichen Nachweise.
- Für nicht abgedeckte Anforderungen bleibt die normale Prüfung bestehen.

Beispiel: *Eine Stelle entscheidet sich, keine harmonisierte Norm zu verwenden, sondern eigene interne Prozesse. Die Behörde prüft dann alle Anforderungen des Artikel 31 im Detail.*

B. Verhältnis zu Artikel 31 KI-VO

- Artikel 31 KI-VO enthält die allgemeinen Pflichten und Qualifikationsanforderungen für notifizierte Stellen (zB Unabhängigkeit, Organisation, Fachpersonal).

- Der hier behandelte Artikel erleichtert die Erfüllung dieser Pflichten, indem die konkreten technischen Details auf harmonisierte Normen ausgelagert werden.

C. Besonderheiten

1. Teilweise Anwendung

- Es ist möglich, dass eine Stelle nur einzelne Teile einer Norm erfüllt. In diesem Fall gilt die Vermutung nur für diese Teile.

2. Freiwillige Anwendung

- Die Verwendung harmonisierter Normen ist **nicht verpflichtend**. Wer andere gleichwertige Verfahren nachweisen kann, erfüllt die Anforderungen ebenfalls – hat aber nicht den Vorteil der gesetzlichen Vermutung.

3. Aktualität

- Nur die jeweils im Amtsblatt veröffentlichten Fassungen sind maßgeblich.

4. Beweislastumkehr

- Die Vermutung gilt, bis das Gegenteil bewiesen wird (zB durch Feststellung einer Normverletzung).

III. Zusammenfassung

Harmonisierte Normen	EU-weit anerkannte Standards, im Amtsblatt veröffentlicht
Rechtswirkung	Erfüllung dieser Normen → Vermutung der Erfüllung von Artikel 31-Anforderungen
Reichweite	Gilt nur für den von der Norm abgedeckten Bereich
Pflicht zur Anwendung	Keine Pflicht, aber Vorteil bei der Notifizierung
Beweislast	Vermutung gilt, bis das Gegenteil nachgewiesen wird

IV. Quellenverzeichnis

- Erwägungsgrund 8 KI-VO (EU) 2024/1689

Artikel 33 KI-VO

Zweigstellen notifizierter Stellen und Vergabe von Unteraufträgen

(1) Vergibt eine notifizierte Stelle bestimmte mit der Konformitätsbewertung verbundene Aufgaben an Unterauftragnehmer oder überträgt sie diese einer Zweigstelle, so stellt sie sicher, dass der Unterauftragnehmer oder die Zweigstelle die Anforderungen des Artikels 31 erfüllt, und informiert die notifizierende Behörde darüber.

(2) Die notifizierten Stellen tragen die volle Verantwortung für Arbeiten, die von jedweden Unterauftragnehmern oder Zweigstellen ausgeführt werden.

(3) Tätigkeiten dürfen nur mit Zustimmung des Anbieters an einen Unterauftragnehmer vergeben oder einer Zweigstelle übertragen werden. Die notifizierten Stellen veröffentlichen ein Verzeichnis ihrer Zweigstellen.

(4) Die einschlägigen Unterlagen über die Bewertung der Qualifikation des Unterauftragnehmers oder der Zweigstelle und die von ihnen gemäß dieser Verordnung ausgeführten Arbeiten werden für einen Zeitraum von fünf Jahren ab dem Datum der Beendigung der Unterauftragsvergabe für die notifizierende Behörde bereitgehalten.

I. Worum geht es?

Artikel 33 regelt, unter welchen Bedingungen eine notifizierte Stelle (also eine offiziell zugelassene Prüfstelle für Hochrisiko-KI-Systeme) Aufgaben an Zweigstellen oder Unterauftragnehmer weitergeben darf.

II. Detailkommentar

A. Voraussetzungen für die Weitergabe von Aufgaben

- **Gleichwertige Anforderungen:** Jede Zweigstelle oder jeder Unterauftragnehmer muss **die** gleichen Anforderungen erfüllen wie die notifizierte Stelle selbst (Artikel 31 KI-VO). Das betrifft vor allem:
    - Unabhängigkeit
    - Fachliche Kompetenz
    - Qualitätsmanagement

- Cybersicherheit

- **Informationspflicht:** Die notifizierende Behörde muss **vorher** informiert werden, wenn Aufgaben ausgelagert werden.

Beispiel: *Eine in Frankreich notifizierte Prüfstelle gibt bestimmte Sicherheitstests an ein Labor in Spanien (Zweigstelle) ab. Sie muss vorher prüfen, ob die spanische Zweigstelle die Anforderungen des Artikel 31 erfüllt, und die französische Notifizierende Behörde informieren*.

B. Verantwortung der notifizierten Stelle

- **Volle Verantwortung:** Auch wenn ein Teil der Arbeit durch Dritte oder Zweigstellen erfolgt, haftet die notifizierte Stelle weiterhin für die vollständige und korrekte Durchführung.
- **Keine Haftungsübertragung möglich:** Rechtlich bleibt die Stelle der alleinige Ansprechpartner für Behörden und Kunden.

C. Zustimmungspflicht des Anbieters

- **Einverständnis erforderlich:** Der Anbieter des geprüften KI-Systems muss zustimmen, bevor Aufgaben an Unterauftragnehmer oder Zweigstellen weitergegeben werden.
- **Transparenzpflicht:** Die notifizierte Stelle muss ein öffentlich zugängliches Verzeichnis ihrer Zweigstellen führen.

Beispiel: *Eine Prüfstelle möchte Teile der Prüfung an ein externes IT-Sicherheitsunternehmen auslagern. Ohne Zustimmung des KI-Anbieters darf dies nicht geschehen.*

D. Dokumentations- und Aufbewahrungspflicht

- Alle Unterlagen zur Qualifikation und zu den ausgeführten Arbeiten müssen mindestens fünf Jahre nach Auftragsende aufbewahrt werden.

- Interne Dokumentation muss so geführt werden, dass die notifizierende Behörde jederzeit Einsicht nehmen kann – zB Prüfprotokolle, Kompetenznachweise, Vertragsunterlagen.

1. Besonderheiten

- **Verhinderung von „Billig-Outsourcing“:** Die Vorschrift soll verhindern, dass Prüfstellen wichtige Aufgaben an ungeeignete externe Anbieter vergeben, um Kosten zu sparen.
- **Stärkung der Transparenz:** Durch das öffentliche Zweigstellenverzeichnis kann nachvollzogen werden, welche Standorte tatsächlich Prüfaufgaben übernehmen.
- **Anbieterschutz:** Die Zustimmungspflicht stellt sicher, dass der Anbieter weiß, wer tatsächlich an der Bewertung seines Systems beteiligt ist.

Beispiel: *Nach Beendigung eines Unterauftrags muss die Prüfstelle die Bewertungsunterlagen fünf Jahre aufbewahren und auf Anfrage der Behörde vorlegen können.*

III. Zusammenfassung

Anforderungen	Unterauftragnehmer/Zweigstellen müssen Artikel 31 KI-VO erfüllen
Informationspflicht	Vorab-Mitteilung an die notifizierende Behörde
Verantwortung	Bleibt bei der notifizierten Stelle
Zustimmungspflicht	Anbieter muss Auslagerung zustimmen
Transparenz	Öffentliches Verzeichnis der Zweigstellen
Dokumentationspflicht	Aufbewahrung aller relevanten Unterlagen für fünf Jahre, jederzeit zugänglich

Artikel 34 KI-VO

Operative Pflichten der notifizierten Stellen

(1) Die notifizierten Stellen überprüfen die Konformität von Hochrisiko-KI-Systemen nach den in Artikel 43 festgelegten Konformitätsbewertungsverfahren.

(2) Die notifizierten Stellen vermeiden bei der Durchführung ihrer Tätigkeiten unnötige Belastungen für die Anbieter und berücksichtigen gebührend die Größe des Anbieters, den Sektor, in dem er tätig ist, seine Struktur sowie die Komplexität des betreffenden Hochrisiko-KI-Systems, um insbesondere den Verwaltungsaufwand und die Befolgungskosten für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG zu minimieren. Die notifizierte Stelle muss jedoch den Grad der Strenge und das Schutzniveau einhalten, die für die Konformität des Hochrisiko-KI-Systems mit den Anforderungen dieser Verordnung erforderlich sind.

(3) Die notifizierten Stellen machen der in Artikel 28 genannten notifizierenden Behörde sämtliche einschlägige Dokumentation, einschließlich der Dokumentation des Anbieters, zugänglich bzw. übermitteln diese auf Anfrage, damit diese Behörde ihre Bewertungs-, Benennungs-, Notifizierungs- und Überwachungstätigkeiten durchführen kann und die Bewertung gemäß diesem Abschnitt erleichtert wird.

I. Worum geht es?

Artikel 34 beschreibt die praktischen Pflichten notifizierter Stellen bei der Prüfung von Hochrisiko-KI-Systemen. Er legt fest, wie Konformitätsprüfungen durchzuführen sind, wie unnötige Belastungen für Anbieter – besonders für kleine und Kleinstunternehmen – vermieden werden sollen, und welche Informationspflichten gegenüber der notifizierenden Behörde bestehen. Kernpunkt ist das Spannungsverhältnis zwischen der Strenge der Prüfung mit dem Verhältnismäßigkeitsprinzip.

II. Detailkommentar

A. Durchführung der Konformitätsprüfung

- Notifizierte Stellen wenden die in Artikel 43 KI-VOfestgelegten Verfahren an.
- **Ziel**: Einheitliche und rechtssichere Prüfungen aller Hochrisiko-KI-Systeme.

B. Verhältnismäßigkeitsprinzip

- **Belastungsminimierung:** Prüfungen sollen keine unnötigen Kosten oder Verwaltungsaufwände verursachen.
- **Berücksichtigung individueller Faktoren:**
  - Größe des Anbieters
  - Tätigkeitssektor
  - Unternehmensstruktur
  - Komplexität des KI-Systems
- **Grenze der Entlastung:** Das geforderte Schutzniveau darf nicht unterschritten werden.
- Besonders relevant für Kleinst- und kleine Unternehmen: Hier sind Verfahren und Dokumentationspflichten anzupassen, ohne die inhaltliche Prüfung zu verwässern.

Beispiel: *Eine Prüfstelle reduziert bei einem Start-up die formalen Berichtspflichten, behält jedoch alle sicherheitsrelevanten Prüfungen vollständig bei.*

Beispiel: *Ein großes Technologieunternehmen muss trotz effizienter Prozesse den vollen Prüfumfang durchlaufen, da Komplexität und Risiko des KI-Systems hoch sind.*

C. Informationspflicht gegenüber der notifizierenden Behörde

- Notifizierte Stellen müssen auf Anfrage alle relevanten Unterlagen, auch vom Anbieter, zur Verfügung stellen.
- **Zweck**: Erleichterung der Überwachung, Benennung und Bewertung durch die Behörde.

D. Besonderheiten

- **Verhältnismäßigkeitsprinzip als Leitgedanke:** Der Artikel betont, dass Strenge und Schutz nicht im Widerspruch zu einer effizienten, praxisgerechten Umsetzung stehen müssen.
- **Förderung von Innovation:** Die Regelung schützt insbesondere kleinere Marktakteure vor übermäßiger Bürokratie.
- **Behördentransparenz:** Offene Dokumentations- und Übermittlungspflichten sichern die Nachvollziehbarkeit jeder Prüfung.

Beispiel: *Auf Nachfrage liefert eine Prüfstelle der notifizierenden Behörde das komplette technische Prüfprotokoll und die Risikobewertung eines geprüften Systems.*

III. Zusammenfassung

Prüfverfahren	Nach Artikel 43 KI-VO
Verhältnismäßigkeit	Belastungen minimieren, ohne Schutzstandard zu senken
Zielgruppe	Besonderer Fokus auf Kleinst- und kleine Unternehmen
Informationspflicht	Vollständige Unterlagenbereitstellung für Notifizierende Behörde

IV. Quellenverzeichnis

- Erwägungsgründe 145, 146 KI-VO (EU) 2024/1689

Artikel 35 KI-VO

Identifizierungsnummern und Verzeichnisse notifizierter Stellen

(1) Die Kommission weist jeder notifizierten Stelle eine einzige Identifizierungsnummer zu, selbst wenn eine Stelle nach mehr als einem Rechtsakt der Union notifiziert wurde.

(2) Die Kommission veröffentlicht das Verzeichnis der nach dieser Verordnung notifizierten Stellen samt ihren Identifizierungsnummern und den Tätigkeiten, für die sie notifiziert wurden. Die Kommission stellt sicher, dass das Verzeichnis auf dem neuesten Stand gehalten wird.

I. Worum geht es?

Artikel 35 regelt die eindeutige Kennzeichnung und öffentliche Bekanntmachung aller nach der KI-VO notifizierten Stellen. Jede Stelle erhält von der EU-Kommission eine einmalige Identifizierungsnummer. Zudem wird ein öffentlich zugängliches Verzeichnis dieser Stellen geführt, das stets aktuell gehalten wird.

II. Detailkommentar

A. Vergabe der Identifizierungsnummer

- **Eindeutigkeit:** Jede notifizierte Stelle erhält nur eine einzige Identifizierungsnummer, auch wenn sie nach mehreren EU-Rechtsakten tätig ist.
- **Praktische Folge:** Vermeidung von Mehrfachnummern und Verwirrung bei der Zuordnung von Prüfberichten und Zertifikaten.

B. Öffentliches Verzeichnis

- **Inhalt:**
  - *Name der notifizierten Stelle*
  - *Identifizierungsnummer*
  - *Tätigkeitsbereiche und Artikel der Konformitätsbewertung*

- **Pflicht zur Aktualität:** Die Kommission muss Änderungen (zB neue Notifizierung, Rücknahme, Erweiterung) umgehend einpflegen.
- **Zweck:** Transparenz für Anbieter, Behörden und die Öffentlichkeit, um schnell zu erkennen, welche Stellen für welche Prüfungen zugelassen sind.

Beispiel*: Ein Anbieter möchte eine Prüfstelle beauftragen und prüft vorab im öffentlichen Verzeichnis, ob diese für seinen KI-Systemtyp zugelassen ist.*

C. Besonderheiten

- **Vermeidung von Doppelstrukturen:** Eine zentrale Nummer für alle Tätigkeiten einer Stelle erleichtert die Verwaltung und Datenbankführung.
- **Markttransparenz:** Das Verzeichnis unterstützt Anbieter bei der Auswahl einer passenden Prüfstelle und erleichtert internationalen Partnern die Verifikation.
- **Kontrollmöglichkeit:** Behörden und Unternehmen können schnell prüfen, ob eine Stelle tatsächlich notifiziert ist.

Beispiel: *Eine Prüfstelle ist sowohl für die Prüfung von Hochrisiko-KI-Systemen als auch für Maschinen unter einer anderen EU-Richtlinie notifiziert. Sie nutzt in beiden Fällen dieselbe Identifizierungsnummer.*

Beispiel: *Nach dem Entzug einer Notifizierung wird die Stelle aus dem Verzeichnis entfernt, sodass keine veralteten Informationen mehr abrufbar sind.*

III. Zusammenfassung

Identifizierungsnummer	Eine eindeutige Nummer pro Stelle, unabhängig von Anzahl der Notifizierungen
Verzeichnisinhalt	Name, Nummer, Tätigkeitsbereiche
Aktualisierungspflicht	Kommission hält das Verzeichnis stets aktuell

Zweck	Transparenz, Kontrolle, einfache Verifizierung

Artikel 36 KI-VO

Änderungen der Notifizierungen

(1) Die notifizierende Behörde unterrichtet die Kommission und die anderen Mitgliedstaaten mithilfe des in Artikel 30 Absatz 2 genannten elektronischen Notifizierungsinstruments über alle relevanten Änderungen der Notifizierung einer notifizierten Stelle.

(2) Für Erweiterungen des Anwendungsbereichs der Notifizierung gelten die in den Artikeln 29 und 30 festgelegten Verfahren.

Für andere Änderungen der Notifizierung als Erweiterungen ihres Anwendungsbereichs gelten die in den Absätzen 3 bis 9 dargelegten Verfahren.

(3) Beschließt eine notifizierte Stelle die Einstellung ihrer Konformitätsbewertungstätigkeiten, so informiert sie die betreffende notifizierende Behörde und die betreffenden Anbieter so bald wie möglich und im Falle einer geplanten Einstellung ihrer Tätigkeiten mindestens ein Jahr vor deren Einstellung darüber. Die Bescheinigungen der notifizierten Stelle können für einen Zeitraum von neun Monaten nach Einstellung der Tätigkeiten der notifizierten Stelle gültig bleiben, sofern eine andere notifizierte Stelle schriftlich bestätigt hat, dass sie die Verantwortung für die von diesen Bescheinigungen abgedeckten Hochrisiko-KI-Systeme übernimmt. Die letztgenannte notifizierte Stelle führt vor Ablauf dieser Frist von neun Monaten eine vollständige Bewertung der betroffenen Hochrisiko-KI-Systeme durch, bevor sie für diese neue Bescheinigungen ausstellt. Stellt die notifizierte Stelle ihre Tätigkeit ein, so widerruft die notifizierende Behörde die Benennung.

(4) Hat eine notifizierende Behörde hinreichenden Grund zu der Annahme, dass eine notifizierte Stelle die in Artikel 31 festgelegten Anforderungen nicht mehr erfüllt oder dass sie ihren Pflichten nicht nachkommt, so untersucht die notifizierende Behörde den Sachverhalt unverzüglich und mit äußerster Sorgfalt. In diesem Zusammenhang teilt sie der betreffenden notifizierten Stelle die erhobenen Einwände mit und gibt ihr die Möglichkeit, dazu Stellung zu nehmen. Kommt die notifizierende Behörde zu dem Schluss, dass die notifizierte Stelle die in Artikel 31 festgelegten Anforderungen nicht mehr

erfüllt oder dass sie ihren Pflichten nicht nachkommt, schränkt sie die Benennung gegebenenfalls ein, setzt sie aus oder widerruft sie, je nach Schwere der Nichterfüllung dieser Anforderungen oder Pflichtverletzung. Sie informiert die Kommission und die anderen Mitgliedstaaten unverzüglich darüber.

(5) Wird die Benennung einer notifizierten Stelle ausgesetzt, eingeschränkt oder vollständig oder teilweise widerrufen, so informiert die notifizierte Stelle die betreffenden Anbieter innerhalb von zehn Tagen darüber.

(6) Wird eine Benennung eingeschränkt, ausgesetzt oder widerrufen, so ergreift die notifizierende Behörde geeignete Maßnahmen, um sicherzustellen, dass die Akten der betreffenden notifizierten Stelle für die notifizierenden Behörden in anderen Mitgliedstaaten und die Marktüberwachungsbehörden bereitgehalten und ihnen auf deren Anfrage zur Verfügung gestellt werden.

(7) Wird eine Benennung eingeschränkt, ausgesetzt oder widerrufen, so geht die notifizierende Behörde wie folgt vor:

a)Sie bewertet die Auswirkungen auf die von der notifizierten Stelle ausgestellten Bescheinigungen;

b)sie legt der Kommission und den anderen Mitgliedstaaten innerhalb von drei Monaten nach Notifizierung der Änderungen der Benennung einen Bericht über ihre diesbezüglichen Ergebnisse vor;

c)sie weist die notifizierte Stelle zur Gewährleistung der fortlaufenden Konformität der im Verkehr befindlichen Hochrisiko-KI-Systeme an, sämtliche nicht ordnungsgemäß ausgestellten Bescheinigungen innerhalb einer von der Behörde festgelegten angemessenen Frist auszusetzen oder zu widerrufen;

d)sie informiert die Kommission und die Mitgliedstaaten über Bescheinigungen, deren Aussetzung oder Widerruf sie angewiesen hat;

e)sie stellt den zuständigen nationalen Behörden des Mitgliedstaats, in dem der Anbieter seine eingetragene Niederlassung hat, alle relevanten Informationen über Bescheinigungen, deren Aussetzung oder Widerruf sie angewiesen hat, zur Verfügung; diese Behörde ergreift erforderlichenfalls geeignete Maßnahmen, um ein mögliches Risiko für Gesundheit, Sicherheit oder Grundrechte zu verhindern.

(8) Abgesehen von den Fällen, in denen Bescheinigungen nicht ordnungsgemäß ausgestellt wurden und in denen eine Benennung ausgesetzt oder eingeschränkt wurde, bleiben die Bescheinigungen unter einem der folgenden Umstände gültig:

a) Die notifizierende Behörde hat innerhalb eines Monats nach der Aussetzung oder Einschränkung bestätigt, dass im Zusammenhang mit den von der Aussetzung oder Einschränkung betroffenen Bescheinigungen kein Risiko für Gesundheit, Sicherheit oder Grundrechte besteht, und die notifizierende Behörde hat einen Zeitplan für Maßnahmen zur Aufhebung der Aussetzung oder Einschränkung genannt oder

b) die notifizierende Behörde hat bestätigt, dass keine von der Aussetzung betroffenen Bescheinigungen während der Dauer der Aussetzung oder Einschränkung ausgestellt, geändert oder erneut ausgestellt werden, und gibt an, ob die notifizierte Stelle in der Lage ist, bestehende ausgestellte Bescheinigungen während der Dauer der Aussetzung oder Einschränkung weiterhin zu überwachen und die Verantwortung dafür zu übernehmen; falls die notifizierende Behörde feststellt, dass die notifizierte Stelle nicht in der Lage ist, bestehende ausgestellte Bescheinigungen weiterzuführen, so bestätigt der Anbieter des von der Bescheinigung abgedeckten Systems den zuständigen nationalen Behörden des Mitgliedstaats, in dem er seine eingetragene Niederlassung hat, innerhalb von drei Monaten nach der Aussetzung oder Einschränkung schriftlich, dass eine andere qualifizierte notifizierte Stelle vorübergehend die Aufgaben der notifizierten Stelle zur Überwachung der Bescheinigung übernimmt und dass sie während der Dauer der Aussetzung oder Einschränkung für die Bescheinigung verantwortlich bleibt.

(9) Abgesehen von den Fällen, in denen Bescheinigungen nicht ordnungsgemäß ausgestellt wurden und in denen eine Benennung widerrufen wurde, bleiben die Bescheinigungen unter folgenden Umständen für eine Dauer von neun Monaten gültig:

a) Die zuständige nationale Behörde des Mitgliedstaats, in dem der Anbieter des von der Bescheinigung abgedeckten Hochrisiko-KI-Systems seine eingetragene Niederlassung hat, hat bestätigt, dass im Zusammenhang mit den betreffenden Hochrisiko-KI-Systemen kein Risiko für Gesundheit, Sicherheit oder Grundrechte besteht, und

b) eine andere notifizierte Stelle hat schriftlich bestätigt, dass sie die unmittelbare Verantwortung für diese KI-Systeme übernehmen und deren

Bewertung innerhalb von 12 Monaten ab dem Widerruf der Benennung abgeschlossen haben wird.

Unter den in Unterabsatz 1 genannten Umständen kann die zuständige nationale Behörde des Mitgliedstaats, in dem der Anbieter des von der Bescheinigung abgedeckten Systems seine Niederlassung hat, die vorläufige Gültigkeit der Bescheinigungen um zusätzliche Zeiträume von je drei Monaten, jedoch nicht um insgesamt mehr als 12 Monate, verlängern.

Die zuständige nationale Behörde oder die notifizierte Stelle, die die Aufgaben der von der Benennungsänderung betroffenen notifizierten Stelle übernimmt, informiert unverzüglich die Kommission, die anderen Mitgliedstaaten und die anderen notifizierten Stellen darüber.

I. Worum geht es?

Artikel 36 beschreibt, wie Änderungen an der Notifizierung einer notifizierten Stelle gehandhabt werden. Er umfasst sowohl Erweiterungen des Tätigkeitsbereichs als auch Einschränkungen, Aussetzungen oder den vollständigen Widerruf einer Notifizierung. Ziel ist es, einen klaren und transparenten Ablauf sicherzustellen, der Risiken für Gesundheit, Sicherheit und Grundrechte minimiert und die fortlaufende Gültigkeit oder den Übergang von Bescheinigungen regelt.

II. Detailkommentar

A. Mitteilungspflichten

- **Elektronische Meldung**: Änderungen werden über das EU-Notifizierungsinstrument gemeldet (vgl Artikel 30 KI-VO Absatz 2).
- **Unterscheidung**:
    - **Erweiterung des Anwendungsbereichs**: Verfahren nach Artikel 29 KI-VO und Artikel 30 KI-VO.
    - **Sonstige Änderungen**: Verfahren nach Absatz 3–9.

B. Einstellung der Tätigkeit

- Frühzeitige Information der Behörde und der betroffenen Anbieter (mindestens ein Jahr vorher bei geplanter Einstellung).
- **Übergangsregel**: Bescheinigungen können neun Monate gültig bleiben, wenn eine andere notifizierte Stelle die Verantwortung übernimmt und eine Neubewertung durchführt.

C. Nichterfüllung von Anforderungen

- **Verdacht:** Behörde prüft unverzüglich und gibt der Stelle Gelegenheit zur Stellungnahme.
- **Maßnahmen:** Einschränkung, Aussetzung oder Widerruf der Notifizierung je nach Schwere.
- **Pflicht zur Information der Anbieter:** Innerhalb von zehn Tagen.

Beispiel: *Wegen wiederholter Pflichtverletzungen wird eine Notifizierung ausgesetzt; betroffene Anbieter werden binnen zehn Tagen informiert.*

D. Folgen für Unterlagen und Bescheinigungen

- **Unterlagen:** Müssen für andere Behörden bereitgehalten werden.
- **Bewertung der Auswirkungen:** Behörde erstellt Bericht und leitet Maßnahmen zur Sicherung der Konformität ein.
- **Bescheinigungen:** Können unter bestimmten Bedingungen vorübergehend gültig bleiben (klare Regeln für Risikoabschätzung und Übergabe an andere Stellen).

E. Besonderheiten

- **Risikoprävention:** Jede Änderung wird auf mögliche Auswirkungen auf die Sicherheit und Grundrechte geprüft.

- **Kontinuität der Konformität:** Übergangsfristen und Übernahme durch andere Stellen verhindern Lücken im Zertifizierungssystem.
- **Transparenz:** Verpflichtende Berichte und Informationsketten zwischen Behörden, Kommission, Mitgliedstaaten und Anbietern.

Beispiel: *Nach dem Widerruf übernimmt eine andere Stelle vorübergehend die Überwachung bestehender Bescheinigungen, um Marktrücknahmen zu vermeiden.*

III. Zusammenfassung

Meldung von Änderungen	Über elektronisches EU-Notifizierungsinstrument
Erweiterung	Verfahren nach Artikel 29 KI-VO und Artikel 30 KI-VO
Einstellung der Tätigkeit	Frühzeitige Info + neun Monate Übergangsfrist bei Übernahme durch andere Stelle
Pflichtverletzungen	Prüfung, evtl Einschränkung, Aussetzung oder Widerruf
Bescheinigungen	Unter bestimmten Bedingungen vorübergehend gültig
Unterlagen	Bereitstellung für andere Behörden

Artikel 37 KI-VO

Anfechtungen der Kompetenz notifizierter Stellen

(1) Die Kommission untersucht erforderlichenfalls alle Fälle, in denen begründete Zweifel an der Kompetenz einer notifizierten Stelle oder daran bestehen, dass eine notifizierte Stelle die in Artikel 31 festgelegten Anforderungen und ihre geltenden Pflichten weiterhin erfüllt.

(2) Die notifizierende Behörde stellt der Kommission auf Anfrage alle Informationen über die Notifizierung oder die Aufrechterhaltung der Kompetenz der betreffenden notifizierten Stelle zur Verfügung.

(3) Die Kommission stellt sicher, dass alle im Verlauf ihrer Untersuchungen gemäß diesem Artikel erlangten sensiblen Informationen gemäß Artikel 78 vertraulich behandelt werden.

(4) Stellt die Kommission fest, dass eine notifizierte Stelle die Anforderungen für ihre Notifizierung nicht oder nicht mehr erfüllt, so informiert sie den notifizierenden Mitgliedstaat entsprechend und fordert ihn auf, die erforderlichen Abhilfemaßnahmen zu treffen, einschließlich einer Aussetzung oder eines Widerrufs der Notifizierung, sofern dies nötig ist. Versäumt es ein Mitgliedstaat, die erforderlichen Abhilfemaßnahmen zu ergreifen, kann die Kommission die Benennung im Wege eines Durchführungsrechtsakts aussetzen, einschränken oder widerrufen. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

I. Worum geht es?

Artikel 37 beschreibt das Verfahren, wenn Zweifel an der Kompetenz oder der Pflichtenerfüllung einer notifizierten Stelle bestehen. Die EU-Kommission kann Untersuchungen durchführen und bei festgestellten Mängeln Maßnahmen anordnen, notwendigerweise kann sie auch die Notifizierung aussetzen oder widerrufen.

II. Detailkommentar

A. Anlass für Untersuchungen

- **Auslöser:** Begründete Zweifel an der Fachkompetenz oder der Einhaltung der Anforderungen aus Artikel 31 KI-VO.
- **Initiator:** Die Kommission wird tätig, wenn sie es für erforderlich hält.

B. Informationspflicht der notifizierenden Behörde

- **Auf Anforderung** muss die notifizierende Behörde alle relevanten Informationen zur Notifizierung oder Kompetenz einer Stelle an die Kommission übermitteln.

Beispiel: *Nach einer Beschwerde stellt sich heraus, dass eine notifizierte Stelle veraltete Prüfverfahren nutzt. Die Kommission fordert den Mitgliedstaat auf, die Benennung auszusetzen.*

C. Vertraulichkeit

- **Schutz sensibler Informationen** nach Artikel 78 KI-VO– betrifft insbesondere Geschäftsgeheimnisse und vertrauliche Prüfunterlagen.

D. Maßnahmen bei Mängeln

- **Feststellung durch Kommission:** Erfüllt eine Stelle die Anforderungen nicht (mehr), muss der Mitgliedstaat Abhilfe schaffen.
- **Eskalation:** Kommt der Mitgliedstaat der Aufforderung nicht nach, kann die Kommission selbst die Benennung aussetzen, einschränken oder widerrufen – mittels Durchführungsrechtsakt.

Beispiel: *Eine Stelle erfüllt Cybersicherheitsanforderungen nicht mehr. Der Mitgliedstaat reagiert nicht, woraufhin die Kommission den Widerruf beschließt.*

E. Besonderheiten

- **Kompetenzkontrolle auf EU-Ebene:** Artikel 37 stärkt die Rolle der Kommission als übergeordnete Kontrollinstanz.
- **Letztes Mittel:** Direkter Eingriff der Kommission erfolgt nur, wenn der Mitgliedstaat untätig bleibt.
- **Rechtsinstrument:** Der Eingriff der Kommission erfolgt im Prüfverfahren gemäß Artikel 98 KI-VO Absatz 2, was den Mitgliedstaaten Mitwirkungsrechte sichert.

III. Zusammenfassung

Auslöser	Zweifel an Kompetenz oder Pflichterfüllung
Informationspflicht	Notifizierende Behörde muss Kommission alle Infos bereitstellen
Vertraulichkeit	Sensible Infos werden nach Artikel 78 KI-VOgeschützt
Maßnahmen	Mitgliedstaat muss handeln; Kommission kann selbst eingreifen
Rechtsgrundlage Eingriff	Durchführungsrechtsakt nach Artikel 98 KI-VOAbsatz 2

IV. Quellenverzeichnis

- Erwägungsgründe 126, 153 KI-VO (EU) 2024/1689

Artikel 38 KI-VO

Koordinierung der notifizierten Stellen

(1) Die Kommission sorgt dafür, dass in Bezug auf Hochrisiko-KI-Systeme eine zweckmäßige Koordinierung und Zusammenarbeit zwischen den an den Konformitätsbewertungsverfahren im Rahmen dieser Verordnung beteiligten notifizierten Stellen in Form einer sektoralen Gruppe notifizierter Stellen eingerichtet und ordnungsgemäß weitergeführt wird.

(2) Jede notifizierende Behörde sorgt dafür, dass sich die von ihr notifizierten Stellen direkt oder über benannte Vertreter an der Arbeit der in Absatz 1 genannten Gruppe beteiligen.

(3) Die Kommission sorgt für den Austausch von Wissen und bewährten Verfahren zwischen den notifizierenden Behörden.

I. Worum geht es?

Artikel 38 regelt, wie die Zusammenarbeit und Abstimmung zwischen den notifizierten Stellen, die Hochrisiko-KI-Systeme prüfen, organisiert wird. Die EU-Kommission richtet dafür eine sektorale Gruppe ein, in der Wissen und bewährte Verfahren ausgetauscht werden. Auch die nationalen notifizierenden Behörden und ihre Stellen müssen sich beteiligen.

II. Detailkommentar

A. Einrichtung einer sektoralen Gruppe

- **Verantwortung der Kommission:** Sie sorgt für eine funktionierende Koordinierung und den Austausch zwischen allen relevanten notifizierten Stellen.
- **Form:** Eine „sektorale Gruppe“ als Plattform für Konformitätsbewertungsthemen bei Hochrisiko-KI.
- **Ziel:** Einheitliche Anwendung der Vorschriften, Vermeidung unterschiedlicher Prüfkriterien.

Beispiel: *Eine neue Prüfmethode zur Bewertung der Datensicherheit von KI-Systemen wird in der sektoralen Gruppe vorgestellt und von allen Mitgliedstaaten übernommen.*

B. Beteiligungspflicht der notifizierten Stellen

- **Pflicht der Mitgliedstaaten:** Die notifizierenden Behörden stellen sicher, dass ihre Stellen – direkt oder durch Vertreter – an den Treffen und Arbeiten teilnehmen.
- **Nutzen:** Frühzeitige Kenntnis neuer Entwicklungen, gemeinsames Lösen von Praxisproblemen.

C. Austausch zwischen Behörden

- **Kommissionsrolle:** Fördert den Wissenstransfer und die Verbreitung von Best Practices zwischen den notifizierenden Behörden.

D. Besonderheiten

- **Zentraler Koordinierungsmechanismus:** Verhindert „Insellösungen" einzelner Mitgliedstaaten.
- **Synergieeffekte:** Zusammenarbeit nutzt auch bestehende Strukturen und EU-Programme wie „Digitales Europa".
- **Qualitätssicherung:** Durch kontinuierlichen Austausch bleiben Prüfstandards hoch und vergleichbar.

Beispiel: *Unterschiedliche Interpretationen einer Vorschrift werden in der Gruppe diskutiert und harmonisiert.*

III. Zusammenfassung

Einrichtung Gruppe	Kommission richtet sektorale Gruppe für notifizierte Stellen ein
Beteiligung	Mitgliedstaaten stellen Teilnahme ihrer Stellen sicher

Austausch Behörden	Kommission fördert Wissens- und Erfahrungsaustausch
Ziel	Einheitliche Standards, bessere Koordination

IV. Quellenverzeichnis

- Erwägungsgrund 148 KI-VO (EU) 2024/1689

Artikel 39 KI-VO

Konformitätsbewertungsstellen in Drittländern

Konformitätsbewertungsstellen, die nach dem Recht eines Drittlands errichtet wurden, mit dem die Union ein Abkommen geschlossen hat, können ermächtigt werden, die Tätigkeiten notifizierter Stellen gemäß dieser Verordnung durchzuführen, sofern sie die Anforderungen gemäß Artikel 31 erfüllen oder das gleiche Maß an Konformität gewährleisten.

I. Worum geht es?

Artikel 39 legt fest, unter welchen Bedingungen Konformitätsbewertungsstellen aus Drittländern (also Nicht-EU-Staaten) in der EU wie notifizierte Stellen tätig werden dürfen. Voraussetzung ist ein entsprechendes Abkommen der EU mit dem Drittland und der Nachweis, dass die Stelle dieselben Anforderungen wie nach Artikel 31 KI-VOerfüllt oder ein gleichwertiges Schutzniveau bietet.

II. Detailkommentar

A. Abkommen mit Drittland

- **Grundvoraussetzung:** Es muss ein formelles Abkommen zwischen EU und dem Drittland bestehen, das die gegenseitige Anerkennung von Konformitätsbewertungen vorsieht.
- **Zweck:** Erleichterung des internationalen Handels und Vermeidung von Doppelprüfungen.

Beispiel: *Die EU schließt mit Kanada ein Abkommen zur gegenseitigen Anerkennung von Konformitätsbewertungen. Eine kanadische Prüfstelle darf daraufhin Zertifikate für Hochrisiko-KI-Systeme ausstellen, die in der EU anerkannt werden.*

B. Gleichwertige Anforderungen (Artikel 31 KI-VO)

- **Kernanforderung:** Die Konformitätsbewertungsstelle des Drittlands muss dieselben Qualitäts-, Unabhängigkeits- und Fachanforderungen erfüllen wie EU-notifizierte Stellen.
- **Alternativ:** Nachweis eines gleichwertigen Schutzniveaus.

C. Besonderheiten

- **Kein Automatismus:** Selbst bei hoher Qualität der Stelle ist eine formelle Vereinbarung zwingend.
- **Marktzugang:** Öffnet Drittländern den Zugang zum EU-Markt für Hochrisiko-KI-Systeme, ohne das Schutzniveau zu senken.

Beispiel: *Ohne ein solches Abkommen bleibt die Anerkennung von Prüfungen einer US-Stelle ausgeschlossen, selbst wenn deren Standards hoch sind.*

III. Zusammenfassung

Abkommen	Erforderlich zwischen EU und Drittland
Anforderungen	Erfüllung Artikel 31 KI-VO oder gleichwertiges Schutzniveau
Ziel	Handelserleichterung, internationale Kooperation
Schutzstandard	Keine Abstriche bei Qualität und Sicherheit

IV. Quellenverzeichnis

- Erwägungsgrund 127 KI-VO (EU) 2024/1689

Artikel 40 KI-VO

Harmonisierte Normen und Normungsdokumente

(1) Bei Hochrisiko-KI-Systemen oder KI-Modellen mit allgemeinem Verwendungszweck, die mit harmonisierten Normen oder Teilen davon, deren Fundstellen gemäß der Verordnung (EU) Nr 1025/2012 im Amtsblatt der Europäischen Union veröffentlicht wurden, übereinstimmen, wird eine Konformität mit den Anforderungen gemäß Abschnitt 2 des vorliegenden Kapitels oder gegebenenfalls mit den Pflichten gemäß Kapitel V Abschnitte 2 und 3 der vorliegenden Verordnung vermutet, soweit diese Anforderungen oder Verpflichtungen von den Normen abgedeckt sind.

(2) Gemäß Artikel 10 der Verordnung (EU) Nr 1025/2012 erteilt die Kommission unverzüglich Normungsaufträge, die alle Anforderungen gemäß Abschnitt 2 des vorliegenden Kapitels abdecken und gegebenenfalls Normungsaufträge, die Pflichten gemäß Kapitel V Abschnitte 2 und 3 der vorliegenden Verordnung abdecken. In dem Normungsauftrag werden auch Dokumente zu den Berichterstattungs- und Dokumentationsverfahren im Hinblick auf die Verbesserung der Ressourcenleistung von KI-Systemen zB durch die Verringerung des Energie- und sonstigen Ressourcenverbrauchs des Hochrisiko-KI-Systems während seines gesamten Lebenszyklus und zu der energieeffizienten Entwicklung von KI-Modellen mit allgemeinem Verwendungszweck verlangt. Bei der Ausarbeitung des Normungsauftrags konsultiert die Kommission das KI-Gremium und die einschlägigen Interessenträger, darunter das Beratungsforum.

Bei der Erteilung eines Normungsauftrags an die europäischen Normungsorganisationen gibt die Kommission an, dass die Normen klar und — ua mit den Normen, die in den verschiedenen Sektoren für Produkte entwickelt wurden, die unter die in Anhang I aufgeführten geltenden Harmonisierungsrechtsvorschriften der Union fallen — konsistent sein müssen und sicherstellen sollen, dass die in der Union in Verkehr gebrachten oder in Betrieb genommenen Hochrisiko-KI-Systeme oder KI-Modelle mit allgemeinem Verwendungszweck die in dieser Verordnung festgelegten einschlägigen Anforderungen oder Pflichten erfüllen.

Die Kommission fordert die europäischen Normungsorganisationen auf, Nachweise dafür vorzulegen, dass sie sich nach besten Kräften bemühen, die in den Unterabsätzen 1 und 2 dieses Absatzes genannten Ziele im Einklang mit Artikel 24 der Verordnung (EU) Nr 1025/2012 zu erreichen.

(3) Die am Normungsprozess Beteiligten bemühen sich, Investitionen und Innovationen im Bereich der KI, ua durch Erhöhung der Rechtssicherheit, sowie der Wettbewerbsfähigkeit und des Wachstums des Unionsmarktes zu fördern und zur Stärkung der weltweiten Zusammenarbeit bei der Normung und zur Berücksichtigung bestehender internationaler Normen im Bereich der KI, die mit den Werten, Grundrechten und Interessen der Union im Einklang stehen, beizutragen und die Multi-Stakeholder-Governance zu verbessern, indem eine ausgewogene Vertretung der Interessen und eine wirksame Beteiligung aller relevanten Interessenträger gemäß den Artikeln 5, 6 und 7 der Verordnung (EU) Nr 1025/2012 sichergestellt werden.

I. Worum geht es?

Artikel 40 regelt, wie harmonisierte Normen und andere Normungsdokumente genutzt werden können, um die Konformität von Hochrisiko-KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck nachzuweisen. Stimmen diese Systeme mit harmonisierten Normen überein, gilt dies als Beleg dafür, dass die relevanten Anforderungen der KI-VO erfüllt sind – soweit die Normen diese Anforderungen abdecken.

II. Detailkommentar

A. Vermutungswirkung harmonisierter Normen

- **Grundprinzip:** Wer eine anerkannte Norm erfüllt, muss nicht gesondert beweisen, dass er die entsprechenden gesetzlichen Anforderungen einhält.
- **Reichweite:** Gilt nur für die Anforderungen, die in der Norm tatsächlich geregelt sind.

Beispiel: *Ein Anbieter nutzt eine harmonisierte Norm zur Datensicherheit für KI-Systeme. Damit entfällt die Pflicht, diesen Aspekt separat im Konformitätsverfahren zu belegen.*

B. Rolle der Kommission

- **Normungsaufträge:** Die Kommission beauftragt europäische Normungsorganisationen (zB CEN, CENELEC) mit der Entwicklung einschlägiger Normen.
- **Konsultationen:** Beteiligung des KI-Gremiums und relevanter Interessenträger zur Qualitätssicherung.
- **Ziel:** Einheitliche, konsistente und klare Normen, auch im Abgleich mit bestehenden Produktnormen.

Beispiel: *Es gibt noch keine harmonisierte Norm zu einem bestimmten Transparenzkriterium. Hier kann die Kommission eine gemeinsame Spezifikation vorgeben, bis eine Norm entwickelt ist.*

C. Nachhaltigkeitsaspekte

Normungsaufträge sollen auch Vorgaben zur Ressourceneffizienz, zB geringerer Energieverbrauch und nachhaltige Entwicklung von KI-Modellen, enthalten.

D. Internationale Dimension

- Berücksichtigung bestehender internationaler Normen, soweit sie mit den Werten und Grundrechten der EU vereinbar sind.
- Förderung der weltweiten Normungszusammenarbeit.

E. Besonderheiten

- **Gemeinsame Spezifikationen:** Wenn harmonisierte Normen fehlen oder unzureichend sind, kann die Kommission eigene technische Vorgaben erlassen – als Ausnahme.
- **Multi-Stakeholder-Ansatz:** Ausgewogene Vertretung von Industrie, KMU, Verbraucher- und Umweltorganisationen.

III. Zusammenfassung

Vermutungswirkung	Erfüllung einer harmonisierten Norm = Konformitätsvermutung
Normungsaufträge	Durch die Kommission an europäische Normungsorganisationen
Nachhaltigkeitsaspekte	Ressourceneffizienz, Lebenszyklusoptimierung
Internationale Kooperation	Nutzung kompatibler globaler Normen, Förderung der Zusammenarbeit
Ersatzmechanismus	Gemeinsame Spezifikationen der Kommission bei Normenlücken

IV. Quellenverzeichnis

- Erwägungsgrund 121 KI-VO (EU) 2024/1689

Artikel 41 KI-VO

Gemeinsame Spezifikationen

(1) Die Kommission kann Durchführungsrechtsakte zur Festlegung gemeinsamer Spezifikationen für die Anforderungen gemäß Abschnitt 2 dieses Kapitels oder gegebenenfalls die Pflichten gemäß Kapitel V Abschnitte 2 und 3 erlassen, wenn die folgenden Bedingungen erfüllt sind:

a) Die Kommission hat gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr 1025/2012 eine oder mehrere europäische Normungsorganisationen damit beauftragt, eine harmonisierte Norm für die in Abschnitt 2 dieses Kapitels festgelegten Anforderungen oder gegebenenfalls für die in Kapitel V Abschnitte 2 und 3 festgelegten Pflichten zu erarbeiten, und

i) der Auftrag wurde von keiner der europäischen Normungsorganisationen angenommen oder

ii) die harmonisierten Normen, die Gegenstand dieses Auftrags sind, werden nicht innerhalb der gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr 1025/2012 festgelegten Frist erarbeitet oder

iii) die einschlägigen harmonisierten Normen tragen den Bedenken im Bereich der Grundrechte nicht ausreichend Rechnung oder

iv) die harmonisierten Normen entsprechen nicht dem Auftrag und

b) im Amtsblatt der Europäischen Union sind keine Fundstellen zu harmonisierten Normen gemäß der Verordnung (EU) Nr 1025/2012 veröffentlicht, die den in Abschnitt 2 dieses Kapitels aufgeführten Anforderungen oder gegebenenfalls den in Kapitel V Abschnitte 2 und 3 aufgeführten Pflichten genügen, und es ist nicht zu erwarten, dass eine solche Fundstelle innerhalb eines angemessenen Zeitraums veröffentlicht wird.

Bei der Verfassung der gemeinsamen Spezifikationen konsultiert die Kommission das in Artikel 67 genannte Beratungsforum.

Die in Unterabsatz 1 des vorliegenden Absatzes genannten Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(2) Vor der Ausarbeitung eines Entwurfs eines Durchführungsrechtsakts informiert die Kommission den in Artikel 22 der Verordnung (EU) Nr

1025/2012 genannten Ausschuss darüber, dass sie die in Absatz 1 des vorliegenden Artikels festgelegten Bedingungen als erfüllt erachtet.

(3) Bei Hochrisiko-KI-Systemen oder KI-Modellen mit allgemeinem Verwendungszweck, die mit den in Absatz 1 genannten gemeinsamen Spezifikationen oder Teilen dieser Spezifikationen übereinstimmen, wird eine Konformität mit den Anforderungen in Abschnitt 2 dieses Kapitels oder gegebenenfalls die Einhaltung der in Kapitel V Abschnitte 2 und 3 genannten Pflichten vermutet, soweit diese Anforderungen oder diese Pflichten von den gemeinsamen Spezifikationen abgedeckt sind.

(4) Wird eine harmonisierte Norm von einer europäischen Normungsorganisation angenommen und der Kommission zur Veröffentlichung ihrer Fundstelle im Amtsblatt der Europäischen Union vorgeschlagen, so bewertet die Kommission die harmonisierte Norm gemäß der Verordnung (EU) Nr 1025/2012. Wird die Fundstelle zu einer harmonisierten Norm im Amtsblatt der Europäischen Union veröffentlicht, so werden die in Absatz 1 genannten Durchführungsrechtsakte, die dieselben Anforderungen gemäß Abschnitt 2 dieses Kapitels oder gegebenenfalls dieselben Pflichten gemäß Kapitel V Abschnitte 2 und 3 erfassen, von der Kommission ganz oder teilweise aufgehoben.

(5) Wenn Anbieter von Hochrisiko-KI-Systemen oder KI-Modellen mit allgemeinem Verwendungszweck die in Absatz 1 genannten gemeinsamen Spezifikationen nicht befolgen, müssen sie hinreichend nachweisen, dass sie technische Lösungen verwenden, die die in Abschnitt 2 dieses Kapitels aufgeführten Anforderungen oder gegebenenfalls die Pflichten gemäß Kapitel V Abschnitte 2 und 3 zumindest in gleichem Maße erfüllen;

(6) Ist ein Mitgliedstaat der Auffassung, dass eine gemeinsame Spezifikation den Anforderungen gemäß Abschnitt 2 nicht vollständig entspricht oder gegebenenfalls die Pflichten gemäß Kapitel V Abschnitte 2 und 3 nicht vollständig erfüllt, so setzt er die Kommission im Rahmen einer ausführlichen Erläuterung davon in Kenntnis. Die Kommission bewertet die betreffende Information und ändert gegebenenfalls den Durchführungsrechtsakt, durch den die betreffende gemeinsame Spezifikation festgelegt wurde.

I. Worum geht es?

Artikel 41 regelt, wann und wie die Kommission sogenannte gemeinsame Spezifikationen festlegen darf. Diese dienen als technische Referenzen, wenn harmonisierte Normen fehlen, zu spät fertig werden oder unzureichend sind. Ziel ist es, eine einheitliche und praxistaugliche Umsetzung der Anforderungen der KI-VO zu sichern.

II. Detailkommentar

A. Voraussetzungen für gemeinsame Spezifikationen

- Harmonisierte Normen sind nicht verfügbar, werden nicht fristgerecht erarbeitet, decken Grundrechtsaspekte nicht ausreichend ab oder entsprechen nicht dem Auftrag.
- Im Amtsblatt gibt es keine einschlägigen Normen, und kurzfristig ist keine Veröffentlichung zu erwarten.
- Vorab informiert die Kommission den zuständigen Normungsausschuss.

Beispiel: *Es gibt noch keine Norm für KI-gestützte Übersetzungssysteme: Die Kommission erlässt eine Spezifikation, die Mindestanforderungen an Datenqualität und Tests festlegt.*

Beispiel: *Eine bestehende Norm berücksichtigt nicht den Schutz sensibler Gesundheitsdaten. Die Kommission erlässt ergänzende Spezifikationen.*

B. Verfahren

- **Konsultation:** Einbeziehung des Beratungsforums.
- **Rechtsform:** Festlegung durch Durchführungsrechtsakt im Prüfverfahren.
- **Aufhebungspflicht:** Werden später passende harmonisierte Normen veröffentlicht, hebt die Kommission die entsprechenden Spezifikationen auf.

C. Vermutungswirkung

Wer die Spezifikationen einhält, profitiert von der Vermutung, die relevanten Anforderungen der KI-VO zu erfüllen.

D. Abweichungsmöglichkeit

Anbieter können eigene Lösungen nutzen, müssen aber gleichwertige Erfüllung der Anforderungen nachweisen.

E. Einwände der Mitgliedstaaten

Mitgliedstaaten können begründete Zweifel an einer Spezifikation melden; die Kommission prüft und passt ggf an.

F. Besonderheiten

Gemeinsame Spezifikationen sind Ausnahmeinstrumente, nicht der Regelfall. Sie sichern Rechtssicherheit, wenn Normungsprozesse ins Stocken geraten.

III. Zusammenfassung

Auslöser	Fehlen, Verspätung oder Mängel harmonisierter Normen
Rechtsform	Durchführungsrechtsakt im Prüfverfahren
Wirkung	Vermutungswirkung bei Einhaltung
Alternative Lösungen	Möglich, wenn gleichwertige Erfüllung nachgewiesen wird
Anpassung	Überprüfung und Änderung bei berechtigten Einwänden von Mitgliedstaaten

IV. Quellenverzeichnis

- Erwägungsgrund 121 KI-VO (EU) 2024/1689

Artikel 42 KI-VO

Vermutung der Konformität mit bestimmten Anforderungen

(1) Für Hochrisiko-KI-Systeme, die mit Daten, in denen sich die besonderen geografischen, verhaltensbezogenen, kontextuellen oder funktionalen Rahmenbedingungen niederschlagen, unter denen sie verwendet werden sollen, trainiert und getestet wurden, gilt die Vermutung, dass sie die in Artikel 10 Absatz 4 festgelegten einschlägigen Anforderungen erfüllen.

(2) Für Hochrisiko-KI-Systeme, die im Rahmen eines der Cybersicherheitszertifizierungssysteme gemäß der Verordnung (EU) 2019/881, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht wurden, zertifiziert wurden oder für die eine solche Konformitätserklärung erstellt wurde, gilt die Vermutung, dass sie die in Artikel 15 der vorliegenden Verordnung festgelegten Cybersicherheitsanforderungen erfüllen, sofern diese Anforderungen von der Cybersicherheitszertifizierung oder der Konformitätserklärung oder Teilen davon abdeckt sind.

I. Worum geht es?

Artikel 42 legt fest, wann bei Hochrisiko-KI-Systemen **vermutet** wird, dass sie bestimmte Anforderungen der KI-VO erfüllen. Diese Vermutungswirkung bezieht sich auf zwei Bereiche:

- **Datenqualität** – wenn Systeme mit für den Einsatz relevanten, realitätsnahen Daten trainiert und getestet wurden.
- **Cybersicherheit** – wenn Systeme eine anerkannte EU-Cybersicherheitszertifizierung haben oder eine entsprechende Konformitätserklärung vorliegt.

II. Detailkommentar

A. Vermutungswirkung bei Datenqualität

- Gilt, wenn Trainings- und Testdaten die besonderen geografischen, verhaltensbezogenen, kontextuellen oder funktionalen Bedingungen widerspiegeln, unter denen das System eingesetzt werden soll.

- Bezieht sich auf die Anforderungen aus Artikel 10 KI-VOAbsatz 4 (Daten-Governance).

Beispiel: *Ein KI-basiertes Verkehrsüberwachungssystem wird mit Daten aus allen relevanten Regionen und unter verschiedenen Wetter- und Verkehrsbedingungen trainiert – Vermutung der Erfüllung von Artikel 10 Absatz 4.*

B. Vermutungswirkung bei Cybersicherheit

- Gilt, wenn ein System nach einem im Amtsblatt veröffentlichten EU-Cybersicherheitszertifizierungssystem zertifiziert ist oder eine Konformitätserklärung vorliegt.
- Deckt nur die Teile der Anforderungen nach Artikel 15 KI-VO ab, die tatsächlich vom Zertifikat oder der Erklärung umfasst sind.

Beispiel*: Ein Medizin-KI-System erhält ein EU-Cybersicherheitszertifikat, das Schutz vor Datenvergiftung und unbefugtem Zugriff bestätigt – Vermutung der Erfüllung der abgedeckten Anforderungen aus Artikel 15.*

C. Verhältnis zu anderen Vorschriften

- Die Regelung gilt zusätzlich zu harmonisierten Normen oder gemeinsamen Spezifikationen.
- Für kritische Produkte mit digitalen Elementen können strengere spezielle Vorgaben aus anderen EU-Rechtsakten gelten.

D. Besonderheiten

- Die Vermutungswirkung entlastet Anbieter bei der Nachweisführung.
- Sie gilt **nur insoweit**, wie Zertifikate oder Datenkonzepte tatsächlich die Anforderungen abdecken.

III. Zusammenfassung

Datenqualität	Vermutete Erfüllung von Artikel 10 KI-VO Absatz 4 bei realitätsnahen Trainings- und Testdaten
Cybersicherheit	Vermutete Erfüllung von Artikel 15 KI-VObei EU-Zertifizierung oder Konformitätserklärung
Reichweite der Vermutung	Nur soweit Anforderungen vom Nachweis abgedeckt sind
Verhältnis zu Normen	Gilt ergänzend zu Normen und Spezifikationen

IV. Quellenverzeichnis

- Erwägungsgründe 77, 78, 122 KI-VO (EU) 2024/1689

Artikel 43 KI-VO

Konformitätsbewertung

(1) Hat ein Anbieter zum Nachweis, dass ein in Anhang III Nummer 1 aufgeführtes Hochrisiko-KI-System die in Abschnitt 2 festgelegten Anforderungen erfüllt, harmonisierte Normen gemäß Artikel 40 oder gegebenenfalls gemeinsame Spezifikationen gemäß Artikel 41 angewandt, so entscheidet er sich für eines der folgenden Konformitätsbewertungsverfahren auf der Grundlage

a) der internen Kontrolle gemäß Anhang VI oder

b) der Bewertung des Qualitätsmanagementsystems und der Bewertung der technischen Dokumentation unter Beteiligung einer notifizierten Stelle gemäß Anhang VII.

Zum Nachweis, dass sein Hochrisiko-KI-System die in Abschnitt 2 festgelegten Anforderungen erfüllt, befolgt der Anbieter das Konformitätsbewertungsverfahren gemäß Anhang VII, wenn

a) es harmonisierte Normen gemäß Artikel 40 nicht gibt und keine gemeinsamen Spezifikationen gemäß Artikel 41 vorliegen,

b) der Anbieter die harmonisierte Norm nicht oder nur teilweise angewandt hat;

c) die unter Buchstabe a genannten gemeinsamen Spezifikationen zwar vorliegen, der Anbieter sie jedoch nicht angewandt hat;

d) eine oder mehrere der unter Buchstabe a genannten harmonisierten Normen mit einer Einschränkung und nur für den eingeschränkten Teil der Norm veröffentlicht wurden.

Für die Zwecke des Konformitätsbewertungsverfahrens gemäß Anhang VII kann der Anbieter eine der notifizierten Stellen auswählen. Soll das Hochrisiko-KI-System jedoch von Strafverfolgungs-, Einwanderungs- oder Asylbehörden oder von Organen, Einrichtungen oder sonstigen Stellen der Union in Betrieb genommen werden, so übernimmt die in Artikel 74 Absatz 8 bzw. 9 genannte Marktüberwachungsbehörde die Funktion der notifizierten Stelle.

(2) Bei den in Anhang III Nummern 2 bis 8 aufgeführten Hochrisiko-KI-Systemen befolgen die Anbieter das Konformitätsbewertungsverfahren auf

der Grundlage einer internen Kontrolle gemäß Anhang VI, das keine Beteiligung einer notifizierten Stelle vorsieht.

(3) Bei den Hochrisiko-KI-Systemen, die unter die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsakte der Union fallen, befolgt der Anbieter die einschlägigen Konformitätsbewertungsverfahren, die nach diesen Rechtsakten erforderlich sind. Die in Abschnitt 2 dieses Kapitels festgelegten Anforderungen gelten für diese Hochrisiko-KI-Systeme und werden in diese Bewertung einbezogen. Anhang VII Nummern 4.3, 4.4 und 4.5 sowie Nummer 4.6 Absatz 5 finden ebenfalls Anwendung.

Für die Zwecke dieser Bewertung sind die notifizierten Stellen, die gemäß diesen Rechtsakten notifiziert wurden, berechtigt, die Konformität der Hochrisiko-KI-Systeme mit den in Abschnitt 2 festgelegten Anforderungen zu kontrollieren, sofern im Rahmen des gemäß diesen Rechtsakten durchgeführten Notifizierungsverfahrens geprüft wurde, dass diese notifizierten Stellen die in Artikel 31 Absätze 4, 5, 10 und 11 festgelegten Anforderungen erfüllen.

Wenn ein in Anhang I Abschnitt A aufgeführter Rechtsakte es dem Hersteller des Produkts ermöglicht, auf eine Konformitätsbewertung durch Dritte zu verzichten, sofern dieser Hersteller alle harmonisierten Normen, die alle einschlägigen Anforderungen abdecken, angewandt hat, so darf dieser Hersteller nur dann von dieser Möglichkeit Gebrauch machen, wenn er auch harmonisierte Normen oder gegebenenfalls gemeinsame Spezifikationen gemäß Artikel 41, die alle in Abschnitt 2 dieses Kapitels festgelegten Anforderungen abdecken, angewandt hat.

(4) Hochrisiko-KI-Systeme, die bereits Gegenstand eines Konformitätsbewertungsverfahren gewesen sind, werden im Falle einer wesentlichen Änderung einem neuen Konformitätsbewertungsverfahren unterzogen, unabhängig davon, ob das geänderte System noch weiter in Verkehr gebracht oder vom derzeitigen Betreiber weitergenutzt werden soll.

Bei Hochrisiko-KI-Systemen, die nach dem Inverkehrbringen oder der Inbetriebnahme weiterhin dazulernen, gelten Änderungen des Hochrisiko-KI-Systems und seiner Leistung, die vom Anbieter zum Zeitpunkt der ursprünglichen Konformitätsbewertung vorab festgelegt wurden und in den Informationen der technischen Dokumentation gemäß Anhang IV Nummer 2 Buchstabe f enthalten sind, nicht als wesentliche Veränderung;

(5) Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zu erlassen, um die Anhänge VI und VII zu ändern, indem sie sie angesichts des technischen Fortschritts aktualisiert.

(6) Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zur Änderung der Absätze 1 und 2 des vorliegenden Artikels zu erlassen, um die in Anhang III Nummern 2 bis 8 genannten Hochrisiko-KI-Systeme dem Konformitätsbewertungsverfahren gemäß Anhang VII oder Teilen davon zu unterwerfen. Die Kommission erlässt solche delegierten Rechtsakte unter Berücksichtigung der Wirksamkeit des Konformitätsbewertungsverfahrens auf der Grundlage einer internen Kontrolle gemäß Anhang VI hinsichtlich der Vermeidung oder Minimierung der von solchen Systemen ausgehenden Risiken für die Gesundheit und Sicherheit und den Schutz der Grundrechte sowie hinsichtlich der Verfügbarkeit angemessener Kapazitäten und Ressourcen in den notifizierten Stellen.

I. Worum geht es?

Artikel 43 beschreibt die Verfahren, mit denen Anbieter nachweisen müssen, dass ihre Hochrisiko-KI-Systeme die Anforderungen der KI-VO erfüllen. Dabei unterscheidet die Vorschrift zwei Hauptverfahren:

- **Interne Kontrolle** – der Anbieter prüft selbst, ob die Anforderungen erfüllt sind.
- **Externe Kontrolle** – eine unabhängige, offiziell benannte Stelle prüft die Konformität.

Welches Verfahren gilt, hängt vom Systemtyp, den angewandten Normen und Spezifikationen sowie vom Einsatzbereich ab.

II. Detailkommentar

A. Verfahren der internen Kontrolle (Anhang VI KI-VO)

- Anbieter führt die Prüfung selbst durch.
- Gilt zB für Hochrisiko-KI-Systeme aus Anhang III KI-VO Nr 2–8.
- Keine externe Stelle beteiligt.

Beispiel: ***Interne Kontrolle:*** *KI zur Bewerberauswahl (Anhang III Nr 4) mit vollständig angewandten harmonisierten Normen.*

B. Verfahren mit notifizierter Stelle (Anhang VII KI-VO)

- Eine unabhängige Stelle prüft Qualitätsmanagement und technische Dokumentation.
- Verpflichtend, wenn:
  - *keine harmonisierten Normen oder gemeinsamen Spezifikationen vorliegen oder*
  - *Normen/Spezifikationen nur teilweise angewendet wurden oder*
  - *Normen nur eingeschränkt veröffentlicht sind.*
- Bei Systemen für Strafverfolgung, Einwanderung oder Asyl übernimmt die Marktüberwachungsbehörde diese Rolle.

Beispiel: ***Notifizierte Stelle:*** Biometrisches Überwachungssystem ohne anwendbare harmonisierte Normen.

C. Systeme unter anderen EU-Harmonisierungsrechtsakten

- Konformitätsbewertung erfolgt nach den Vorschriften dieser Rechtsakte.
- Anforderungen der KI-VO werden in diese Bewertung integriert.

D. Wesentliche Änderungen

- Bei erheblichen Änderungen muss ein neues Verfahren durchgeführt werden.
- **Ausnahmen**: vorab definierte, erwartete Änderungen bei selbstlernenden Systemen.

E. Besonderheiten

- Die Wahl des Verfahrens beeinflusst Aufwand und Dauer der Marktzulassung.
- Selbstkontrolle ist einfacher, setzt aber die vollständige Anwendung relevanter Normen voraus.

III. Zusammenfassung

Verfahren	Wann verpflichtend?	Beteiligung Dritter?
Interne Kontrolle (Anhang VI KI-VO)	Bei Anhang III KI-VO Nr 2–8 oder vollständiger Anwendung aller Normen	Nein
Notifizierte Stelle (Anhang VII KI-VO)	Bei fehlenden oder unvollständigen Normen/Spezifikationen, eingeschränkter Veröffentlichung	Ja

IV. Quellenverzeichnis

- Erwägungsgründe 78, 123, 124, 125, 126, 128 KI-VO (EU) 2024/1689

Artikel 44 KI-VO

Bescheinigungen

(1) Die von notifizierten Stellen gemäß Anhang VII ausgestellten Bescheinigungen werden in einer Sprache ausgefertigt, die für die einschlägigen Behörden des Mitgliedstaats, in dem die notifizierte Stelle niedergelassen ist, leicht verständlich ist.

(2) Die Bescheinigungen sind für die darin genannte Dauer gültig, die maximal fünf Jahre für unter Anhang I fallende KI-Systeme und maximal vier Jahre für unter Anhang III fallende KI-Systeme beträgt. Auf Antrag des Anbieters kann die Gültigkeit einer Bescheinigung auf der Grundlage einer Neubewertung gemäß den geltenden Konformitätsbewertungsverfahren um weitere Zeiträume von jeweils höchstens fünf Jahren für unter Anhang I fallende KI-Systeme und höchstens vier Jahre für unter Anhang III fallende KI-Systeme verlängert werden. Eine Ergänzung zu einer Bescheinigung bleibt gültig, sofern die Bescheinigung, zu der sie gehört, gültig ist.

(3) Stellt eine notifizierte Stelle fest, dass ein KI-System die in Abschnitt 2 festgelegten Anforderungen nicht mehr erfüllt, so setzt sie die ausgestellte Bescheinigung aus, widerruft sie oder schränkt sie ein, jeweils unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit, sofern die Einhaltung der Anforderungen nicht durch geeignete Korrekturmaßnahmen des Anbieters des Systems innerhalb einer von der notifizierten Stelle gesetzten angemessenen Frist wiederhergestellt wird. Die notifizierte Stelle begründet ihre Entscheidung.

Es muss ein Einspruchsverfahren gegen die Entscheidungen der notifizierten Stellen, auch solche über ausgestellte Konformitätsbescheinigungen, vorgesehen sein.

I. Worum geht es?

Artikel 44 regelt, wie Bescheinigungen über die Konformität von Hochrisiko-KI-Systemen ausgestellt, wie lange sie gültig sind und unter welchen Umständen sie widerrufen, ausgesetzt oder eingeschränkt werden können. Zudem ist ein Einspruchsverfahren gegen Entscheidungen der notifizierten Stellen vorgeschrieben.

II. Detailkommentar

A. Sprache der Bescheinigungen

Müssen in einer Sprache verfasst sein, die für die Behörden des Mitgliedstaates der notifizierten Stelle leicht verständlich ist, also in einer der Amtssprachen der Union.

B. Gültigkeit und Verlängerung

- **Maximale Gültigkeit:**
  - Fünf Jahre für KI-Systeme unter Anhang I KI-VO.
  - Vier Jahre für KI-Systeme unter Anhang III KI-VO.
- **Verlängerung:**
  - Auf Antrag des Anbieters möglich.
  - Erneute Bewertung nach geltendem Konformitätsbewertungsverfahren erforderlich.
  - Ergänzungen gelten so lange wie die zugehörige Hauptbescheinigung.

Beispiel: ***Verlängerung:*** *Ein Anbieter eines Medizinprodukts mit KI-Anteil beantragt nach fünf Jahren eine neue Bescheinigung, nachdem das System erneut bewertet wurde.*

C. Aussetzung, Widerruf, Einschränkung

- Wenn Anforderungen nicht mehr erfüllt sind, kann die notifizierte Stelle Maßnahmen ergreifen.
- Es gilt der **Grundsatz der Verhältnismäßigkeit**.
- Anbieter hat die Möglichkeit, Korrekturmaßnahmen innerhalb einer angemessenen Frist umzusetzen.
- Entscheidungen müssen begründet werden.

Beispiel: ***Aussetzung:*** *Ein Übersetzungstool für Asylverfahren verstößt nachträglich gegen Datenschutzanforderungen; die Bescheinigung wird ausgesetzt, bis die Mängel behoben sind.*

D. Einspruchsverfahren

Pflicht zur Einrichtung eines Verfahrens, um gegen Entscheidungen der notifizierten Stellen vorzugehen.

E. Besonderheiten

- Die Gültigkeitsdauer sorgt für regelmäßige Neubewertungen.
- Verhältnismäßigkeitsgrundsatz schützt vor unverhältnismäßigen Eingriffen.

III. Zusammenfassung

Sprache	Leicht verständlich für nationale Behörden
Gültigkeit	fünf Jahre (Anhang I KI-VO), vier Jahre (Anhang III KI-VO)
Verlängerung	Auf Antrag, nach Neubewertung
Einschränkung/Widerruf	Bei Nichterfüllung der Anforderungen
Einspruchsverfahren	Verpflichtend einzurichten

Artikel 45 KI-VO

Informationspflichten der notifizierten Stellen

(1) Die notifizierten Stellen informieren die notifizierende Behörde über

a) alle Unionsbescheinigungen über die Bewertung der technischen Dokumentation, etwaige Ergänzungen dieser Bescheinigungen und alle Genehmigungen von Qualitätsmanagementsystemen, die gemäß den Anforderungen des Anhangs VII erteilt wurden;

b) alle Verweigerungen, Einschränkungen, Aussetzungen oder Rücknahmen von Unionsbescheinigungen über die Bewertung der technischen Dokumentation oder Genehmigungen von Qualitätsmanagementsystemen, die gemäß den Anforderungen des Anhangs VII erteilt wurden;

c) alle Umstände, die Folgen für den Anwendungsbereich oder die Bedingungen der Notifizierung haben;

d) alle Auskunftsersuchen über Konformitätsbewertungstätigkeiten, die sie von den Marktüberwachungsbehörden erhalten haben;

e) auf Anfrage die Konformitätsbewertungstätigkeiten, denen sie im Anwendungsbereich ihrer Notifizierung nachgegangen sind, und sonstige Tätigkeiten, einschließlich grenzüberschreitender Tätigkeiten und Vergabe von Unteraufträgen, die sie durchgeführt haben.

(2) Jede notifizierte Stelle informiert die anderen notifizierten Stellen über

a) die Genehmigungen von Qualitätsmanagementsystemen, die sie verweigert, ausgesetzt oder zurückgenommen hat, und auf Anfrage die Genehmigungen von Qualitätsmanagementsystemen, die sie erteilt hat;

b) die Bescheinigungen der Union über die Bewertung der technischen Dokumentation und deren etwaige Ergänzungen, die sie verweigert, ausgesetzt oder zurückgenommen oder anderweitig eingeschränkt hat, und auf Anfrage die Bescheinigungen und/oder deren Ergänzungen, die sie ausgestellt hat.

(3) Jede notifizierte Stelle übermittelt den anderen notifizierten Stellen, die ähnlichen Konformitätsbewertungstätigkeiten für die gleichen Arten der KI-Systeme nachgehen, einschlägige Informationen über negative und auf Anfrage über positive Konformitätsbewertungsergebnisse.

(4) Notifizierende Behörden gewährleisten gemäß Artikel 78 die Vertraulichkeit der von ihnen erlangten Informationen.

I. Worum geht es?

Artikel 45 legt fest, welche Informationen notifizierte Stellen an Behörden und andere notifizierte Stellen weitergeben müssen. Ziel ist ein transparenter Informationsfluss, um Qualität und Einheitlichkeit bei Konformitätsbewertungen zu sichern. Gleichzeitig ist die Vertraulichkeit sensibler Daten zu wahren.

II. Detailkommentar

A. Meldungen an die notifizierende Behörde

Umfang der Informationen:

- Ausgestellte Bescheinigungen und Genehmigungen von QMS.
- Ablehnungen, Einschränkungen, Aussetzungen oder Rücknahmen.
- Änderungen, die den Anwendungsbereich oder die Bedingungen der Notifizierung betreffen.
- Anfragen von Marktüberwachungsbehörden.
- Auf Anfrage: Überblick über alle relevanten Tätigkeiten, inkl grenzüberschreitender Arbeiten oder Unteraufträge.

Beispiel: ***Behördenmeldung:*** *Eine notifizierte Stelle widerruft eine Bescheinigung für ein KI-System in der Gesichtserkennung und informiert unverzüglich die zuständige Behörde.*

B. Meldungen an andere notifizierte Stellen

- Austausch zu verweigerten, ausgesetzten oder zurückgenommenen Genehmigungen und Bescheinigungen.
- Auf Anfrage: Informationen zu erteilten Genehmigungen und ausgestellten Bescheinigungen.

- Gegenseitige Weitergabe relevanter negativer und – auf Anfrage – positiver Konformitätsbewertungsergebnisse.

Beispiel: ***Stellenmeldung:*** *Eine Stelle teilt einer anderen mit, dass ein System für Kreditwürdigkeitsprüfungen die Anforderungen nicht mehr erfüllt.*

C. Vertraulichkeit

- **Pflicht der Behörden:** Wahrung der Vertraulichkeit nach Unions- und nationalem Recht.
- Schutz von Geschäftsgeheimnissen, geistigem Eigentum, Sicherheitsinteressen und laufenden Verfahren.

D. Besonderheiten

- Der Artikel dient der **Koordination** zwischen den Prüfstellen.
- Informationsaustausch ist ein **Sicherheitsnetz**, um unsichere oder nicht-konforme Systeme schnell zu identifizieren.
- Vertraulichkeitsregeln stellen sicher, dass die Offenlegungspflicht nicht zu wirtschaftlichen Schäden führt.

III. Zusammenfassung

Empfänger	Notifizierende Behörde, andere notifizierte Stellen
Inhalte	Bescheinigungen, Genehmigungen, Änderungen, Anfragen, Bewertungsergebnisse
Ziel	Transparenz, Qualitätssicherung
Vertraulichkeit	Schutz sensibler Daten muss gewährleistet werden

IV. Quellenverzeichnis

- Erwägungsgrund 167 KI-VO (EU) 2024/1689

Artikel 46 KI-VO

Ausnahme vom Konformitätsbewertungsverfahren

(1) Abweichend von Artikel 43 und auf ein hinreichend begründetes Ersuchen kann eine Marktüberwachungsbehörde das Inverkehrbringen oder die Inbetriebnahme bestimmter Hochrisiko-KI-Systeme im Hoheitsgebiet des betreffenden Mitgliedstaats aus außergewöhnlichen Gründen der öffentlichen Sicherheit, des Schutzes des Lebens und der Gesundheit von Personen, des Umweltschutzes oder des Schutzes wichtiger Industrie- und Infrastrukturanlagen genehmigen. Diese Genehmigung wird auf die Dauer der erforderlichen Konformitätsbewertungsverfahren befristet, wobei den außergewöhnlichen Gründen für die Ausnahme Rechnung getragen wird. Der Abschluss dieser Verfahren erfolgt unverzüglich.

(2) In hinreichend begründeten dringenden Fällen aus außergewöhnlichen Gründen der öffentlichen Sicherheit oder in Fällen einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen können Strafverfolgungsbehörden oder Katastrophenschutzbehörden ein bestimmtes Hochrisiko-KI-System ohne die in Absatz 1 genannte Genehmigung in Betrieb nehmen, sofern diese Genehmigung während der Verwendung oder im Anschluss daran unverzüglich beantragt wird. Falls die Genehmigung gemäß Absatz 1 abgelehnt wird, wird Verwendung des Hochrisiko-KI-Systems mit sofortiger Wirkung eingestellt und sämtliche Ergebnisse und Ausgaben dieser Verwendung werden unverzüglich verworfen.

(3) Die in Absatz 1 genannte Genehmigung wird nur erteilt, wenn die Marktüberwachungsbehörde zu dem Schluss gelangt, dass das Hochrisiko-KI-System die Anforderungen des Abschnitts 2 erfüllt. Die Marktüberwachungsbehörde informiert die Kommission und die anderen Mitgliedstaaten über alle von ihr gemäß den Absätzen 1 und 2 erteilten Genehmigungen. Diese Pflicht erstreckt sich nicht auf sensible operative Daten zu den Tätigkeiten von Strafverfolgungsbehörden.

(4) Erhebt weder ein Mitgliedstaat noch die Kommission innerhalb von 15 Kalendertagen nach Erhalt der in Absatz 3 genannten Mitteilung Einwände gegen die von einer Marktüberwachungsbehörde eines Mitgliedstaats gemäß Absatz 1 erteilte Genehmigung, so gilt diese Genehmigung als gerechtfertigt.

(5) Erhebt innerhalb von 15 Kalendertagen nach Erhalt der in Absatz 3 genannten Mitteilung ein Mitgliedstaat Einwände gegen eine von einer Marktüberwachungsbehörde eines anderen Mitgliedstaats erteilte Genehmigung oder ist die Kommission der Auffassung, dass die Genehmigung mit dem Unionsrecht unvereinbar ist oder dass die Schlussfolgerung der Mitgliedstaaten in Bezug auf die Konformität des in Absatz 3 genannten Systems unbegründet ist, so nimmt die Kommission unverzüglich Konsultationen mit dem betreffenden Mitgliedstaat auf. Die betroffenen Akteure werden konsultiert und erhalten Gelegenheit, dazu Stellung zu nehmen. In Anbetracht dessen entscheidet die Kommission, ob die Genehmigung gerechtfertigt ist. Die Kommission richtet ihren Beschluss an den betroffenen Mitgliedstaat und an die betroffenen Akteure.

(6) Wird die Genehmigung von der Kommission als ungerechtfertigt erachtet, so muss sie von der Marktüberwachungsbehörde des betreffenden Mitgliedstaats zurückgenommen werden.

(7) Für Hochrisiko-KI-Systeme im Zusammenhang mit Produkten, die unter die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, gelten nur die in diesen Harmonisierungsrechtsvorschriften der Union festgelegten Ausnahmen von den Konformitätsbewertungsverfahren.

I. Worum geht es?

Artikel 46 beschreibt Ausnahmeregelungen, bei denen Hochrisiko-KI-Systeme ausnahmsweise ohne vorherige Konformitätsbewertung in Verkehr gebracht oder in Betrieb genommen werden dürfen. Diese Ausnahmen sind nur in außergewöhnlichen Situationen und unter strengen Voraussetzungen zulässig – insb zum Schutz von Menschenleben, öffentlicher Sicherheit, Umwelt und kritischer Infrastruktur.

II. Detailkommentar

A. Genehmigung durch Marktüberwachungsbehörde

- **Voraussetzungen:** Außergewöhnliche Gründe (öffentliche Sicherheit, Schutz von Leben/Gesundheit, Umwelt, kritische Anlagen).

- **Befristung:** Gilt nur für die Dauer des nötigen Konformitätsverfahrens.
- **Ziel:** Schneller Einsatz wichtiger Technik bei gleichzeitiger Nachholung der Prüfung.

B. Dringende Fälle durch Behörden

- **Sonderfall:** Strafverfolgungs- oder Katastrophenschutzbehörden dürfen im Notfall sofort einsetzen.
- **Pflicht:** Genehmigung unverzüglich nachträglich beantragen.
- **Folge bei Ablehnung:** Sofortige Einstellung und Vernichtung aller Ergebnisse.

Beispiel: *Katastrophenschutz*: *Einsatz eines noch nicht zertifizierten KI-Systems zur Erdbeben-Früherkennung unmittelbar nach einer schweren Erschütterung.*

C. Anforderungen und Kontrolle

- Genehmigung nur bei vermuteter Erfüllung der Anforderungen des Abschnitts 2.
- Informationspflicht der nationalen Behörde an Kommission und andere Mitgliedstaaten.
- **Einspruchsfrist**: 15 Kalendertage.
- Kommission kann Genehmigung bestätigen oder die Behörde muss sie zurücknehmen.

D. Besondere Regel für Anhang-I-Produkte

Für diese gelten nur die in den jeweiligen Harmonisierungsrechtsvorschriften vorgesehenen Ausnahmen.

E. Besonderheiten

- **Balance:** Sicherheit vor Schnelligkeit – Ausnahme nur bei zwingender Notwendigkeit.
- **EU-weit abgestimmt:** Einwände anderer Mitgliedstaaten oder der Kommission möglich.
- **Missbrauchsverhinderung:** Zeitliche Befristung und sofortige Beendigung bei Ablehnung.

III. Zusammenfassung

Genehmigung	Marktüberwachungsbehörde bei außergewöhnlichen Gründen
Dringende Fälle	Sofortige Nutzung durch Strafverfolgung/Katastrophenschutz, Genehmigung nachholen
Kontrolle	Meldung an Kommission + Mitgliedstaaten, Einspruchsfrist 15 Tage
Einschränkung	Nur befristet, ggf sofortiger Stopp

IV. Quellenverzeichnis

- Erwägungsgrund 130 KI-VO (EU) 2024/1689

Artikel 47 KI-VO

EU-Konformitätserklärung

(1) Der Anbieter stellt für jedes Hochrisiko-KI-System eine schriftliche maschinenlesbare, physische oder elektronisch unterzeichnete EU-Konformitätserklärung aus und hält sie für einen Zeitraum von 10 Jahren ab dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems für die zuständigen nationalen Behörden bereit. Aus der EU-Konformitätserklärung geht hervor, für welches Hochrisiko-KI-System sie ausgestellt wurde. Eine Kopie der EU-Konformitätserklärung wird den zuständigen nationalen Behörden auf Anfrage übermittelt.

(2) Die EU-Konformitätserklärung muss feststellen, dass das betreffende Hochrisiko-KI-System die in Abschnitt 2 festgelegten Anforderungen erfüllt. Die EU-Konformitätserklärung enthält die in Anhang V festgelegten Informationen und wird in eine Sprache übersetzt, die für die zuständigen nationalen Behörden der Mitgliedstaaten, in denen das Hochrisiko-KI-System in Verkehr gebracht oder bereitgestellt wird, leicht verständlich ist.

(3) Unterliegen Hochrisiko-KI-Systeme anderen Harmonisierungsrechtsvorschriften der Union, die ebenfalls eine EU-Konformitätserklärung vorschreiben, so wird eine einzige EU-Konformitätserklärung ausgestellt, die sich auf alle für das Hochrisiko-KI-System geltenden Rechtsvorschriften der Union bezieht. Die Erklärung enthält alle erforderlichen Informationen zur Feststellung der Harmonisierungsrechtsvorschriften der Union, auf die sich die Erklärung bezieht.

(4) Mit der Ausstellung der EU-Konformitätserklärung übernimmt der Anbieter die Verantwortung für die Erfüllung der in Abschnitt 2 festgelegten Anforderungen. Der Anbieter hält die EU-Konformitätserklärung gegebenenfalls auf dem neuesten Stand.

(5) Der Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zur Aktualisierung des in Anhang V festgelegten Inhalts der EU-Konformitätserklärung zu erlassen, um den genannten Anhang durch die Einführung von Elementen zu ändern, die angesichts des technischen Fortschritts erforderlich werden.

I. Worum geht es?

Artikel 47 legt fest, dass für jedes Hochrisiko-KI-System eine EU-Konformitätserklärung erstellt werden muss. Diese Erklärung bescheinigt, dass das System alle Anforderungen des Abschnitts 2 erfüllt, und dient als rechtlich verbindliche Eigenbestätigung des Anbieters gegenüber Behörden. Sie ist zentraler Nachweis der Konformität und muss zehn Jahre lang verfügbar bleiben.

II. Detailkommentar

A. Pflicht zur Ausstellung

- **Form:** Schriftlich, maschinenlesbar, physisch oder elektronisch signiert.
- **Inhalt:** Muss klar angeben, für welches System sie gilt und bestätigen, dass die Anforderungen erfüllt sind.
    - **Sprache:** Für nationale Behörden leicht verständlich, also in der jeweiligen Amtssprache abzugeben.
    - **Bereithaltung:** 10 Jahre ab Inverkehrbringen/Inbetriebnahme.

B. Einheitliche Erklärung bei mehreren EU-Vorschriften mit Konformitätserklärungen

- **Sinn:** Vermeidung doppelter Dokumente, wenn andere EU-Rechtsakte ebenfalls eine Konformitätserklärung verlangen.
- **Vorgabe:** Eine kombinierte Erklärung mit allen relevanten Vorschriften.

Beispiel: *Ein Hersteller eines KI-gestützten medizinischen Diagnosesystems erstellt eine EU-Konformitätserklärung, die sowohl die KI-VO als auch die Medizinprodukte-Verordnung abdeckt.*

C. Verantwortung und Aktualisierung

- Mit der Unterschrift übernimmt der Anbieter volle Verantwortung für die Einhaltung.
- Erklärung muss aktuell gehalten werden, zB bei Änderungen am System.

D. Anpassungsmöglichkeit durch Kommission

- **Befugnis:** Kommission kann den Inhalt der Erklärung (Anhang V KI-VO) per delegiertem Rechtsakt anpassen.
- **Ziel:** Berücksichtigung technischer Entwicklungen.

E. Besonderheiten

- **Verbindlichkeit:** Die Erklärung ist ein Rechtsdokument – falsche Angaben können rechtliche Folgen haben.
- **Schnittstelle zu Cybersicherheit:** Erfüllung bestimmter Cybersicherheitsanforderungen aus anderen EU-Rechtsakten kann die Anforderungen der KI-VO erfüllen.

Beispiel: *Ein Anbieter aktualisiert die Erklärung, nachdem eine wesentliche Änderung an der Datenverarbeitungslogik vorgenommen wurde.*

III. Zusammenfassung

Form	Schriftlich, maschinenlesbar, physisch/elektronisch signiert
Inhalt	Angaben zum System + Bestätigung der Erfüllung aller Anforderungen
Gültigkeit	Bereithaltung für 10 Jahre
Mehrere EU-Vorschriften mit Konformitätserklärungen	Eine kombinierte Erklärung möglich
Verantwortung	Anbieter trägt volle Verantwortung

IV. Quellenverzeichnis

- Erwägungsgründe 77, 122, 17 KI-VO (EU) 2024/1689

Artikel 48 KI-VO

CE-Kennzeichnung

(1) Für die CE-Kennzeichnung gelten die in Artikel 30 der Verordnung (EG) Nr 765/2008 festgelegten allgemeinen Grundsätze.

(2) Bei digital bereitgestellten Hochrisiko-KI-Systemen wird eine digitale CE-Kennzeichnung nur dann verwendet, wenn sie über die Schnittstelle, von der aus auf dieses System zugegriffen wird, oder über einen leicht zugänglichen maschinenlesbaren Code oder andere elektronische Mittel leicht zugänglich ist.

(3) Die CE-Kennzeichnung wird gut sichtbar, leserlich und dauerhaft an Hochrisiko-KI-Systemen angebracht. Falls die Artikel des Hochrisiko-KI-Systems dies nicht zulässt oder nicht rechtfertigt, wird sie auf der Verpackung bzw. der beigefügten Dokumentation angebracht.

(4) Gegebenenfalls wird der CE-Kennzeichnung die Identifizierungsnummer der für die in Artikel 43 festgelegten Konformitätsbewertungsverfahren zuständigen notifizierten Stelle hinzugefügt. Die Identifizierungsnummer der notifizierten Stelle ist entweder von der Stelle selbst oder nach ihren Anweisungen durch den Anbieter oder den Bevollmächtigten des Anbieters anzubringen. Diese Identifizierungsnummer wird auch auf jeglichem Werbematerial angegeben, in dem darauf hingewiesen wird, dass das Hochrisiko-KI-System die Anforderungen für die CE-Kennzeichnung erfüllt.

(5) Falls Hochrisiko-KI-Systeme ferner unter andere Rechtsvorschriften der Union fallen, in denen die CE-Kennzeichnung auch vorgesehen ist, bedeutet die CE-Kennzeichnung, dass das Hochrisiko-KI-System auch die Anforderungen dieser anderen Rechtsvorschriften erfüllt.

I. Worum geht es?

Artikel 48 regelt die Anbringung der CE-Kennzeichnung für Hochrisiko-KI-Systeme. Sie zeigt an, dass das System den Anforderungen der KI-VO und ggf. weiterer EU-Rechtsvorschriften entspricht. Die Kennzeichnung ist damit der sichtbare Nachweis der Konformität und ermöglicht den freien Verkehr im Binnenmarkt.

II. Detailkommentar

A. Allgemeine Grundsätze

- Verweis auf die Grundsätze in Artikel 30 der Verordnung (EG) Nr 765/2008.
- Einheitliche Bedeutung in allen EU-Staaten.

B. Digitale CE-Kennzeichnung

- **Voraussetzung:** Nur bei rein digital bereitgestellten KI-Systemen.
- **Zugänglichkeit:** Über die Benutzeroberfläche, QR-Code oder andere elektronische Mittel leicht abrufbar.

Beispiel: *Eine ausschließlich cloudbasierte KI erhält eine digitale CE-Kennzeichnung, die über die Nutzeroberfläche abrufbar ist.*

C. Sichtbarkeit und Anbringungsorte

- **Grundsatz**: Gut sichtbar, leserlich und dauerhaft am System angebracht.
- Falls nicht möglich: Auf Verpackung oder Dokumentation.

Beispiel: *Ein KI-gestütztes Produktionsüberwachungssystem wird mit physischer CE-Kennzeichnung am Gehäuse und ergänzend digital im Interface versehen.*

D. Identifizierungsnummer der notifizierten Stelle

- Ergänzung, wenn eine notifizierte Stelle im Konformitätsbewertungsverfahren beteiligt war.
- Identifizierungsnummer wird auch in Werbematerial angegeben.

E. Mehrfachregelungen

- CE-Kennzeichnung gilt auch für andere Rechtsakte, wenn deren Anforderungen erfüllt sind.

F. Besonderheiten

- **Digitale vs. physische Kennzeichnung:** Abhängig von der Bereitstellungsform.
- **Rechtswirkung:** Mitgliedstaaten dürfen den Marktzugang nicht verweigern, wenn ein System korrekt gekennzeichnet ist.

III. Zusammenfassung

Form	Physisch oder digital (bei rein digitaler Bereitstellung)
Anbringung	Sichtbar, leserlich, dauerhaft; ggf auf Verpackung/Dokumentation
Notifizierte Stelle	Identifizierungsnummer ergänzend anbringen
Wirkung	Kennzeichnung gilt auch für andere EU-Rechtsakte

IV. Quellenverzeichnis

- Erwägungsgrund 129 KI-VO (EU) 2024/1689

Artikel 49 KI-VO

Registrierung

(1) Vor dem Inverkehrbringen oder der Inbetriebnahme eines in Anhang III aufgeführten Hochrisiko-KI-Systems — mit Ausnahme der in Anhang III Nummer 2 genannten Hochrisiko-KI-Systeme — registriert der Anbieter oder gegebenenfalls sein Bevollmächtigter sich und sein System in der in Artikel 71 genannten EU-Datenbank.

(2) Vor dem Inverkehrbringen oder der Inbetriebnahme eines Hochrisiko-KI-Systems, bei dem der Anbieter zu dem Schluss gelangt ist, dass es nicht hochriskant gemäß Artikel 6 Absatz 3 ist, registriert dieser Anbieter oder gegebenenfalls sein Bevollmächtigter sich und dieses System in der in Artikel 71 genannten EU-Datenbank.

(3) Vor der Inbetriebnahme oder Verwendung eines in Anhang III aufgeführten Hochrisiko-KI-Systems — mit Ausnahme der in Anhang III Nummer 2 aufgeführten Hochrisiko-KI-Systeme — registrieren sich Betreiber, bei denen es sich um Behörden oder Organe, Einrichtungen oder sonstige Stellen der Union oder in ihrem Namen handelnde Personen handelt, in der in Artikel 71 genannten EU-Datenbank, wählen das System aus und registrieren es dort.

(4) Bei den in Anhang III Nummern 1, 6 und 7 genannten Hochrisiko-KI-Systemen erfolgt in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrolle die Registrierung gemäß den Absätzen 1, 2 und 3 des vorliegenden Artikels in einem sicheren nicht öffentlichen Teil der in Artikel 71 genannten EU-Datenbank und enthält, soweit zutreffend, lediglich die Informationen gemäß

a) Anhang VIII Abschnitt A Nummern 1 bis 10 mit Ausnahme der Nummern 6, 8 und 9,

b) Anhang VIII Abschnitt B Nummern 1 bis 5 sowie Nummern 8 und 9,

c) Anhang VIII Abschnitt C Nummern 1 bis 3,

d) Anhang IX Nummern 1, 2, 3 und Nummer 5.

Nur die Kommission und die in Artikel 74 Absatz 8 genannten nationalen Behörden haben Zugang zu den jeweiligen beschränkten Teilen der EU-Datenbank gemäß Unterabsatz 1 dieses Absatzes.

(5) Die in Anhang III Nummer 2 genannten Hochrisiko-KI-Systeme werden auf nationaler Ebene registriert.

I. Worum geht es?

Artikel 49 legt fest, dass bestimmte Hochrisiko-KI-Systeme vor ihrem Einsatz in einer EU-Datenbank registriert werden müssen. Die Regelung dient der Transparenz, der Marktüberwachung und dem Schutz sensibler Bereiche. Je nach Anwendungsbereich und Artikel des Systems gelten unterschiedliche Registrierungsverfahren – teils öffentlich, teils in gesicherten, nicht öffentlichen Bereichen.

II. Detailkommentar

A. Registrierungspflichten der Anbieter

- **Pflicht zur Registrierung** für alle in Anhang III KI-VO genannten Hochrisiko-KI-Systeme (außer Anhang III Z 2).
- Auch Anbieter, die zu dem Schluss kommen, dass ein System trotz Auflistung **nicht hochriskant** ist, müssen es registrieren.

B. Registrierungspflichten der Betreiber

- Behörden, EU-Organe oder in ihrem Auftrag handelnde Stellen müssen sich und das System **vor Einsatz** registrieren.
- Gilt nur für die in Anhang III KI-VO genannten Systeme (außer Z 2).

Beispiel: *Ein KI-System zur Bewerberauswahl (Anhang III Z 4) muss vor Einsatz durch den Anbieter registriert werden.*

C. Sensible Bereiche

- Betrifft va Systeme in Strafverfolgung, Migration, Asyl, Grenzkontrolle.
- Registrierung erfolgt in einem gesicherten, nicht öffentlichen Teil der Datenbank.

- Zugriff nur für die Kommission und bestimmte nationale Behörden.
- Erfasste Daten sind auf bestimmte Informationskategorien (aus Anhängen VIII und IX) beschränkt.

Beispiel: *Eine Grenzkontroll-KI (Anhang III Z 7) wird nur im gesicherten Bereich eingetragen, um operative Details zu schützen.*

D. Nationale Registrierungspflichten

Systeme nach Anhang III KI-VO Z 2 (kritische Infrastrukturen) werden nur national registriert.

Beispiel: *Ein kritisches Infrastruktur-KI-System (Anhang III Nr 2) wird nicht in der EU-Datenbank, sondern in einer nationalen Datenbank registriert.*

E. Besonderheiten

- **Öffentlichkeit vs. Vertraulichkeit:** Normalerweise ist die EU-Datenbank öffentlich, für sensible Anwendungen aber nur eingeschränkt zugänglich.
- **Transparenzfunktion:** Die öffentliche Datenbank ermöglicht Einblick für Bürger, Forschung und Wirtschaft.
- **Cybersicherheit:** Die Verwaltung der Datenbank muss besonders sicher sein.

III. Zusammenfassung

Registrierungspflicht	Anbieter und Betreiber bestimmter Hochrisiko-KI-Systeme
Ausnahme	Systeme nach Anhang III KI-VO Z 2 nur national
Datenbank	EU-Datenbank nach Artikel 71 KI-VO, teils öffentlich, teils gesichert
Sensible Bereiche	Registrierung nur im nicht öffentlichen Teil
Ziel	Transparenz, Aufsicht, Schutz sensibler Informationen

IV. Quellenverzeichnis

- Erwägungsgrund 131 KI-VO (EU) 2024/1689

Artikel 50 KI-VO

Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme

(1) Die Anbieter stellen sicher, dass KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt sind, so konzipiert und entwickelt werden, dass die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren, es sei denn, dies ist aus Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Diese Pflicht gilt nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten zugelassene KI-Systeme, wenn geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen, es sei denn, diese Systeme stehen der Öffentlichkeit zur Anzeige einer Straftat zur Verfügung.

(2) Anbieter von KI-Systemen, einschließlich KI-Systemen mit allgemeinem Verwendungszweck, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen, stellen sicher, dass die Ausgaben des KI-Systems in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind. Die Anbieter sorgen dafür, dass — soweit technisch möglich — ihre technischen Lösungen wirksam, interoperabel, belastbar und zuverlässig sind und berücksichtigen dabei die Besonderheiten und Beschränkungen der verschiedenen Arten von Inhalten, die Umsetzungskosten und den allgemein anerkannten Stand der Technik, wie er in den einschlägigen technischen Normen zum Ausdruck kommen kann. Diese Pflicht gilt nicht, soweit die KI-Systeme eine unterstützende Funktion für die Standardbearbeitung ausführen oder die vom Betreiber bereitgestellten Eingabedaten oder deren Semantik nicht wesentlich verändern oder wenn sie zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen sind.

(3) Die Betreiber eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung informieren die davon betroffenen natürlichen Personen über den Betrieb des Systems und verarbeiten personenbezogene Daten gemäß den Verordnungen (EU) 2016/679 und (EU) 2018/1725 und der Richtlinie (EU) 2016/680. Diese Pflicht gilt nicht für gesetzlich zur Aufdeckung, Verhütung oder Ermittlung von Straftaten zugelassene KI-Systeme, die zur biometrischen Kategorisierung und Emotionserkennung im Einklang mit dem Unionsrecht verwendet werden, sofern geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen.

(4) Betreiber eines KI-Systems, das Bild-, Ton- oder Videoinhalte erzeugt oder manipuliert, die ein Deepfake sind, müssen offenlegen, dass die Inhalte künstlich erzeugt oder manipuliert wurden. Diese Pflicht gilt nicht, wenn die Verwendung zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen ist. Ist der Inhalt Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms, so beschränken sich die in diesem Absatz festgelegten Transparenzpflichten darauf, das Vorhandensein solcher erzeugten oder manipulierten Inhalte in geeigneter Weise offenzulegen, die die Darstellung oder den Genuss des Werks nicht beeinträchtigt.

Betreiber eines KI-Systems, das Text erzeugt oder manipuliert, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, müssen offenlegen, dass der Text künstlich erzeugt oder manipuliert wurde. Diese Pflicht gilt nicht, wenn die Verwendung zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten gesetzlich zugelassen ist oder wenn die durch KI erzeugten Inhalte einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurden und wenn eine natürliche oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung der Inhalte trägt.

(5) Die in den Absätzen 1 bis 4 genannten Informationen werden den betreffenden natürlichen Personen spätestens zum Zeitpunkt der ersten Interaktion oder Aussetzung in klarer und eindeutiger Weise bereitgestellt. Die Informationen müssen den geltenden Barrierefreiheitsanforderungen entsprechen.

(6) Die Absätze 1 bis 4 lassen die in Kapitel III festgelegten Anforderungen und Pflichten unberührt und berühren nicht andere Transparenzpflichten, die im Unionsrecht oder dem nationalen Recht für Betreiber von KI-Systemen festgelegt sind.

(7) Das Büro für Künstliche Intelligenz fördert und erleichtert die Ausarbeitung von Praxisleitfäden auf Unionsebene, um die wirksame Umsetzung der Pflichten in Bezug auf die Feststellung und Kennzeichnung künstlich erzeugter oder manipulierter Inhalte zu erleichtern. Die Kommission kann Durchführungsrechtsakte zur Genehmigung dieser Praxisleitfäden nach dem in Artikel 56 Absatz 6 festgelegten Verfahren erlassen. Hält sie einen Kodex für nicht angemessen, so kann die Kommission einen Durchführungsrechtsakt gemäß dem in Artikel 98 Absatz

2 genannten Prüfverfahren erlassen, in dem gemeinsame Vorschriften für die Umsetzung dieser Pflichten festgelegt werden.

I. Worum geht es?

Artikel 50 KI-VO schafft besondere Transparenzpflichten für bestimmte KI-Systeme, die mit Menschen interagieren oder Inhalte erzeugen. Ziel ist es, Täuschung, Manipulation und Identitätsbetrug zu verhindern. Nutzer sollen klar erkennen können, ob sie mit einem KI-System interagieren oder ob ein Inhalt künstlich erzeugt bzw verändert wurde. Transparenzpflichten sind dabei in Oberbegriff. Sie umfassen zwei Arten von Pflichten: Kennzeichnungspflichten (zB technische Markierungen wie Wasserzeichen) und Offenlegungspflichten (zB direkte Hinweise für Nutzer beim ersten Kontakt).

II. Detailkommentar

A. Interaktion mit Menschen

- **Informationspflicht bei Interaktion**: Wenn ein KI-System direkt mit Menschen interagiert, muss offengelegt werden, dass es sich um ein KI-System handelt.
- **Ausnahme bei „Offensichtlichkeit“**: Eine zusätzliche Information ist nicht nötig, wenn für eine durchschnittlich aufmerksame und verständige Person sofort erkennbar ist, dass sie mit einer KI zu tun hat (zB Chatbot mit Roboterstimme) Damit ist ein normaler Nutzer gemeint, der grundlegende digitale Kenntnisse hat und sich aufmerksam verhält, ohne Experte zu sein. Dennoch ist der Begriff „offensichtlich“ sehr vage. Für wen etwas offensichtlich ist, hängt stark von Alter, Bildungsgrad und digitaler Kompetenz der Nutzer ab.
- **Ausnahme Strafverfolgung**: KI-Systeme im Rahmen von Ermittlungen sind von der Pflicht befreit, sofern Rechte Dritter durch Schutzmaßnahmen gesichert sind.

Beispiel: *Eine Bank setzt einen Chatbot für Kundenfragen ein. Der Bot muss zu Beginn klarstellen, dass es sich um eine KI handelt. Nutzt die Polizei verdeckte KI-Tools bei Ermittlungen, entfällt diese Pflicht.*

B. Erzeugung synthetischer Inhalte

- **Kennzeichnungspflicht**: Inhalte wie Texte, Bilder, Videos oder Audio, die durch KI erzeugt oder verändert wurden, müssen so markiert werden, dass klar erkennbar ist: „Dieser Inhalt stammt von einer KI."
- **Technische Anforderungen**: Diese Markierung soll technisch zuverlässig sein und sich am aktuellen Stand der Technik orientieren. In der Verordnung heißt es dazu „soweit technisch möglich" – gemeint ist, dass die Kennzeichnung mit den jeweils verfügbaren Methoden umgesetzt werden soll. Zusätzlich muss die Kennzeichnung so gestaltet sein, dass sie auch von anderen Programmen automatisch erkannt werden kann, zB durch ein eingebettetes Wasserzeichen oder ein spezielles Tag im Dateicode. Für normale Nutzer bedeutet das: Die Markierung soll sowohl für Menschen sichtbar als auch für Computer eindeutig erkennbar sein.
- **Ausnahmen**: Unterstützende KI, die Eingaben nicht wesentlich verändert, oder rechtmäßige Strafverfolgungszwecke.

C. Emotionserkennung und biometrische Kategorisierung

- **Informationspflicht**: Nutzer müssen darüber informiert werden, wenn Systeme Emotionen erkennen oder biometrische Daten (zB Alter, Geschlecht, Herkunft) zur Kategorisierung verarbeiten.
- **Verknüpfung mit Datenschutzrecht**: Die Verarbeitung unterliegt zusätzlich den EU-Datenschutzvorschriften (DSGVO, Richtlinie für Polizei und Justiz).
- **Ausnahme Strafverfolgung**: Zulässig bei rechtlicher Grundlage und Schutzmaßnahmen.

Beispiel: *Ein Museum verwendet eine KI, die Emotionen der Besucher analysiert. Vor Betreten der Ausstellung muss klar darauf hingewiesen werden.*

D. Deepfakes und Texte mit öffentlichem Interesse

1. Deepfakes

- **Offenlegungspflicht**: Deepfakes (veränderte oder künstliche Bild-, Ton- oder Videoinhalte) müssen als solche offengelegt werden. Die Verordnung schreibt nicht genau vor, wie – möglich sind etwa ein sichtbares Wasserzeichen, ein Hinweis im Video oder ein begleitender Text. Wichtig ist, dass für die Nutzer klar wird: „Dieser Inhalt wurde künstlich erzeugt oder manipuliert."
- **Ausnahme Kunst und Satire**: Hier reicht ein Hinweis, dass künstliche Inhalte enthalten sind – allerdings in einer Form, die den künstlerischen Ausdruck nicht stört, zum Beispiel ein Vermerk in den Begleitinformationen oder im Abspann.

2. Texte im öffentlichen Interesse

- **Transparenzpflicht**: Wird ein KI-Text veröffentlicht, der die Öffentlichkeit über wichtige Themen informiert, muss er als KI-generiert kenntlich sein.
- **Ausnahme**: Entfällt, wenn der Text von einem Redakteur geprüft und verantwortet wird.

Beispiel: *Eine Online-Zeitung veröffentlicht einen KI-generierten Artikel über neue Gesetze. Ohne menschliche Kontrolle muss die KI-Autorenschaft offengelegt werden.*

E. Zeitpunkt und Form der Information

- **Zeitpunkt**: Spätestens bei der ersten Interaktion oder Aussetzung.
- **Form**: Klar, eindeutig und barrierefrei, auch für Menschen mit Behinderungen.

Beispiel: *Ein KI-Chatbot zeigt zu Beginn ein gut lesbares Hinweisfenster, das den Nutzer informiert.*

F. Verhältnis zu anderen Vorschriften

Transparenzpflichten bestehen zusätzlich zu den allgemeinen Anforderungen der KI-VO und sonstigem EU- oder nationalem Recht.

Beispiel: *Ein hochriskantes KI-System muss sowohl Transparenzpflichten nach Artikel 50 als auch die speziellen Pflichten nach Kapitel III erfüllen.*

G. Rolle des Amtes für Künstliche Intelligenz

- **Praxisleitfäden**: Förderung einheitlicher Standards durch Leitfäden.
- **Kommissionskompetenz**: Möglichkeit zur Verabschiedung gemeinsamer Vorschriften durch Durchführungsrechtsakte.

Beispiel: *Die Kommission könnte verbindliche Standards für Wasserzeichen in KI-Bildern festlegen.*

H. Ethischer Bezug

Hinter den Transparenzpflichten steht ein grundlegender Gedanke: Menschen sollen nicht getäuscht werden und ihre Entscheidungen frei treffen können. Wenn klar erkennbar ist, dass ein Inhalt von einer KI stammt, können Nutzer selbst beurteilen, wie sie diese Information einordnen. Damit schützt die Verordnung die Autonomie und stärkt das Vertrauen in neue Technologien.

III. Zusammenfassung

Kernidee: Nutzer sollen vor Täuschung geschützt werden. Transparenzpflichten schaffen Vertrauen und erleichtern die Einordnung künstlich erzeugter Inhalte.

Bereich	**Ausnahme**
Interaktion mit Menschen	Offensichtlichkeit, Strafverfolgung
Synthetische Inhalte	Unterstützende KI, Strafverfolgung
Emotionserkennung und biometrische Kategorisierung	Strafverfolgung
Deepfakes	Kunst, Satire, Strafverfolgung
Texte im öffentlichen Interesse	Redaktionelle Verantwortung

IV. Quellenverzeichnis

- Erwägungsgrund 132 KI-VO (EU) 2024/1689

Artikel 51 KI-VO

Einstufung von KI-Modellen mit allgemeinem Verwendungszweck als KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko

(1) Ein KI-Modell mit allgemeinem Verwendungszweck wird als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft, wenn eine der folgenden Bedingungen erfüllt ist:

a) Es verfügt über Fähigkeiten mit hohem Wirkungsgrad, die mithilfe geeigneter technischer Instrumente und Methoden, einschließlich Indikatoren und Benchmarks, bewertet werden;

b) einem unter Berücksichtigung der in Anhang XIII festgelegten Kriterien von der Kommission von Amts wegen oder aufgrund einer qualifizierten Warnung des wissenschaftlichen Gremiums getroffenen Entscheidung zufolge verfügt es über Fähigkeiten oder eine Wirkung, die denen gemäß Buchstabe a entsprechen.

(2) Bei einem KI-Modell mit allgemeinem Verwendungszweck wird angenommen, dass es über Fähigkeiten mit hohem Wirkungsgrad gemäß Absatz 1 Buchstabe a verfügt, wenn die kumulierte Menge der für sein Training verwendeten Berechnungen, gemessen in Gleitkommaoperationen, mehr als 10^{25} beträgt.

(3) Die Kommission erlässt gemäß Artikel 97 delegierte Rechtsakte zur Änderung der in den Absätzen 1 und 2 des vorliegenden Artikels aufgeführten Schwellenwerte sowie zur Ergänzung von Benchmarks und Indikatoren vor dem Hintergrund sich wandelnder technologischer Entwicklungen, wie zB algorithmische Verbesserungen oder erhöhte Hardwareeffizienz, wenn dies erforderlich ist, damit diese Schwellenwerte dem Stand der Technik entsprechen.

I. Worum geht es?

Artikel 51 legt fest, wann ein KI-Modell mit allgemeinem Verwendungszweck als besonders gefährlich einzustufen ist, nämlich als Modell mit systemischem Risiko. Der Hintergrund ist, dass sehr leistungsstarke KI-Modelle Auswirkungen auf viele Bereiche gleichzeitig haben können. Sie bergen deshalb ein Risiko für die Gesellschaft und müssen strengeren Regeln folgen.

II. Detailkommentar

A. Ausgangspunkt: Allgemeine KI-Modelle

Allgemeiner Verwendungszweck: Diese Modelle können flexibel in vielen Bereichen eingesetzt werden (zB Sprachmodelle, die Texte, Bilder oder Videos erzeugen).

Beispiel: *Ein großes Sprachmodell kann gleichzeitig im Kundenservice, bei der Erstellung von Programmcode oder bei der Produktion von Nachrichtenbeiträgen genutzt werden.*

B. Kriterien für die Einstufung

1. Hoher Wirkungsgrad

- Modelle gelten als riskant, wenn ihre Fähigkeit technisch nachgewiesen besonders stark ist.
- Hierzu dienen Indikatoren und Benchmarks, also objektive Vergleichswerte aus Tests.

Beispiel: *Ein Modell erreicht bei standardisierten Tests zur Sprachverarbeitung Werte, die weit über allen bisherigen Systemen liegen.*

2. Entscheidung der Kommission

- Auch ohne klare Messwerte kann die Kommission eingreifen.
- Grundlage sind die Kriterien aus Anhang XIII KI-VO und mögliche Warnungen des wissenschaftlichen Gremiums.

Beispiel: *Ein Modell zeigt in der Praxis unerwartet starke Fähigkeiten zur Manipulation von Bildern, weshalb die Kommission es als systemisch riskant einstuft.*

3. Automatische Vermutung

Ab einem Trainingsaufwand von mehr als **10^25 Gleitkommaoperationen** (das entspricht einer unvorstellbar großen Zahl von Rechenoperationen – zur

Veranschaulichung: würde ein normaler Laptop versuchen, diese Menge abzuarbeiten, bräuchte er dafür weit länger als das bisherige Alter des Universums.) wird vermutet, dass das Modell hochwirksam ist.

Dieser Wert ist eine Artikel technische "Schallmauer", die eine klare Grenze zwischen normalen und extrem leistungsstarken Modellen zieht.

Beispiel: *Ein Unternehmen trainiert ein neues Modell mit enormem Rechenaufwand. Auch wenn es noch nicht getestet wurde, gilt es automatisch als riskant.*

C. Anpassungsmöglichkeit

- Die Kommission kann Schwellenwerte, Benchmarks und Indikatoren ändern.
- Grund: Technische Entwicklung schreitet schnell voran (zB effizientere Hardware).
- So bleibt die Regelung flexibel und aktuell.

Beispiel: *Wenn Computer in Zukunft doppelt so schnell rechnen, kann der Schwellenwert angepasst werden, damit er weiter sinnvoll bleibt.*

III. Zusammenfassung

Ausgangslage	Allgemeine KI-Modelle können in vielen Bereichen eingesetzt werden
Einstufung	Erfolgt bei hohem Wirkungsgrad oder Entscheidung der Kommission
Schwellenwert	Automatische Annahme ab 10^25 Gleitkommaoperationen beim Training
Anpassung	Kommission kann Schwellenwerte ändern und Indikatoren ergänzen
Besonderheit	Ziel ist Schutz vor systemischen Risiken großer Modelle

IV. Quellenverzeichnis

- Erwägungsgründe 99, 100, 103 KI-VO (EU) 2024/1689

Artikel 52 KI-VO

Verfahren

(1) Erfüllt ein KI-Modell mit allgemeinem Verwendungszweck die Bedingung gemäß Artikel 51 Absatz 1 Buchstabe a, so teilt der betreffende Anbieter dies der Kommission unverzüglich, in jedem Fall jedoch innerhalb von zwei Wochen, nachdem diese Bedingung erfüllt ist oder bekannt wird, dass sie erfüllt wird, mit. Diese Mitteilung muss die Informationen enthalten, die erforderlich sind, um nachzuweisen, dass die betreffende Bedingung erfüllt ist. Erlangt die Kommission Kenntnis von einem KI-Modell mit allgemeinem Verwendungszweck, das systemische Risiken birgt, die ihr nicht mitgeteilt wurden, so kann sie entscheiden, es als Modell mit systemischen Risiken auszuweisen.

(2) Der Anbieter eines KI-Modells mit allgemeinem Verwendungszweck, das die in Artikel 51 Absatz 1 Buchstabe a genannte Bedingung erfüllt, kann in seiner Mitteilung hinreichend begründete Argumente vorbringen, um nachzuweisen, dass das KI-Modell mit allgemeinem Verwendungszweck, obwohl es diese Bedingung erfüllt, aufgrund seiner besonderen Merkmale außerordentlicherweise keine systemischen Risiken birgt und daher nicht als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko eingestuft werden sollte.

(3) Gelangt die Kommission zu dem Schluss, dass die gemäß Absatz 2 vorgebrachten Argumente nicht hinreichend begründet sind, und konnte der betreffende Anbieter nicht nachweisen, dass das KI-Modell mit allgemeinem Verwendungszweck aufgrund seiner besonderen Merkmale keine systemischen Risiken aufweist, weist sie diese Argumente zurück, und das KI-Modell mit allgemeinem Verwendungszweck gilt als KI-Modell mit allgemeiner Zweckbestimmung mit systemischem Risiko.

(4) Die Kommission kann ein KI-Modell mit allgemeinem Verwendungszweck von Amts wegen oder aufgrund einer qualifizierten Warnung des wissenschaftlichen Gremiums gemäß Artikel 90 Absatz 1 Buchstabe a auf der Grundlage der in Anhang XIII festgelegten Kriterien als KI-Modell mit systemischen Risiken ausweisen.

Die Kommission ist befugt, gemäß Artikel 97 delegierte Rechtsakte zu erlassen, um Anhang XIII zu ändern, indem die in dem genannten Anhang genannten Indikatoren präzisiert und aktualisiert werden.

(5) Stellt der Anbieter, dessen Modell gemäß Absatz 4 als KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko ausgewiesen wurde, einen entsprechenden Antrag, berücksichtigt die Kommission den Antrag und kann entscheiden, erneut zu prüfen, ob beim KI-Modell mit allgemeinem Verwendungszweck auf der Grundlage der in Anhang XIII festgelegten Kriterien immer noch davon ausgegangen werden kann, dass es systemische Risiken aufweist. Dieser Antrag muss objektive, detaillierte und neue Gründe enthalten, die sich seit der Entscheidung zur Ausweisung ergeben haben. Die Anbieter können frühestens sechs Monate nach der Entscheidung zur Ausweisung eine Neubewertung beantragen. Entscheidet die Kommission nach ihrer Neubewertung, die Ausweisung als KI-Modell mit allgemeiner Zweckbestimmung mit systemischem Risiko beizubehalten, können die Anbieter frühestens sechs Monate nach dieser Entscheidung eine Neubewertung beantragen.

(6) Die Kommission stellt sicher, dass eine Liste von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko veröffentlicht wird, und hält diese Liste unbeschadet der Notwendigkeit, Rechte des geistigen Eigentums und vertrauliche Geschäftsinformationen oder Geschäftsgeheimnisse im Einklang mit dem Unionsrecht und dem nationalen Recht zu achten und zu schützen, auf dem neuesten Stand.

I. Worum geht es?

Artikel 52 regelt das Verfahren zur Einstufung von KI-Modellen mit allgemeinem Verwendungszweck als Modelle mit systemischem Risiko. Ziel ist es, sicherzustellen, dass Modelle, die besonders leistungsfähig sind und damit potenziell große gesellschaftliche Auswirkungen haben, frühzeitig von der Kommission erfasst und überwacht werden. Anbieter müssen solche Modelle melden, die Kommission kann sie einstufen und eine Liste veröffentlichen. Gleichzeitig wird den Anbietern ein Recht auf Gegenvortrag eingeräumt.

II. Detailkommentar

A. Mitteilungspflicht der Anbieter

- **Pflicht zur Mitteilung**: Sobald ein KI-Modell die Voraussetzungen für ein mögliches systemisches Risiko erfüllt, muss der Anbieter dies innerhalb von zwei Wochen der Kommission melden.
- **Inhalt der Mitteilung**: Sie muss die notwendigen Informationen enthalten, damit die Kommission prüfen kann, ob die Voraussetzungen tatsächlich erfüllt sind.

B. Möglichkeit des Gegenvortrags

- **Besondere Merkmale**: Anbieter können argumentieren, dass ihr Modell trotz Erfüllung der Schwellenwerte keine systemischen Risiken birgt.
- **Begründungspflicht**: Die Argumente müssen detailliert und nachvollziehbar sein.
- **Folge bei Ablehnung**: Gelingt der Nachweis nicht, gilt das Modell automatisch als Modell mit systemischem Risiko.

Beispiel: *Ein Modell wird zwar mit sehr vielen Daten trainiert, ist aber auf ein sehr spezielles Fachgebiet beschränkt (zB chemische Formeln) und hat keinen Einfluss auf die breite Gesellschaft. Der Anbieter kann darlegen, dass keine systemischen Risiken bestehen.*

C. Einstufung durch die Kommission

- **Von Amts wegen**: Die Kommission kann selbst tätig werden, wenn sie von einem möglichen Risiko erfährt.
- **Qualifizierte Warnung**: Auch ein Hinweis des wissenschaftlichen Gremiums kann eine Einstufung auslösen.
- **Kriterien in Anhang XIII KI-VO**: Die Kommission muss sich bei ihrer Entscheidung an festgelegte Kriterien halten. Über delegierte Rechtsakte kann die Kommission die Kriterien anpassen und aktualisieren.

D. Neubewertung auf Antrag

- **Antrag des Anbieters**: Wenn ein Modell als systemisches Risiko eingestuft wurde, kann der Anbieter nach sechs Monaten eine Neubewertung beantragen.
- **Voraussetzungen**: Der Antrag muss objektive, neue und detaillierte Gründe enthalten.
- **Wiederholte Neubewertung**: Wird die Einstufung bestätigt, ist erneut frühestens nach sechs Monaten ein Antrag möglich.

Beispiel: *Ein Modell wurde zunächst als systemisches Risiko eingestuft, später aber so angepasst, dass es deutlich eingeschränkter nutzbar ist. Der Anbieter kann eine Neubewertung beantragen.*

E. Veröffentlichung einer Liste

- **Verpflichtung der Kommission**: Eine aktuelle Liste der Modelle mit systemischem Risiko muss veröffentlicht werden.
- **Schutzinteressen**: Dabei sind geistige Eigentumsrechte und Geschäftsgeheimnisse zu wahren.
- **Funktion**: Die Liste schafft Transparenz für Unternehmen, Behörden und die Öffentlichkeit.

F. Besonderheiten

- **Früherkennung**: Anbieter wissen oft schon vor Abschluss des Trainings wissen, ob ihr Modell die relevanten Schwellenwerte erreichen wird.
- **Quelloffene Modelle**: Bei Open-Source-Modellen ist die rechtzeitige Mitteilung besonders wichtig, weil nach Veröffentlichung eine nachträgliche Kontrolle kaum möglich ist.

- **Zusammenarbeit mit dem KI-Büro**: Frühzeitige Informationen helfen der Kommission, sich vorzubereiten und die Anbieter einzubinden.

III. Zusammenfassung

Mitteilungspflicht	Anbieter müssen binnen zwei Wochen melden, wenn ein Modell die Voraussetzungen für systemisches Risiko erfüllt.
Gegenvortrag	Anbieter können nachweisen, dass trotz Erfüllung der Schwellenwerte keine systemischen Risiken bestehen.
Entscheidung der Kommission	Bei unzureichender Begründung oder von Amts wegen kann die Kommission das Modell als Risiko einstufen.
Neubewertung	Anbieter können frühestens nach sechs Monaten eine Neubewertung beantragen, mit neuen objektiven Gründen.
Veröffentlichung	Die Kommission führt und aktualisiert eine öffentliche Liste der riskanten Modelle.
Besonderheiten	Wichtig für Open-Source-Modelle, da nach Veröffentlichung kaum Korrekturen möglich sind.

IV. Quellenverzeichnis

- Erwägungsgrund 112 KI-VO (EU) 2024/1689

Artikel 53 KI-VO

Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

(1) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

a) erstellen und aktualisieren die technische Dokumentation des Modells, einschließlich seines Trainings- und Testverfahrens und der Ergebnisse seiner Bewertung, die mindestens die in Anhang XI aufgeführten Informationen enthält, damit sie dem Büro für Künstliche Intelligenz und den zuständigen nationalen Behörden auf Anfrage zur Verfügung gestellt werden kann;

b) erstellen und aktualisieren Informationen und die Dokumentation und stellen sie Anbietern von KI-Systemen zur Verfügung, die beabsichtigen, das KI-Modell mit allgemeinem Verwendungszweck in ihre KI-Systeme zu integrieren. Unbeschadet der Notwendigkeit, die Rechte des geistigen Eigentums und vertrauliche Geschäftsinformationen oder Geschäftsgeheimnisse im Einklang mit dem Unionsrecht und dem nationalen Recht zu achten und zu schützen, müssen die Informationen und die Dokumentation

i) die Anbieter von KI-Systemen in die Lage versetzen, die Fähigkeiten und Grenzen des KI-Modells mit allgemeinem Verwendungszweck gut zu verstehen und ihren Pflichten gemäß dieser Verordnung nachzukommen, und

ii) zumindest die in Anhang XII genannten Elemente enthalten;

c) bringen eine Strategie zur Einhaltung des Urheberrechts der Union und damit zusammenhängender Rechte und insbesondere zur Ermittlung und Einhaltung eines gemäß Artikel 4 Absatz 3 der Richtlinie (EU) 2019/790 geltend gemachten Rechtsvorbehalts, auch durch modernste Technologien, auf den Weg;

d) erstellen und veröffentlichen eine hinreichend detaillierte Zusammenfassung der für das Training des KI-Modells mit allgemeinem Verwendungszweck verwendeten Inhalte nach einer vom Büro für Künstliche Intelligenz bereitgestellten Vorlage.

(2) Die Pflichten gemäß Absatz 1 Buchstaben a und b gelten nicht für Anbieter von KI-Modellen, die im Rahmen einer freien und quelloffenen Lizenz bereitgestellt werden, die den Zugang, die Nutzung, die Änderung und

die Verbreitung des Modells ermöglicht und deren Parameter, einschließlich Gewichte, Informationen über die Modellarchitektur und Informationen über die Modellnutzung, öffentlich zugänglich gemacht werden. Diese Ausnahme gilt nicht für KI-Modellen mit allgemeinem Verwendungszweck mit systemischen Risiken.

(3) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck arbeiten bei der Ausübung ihrer Zuständigkeiten und Befugnisse gemäß dieser Verordnung erforderlichenfalls mit der Kommission und den zuständigen nationalen Behörden zusammen.

(4) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck können sich bis zur Veröffentlichung einer harmonisierten Norm auf Praxisleitfäden im Sinne des Artikels 56 stützen, um die Einhaltung der in Absatz 1 des vorliegenden Artikels genannten Pflichten nachzuweisen. Die Einhaltung der harmonisierten europäischen Norm begründet für die Anbieter die Vermutung der Konformität, insoweit diese Normen diese Verpflichtungen abdecken. Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die keinen genehmigten Praxisleitfaden befolgen oder eine harmonisierte europäische Norm nicht einhalten, müssen geeignete alternative Verfahren der Einhaltung aufzeigen, die von der Kommission zu bewerten sind.

(5) Um die Einhaltung von Anhang XI, insbesondere Nummer 2 Buchstaben d und e, zu erleichtern, ist die Kommission befugt, gemäß Artikel 97 delegierte Rechtsakte zu erlassen, um die Mess- und Berechnungsmethoden im Einzelnen festzulegen, damit eine vergleichbare und überprüfbare Dokumentation ermöglicht wird.

(6) Die Kommission ist befugt, gemäß Artikel 97 Absatz 2 delegierte Rechtsakte zu erlassen, um die Anhänge XI und XII vor dem Hintergrund sich wandelnder technologischer Entwicklungen zu ändern.

(7) Jegliche Informationen oder Dokumentation, die gemäß diesem Artikel erlangt werden, einschließlich Geschäftsgeheimnisse, werden im Einklang mit den in Artikel 78 festgelegten Vertraulichkeitspflichten behandelt.

I. Worum geht es?

Artikel 53 regelt die besonderen Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck. Diese Modelle bilden die Grundlage für viele nachgelagerte Systeme, die von anderen Anbietern genutzt werden.

Ziel des Artikels ist es, Transparenz, Nachvollziehbarkeit und Rechtskonformität zu schaffen. Anbieter solcher Modelle müssen deshalb technische Dokumentationen erstellen, Informationen für nachgelagerte Anbieter bereitstellen, eine Urheberrechtsstrategie entwickeln und eine Zusammenfassung der Trainingsdaten veröffentlichen. Gleichzeitig werden Ausnahmen für Open-Source-Modelle vorgesehen, solange keine systemischen Risiken bestehen.

I. Detailkommentar

A. Technische Dokumentation

- **Pflicht zur Dokumentation**: Anbieter müssen eine umfassende technische Dokumentation über ihr Modell erstellen und laufend aktualisieren. Diese enthält ua Trainings- und Testverfahren sowie Bewertungsergebnisse.
- **Zweck**: Behörden wie das Büro für Künstliche Intelligenz sollen auf Anfrage prüfen können, ob das Modell regelkonform entwickelt und eingesetzt wird.

Beispiel: *Ein Unternehmen entwickelt ein Sprachmodell. Es muss detailliert darlegen, mit welchen Daten trainiert wurde und wie die Qualität und Sicherheit getestet wurden.*

B. Informationen für nachgelagerte Anbieter

- **Transparenz**: Anbieter müssen anderen Unternehmen, die das Modell in ihre Systeme einbauen, klare Informationen liefern.
- **Inhalte**: Diese Informationen müssen sowohl die Fähigkeiten als auch die Grenzen des Modells erläutern. Zusätzlich müssen Mindestangaben nach Anhang XII KI-VO bereitgestellt werden.
- **Abwägung mit Geheimnisschutz**: Geschäftsgeheimnisse und Rechte an geistigem Eigentum müssen nicht proaktiv offengelegt werden, der integrierende Anbieter muss das KI-Modell allerdings gut verstehen können.

C. Urheberrechtsstrategie

- **Pflicht zur Einhaltung des Urheberrechts**: Anbieter müssen Strategien entwickeln, um sicherzustellen, dass beim Training verwendete Daten keine Urheberrechte verletzen.
- **Praktische Umsetzung**: Moderne Technologien zur Erkennung urheberrechtlich geschützter Inhalte sollen genutzt werden.

Beispiel: *Ein Anbieter prüft seine Trainingsdatenbank systematisch darauf, ob Werke enthalten sind, die mit einem Urheberrechtsvorbehalt versehen wurden.*

D. Veröffentlichung einer Trainingsdaten-Zusammenfassung

- **Transparenz für Betroffene**: Anbieter müssen eine allgemein verständliche Zusammenfassung der verwendeten Trainingsdaten veröffentlichen.
- **Form**: Diese erfolgt nach einer standardisierten Vorlage des Büros für Künstliche Intelligenz.
- **Inhalt**: Keine technische Detailtiefe, sondern Beschreibung wichtiger Datenquellen, zB große Datenbanken oder Archive.

Beispiel: *Ein Modellanbieter gibt bekannt, dass sein System mit einer Mischung aus Wikipedia-Artikeln, europäischem Rechtsmaterial und öffentlichen Datensätzen trainiert wurde.*

E. Ausnahme für Open-Source-Modelle

- **Grundsatz**: Open-Source-Anbieter sind von einigen Dokumentations- und Informationspflichten befreit.
- **Voraussetzung**: Das Modell muss frei zugänglich sein, inklusive der Parameter (Gewichte, Architektur, Nutzungsinformationen).
- **Einschränkung**: Bei systemischem Risiko greift die Ausnahme nicht. Zudem bleibt die Pflicht zur Urheberrechtsstrategie und zur Zusammenfassung der Trainingsdaten bestehen.

Beispiel: *Ein frei verfügbares Open-Source-Modell ist grundsätzlich von Dokumentationspflichten befreit. Wird es jedoch so mächtig, dass es als riskant gilt, greifen wieder volle Transparenzpflichten.*

F. Zusammenarbeit mit Behörden

Anbieter müssen auf Anfrage mit der Kommission und nationalen Behörden zusammenarbeiten.

G. Bezug zu Normen und Leitfäden

Anbieter können auf Leitfäden oder harmonisierte Standards zurückgreifen, um ihre Pflichten nachzuweisen. Fehlen solche Standards, müssen Anbieter eigene Verfahren entwickeln, die von der Kommission geprüft werden.

H. Delegierte Rechtsakte

Die Kommission kann künftig Methoden zur Messung und Dokumentation präzisieren und die Anhänge XI und XII an technologische Entwicklungen anpassen.

I. Vertraulichkeit

Alle im Rahmen des Artikels erlangten Informationen unterliegen strengen Vertraulichkeitsvorschriften.

II. Zusammenfassung

Kernpflicht	Inhalt	Besonderheit
Technische Dokumentation	Erstellung und Aktualisierung mit Mindestangaben nach Anhang XI KI-VO	Zugriff für Behörden
Informationen für integrierende Anbieter	Bereitstellung von Fähigkeiten und Grenzen, Mindestangaben	Schutz von Geschäftsgeheimnissen bleibt gewahrt

	nach Anhang XII KI-VO	
Urheberrechtsstrategie	Nachweis der Einhaltung von Urheberrechten, Einsatz modernster Technologien	Pflicht gilt immer, auch bei Open-Source
Trainingsdaten-Zusammenfassung	Veröffentlichung nach Standardvorlage, Beschreibung wichtiger Datenquellen	Keine Detailoffenlegung nötig
Ausnahme Open-Source	Erleichterungen bei Dokumentation und Informationspflichten	Keine Ausnahme bei systemischen Risiken
Zusammenarbeit mit Behörden	Pflicht zur Kooperation	Gilt für alle Anbieter
Bezug zu Normen	Nutzung harmonisierter Standards oder Leitfäden möglich	Alternative Verfahren zulässig
Delegierte Rechtsakte	Anpassung der Anhänge XI und XII, Festlegung von Messmethoden	Flexibilität bei technologischem Fortschritt
Vertraulichkeit	Strenger Schutz aller erhaltenen Informationen	Geschäftsgeheimnisse bleiben geschützt

III. Quellenverzeichnis

- Erwägungsgründe 101, 102, 104, 107, 108 KI-VO (EU) 2024/1689

Artikel 54 KI-VO

Bevollmächtigte der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

(1) Anbieter, die in Drittländern niedergelassen sind, benennen vor dem Inverkehrbringen eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt schriftlich einen in der Union niedergelassenen Bevollmächtigten.

(2) Der Anbieter muss seinem Bevollmächtigten ermöglichen, die Aufgaben wahrzunehmen, die im vom Anbieter erhaltenen Auftrag festgelegt sind.

(3) Der Bevollmächtigte nimmt die Aufgaben wahr, die in seinem vom Anbieter erhaltenen Auftrag festgelegt sind. Er stellt dem Büro für Künstliche Intelligenz auf Anfrage eine Kopie des Auftrags in einer der Amtssprachen der Institutionen der Union bereit. Für die Zwecke dieser Verordnung ermächtigt der Auftrag den Bevollmächtigten zumindest zur Wahrnehmung folgender Aufgaben:

a) Überprüfung, ob die technische Dokumentation gemäß Anhang XI erstellt wurde und alle Pflichten gemäß Artikel 53 und gegebenenfalls gemäß Artikel 55 vom Anbieter erfüllt wurden;

b) Bereithaltung einer Kopie der technischen Dokumentation gemäß Anhang XI für das Büro für Künstliche Intelligenz und die zuständigen nationalen Behörden für einen Zeitraum von zehn Jahren nach dem Inverkehrbringen des KI-Modells mit allgemeinem Verwendungszweck und der Kontaktdaten des Anbieters, der den Bevollmächtigten benannt hat;

c) Bereitstellung sämtlicher zum Nachweis der Einhaltung der Pflichten gemäß diesem Kapitel erforderlichen Informationen und Dokumentation, einschließlich der unter Buchstabe b genannten Informationen und Dokumentation, an das Büro für Künstliche Intelligenz auf begründeten Antrag;

d) Zusammenarbeit mit dem Büro für Künstliche Intelligenz und den zuständigen Behörden auf begründeten Antrag bei allen Maßnahmen, die sie im Zusammenhang mit einem KI-Modell mit allgemeinem Verwendungszweck ergreifen, auch wenn das Modell in KI-Systeme integriert ist, die in der Union in Verkehr gebracht oder in Betrieb genommen werden.

(4) Mit dem Auftrag wird der Bevollmächtigte ermächtigt, neben oder anstelle des Anbieters als Ansprechpartner für das Büro für Künstliche Intelligenz oder die zuständigen Behörden in allen Fragen zu dienen, die die Gewährleistung der Einhaltung dieser Verordnung betreffen.

(5) Der Bevollmächtigte beendet den Auftrag, wenn er der Auffassung ist oder Grund zu der Annahme hat, dass der Anbieter gegen seine Pflichten gemäß dieser Verordnung verstößt. In einem solchen Fall informiert er auch das Büro für Künstliche Intelligenz unverzüglich über die Beendigung des Auftrags und die Gründe dafür.

(6) Die Pflicht gemäß diesem Artikel gilt nicht für Anbieter von KI-Modellen, die im Rahmen einer freien und quelloffenen Lizenz bereitgestellt werden, die den Zugang, die Nutzung, die Änderung und die Verbreitung des Modells ermöglicht und deren Parameter, einschließlich Gewichte, Informationen über die Modellarchitektur und Informationen über die Modellnutzung, öffentlich zugänglich gemacht werden, es sei denn, die KI-Modelle mit allgemeinem Verwendungszweck bergen systemische Risiken.

I. Worum geht es?

Artikel 54 regelt die Pflicht für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die außerhalb der EU ansässig sind, einen in der EU niedergelassenen Bevollmächtigten zu benennen. Dieser Bevollmächtigte fungiert als zentraler Ansprechpartner für die Behörden und sorgt dafür, dass die rechtlichen Vorgaben der KI-VO eingehalten werden. Die Vorschrift soll sicherstellen, dass auch Anbieter aus Drittländern den europäischen Aufsichtsbehörden gegenüber rechenschaftspflichtig bleiben.

II. Detailkommentar

A. Benennungspflicht

Jeder Anbieter aus einem Drittland muss vor dem Inverkehrbringen seines KI-Modells in der EU einen Bevollmächtigten benennen.

- **Schriftform**: Die Benennung muss schriftlich erfolgen, um klare Nachweise zu schaffen.

- **Ziel**: Damit wird sichergestellt, dass die Behörden jederzeit einen Ansprechpartner in der EU haben.

Beispiel: *Ein US-Unternehmen möchte ein großes Sprachmodell in Europa vermarkten. Es muss vorher einen in der EU ansässigen Vertreter benennen, der die Kommunikation mit den Behörden übernimmt.*

B. Aufgaben und Befugnisse des Bevollmächtigten

1. **Technische Dokumentation prüfen**: Der Bevollmächtigte muss sicherstellen, dass die erforderliche Dokumentation vorliegt und die Anbieterpflichten eingehalten wurden.
2. **Dokumentation bereithalten**: Er muss die technischen Unterlagen für zehn Jahre verfügbar machen.
3. **Informationen bereitstellen**: Auf Anfrage muss er den Behörden alle notwendigen Nachweise vorlegen.
4. **Zusammenarbeit mit Behörden**: Er ist verpflichtet, aktiv mit dem Büro für Künstliche Intelligenz und den nationalen Behörden zusammenzuarbeiten.

Beispiel: *Eine nationale Aufsichtsbehörde fordert Einsicht in die Dokumentation eines KI-Modells. Der Bevollmächtigte muss die Unterlagen vorlegen.*

C. Stellung als Ansprechpartner

- **Ansprechpartner neben oder statt des Anbieters**: Der Bevollmächtigte kann direkt mit den Behörden kommunizieren und ersetzt damit in vielen Fällen den Anbieter selbst.
- **Praktische Bedeutung**: Für die Behörden erleichtert dies die Durchsetzung der Vorschriften erheblich.

Beispiel: *Wenn die Kommission Nachfragen zu einem Modell hat, kann sie direkt den Bevollmächtigten anschreiben, ohne den Anbieter im Ausland kontaktieren zu müssen.*

D. Pflicht zur Vertragsbeendigung

- **Beendigung bei Verstößen**: Stellt der Bevollmächtigte fest, dass der Anbieter gegen die KI-VO verstößt, muss er den Auftrag beenden.
- **Meldepflicht**: Gleichzeitig muss er das Büro für Künstliche Intelligenz unverzüglich informieren und die Gründe nennen.
- **Sinn und Zweck**: Der Bevollmächtigte darf nicht als bloßer Erfüllungsgehilfe dienen, sondern muss eigenständig zur Durchsetzung beitragen.

E. Ausnahme für Open-Source-Modelle

- **Keine Pflicht bei Open Source**: Wenn ein KI-Modell unter einer freien, quelloffenen Lizenz bereitgestellt wird und die wesentlichen Informationen öffentlich zugänglich sind, entfällt die Pflicht zur Benennung.
- **Einschränkung bei systemischen Risiken**: Die Ausnahme gilt jedoch nicht, wenn das Modell erhebliche Risiken für das Gemeinwesen mit sich bringt.
- **Abwägung**: Damit wird die Open-Source-Entwicklung geschützt, zugleich aber ein Sicherheitsnetz für risikoreiche Modelle geschaffen.

Beispiel: *Ein Forschungsinstitut veröffentlicht ein Open-Source-Modell samt Architektur und Gewichten. Es braucht keinen Bevollmächtigten. Stellt sich aber heraus, dass das Modell für kritische Infrastrukturen missbraucht werden kann, entfällt die Ausnahme.*

III. III. Zusammenfassung

Benennungspflicht	Anbieter aus Drittländern müssen einen Bevollmächtigten in der EU benennen.
Aufgaben	Dokumentation prüfen, bereithalten, Informationen liefern, Behördenkooperation.
Ansprechpartner	Bevollmächtigter ist direkter Kontakt für die Behörden.

Vertragsbeendigung	Pflicht zur Kündigung bei Verstößen des Anbieters und Information der Behörden.
Ausnahme	Keine Pflicht für Open-Source-Modelle, außer bei systemischen Risiken.

IV. Quellenverzeichnis

- Erwägungsgrund 82 KI-VO (EU) 2024/1689

Artikel 55 KI-VO

Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko

(1) Zusätzlich zu den in den Artikeln 53 und 54 aufgeführten Pflichten müssen Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko

a) eine Modellbewertung mit standardisierten Protokollen und Instrumenten, die dem Stand der Technik entsprechen, durchführen, wozu auch die Durchführung und Dokumentation von Angriffstests beim Modell gehören, um systemische Risiken zu ermitteln und zu mindern,

b) mögliche systemische Risiken auf Unionsebene — einschließlich ihrer Ursachen —, die sich aus der Entwicklung, dem Inverkehrbringen oder der Verwendung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko ergeben können, bewerten und mindern,

c) einschlägige Informationen über schwerwiegende Vorfälle und mögliche Abhilfemaßnahmen erfassen und dokumentieren und das Büro für Künstliche Intelligenz und gegebenenfalls die zuständigen nationalen Behörden unverzüglich darüber unterrichten,

d) ein angemessenes Maß an Cybersicherheit für die KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko und die physische Infrastruktur des Modells gewährleisten.

(2) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko können sich bis zur Veröffentlichung einer harmonisierten Norm auf Praxisleitfäden im Sinne des Artikels 56 stützen, um die Einhaltung der in Absatz 1 des vorliegenden Artikels genannten Pflichten nachzuweisen. Die Einhaltung der harmonisierten europäischen Norm begründet für die Anbieter die Vermutung der Konformität, insoweit diese Normen diese Verpflichtungen abdecken. Anbieter von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko, die einen genehmigten Praxisleitfaden nicht befolgen oder eine harmonisierte europäische Norm nicht einhalten, müssen geeignete alternative Verfahren der Einhaltung aufzeigen, die von der Kommission zu bewerten sind.

(3) Jegliche Informationen oder Dokumentation, die gemäß diesem Artikel erlangt werden, werden im Einklang mit den in Artikel 78 festgelegten Vertraulichkeitspflichten behandelt.

I. Worum geht es?

Artikel 55 legt besondere Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die ein systemisches Risiko bergen, fest. Diese Modelle können aufgrund ihrer Vielseitigkeit und Leistungsfähigkeit große Auswirkungen auf Gesellschaft, Wirtschaft und Sicherheit haben. Der Artikel verpflichtet Anbieter dazu, Risiken umfassend zu prüfen, Sicherheitsmaßnahmen zu ergreifen und Transparenz gegenüber Behörden herzustellen. Damit sollen Gefahren wie Missbrauch, Fehlfunktionen oder massive gesellschaftliche Störungen begrenzt werden.

II. Detailkommentar

A. Hintergrund und Einordnung

- **Abgrenzung zu KI-Systemen**: KI-Modelle sind die Grundlage von KI-Systemen, aber noch keine fertigen Systeme. Sie werden erst durch zusätzliche Komponenten zu einem KI-System. Dennoch sind bestimmte Modelle so mächtig, dass sie schon als Modell strenge Auflagen erhalten (vgl Ausführungen zu Artikel 3 KI-VO Z 1).
- **Systemisches Risiko**: Gemeint sind Risiken, die nicht nur einzelne Nutzer betreffen, sondern potenziell die gesamte Gesellschaft oder zentrale Infrastrukturen. Beispiel: groß angelegte Desinformationskampagnen mit Hilfe von generativen Sprachmodellen.

B. Pflichten der Anbieter

1. Modellbewertung und Angriffstests

- Anbieter müssen ihre Modelle nach dem Stand der Technik überprüfen. Dazu gehören standardisierte Protokolle und Tests.
- Angriffstests dienen dazu, Schwachstellen bewusst zu provozieren, um die Robustheit und Sicherheit des Modells zu prüfen.

2. Bewertung und Minderung systemischer Risiken

- Anbieter müssen mögliche großflächige Folgen analysieren, die aus Entwicklung, Vertrieb oder Nutzung entstehen können.
- Risiken sollen nicht nur erkannt, sondern auch durch geeignete Maßnahmen reduziert werden.

3. Meldung schwerwiegender Vorfälle

- Anbieter sind verpflichtet, schwerwiegende Zwischenfälle und Abhilfemaßnahmen zu dokumentieren.
- Sie müssen das Büro für Künstliche Intelligenz und ggf nationale Behörden unverzüglich informieren.

4. Cybersicherheit und physische Sicherheit

- Anbieter müssen ein hohes Maß an IT-Sicherheit gewährleisten, sowohl für die Modelle selbst als auch für die Infrastruktur, auf der sie laufen.

C. Nachweis der Einhaltung

- **Praxisleitfäden und Normen**: Bis harmonisierte europäische Normen veröffentlicht sind, können Anbieter auf genehmigte Praxisleitfäden zurückgreifen.
- **Vermutung der Konformität**: Wer Normen einhält, gilt automatisch als gesetzeskonform.
- **Alternative Verfahren**: Anbieter, die keine Normen nutzen, müssen eigene Nachweise erbringen, die von der Kommission bewertet werden.

Beispiel: *Ein Anbieter entwickelt eigene Sicherheitsprotokolle statt die Norm einzuhalten. Er muss der Kommission zeigen, dass diese gleichwertig sind.*

D. Vertraulichkeit

- Alle nach diesem Artikel erhobenen Daten und Dokumente unterliegen den strengen Vertraulichkeitspflichten nach Artikel 78 KI-VO.
- Dies soll sicherstellen, dass sensible Informationen (zB technische Details oder Geschäftsgeheimnisse) geschützt bleiben.

III. Zusammenfassung

Modellbewertung	Tests nach Stand der Technik, inkl Angriffstests
Risikobewertung	Ermittlung und Minderung systemischer Risiken
Meldung von Vorfällen	Dokumentation und sofortige Information der Behörden
Cybersicherheit	Schutz der Modelle und Infrastruktur
Nachweis	Leitfäden oder Normen nutzen; sonst eigene Nachweise
Vertraulichkeit	Behandlung aller Infos nach Artikel 78 KI-VO

IV. Quellenverzeichnis

- Erwägungsgrund 97 KI-VO (EU) 2024/1689

Artikel 56 KI-VO

Praxisleitfäden

(1) Das Büro für Künstliche Intelligenz fördert und erleichtert die Ausarbeitung von Praxisleitfäden auf Unionsebene, um unter Berücksichtigung internationaler Ansätze zur ordnungsgemäßen Anwendung dieser Verordnung beizutragen.

(2) Das Büro für Künstliche Intelligenz und das KI-Gremium streben an, sicherzustellen, dass die Praxisleitfäden mindestens die in den Artikeln 53 und 55 vorgesehenen Pflichten abdecken, einschließlich der folgenden Aspekte:

a) Mittel, mit denen sichergestellt wird, dass die in Artikel 53 Absatz 1 Buchstaben a und b genannten Informationen vor dem Hintergrund der Marktentwicklungen und technologischen Entwicklungen auf dem neuesten Stand gehalten werden;

b) die angemessene Detailgenauigkeit bei der Zusammenfassung der für das Training verwendeten Inhalte;

c) die Ermittlung von Artikel und Wesen der systemischen Risiken auf Unionsebene, gegebenenfalls einschließlich ihrer Ursachen;

d) die Maßnahmen, Verfahren und Modalitäten für die Bewertung und das Management der systemischen Risiken auf Unionsebene, einschließlich ihrer Dokumentation, die in einem angemessenen Verhältnis zu den Risiken stehen, ihrer Schwere und Wahrscheinlichkeit Rechnung tragen und die spezifischen Herausforderungen bei der Bewältigung dieser Risiken vor dem Hintergrund der möglichen Arten der Entstehung und des Eintretens solcher Risiken entlang der KI-Wertschöpfungskette berücksichtigen.

(3) Das Büro für Künstliche Intelligenz kann alle Anbieter von KI-Modellen mit allgemeinem Verwendungszweck sowie die einschlägigen zuständigen nationalen Behörden ersuchen, sich an der Ausarbeitung von Praxisleitfäden zu beteiligen. Organisationen der Zivilgesellschaft, die Industrie, die Wissenschaft und andere einschlägige Interessenträger wie nachgelagerte Anbieter und unabhängige Sachverständige können den Prozess unterstützen.

(4) Das Büro für Künstliche Intelligenz und das KI-Gremium streben an, sicherzustellen, dass in den Praxisleitfäden ihre spezifischen Ziele eindeutig

festgelegt sind und Verpflichtungen oder Maßnahmen, gegebenenfalls einschließlich wesentlicher Leistungsindikatoren, enthalten, um die Verwirklichung dieser Ziele gewährleisten, und dass sie den Bedürfnissen und Interessen aller interessierten Kreise, einschließlich betroffener Personen, auf Unionsebene gebührend Rechnung tragen.

(5) Das Büro für Künstliche Intelligenz strebt an, sicherzustellen, dass die an Praxisleitfäden Beteiligten dem Büro für Künstliche Intelligenz regelmäßig über die Umsetzung der Verpflichtungen, die ergriffenen Maßnahmen und deren Ergebnisse, die gegebenenfalls auch anhand der wesentlichen Leistungsindikatoren gemessen werden, Bericht erstatten. Bei den wesentlichen Leistungsindikatoren und den Berichtspflichten wird den Größen- und Kapazitätsunterschieden zwischen den verschiedenen Beteiligten Rechnung getragen.

(6) Das Büro für Künstliche Intelligenz und KI-Gremium überwachen und bewerten regelmäßig die Verwirklichung der Ziele der Praxisleitfäden durch die Beteiligten und deren Beitrag zur ordnungsgemäßen Anwendung dieser Verordnung. Das Büro für Künstliche Intelligenz und das KI-Gremium bewerten, ob die Praxisleitfäden die in den Artikeln 53 und 55 vorgesehenen Pflichten abdecken, und überwachen und bewerten regelmäßig die Verwirklichung von deren Zielen. Sie veröffentlichen ihre Bewertung der Angemessenheit der Praxisleitfäden.

Die Kommission kann im Wege eines Durchführungsrechtsakts einen Praxisleitfaden genehmigen und ihm in der Union allgemeine Gültigkeit verleihen. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(7) Das Büro für Künstliche Intelligenz kann alle Anbieter von KI-Modellen mit allgemeinem Verwendungszweck ersuchen, die Praxisleitfäden zu befolgen. Für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die keine systemischen Risiken bergen, kann diese Befolgung auf die in Artikel 53 vorgesehenen Pflichten beschränkt werden, es sei denn, sie erklären ausdrücklich ihr Interesse, sich dem ganzen Kodex anzuschließen.

(8) Das Büro für Künstliche Intelligenz fördert und erleichtert gegebenenfalls auch die Überprüfung und Anpassung der Praxisleitfäden, insbesondere vor dem Hintergrund neuer Normen. Das Büro für Künstliche Intelligenz unterstützt bei der Bewertung der verfügbaren Normen.

(9) Praxisleitfäden müssen spätestens am 2. Mai 2025 vorliegen. Das Büro für Künstliche Intelligenz unternimmt die erforderlichen Schritte, einschließlich des Ersuchens von Anbietern gemäß Absatz 7.

Kann bis zum 2. August 2025 ein Verhaltenskodex nicht fertiggestellt werden oder erachtet das Büro für Künstliche Intelligenz dies nach seiner Bewertung gemäß Absatz 6 des vorliegenden Artikels für nicht angemessen, kann die Kommission im Wege von Durchführungsrechtsakten gemeinsame Vorschriften für die Umsetzung der in den Artikeln 53 und 55 vorgesehenen Pflichten, einschließlich der in Absatz 2 des vorliegenden Artikels genannten Aspekte, festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

I. Worum geht es?

Artikel 56 regelt die sogenannten Praxisleitfäden. Diese Leitfäden sind praktische Handlungsanleitungen, die Unternehmen und Behörden dabei unterstützen sollen, die Vorgaben der KI-VO einheitlich und wirksam umzusetzen. Zuständig für die Entwicklung, Koordinierung und Überwachung dieser Leitfäden ist das Büro für Künstliche Intelligenz gemeinsam mit dem KI-Gremium. Ziel ist es, einheitliche Standards zu schaffen, die praxisnah, flexibel und an neue technologische Entwicklungen anpassbar sind.

II. Detailkommentar

A. Funktion und Zweck der Praxisleitfäden

- **Unterstützung der Anwendung**: Praxisleitfäden sollen die komplexen Vorgaben der KI-VO in konkrete Handlungsschritte übersetzen.
- **Harmonisierung**: Sie fördern eine einheitliche Umsetzung in allen Mitgliedstaaten und verhindern nationale Sonderwege.
- **Flexibilität**: Leitfäden können schneller angepasst werden als die Verordnung selbst und reagieren so auf neue Technologien.

B. Inhaltliche Schwerpunkte

5. **Informationspflichten**: Leitfäden legen fest, wie Anbieter Informationen aktuell halten müssen, insbesondere angesichts schneller technischer Entwicklungen.
6. **Transparenz bei Trainingsdaten**: Sie geben Hinweise, wie detailliert Angaben zu Trainingsdaten sein sollen, ohne Geschäftsgeheimnisse unnötig preiszugeben.
7. **Systemische Risiken**: Sie helfen dabei, typische Risiken für Demokratie, Gesellschaft oder Wahlprozesse zu identifizieren und zu managen.
8. **Risikomanagement**: Leitfäden enthalten Verfahren, wie Risiken bewertet, dokumentiert und überwacht werden.

C. Beteiligung relevanter Akteure

- **Anbieter von KI-Modellen**: Sie werden aktiv in die Ausarbeitung einbezogen.
- **Nationale Behörden**: Stellen sicher, dass nationale Besonderheiten berücksichtigt werden.
- **Zivilgesellschaft und Wissenschaft**: Bringen Perspektiven ein, die über rein wirtschaftliche Interessen hinausgehen.

D. Zielklarheit und Erfolgskontrolle

- **Klare Ziele**: Leitfäden müssen eindeutige Zielsetzungen enthalten.
- **Messbare Indikatoren**: Mit Leistungsindikatoren kann überprüft werden, ob Ziele erreicht wurden.
- **Berichtspflichten**: Beteiligte müssen regelmäßig berichten, wie sie die Leitfäden umsetzen.

E. Rechtsstellung der Praxisleitfäden

- **Grundsätzlich freiwillig**: Leitfäden sind zunächst keine zwingenden Vorschriften.
- **Verbindlichkeit durch Kommission**: Die Kommission kann sie durch Durchführungsrechtsakte allgemeinverbindlich machen.
- **Aufforderung zur Befolgung**: Das Büro für Künstliche Intelligenz kann Anbieter auffordern, Leitfäden einzuhalten, besonders wenn systemische Risiken betroffen sind.

F. Fristen und Notfallmechanismus

- **Frist zur Erstellung**: Bis 2. Mai 2025 müssen Leitfäden vorliegen.
- **Frist für Verhaltenskodex**: Spätestens bis 2. August 2025 muss ein Kodex fertig sein.
- **Ersatzregelung**: Wenn kein Leitfaden zustande kommt, kann die Kommission verbindliche Vorschriften erlassen.

III. Zusammenfassung

Zweck	Einheitliche, praxisnahe Umsetzung der KI-VO
Inhalt	Infos aktuell halten, Transparenz bei Trainingsdaten, systemische Risiken erkennen und managen
Beteiligte	Anbieter, Behörden, Zivilgesellschaft, Wissenschaft
Rechtscharakter	Zunächst freiwillig, durch Kommission verbindlich machbar
Kontrolle	Ziele, Indikatoren, Berichtspflichten

IV. Quellenverzeichnis

- Erwägungsgrund 120 KI-VO (EU) 2024/1689

Artikel 57 KI-VO

KI-Reallabore

(1) Die Mitgliedstaaten sorgen dafür, dass ihre zuständigen Behörden mindestens ein KI-Reallabor auf nationaler Ebene einrichten, das bis zum 2. August 2026 einsatzbereit sein muss. Dieses Reallabor kann auch gemeinsam mit den zuständigen Behörden anderer Mitgliedstaaten eingerichtet werden. Die Kommission kann technische Unterstützung, Beratung und Instrumente für die Einrichtung und den Betrieb von KI-Reallaboren bereitstellen.

Die Verpflichtung nach Unterabsatz 1 kann auch durch Beteiligung an einem bestehenden Reallabor erfüllt werden, sofern eine solche Beteiligung die nationale Abdeckung der teilnehmenden Mitgliedstaaten in gleichwertigem Maße gewährleistet.

(2) Es können auch zusätzliche KI-Reallabore auf regionaler oder lokaler Ebene oder gemeinsam mit den zuständigen Behörden anderer Mitgliedstaaten eingerichtet werden;

(3) Der Europäische Datenschutzbeauftragte kann auch ein KI-Reallabor für Organe, Einrichtungen und sonstige Stellen der Union einrichten und die Rollen und Aufgaben der zuständigen nationalen Behörden im Einklang mit diesem Kapitel wahrnehmen.

(4) Die Mitgliedstaaten stellen sicher, dass die in den Absätzen 1 und 2 genannten zuständigen Behörden ausreichende Mittel bereitstellen, um diesem Artikel wirksam und zeitnah nachzukommen. Gegebenenfalls arbeiten die zuständigen nationalen Behörden mit anderen einschlägigen Behörden zusammen und können die Einbeziehung anderer Akteure des KI-Ökosystems gestatten. Andere Reallabore, die im Rahmen des Unionsrechts oder des nationalen Rechts eingerichtet wurden, bleiben von diesem Artikel unberührt. Die Mitgliedstaaten sorgen dafür, dass die diese anderen Reallabore beaufsichtigenden Behörden und die zuständigen nationalen Behörden angemessen zusammenarbeiten.

(5) Die nach Absatz 1 eingerichteten KI-Reallabore bieten eine kontrollierte Umgebung, um Innovation zu fördern und die Entwicklung, das Training, das Testen und die Validierung innovativer KI-Systeme für einen begrenzten Zeitraum vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme nach einem bestimmten zwischen den Anbietern oder zukünftigen Anbietern und der zuständigen Behörde vereinbarten Reallabor-Plan zu erleichtern. In

diesen Reallaboren können auch darin beaufsichtigte Tests unter Realbedingungen durchgeführt werden.

(6) Die zuständigen Behörden stellen innerhalb der KI-Reallabore gegebenenfalls Anleitung, Aufsicht und Unterstützung bereit, um Risiken, insbesondere im Hinblick auf Grundrechte, Gesundheit und Sicherheit, Tests und Risikominderungsmaßnahmen sowie deren Wirksamkeit hinsichtlich der Pflichten und Anforderungen dieser Verordnung und gegebenenfalls anderem Unionsrecht und nationalem Recht, deren Einhaltung innerhalb des Reallabors beaufsichtigt wird, zu ermitteln.

(7) Die zuständigen Behörden stellen den Anbietern und zukünftigen Anbietern, die am KI-Reallabor teilnehmen, Leitfäden zu regulatorischen Erwartungen und zur Erfüllung der in dieser Verordnung festgelegten Anforderungen und Pflichten zur Verfügung.

Die zuständige Behörde legt dem Anbieter oder zukünftigen Anbieter des KI-Systems auf dessen Anfrage einen schriftlichen Nachweis für die im Reallabor erfolgreich durchgeführten Tätigkeiten vor. Außerdem legt die zuständige Behörde einen Abschlussbericht vor, in dem sie die im Reallabor durchgeführten Tätigkeiten, deren Ergebnisse und die gewonnenen Erkenntnisse im Einzelnen darlegt. Die Anbieter können diese Unterlagen nutzen, um im Rahmen des Konformitätsbewertungsverfahrens oder einschlägiger Marktüberwachungstätigkeiten nachzuweisen, dass sie dieser Verordnung nachkommen. In diesem Zusammenhang werden die Abschlussberichte und die von der zuständigen nationalen Behörde vorgelegten schriftlichen Nachweise von den Marktüberwachungsbehörden und den notifizierten Stellen im Hinblick auf eine Beschleunigung der Konformitätsbewertungsverfahren in angemessenem Maße positiv gewertet.

(8) Vorbehaltlich der in Artikel 78 enthaltenen Bestimmungen über die Vertraulichkeit und im Einvernehmen mit den Anbietern oder zukünftigen Anbietern, sind die Kommission und das KI-Gremium befugt, die Abschlussberichte einzusehen und tragen diesen gegebenenfalls bei der Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung Rechnung. Wenn der Anbieter oder der zukünftige Anbieter und die zuständige nationale Behörde ihr ausdrückliches Einverständnis erklären, kann der Abschlussbericht über die in diesem Artikel genannte zentrale Informationsplattform veröffentlicht werden.

(9) Die Einrichtung von KI-Reallaboren soll zu den folgenden Zielen beitragen:

a) Verbesserung der Rechtssicherheit, um für die Einhaltung der Regulierungsvorschriften dieser Verordnung oder, gegebenenfalls, anderem geltenden Unionsrecht und nationalem Recht zu sorgen;

b) Förderung des Austauschs bewährter Verfahren durch Zusammenarbeit mit den am KI-Reallabor beteiligten Behörden;

c) Förderung von Innovation und Wettbewerbsfähigkeit sowie Erleichterung der Entwicklung eines KI-Ökosystems;

d) Leisten eines Beitrags zum evidenzbasierten regulatorischen Lernen;

e) Erleichterung und Beschleunigung des Zugangs von KI-Systemen zum Unionsmarkt, insbesondere wenn sie von KMU — einschließlich Start-up-Unternehmen — angeboten werden.

(10) Soweit die innovativen KI-Systeme personenbezogene Daten verarbeiten oder anderweitig der Aufsicht anderer nationaler Behörden oder zuständiger Behörden unterstehen, die den Zugang zu personenbezogenen Daten gewähren oder unterstützen, sorgen die zuständigen nationalen Behörden dafür, dass die nationalen Datenschutzbehörden oder diese anderen nationalen oder zuständigen Behörden in den Betrieb des KI-Reallabors sowie in die Überwachung dieser Aspekte im vollen Umfang ihrer entsprechenden Aufgaben und Befugnisse einbezogen werden.

(11) Die KI-Reallabore lassen die Aufsichts- oder Abhilfebefugnisse der die Reallabore beaufsichtigenden zuständigen Behörden, einschließlich auf regionaler oder lokaler Ebene, unberührt. Alle erheblichen Risiken für die Gesundheit und Sicherheit und die Grundrechte, die bei der Entwicklung und Erprobung solcher KI-Systeme festgestellt werden, führen zur sofortigen und angemessenen Risikominderung. Die zuständigen nationalen Behörden sind befugt, das Testverfahren oder die Beteiligung am Reallabor vorübergehend oder dauerhaft auszusetzen, wenn keine wirksame Risikominderung möglich ist, und unterrichten das Büro für Künstliche Intelligenz über diese Entscheidung. Um Innovationen im Bereich KI in der Union zu fördern, üben die zuständigen nationalen Behörden ihre Aufsichtsbefugnisse im Rahmen des geltenden Rechts aus, indem sie bei der Anwendung der Rechtsvorschriften auf ein bestimmtes KI-Reallabor ihren Ermessensspielraum nutzen.

(12) Die am KI-Reallabor beteiligten Anbieter und zukünftigen Anbieter bleiben nach geltendem Recht der Union und nationalem Haftungsrecht für

Schäden haftbar, die Dritten infolge der Erprobung im Reallabor entstehen. Sofern die zukünftigen Anbieter den spezifischen Plan und die Bedingungen für ihre Beteiligung beachten und der Anleitung durch die zuständigen nationalen Behörden in gutem Glauben folgen, werden jedoch von den Behörden keine Geldbußen für Verstöße gegen diese Verordnung verhängt. In Fällen, in denen andere zuständige Behörden, die für anderes Unionsrecht und nationales Recht zuständig sind, aktiv an der Beaufsichtigung des KI-Systems im Reallabor beteiligt waren und Anleitung für die Einhaltung gegeben haben, werden im Hinblick auf dieses Recht keine Geldbußen verhängt.

(13) Die KI-Reallabore sind so konzipiert und werden so umgesetzt, dass sie gegebenenfalls die grenzüberschreitende Zusammenarbeit zwischen zuständigen nationalen Behörden erleichtern.

(14) Die zuständigen nationalen Behörden koordinieren ihre Tätigkeiten und arbeiten im Rahmen des KI-Gremiums zusammen.

(15) Die zuständigen nationalen Behörden unterrichten das Büro für Künstliche Intelligenz und das KI-Gremium über die Einrichtung eines Reallabors und können sie um Unterstützung und Anleitung bitten. Das Büro für Künstliche Intelligenz veröffentlicht eine Liste der geplanten und bestehenden Reallabore und hält sie auf dem neuesten Stand, um eine stärkere Interaktion in den KI-Reallaboren und die grenzüberschreitende Zusammenarbeit zu fördern.

(16) Die zuständigen nationalen Behörden übermitteln dem Büro für Künstliche Intelligenz und dem KI-Gremium jährliche Berichte, und zwar ab einem Jahr nach der Einrichtung des Reallabors und dann jedes Jahr bis zu dessen Beendigung, sowie einen Abschlussbericht. Diese Berichte informieren über den Fortschritt und die Ergebnisse der Umsetzung dieser Reallabore, einschließlich bewährter Verfahren, Vorfällen, gewonnener Erkenntnisse und Empfehlungen zu deren Aufbau, sowie gegebenenfalls über die Anwendung und mögliche Überarbeitung dieser Verordnung, einschließlich ihrer delegierten Rechtsakte und Durchführungsrechtsakte, sowie über die Anwendung anderen Unionsrechts, deren Einhaltung von den zuständigen Behörden innerhalb des Reallabors beaufsichtigt wird. Die zuständigen nationalen Behörden stellen diese jährlichen Berichte oder Zusammenfassungen davon der Öffentlichkeit online zur Verfügung. Die Kommission trägt den jährlichen Berichten gegebenenfalls bei der Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung Rechnung.

(17) Die Kommission richtet eine eigene Schnittstelle ein, die alle relevanten Informationen zu den KI-Reallaboren enthält, um es den Interessenträgern zu ermöglichen, mit den KI-Reallaboren zu interagieren und Anfragen an die zuständigen Behörden zu richten und unverbindliche Beratung zur Konformität von innovativen Produkten, Dienstleistungen und Geschäftsmodellen mit integrierter KI-Technologie im Einklang mit Artikel 62 Absatz 1 Buchstabe c einzuholen. Die Kommission stimmt sich gegebenenfalls proaktiv mit den zuständigen nationalen Behörden ab.

I. Worum geht es?

Artikel 57 regelt die Einrichtung sogenannter KI-Reallabore. Diese bieten eine kontrollierte Umgebung, in der Unternehmen ihre KI-Systeme vor der Markteinführung entwickeln, testen und validieren können. Ziel ist es, Innovation zu fördern und gleichzeitig Risiken, insbesondere für Grundrechte, Gesundheit und Sicherheit, wirksam zu kontrollieren. Damit wird ein Ausgleich geschaffen zwischen Technologieentwicklung und rechtlicher Sicherheit.

II. Detailkommentar

A. Verpflichtung zur Einrichtung

- **Mindestens ein nationales Reallabor**: Jeder Mitgliedstaat muss bis 2. August 2026 ein KI-Reallabor einrichten.
- **Alternative Teilnahme**: Mitgliedstaaten können sich auch einem bestehenden Reallabor anschließen, solange eine gleichwertige nationale Abdeckung gewährleistet ist.
- **Europäische Dimension**: Neben nationalen Reallaboren **sind auch regionale, lokale oder grenzüberschreitende Projekte erlaubt.**

Beispiel: *Ein kleines Land ohne eigene Infrastruktur kann sich an einem deutsch-französischen Reallabor beteiligen, solange dort auch seine nationalen Bedürfnisse abgedeckt werden.*

B. Aufgaben und Funktionsweise

- **Kontrollierte Umgebung**: Tests finden unter strenger Aufsicht statt, um Risiken rechtzeitig zu erkennen und zu mindern.
- **Umfang der Tests**: Entwicklung, Training, Validierung sowie – mit Zustimmung – Tests unter Realbedingungen.
- **Reallabor-Plan**: Anbieter und Behörden legen im Voraus einen Plan mit Dauer, Umfang und Regeln des Tests fest.

C. Rolle der zuständigen Behörden

- **Aufsicht und Anleitung**: Behörden begleiten die Tests, geben regulatorische Leitfäden und überwachen die Einhaltung der KI-VO sowie anderer Vorschriften.
- **Schutz der Grundrechte**: Besondere Aufmerksamkeit gilt Risiken für Grundrechte, Gesundheit und Sicherheit.
- **Berichte und Nachweise**: Behörden stellen am Ende schriftliche Nachweise und Abschlussberichte aus, die im Konformitätsverfahren anerkannt werden.

D. Zusammenarbeit und Transparenz

- **Einbindung anderer Akteure**: Nationale Datenschutzbehörden, Marktüberwachungsbehörden oder auch Normungsorganisationen können beteiligt werden.
- **Grenzüberschreitende Kooperation**: Die Reallabore sollen auch Zusammenarbeit zwischen Mitgliedstaaten erleichtern.
- **Transparenz**: Jahresberichte werden öffentlich zugänglich gemacht. Mit Zustimmung können Abschlussberichte auch online veröffentlicht werden.

E. Haftung und Sanktionen

- **Haftung bleibt bestehen**: Anbieter haften weiterhin für Schäden gegenüber Dritten.
- **Kein Bußgeld bei gutem Glauben**: Wer den vereinbarten Reallabor-Plan beachtet und Anweisungen der Behörden befolgt, muss keine Strafen wegen Verstößen im Reallabor fürchten.

Beispiel: *Ein Unternehmen testet eine KI, die unerwartet fehlerhafte Ergebnisse liefert. Solange es nachweislich den Anweisungen der Behörden folgt, droht kein Bußgeld.*

F. Besonderheiten im Datenschutz

Innerhalb von Reallaboren dürfen auch personenbezogene Daten verwendet werden, die ursprünglich für andere Zwecke erhoben wurden. Dies gilt nur unter strenger Aufsicht, mit Schutzmaßnahmen und im öffentlichen Interesse.

III. Zusammenfassung

Einrichtung	Jeder Mitgliedstaat muss bis 2026 mindestens ein KI-Reallabor haben, auch gemeinsam mit anderen Mitgliedstaaten möglich.
Zweck	Sichere Testumgebung für KI-Systeme vor Markteinführung.
Behördenrolle	Aufsicht, Anleitung, Berichte und Nachweise.
Zusammenarbeit	Beteiligung anderer Stellen, grenzüberschreitende Kooperation, Transparenz durch Berichte.
Ziele	Innovation fördern, Rechtssicherheit schaffen, Marktzugang beschleunigen, regulatorisches Lernen.
Haftung	Anbieter bleiben haftbar; keine Bußgelder bei gutgläubiger Teilnahme.
Datenschutz	Nutzung vorhandener personenbezogener Daten unter strengen Bedingungen erlaubt.

IV. Quellenverzeichnis

- Erwägungsgründe 138-140 KI-VO (EU) 2024/1689

Artikel 58 KI-VO

Detaillierte Regelungen für KI-Reallabore und deren Funktionsweise

(1) Um eine Zersplitterung in der Union zu vermeiden, erlässt die Kommission Durchführungsrechtsakte, in denen detaillierte Regelungen für die Einrichtung, Entwicklung, Umsetzung, den Betrieb und die Beaufsichtigung der KI-Reallabore enthalten sind. In den Durchführungsrechtsakten sind gemeinsame Grundsätze zu den folgenden Aspekten festgelegt:

a) Voraussetzungen und Auswahlkriterien für eine Beteiligung am KI-Reallabor;

b) Verfahren für Antragstellung, Beteiligung, Überwachung, Ausstieg und Beendigung bezüglich des KI-Reallabors, einschließlich Plan und Abschlussbericht für das Reallabor;

c) für Beteiligte geltende Anforderungen und Bedingungen.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(2) Die in Absatz 1 genannten Durchführungsrechtsakte gewährleisten,

a) dass KI-Reallabore allen Anbietern oder zukünftigen Anbietern eines KI-Systems, die einen Antrag stellen und die Voraussetzungen und Auswahlkriterien erfüllen, offen stehen; diese Voraussetzungen und Kriterien sind transparent und fair und die zuständigen nationalen Behörden informieren die Antragsteller innerhalb von drei Monaten nach Antragstellung über ihre Entscheidung;

b) dass die KI-Reallabore einen breiten und gleichberechtigten Zugang ermöglichen und mit der Nachfrage nach Beteiligung Schritt halten; die Anbieter und zukünftigen Anbieter auch Anträge zusammen mit Betreibern oder einschlägigen Dritten, die ihre Partner sind, stellen können;

c) dass die detaillierten Regelungen und Bedingungen für KI-Reallabore so gut wie möglich die Flexibilität der zuständigen nationalen Behörden bei der Einrichtung und dem Betrieb ihrer KI-Reallabore unterstützen;

d) dass der Zugang zu KI-Reallaboren für KMU, einschließlich Start-up-Unternehmen, kostenlos ist, unbeschadet außergewöhnlicher Kosten, die

die zuständigen nationalen Behörden in einer fairen und verhältnismäßigen Weise einfordern können;

e)dass den Anbietern und zukünftigen Anbietern die Einhaltung der Verpflichtungen zur Konformitätsbewertung nach dieser Verordnung oder die freiwillige Anwendung der in Artikel 95 genannten Verhaltenskodizes mittels der gewonnenen Erkenntnisse der KI-Reallabore erleichtert wird;

f)dass KI-Reallabore die Einbeziehung anderer einschlägiger Akteure innerhalb des KI-Ökosystems, wie etwa notifizierte Stellen und Normungsorganisationen, KMU, einschließlich Start-up-Unternehmen, Unternehmen, Innovatoren, Test- und Versuchseinrichtungen, Forschungs- und Versuchslabore, europäische digitale Innovationszentren, Kompetenzzentren und einzelne Forscher begünstigen, um die Zusammenarbeit mit dem öffentlichen und dem privaten Sektor zu ermöglichen und zu erleichtern;

g)dass die Verfahren, Prozesse und administrativen Anforderungen für die Antragstellung, die Auswahl, die Beteiligung und den Ausstieg aus dem KI-Reallabor einfach, leicht verständlich und klar kommuniziert sind, um die Beteiligung von KMU, einschließlich Start-up-Unternehmen, mit begrenzten rechtlichen und administrativen Kapazitäten zu erleichtern, sowie unionsweit gestrafft sind, um eine Zersplitterung zu vermeiden, und dass die Beteiligung an einem von einem Mitgliedstaat oder dem Europäischen Datenschutzbeauftragten eingerichteten KI-Reallabor gegenseitig und einheitlich anerkannt wird und in der gesamten Union die gleiche Rechtswirkung hat;

h)dass die Beteiligung an dem KI-Reallabor auf einen der Komplexität und dem Umfang des Projekts entsprechenden Zeitraum beschränkt ist, der von der zuständigen nationalen Behörde verlängert werden kann;

i)dass die KI-Reallabore die Entwicklung von Instrumenten und Infrastruktur für das Testen, das Benchmarking, die Bewertung und die Erklärung der Dimensionen von KI-Systemen erleichtern, die für das regulatorische Lernen Bedeutung sind, wie etwa Genauigkeit, Robustheit und Cybersicherheit, sowie Maßnahmen zur Risikominderung im Hinblick auf die Grundrechte und die Gesellschaft als Ganzes fördern.

(3) Zukünftige Anbieter in den KI-Reallaboren, insbesondere KMU und Start-up-Unternehmen, werden gegebenenfalls vor der Einrichtung an Dienste verwiesen, die beispielsweise eine Anleitung zur Umsetzung dieser

Verordnung oder andere Mehrwertdienste wie Hilfe bei Normungsdokumenten bereitstellen, sowie an Zertifizierungs-, Test- und Versuchseinrichtungen, europäische digitale Innovationszentren und Exzellenzzentren.

(4) Wenn zuständige nationale Behörden in Betracht ziehen, Tests unter Realbedingungen zu genehmigen, die im Rahmen eines KI-Reallabors beaufsichtigt werden, welches nach diesem Artikel einzurichten ist, vereinbaren sie mit den Beteiligten ausdrücklich die Anforderungen und Bedingungen für diese Tests und insbesondere geeignete Schutzvorkehrungen für Grundrechte, Gesundheit und Sicherheit. Gegebenenfalls arbeiten sie mit anderen zuständigen nationalen Behörden zusammen, um für unionsweit einheitliche Verfahren zu sorgen.

I. Worum geht es?

Artikel 58 regelt detaillierte Regelungen für die KI-Reallabore. Das sind geschützte Umgebungen, in denen KI-Systeme unter realen Bedingungen getestet werden können, bevor sie breit eingesetzt werden. Ziel ist es, Innovation zu fördern, gleichzeitig aber rechtliche Sicherheit zu schaffen. Damit soll verhindert werden, dass jeder Mitgliedstaat eigene Sonderregeln entwickelt, was zu einer Zersplitterung führen würde. Die Kommission legt durch Durchführungsrechtsakte einheitliche Rahmenbedingungen fest, die von allen Mitgliedstaaten zu beachten sind.

II. Detailkommentar

A. Ziel und Funktion der Durchführungsrechtsakte

- **Vermeidung von Zersplitterung**: Einheitliche Regeln verhindern, dass jeder Mitgliedstaat eigene Verfahren und Bedingungen für Reallabore aufstellt.
- **Rahmen für nationale Behörden**: Die Kommission gibt Vorgaben, innerhalb derer die nationalen Behörden ihre Reallabore einrichten und betreiben können.
- **Flexibilität**: Trotz gemeinsamer Standards bleibt Spielraum für Anpassungen an nationale Besonderheiten.

B. Offener Zugang und faire Verfahren

- **Offen für alle Anbieter**: Jedes Unternehmen, das die Kriterien erfüllt, kann teilnehmen. Dies verhindert Diskriminierung und Wettbewerbsverzerrung.
- **Transparente Kriterien**: Voraussetzungen müssen klar und nachvollziehbar sein.
- **Schnelle Entscheidungen**: Nationale Behörden müssen innerhalb von drei Monaten über Anträge entscheiden.

C. Unterstützung für KMU und Start-ups

- **Kostenfreiheit**: Für kleine und mittlere Unternehmen (KMU) ist die Teilnahme grundsätzlich kostenlos.
- **Einfache Verfahren**: Bewerbungs- und Ausstiegsprozesse müssen klar und verständlich sein.
- **Anerkennung in der gesamten EU**: Wer in einem Mitgliedstaat zugelassen ist, wird automatisch auch in anderen Staaten anerkannt.

D. Kooperation und Einbindung weiterer Akteure

- **Breite Beteiligung**: Reallabore sollen nicht nur Anbieter einbinden, sondern auch zB Forschungszentren, Normungsorganisationen oder Testeinrichtungen.
- **Stärkung des Ökosystems**: Zusammenarbeit zwischen Wirtschaft, Wissenschaft und Verwaltung wird gezielt gefördert.

E. Verbindung mit regulatorischen Anforderungen

- **Konformitätsbewertung erleichtern**: Ergebnisse aus Reallaboren sollen helfen, die verpflichtenden Prüfungen nach der KI-VO besser zu bestehen.
- **Anwendung freiwilliger Standards erleichtern**: Durch in den Reallaboren gewonnene Erkenntnisse können auch Verhaltenskodizes leichter angewendet werden.

F. Schutz bei Tests unter Realbedingungen

- **Klare Vereinbarungen**: Bedingungen für Tests in der Praxis müssen vorher ausdrücklich festgelegt werden.
- **Schutzvorkehrungen**: Grundrechte, Gesundheit und Sicherheit müssen stets gewahrt bleiben.
- **Zusammenarbeit**: Nationale Behörden stimmen sich ab, um europaweit einheitliche Verfahren zu gewährleisten.

III. Zusammenfassung

Einheitlichkeit	Kommission erlässt gemeinsame Vorgaben für alle Mitgliedstaaten
Offener Zugang	Reallabore stehen allen Anbietern offen, mit klaren und fairen Kriterien
KMU-Förderung	Kostenfreiheit, einfache Verfahren, EU-weite Anerkennung
Zusammenarbeit	Breite Einbindung von Unternehmen, Forschung, Normung, Verwaltung
Rechtliche Unterstützung	Erleichterung von Konformitätsbewertung und freiwilligen Standards
Schutzmechanismen	Klare Regeln für Tests unter Realbedingungen, Sicherung von Grundrechten
Gesellschaftlicher Nutzen	Fokus auf sozial und ökologisch vorteilhafte KI-Projekte

IV. Quellenverzeichnis

- Erwägungsgrund 142 KI-VO (EU) 2024/1689

Artikel 59 KI-VO

Weiterverarbeitung personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor

(1) Rechtmäßig für andere Zwecke erhobene personenbezogene Daten dürfen im KI-Reallabor ausschließlich für die Zwecke der Entwicklung, des Trainings und des Testens bestimmter KI-Systeme im Reallabor verarbeitet werden, wenn alle der folgenden Bedingungen erfüllt sind:

a) Die KI-Systeme werden zur Wahrung eines erheblichen öffentlichen Interesses durch eine Behörde oder eine andere natürliche oder juristische Person und in einem oder mehreren der folgenden Bereiche entwickelt:

i) öffentliche Sicherheit und öffentliche Gesundheit, einschließlich Erkennung, Diagnose, Verhütung, Bekämpfung und Behandlung von Krankheiten sowie Verbesserung von Gesundheitsversorgungssystemen;

ii) hohes Umweltschutzniveau und Verbesserung der Umweltqualität, Schutz der biologischen Vielfalt, Schutz gegen Umweltverschmutzung, Maßnahmen für den grünen Wandel sowie Klimaschutz und Anpassung an den Klimawandel;

iii) nachhaltige Energie;

iv) Sicherheit und Widerstandsfähigkeit von Verkehrssystemen und Mobilität, kritischen Infrastrukturen und Netzen;

v) Effizienz und Qualität der öffentlichen Verwaltung und öffentlicher Dienste;

b) die verarbeiteten Daten sind für die Erfüllung einer oder mehrerer der in Kapitel III Abschnitt 2 genannten Anforderungen erforderlich, sofern diese Anforderungen durch die Verarbeitung anonymisierter, synthetischer oder sonstiger nicht personenbezogener Daten nicht wirksam erfüllt werden können;

c) es bestehen wirksame Überwachungsmechanismen, mit deren Hilfe festgestellt wird, ob während der Reallaborversuche hohe Risiken für die Rechte und Freiheiten betroffener Personen gemäß Artikel 35 der Verordnung (EU) 2016/679 und gemäß Artikel 39 der Verordnung (EU) 2018/1725 auftreten können, sowie Reaktionsmechanismen, mit deren Hilfe diese Risiken umgehend eingedämmt werden können und die Verarbeitung bei Bedarf beendet werden kann;

d)personenbezogene Daten, die im Rahmen des Reallabors verarbeitet werden sollen, befinden sich in einer funktional getrennten, isolierten und geschützten Datenverarbeitungsumgebung unter der Kontrolle des zukünftigen Anbieters, und nur befugte Personen haben Zugriff auf diese Daten;

e)Anbieter dürfen die ursprünglich erhobenen Daten nur im Einklang mit dem Datenschutzrecht der Union weitergeben; personenbezogene Daten, die im Reallabor erstellt wurden, dürfen nicht außerhalb des Reallabors weitergegeben werden;

f)eine Verarbeitung personenbezogener Daten im Rahmen des Reallabors führt zu keinen Maßnahmen oder Entscheidungen, die Auswirkungen auf die betroffenen Personen haben, und berührt nicht die Anwendung ihrer Rechte, die in den Rechtsvorschriften der Union über den Schutz personenbezogener Daten festgelegt sind;

g)im Rahmen des Reallabors verarbeitete personenbezogene Daten sind durch geeignete technische und organisatorische Maßnahmen geschützt und werden gelöscht, sobald die Beteiligung an dem Reallabor endet oder das Ende der Speicherfrist für die personenbezogenen Daten erreicht ist;

h)die Protokolle der Verarbeitung personenbezogener Daten im Rahmen des Reallabors werden für die Dauer der Beteiligung am Reallabor aufbewahrt, es sei denn, im Unionsrecht oder nationalen Recht ist etwas anderes bestimmt;

i)eine vollständige und detaillierte Beschreibung des Prozesses und der Gründe für das Trainieren, Testen und Validieren des KI-Systems wird zusammen mit den Testergebnissen als Teil der technischen Dokumentation gemäß Anhang IV aufbewahrt;

j)eine kurze Zusammenfassung des im Reallabor entwickelten KI-Projekts, seiner Ziele und der erwarteten Ergebnisse wird auf der Website der zuständigen Behörden veröffentlicht; diese Pflicht erstreckt sich nicht auf sensible operative Daten zu den Tätigkeiten von Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden.

(2) Für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung — einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit — unter der Kontrolle und Verantwortung der Strafverfolgungsbehörden erfolgt die Verarbeitung personenbezogener Daten in KI-Reallaboren auf der

Grundlage eines spezifischen Unionsrechts oder nationalen Rechts und unterliegt den kumulativen Bedingungen des Absatzes 1.

(3) Das Unionsrecht oder nationale Recht, das die Verarbeitung personenbezogener Daten für andere Zwecke als die ausdrücklich in jenem Recht genannten ausschließt, sowie Unionsrecht oder nationales Recht, in dem die Grundlagen für eine für die Zwecke der Entwicklung, des Testens oder des Trainings innovativer KI-Systeme notwendige Verarbeitung personenbezogener Daten festgelegt sind, oder jegliche anderen dem Unionsrecht zum Schutz personenbezogener Daten entsprechenden Rechtsgrundlagen bleiben von Absatz 1 unberührt.

I. Worum geht es?

Artikel 59 erlaubt es, personenbezogene Daten, die ursprünglich zu einem anderen Zweck erhoben wurden, in einem KI-Reallabor weiterzuverarbeiten. Dies ist nur in engen Grenzen zulässig, wenn es um die Entwicklung, das Training und das Testen bestimmter KI-Systeme geht, die einem erheblichen öffentlichen Interesse dienen. Damit soll ein Ausgleich geschaffen werden zwischen dem Schutz persönlicher Daten und der Möglichkeit, KI für wichtige gesellschaftliche Ziele nutzbar zu machen.

II. Detailkommentar

A. Grundgedanke

- **Ermöglichung von Innovation:** KI-Reallabore sollen Raum schaffen, um neue Systeme mit echten Daten zu testen, ohne dass sofort eine umfassende Marktzulassung notwendig ist.
- **Datenschutz bleibt zentral:** Trotz dieser Öffnung bleibt der Schutz personenbezogener Daten gewahrt. Artikel 59 enthält daher einen Katalog strenger Bedingungen.
- **Öffentliches Interesse als Schranke:** Nur Projekte, die einen klaren Nutzen für die Gesellschaft haben, dürfen personenbezogene Daten im Reallabor nutzen.

B. Voraussetzungen für die Datenverarbeitung

1. **Öffentliches Interesse**: Nur bestimmte Bereiche sind zugelassen: öffentliche Sicherheit, Gesundheit, Umwelt, Energie, kritische Infrastrukturen und effiziente Verwaltung.

   Beispiel: *Ein Reallabor darf Patientendaten nutzen, um eine KI zu entwickeln, die seltene Krankheiten schneller diagnostiziert.*

2. **Keine Alternativen**: Personenbezogene Daten dürfen nur dann verwendet werden, wenn anonymisierte oder synthetische Daten nicht ausreichen.

   Beispiel: *Bei einem KI-System zur Betrugserkennung kann es nötig sein, echte Zahlungsdaten zu verwenden, da synthetische Daten die Muster nicht realistisch abbilden.*

3. **Risikokontrolle**: Es müssen Mechanismen existieren, die mögliche Risiken für Betroffene erkennen und eindämmen.

   Beispiel: *Stellt sich während eines Tests heraus, dass sensible Gesundheitsdaten ungeschützt abrufbar sind, muss der Versuch sofort gestoppt werden.*

4. **Technische Sicherung**: Daten dürfen nur in isolierten, geschützten Umgebungen verarbeitet werden; nur befugte Personen haben Zugriff.

5. **Weitergabe beschränkt**: Ursprüngliche Daten dürfen nur datenschutzkonform weitergegeben werden. Im Reallabor generierte personenbezogene Daten dürfen das Labor nicht verlassen.

6. **Keine Folgen für Betroffene**: Die Verarbeitung darf nicht zu realen Entscheidungen über einzelne Personen führen.

   Beispiel: *Eine KI zur Risikoeinschätzung von Straftaten darf im Reallabor keine Auswirkungen auf laufende Verfahren haben.*

7. **Löschungspflicht**: Daten müssen gelöscht werden, sobald die Teilnahme am Reallabor endet oder die Speicherfrist abläuft.

8. **Dokumentation**: Sowohl Verarbeitungsvorgänge als auch die Gründe und Testergebnisse müssen dokumentiert und aufbewahrt werden.

9. **Transparenzpflicht**: Eine Kurzbeschreibung des Projekts wird veröffentlicht, mit Ausnahme sensibler Bereiche wie Strafverfolgung oder Grenzschutz.

C. Besonderheiten bei Strafverfolgung

- Wenn Strafverfolgungsbehörden Daten in Reallaboren nutzen, braucht es grundsätzlich eine **spezifische Rechtsgrundlage** im Unions- oder nationalen Recht.
- Die Bedingungen aus Absatz 1 gelten trotzdem.

D. Verhältnis zu anderem Datenschutzrecht

- Artikel 59 ergänzt die bestehenden Vorschriften der DSGVO und anderer Datenschutzgesetze.
- Er schafft **keine allgemeine Ausnahme**, sondern nur eine **spezielle Erlaubnis** für Reallabore.
- Rechte der Betroffenen, zB Auskunft oder Löschung, bleiben unberührt.

III. Zusammenfassung

Zweck	Nutzung personenbezogener Daten in Reallaboren für KI-Systeme im öffentlichen Interesse
Voraussetzungen	Strenger Katalog: öffentliches Interesse, keine Alternativen, Risikokontrolle, Schutzmaßnahmen, Löschung, Dokumentation, Transparenz
Einschränkungen	Keine Folgen für Betroffene, keine Weitergabe außerhalb des Reallabors
Strafverfolgung	Nur mit spezieller Rechtsgrundlage und unter denselben Bedingungen
Verhältnis zum Datenschutzrecht	Ergänzung, kein Ersatz; Rechte der Betroffenen bleiben bestehen

IV. Quellenverzeichnis

- Erwägungsgrund 140 KI-VO (EU) 2024/1689

Artikel 60 KI-VO

Tests von Hochrisiko-KI-Systemen unter Realbedingungen außerhalb von KI-Reallaboren

(1) Tests von Hochrisiko-KI-Systemen unter Realbedingungen können von Anbietern oder zukünftigen Anbietern von in Anhang III aufgeführten Hochrisiko-KI-Systemen außerhalb von KI-Reallaboren gemäß diesem Artikel und — unbeschadet der Bestimmungen unter Artikel 5 — dem in diesem Artikel genannten Plan für einen Test unter Realbedingungen durchgeführt werden.

Die Kommission legt die einzelnen Elemente des Plans für einen Test unter Realbedingungen im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

Das Unionsrecht oder nationale Recht für das Testen von Hochrisiko-KI-Systemen unter Realbedingungen im Zusammenhang mit Produkten, die unter die in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, bleibt von dieser Bestimmung unberührt.

(2) Anbieter oder zukünftige Anbieter können in Anhang III genannte Hochrisiko-KI-Systeme vor deren Inverkehrbringen oder Inbetriebnahme jederzeit selbst oder in Partnerschaft mit einem oder mehreren Betreibern oder zukünftigen Betreibern unter Realbedingungen testen.

(3) Tests von KI-Systemen unter Realbedingungen gemäß diesem Artikel lassen nach dem Unionsrecht oder dem nationalen Recht gegebenenfalls vorgeschriebene Ethikprüfungen unberührt.

(4) Tests unter Realbedingungen dürfen von Anbietern oder zukünftigen Anbietern nur durchgeführt werden, wenn alle der folgenden Bedingungen erfüllt sind:

a) Der Anbieter oder der zukünftige Anbieter hat einen Plan für einen Test unter Realbedingungen erstellt und diesen bei der Marktüberwachungsbehörde in dem Mitgliedstaat eingereicht, in dem der Test unter Realbedingungen stattfinden soll;

b) die Marktüberwachungsbehörde in dem Mitgliedstaat, in dem der Test unter Realbedingungen stattfinden soll, hat den Test unter Realbedingungen und den Plan für einen Test unter Realbedingungen genehmigt; hat die Marktüberwachungsbehörde innerhalb von 30 Tagen

keine Antwort gegeben, so gelten der Test unter Realbedingungen und der Plan für einen Test unter Realbedingungen als genehmigt; ist im nationalen Recht keine stillschweigende Genehmigung vorgesehen, so bleibt der Test unter Realbedingungen genehmigungspflichtig;

c) der Anbieter oder zukünftige Anbieter, mit Ausnahme der in Anhang III Nummern 1, 6 und 7 genannten Anbieter oder zukünftigen Anbieter von Hochrisiko-KI-Systemen in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrolle und der in Anhang III Nummer 2 genannten Hochrisiko-KI-Systeme, hat den Test unter Realbedingungen unter Angabe einer unionsweit einmaligen Identifizierungsnummer und der in Anhang IX festgelegten Informationen gemäß Artikel 71 Absatz 4 registriert; der Anbieter oder zukünftige Anbieter von Hochrisiko-KI-Systemen gemäß Anhang III Nummern 1, 6 und 7 in den Bereichen Strafverfolgung, Migration, Asyl und Grenzkontrollmanagement hat die Tests unter Realbedingungen im sicheren nicht öffentlichen Teil der EU-Datenbank gemäß Artikel 49 Absatz 4 Buchstabe d mit einer unionsweit einmaligen Identifizierungsnummer und den darin festgelegten Informationen registriert; der Anbieter oder zukünftige Anbieter von Hochrisiko-KI-Systemen gemäß Anhang III Nummer 2 hat die Tests unter Realbedingungen gemäß Artikel 49 Absatz 5 registriert;

d) der Anbieter oder der zukünftige Anbieter, der den Test unter Realbedingungen durchführt, ist in der Union niedergelassen oder hat einen in der Union niedergelassenen gesetzlichen Vertreter bestellt;

e) die für die Zwecke des Tests unter Realbedingungen erhobenen und verarbeiteten Daten werden nur dann an Drittländer übermittelt, wenn gemäß Unionsrecht geeignete und anwendbare Schutzvorkehrungen greifen;

f) der Test unter Realbedingungen dauert nicht länger als zur Erfüllung seiner Zielsetzungen nötig und in keinem Fall länger als sechs Monate; dieser Zeitraum kann um weitere sechs Monate verlängert werden, sofern der Anbieter oder der zukünftige Anbieter die Marktüberwachungsbehörde davon vorab in Kenntnis setzt und erläutert, warum eine solche Verlängerung erforderlich ist;

g) Testteilnehmer im Rahmen von Tests unter Realbedingungen, die aufgrund ihres Alters oder einer Behinderung schutzbedürftigen Gruppen angehören, sind angemessen geschützt;

h)wenn ein Anbieter oder zukünftiger Anbieter den Test unter Realbedingungen in Zusammenarbeit mit einem oder mehreren Betreibern oder zukünftigen Betreibern organisiert, werden Letztere vorab über alle für ihre Teilnahmeentscheidung relevanten Aspekte des Tests informiert und erhalten die einschlägigen in Artikel 13 genannten Betriebsanleitungen für das KI-System; der Anbieter oder zukünftige Anbieter und der Betreiber oder zukünftige Betreiber schließen eine Vereinbarung, in der ihre Aufgaben und Zuständigkeiten festgelegt sind, um für die Einhaltung der nach dieser Verordnung und anderem Unionsrecht und nationalem Recht für Tests unter Realbedingungen geltenden Bestimmungen zu sorgen;

i)die Testteilnehmer im Rahmen von Tests unter Realbedingungen erteilen ihre informierte Einwilligung gemäß Artikel 61, oder, wenn im Fall der Strafverfolgung die Einholung einer informierten Einwilligung den Test des KI-Systems verhindern würde, dürfen sich der Test und die Ergebnisse des Tests unter Realbedingungen nicht negativ auf die Testteilnehmer auswirken und ihre personenbezogenen Daten werden nach Durchführung des Tests gelöscht;

j)der Anbieter oder zukünftige Anbieter und die Betreiber und zukünftigen Betreiber lassen den Test unter Realbedingungen von Personen wirksam überwachen, die auf dem betreffenden Gebiet angemessen qualifiziert sind und über die Fähigkeit, Ausbildung und Befugnis verfügen, die für die Wahrnehmung ihrer Aufgaben erforderlich sind;

k)die Vorhersagen, Empfehlungen oder Entscheidungen des KI-Systems können effektiv rückgängig gemacht und außer Acht gelassen werden.

(5) Jeder Testteilnehmer bezüglich des Tests unter Realbedingungen oder gegebenenfalls dessen gesetzlicher Vertreter kann seine Teilnahme an dem Test jederzeit durch Widerruf seiner informierten Einwilligung beenden und die unverzügliche und dauerhafte Löschung seiner personenbezogenen Daten verlangen, ohne dass ihm daraus Nachteile entstehen und er dies in irgendeiner Weise begründen müsste. Der Widerruf der informierten Einwilligung wirkt sich nicht auf bereits durchgeführte Tätigkeiten aus.

(6) Im Einklang mit Artikel 75 übertragen die Mitgliedstaaten ihren Marktüberwachungsbehörden die Befugnis, Anbieter und zukünftige Anbieter zur Bereitstellung von Informationen zu verpflichten, unangekündigte Ferninspektionen oder Vor-Ort-Inspektionen durchzuführen und die Durchführung der Tests unter Realbedingungen und

damit zusammenhängende Hochrisiko-KI-Systeme zu prüfen. Die Marktüberwachungsbehörden nutzen diese Befugnisse, um für die sichere Entwicklung von Tests unter Realbedingungen zu sorgen.

(7) Jegliche schwerwiegenden Vorfälle im Verlauf des Tests unter Realbedingungen sind den nationalen Marktüberwachungsbehörden gemäß Artikel 73 zu melden. Der Anbieter oder zukünftige Anbieter trifft Sofortmaßnahmen zur Schadensbegrenzung; andernfalls setzt er den Test unter Realbedingungen so lange aus, bis eine Schadensbegrenzung stattgefunden hat, oder bricht ihn ab. Im Fall eines solchen Abbruchs des Tests unter Realbedingungen richtet der Anbieter oder zukünftige Anbieter ein Verfahren für den sofortigen Rückruf des KI-Systems ein.

(8) Anbieter oder zukünftige Anbieter setzen die nationalen Marktüberwachungsbehörde in dem Mitgliedstaat, in dem der Test unter Realbedingungen stattfindet, über die Aussetzung oder den Abbruch des Tests unter Realbedingungen und die Endergebnisse in Kenntnis.

(9) Anbieter oder zukünftige Anbieter sind nach geltendem Recht der Union und geltendem nationalen Recht für Schäden haftbar, die während ihrer Tests unter Realbedingungen entstehen.

I. Worum geht es?

Artikel 60 regelt, wie Hochrisiko-KI-Systeme außerhalb von speziellen KI-Reallaboren unter realen Bedingungen getestet werden dürfen. Ziel ist es, Innovation und Entwicklung zu ermöglichen, gleichzeitig aber klare Schutzmaßnahmen für Betroffene, Testteilnehmer und die Allgemeinheit vorzusehen. Es wird ein Verfahren eingeführt, das Planung, Genehmigung, Überwachung und Schutzrechte der Teilnehmer umfasst.

II. Detailkommentar

A. Grundprinzip

- **Testmöglichkeit außerhalb von Reallaboren**: Anbieter können ihre Hochrisiko-KI-Systeme auch direkt in realen Umgebungen erproben, ohne an ein KI-Reallabor gebunden zu sein.

- **Ziel**: Beschleunigung der Entwicklung, aber nur unter strengen Auflagen zum Schutz von Personen, Daten und Rechten.

Beispiel: *Ein Hersteller von KI-gestützter Bewerbungssoftware darf diese in einem echten Unternehmen testen, muss aber vorher einen Plan einreichen und die Einwilligung der Bewerber einholen.*

B. Voraussetzungen für Tests

1. **Testplan**: Der Anbieter muss einen detaillierten Plan bei der zuständigen Marktüberwachungsbehörde einreichen. Darin werden Ablauf, Ziele und Schutzmaßnahmen festgelegt.
2. **Genehmigungspflicht**: Die Behörde muss zustimmen. Erfolgt binnen 30 Tagen keine Reaktion, gilt die Genehmigung stillschweigend als erteilt – außer das nationale Recht verbietet dies.
3. **Registrierungspflicht**: Die Tests müssen in der EU-Datenbank registriert werden, mit Ausnahme bestimmter sensibler Bereiche wie Strafverfolgung oder Migration, die in einem geschützten Bereich registriert werden.
4. **Niederlassung in der EU**: Nur Anbieter mit Sitz oder Vertretung in der EU dürfen solche Tests durchführen.
5. **Datenübermittlung**: Daten dürfen nur in Drittländer übermittelt werden, wenn unionsrechtliche Schutzmaßnahmen greifen.
6. **Zeitliche Begrenzung**: Tests sind auf sechs Monate beschränkt, eine Verlängerung ist nur mit Begründung möglich.
7. **Schutz vulnerabler Gruppen**: Minderjährige oder Menschen mit Behinderung benötigen besonderen Schutz.
8. **Kooperation mit Betreibern**: Falls Betreiber eingebunden sind, muss eine schriftliche Vereinbarung über Verantwortlichkeiten bestehen.
9. **Einwilligung der Teilnehmer**: Grundsätzlich ist eine informierte Einwilligung erforderlich. Ausnahme: Strafverfolgung, wenn diese die Testdurchführung sonst unmöglich machen würde.
10. **Überwachung durch Fachpersonal**: Der Test muss durch qualifiziertes Personal überwacht werden.

11. **Widerrufbarkeit von Entscheidungen**: Ergebnisse des KI-Systems müssen jederzeit rückgängig gemacht werden können.

C. Rechte der Teilnehmer

- **Widerruf der Teilnahme**: Teilnehmer können jederzeit ihre Einwilligung zurückziehen und die Löschung ihrer Daten verlangen.
- **Keine Nachteile**: Der Widerruf darf keine negativen Folgen für die betroffene Person haben.

D. Aufsicht und Kontrolle

- **Befugnisse der Behörden**: Marktüberwachungsbehörden dürfen Informationen einfordern, unangekündigte Inspektionen vornehmen und Tests kontrollieren.
- **Ziel**: Sicherstellung, dass die Tests sicher und im Einklang mit der Verordnung ablaufen.

E. Umgang mit Zwischenfällen

- **Meldepflicht**: Schwere Vorfälle müssen unverzüglich gemeldet werden.
- **Sofortmaßnahmen**: Der Anbieter muss den Schaden begrenzen oder den Test aussetzen/abbrechen.
- **Rückrufpflicht**: Bei Abbruch muss ein sofortiger Rückruf des Systems erfolgen.
- **Informationspflicht**: Nach Abschluss, Abbruch oder Aussetzung sind die Behörden zu informieren.
- **Volle Haftung**: Anbieter haften nach geltendem EU- und nationalem Recht für Schäden, die während der Tests entstehen.

III. Zusammenfassung

Ziel	Ermöglichung von Realtests ohne Reallabor, mit Schutzvorkehrungen
Genehmigung	Plan erforderlich, Zustimmung durch Marktüberwachungsbehörde (30 Tage Frist)
Registrierung	Eintragung in EU-Datenbank (Ausnahmen für sensible Bereiche)
Dauer	Max sechs Monate, Verlängerung um sechs Monate möglich
Teilnehmerrechte	Informierte Einwilligung, Widerruf, Löschung der Daten, Schutz vulnerabler Gruppen
Aufsicht	Marktüberwachungsbehörden mit weitreichenden Befugnissen
Zwischenfälle	Meldepflicht, Sofortmaßnahmen, Abbruchpflicht
Haftung	Anbieter haften für Schäden nach EU- und nationalem Recht

IV. Quellenverzeichnis

- Erwägungsgrund 141 KI-VO (EU) 2024/1689

Artikel 61 KI-VO

Informierte Einwilligung zur Teilnahme an einem Test unter Realbedingungen außerhalb von KI-Reallaboren

(1) Für die Zwecke von Tests unter Realbedingungen gemäß Artikel 60 ist von den Testteilnehmern eine freiwillig erteilte informierte Einwilligung einzuholen, bevor sie an dem Test teilnehmen und nachdem sie mit präzisen, klaren, relevanten und verständlichen Informationen über Folgendes ordnungsgemäß informiert wurden:

a) die Artikel und die Zielsetzungen des Tests unter Realbedingungen und etwaige mit ihrer Teilnahme verbundene Unannehmlichkeiten;

b) die Bedingungen, unter denen der Test unter Realbedingungen erfolgen soll, einschließlich der voraussichtlichen Dauer der Teilnahme des Testteilnehmers oder der Testteilnehmer;

c) ihre Rechte und Garantien, die ihnen bezüglich ihrer Teilnahme zustehen, insbesondere ihr Recht, die Teilnahme an dem Test unter Realbedingungen zu verweigern oder diese Teilnahme jederzeit zu beenden, ohne dass ihnen daraus Nachteile entstehen und sie dies in irgendeiner Weise begründen müssten;

d) die Regelungen, unter denen die Rückgängigmachung oder Außerachtlassung der Vorhersagen, Empfehlungen oder Entscheidungen des KI-Systems beantragt werden kann;

e) die unionsweit einmalige Identifizierungsnummer des Tests unter Realbedingungen gemäß Artikel 60 Absatz 4 Buchstabe c und die Kontaktdaten des Anbieters oder seines gesetzlichen Vertreters, bei dem weitere Informationen eingeholt werden können.

(2) Die informierte Einwilligung ist zu datieren und zu dokumentieren, und eine Kopie wird den Testteilnehmern oder ihren gesetzlichen Vertretern ausgehändigt.

I. Worum geht es?

Artikel 61 regelt die informierte Einwilligung von Personen, die an einem Test unter Realbedingungen teilnehmen sollen. Solche Tests finden außerhalb von KI-Reallaboren statt und dienen dazu, Hochrisiko-KI-Systeme in der Praxis zu erproben. Ziel ist es, die Selbstbestimmung und

Rechte der Testteilnehmer zu sichern: Niemand soll ohne klare Information und freiwillige Zustimmung in einen solchen Test einbezogen werden.

II. Detailkommentar

A. Zweck der Einwilligung

- **Freiwilligkeit**: Die Teilnahme darf nicht erzwungen oder durch Druck herbeigeführt werden. Entscheidend ist eine selbstbestimmte Zustimmung.
- **Informiertheit**: Die Einwilligung ist nur wirksam, wenn die Person zuvor verständlich über alle relevanten Aspekte aufgeklärt wurde.
- **Abgrenzung zur DSGVO-Einwilligung**: Diese Einwilligung betrifft die Teilnahme am Test, nicht die Datenverarbeitung. Datenschutzrechtliche Einwilligungen bleiben gesondert bestehen.

B. Inhalte der Einwilligung

1. **Artikel und Zielsetzung des Tests**: Die Teilnehmer müssen wissen, wozu der Test dient und welche Belastungen entstehen können.

   Beispiel: *Teilnehmer sollen erfahren, dass das KI-System ihre Bewerbungsunterlagen automatisch analysiert und welche möglichen Einschränkungen oder Fehlbewertungen auftreten können.*

2. **Bedingungen und Dauer**: Klare Informationen zur praktischen Durchführung, etwa Zeitaufwand oder besondere Rahmenbedingungen.

   Beispiel: *Ein Test dauert drei Monate, in denen Teilnehmer regelmäßig Rückmeldungen geben sollen.*

3. **Rechte und Garantien**: Besonders wichtig ist das Recht, den Test jederzeit ohne Nachteile zu beenden.

   Beispiel: *Ein Patient, der ein KI-gestütztes Diagnosesystem testet, darf seine Teilnahme sofort beenden, ohne dass dies seine medizinische Behandlung beeinträchtigt.*

4. **Rückgängigmachung von KI-Entscheidungen**: Teilnehmer müssen wissen, wie sie erreichen können, dass Vorhersagen oder Empfehlungen des Systems nicht berücksichtigt werden.

   Beispiel: *Ein Schüler darf beantragen, dass die Empfehlung der KI bei der Schulzuweisung nicht beachtet wird.*

5. **Identifikationsnummer und Kontaktperson**: Jeder Test hat eine eindeutige Nummer in der EU-Datenbank. Teilnehmer müssen eine Anlaufstelle haben, an die sie sich wenden können.

   Beispiel: *Teilnehmer erhalten die EU-ID und die E-Mail-Adresse des verantwortlichen Anbieters.*

C. Form und Dokumentation

- **Schriftform**: Die Einwilligung muss datiert und dokumentiert werden. Damit ist sie überprüfbar und nachvollziehbar.
- **Kopie für Teilnehmer**: Jeder Teilnehmer oder sein Vertreter bekommt eine Kopie. Das stärkt Transparenz und Nachweisbarkeit.

D. Besonderheiten

- **Abweichung bei Strafverfolgung**: Es ist keine Einwilligung nötig, wenn dadurch Tests im Bereich der Strafverfolgung unmöglich wären.
- **Zusatzschutz** bei schutzbedürftigen Gruppen: Für Kinder, Kranke oder andere besonders Schutzbedürftige gelten erhöhte Anforderungen.
- **Zusammenhang mit Artikel 60 KI-VO**: Artikel 61 ergänzt die Regelungen zum Ablauf und zur Registrierung der Tests unter Realbedingungen.

III. Zusammenfassung

Ziel	Schutz der Selbstbestimmung der Teilnehmer bei Tests unter Realbedingungen

Voraussetzung	Freiwillige und informierte Einwilligung vor Teilnahme
Inhalte	Artikel/Ziele, Bedingungen/Dauer, Rechte, Rückgängigmachung von Entscheidungen, Test-ID und Kontakt
Form	Schriftlich, datiert, dokumentiert, Kopie für Teilnehmer
Besonderheiten	Abweichung bei Strafverfolgung, zusätzlicher Schutz für vulnerable Gruppen

IV. Quellenverzeichnis

- Erwägungsgrund 141 KI-VO (EU) 2024/1689

Artikel 62 KI-VO

Maßnahmen für Anbieter und Betreiber, insbesondere KMU, einschließlich Start-up-Unternehmen

(1) Die Mitgliedstaaten ergreifen die folgenden Maßnahmen:

a) Sie gewähren KMU — einschließlich Start-up-Unternehmen —, die ihren Sitz oder eine Zweigniederlassung in der Union haben, soweit sie die Voraussetzungen und Auswahlkriterien erfüllen, vorrangigen Zugang zu den KI-Reallaboren; der vorrangige Zugang schließt nicht aus, dass andere als die in diesem Absatz genannten KMU, einschließlich Start-up-Unternehmen, Zugang zum KI-Reallabor erhalten, sofern sie ebenfalls die Zulassungsvoraussetzungen und Auswahlkriterien erfüllen;

b) sie führen besondere Sensibilisierungs- und Schulungsmaßnahmen für die Anwendung dieser Verordnung durch, die auf die Bedürfnisse von KMU, einschließlich Start-up-Unternehmen, Betreibern sowie gegebenenfalls lokalen Behörden ausgerichtet sind;

c) sie nutzen entsprechende bestehende Kanäle und richten gegebenenfalls neue Kanäle für die Kommunikation mit KMU, einschließlich Start-up-Unternehmen, Betreibern, anderen Innovatoren sowie gegebenenfalls lokalen Behörden ein, um Ratschläge zu geben und Fragen zur Durchführung dieser Verordnung, auch bezüglich der Beteiligung an KI-Reallaboren, zu beantworten;

d) sie fördern die Beteiligung von KMU und anderen einschlägigen Interessenträgern an der Entwicklung von Normen.

(2) Bei der Festsetzung der Gebühren für die Konformitätsbewertung gemäß Artikel 43 werden die besonderen Interessen und Bedürfnisse von KMU, einschließlich Start-up-Unternehmen, berücksichtigt, indem diese Gebühren proportional zur Größe der Unternehmen, der Größe ihres Marktes und anderen einschlägigen Kennzahlen gesenkt werden.

(3) Das Büro für Künstliche Intelligenz ergreift die folgenden Maßnahmen:

a) es stellt standardisierte Muster für die unter diese Verordnung fallenden Bereiche bereit, wie vom KI-Gremium in seinem Antrag festgelegt;

b) es entwickelt und führt eine zentrale Informationsplattform, über die allen Akteuren in der Union leicht nutzbare Informationen zu dieser Verordnung bereitgestellt werden;

c)es führt geeignete Informationskampagnen durch, um für die aus dieser Verordnung erwachsenden Pflichten zu sensibilisieren;

d)es bewertet und fördert die Zusammenführung bewährter Verfahren im Bereich der mit KI-Systemen verbundenen Vergabeverfahren.

I. Worum geht es?

Artikel 62 legt fest, wie kleine und mittlere Unternehmen (KMU), insbesondere Start-ups, bei der Umsetzung der KI-VO unterstützt werden sollen. Die Norm verpflichtet sowohl die Mitgliedstaaten als auch das Büro für Künstliche Intelligenz, konkrete Hilfsmaßnahmen einzurichten. Ziel ist es, KMU den Zugang zu Ressourcen zu erleichtern, Informationsdefizite zu verringern und die Kostenbelastung abzumildern. Damit soll verhindert werden, dass die Verordnung Innovation hemmt oder kleinere Marktteilnehmer überfordert.

II. Detailkommentar

A. Maßnahmen der Mitgliedstaaten

1. Vorrangiger Zugang zu KI-Reallaboren:

KMU mit Sitz oder Niederlassung in der EU sollen leichter Zugang zu Testumgebungen für KI erhalten. Dieser Vorrang schließt andere Anbieter nicht aus, wenn sie die gleichen Kriterien erfüllen.

Beispiel: *Ein Start-up aus Österreich möchte eine KI-Anwendung im Justizbereich erproben. Da es als KMU gilt, soll es vorrangig in ein Reallabor aufgenommen werden, sofern es die Zulassungskriterien erfüllt.*

2. Sensibilisierung und Schulung:

Mitgliedstaaten sollen spezielle Programme anbieten, die KMU über die Pflichten aus der KI-VO informieren und praktische Anleitungen geben.

Beispiel: *Ein Schulungsprogramm erklärt einem kleinen Software-Unternehmen, wie es die erforderliche Risikobewertung korrekt dokumentiert.*

3. Kommunikationskanäle:

Bestehende Anlaufstellen sollen genutzt und ggf. neue geschaffen werden, um KMU kontinuierlich zu beraten.

Beispiel: *Eine zentrale Hotline beantwortet Fragen eines Start-ups zur Einordnung seines Systems als Hochrisiko-KI.*

4. Beteiligung an Normenentwicklung:

KMU sollen in die Standardisierungsarbeit eingebunden werden, damit technische Normen nicht nur von großen Konzernen geprägt werden.

Beispiel: *Ein kleines Unternehmen mit Expertise in Spracherkennung kann Input bei der Entwicklung von Normen zu Transparenzpflichten geben.*

B. Gebührenregelung

Konformitätsbewertungen sind für KMU günstiger, da sie proportional zur Unternehmens- und Marktgröße berechnet werden.

C. Maßnahmen des Büros für Künstliche Intelligenz

1. **Bereitstellung standardisierter Muster**: Das Büro erstellt Vorlagen für verpflichtende Dokumentationen, um den Aufwand für KMU zu verringern.
2. **Zentrale Informationsplattform**: Alle Akteure erhalten online leicht zugängliche Informationen zur KI-VO.
3. **Informationskampagnen**: Die Pflichten aus der KI-VO sollen aktiv kommuniziert werden, damit auch kleinere Marktteilnehmer davon erfahren.
4. **Förderung bewährter Verfahren**: Das Büro sammelt und verbreitet Best Practices für KI-bezogene Vergabeverfahren.

D. Besonderheiten

- **Systematischer Zusammenhang**: Dieser Artikel ergänzt die allgemeinen Pflichten der Anbieter, indem er gezielt auf KMU zugeschnittene Unterstützungsmaßnahmen schafft. Er steht damit im engen Zusammenhang mit Artikel 55 KI-VOff (Büro für Künstliche Intelligenz) und Artikel 43 KI-VO(Konformitätsbewertung).
- **Zielsetzung der Norm**: Zweck ist die Förderung von Innovation und die Vermeidung von Markteintrittsbarrieren für kleinere Akteure. Ohne diese Maßnahmen bestünde die Gefahr, dass nur große Unternehmen die Anforderungen der KI-VO erfüllen könnten.

III. Zusammenfassung

Bereich	Maßnahmen	Nutzen für KMU
Mitgliedstaaten	Vorrangiger Zugang zu Reallaboren, Schulungen, Beratungsstellen, Normungsbeteiligung	Leichter Zugang zu Tests, mehr Wissen, bessere Unterstützung
Gebühren	Proportionale Senkung der Kosten für Konformitätsbewertung	Finanzielle Entlastung
Büro für Künstliche Intelligenz	Standardisierte Vorlagen, Informationsplattform, Kampagnen, Best Practices	Weniger Bürokratie, zentrale Infos, praktische Hilfestellungen

IV. Quellenverzeichnis

- Erwägungsgründe 143, 145 KI-VO (EU) 2024/1689

Artikel 63 KI-VO

Ausnahmen für bestimmte Akteure

(1) Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG können bestimmte Elemente des in Artikel 17 dieser Verordnung vorgeschriebenen Qualitätsmanagementsystems in vereinfachter Weise einhalten, sofern sie keine Partnerunternehmen oder verbundenen Unternehmen im Sinne dieser Empfehlung haben. Zu diesem Zweck arbeitet die Kommission Leitlinien zu den Elementen des Qualitätsmanagementsystems aus, die unter Berücksichtigung der Bedürfnisse von Kleinstunternehmen in vereinfachter Weise eingehalten werden können, ohne das Schutzniveau oder die Notwendigkeit zur Einhaltung der Anforderungen in Bezug auf Hochrisiko-KI-Systeme zu beeinträchtigen.

(2) Absatz 1 dieses Artikels ist nicht dahin gehend auszulegen, dass diese Akteure auch von anderen in dieser Verordnung festgelegten Anforderungen oder Pflichten, einschließlich der nach den Artikeln 9, 10, 11, 12, 13, 14, 15, 72 und 73 geltenden, befreit sind.

I. Worum geht es?

Artikel 63 schafft eine Erleichterung für Kleinstunternehmen bei der Umsetzung des QMS, das grundsätzlich für Anbieter von Hochrisiko-KI-Systemen vorgeschrieben ist. Kleinstunternehmen dürfen ein vereinfachtes Verfahren anwenden, um die Kosten und den Verwaltungsaufwand zu reduzieren. Zugleich bleibt aber klar: Alle anderen Pflichten der KI-VO müssen vollständig eingehalten werden. Ziel ist es also, Innovation nicht durch übermäßige Bürokratie zu behindern, ohne dabei das Schutzniveau für die Nutzer zu senken.

II. Detailkommentar

A. Begünstigte Unternehmen

- **Kleinstunternehmen**: Gemeint sind Unternehmen mit weniger als zehn Beschäftigten und einem Jahresumsatz oder einer Jahresbilanzsumme von höchstens zwei Mio. Euro.

- **Keine Verbundstrukturen**: Die Erleichterung gilt nur, wenn das Unternehmen nicht Teil einer größeren Unternehmensgruppe ist. Damit soll verhindert werden, dass größere Unternehmen künstlich von der Regelung profitieren.

B. Inhalt der Erleichterung

- **QMS**: Grundsätzlich verlangt die KI-VO ein umfassendes System zur Qualitätssicherung bei Hochrisiko-KI.
- **Vereinfachung**: Kleinstunternehmen dürfen bestimmte Elemente vereinfacht umsetzen. Welche Elemente das sind, legt die Kommission in Leitlinien fest.
- **Keine Abstriche beim Schutzniveau**: Auch bei vereinfachter Anwendung muss die Sicherheit und Rechtskonformität gewährleistet bleiben.

C. Grenzen der Erleichterung

- **Keine Befreiung von Kernpflichten**: Artikel 63 stellt klar, dass Kleinstunternehmen weiterhin alle materiellen Anforderungen der KI-VO erfüllen müssen. Dazu gehören insbesondere:
    - Risikomanagement
    - Daten- und Datenqualitätsanforderungen
    - Technische Dokumentation
    - Transparenzpflichten
    - Menschliche Aufsicht
    - Genauigkeit, Robustheit und Cybersicherheit
- **Rechtsklarheit**: Die Erleichterung betrifft nur das *Wie* des Qualitätsmanagements, nicht das *Ob* anderer Pflichten.

III. Zusammenfassung

Begünstigte	Nur Kleinstunternehmen ohne Partner- oder Tochterunternehmen
Inhalt	Vereinfachte Umsetzung des QMS
Grenze	Keine Befreiung von anderen Pflichten der KI-VO
Zweck	Verhältnismäßigkeit und Innovationsförderung ohne Sicherheitsverlust

IV. Quellenverzeichnis

- Erwägungsgrund 146 KI-VO (EU) 2024/1689

Artikel 64 KI-VO

Büro für Künstliche Intelligenz

(1) Die Kommission entwickelt über das Büro für Künstliche Intelligenz die Sachkenntnis und Fähigkeiten der Union auf dem Gebiet der KI.

(2) Die Mitgliedstaaten erleichtern dem Büro für Künstliche Intelligenz die ihm gemäß dieser Verordnung übertragenen Aufgaben.

I. Worum geht es?

Artikel 64 regelt die Einrichtung des Büros für Künstliche Intelligenz bei der EU-Kommission. Dieses Büro ist das zentrale Fachzentrum für KI auf Unionsebene. Es bündelt Wissen, koordiniert die Umsetzung der KI-VO und übernimmt zentrale Aufsichtsaufgaben – insbesondere bei KI-Modellen mit allgemeinem Verwendungszweck. Damit ist es die Schaltstelle für die EU-weite Governance im KI-Bereich.

II. Detailkommentar

A. Aufgaben des Büros

- Aufbau und Pflege von Fachwissen über KI.
- Unterstützung bei Anwendung und Durchsetzung der KI-VO.
- Beobachtung und Bewertung technologischer Entwicklungen.

B. Unterstützung durch die Mitgliedstaaten

- Pflicht zur Zusammenarbeit mit dem Büro.
- **Ziel**: Einheitliche Anwendung und Vermeidung von Doppelstrukturen.

C. Referate des Büros

Das Büro gliedert sich in mehrere Referate mit unterschiedlichen Aufgaben:

- **Regulatorische Aufsicht**: Überwachung der Pflichten von Anbietern, v.a. bei KI-Modellen mit allgemeinem Verwendungszweck.
- **Technische Expertise**: Analyse neuer Technologien, Nutzung von Test- und Versuchseinrichtungen.
- **Wissenschaftliches Referat**: Einbindung unabhängiger Experten und Gutachter.
- **Koordinierung und Zusammenarbeit**: Schnittstelle zu nationalen Behörden und zum KI-Gremium.
- **Marktüberwachung und Durchsetzung**: Unterstützung bei Ermittlungen, Anforderung von Unterlagen, Verhängung von Maßnahmen (zB Einschränkung oder Rücknahme eines Modells).

D. Besonderheiten

- Das Büro hat in bestimmten Fällen die **Befugnisse einer Marktüberwachungsbehörde** (vgl Verordnung (EU) 2019/1020).
- Zuständig insbesondere für **KI-Modelle mit allgemeinem Verwendungszweck**, wenn Modell und System gemeinsam bereitgestellt werden.
- Nationale Marktüberwachungsbehörden bleiben zuständig für die meisten Hochrisiko-KI-Systeme, müssen jedoch eng mit dem Büro kooperieren.

Beispiel: *Eine nationale Behörde ermittelt gegen ein Hochrisiko-KI-System, hat jedoch keinen Zugang zu bestimmten Modelldaten. Sie wendet sich an das Büro, das die Daten einfordern und die Untersuchung unterstützen kann.*

III. Zusammenfassung

Büro	Zentrales Fachzentrum für KI in der EU
Hauptaufgaben	Wissen aufbauen, Aufsicht, Koordinierung
Mitgliedstaaten	Müssen das Büro unterstützen

Zuständigkeit	Besonders für KI-Modelle mit allgemeinem Verwendungszweck
Referate	Regulatorik, Technik, Wissenschaft, Kooperation, Marktüberwachung

IV. Quellenverzeichnis

- Erwägungsgründe 148, 161, 162, 164 KI-VO (EU) 2024/1689

Artikel 65 KI-VO

Einrichtung und Struktur des Europäischen Gremiums für Künstliche Intelligenz

(1) Ein Europäisches Gremium für Künstliche Intelligenz (im Folgenden „KI-Gremium") wird hiermit eingerichtet.

(2) Das KI-Gremium setzt sich aus einem Vertreter je Mitgliedstaat zusammen. Der Europäische Datenschutzbeauftragte nimmt als Beobachter teil. Das Büro für Künstliche Intelligenz nimmt ebenfalls an den Sitzungen des KI-Gremiums teil, ohne sich jedoch an den Abstimmungen zu beteiligen. Andere Behörden oder Stellen der Mitgliedstaaten und der Union oder Sachverständige können im Einzelfall zu den Sitzungen des KI-Gremiums eingeladen werden, wenn die erörterten Fragen für sie von Belang sind.

(3) Die Vertreter werden von ihren Mitgliedstaaten für einen Zeitraum von drei Jahren benannt, der einmal verlängert werden kann.

(4) Die Mitgliedstaaten sorgen dafür, dass ihre Vertreter im KI-Gremium

a) in ihrem Mitgliedstaat über die einschlägigen Kompetenzen und Befugnisse verfügen, sodass sie aktiv zur Bewältigung der in Artikel 66 genannten Aufgaben des KI-Gremiums beitragen können;

b) gegenüber dem KI-Gremium sowie gegebenenfalls, unter Berücksichtigung der Erfordernisse der Mitgliedstaaten, gegenüber Interessenträgern als zentrale Ansprechpartner fungieren;

c) ermächtigt sind, auf die Kohärenz und die Abstimmung zwischen den zuständigen nationalen Behörden in ihrem Mitgliedstaat bei der Durchführung dieser Verordnung hinzuwirken, auch durch Erhebung einschlägiger Daten und Informationen für die Zwecke der Erfüllung ihrer Aufgaben im KI-Gremium.

(5) Die benannten Vertreter der Mitgliedstaaten nehmen die Geschäftsordnung des KI-Gremiums mit einer Zweidrittelmehrheit an. In der Geschäftsordnung sind insbesondere die Vorgehensweise für das Auswahlverfahren, die Dauer des Mandats und die genauen Aufgaben des Vorsitzes, die Abstimmungsregelungen und die Organisation der Tätigkeiten des KI-Gremiums und seiner Untergruppen festgelegt.

(6) Das KI-Gremium richtet zwei ständige Untergruppen ein, um Marktüberwachungsbehörden eine Plattform für die Zusammenarbeit und den Austausch zu bieten und Behörden über Angelegenheiten, die jeweils die Marktüberwachung und notifizierte Stellen betreffen, zu unterrichten.

Die ständige Untergruppe für Marktüberwachung sollte für diese Verordnung als Gruppe für die Verwaltungszusammenarbeit (ADCO-Gruppe) im Sinne des Artikels 30 der Verordnung (EU) 2019/1020 fungieren.

Das KI-Gremium kann weitere ständige oder nichtständige Untergruppen einrichten, falls das für die Prüfung bestimmter Fragen zweckmäßig sein sollte. Gegebenenfalls können Vertreter des in Artikel 67 genannten Beratungsforums als Beobachter zu diesen Untergruppen oder zu bestimmten Sitzungen dieser Untergruppen eingeladen werden.

(7) Das KI-Gremium wird so organisiert und geführt, dass bei seinen Tätigkeiten Objektivität und Unparteilichkeit gewahrt sind.

(8) Den Vorsitz im KI-Gremium führt einer der Vertreter der Mitgliedstaaten. Die Sekretariatsgeschäfte des KI-Gremiums werden vom Büro für Künstliche Intelligenz geführt; dieses beruft auf Anfrage des Vorsitzes die Sitzungen ein und erstellt die Tagesordnung im Einklang mit den Aufgaben des KI-Gremiums gemäß dieser Verordnung und seiner Geschäftsordnung.

I. Worum geht es?

Artikel 65 schafft das Europäische Gremium für Künstliche Intelligenz (KI-Gremium). Dieses Gremium ist ein Zusammenschluss der Mitgliedstaaten auf EU-Ebene und dient als zentrale Koordinierungs- und Beratungsinstanz. Es soll für eine einheitliche Anwendung der KI-VO sorgen, Marktüberwachungsbehörden vernetzen und als Plattform für Fachwissen und Austausch dienen. Damit ergänzt das KI-Gremium die Arbeit des Büros für Künstliche Intelligenz.

II. Detailkommentar

A. Zusammensetzung

- **Mitglieder**: je ein Vertreter pro Mitgliedstaat.

- **Beobachter**: Europäischer Datenschutzbeauftragter.
- **Teilnehmer ohne Stimmrecht**: Büro für Künstliche Intelligenz.
- **Weitere Einladungen**: andere Behörden oder Sachverständige bei Bedarf.
- **Amtszeit**: drei Jahre, einmal verlängerbar.

B. Anforderungen an die Vertreter

Die Vertreter müssen:

- **Kompetenz und Befugnisse** besitzen, um im KI-Gremium wirksam mitzuwirken.
- Als **zentrale Ansprechpartner** für ihr Land und ggf. auch für Interessenträger fungieren.
- Die **Koordination zwischen nationalen Behörden** sicherstellen und Daten sammeln.

Beispiel: ***Harmonisierung:*** *Ein Mitgliedstaat möchte strengere Vorgaben für KI-Prüfungen einführen. Das Thema wird im KI-Gremium diskutiert, um EU-weite Einheitlichkeit zu wahren.*

C. Organisation und Geschäftsordnung

- Annahme durch Zweidrittelmehrheit.
- Regelt ua Auswahlverfahren, Mandatsdauer, Aufgaben des Vorsitzes, Abstimmungsregeln und Arbeitsweise.

D. Untergruppen

- **Pflichtuntergruppen**:
    - Marktüberwachung (fungiert als ADCO-Gruppe gem Artikel 30 VO (EU) 2019/1020).
    - Notifizierte Stellen.

- **Optionale Untergruppen**: weitere permanente oder temporäre Gruppen möglich.
- **Teilnahme von Beobachtern** (zB Beratungsforum) nach Bedarf.

Beispiel: ***Koordination bei Marktüberwachung:*** *Nationale Behörden stimmen sich in der Untergruppe ab, um ein einheitliches Vorgehen gegen ein fehlerhaftes KI-System sicherzustellen.*

E. Leitung und Organisation

- **Vorsitz**: von einem Mitgliedstaat-Vertreter geführt.
- **Sekretariat**: Büro für Künstliche Intelligenz (koordiniert Sitzungen, Agenda, Dokumentation).
- **Objektivität und Unparteilichkeit**: verpflichtende Leitprinzipien.

F. Besonderheiten

- Das KI-Gremium ist **kein Entscheidungsgremium**, sondern ein **Beratungs- und Koordinationsforum**.
- Es spiegelt die Vielfalt der Mitgliedstaaten wider und sorgt für **Harmonisierung**, ohne nationale Zuständigkeiten vollständig zu ersetzen.
- Durch die Untergruppen wird eine **praktische Zusammenarbeit** zwischen Marktüberwachungsbehörden und notifizierten Stellen erleichtert.

Beispiel*: Unterstützung nationaler Behörden**: Bei Unsicherheiten über die Auslegung technischer Normen kann das KI-Gremium Empfehlungen erarbeiten.*

III. Zusammenfassung

Einrichtung	Gremium aus Vertretern aller Mitgliedstaaten
Mitglieder	Vertreter mit Fachkompetenz und Befugnissen

Untergruppen	Marktüberwachung (ADCO), Notifizierte Stellen, weitere möglich
Leitung	Vorsitz durch Mitgliedstaat, Sekretariat durch Büro für Künstliche Intelligenz
Funktion	Beratungs- und Koordinierungsorgan, kein Entscheidungsgremium

IV. Quellenverzeichnis

- Erwägungsgründe 20, 53, 121, 143, 148, 149, 150, 161 KI-VO (EU) 2024/1689

Artikel 66 KI-VO

Aufgaben des KI-Gremiums

Das KI-Gremium berät und unterstützt die Kommission und die Mitgliedstaaten, um die einheitliche und wirksame Anwendung dieser Verordnung zu erleichtern. Für diese Zwecke kann das KI-Gremium insbesondere

a)zur Koordinierung zwischen den für die Anwendung dieser Verordnung zuständigen nationalen Behörden beitragen und in Zusammenarbeit mit den betreffenden Marktüberwachungsbehörden und vorbehaltlich ihrer Zustimmung gemeinsame Tätigkeiten der Marktüberwachungsbehörden gemäß Artikel 74 Absatz 11 unterstützen;

b)technisches und regulatorisches Fachwissen und bewährte Verfahren zusammentragen und unter den Mitgliedstaaten verbreiten;

c)zur Durchführung dieser Verordnung Beratung anbieten, insbesondere im Hinblick auf die Durchsetzung der Vorschriften zu KI-Modellen mit allgemeinem Verwendungszweck;

d)zur Harmonisierung der Verwaltungspraxis in den Mitgliedstaaten beitragen, auch bezüglich der Ausnahme vom Konformitätsbewertungsverfahren gemäß Artikel 46 und der Funktionsweise von KI-Reallaboren und Tests unter Realbedingungen gemäß den Artikeln 57, 59 und 60;

e)auf Anfrage der Kommission oder in Eigeninitiative Empfehlungen und schriftliche Stellungnahmen zu einschlägigen Fragen der Durchführung dieser Verordnung und ihrer einheitlichen und wirksamen Anwendung abgeben, einschließlich

i)zur Entwicklung und Anwendung von Verhaltenskodizes und Praxisleitfäden gemäß dieser Verordnung sowie der Leitlinien der Kommission;

ii)zur Bewertung und Überprüfung dieser Verordnung gemäß Artikel 112, auch in Bezug auf die Meldung schwerwiegender Vorfälle gemäß Artikel 73 und das Funktionieren der EU-Datenbank gemäß Artikel 71, die Ausarbeitung der delegierten Rechtsakte oder Durchführungsrechtsakte sowie im Hinblick auf mögliche Anpassungen dieser Verordnung an die

in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union;

iii) zu technischen Spezifikationen oder geltenden Normen in Bezug auf die in Kapitel III Abschnitt 2 festgelegten Anforderungen;

iv) zur Anwendung der in den Artikeln 40 und 41 genannten harmonisierten Normen oder gemeinsamen Spezifikationen;

v) zu Tendenzen, etwa im Bereich der globalen Wettbewerbsfähigkeit Europas auf dem Gebiet der KI, bei der Verbreitung von KI in der Union und bei der Entwicklung digitaler Fähigkeiten;

vi) zu Tendenzen im Bereich der sich ständig weiterentwickelnden Typologie der KI-Wertschöpfungsketten insbesondere hinsichtlich der sich daraus ergebenden Auswirkungen auf die Rechenschaftspflicht;

vii) zur möglicherweise notwendigen Änderung des Anhangs III im Einklang mit Artikel 7 und zur möglicherweise notwendigen Überarbeitung des Artikels 5 gemäß Artikel 112 unter Berücksichtigung der einschlägigen verfügbaren Erkenntnisse und der neuesten technologischen Entwicklungen;

f) die Kommission bei der Förderung der KI-Kompetenz, der Sensibilisierung und Aufklärung der Öffentlichkeit in Bezug auf die Vorteile, Risiken, Schutzmaßnahmen, Rechte und Pflichten im Zusammenhang mit der Nutzung von KI-Systemen unterstützen;

g) die Entwicklung gemeinsamer Kriterien und eines gemeinsamen Verständnisses der Marktteilnehmer und der zuständigen Behörden in Bezug auf die in dieser Verordnung vorgesehenen einschlägigen Konzepte erleichtern, auch durch einen Beitrag zur Entwicklung von Benchmarks;

h) gegebenenfalls mit anderen Organen, Einrichtungen und sonstigen Stellen der EU, einschlägigen Sachverständigengruppen und Netzwerken der EU insbesondere in den Bereichen Produktsicherheit, Cybersicherheit, Wettbewerb, digitale und Mediendienste, Finanzdienstleistungen, Verbraucherschutz, Datenschutz und Schutz der Grundrechte zusammenarbeiten;

i) zur wirksamen Zusammenarbeit mit den zuständigen Behörden von Drittstaaten und mit internationalen Organisationen beitragen;

j)die zuständigen nationalen Behörden und die Kommission beim Aufbau des für die Durchführung dieser Verordnung erforderlichen organisatorischen und technischen Fachwissens beraten, unter anderem durch einen Beitrag zur Einschätzung des Schulungsbedarfs des Personals der Mitgliedstaaten, das an der Durchführung dieser Verordnung beteiligt ist;

k)dem Büro für Künstliche Intelligenz helfen, die zuständigen nationalen Behörden bei der Einrichtung und Entwicklung von KI-Reallaboren zu unterstützen, und die Zusammenarbeit und den Informationsaustausch zwischen KI-Reallaboren erleichtern;

l)zur Entwicklung von Leitfäden beitragen und diesbezüglich entsprechend beraten;

m)die Kommission zu internationalen Angelegenheiten im Bereich der KI beraten;

n)der Kommission Stellungnahmen zu qualifizierten Warnungen in Bezug auf KI-Modelle mit allgemeinem Verwendungszweck vorlegen;

o)Stellungnahmen der Mitgliedstaaten zu qualifizierten Warnungen in Bezug auf KI-Modelle mit allgemeinem Verwendungszweck entgegennehmen sowie zu nationalen Erfahrungen und Praktiken bei der Überwachung und Durchsetzung von KI-Systemen, insbesondere von Systemen, die KI-Modelle mit allgemeinem Verwendungszweck integrieren.

I. Worum geht es?

Artikel 66 legt die Aufgaben des Europäischen KI-Gremiums fest. Das Gremium soll die Kommission und die Mitgliedstaaten beraten und unterstützen, damit die KI-VO in allen EU-Ländern einheitlich und wirksam angewendet wird. Es fungiert damit als zentrales Koordinations- und Beratungsorgan, das Fachwissen sammelt, den Erfahrungsaustausch erleichtert und praktische Orientierung gibt.

II. Detailkommentar

A. Kernaufgabe

- **Beratung und Unterstützung**: Das Gremium hilft Kommission und Mitgliedstaaten, die KI-VO einheitlich umzusetzen.

- **Koordination**: Es vernetzt nationale Behörden, damit kein Flickenteppich an unterschiedlichen Regeln entsteht.

Beispiel: *Ein Mitgliedstaat versteht die Pflichten für KI-Reallabore anders als andere. Das Gremium erarbeitet eine gemeinsame Linie.*

B. Zentrale Tätigkeitsfelder

1. Koordinierung der Behörden

- Unterstützung gemeinsamer Aktionen von Marktüberwachungsbehörden.
- Austausch über nationale Vollzugspraktiken.

Beispiel*: Ein KI-System fällt in mehreren Staaten gleichzeitig auf – das Gremium hilft, die Kontrollen abzustimmen.*

2. Sammlung und Verbreitung von Fachwissen

- Bereitstellung von technischem und regulatorischem Wissen.
- Austausch bewährter Verfahren („Best Practices").

Beispiel: ***Warnsystem****: Ein Mitgliedstaat meldet Probleme mit einem KI-Modell. Das Gremium bündelt die Informationen und entwickelt Empfehlungen für die gesamte EU.*

3. Beratung zur Umsetzung

- Empfehlungen zur Durchsetzung, zB bei KI-Modellen mit allgemeinem Verwendungszweck.
- Stellungnahmen zu Leitlinien, Normen oder Rechtsakten.

Beispiel*: Die Kommission fragt, wie neue technische Normen für Transparenzanforderungen praktisch umgesetzt werden können.*

4. Harmonisierung der Verwaltungspraxis

- Einheitliche Vorgehensweisen bei Ausnahmen von Konformitätsprüfungen.
- Begleitung von KI-Reallaboren und Tests unter Realbedingungen.

5. Empfehlungen und Stellungnahmen

- Eigene Initiativen oder Antworten auf Anfragen der Kommission.
- Themen: Verhaltenskodizes, Überprüfung der Verordnung, technische Spezifikationen, Normen, internationale Trends.

Beispiel*: Das Gremium empfiehlt einen freiwilligen Kodex für KI-Anbieter zur besseren Nutzeraufklärung.*

6. Förderung von KI-Kompetenz

- Unterstützung bei Aufklärung und Öffentlichkeitsarbeit.
- **Ziel**: mehr Wissen über Rechte, Risiken und Chancen von KI.

Beispiel: *Öffentlichkeitsarbeit - Das Gremium unterstützt eine EU-weite Kampagne, um Bürger über ihre Rechte im Umgang mit KI aufzuklären.*

7. Zusammenarbeit und Vernetzung

- Austausch mit EU-Agenturen (zB ENISA, Verbraucher- und Wettbewerbsbehörden).
- Zusammenarbeit mit Drittstaaten und internationalen Organisationen.

8. Unterstützung beim Kapazitätsaufbau

- Beratung zu Schulungsbedarf für Behörden.
- Unterstützung bei der Einrichtung und Vernetzung von KI-Reallaboren.

9. Internationale Dimension

- Beratung der Kommission in globalen KI-Fragen.
- Stellungnahmen zu Warnungen über KI-Modelle mit allgemeinem Verwendungszweck.

Beispiel: *Internationale Abstimmung - Ein Drittstaat führt strenge Vorgaben für KI-Systeme ein. Das Gremium berät die Kommission, wie darauf reagiert werden kann.*

C. Besonderheiten

- **Breites Aufgabenspektrum**: Von technischer Normung über internationale Kooperation bis zur Öffentlichkeitsarbeit.
- **Keine Entscheidungsgewalt**: Das Gremium kann nur beraten, Empfehlungen abgeben und koordinieren.
- **Flexibilität**: Es kann auch eigene Initiativen starten und Themen aufgreifen, die nicht direkt von der Kommission angefragt wurden.

III. Zusammenfassung

Koordinierung	Vernetzung nationaler Behörden, Unterstützung gemeinsamer Aktionen
Fachwissen	Sammlung und Verbreitung von Know-how und Best Practices
Beratung	Empfehlungen zu Umsetzung, Normen, Rechtsakten, internationalen Trends
Harmonisierung	Einheitliche Verwaltungspraxis und Handhabung von Reallaboren
Kompetenzförderung	Aufklärung der Öffentlichkeit, Stärkung von KI-Kenntnissen
Internationale Rolle	Zusammenarbeit mit Drittstaaten und Organisationen, globale Beratung

IV. Quellenverzeichnis

- Erwägungsgrund 149 KI-VO (EU) 2024/1689

Artikel 67 KI-VO

Beratungsforum

(1) Es wird ein Beratungsforum eingerichtet, das technisches Fachwissen bereitstellt, das KI-Gremium und die Kommission berät und zu deren Aufgaben im Rahmen dieser Verordnung beiträgt.

(2) Die Mitglieder des Beratungsforums vertreten eine ausgewogene Auswahl von Interessenträgern, darunter die Industrie, Start-up-Unternehmen, KMU, die Zivilgesellschaft und die Wissenschaft. Bei der Zusammensetzung des Beratungsforums wird auf ein ausgewogenes Verhältnis zwischen wirtschaftlichen und nicht-wirtschaftlichen Interessen und innerhalb der Kategorie der wirtschaftlichen Interessen zwischen KMU und anderen Unternehmen geachtet.

(3) Die Kommission ernennt die Mitglieder des Beratungsforums gemäß den in Absatz 2 genannten Kriterien aus dem Kreis der Interessenträger mit anerkanntem Fachwissen auf dem Gebiet der KI.

(4) Die Amtszeit der Mitglieder des Beratungsforums beträgt zwei Jahre; sie kann bis zu höchstens vier Jahre verlängert werden.

(5) Die Agentur der Europäischen Union für Grundrechte, ENISA, das Europäische Komitee für Normung (CEN), das Europäische Komitee für elektrotechnische Normung (CENELEC) und das Europäische Institut für Telekommunikationsnormen (ETSI) sind ständige Mitglieder des Beratungsforums.

(6) Das Beratungsforum gibt sich eine Geschäftsordnung. Es wählt gemäß den in Absatz 2 festgelegten Kriterien zwei Ko-Vorsitzende unter seinen Mitgliedern. Die Amtszeit der Ko-Vorsitzenden beträgt zwei Jahre und kann einmal verlängert werden.

(7) Das Beratungsforum hält mindestens zweimal pro Jahr Sitzungen ab. Das Beratungsforum kann Sachverständige und andere Interessenträger zu seinen Sitzungen einladen.

(8) Das Beratungsforum kann auf Ersuchen des KI-Gremiums oder der Kommission Stellungnahmen, Empfehlungen und schriftliche Beiträge ausarbeiten.

(9) Das Beratungsforum kann gegebenenfalls ständige oder zeitweilige Untergruppen einsetzen, um spezifische Fragen im Zusammenhang mit den Zielen dieser Verordnung zu prüfen.

(10) Das Beratungsforum erstellt jährlich einen Bericht über seine Tätigkeit. Dieser Bericht wird veröffentlicht.

I. Worum geht es?

Artikel 67 regelt die Einrichtung eines **Beratungsforums**, das die Kommission und das KI-Gremium mit technischem Fachwissen unterstützt. Es stellt sicher, dass **verschiedene Interessengruppen** – von Industrie bis Zivilgesellschaft – an der Umsetzung der KI-VO beteiligt sind. Damit wird die Verordnung nicht nur von Behörden getragen, sondern auch durch Wissen und Perspektiven aus Wirtschaft, Wissenschaft und Gesellschaft ergänzt.

II. Detailkommentar

A. Zusammensetzung

- **Ausgewogene Vertretung**: Industrie, Start-ups, KMU, Wissenschaft und Zivilgesellschaft.
- **Ständige Mitglieder**: Agentur für Grundrechte, ENISA, CEN, CENELEC, ETSI.
- **Ernennung**: Die Kommission wählt Mitglieder anhand von Fachwissen und Ausgewogenheit.
- **Amtszeit**: Zwei Jahre, verlängerbar bis vier Jahre.

Beispiel: *Ein kleines KI-Start-up und eine NGO gegen Diskriminierung sitzen gemeinsam im Forum, um beide Seiten einzubringen.*

B. Organisation und Arbeitsweise

1. Struktur

- Geschäftsordnung vom Forum selbst beschlossen.

- Zwei Co-Vorsitzende, gewählt für zwei Jahre (einmal verlängerbar).

2. Sitzungen

- Mindestens zweimal pro Jahr.
- Möglichkeit, Sachverständige und weitere Stakeholder einzuladen.

3. Untergruppen

- Ständige oder temporäre Arbeitsgruppen zu spezifischen Fragen möglich.

Beispiel: *Eine Untergruppe analysiert den Einsatz von KI im Gesundheitswesen, während eine andere sich mit Standards für KI in Schulen beschäftigt.*

C. Aufgaben

- **Fachliche Beratung**: Unterstützung der Kommission und des KI-Gremiums bei deren Aufgaben.
- **Beiträge**: Stellungnahmen, Empfehlungen und schriftliche Analysen auf Anfrage oder aus eigener Initiative.
- **Berichtspflicht**: Jährlicher Tätigkeitsbericht, öffentlich zugänglich.

Beispiel: *Das Forum empfiehlt Leitlinien für bessere Transparenz bei KI-basierten Chatbots im Kundenservice.*

D. Besonderheiten

- **Beteiligung von Interessenträgern**: Sicherstellung, dass die Umsetzung der KI-VO nicht allein staatlich gesteuert wird.
- **Ausgewogenheit**: Gleiche Gewichtung von wirtschaftlichen und nicht-wirtschaftlichen Interessen.
- **Transparenz**: Veröffentlichung des Jahresberichts sorgt für Einblick in Arbeitsweise und Empfehlungen.

Beispiel: ***Ausgewogenheit:*** *Das Forum verhindert, dass nur große Tech-Konzerne den Ton angeben, indem auch KMU und NGOs repräsentiert sind.*

Beispiel: ***Unterstützung der Kommission:*** *Vor einer geplanten Änderung von Anhang III liefert das Forum technische Einschätzungen zu neuen Risikokategorien.*

Beispiel*: Öffentlichkeitswirksamkeit:* *Der jährliche Bericht des Forums wird breit kommuniziert und schafft Vertrauen in die KI-Regulierung.*

III. Zusammenfassung

Zusammensetzung	Breite Vertretung von Industrie, Zivilgesellschaft, Wissenschaft und Standardisierungsorganisationen
Organisation	Geschäftsordnung, zwei Co-Vorsitzende, Untergruppen möglich
Arbeitsweise	Mindestens zwei Sitzungen pro Jahr, Möglichkeit zur Einladung von Experten
Aufgaben	Beratung, Stellungnahmen, Empfehlungen, jährlicher Bericht
Besonderheiten	Transparenz, Ausgewogenheit, Einbindung von KMU und NGOs

IV. Quellenverzeichnis

- Erwägungsgrund 150 KI-VO (EU) 2024/1689

Artikel 68 KI-VO

Wissenschaftliches Gremium unabhängiger Sachverständiger

(1) Die Kommission erlässt im Wege eines Durchführungsrechtsakts Bestimmungen über die Einrichtung eines wissenschaftlichen Gremiums unabhängiger Sachverständiger („wissenschaftliches Gremium"), das die Durchsetzungstätigkeiten im Rahmen dieser Verordnung unterstützen soll. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(2) Das wissenschaftliche Gremium setzt sich aus Sachverständigen zusammen, die von der Kommission auf der Grundlage aktueller wissenschaftlicher oder technischer Fachkenntnisse auf dem Gebiet der KI, die zur Erfüllung der in Absatz 3 genannten Aufgaben erforderlich sind, ausgewählt werden, und muss nachweisen können, dass es alle folgenden Bedingungen erfüllt:

a) es verfügt über besondere Fachkenntnisse und Kompetenzen sowie über wissenschaftliches oder technisches Fachwissen auf dem Gebiet der KI;

b) es ist von Anbietern von KI-Systemen oder KI-Modellen mit allgemeinem Verwendungszweck unabhängig;

c) es ist in der Lage, Tätigkeiten sorgfältig, präzise und objektiv auszuführen.

Die Kommission legt in Absprache mit dem KI-Gremium die Anzahl der Sachverständigen des Gremiums nach Maßgabe der jeweiligen Erfordernisse fest und sorgt für eine ausgewogene Vertretung der Geschlechter und eine gerechte geografische Verteilung.

(3) Das wissenschaftliche Gremium berät und unterstützt das Büro für Künstliche Intelligenz, insbesondere in Bezug auf folgende Aufgaben:

a) Unterstützung bei der Durchführung und Durchsetzung dieser Verordnung in Bezug auf KI-Modelle und -Systeme mit allgemeinem Verwendungszweck, insbesondere indem es

i) das Büro für Künstliche Intelligenz im Einklang mit Artikel 90 vor möglichen systemischen Risiken von KI-Modellen mit allgemeinem Verwendungszweck auf Unionsebene warnt;

ii) einen Beitrag zur Entwicklung von Instrumenten und Methoden für die Bewertung der Fähigkeiten von KI-Modellen und -Systemen mit allgemeinem Verwendungszweck, auch durch Benchmarks, leistet;

iii) Beratung über die Einstufung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko anbietet;

iv) Beratung über die Einstufung verschiedener KI-Modelle und -Systeme mit allgemeinem Verwendungszweck anbietet;

v) einen Beitrag zur Entwicklung von Instrumenten und Mustern leistet;

b) Unterstützung der Arbeit der Marktüberwachungsbehörden auf deren Ersuchen;

c) Unterstützung grenzüberschreitender Marktüberwachungstätigkeiten gemäß Artikel 74 Absatz 11, ohne dass die Befugnisse der Marktüberwachungsbehörden berührt werden;

d) Unterstützung des Büros für Künstliche Intelligenz bei der Wahrnehmung seiner Aufgaben im Rahmen des Schutzklauselverfahrens der Union gemäß Artikel 81.

(4) Die Sachverständigen des wissenschaftlichen Gremiums führen ihre Aufgaben nach den Grundsätzen der Unparteilichkeit und der Objektivität aus und gewährleisten die Vertraulichkeit der Informationen und Daten, in deren Besitz sie bei der Ausführung ihrer Aufgaben und Tätigkeiten gelangen. Sie dürfen bei der Wahrnehmung ihrer Aufgaben nach Absatz 3 weder Weisungen anfordern noch entgegennehmen. Jeder Sachverständige gibt eine Interessenerklärung ab, die öffentlich zugänglich gemacht wird. Das Büro für Künstliche Intelligenz richtet Systeme und Verfahren ein, mit denen mögliche Interessenkonflikte aktiv bewältigt und verhindert werden können.

(5) Der in Absatz 1 genannte Durchführungsrechtsakt enthält Bestimmungen über die Bedingungen, Verfahren und detaillierten Regelungen nach denen das wissenschaftliche Gremium und seine Mitglieder Warnungen ausgeben und das Büro für Künstliche Intelligenz um Unterstützung bei der Wahrnehmung der Aufgaben des wissenschaftlichen Gremiums ersuchen können.

I. Worum geht es?

Artikel 68 regelt die Einrichtung eines wissenschaftlichen Gremiums unabhängiger Sachverständiger, das die Umsetzung und Durchsetzung der KI-VO unterstützt. Dieses Gremium liefert wissenschaftliche und technische Expertise, insbesondere zu KI-Modellen mit allgemeinem Verwendungszweck, und soll die Arbeit des Büros für Künstliche Intelligenz und der nationalen Behörden fachlich absichern. Seine Unabhängigkeit und Objektivität sind zentrale Prinzipien.

II. Detailkommentar

A. Einrichtung und Zusammensetzung

- **Rechtsgrundlage**: Einrichtung erfolgt durch einen Durchführungsrechtsakt der Kommission.
- **Mitglieder**: Auswahl durch die Kommission auf Basis aktueller wissenschaftlicher und technischer Expertise im KI-Bereich.
- **Anforderungen**: Fachkenntnisse, Unabhängigkeit von Anbietern, sorgfältige und objektive Arbeitsweise.
- **Ausgewogenheit**: Kommission sorgt für Geschlechterbalance und geografische Verteilung.

B. Aufgaben

1. Unterstützung bei Durchsetzung

- Warnung vor systemischen Risiken durch KI-Modelle.
- Beratung zur Einstufung von KI-Modellen und -Systemen.
- Entwicklung von Instrumenten und Benchmarks für Leistungsbewertungen.

2. Unterstützung der Marktüberwachung

- Fachliche Hilfe für nationale Marktüberwachungsbehörden auf Anfrage.
- Beteiligung an grenzüberschreitenden Maßnahmen.

3. Zusammenarbeit mit dem Büro für Künstliche Intelligenz

- Unterstützung bei Verfahren zur Schutzklausel.
- Fachliche Beratung zu risikobehafteten Entwicklungen.

Beispiel: *Das Gremium entwickelt ein Testverfahren, um zu prüfen, ob ein Sprachmodell ein systemisches Risiko darstellt.*

C. Arbeitsweise und Unabhängigkeit

- **Grundsätze**: Unparteilichkeit, Objektivität, Vertraulichkeit.
- **Keine Weisungen**: Mitglieder arbeiten unabhängig und dürfen keine Vorgaben von außen annehmen.
- **Interessenerklärungen**: Offenlegungspflicht, öffentlich zugänglich.
- **Konfliktmanagement**: Büro für Künstliche Intelligenz richtet Systeme zur Vermeidung von Interessenkonflikten ein.

Beispiel: *Ein Experte legt offen, dass er nebenbei für ein Beratungsunternehmen tätig ist, das aber nicht im KI-Sektor arbeitet. Dadurch kann ein potenzieller Konflikt ausgeschlossen werden.*

D. Verfahren und Rahmenbedingungen

- **Durchführungsrechtsakt**: Legt Regeln für Arbeitsweise, Verfahren zur Abgabe von Warnungen und Unterstützung fest.
- **Flexibilität**: Anzahl der Sachverständigen orientiert sich am Bedarf.
- **Einbindung**: Zusammenarbeit mit KI-Gremium zur Abstimmung.

Beispiel: *Das wissenschaftliche Gremium gibt eine qualifizierte Warnung zu einem generativen KI-System ab, woraufhin das Büro für* Künstliche Intelligenz *eine Untersuchung einleitet.*

E. Besonderheiten

- **Stärkung der Durchsetzung**: Ergänzung der Kapazitäten der Mitgliedstaaten.
- **Fokus auf systemische Risiken**: Frühwarnmechanismus für problematische KI-Modelle.
- **Wissenschaftliche Autorität**: Expertise als Gegengewicht zu wirtschaftlichen Interessen.

III. Zusammenfassung

Einrichtung	Durchführungsrechtsakt der Kommission, Auswahl unabhängiger Experten
Zusammensetzung	Fachwissen, Unabhängigkeit, ausgewogene Verteilung
Aufgaben	Unterstützung Büro für Künstliche Intelligenz, Warnungen, Beratung, Unterstützung Marktüberwachung
Arbeitsweise	Objektiv, unparteiisch, vertraulich, Interessenerklärungen
Besonderheiten	Fokus auf systemische Risiken, Stärkung der Durchsetzung, wissenschaftliche Autorität

Artikel 69 KI-VO

Zugang zum Pool von Sachverständigen durch die Mitgliedstaaten

(1) Die Mitgliedstaaten können Sachverständige des wissenschaftlichen Gremiums hinzuziehen, um ihre Durchsetzungstätigkeiten im Rahmen dieser Verordnung zu unterstützen.

(2) Die Mitgliedstaaten können verpflichtet werden, für die Beratung und Unterstützung durch die Sachverständigen Gebühren zu entrichten. Struktur und Höhe der Gebühren sowie Umfang und Struktur erstattungsfähiger Kosten werden in dem in Artikel 68 Absatz 1 genannten Durchführungsrechtsakt festgelegt, wobei die Zielsetzung berücksichtigt wird, für die angemessene Durchführung dieser Verordnung, für Kosteneffizienz sowie dafür zu sorgen, dass alle Mitgliedstaaten effektiven Zugang zu Sachverständigen haben müssen.

(3) Die Kommission ermöglicht den Mitgliedstaaten bei Bedarf einen rechtzeitigen Zugang zu den Sachverständigen und sorgt dafür, dass die Kombination aus unterstützenden Tätigkeiten durch die Union zur Prüfung von KI gemäß Artikel 84 und durch die Sachverständigen gemäß dem vorliegenden Artikel effizient organisiert ist und den bestmöglichen zusätzlichen Nutzen bringt.

I. Worum geht es?

Der Artikel regelt den **Zugang der Mitgliedstaaten zu einem Pool von Sachverständigen**, die im wissenschaftlichen Gremium organisiert sind. Ziel ist es, den Mitgliedstaaten bei der Durchsetzung der KI-VO fachliche Unterstützung zu geben. Die Vorschrift schafft damit eine Artikel „Expertenreserve“, auf die nationale Behörden zurückgreifen können, wenn ihnen selbst das notwendige technische oder wissenschaftliche Fachwissen fehlt. Gleichzeitig stellt die Norm sicher, dass der Zugang fair, effizient und finanziell tragbar organisiert wird.

II. Detailkommentar

A. Grundidee des Sachverständigenpools

- **Pool von Sachverständigen**: Der Artikel ermöglicht den Mitgliedstaaten, unabhängige Experten aus dem wissenschaftlichen Gremium zur Unterstützung bei der Umsetzung der KI-VO hinzuziehen.
- **Ziel**: Stärkung der nationalen Kapazitäten, insbesondere dort, wo es an technischem Detailwissen zur Bewertung von KI-Systemen fehlt.
- Es wird klargestellt, dass das Gremium unabhängig und unparteiisch arbeiten soll und die Mitglieder aufgrund ihres Fachwissens ausgewählt werden.

Beispiel: *Eine nationale Aufsichtsbehörde möchte prüfen, ob ein KI-System zur Gesichtserkennung die Anforderungen an Genauigkeit und Nichtdiskriminierung erfüllt. Da ihr eigenes Team nicht über ausreichend Fachwissen in Bildverarbeitung verfügt, zieht sie einen Experten aus dem Pool hinzu.*

B. Gebührenregelung

- **Mögliche Gebührenpflicht**: Mitgliedstaaten können verpflichtet werden, für die Inanspruchnahme der Experten eine Gebühr zu zahlen.
- **Rechtsgrundlage**: Die Details – also Höhe, Struktur und erstattungsfähige Kosten – werden durch einen Durchführungsrechtsakt nach Artikel 68 KI-VO Absatz 1 festgelegt.
- **Ziele**: Die Gebühren müssen so ausgestaltet sein, dass die Umsetzung der KI-VO praktikabel bleibt, Kosten effizient eingesetzt werden und alle Mitgliedstaaten – auch kleinere mit weniger Ressourcen – einen fairen Zugang zu den Experten haben.

C. Organisation des Zugangs

- **Verantwortung der Kommission**: Sie sorgt dafür, dass die Mitgliedstaaten rechtzeitig Zugang zu den Sachverständigen erhalten.

- **Koordination**: Die Kommission organisiert die Unterstützung so, dass diese mit anderen Unterstützungsmaßnahmen (insb nach Artikel 84 KI-VO– Prüfungen von KI-Systemen durch die Union) sinnvoll zusammenpasst.
- **Zielsetzung**: Maximierung des Nutzens durch klare Abstimmung zwischen nationaler und europäischer Ebene.

Beispiel: *Die Kommission stimmt ab, dass ein Expertenteam parallel sowohl eine nationale Untersuchung unterstützt als auch Ergebnisse für eine unionsweite Marktüberwachung liefert, um Doppelarbeit zu vermeiden.*

D. Besonderheiten

- **Unabhängigkeit der Experten**
- **Kapazitätsaufstockung**: Der Artikel ist als Ergänzung zu nationalen Strukturen gedacht, nicht als Ersatz. Nationale Behörden bleiben für die Umsetzung verantwortlich.
- **Flexibilität**: Mitgliedstaaten entscheiden selbst, ob und wann sie auf den Pool zurückgreifen.

III. Zusammenfassung

Ziel	Unterstützung der Mitgliedstaaten durch unabhängige Experten bei der Durchsetzung der KI-VO
Zugang	Mitgliedstaaten können Experten aus dem wissenschaftlichen Gremium hinzuziehen
Kosten	Gebühren können erhoben werden; Details durch Durchführungsrechtsakt (Artikel 68 KI-VO Absatz 1)
Organisation	Kommission sorgt für rechtzeitigen Zugang und effiziente Abstimmung mit anderen Unterstützungsmaßnahmen
Besonderheit	Sicherstellung der Unabhängigkeit und Fachkompetenz der Experten, fairer Zugang für alle Mitgliedstaaten

IV. Quellenverzeichnis

- Erwägungsgrund 151 KI-VO (EU) 2024/1689

Artikel 70 KI-VO

Benennung von zuständigen nationalen Behörden und zentrale Anlaufstelle

(1) Jeder Mitgliedstaat muss für die Zwecke dieser Verordnung mindestens eine notifizierende Behörde und mindestens eine Marktüberwachungsbehörde als zuständige nationale Behörden einrichten oder benennen. Diese zuständigen nationalen Behörden üben ihre Befugnisse unabhängig, unparteiisch und unvoreingenommen aus, um die Objektivität ihrer Tätigkeiten und Aufgaben zu gewährleisten und die Anwendung und Durchführung dieser Verordnung sicherzustellen. Die Mitglieder dieser Behörden haben jede Handlung zu unterlassen, die mit ihren Aufgaben unvereinbar ist. Sofern diese Grundsätze gewahrt werden, können die betreffenden Tätigkeiten und Aufgaben gemäß den organisatorischen Erfordernissen des Mitgliedstaats von einer oder mehreren benannten Behörden wahrgenommen werden.

(2) Die Mitgliedstaaten teilen der Kommission die Namen der notifizierenden Behörden und der Marktüberwachungsbehörden und die Aufgaben dieser Behörden sowie alle späteren Änderungen mit. Die Mitgliedstaaten machen Informationen darüber, wie die zuständigen Behörden und zentralen Anlaufstellen bis zum 2. August 2025 auf elektronischem Wege kontaktiert werden können, öffentlich zugänglich. Die Mitgliedstaaten benennen eine Marktüberwachungsbehörde, die als zentrale Anlaufstelle für diese Verordnung fungiert, und teilen der Kommission den Namen der zentralen Anlaufstelle mit. Die Kommission erstellt eine öffentlich verfügbare Liste der zentralen Anlaufstellen.

(3) Die Mitgliedstaaten sorgen dafür, dass ihre zuständigen nationalen Behörden mit angemessenen technischen und finanziellen Mitteln sowie geeignetem Personal und Infrastrukturen ausgestattet werden, damit sie ihre Aufgaben im Rahmen dieser Verordnung wirksam erfüllen können. Insbesondere müssen die zuständigen nationalen Behörden zu jeder Zeit über eine ausreichende Zahl von Mitarbeitern verfügen, zu deren Kompetenzen und Fachwissen ein tiefes Verständnis der KI-Technologien, der Daten und Datenverarbeitung, des Schutzes personenbezogener Daten, der Cybersicherheit, der Grundrechte, der Gesundheits- und Sicherheitsrisiken sowie Kenntnis der bestehenden Normen und rechtlichen Anforderungen gehört. Die Mitgliedstaaten bewerten und aktualisieren, falls

erforderlich, jährlich die in diesem Absatz genannten Erfordernisse bezüglich Kompetenzen und Ressourcen.

(4) Die zuständigen nationalen Behörden ergreifen geeignete Maßnahmen zur Sicherstellung eines angemessenen Maßes an Cybersicherheit.

(5) Bei der Erfüllung ihrer Aufgaben halten sich die zuständigen nationalen Behörden an die in Artikel 78 festgelegten Vertraulichkeitspflichten.

(6) Bis zum 2. August 2025 und anschließend alle zwei Jahre erstatten die Mitgliedstaaten der Kommission Bericht über den Sachstand bezüglich der finanziellen Mittel und des Personals der zuständigen nationalen Behörden und geben eine Einschätzung über deren Angemessenheit ab. Die Kommission leitet diese Informationen zur Erörterung und etwaigen Abgabe von Empfehlungen an das KI-Gremium weiter.

(7) Die Kommission fördert den Erfahrungsaustausch zwischen den zuständigen nationalen Behörden.

(8) Die zuständigen nationalen Behörden können gegebenenfalls insbesondere KMU, einschließlich Start-up-Unternehmen, unter Berücksichtigung der Anleitung und Beratung durch das KI-Gremium oder der Kommission mit Anleitung und Beratung bei der Durchführung dieser Verordnung zur Seite stehen. Wenn zuständige nationale Behörden beabsichtigen, Anleitung und Beratung in Bezug auf ein KI-System in Bereichen anzubieten, die unter das Unionrecht fallen, so sind gegebenenfalls die nach jenen Unionsrecht zuständigen nationalen Behörden zu konsultieren.

(9) Soweit Organe, Einrichtungen und sonstige Stellen der Union in den Anwendungsbereich dieser Verordnung fallen, übernimmt der Europäische Datenschutzbeauftragte die Funktion der für ihre Beaufsichtigung zuständigen Behörde.

I. Worum geht es?

Dieser Artikel legt fest, dass jeder Mitgliedstaat bestimmte nationale Behörden benennen muss, die für die Umsetzung und Überwachung der KI-VO zuständig sind. Zentral ist die Einrichtung einer **notifizierenden Behörde** (zuständig für die Benennung und Überwachung von Konformitätsbewertungsstellen) sowie einer **Marktüberwachungsbehörde** (zuständig für Kontrolle und Durchsetzung).

Zudem wird eine **zentrale Anlaufstelle** eingerichtet, um Bürgern und Unternehmen den Zugang zu erleichtern. Der Artikel regelt auch Anforderungen an Unabhängigkeit, Ausstattung, Cybersicherheit, Vertraulichkeit sowie die Berichtspflichten der Mitgliedstaaten.

II. Detailkommentar

A. Grundstruktur und Pflicht zur Benennung

- **Mindestanforderung**: Jeder Mitgliedstaat muss mindestens eine notifizierende Behörde und eine Marktüberwachungsbehörde benennen.
- **Flexibilität**: Mitgliedstaaten können frei entscheiden, welche öffentlichen Einrichtungen sie benennen, solange diese die Anforderungen erfüllen.
- **Kombinierbarkeit**: Tätigkeiten können auch durch mehrere Behörden ausgeübt werden, wenn nationale organisatorische Bedürfnisse dies erfordern.
- **Zentrale Anlaufstelle**: Eine Marktüberwachungsbehörde muss zugleich als zentrale Anlaufstelle fungieren.

Beispiel: *Ein Mitgliedstaat benennt das Wirtschaftsministerium als notifizierende Behörde und die nationale IT-Sicherheitsagentur als Marktüberwachungsbehörde. Letztere übernimmt zugleich die Rolle der zentralen Anlaufstelle.*

B. Unabhängigkeit und Objektivität

- **Unabhängigkeit**: Behörden müssen unparteiisch und objektiv handeln.
- **Pflicht zur Neutralität**: Mitglieder der Behörden dürfen keine Handlungen setzen, die ihre Unparteilichkeit gefährden könnten.
- **Verschwiegenheitspflichten**: Bezug zu Artikel 78 KI-VO, ergänzt durch Erwägungsgrund 154.

Beispiel: *Ein Mitarbeiter der Behörde darf nicht gleichzeitig für ein KI-Unternehmen arbeiten, das von der Behörde überwacht wird.*

C. Ausstattung und Ressourcen

- **Technische und finanzielle Mittel**: Mitgliedstaaten müssen sicherstellen, dass ihre Behörden über ausreichende Mittel verfügen (Absatz 3).
- **Kompetenzanforderungen**: Wissen über KI-Technologien, Datenschutz, Cybersicherheit, Grundrechte, Gesundheits- und Sicherheitsrisiken sowie Normen ist erforderlich.
- **Dynamische Anpassung**: Mitgliedstaaten müssen jährlich prüfen, ob Kompetenzen und Ressourcen noch ausreichen.

Beispiel: *Ein Staat muss regelmäßig überprüfen, ob seine Behörden genügend KI-Expertise für neuartige Modelle wie generative KI haben.*

D. Weitere Pflichten der Behörden

- **Cybersicherheit**: Behörden müssen geeignete Maßnahmen zur Sicherstellung der Cybersicherheit ergreifen.
- **Vertraulichkeit**: Verpflichtung zur Geheimhaltung gemäß Artikel 78 KI-VO.
- **Berichtspflichten**: Bis 2. August 2025, danach alle zwei Jahre, müssen Berichte zu Personal- und Finanzlage an die Kommission übermittelt werden.
- **Koordination durch die Kommission**: Förderung von Erfahrungsaustausch zwischen Behörden.
- **Beratung für Unternehmen**: Behörden können KMU und Start-ups beraten, müssen dabei aber ggf andere Behörden konsultieren, um Kompetenzkonflikte zu vermeiden.

Beispiel: *Ein Start-up entwickelt ein KI-System zur medizinischen Diagnose. Die nationale Marktüberwachungsbehörde darf beraten, muss aber die nationale Gesundheitsbehörde einbeziehen, wenn EU-Recht im Medizinbereich betroffen ist.*

E. Besonderheiten bei Unionsorganen

- **Sonderregelung**: Für EU-Organe und -Einrichtungen übernimmt der Europäische Datenschutzbeauftragte (EDSB) die Rolle der Marktüberwachungsbehörde.

Beispiel: *Wenn die Europäische Kommission ein internes KI-System einsetzt, überwacht der EDSB dessen Einhaltung der KI-VO.*

III. Zusammenfassung

Zuständige Behörden	Mindestens eine notifizierende Behörde und eine Marktüberwachungsbehörde je Mitgliedstaat
Zentrale Anlaufstelle	Eine Marktüberwachungsbehörde fungiert als zentrale Anlaufstelle
Unabhängigkeit	Objektivität, Unparteilichkeit, Vertraulichkeit verpflichtend
Ausstattung	Finanzielle Mittel, Fachpersonal, Infrastruktur, jährliche Überprüfung
Pflichten	Cybersicherheit, Berichterstattung, Erfahrungsaustausch, Beratung von KMU
Sonderregel	EDSB überwacht die Anwendung der KI-VO in EU-Organen

IV. Quellenverzeichnis

- Erwägungsgründe 153, 154, 156, 157 KI-VO (EU) 2024/1689

Artikel 71 KI-VO

EU-Datenbank für die in Anhang III aufgeführten Hochrisiko-KI-Systeme

(1) Die Kommission errichtet und führt in Zusammenarbeit mit den Mitgliedstaaten eine EU-Datenbank mit den in den Absätzen 2 und 3 dieses Artikels genannten Informationen über Hochrisiko-KI-Systeme nach Artikel 6 Absatz 2, die gemäß den Artikeln 49 und 60 registriert werden und über KI-Systeme, die nicht als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 3 gelten und gemäß Artikel 6 Absatz 4 und Artikel 49 registriert werden. Bei der Festlegung der Funktionsspezifikationen dieser Datenbank konsultiert die Kommission die einschlägigen Sachverständigen und bei der Aktualisierung der Funktionsspezifikationen dieser Datenbank konsultiert sie das KI-Gremium.

(2) Die in Anhang VIII Abschnitte A und B aufgeführten Daten werden vom Anbieter oder gegebenenfalls vom Bevollmächtigten in die EU-Datenbank eingegeben.

(3) Die in Anhang VIII Abschnitt C aufgeführten Daten werden vom Betreiber, der eine Behörde, Einrichtung oder sonstige Stelle ist oder in deren Namen handelt, gemäß Artikel 49 Absätze 3 und 4 in die EU-Datenbank eingegeben.

(4) Mit Ausnahme des in Artikel 49 Absatz 4 und Artikel 60 Absatz 4 Buchstabe c genannten Abschnitts müssen die gemäß Artikel 49 in der Datenbank registrierten und dort enthaltenen Informationen auf benutzerfreundliche Weise zugänglich und öffentlich verfügbar sein. Die Informationen sollten leicht handhabbar und maschinenlesbar sein. Auf die gemäß Artikel 60 registrierten Informationen können nur Marktüberwachungsbehörden und die Kommission zugreifen, es sei denn, der zukünftige Anbieter oder der Anbieter hat seine Zustimmung dafür erteilt, dass die Informationen auch öffentlich zugänglich sind.

(5) Die EU-Datenbank enthält personenbezogene Daten nur, soweit dies für die Erfassung und Verarbeitung von Informationen gemäß dieser Verordnung erforderlich ist. Zu diesen Informationen gehören die Namen und Kontaktdaten der natürlichen Personen, die für die Registrierung des Systems verantwortlich sind und die rechtlich befugt sind, den Anbieter oder gegebenenfalls den Betreiber zu vertreten.

(6) Die Kommission gilt als für die EU-Datenbank Verantwortlicher. Sie stellt Anbietern, zukünftigen Anbietern und Betreibern angemessene technische und administrative Unterstützung bereit. Die EU-Datenbank muss den geltenden Barrierefreiheitsanforderungen entsprechen.

I. Worum geht es?

Artikel 71 regelt die Einrichtung und Führung einer EU-Datenbank für Hochrisiko-KI-Systeme. Diese Datenbank soll Transparenz schaffen, die Marktüberwachung erleichtern und sowohl der Öffentlichkeit als auch den Behörden den Zugang zu wichtigen Informationen ermöglichen. Anbieter und bestimmte Betreiber müssen ihre Systeme dort registrieren. Dabei wird zwischen öffentlich zugänglichen und nicht-öffentlichen Bereichen unterschieden.

II. Detailkommentar

A. Einrichtung und Verwaltung der Datenbank

- **Verantwortung der Kommission**: Die Kommission richtet die Datenbank ein und führt sie in Zusammenarbeit mit den Mitgliedstaaten.
- **Technische Spezifikationen**: Vor Festlegung und Aktualisierung werden Sachverständige bzw. das KI-Gremium konsultiert.
- **Datenschutz und Barrierefreiheit**: Die Datenbank muss die geltenden Datenschutzvorschriften und Barrierefreiheitsanforderungen erfüllen.

Beispiel: *Ein Anbieter entwickelt ein KI-System zur Bewerberauswahl. Vor dem Einsatz muss er dieses in die Datenbank eintragen. Die Datenbank muss so gestaltet sein, dass auch Menschen mit Sehbehinderung Zugang haben.*

B. Registrierungspflichten

1. Anbieterpflichten

- Anbieter oder Bevollmächtigte geben die in Anhang VIII KI-VO Abschnitte A und B genannten Daten ein.

- Dies betrifft Hochrisiko-KI-Systeme nach Artikel 6 KI-VOAbsatz 2 sowie Systeme, die unter Ausnahmen nach Artikel 6 Absatz 3 fallen und nach Artikel 6 Absatz 4 und Artikel 49 KI-VOregistriert werden.

2. Betreiberpflichten

- Betreiber, die Behörden, Einrichtungen oder sonstige Stellen sind, müssen bestimmte Daten (Anhang VIII KI-VO Abschnitt C) eintragen.
- Dies gilt insbesondere, wenn sie ein Hochrisiko-KI-System einsetzen wollen.

Beispiel: *Eine Arbeitsagentur plant, ein KI-System zur Jobvermittlung einzusetzen. Sie muss ihre Nutzung des Systems zusätzlich in der Datenbank registrieren.*

C. Öffentlich zugängliche und nicht-öffentliche Informationen

- **Öffentlichkeit**: Grundsätzlich sind die registrierten Informationen für jedermann leicht zugänglich, benutzerfreundlich und maschinenlesbar.
- **Ausnahmen**: Für sensible Bereiche (zB Strafverfolgung, Migration, Asyl) gibt es geschützte, nicht-öffentliche Teile. Zugriff nur für Marktüberwachungsbehörden und die Kommission.
- **Freiwillige Freigabe**: Anbieter können zusätzliche Informationen freiwillig öffentlich machen.

Beispiel: *Ein Hersteller gibt bewusst zusätzliche Informationen zu seinem KI-System preis, um Vertrauen in seine Transparenz zu stärken.*

D. Artikel der gespeicherten Daten

- **Personenbezogene Daten**: Nur soweit erforderlich, zB Name und Kontaktdaten der für die Registrierung verantwortlichen Personen.
- **Inhaltliche Angaben**: Angaben zu den Funktionen, Risiken und Einsatzbereichen des KI-Systems.

- **Aktualisierungspflicht**: Jede wesentliche Veränderung eines Hochrisiko-KI-Systems ist erneut zu registrieren.

E. Besondere Aspekte

- **Sicherheitsanforderungen**: Berücksichtigung von Cybersicherheitsrisiken.
- **Kritische Infrastrukturen**: Registrierung erfolgt nur auf nationaler Ebene.

III. Zusammenfassung

Einrichtung	Kommission baut und verwaltet die EU-Datenbank für Hochrisiko-KI-Systeme.
Registrierung	Anbieter und bestimmte Betreiber müssen ihre Systeme registrieren.
Öffentlichkeit	Grundsätzlich sind Daten öffentlich zugänglich; Ausnahme für sensible Systeme.
Datenschutz	Nur notwendige personenbezogene Daten werden gespeichert.
Besonderheiten	Cybersicherheit, Barrierefreiheit, nationale Registrierung für kritische Infrastrukturen.

IV. Quellenverzeichnis

- Erwägungsgrund 131 KI-VO (EU) 2024/1689

Artikel 72 KI-VO

Beobachtung nach dem Inverkehrbringen durch die Anbieter und Plan für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme

(1) Anbieter müssen ein System zur Beobachtung nach dem Inverkehrbringen, das im Verhältnis zur Artikel der KI-Technik und zu den Risiken des Hochrisiko-KI-Systems steht, einrichten und dokumentieren.

(2) Mit dem System zur Beobachtung nach dem Inverkehrbringen müssen sich die einschlägigen Daten zur Leistung der Hochrisiko-KI-Systeme, die von den Anbietern oder den Betreibern bereitgestellt oder aus anderen Quellen erhoben werden können, über ihre gesamte Lebensdauer hinweg aktiv und systematisch erheben, dokumentieren und analysieren lassen, und der Anbieter muss damit die fortdauernde Einhaltung der in Kapitel III Abschnitt 2 genannten Anforderungen an die KI-Systeme bewerten können. Gegebenenfalls umfasst die Beobachtung nach dem Inverkehrbringen eine Analyse der Interaktion mit anderen KI-Systemen. Diese Pflicht gilt nicht für sensible operative Daten von Betreibern, die Strafverfolgungsbehörden sind.

(3) Das System zur Beobachtung nach dem Inverkehrbringen muss auf einem Plan für die Beobachtung nach dem Inverkehrbringen beruhen. Der Plan für die Beobachtung nach dem Inverkehrbringen ist Teil der in Anhang IV genannten technischen Dokumentation. Die Kommission erlässt einen Durchführungsrechtsakt, in dem sie detaillierte Bestimmungen für die Erstellung eines Musters des Plans für die Beobachtung nach dem Inverkehrbringen sowie die Liste der in den Plan aufzunehmenden Elemente bis zum 2. Februar 2026 detailliert festlegt. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(4) Bei Hochrisiko-KI-Systemen, die unter die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, und für die auf der Grundlage dieser Rechtvorschriften bereits ein System zur Beobachtung nach dem Inverkehrbringen sowie ein entsprechender Plan festgelegt wurden, haben die Anbieter zur Gewährleistung der Kohärenz, zur Vermeidung von Doppelarbeit und zur Minimierung zusätzlicher Belastungen die Möglichkeit, unter Verwendung des Musters nach Absatz 3, gegebenenfalls die in den Absätzen 1, 2 und 3 genannten erforderlichen Elemente in die im Rahmen dieser Vorschriften bereits vorhandenen Systeme und Pläne zu integrieren, sofern ein gleichwertiges Schutzniveau erreicht wird.

Unterabsatz 1 dieses Absatzes gilt auch für in Anhang III Nummer 5 genannte Hochrisiko-KI-Systeme, die von Finanzinstituten in Verkehr gebracht oder in Betrieb genommen wurden, die bezüglich ihrer internen Unternehmensführung, Regelungen oder Verfahren Anforderungen gemäß den Rechtsvorschriften der Union über Finanzdienstleistungen unterliegen.

Worum geht es?

Artikel 72 verpflichtet Anbieter von Hochrisiko-KI-Systemen, ihre Produkte auch nach dem Inverkehrbringen systematisch zu überwachen. Damit soll sichergestellt werden, dass die Systeme dauerhaft den gesetzlichen Anforderungen entsprechen und Risiken frühzeitig erkannt werden. Zentrales Instrument ist ein Beobachtungsplan, der Teil der technischen Dokumentation ist.

II. Detailkommentar

A. Pflicht zur Beobachtung nach dem Inverkehrbringen

- **Systempflicht**: Anbieter müssen ein System zur Beobachtung nach dem Inverkehrbringen einrichten.
- **Verhältnismäßigkeit**: Das System muss zur Artikel der KI-Technik und den spezifischen Risiken passen.
- **Ziel**: Risiken im Betrieb erkennen, Nachbesserungen ermöglichen und Compliance sicherstellen.

Beispiel: *Ein Anbieter von KI-gestützter Kreditwürdigkeitsprüfung muss regelmäßig prüfen, ob das System diskriminierungsfrei funktioniert*.

B. Inhalt und Umfang der Beobachtung

- **Datenbasis**: Anbieter müssen relevante Leistungsdaten sammeln – sowohl eigene Daten, Daten der Betreiber als auch externe Quellen.
- **Aktiv und systematisch**: Die Erhebung darf nicht zufällig erfolgen, sondern muss planvoll sein.

- **Analysepflicht**: Daten sind zu dokumentieren und zu bewerten, um die fortdauernde Einhaltung der Anforderungen (Kapitel III Abschnitt 2) zu überprüfen.
- **Interaktion mit anderen Systemen**: Wenn nötig, ist auch die Zusammenarbeit mit anderen KI-Systemen zu analysieren.
- **Ausnahme**: Keine Pflicht zur Auswertung sensibler Daten von Strafverfolgungsbehörden.

Beispiel: *Ein medizinisches Diagnose-KI-System muss laufend überprüft werden, ob neue Daten aus der Praxis die Genauigkeit verändern.*

C. Plan für die Beobachtung

- **Dokumentationspflicht**: Das Beobachtungssystem muss auf einem Plan beruhen.
- **Technische Dokumentation**: Dieser Plan ist Teil der Unterlagen nach Anhang IV KI-VO.
- **Kommende Muster**: Die Kommission erstellt bis Februar 2026 ein verbindliches Muster sowie eine Liste von Mindestinhalten.

Beispiel: *Der Plan könnte vorschreiben, in welchen Abständen Nutzerdaten ausgewertet und mit Referenzwerten abgeglichen werden.*

D. Integration bestehender Systeme

- **Harmonisierte Vorschriften**: Für KI-Systeme, die bereits unter bestehende Harmonisierungsrechtsakte fallen, können bestehende Beobachtungspläne genutzt und erweitert werden.
- **Finanzinstitute**: Gleiches gilt für Banken und Versicherungen, die ohnehin strengen Regeln zur Unternehmensführung unterliegen.
- **Ziel**: Vermeidung von Doppelarbeit und unnötiger Bürokratie.

Beispiel: *Eine Bank mit internen Risikomanagement-Systemen kann diese für die KI-VO anpassen, statt ein paralleles neues System aufzubauen.*

E. Besonderheiten und Kontext

- **Sinn und Zweck**: Beobachtung dient dem Schutz vor neuen Risiken, die erst im laufenden Betrieb auftreten.
- **Zusammenhang zu Meldungspflichten**: Eng verknüpft mit Artikel 73 KI-VO (Meldung schwerwiegender Vorfälle).
- Es wird betont, dass Erfahrungen im Betrieb direkt in die Weiterentwicklung der Systeme einfließen sollen. Erwägungsgrund 158 stellt klar, dass es für Finanzinstitute eine enge Verzahnung mit bestehenden Aufsichtssystemen gibt.

III. Zusammenfassung

Systempflicht	Anbieter müssen ein Beobachtungssystem einrichten
Datenanalyse	Aktive, systematische Datenerhebung und Bewertung
Beobachtungsplan	Teil der technischen Dokumentation, Muster durch EU-Kommission
Integration	Nutzung bestehender Systeme in harmonisierten Bereichen und Finanzwesen

IV. Quellenverzeichnis

- Erwägungsgründe 155, 158 KI-VO (EU) 2024/1689

Artikel 73 KI-VO

Meldung schwerwiegender Vorfälle

(1) Anbieter von in der Union in Verkehr gebrachten Hochrisiko-KI-Systemen melden schwerwiegende Vorfälle den Marktüberwachungsbehörden der Mitgliedstaaten, in denen der Vorfall stattgefunden hat.

(2) Die Meldung nach Absatz 1 erfolgt unmittelbar, nachdem der Anbieter den kausalen Zusammenhang zwischen dem KI-System und dem schwerwiegenden Vorfall oder die naheliegende Wahrscheinlichkeit eines solchen Zusammenhangs festgestellt hat und in jedem Fall spätestens 15 Tage, nachdem der Anbieter oder gegebenenfalls der Betreiber Kenntnis von diesem schwerwiegenden Vorfall erlangt hat.

Bezüglich des in Unterabsatz 1 genannten Meldezeitraums wird der Schwere des schwerwiegenden Vorfalls Rechnung getragen.

(3) Ungeachtet des Absatzes 2 dieses Artikels erfolgt die in Absatz 1 dieses Artikels genannte Meldung im Falle eines weitverbreiteten Verstoßes oder eines schwerwiegenden Vorfalls im Sinne des Artikels 3 Nummer 49 Buchstabe b unverzüglich, spätestens jedoch zwei Tage nachdem der Anbieter oder gegebenenfalls der Betreiber von diesem Vorfall Kenntnis erlangt hat.

(4) Ungeachtet des Absatzes 2 erfolgt die Meldung im Falle des Todes einer Person unverzüglich nachdem der Anbieter oder der Betreiber einen kausalen Zusammenhang zwischen dem Hochrisiko-KI-System und dem schwerwiegenden Vorfall festgestellt hat, oder einen solchen vermutet, spätestens jedoch zehn Tage nach dem Datum, an dem der Anbieter oder gegebenenfalls der Betreiber von dem schwerwiegenden Vorfall Kenntnis erlangt hat.

(5) Wenn es zur Gewährleistung der rechtzeitigen Meldung erforderlich ist, kann der Anbieter oder gegebenenfalls der Betreiber einen unvollständigen Erstbericht vorlegen, dem ein vollständiger Bericht folgt.

(6) Im Anschluss an die Meldung eines schwerwiegenden Vorfalls gemäß Absatz 1 führt der Anbieter unverzüglich die erforderlichen Untersuchungen im Zusammenhang mit dem schwerwiegenden Vorfall und dem betroffenen KI-System durch. Dies umfasst eine Risikobewertung des Vorfalls sowie Korrekturmaßnahmen.

Der Anbieter arbeitet bei den Untersuchungen gemäß Unterabsatz 1 mit den zuständigen Behörden und gegebenenfalls mit der betroffenen notifizierten Stelle zusammen und nimmt keine Untersuchung vor, die zu einer Veränderung des betroffenen KI-Systems in einer Weise führt, die möglicherweise Auswirkungen auf eine spätere Bewertung der Ursachen des Vorfalls hat, bevor er die zuständigen Behörden über eine solche Maßnahme nicht unterrichtet hat.

(7) Sobald die zuständige Marktüberwachungsbehörde eine Meldung über einen in Artikel 3 Nummer 49 Buchstabe c genannten schwerwiegenden Vorfall erhält, informiert sie die in Artikel 77 Absatz 1 genannten nationalen Behörden oder öffentlichen Stellen. Zur leichteren Einhaltung der Pflichten nach Absatz 1 dieses Artikels arbeitet die Kommission entsprechende Leitlinien aus. Diese Leitlinien werden bis zum 2. August 2025 veröffentlicht und regelmäßig bewertet.

(8) Die Marktüberwachungsbehörde ergreift innerhalb von sieben Tagen nach Eingang der in Absatz 1 dieses Artikels genannten Meldung geeignete Maßnahmen gemäß Artikel 19 der Verordnung (EU) 2019/1020 und befolgt die in der genannten Verordnung vorgesehenen Meldeverfahren.

(9) Bei Hochrisiko-KI-Systemen nach Anhang III, die von Anbietern in Verkehr gebracht oder in Betrieb genommen wurden, die Rechtsinstrumenten der Union mit gleichwertigen Meldepflichten wie jenen in dieser Verordnung festgesetzten unterliegen, müssen nur jene schwerwiegenden Vorfälle gemeldet werden, die in Artikel 3 Nummer 49 Buchstabe c genannt werden.

(10) Bei Hochrisiko-KI-Systemen, bei denen es sich um Sicherheitsbauteile von Produkten handelt, die unter die Verordnungen (EU) 2017/745 und (EU) 2017/746 fallen, oder die selbst solche Produkte sind, müssen nur die in Artikel 3 Nummer 49 Buchstabe c dieser Verordnung genannten schwerwiegenden Vorfälle gemeldet werden, und zwar der zuständigen nationalen Behörde, die für diesen Zweck von den Mitgliedstaaten, in denen der Vorfall stattgefunden hat, ausgewählt wurde.

(11) Die zuständigen nationalen Behörden melden der Kommission unverzüglich jeden schwerwiegenden Vorfall gemäß Artikel 20 der Verordnung (EU) 2019/1020, unabhängig davon, ob sie diesbezüglich Maßnahmen ergriffen haben.

I. Worum geht es?

Artikel 73 verpflichtet Anbieter von Hochrisiko-KI-Systemen, schwerwiegende Vorfälle den zuständigen Marktüberwachungsbehörden zu melden. Die Norm stellt sicher, dass Risiken früh erkannt und Schäden begrenzt werden. So wird ein effektiver Schutz von Gesundheit, Sicherheit und Grundrechten gewährleistet.

II. Detailkommentar

A. Meldepflichtige Akteure

- **Anbieter**: Hauptverantwortlich für Meldungen sind die Anbieter von Hochrisiko-KI-Systemen, die in der EU in Verkehr gebracht wurden.
- **Betreiber**: Kann ebenfalls meldepflichtig sein, wenn er zuerst Kenntnis vom Vorfall hat.

B. Meldegegenstand

- **Schwerwiegende Vorfälle**: Definiert in Artikel 3 KI-VO Nr 49, zB Todesfälle, schwere Gesundheitsschäden, gravierende Störungen kritischer Infrastrukturen, schwere Sach- oder Umweltschäden oder Verstöße gegen Grundrechte.

Beispiel: *Ein KI-gestütztes Diagnosegerät übersieht eine akute Krankheit, was zu einem tödlichen Behandlungsfehler führt.*

C. Fristen

- **Allgemein**: Unverzüglich nach Feststellung des Zusammenhangs, spätestens 15 Tage nach Kenntnis.
- Weitverbreitete Verstöße / Grundrechtsverletzungen: Meldung spätestens nach zwei Tagen.
- **Todesfälle**: Meldung unverzüglich, spätestens zehn Tage.
- **Flexibilität**: Erst unvollständiger Bericht möglich, später Ergänzung.

Beispiel: *Ein Kredit-Scoring-KI-System diskriminiert ganze Bevölkerungsgruppen. Da es sich um eine Grundrechtsverletzung handelt, ist die Meldung binnen zwei Tagen nötig.*

D. Untersuchungspflichten

- **Analyse**: Anbieter müssen den Vorfall untersuchen, Risiken bewerten und Korrekturmaßnahmen ergreifen.
- **Zusammenarbeit**: Pflicht zur Kooperation mit Behörden und ggf notifizierten Stellen.
- **Beweissicherung**: Änderungen am System, die Ursachenanalyse erschweren könnten, nur nach Mitteilung an Behörden.

E. Rolle der Behörden

- **Marktüberwachungsbehörden**: Reagieren binnen sieben Tagen nach Meldung mit geeigneten Maßnahmen.
- **Nationale Behörden**: Werden bei bestimmten Vorfällen informiert und melden an die Kommission.
- **Koordination**: Durch Verweis auf Verordnung (EU) 2019/1020 wird ein einheitliches Verfahren gesichert.

F. Sonderregeln

- **Andere EU-Rechtsakte**: Wenn bereits gleichwertige Meldepflichten bestehen, müssen nur Grundrechtsverletzungen gemeldet werden.
- **Medizinprodukte**: Für KI-Systeme nach den Medizinprodukte-Verordnungen gelten reduzierte Meldepflichten an spezielle nationale Behörden.

Beispiel: *Ein KI-Medizinprodukt fällt unter die VO (EU) 2017/745. Es muss nur Grundrechtsverletzungen nach Artikel 3 Nr 49 lit c melden.*

III. Zusammenfassung

Wer muss melden?	Anbieter, ggf Betreiber
Was ist zu melden?	Schwerwiegende Vorfälle nach Artikel 3 KI-VO Nr 49
Fristen	Allgemein: 15 Tage; Grundrechtsverstöße: zwei Tage; Todesfälle: zehn Tage
Bericht	Zunächst unvollständig möglich, später vollständig
Nach der Meldung	Untersuchungspflicht, Zusammenarbeit mit Behörden
Behörden	Marktüberwachungsbehörden handeln binnen 7siebenTagen, nationale Stellen informieren Kommission
Besonderheiten	Vereinfachungen bei Überschneidung mit anderen EU-Regelungen (zB Medizinprodukte)

IV. Quellenverzeichnis

- Erwägungsgründe 155, 157 KI-VO (EU) 2024/1689

Artikel 74 KI-VO

Marktüberwachung und Kontrolle von KI-Systemen auf dem Unionsmarkt

(1) Die Verordnung (EU) 2019/1020 gilt für KI-Systeme, die unter die vorliegende Verordnung fallen. Für die Zwecke einer wirksamen Durchsetzung der vorliegenden Verordnung gilt Folgendes:

a) Jede Bezugnahme auf einen Wirtschaftsakteur nach der Verordnung (EU) 2019/1020 gilt auch als Bezugnahme auf alle Akteure, die in Artikel 2 Absatz 1 der vorliegenden Verordnung genannt werden;

b) jede Bezugnahme auf ein Produkt nach der Verordnung (EU) 2019/1020 gilt auch als Bezugnahme auf alle KI-Systeme, die in den Anwendungsbereich der vorliegenden Verordnung fallen.

(2) Im Rahmen ihrer Berichtspflichten gemäß Artikel 34 Absatz 4 der Verordnung (EU) 2019/1020 melden die Marktüberwachungsbehörden der Kommission und den einschlägigen nationalen Wettbewerbsbehörden jährlich alle Informationen, die sie im Verlauf ihrer Marktüberwachungstätigkeiten erlangt haben und die für die Anwendung von Unionsrecht im Bereich der Wettbewerbsregeln von Interesse sein könnten. Ferner erstatten sie der Kommission jährlich Bericht über die Anwendung verbotener Praktiken in dem betreffenden Jahr und über die ergriffenen Maßnahmen.

(3) Bei Hochrisiko-KI-Systemen und damit in Zusammenhang stehenden Produkten, auf die die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union Anwendung finden, gilt als Marktüberwachungsbehörde für die Zwecke dieser Verordnung die in jenen Rechtsakten für die Marktüberwachung benannte Behörde.

Abweichend von Unterabsatz 1 und unter geeigneten Umständen können die Mitgliedstaaten eine andere einschlägige Behörde benennen, die die Funktion der Marktüberwachungsbehörde übernimmt, sofern sie die Koordinierung mit den einschlägigen sektorspezifischen Marktüberwachungsbehörden, die für die Durchsetzung der in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union zuständig sind, sicherstellen.

(4) Die Verfahren gemäß den Artikeln 79 bis 83 der vorliegenden Verordnung gelten nicht für KI-Systeme, die im Zusammenhang mit

Produkten stehen, auf die die in Anhang I Abschnitt A aufgeführten Harmonisierungsrechtsvorschriften der Union Anwendung finden, wenn in diesen Rechtsakten bereits Verfahren, die ein gleichwertiges Schutzniveau sicherstellen und dasselbe Ziel haben, vorgesehen sind. In diesen Fällen kommen stattdessen die einschlägigen sektorspezifischen Verfahren zur Anwendung.

(5) Unbeschadet der Befugnisse der Marktüberwachungsbehörden gemäß Artikel 14 der Verordnung (EU) 2019/1020 können die Marktüberwachungsbehörden für die Zwecke der Sicherstellung der wirksamen Durchsetzung der vorliegenden Verordnung die in Artikel 14 Absatz 4 Buchstaben d und j der genannten Verordnung genannten Befugnisse gegebenenfalls aus der Ferne ausüben.

(6) Bei Hochrisiko-KI-Systemen, die von auf der Grundlage des Unionsrechts im Bereich der Finanzdienstleistungen regulierten Finanzinstituten in Verkehr gebracht, in Betrieb genommen oder verwendet werden, gilt die in jenen Rechtsvorschriften für die Finanzaufsicht über diese Institute benannte nationale Behörde als Marktüberwachungsbehörde für die Zwecke dieser Verordnung, sofern das Inverkehrbringen, die Inbetriebnahme oder die Verwendung des KI-Systems mit der Erbringung dieser Finanzdienstleistungen in direktem Zusammenhang steht.

(7) Abweichend von Absatz 6 kann der Mitgliedstaat — unter geeigneten Umständen und wenn für Abstimmung gesorgt ist — eine andere einschlägige Behörde als Marktüberwachungsbehörde für die Zwecke dieser Verordnung benennen.

Nationale Marktüberwachungsbehörden, die unter die Richtlinie 2013/36/EU fallende Kreditinstitute, welche an dem mit der Verordnung (EU) Nr 1024/2013 eingerichteten einheitlichen Aufsichtsmechanismus teilnehmen, beaufsichtigen, sollten der Europäischen Zentralbank unverzüglich alle im Zuge ihrer Marktüberwachungstätigkeiten ermittelten Informationen übermitteln, die für die in der genannten Verordnung festgelegten Aufsichtsaufgaben der Europäischen Zentralbank von Belang sein könnten.

(8) Für die in Anhang III Nummer 1 der vorliegenden Verordnung genannten Hochrisiko-KI-Systeme, sofern diese Systeme für Strafverfolgungszwecke, Grenzmanagement und Justiz und Demokratie eingesetzt werden, und für die in Anhang III Nummern 6, 7 und 8 genannten Hochrisiko-KI-Systeme benennen die Mitgliedstaaten für die Zwecke dieser

Verordnung als Marktüberwachungsbehörden entweder die nach der Verordnung (EU) 2016/679 oder der Richtlinie (EU) 2016/680 für den Datenschutz zuständigen Aufsichtsbehörden oder jede andere gemäß denselben Bedingungen wie den in den Artikeln 41 bis 44 der Richtlinie (EU) 2016/680 festgelegten benannte Behörde. Marktüberwachungstätigkeiten dürfen in keiner Weise die Unabhängigkeit von Justizbehörden beeinträchtigen oder deren Handlungen im Rahmen ihrer justiziellen Tätigkeit anderweitig beeinflussen.

(9) Soweit Organe, Einrichtungen und sonstige Stellen der Union in den Anwendungsbereich dieser Verordnung fallen, übernimmt der Europäische Datenschutzbeauftragte die Funktion der für sie zuständigen Marktüberwachungsbehörde — ausgenommen für den Gerichtshof der Europäischen Union im Rahmen seiner Rechtsprechungstätigkeit.

(10) Die Mitgliedstaaten erleichtern die Koordinierung zwischen den auf der Grundlage dieser Verordnung benannten Marktüberwachungsbehörden und anderen einschlägigen nationalen Behörden oder Stellen, die die Anwendung der in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union oder sonstigen Unionsrechts überwachen, das für die in Anhang III genannten Hochrisiko-KI-Systeme relevant sein könnte.

(11) Die Marktüberwachungsbehörden und die Kommission können gemeinsame Tätigkeiten, einschließlich gemeinsamer Untersuchungen, vorschlagen, die von den Marktüberwachungsbehörden oder von den Marktüberwachungsbehörden gemeinsam mit der Kommission durchgeführt werden, um Konformität zu fördern, Nichtkonformität festzustellen, zu sensibilisieren oder Orientierung zu dieser Verordnung und bestimmten Kategorien von Hochrisiko-KI-Systemen, bei denen festgestellt wird, dass sie in zwei oder mehr Mitgliedstaaten gemäß Artikel 9 der Verordnung (EU) 2019/1020 ein ernstes Risiko darstellen, zu geben. Das Büro für Künstliche Intelligenz unterstützt die Koordinierung der gemeinsamen Untersuchungen.

(12) Die Anbieter gewähren den Marktüberwachungsbehörden unbeschadet der Befugnisübertragung gemäß der Verordnung (EU) 2019/1020 — sofern dies relevant ist und beschränkt auf das zur Wahrnehmung der Aufgaben dieser Behörden erforderliche Maß — uneingeschränkten Zugang zur Dokumentation sowie zu den für die Entwicklung von Hochrisiko-KI-Systemen verwendeten Trainings-,

Validierungs- und Testdatensätzen, gegebenenfalls und unter Einhaltung von Sicherheitsvorkehrungen auch über die Anwendungsprogrammierschnittstellen (im Folgenden „API“) oder andere einschlägige technische Mittel und Instrumente, die den Fernzugriff ermöglichen.

(13) Zum Quellcode des Hochrisiko-KI-Systems erhalten Marktüberwachungsbehörden auf begründete Anfrage und nur dann Zugang, wenn die beiden folgenden Bedingungen erfüllt sind:

a) Der Zugang zum Quellcode ist zur Bewertung der Konformität eines Hochrisiko-KI-Systems mit den in Kapitel III Abschnitt 2 festgelegten Anforderungen notwendig und

b) die Test- oder Prüfverfahren und Überprüfungen aufgrund der vom Anbieter bereitgestellten Daten und Dokumentation wurden ausgeschöpft oder haben sich als unzureichend erwiesen.

(14) Jegliche Informationen oder Dokumentation, in deren Besitz die Marktüberwachungsbehörden gelangen, werden im Einklang mit den in Artikel 78 festgelegten Vertraulichkeitspflichten behandelt.

I. Worum geht es?

Artikel 74 regelt die Marktüberwachung und Kontrolle von KI-Systemen auf dem Unionsmarkt. Ziel ist es, eine wirksame Durchsetzung der KI-VO sicherzustellen, indem die bestehenden Strukturen der EU-Marktüberwachungsverordnung (EU) 2019/1020 genutzt und auf KI-Systeme ausgeweitet werden. Besondere Regeln gelten für Hochrisiko-KI-Systeme, insbesondere in den Bereichen Finanzdienstleistungen, Strafverfolgung, Justiz und biometrische Daten.

II. Detailkommentar

A. Grundsatz: Anwendbarkeit der Verordnung (EU) 2019/1020

- **Einbeziehung bestehender Regeln**: Die Marktüberwachung der KI-VO erfolgt grundsätzlich nach den Mechanismen der Verordnung (EU) 2019/1020 (sog Marktüberwachungsverordnung).

■■■**Auch Bulletpoint?**■■■**Wirtschaftsakteure und Produkte**: Alle Akteure der KI-VO (zB Anbieter, Importeure, Nutzer) gelten als „Wirtschaftsakteure"; KI-Systeme gelten als „Produkte" im Sinne der Marktüberwachungsverordnung.

B. Berichtspflichten der Marktüberwachungsbehörden

- **Jährliche Berichte**: Behörden melden der Kommission und Wettbewerbsbehörden relevante Informationen, zB zu verbotenen Praktiken oder Risiken.
- **Verknüpfung mit Wettbewerbsrecht**: Auch wettbewerbsrechtlich relevante Daten werden weitergeleitet.

Beispiel: *Eine Behörde entdeckt, dass mehrere Anbieter Preisabsprachen bei KI-Software getroffen haben. Diese Informationen werden an Wettbewerbsbehörden gemeldet.*

C. Zuständigkeit der Marktüberwachungsbehörden

1. **Grundsatz**: Für Hochrisiko-KI-Systeme gelten die in Anhang I KI-VO Abschnitt A genannten sektoralen Behörden.
2. **Abweichungsmöglichkeit**: Mitgliedstaaten können andere Behörden benennen, müssen aber Koordination sicherstellen.
3. **Finanzsektor**: Bei Finanzinstituten gelten die bestehenden Finanzaufsichtsbehörden als Marktüberwachungsbehörden (zB BaFin in Deutschland).
4. **Strafverfolgung, Justiz und Demokratie**: Hier sind Datenschutzbehörden oder vergleichbare Stellen zuständig; richterliche Unabhängigkeit bleibt unberührt.
5. **EU-Organe**: Für EU-Organe ist der Europäische Datenschutzbeauftragte zuständig (mit Ausnahme des EuGH).

Beispiel: *Ein Hochrisiko-KI-System wird in einem Strafverfahren eingesetzt. Die Datenschutzbehörde überwacht dessen Rechtmäßigkeit, ohne die richterliche Entscheidungshoheit zu beeinträchtigen.*

D. Verfahren und Befugnisse

- **Ausnahme bei Doppelregelungen**: Wenn andere Unionsrechtsakte gleichwertige Verfahren vorsehen, gelten diese statt der KI-VO-Verfahren.
- **Fernmaßnahmen**: Marktüberwachungsbehörden können bestimmte Befugnisse auch aus der Ferne ausüben.
- **Gemeinsame Untersuchungen**: Marktüberwachungsbehörden und Kommission können zusammenarbeiten, unterstützt vom Büro für Künstliche Intelligenz.
- **Zugangsbefugnisse**: Behörden erhalten Zugang zu Dokumentation, Daten und ggf Quellcode, allerdings nur bei klarer Notwendigkeit und nach Ausschöpfung anderer Mittel.

Beispiel: *Eine Behörde verlangt Einsicht in Trainingsdaten eines KI-Systems zur Gesichtserkennung, um dessen Konformität zu prüfen. Auf den Quellcode darf sie nur zugreifen, wenn die Dokumentation nicht ausreicht.*

E. Besondere Schutzmechanismen

- **Unabhängigkeit**: Marktüberwachung darf die Unabhängigkeit von Justiz oder Aufsichtsorganen nicht beeinträchtigen.
- **Datenschutz**: Datenschutzbehörden behalten ihre Befugnisse, insbesondere im Bereich biometrischer Daten.
- **Vertraulichkeit**: Alle erlangten Informationen unterliegen den Vertraulichkeitsregeln nach Artikel 78 KI-VO.

III. Zusammenfassung

Grundlage	Anwendung der Marktüberwachungsverordnung (EU) 2019/1020 auf KI-Systeme
Akteure und Produkte	KI-Anbieter/Nutzer = Wirtschaftsakteure; KI-Systeme = Produkte

Zuständigkeit	Sektorale Behörden; bei Finanzsektor Finanzaufsicht; bei Justiz/Strafverfolgung Datenschutzbehörden; für EU-Organe EDPS
Verfahren	Vorrang sektoraler Verfahren, Fernmaßnahmen möglich, gemeinsame Untersuchungen
Befugnisse	Zugang zu Dokumentation, Daten, ggf Quellcode bei Notwendigkeit
Schutzmechanismen	Wahrung von Unabhängigkeit, Datenschutz, Vertraulichkeit

IV. Quellenverzeichnis

- Erwägungsgründe 156-160 KI-VO (EU) 2024/1689

Artikel 75 KI-VO

Amtshilfe, Marktüberwachung und Kontrolle von KI-Systemen mit allgemeinem Verwendungszweck

(1) Beruht ein KI-System auf einem KI-Modell mit allgemeinem Verwendungszweck und werden das Modell und das System vom selben Anbieter entwickelt, so ist das Büro für Künstliche Intelligenz befugt, die Konformität des KI-Systems mit den Pflichten aus dieser Verordnung zu überwachen und beaufsichtigen. Zur Wahrnehmung seiner Beobachtungs- und Überwachungsaufgaben hat das Büro für Künstliche Intelligenz alle in diesem Abschnitt und in der Verordnung (EU) 2019/1020 vorgesehenen Befugnisse einer Marktüberwachungsbehörde.

(2) Haben die zuständigen Marktüberwachungsbehörden hinreichenden Grund für die Auffassung, dass KI-Systeme mit allgemeinem Verwendungszweck, die von Betreibern direkt für mindestens einen Zweck, der gemäß dieser Verordnung als hochriskant eingestuft ist, verwendet werden können, nicht mit den in dieser Verordnung festgelegten Anforderungen konform sind, so arbeiten sie bei der Durchführung von Konformitätsbewertungen mit dem Büro für Künstliche Intelligenz zusammen und unterrichten das KI-Gremium und andere Marktüberwachungsbehörden entsprechend.

(3) Ist eine Marktüberwachungsbehörde wegen der Unzugänglichkeit bestimmter Informationen im Zusammenhang mit dem KI-Modell mit allgemeinem Verwendungszweck nicht in der Lage, ihre Ermittlungen zu dem Hochrisiko-KI-System abzuschließen, obwohl sie alle angemessenen Anstrengungen unternommen hat, diese Informationen zu erhalten, kann sie ein begründetes Ersuchen an das Büro für Künstliche Intelligenz richten, durch das der Zugang zu den Informationen durchgesetzt werden kann. In diesem Fall übermittelt das Büro für Künstliche Intelligenz der ersuchenden Behörde unverzüglich, spätestens aber innerhalb von 30 Tagen, alle Informationen, die das Büro für Künstliche Intelligenz für die Feststellung, ob ein Hochrisiko-KI-System nicht konform ist, für erforderlich erachtet. Die Marktüberwachungsbehörden gewährleisten gemäß Artikel 78 der vorliegenden Verordnung die Vertraulichkeit der von ihnen erlangten Informationen. Das Verfahren nach Kapitel VI der Verordnung (EU) 2019/1020 gilt entsprechend.

I. Worum geht es?

Artikel 75 regelt die Aufsicht und Zusammenarbeit bei KI-Systemen, die auf KI-Modellen mit allgemeinem Verwendungszweck beruhen. Da diese Modelle besonders flexibel einsetzbar sind und auch in Hochrisiko-Bereichen Anwendung finden können, legt die Norm fest, welche Behörde zuständig ist und wie Informationen zwischen Behörden geteilt werden. Im Kern geht es um die Abstimmung zwischen dem Büro für Künstliche Intelligenz (AI Office) und den nationalen Marktüberwachungsbehörden.

II. Detailkommentar

A. Zuständigkeit des Büro für Künstliche Intelligenz

- **Grundsatz**: Wenn Modell und System vom selben Anbieter kommen, überwacht das Büro für Künstliche Intelligenz die Konformität.
- **Befugnisse**: Das Büro für Künstliche Intelligenz hat hier dieselben Rechte wie eine Marktüberwachungsbehörde nach der Verordnung (EU) 2019/1020 (zB Akteneinsicht, Inspektionen, Anordnungen).
- **Systematik**: Dies vermeidet Doppelzuständigkeiten, da nicht die nationalen Behörden, sondern eine zentrale EU-Stelle prüft.

Beispiel: *Ein Anbieter entwickelt ein Sprachmodell und bringt gleichzeitig ein Chatbot-System auf den Markt. Das Büro für Künstliche Intelligenz kontrolliert in diesem Fall direkt, ob das gesamte System den Anforderungen entspricht.*

B. Zusammenarbeit bei Hochrisiko-Anwendungen

- **Hochrisiko-Fokus**: Wenn ein allgemeines Modell direkt für einen hochriskanten Zweck verwendet werden kann, prüfen die Marktüberwachungsbehörden.
- **Kooperation**: Diese Behörden arbeiten eng mit dem Büro für Künstliche Intelligenz zusammen.
- **Informationspflicht**: Ergebnisse werden auch dem KI-Gremium und anderen Behörden mitgeteilt, um EU-weite Konsistenz sicherzustellen.

Beispiel: *Eine nationale Behörde prüft ein medizinisches Diagnose-Tool, das auf einem allgemeinen Modell basiert. Sie bindet das Büro für Künstliche Intelligenz ein, um die Modellgrundlage zu bewerten.*

C. Amtshilfe durch das Büro für Künstliche Intelligenz

- **Problem**: Nationale Behörden haben oft keinen Zugang zu internen Modelldaten.
- **Lösung**: Wenn trotz aller Bemühungen Informationen fehlen, können sie das Büro für Künstliche Intelligenz um Unterstützung bitten.
- **Frist**: Das Büro für Künstliche Intelligenz muss innerhalb von 30 Tagen die nötigen Infos liefern.
- **Vertraulichkeit**: Behörden müssen die Daten vertraulich behandeln (Artikel 78 KI-VO).
- **Verweis**: Es gilt das Verfahren zur grenzübergreifenden Amtshilfe nach der Marktüberwachungsverordnung 2019/1020.

Beispiel: *Eine Behörde prüft ein KI-System zur Kreditvergabe, kann aber die Trainingsdaten des zugrundeliegenden Modells nicht einsehen. Sie ersucht das Büro für Künstliche Intelligenz, Zugang zu erhalten.*

D. Besonderheiten

- **Kompetenzaufteilung**: Klarstellung, wann die EU und wann die Mitgliedstaaten zuständig sind.
- **Zentrale Rolle des Büro für Künstliche Intelligenz**: Es fungiert als **Informations- und Durchsetzungsdrehscheibe** für KI-Systeme mit allgemeinem Verwendungszweck.
- **Wissenschaftliche Unterstützung**: Das Büro für Künstliche Intelligenz kann sich durch das wissenschaftliche Gremium beraten lassen, wenn systemische Risiken drohen.

III. Zusammenfassung

Zuständigkeit	Bei System und Modell vom selben Anbieter ist das Büro für Künstliche Intelligenz zuständig.
Kooperation	Nationale Behörden + Büro für Künstliche Intelligenz arbeiten bei hochriskanten Anwendungen zusammen.
Amtshilfe	Wenn Behörden keine Infos erhalten, kann das Büro für Künstliche Intelligenz diese erzwingen (30-Tage-Frist).
Schutzmaßnahmen	Vertraulichkeit und Verfahren nach Verordnung (EU) 2019/1020 gelten ergänzend.

IV. Quellenverzeichnis

- Erwägungsgründe 161-164 KI-VO (EU) 2024/1689

Artikel 76 KI-VO

Beaufsichtigung von Tests unter Realbedingungen durch Marktüberwachungsbehörden

(1) Marktüberwachungsbehörden müssen über die Kompetenzen und Befugnisse verfügen, um sicherzustellen, dass Tests unter Realbedingungen gemäß dieser Verordnung erfolgen.

(2) Wenn ein Test unter Realbedingungen für KI-Systeme durchgeführt wird, die in einem KI-Reallabor gemäß Artikel 58 beaufsichtigt werden, überprüfen die Marktüberwachungsbehörden im Rahmen ihrer Aufsichtsaufgaben für das KI-Reallabor die Einhaltung des Artikels 60. Die Behörden können gegebenenfalls gestatten, dass der Anbieter oder zukünftige Anbieter den Test unter Realbedingungen in Abweichung von den in Artikel 60 Absatz 4 Buchstaben f und g festgelegten Bedingungen durchführt.

(3) Wenn eine Marktüberwachungsbehörde vom zukünftigen Anbieter, vom Anbieter oder von einem Dritten über einen schwerwiegenden Vorfall informiert wurde oder Grund zu der Annahme hat, dass die in den Artikeln 60 und 61 festgelegten Bedingungen nicht erfüllt sind, kann sie — je nachdem, was angemessen ist — in ihrem Hoheitsgebiet gegebenenfalls entscheiden, entweder

a) den Test unter Realbedingungen auszusetzen oder abzubrechen oder

b) den Anbieter oder zukünftigen Anbieter und die Betreiber oder zukünftigen Betreiber zur Änderung eines beliebigen Aspekts des Tests unter Realbedingungen zu verpflichten.

(4) Wenn eine Marktüberwachungsbehörde eine Entscheidung nach Absatz 3 des vorliegenden Artikels getroffen oder Einwände im Sinne des Artikels 60 Absatz 4 Buchstabe b erhoben hat, sind im Rahmen der Entscheidung oder der Einwände die Gründe dafür zu nennen sowie anzugeben, wie der Anbieter oder zukünftige Anbieter die Entscheidung oder die Einwände anfechten kann.

(5) Wenn eine Marktüberwachungsbehörde eine Entscheidung nach Absatz 3 getroffen hat, teilt sie ihre Gründe dafür gegebenenfalls den Marktüberwachungsbehörden anderer Mitgliedstaaten mit, in denen das KI-System gemäß dem Plan für den Test getestet wurde.

I. Worum geht es?

Artikel 76 regelt die Rolle der Marktüberwachungsbehörden beim Testen von KI-Systemen unter realen Bedingungen. Ziel ist es, sicherzustellen, dass diese Tests rechtmäßig, sicher und im Einklang mit den Anforderungen der KI-VO erfolgen. Die Behörden erhalten dafür klare Befugnisse: Sie können Tests überwachen, Anpassungen verlangen oder diese sogar aussetzen, wenn Risiken oder Verstöße auftreten.

II. Detailkommentar

A. Zuständigkeit und Befugnisse

- **Kompetenzen sicherstellen**: Die Marktüberwachungsbehörden müssen in der Lage sein, Tests unter Realbedingungen wirksam zu beaufsichtigen. Dazu gehören Prüfungsrechte, Kontrollmöglichkeiten und Eingriffsbefugnisse.
- **Ziel**: Vermeidung von Missbrauch und Gewährleistung, dass Tests nicht unkontrolliert oder außerhalb der gesetzlichen Rahmenbedingungen stattfinden.

Beispiel: *Ein Start-up testet ein neues KI-System für Bewerbungsprozesse direkt in einem Unternehmen. Die Marktüberwachungsbehörde kann prüfen, ob die Testpersonen informiert wurden und ob Risiken ausreichend abgesichert sind.*

B. Tests im KI-Reallabor

- **Reallabor-Bezug**: Wenn ein Test im Rahmen eines KI-Reallabors erfolgt, erfolgt die Aufsicht durch die Marktüberwachungsbehörden anhand der speziellen Reallabor-Regeln.
- **Flexibilität**: Die Behörden dürfen Abweichungen von bestimmten Detailpflichten (zB Dokumentationsanforderungen) erlauben, um praxisgerechtes Testen zu ermöglichen.

Beispiel: *Ein medizinisches KI-System wird im Krankenhaus getestet. Um den Ablauf nicht zu behindern, erlaubt die Behörde eine vereinfachte Dokumentation während des laufenden Tests.*

C. Eingriffsbefugnisse bei Verstößen

- **Auslöser**: Ein Vorfall, eine Beschwerde oder ein Hinweis auf Verstöße gegen Testbedingungen.
- **Maßnahmen**:
  1. Aussetzung oder Abbruch des Tests.
  2. Verpflichtung zur Änderung einzelner Aspekte des Tests (zB Datensicherheit, Einholung von Einwilligungen).
- **Verhältnismäßigkeit**: Die Behörde entscheidet, was im konkreten Fall angemessen ist.

Beispiel: *Eine KI zur Schülerbewertung zeigt diskriminierende Ergebnisse. Die Behörde kann den Test stoppen oder anordnen, dass nur anonymisierte Daten genutzt werden.*

D. Begründungspflicht und Rechtsschutz

- **Transparenz**: Jede Entscheidung der Behörde muss begründet werden.
- **Rechtsmittel**: Anbieter erhalten Hinweise, wie sie gegen die Entscheidung vorgehen können.

Beispiel: *Eine Behörde untersagt den Test eines KI-Systems zur Gesichtserkennung. Der Anbieter erhält eine schriftliche Begründung und Hinweise zu Beschwerdewegen.*

E. Informationspflicht gegenüber anderen Mitgliedstaaten

- **Kooperation**: Entscheidungen müssen mitgeteilt werden, wenn der Test in mehreren Mitgliedstaaten stattfindet.
- **Ziel**: Einheitliche Aufsicht und Vermeidung widersprüchlicher Entscheidungen.

Beispiel: *Ein Anbieter testet ein KI-System zur Verkehrssteuerung in Österreich und Deutschland. Stoppt die österreichische Behörde den Test, wird dies auch der deutschen Behörde gemeldet.*

F. Besonderheiten

- **Abwägung zwischen Innovation und Schutz**: Die Regelung schafft Balance zwischen Förderung neuer Technologien (durch Reallabore und flexible Testbedingungen) und dem Schutz von Grundrechten.
- **Schutz vulnerabler Gruppen**: Insbesondere bei Tests mit potenziellen Auswirkungen auf Einzelpersonen (zB Schüler, Patienten) wird besonderer Wert auf Eingriffsmöglichkeiten gelegt.

III. Zusammenfassung

Ziel	Sicherstellung sicherer und rechtmäßiger Tests von KI-Systemen unter Realbedingungen
Befugnisse	Kontrolle, Anpassung, Aussetzung oder Abbruch von Tests
Reallabor	Besondere Regeln, Möglichkeit von Ausnahmen zur Förderung von Innovation
Vorfälle	Eingriff bei Verstößen oder schwerwiegenden Vorfällen
Rechtsschutz	Begründungspflicht und Möglichkeit zur Anfechtung
EU-Kooperation	Informationspflicht bei grenzüberschreitenden Tests

IV. Quellenverzeichnis

- Erwägungsgründe 139, 141 KI-VO (EU) 2024/1689

Artikel 77 KI-VO

Befugnisse der für den Schutz der Grundrechte zuständigen Behörden

(1) Nationale Behörden oder öffentliche Stellen, die die Einhaltung des Unionsrechts zum Schutz der Grundrechte, einschließlich des Rechts auf Nichtdiskriminierung, in Bezug auf die Verwendung der in Anhang III genannten Hochrisiko-KI-Systeme beaufsichtigen oder durchsetzen, sind befugt, sämtliche auf der Grundlage dieser Verordnung in zugänglicher Sprache und Format erstellte oder geführte Dokumentation anzufordern und einzusehen, sofern der Zugang zu dieser Dokumentation für die wirksame Ausübung ihrer Aufträge im Rahmen ihrer Befugnisse innerhalb der Grenzen ihrer Hoheitsgewalt notwendig ist. Die jeweilige Behörde oder öffentliche Stelle informiert die Marktüberwachungsbehörde des betreffenden Mitgliedstaats von jeder diesbezüglichen Anfrage.

(2) Bis 2. November 2024 muss jeder Mitgliedstaat die in Absatz 1 genannten Behörden oder öffentlichen Stellen benennen und in einer öffentlichen Liste verfügbar machen. Die Mitgliedstaaten übermitteln die Liste der Kommission und den anderen Mitgliedstaaten und halten die Liste auf dem neuesten Stand.

(3) Sollte die in Absatz 1 genannte Dokumentation nicht ausreichen, um feststellen zu können, ob ein Verstoß gegen das Unionsrecht zum Schutz der Grundrechte vorliegt, so kann die in Absatz 1 genannte Behörde oder öffentliche Stelle bei der Marktüberwachungsbehörde einen begründeten Antrag auf Durchführung eines technischen Tests des Hochrisiko-KI-Systems stellen. Die Marktüberwachungsbehörde führt den Test unter enger Einbeziehung der beantragenden Behörde oder öffentlichen Stelle innerhalb eines angemessenen Zeitraums nach Eingang des Antrags durch.

(4) Jegliche Informationen oder Dokumentation, in deren Besitz die in Absatz 1 des vorliegenden Artikels genannten nationalen Behörden oder öffentlichen Stellen auf der Grundlage des vorliegenden Artikels gelangen, werden im Einklang mit den in Artikel 78 festgelegten Vertraulichkeitspflichten behandelt.

I. Worum geht es?

Artikel 77 regelt die Befugnisse der nationalen Behörden, die für den Schutz der Grundrechte zuständig sind, im Zusammenhang mit Hochrisiko-KI-

Systemen. Ziel ist es, sicherzustellen, dass diese Behörden Zugang zu allen relevanten Informationen haben, um mögliche Grundrechtsverletzungen – insbesondere Diskriminierungen – wirksam überprüfen zu können. Zudem werden die Mitgliedstaaten verpflichtet, entsprechende Stellen offiziell zu benennen und transparent zu machen. Artikel 77 ergänzt damit die Marktüberwachung, indem er den Grundrechtsschutz in den Mittelpunkt stellt.

II. Detailkommentar

A. Zuständige Behörden

- **Nationale Stellen**: Gemeint sind Behörden oder öffentliche Stellen, die die Einhaltung von Grundrechten überwachen, etwa Gleichbehandlungsstellen oder Datenschutzbehörden.
- **Keine Einschränkung der Zuständigkeit**: Nach Erwägungsgrund 157 bleibt ihre Unabhängigkeit und bestehende Kompetenz unberührt. Sie erhalten jedoch zusätzliche Zugriffsrechte auf Dokumentation nach der KI-VO.

Beispiel: *Eine nationale Antidiskriminierungsstelle prüft, ob ein KI-basiertes Bewerberauswahlverfahren bestimmte Bevölkerungsgruppen systematisch benachteiligt.*

B. Befugnisse zur Dokumenteneinsicht

- **Dokumentationszugang**: Die Behörden können sämtliche Dokumente anfordern, die nach der KI-VO vorgeschrieben sind. Diese müssen in verständlicher Sprache und in geeigneter Form vorliegen.
- **Notwendigkeit der Einsicht**: Zugang besteht nur, wenn die Dokumente für die Erfüllung des behördlichen Auftrags erforderlich sind.
- **Informationspflicht**: Jede Anfrage muss der zuständigen Marktüberwachungsbehörde gemeldet werden, um Doppelstrukturen zu vermeiden und Koordination sicherzustellen.

Beispiel: *Eine Behörde verlangt die Risikobewertung eines KI-Systems, um prüfen zu können, ob Diskriminierungen erkannt und berücksichtigt wurden.*

C. Benennung der Behörden

- **Frist**: Bis zum 2. November 2024 müssen die Mitgliedstaaten die zuständigen Stellen benennen.
- **Öffentliche Liste**: Die benannten Stellen müssen veröffentlicht werden. Zusätzlich sind sie der Kommission und den anderen Mitgliedstaaten mitzuteilen.
- **Aktualisierungspflicht**: Änderungen müssen laufend nachgetragen werden.

Beispiel: *Ein Mitgliedstaat benennt seine nationale Datenschutzbehörde und die Gleichbehandlungsstelle und führt diese in einer zentralen Online-Liste an.*

D. Technische Tests

- **Ergänzende Befugnis**: Reicht die Dokumentation nicht aus, kann eine Behörde über die Marktüberwachungsbehörde einen technischen Test beantragen.
- **Kooperation**: Der Test wird von der Marktüberwachungsbehörde durchgeführt, allerdings unter enger Einbeziehung der beantragenden Grundrechtsbehörde.
- **Frist**: Der Test muss in angemessener Zeit erfolgen.

Beispiel: *Die Dokumentation eines KI-Systems für Kreditwürdigkeitsprüfungen ist unklar. Die zuständige Behörde beantragt deshalb einen Praxistest, um die tatsächliche Funktionsweise zu untersuchen.*

E. Vertraulichkeit

- **Pflicht zur Verschwiegenheit**: Alle erhaltenen Informationen unterliegen den Vertraulichkeitsregeln nach Artikel 78 KI-VO.
- **Schutz sensibler Daten**: Damit soll ein Ausgleich geschaffen werden zwischen effektiver Kontrolle und Schutz der Geschäftsgeheimnisse der Anbieter.

Beispiel: *Eine Behörde erhält interne Trainingsdaten eines KI-Systems. Sie darf diese nicht veröffentlichen, sondern nur für die Prüfung der Grundrechtskonformität nutzen.*

F. Besonderheiten

- **Unabhängigkeit**: Die Behördenmüssen unparteiisch und unvoreingenommen handeln. Ihre Mitglieder dürfen keine Handlungen setzen, die ihre Neutralität gefährden.
- **Abgrenzung zur Marktüberwachung**: Während die Marktüberwachungsbehörde primär für Sicherheit und Funktionsfähigkeit zuständig ist, liegt der Fokus der hier genannten Stellen auf dem Grundrechtsschutz.

III. Zusammenfassung

Zuständige Behörden	Nationale Stellen zum Schutz der Grundrechte (zB Gleichbehandlungs- oder Datenschutzbehörden)
Befugnisse	Zugang zu Dokumentation, Antrag auf technische Tests über Marktüberwachungsbehörde
Transparenz	Mitgliedstaaten müssen Stellen bis 2. November 2024 benennen und veröffentlichen
Zusammenarbeit	Informationspflicht gegenüber Marktüberwachungsbehörde; enge Kooperation bei Tests
Vertraulichkeit	Strenge Verschwiegenheitspflichten gem Artikel 78 KI-VO
Besonderheit	Unabhängigkeit und Unvoreingenommenheit der Behörden ist zentral

IV. Quellenverzeichnis

- Erwägungsgründe 154, 157 KI-VO (EU) 2024/1689

Artikel 78 KI-VO

Vertraulichkeit

(1) Die Kommission, die Marktüberwachungsbehörden und die notifizierten Stellen sowie alle anderen natürlichen oder juristischen Personen, die an der Anwendung dieser Verordnung beteiligt sind, wahren gemäß dem Unionsrecht oder dem nationalen Recht die Vertraulichkeit der Informationen und Daten, in deren Besitz sie bei der Ausführung ihrer Aufgaben und Tätigkeiten gelangen, sodass insbesondere Folgendes geschützt ist:

a) die Rechte des geistigen Eigentums sowie vertrauliche Geschäftsinformationen oder Geschäftsgeheimnisse natürlicher oder juristischer Personen, einschließlich Quellcodes, mit Ausnahme der in Artikel 5 der Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates;

b) die wirksame Durchführung dieser Verordnung, insbesondere für die Zwecke von Inspektionen, Untersuchungen oder Audits;

c) öffentliche und nationale Sicherheitsinteressen;

d) die Durchführung von Straf- oder Verwaltungsverfahren;

e) gemäß dem Unionsrecht oder dem nationalen Recht als Verschlusssache eingestufte Informationen.

(2) Die gemäß Absatz 1 an der Anwendung dieser Verordnung beteiligten Behörden fragen nur Daten an, die für die Bewertung des von KI-Systemen ausgehenden Risikos und für die Ausübung ihrer Befugnisse in Übereinstimmung mit dieser Verordnung und mit der Verordnung (EU) 2019/1020 unbedingt erforderlich sind. Sie ergreifen angemessene und wirksame Cybersicherheitsmaßnahmen zum Schutz der Sicherheit und Vertraulichkeit der erlangten Informationen und Daten und löschen im Einklang mit dem geltenden Unionsrecht oder nationalen Recht die erhobenen Daten, sobald sie für den Zweck, für den sie erlangt wurden, nicht mehr benötigt werden.

(3) Unbeschadet der Absätze 1 und 2 darf der Austausch vertraulicher Informationen zwischen den zuständigen nationalen Behörden untereinander oder zwischen den zuständigen nationalen Behörden und der Kommission nicht ohne vorherige Rücksprache mit der zuständigen nationalen Behörde, von der die Informationen stammen, und dem Betreiber

offengelegt werden, sofern die in Anhang III Nummer 1, 6 oder 7 genannten Hochrisiko-KI-Systeme von Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden verwendet werden und eine solche Offenlegung die öffentlichen und nationalen Sicherheitsinteressen gefährden könnte. Dieser Informationsaustausch erstreckt sich nicht auf sensible operative Daten zu den Tätigkeiten von Strafverfolgungs-, Grenzschutz-, Einwanderungs- oder Asylbehörden.

Handeln Strafverfolgungs-, Einwanderungs- oder Asylbehörden als Anbieter von in Anhang III Nummer 1, 6 oder 7 genannten Hochrisiko-KI-Systemen, so verbleibt die technische Dokumentation nach Anhang IV in den Räumlichkeiten dieser Behörden. Diese Behörden sorgen dafür, dass die in Artikel 74 Absätze 8 und 9 genannten Marktüberwachungsbehörden auf Anfrage unverzüglich Zugang zu dieser Dokumentation oder eine Kopie davon erhalten. Zugang zu dieser Dokumentation oder zu einer Kopie davon darf nur das Personal der Marktüberwachungsbehörde erhalten, das über eine entsprechende Sicherheitsfreigabe verfügt.

(4) Die Absätze 1, 2 und 3 dürfen sich weder auf die Rechte oder Pflichten der Kommission, der Mitgliedstaaten und ihrer einschlägigen Behörden sowie der notifizierten Stellen in Bezug auf den Informationsaustausch und die Weitergabe von Warnungen, einschließlich im Rahmen der grenzüberschreitenden Zusammenarbeit, noch auf die Pflichten der betreffenden Parteien auswirken, Informationen auf der Grundlage des Strafrechts der Mitgliedstaaten bereitzustellen.

(5) Die Kommission und die Mitgliedstaaten können erforderlichenfalls und im Einklang mit den einschlägigen Bestimmungen internationaler Übereinkommen und Handelsabkommen mit Regulierungsbehörden von Drittstaaten, mit denen sie bilaterale oder multilaterale Vertraulichkeitsvereinbarungen getroffen haben und die ein angemessenes Niveau an Vertraulichkeit gewährleisten, vertrauliche Informationen austauschen.

I. Worum geht es?

Artikel 78 regelt die **Vertraulichkeit** im Rahmen der Anwendung der KI-VO. Alle an der Durchführung beteiligten Akteure – von der Kommission über nationale Behörden bis zu notifizierten Stellen – müssen sicherstellen, dass vertrauliche Informationen, die sie im Zuge ihrer Arbeit erhalten,

geschützt bleiben. Dabei geht es um sensible Daten wie Geschäftsgeheimnisse, Quellcodes, Sicherheitsinteressen oder strafrechtlich relevante Informationen. Der Artikel soll eine Balance herstellen: Einerseits sollen Behörden wirksam kontrollieren können, andererseits müssen Rechte von Unternehmen, staatliche Sicherheitsinteressen und der Schutz vertraulicher Daten gewahrt bleiben.

II. Detailkommentar

A. Schutzbereiche

- **Geistiges Eigentum**: Dazu zählen insbesondere Patente, Marken oder Software-Quellcodes. Diese dürfen durch Behördenzugriff nicht unrechtmäßig offenbart werden.
- **Geschäftsgeheimnisse**: Darunter fallen vertrauliche Geschäftsinformationen, zB interne Strategien oder Algorithmen.
- **Wirksame Durchführung der KI-VO**: Inspektionen und Audits müssen möglich sein, ohne dass durch Offenlegung ihre Wirksamkeit untergraben wird.
- **Öffentliche und nationale Sicherheit**: Daten, die etwa Terrorabwehrmaßnahmen betreffen, sind besonders geschützt.
- **Straf- und Verwaltungsverfahren**: Informationen dürfen nicht so offengelegt werden, dass Verfahren beeinträchtigt werden.
- **Verschlusssachen**: Informationen, die nach nationalem oder Unionsrecht als geheim eingestuft sind, bleiben geschützt.

Beispiel: *Eine Behörde erhält im Rahmen einer Marktüberwachung den Quellcode eines KI-Systems. Dieser darf nicht an Wettbewerber weitergegeben oder veröffentlicht werden.*

B. Datenanfragen und -verwendung

- **Minimalprinzip**: Behörden dürfen nur die Daten anfragen, die unbedingt notwendig sind, um das Risiko eines KI-Systems zu bewerten.

- **Cybersicherheitspflicht**: Behörden müssen geeignete Maßnahmen treffen, um die Daten vor unbefugtem Zugriff zu schützen.
- **Löschungspflicht**: Erhobene Daten sind zu löschen, sobald sie nicht mehr für den ursprünglichen Zweck benötigt werden.

Beispiel: *Eine Marktüberwachungsbehörde darf die Trainingsdaten eines KI-Systems nur insoweit anfordern, wie es zur Risikobewertung nötig ist, und muss sie nach Abschluss des Verfahrens löschen.*

C. Besondere Regeln für Sicherheitsbehörden

- **Eingeschränkte Offenlegung**: Informationen aus Hochrisiko-KI-Systemen in Bereichen wie Strafverfolgung, Grenzschutz oder Asyl dürfen nur nach Rücksprache mit der Behörde, die sie bereitgestellt hat, weitergegeben werden.
- **Technische Dokumentation**: Diese verbleibt bei den Sicherheitsbehörden selbst und wird nur unter strengen Bedingungen an Marktüberwachungsbehörden weitergegeben.
- **Sicherheitsfreigabe**: Nur autorisiertes Personal mit entsprechender Freigabe darf Zugriff auf sensible Dokumentationen erhalten.

Beispiel: *Ein KI-System zur Gesichtserkennung im Grenzschutz (Anhang III Z 7) darf seine technische Dokumentation nicht frei zugänglich machen. Nur überprüfte Beamte einer Marktüberwachungsbehörde dürfen Einsicht nehmen.*

D. Grenzen der Vertraulichkeit

- **Informationsaustausch**: Artikel 78 beschränkt nicht den Informationsaustausch, wenn er im Rahmen der Marktüberwachung oder Strafverfolgung erforderlich ist.
- **Strafrechtliche Pflichten**: Behörden müssen trotz Vertraulichkeit weiterhin Informationen bereitstellen, wenn nationales Strafrecht dies verlangt.

E. Zusammenarbeit mit Drittstaaten

- **Internationale Kooperation**: Kommission und Mitgliedstaaten dürfen vertrauliche Informationen mit Drittstaaten austauschen, wenn Vertraulichkeitsvereinbarungen bestehen und ein angemessenes Schutzniveau gewährleistet ist.

Beispiel: *Die EU kann mit einer US-Behörde vertrauliche Informationen zu einem KI-System austauschen, sofern ein Abkommen über Vertraulichkeit vorliegt.*

III. Zusammenfassung

Schutzbereiche	Geistiges Eigentum, Geschäftsgeheimnisse, Sicherheit, Verfahren, Verschlusssachen
Datenzugriff	Nur notwendige Daten dürfen angefordert werden; Cybersicherheit und Löschungspflicht bestehen
Sicherheitsbehörden	Besondere Regeln, Dokumentation verbleibt intern, Zugang nur mit Freigabe
Grenzen	Informationsaustausch und strafrechtliche Pflichten bleiben bestehen
Internationale Kooperation	Austausch mit Drittstaaten nur bei ausreichendem Schutz möglich

IV. Quellenverzeichnis

- Erwägungsgrund 167 KI-VO (EU) 2024/1689

Artikel 79 KI-VO

Verfahren auf nationaler Ebene für den Umgang mit KI-Systemen, die ein Risiko bergen

(1) Als KI-Systeme, die ein Risiko bergen, gelten „Produkte, mit denen ein Risiko verbunden ist" im Sinne des Artikels 3 Nummer 19 der Verordnung (EU) 2019/1020, sofern sie Risiken für die Gesundheit oder Sicherheit oder Grundrechte von Personen bergen.

(2) Hat die Marktüberwachungsbehörde eines Mitgliedstaats hinreichend Grund zu der Annahme, dass ein KI-System ein Risiko nach Absatz 1 des vorliegenden Artikels birgt, so prüft sie das betreffende KI-System im Hinblick auf die Erfüllung aller in der vorliegenden Verordnung festgelegten Anforderungen und Pflichten. Besondere Aufmerksamkeit gilt KI-Systemen, die für schutzbedürftige Gruppen ein Risiko bergen. Wenn Risiken für die Grundrechte festgestellt werden, informiert die Marktüberwachungsbehörde auch die in Artikel 77 Absatz 1 genannten einschlägigen nationalen Behörden oder öffentlichen Stellen und arbeitet uneingeschränkt mit ihnen zusammen. Die betreffenden Akteure arbeiten erforderlichenfalls mit der Marktüberwachungsbehörde und den in Artikel 77 Absatz 1 genannten anderen Behörden oder öffentlichen Stellen zusammen.

Stellt die Marktüberwachungsbehörde oder gegebenenfalls die Marktüberwachungsbehörde in Zusammenarbeit mit der in Artikel 77 Absatz 1 genannten nationalen Behörde im Verlauf dieser Prüfung fest, dass das KI-System die in dieser Verordnung festgelegten Anforderungen und Pflichten nicht erfüllt, fordert sie den jeweiligen Akteur unverzüglich auf, alle Korrekturmaßnahmen zu ergreifen, die geeignet sind, die Konformität des KI-Systems herzustellen, das KI-System vom Markt zu nehmen oder es innerhalb einer Frist, die die Marktüberwachungsbehörde vorgeben kann, in jedem Fall innerhalb von weniger als 15 Arbeitstagen, oder gemäß den einschlägigen Harmonisierungsrechtsvorschriften der Union zurückzurufen.

Die Marktüberwachungsbehörde informiert die betreffende notifizierte Stelle entsprechend. Artikel 18 der Verordnung (EU) 2019/1020 gilt für die in Unterabsatz 2 des vorliegenden Absatzes genannten Maßnahmen.

(3) Gelangt die Marktüberwachungsbehörde zu der Auffassung, dass die Nichtkonformität nicht auf ihr nationales Hoheitsgebiet beschränkt ist, so informiert sie die Kommission und die anderen Mitgliedstaaten unverzüglich

über die Ergebnisse der Prüfung und über die Maßnahmen, zu denen sie den Akteur aufgefordert hat.

(4) Der Akteur sorgt dafür, dass alle geeigneten Korrekturmaßnahmen in Bezug auf alle betreffenden KI-Systeme, die er auf dem Unionsmarkt bereitgestellt hat, getroffen werden.

(5) Ergreift der Akteur in Bezug auf sein KI-System keine geeigneten Korrekturmaßnahmen innerhalb der in Absatz 2 genannten Frist, trifft die Marktüberwachungsbehörde alle geeigneten vorläufigen Maßnahmen, um die Bereitstellung oder Inbetriebnahme des KI-Systems auf ihrem nationalen Markt zu verbieten oder einzuschränken, das Produkt oder das eigenständige KI-System von diesem Markt zu nehmen oder es zurückzurufen. Diese Behörde notifiziert unverzüglich die Kommission und die anderen Mitgliedstaaten über diese Maßnahmen.

(6) Die Notifizierung nach Absatz 5 enthält alle vorliegenden Angaben, insbesondere die für die Identifizierung des nicht konformen Systems notwendigen Informationen, den Ursprung des KI-Systems und die Lieferkette, die Artikel der vermuteten Nichtkonformität und das sich daraus ergebende Risiko, die Artikel und Dauer der ergriffenen nationalen Maßnahmen und die von dem betreffenden Akteur vorgebrachten Argumente. Die Marktüberwachungsbehörden geben insbesondere an, ob die Nichtkonformität eine oder mehrere der folgenden Ursachen hat:

a) Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken;

b) Nichterfüllung der in Kapitel III Abschnitt 2 festgelegten Anforderungen durch ein Hochrisiko-KI-System;

c) Mängel in den in den Artikeln 40 und 41 genannten harmonisierten Normen oder gemeinsamen Spezifikationen, die eine Konformitätsvermutung begründen;

d) Nichteinhaltung des Artikels 50.

(7) Die anderen Marktüberwachungsbehörden — mit Ausnahme der Marktüberwachungsbehörde des Mitgliedstaats, der das Verfahren eingeleitet hat — informieren unverzüglich die Kommission und die anderen Mitgliedstaaten über jegliche Maßnahmen und ihnen vorliegende zusätzlichen Informationen zur Nichtkonformität des betreffenden KI-Systems sowie — falls sie die ihnen mitgeteilte nationale Maßnahme ablehnen — über ihre Einwände.

(8) Erhebt weder eine Marktüberwachungsbehörde eines Mitgliedstaats noch die Kommission innerhalb von drei Monaten nach Eingang der in Absatz 5 des vorliegenden Artikels genannten Notifizierung Einwände gegen eine von einer Marktüberwachungsbehörde eines anderen Mitgliedstaats erlassene vorläufige Maßnahme, so gilt diese Maßnahme als gerechtfertigt. Die Verfahrensrechte des betreffenden Akteurs nach Artikel 18 der Verordnung (EU) 2019/1020 bleiben hiervon unberührt. Die Frist von drei Monaten gemäß dem vorliegenden Absatz wird bei Nichteinhaltung des Verbots der in Artikel 5 der vorliegenden Verordnung genannten KI-Praktiken auf 30 Tage verkürzt.

(9) Die Marktüberwachungsbehörden tragen dafür Sorge, dass geeignete einschränkende Maßnahmen in Bezug auf das betreffende Produkt oder KI-System ergriffen werden, beispielsweise die unverzügliche Rücknahme des Produkts oder KI-Systems von ihrem Markt.

I. Worum geht es?

Artikel 79 regelt das Verfahren, wenn nationale Behörden feststellen, dass ein KI-System ein Risiko für Gesundheit, Sicherheit oder Grundrechte darstellt. Ziel ist es, schnelle Maßnahmen zu ermöglichen, um gefährliche oder rechtswidrige KI-Systeme vom Markt zu nehmen oder deren Einsatz einzuschränken. Der Artikel baut auf den bestehenden Marktüberwachungsvorschriften der EU auf und stellt sicher, dass die Zusammenarbeit zwischen Mitgliedstaaten, der Kommission und betroffenen Akteuren funktioniert.

II. Detailkommentar

A. Begriff des „Risikos“

- **Risikosystem**: Ein KI-System gilt als Risiko, wenn es wie ein „Produkt, mit dem ein Risiko verbunden ist“ nach Artikel 3 Nr 19 der Verordnung (EU) 2019/1020 einzustufen ist und konkrete Gefahren für Gesundheit, Sicherheit oder Grundrechte birgt.
- **Grundrechtsrisiken**: Besonders relevant sind Gefahren wie Diskriminierung, Verletzung der Privatsphäre oder unrechtmäßige Überwachung.

- **Schutzbedürftige Gruppen**: Kinder, ältere Menschen oder sozial benachteiligte Gruppen verdienen besonderen Schutz.

Beispiel: *Eine Gesichtserkennungssoftware weist hohe Fehlerraten bei Personen mit dunkler Hautfarbe auf und gefährdet damit das Grundrecht auf Gleichbehandlung.*

B. Verfahren der Marktüberwachungsbehörden

- **Prüfung**: Hat eine nationale Behörde Hinweise auf Risiken, untersucht sie das KI-System vollständig.
- **Kooperation**: Bei Grundrechtsverletzungen muss zusätzlich die zuständige nationale Behörde (zB Datenschutzbehörde) informiert und eingebunden werden.
- **Korrekturmaßnahmen**: Stellt sich eine Nichtkonformität heraus, muss der Anbieter das System innerhalb von maximal 15 Arbeitstagen anpassen, vom Markt nehmen oder zurückrufen.

Beispiel: *Eine Behörde entdeckt, dass ein Bewerbungs-KI-System systematisch Frauen benachteiligt. Der Anbieter muss innerhalb von 15 Tagen Änderungen vornehmen oder das System zurückziehen.*

C. Informationspflichten und EU-weite Wirkung

- **Grenzüberschreitende Risiken**: Erkennt eine Behörde, dass die Gefahr nicht nur im eigenen Staat besteht, informiert sie sofort Kommission und andere Mitgliedstaaten.
- **Pflicht des Anbieters**: Der Anbieter muss für alle bereits vertriebenen Systeme geeignete Maßnahmen setzen.
- **Notifizierung**: Wenn der Anbieter nicht handelt, muss die Behörde Maßnahmen wie Verbot oder Rückruf ergreifen und dies der Kommission sowie anderen Mitgliedstaaten mitteilen.

D. Inhalt der Notifizierung

- **Pflichtangaben**: Dazu gehören Identität des Systems, Herkunft, Lieferkette, Artikel der Nichtkonformität, Risiko sowie Einwände des Anbieters.
- **Mögliche Ursachen**:
  a. Verstoß gegen Verbote nach Artikel 5 KI-VO (zB manipulative Systeme).
  b. Nichterfüllung der Anforderungen für Hochrisiko-KI nach Kapitel III Abschnitt 2.
  c. Fehler in Normen oder Spezifikationen.
  d. Missachtung der Transparenzpflichten nach Artikel 50 KI-VO.

E. Einwände anderer Mitgliedstaaten

- **Koordination**: Andere Staaten können eigene Informationen oder Einwände beisteuern.
- **Fristen**: Reagiert binnen drei Monaten niemand, gilt die Maßnahme als gerechtfertigt. Bei verbotenen Praktiken nach Artikel 5 KI-VObeträgt die Frist nur 30 Tage.

Beispiel: *Ein Mitgliedstaat verbietet ein Social-Scoring-System. Widerspricht kein anderer Staat oder die Kommission innerhalb von 30 Tagen, wird das Verbot unionsweit anerkannt.*

F. Durchsetzung

Endmaßnahmen: Behörden müssen sicherstellen, dass gefährliche Systeme sofort vom Markt verschwinden oder zurückgerufen werden.

III. Zusammenfassung

Ziel	Schutz von Gesundheit, Sicherheit und Grundrechten durch schnelles Eingreifen bei riskanten KI-Systemen
Zuständigkeit	Nationale Marktüberwachungsbehörden, in Kooperation mit anderen Behörden und der Kommission

Maßnahmen	Prüfung, Anordnung von Korrekturen, Marktverbot, Rückruf
Fristen	Maximal 15 Arbeitstage für Anbieter, drei Monate (bzw 30 Tage) für Einwände anderer Staaten
Ursachen für Nichtkonformität	Verbotene Praktiken, fehlende Erfüllung von Hochrisiko-Anforderungen, Mängel in Normen, Verletzung von Transparenzpflichten

IV. Quellenverzeichnis

- Erwägungsgründe 96, 153, 156, 157, 160 KI-VO (EU) 2024/1689

Artikel 80 KI-VO

Verfahren für den Umgang mit KI-Systemen, die vom Anbieter gemäß Anhang III als nicht hochriskant eingestuft werden

(1) Hat eine Marktüberwachungsbehörde hinreichend Grund zu der Annahme, dass ein vom Anbieter als nicht hochriskant gemäß Artikel 6 Absatz 3 eingestuftes KI-System tatsächlich hochriskant ist, so prüft die Marktüberwachungsbehörde das betreffende KI-System im Hinblick auf seine Einstufung als Hochrisiko-KI-System auf der Grundlage der in Artikel 6 Absatz 3 festgelegten Bedingungen und den Leitlinien der Kommission.

(2) Stellt die Marktüberwachungsbehörde im Verlauf dieser Prüfung fest, dass das betreffende KI-System hochriskant ist, fordert sie den jeweiligen Anbieter unverzüglich auf, alle erforderlichen Maßnahmen zu ergreifen, um die Konformität des KI-Systems mit den in dieser Verordnung festgelegten Anforderungen und Pflichten herzustellen, sowie innerhalb einer Frist, die die Marktüberwachungsbehörde vorgeben kann, geeignete Korrekturmaßnahmen zu ergreifen.

(3) Gelangt die Marktüberwachungsbehörde zu der Auffassung, dass die Verwendung des betreffenden KI-Systems nicht auf ihr nationales Hoheitsgebiet beschränkt ist, so informiert sie die Kommission und die anderen Mitgliedstaaten unverzüglich über die Ergebnisse der Prüfung und über die Maßnahmen, zu denen sie den Anbieter aufgefordert hat.

(4) Der Anbieter sorgt dafür, dass alle erforderlichen Maßnahmen ergriffen werden, um die Konformität des KI-Systems mit den in dieser Verordnung festgelegten Anforderungen und Pflichten herzustellen. Stellt der Anbieter eines betroffenen KI-Systems die Konformität des KI-Systems mit diesen Anforderungen und Pflichten nicht innerhalb der in Absatz 2 des vorliegenden Artikels genannten Frist her, so werden gegen den Anbieter Geldbußen gemäß Artikel 99 verhängt.

(5) Der Anbieter sorgt dafür, dass alle geeigneten Korrekturmaßnahmen in Bezug auf alle betreffenden KI-Systeme, die er auf dem Unionsmarkt bereitgestellt hat, getroffen werden.

(6) Ergreift der Anbieter des betreffenden KI-Systems innerhalb der in Absatz 2 des vorliegenden Artikels genannten Frist keine angemessenen Korrekturmaßnahmen, so findet Artikel 79 Absätze 5 bis 9 Anwendung.

(7) Stellt die Marktüberwachungsbehörde im Verlauf der Prüfung gemäß Absatz 1 des vorliegenden Artikels fest, dass das KI-System vom Anbieter fälschlich als nicht hochriskant eingestuft wurde, um die Geltung der Anforderungen von Kapitel III Abschnitt 2 zu umgehen, so werden gegen den Anbieter Geldbußen gemäß Artikel 99 verhängt.

(8) Bei der Ausübung ihrer Befugnis zur Überwachung der Anwendung dieses Artikels können die Marktüberwachungsbehörden im Einklang mit Artikel 11 der Verordnung (EU) 2019/1020 geeignete Überprüfungen durchführen, wobei sie insbesondere Informationen berücksichtigen, die in der EU-Datenbank gemäß Artikel 71 der vorliegenden Verordnung gespeichert sind.

I. Worum geht es?

Artikel 80 regelt, wie Behörden vorgehen, wenn ein Anbieter ein KI-System fälschlich als nicht hochriskant eingestuft hat. Der Artikel stellt sicher, dass eine nachträgliche Überprüfung stattfindet, Anbieter nötigenfalls Korrekturmaßnahmen setzen und Sanktionen verhängt werden können. Ziel ist es, Umgehungen der strengen Regeln für Hochrisiko-Systeme zu verhindern und den Schutz von Gesundheit, Sicherheit und Grundrechten zu gewährleisten.

II. Detailkommentar

A. Auslöser des Verfahrens

- **Hinreichender Grund**: Die Marktüberwachungsbehörde wird tätig, wenn es Anhaltspunkte gibt, dass ein vermeintlich nicht hochriskantes System tatsächlich hochriskant ist.
- **Prüfmaßstab**: Grundlage sind die Kriterien in Artikel 6 KI-VOAbsatz 3 sowie die Leitlinien der Kommission.

Beispiel: *Ein Anbieter bringt eine KI-Software zur Bewerberauswahl auf den Markt und stuft sie als „nicht hochriskant" ein. Die Behörde prüft jedoch, ob die Software unter Anhang III fällt, da sie über den Zugang zu Beschäftigung entscheidet.*

B. Maßnahmen der Behörde

- **Feststellung Hochrisiko**: Ergibt die Prüfung, dass das System hochriskant ist, muss der Anbieter es an die Anforderungen der KI-VO anpassen.
- **Korrekturmaßnahmen**: Diese sind innerhalb einer von der Behörde gesetzten Frist umzusetzen.
- **Informationspflicht**: Wenn das System auch in anderen Mitgliedstaaten verwendet wird, informiert die Behörde Kommission und andere Mitgliedstaaten.

Beispiel: *Die deutsche Behörde entdeckt ein Hochrisiko-System, das europaweit vertrieben wird. Sie informiert sofort die Kommission und Frankreich, wo das System ebenfalls eingesetzt wird.*

C. Pflichten des Anbieters

- **Konformität herstellen**: Anbieter müssen alle Vorgaben der KI-VO erfüllen.
- **Sanktionen**: Erfolgt dies nicht fristgerecht, drohen Geldbußen nach Artikel 99 KI-VO.
- **EU-weiter Geltungsbereich**: Korrekturmaßnahmen müssen für alle betroffenen Systeme auf dem Unionsmarkt umgesetzt werden.

D. Folgen bei Untätigkeit

- **Keine Korrekturmaßnahmen**: Dann greifen die schärferen Maßnahmen aus Artikel 79 KI-VOAbsatz 5–9 (bis hin zu Rückruf oder Verbot).
- **Umgehungsabsicht**: Wird festgestellt, dass die falsche Einstufung bewusst erfolgte, um die Hochrisiko-Pflichten zu umgehen, folgt zwingend eine Geldbuße.

Beispiel: *Ein Anbieter verschleiert bewusst die Hochrisiko-Eigenschaft seiner KI, um sich das aufwendige Konformitätsverfahren zu sparen. Wird dies entdeckt, ist eine Strafe unvermeidlich.*

E. Befugnisse der Marktüberwachungsbehörden

- **Kontrollbefugnis**: Die Behörden können Prüfungen durchführen, insbesondere unter Rückgriff auf Informationen aus der EU-Datenbank (Artikel 71 KI-VO).
- **Unabhängigkeit**: Behörden müssen unparteiisch und unabhängig handeln.

III. Zusammenfassung

Zweck	Schutz vor falscher Einstufung von Hochrisiko-Systemen
Auslöser	Verdacht der Behörde auf fehlerhafte Einstufung
Prüfmaßstab	Kriterien aus Artikel 6 KI-VOAbsatz 3, Leitlinien der Kommission
Pflichten Anbieter	Herstellung der Konformität, Umsetzung von Korrekturmaßnahmen EU-weit
Sanktionen	Geldbußen nach Artikel 99 KI-VO, ggf Maßnahmen nach Artikel 79 KI-VO
Besondere Schärfe	Strafen bei vorsätzlicher Falscheinstufung

IV. Quellenverzeichnis

- Erwägungsgründe 153, 156, 157, 160 KI-VO (EU) 2024/1689

Artikel 81 KI-VO

Schutzklauselverfahren der Union

(1) Erhebt eine Marktüberwachungsbehörde eines Mitgliedstaats innerhalb von drei Monaten nach Eingang der in Artikel 79 Absatz 5 genannten Notifizierung — oder bei Nichteinhaltung des Verbots der in Artikel 5 genannten KI-Praktiken innerhalb von 30 Tagen — Einwände gegen eine von der Marktüberwachungsbehörde eines anderen Mitgliedstaats getroffene Maßnahme oder ist die Kommission der Ansicht, dass die Maßnahme mit dem Unionsrecht unvereinbar ist, so nimmt die Kommission unverzüglich Konsultationen mit der Marktüberwachungsbehörde des betreffenden Mitgliedstaats und dem Akteur bzw. den Akteuren auf und prüft die nationale Maßnahme. Anhand der Ergebnisse dieser Prüfung entscheidet die Kommission innerhalb von sechs Monaten — oder bei Nichteinhaltung des Verbots der in Artikel 5 genannten KI-Praktiken innerhalb von 60 Tagen — ab dem Eingang der in Artikel 79 Absatz 5 genannten Notifizierung, ob die nationale Maßnahme gerechtfertigt ist, und teilt der Marktüberwachungsbehörde des betreffenden Mitgliedstaats ihre Entscheidung mit. Die Kommission unterrichtet auch alle übrigen Marktüberwachungsbehörden über ihre Entscheidung.

(2) Ist die Kommission der Ansicht, dass die von dem betreffenden Mitgliedstaat ergriffene Maßnahme gerechtfertigt ist, so tragen alle Mitgliedstaaten dafür Sorge, dass sie geeignete einschränkende Maßnahmen in Bezug auf das betreffende KI-System ergreifen, etwa die Anordnung der unverzüglichen Rücknahme des KI-Systems von ihrem Markt, und informiert die Kommission darüber. Erachtet die Kommission die nationale Maßnahme als nicht gerechtfertigt, nimmt der betreffende Mitgliedstaat die Maßnahme zurück und informiert die Kommission darüber.

(3) Gilt die nationale Maßnahme als gerechtfertigt und wird die Nichtkonformität des KI-Systems auf Mängel in den in den Artikeln 40 und 41 dieser Verordnung genannten harmonisierten Normen oder gemeinsamen Spezifikationen zurückgeführt, so leitet die Kommission das in Artikel 11 der Verordnung (EU) Nr 1025/2012 festgelegte Verfahren ein.

I. Worum geht es?

Artikel 81 regelt das sogenannte Schutzklauselverfahren der Union. Dieses Verfahren dient dazu, Konflikte zwischen nationalen Marktüberwachungsbehörden verschiedener Mitgliedstaaten oder zwischen einem Mitgliedstaat und der Kommission über Maßnahmen gegen ein KI-System zu lösen. Ziel ist es, eine einheitliche Entscheidung in der gesamten EU herbeizuführen, um Rechtsklarheit und gleiche Marktbedingungen zu sichern.

II. Detailkommentar

A. Ausgangspunkt

- **Marktüberwachungsbehörden**: Nationale Behörden prüfen KI-Systeme und können Maßnahmen ergreifen, wenn sie Risiken sehen.
- **Konfliktfälle**: Entsteht Uneinigkeit zwischen Behörden, greift Artikel 81.
- **Schutzklausel**: Sie stellt sicher, dass Maßnahmen nicht nur national, sondern unionsweit abgestimmt werden.

Beispiel: *Die Marktüberwachungsbehörde in Frankreich verbietet ein KI-System wegen Diskriminierungsrisiken. Die deutsche Behörde hält das Verbot für überzogen. In diesem Fall prüft die Kommission nach Artikel 81 die Maßnahme.*

B. Ablauf des Verfahrens

1. Einwände einer Marktüberwachungsbehörde

- Erhebt eine Marktüberwachungsbehörde eines Mitgliedstaats Einwände gegen die Maßnahme einer anderen nationalen Behörde, so beträgt die Frist hierfür grundsätzlich drei Monate ab Eingang der Notifizierung nach Artikel 79 KI-VOAbsatz 5.
- Im Falle von verbotenen KI-Praktiken nach Artikel 5 KI-VO gilt eine verkürzte Frist von 30 Tagen.

2. Initiative der Kommission

- Auch unabhängig von Einwänden einer nationalen Behörde kann die Kommission tätig werden, wenn sie der Ansicht ist, dass die nationale Maßnahme mit Unionsrecht unvereinbar ist.
- In diesem Fall nimmt die Kommission unverzüglich Konsultationen mit der betroffenen Marktüberwachungsbehörde sowie mit den betroffenen Anbietern auf und leitet eine Prüfung der Maßnahme ein.

3. Prüfung und Entscheidung der Kommission

- Auf Grundlage der Konsultationen und ihrer Prüfung entscheidet die Kommission, ob die nationale Maßnahme gerechtfertigt ist.
- Die Entscheidung ergeht innerhalb von sechs Monaten (bzw 60 Tagen bei Artikel 5-Verstößen) ab Eingang der Notifizierung.
- Die Kommission teilt ihre Entscheidung sowohl der betroffenen Marktüberwachungsbehörde als auch allen übrigen Marktüberwachungsbehörden mit.

Beispiel: *Eine Behörde meldet ein KI-System, das verbotene biometrische Überwachung durchführt. Die Kommission entscheidet innerhalb von 60 Tagen, ob ein unionsweites Verbot verhängt wird.*

C. Folgen der Entscheidung

- **Maßnahme gerechtfertigt**: Alle Mitgliedstaaten müssen vergleichbare Maßnahmen treffen, zB Rücknahme vom Markt.
- **Maßnahme nicht gerechtfertigt**: Ursprünglicher Mitgliedstaat muss die Maßnahme zurücknehmen.

Beispiel: *Die Kommission bestätigt, dass ein System Sicherheitsrisiken birgt. Dann müssen alle Mitgliedstaaten den Vertrieb dieses Systems verbieten.*

D. Zusammenhang mit Normenmängeln

- Wenn ein Problem auf fehlerhafte **harmonisierte Normen oder Spezifikationen** (Artikel 40 KI-VO **und** Artikel 41 KI-VO) zurückgeht, muss die Kommission nach Verordnung (EU) Nr 1025/2012 das Verfahren zur Überarbeitung dieser Normen einleiten.

Beispiel: *Ein KI-System erfüllt zwar die harmonisierte Norm, zeigt aber trotzdem gefährliche Fehler. Dann prüft die Kommission die Norm selbst und veranlasst eine Korrektur.*

E. Besonderheiten

- **Schnellverfahren bei Artikel 5 KI-VO**: Verstöße gegen verbotene KI-Praktiken (zB Social Scoring) lösen besonders kurze Fristen aus.
- **Unionsweite Wirkung**: Die Entscheidung der Kommission wirkt wie ein Hebel, damit nicht jedes Land unterschiedlich reagiert.
- **Schutz von Grundrechten**: Nach Erwägungsgrund 157 dient das Verfahren besonders dazu, Risiken für Gesundheit, Sicherheit und Grundrechte rasch abzustellen.

III. Zusammenfassung

Zweck	Einheitliche EU-weite Lösung bei Konflikten über nationale Maßnahmen gegen KI-Systeme
Ablauf	Einwand → Konsultation → Prüfung durch Kommission → Entscheidung
Fristen	drei Monate/sechs Monate allgemein, 30 Tage/60 Tage bei verbotenen Praktiken
Folgen	Gerechtfertigt → EU-weite Maßnahmen; nicht gerechtfertigt → Rücknahme der nationalen Maßnahme
Besonderheit	Prüfung auch von Normen und Spezifikationen möglich

IV. Quellenverzeichnis

- Erwägungsgründe 153, 156, 157 KI-VO (EU) 2024/1689

Artikel 82 KI-VO

Konforme KI-Systeme, die ein Risiko bergen

(1) Stellt die Marktüberwachungsbehörde eines Mitgliedstaats — nach einer Konsultation der in Artikel 77 Absatz 1 genannten betreffenden nationalen Behörde — nach der gemäß Artikel 79 durchgeführten Prüfung fest, dass ein Hochrisiko-KI-System zwar dieser Verordnung entspricht, aber dennoch ein Risiko für die Gesundheit oder Sicherheit von Personen, für die Grundrechte oder für andere Aspekte des Schutzes öffentlicher Interessen darstellt, so fordert sie unverzüglich den betreffenden Akteur auf, alle geeigneten Maßnahmen zu treffen, damit das betreffende KI-System zum Zeitpunkt des Inverkehrbringens oder der Inbetriebnahme dieses Risiko nicht mehr birgt, und zwar innerhalb einer Frist, die sie vorgeben kann.

(2) Der Anbieter oder der andere einschlägige Akteur sorgt dafür, dass in Bezug auf alle betroffenen KI-Systeme, die er auf dem Unionsmarkt bereitgestellt hat, innerhalb der Frist, die von der in Absatz 1 genannten Marktüberwachungsbehörde des Mitgliedstaats vorgegeben wurde, Korrekturmaßnahmen ergriffen werden.

(3) Die Mitgliedstaaten unterrichten unverzüglich die Kommission und die anderen Mitgliedstaaten über Feststellungen gemäß Absatz 1. Diese Unterrichtung enthält alle vorliegenden Angaben, insbesondere die für die Identifizierung des betreffenden KI-Systems notwendigen Daten, den Ursprung und die Lieferkette des KI-Systems, die Artikel des sich daraus ergebenden Risikos sowie die Artikel und Dauer der ergriffenen nationalen Maßnahmen.

(4) Die Kommission nimmt unverzüglich mit den betreffenden Mitgliedstaaten und den jeweiligen Akteuren Konsultationen auf und prüft die ergriffenen nationalen Maßnahmen. Anhand der Ergebnisse dieser Prüfung entscheidet die Kommission, ob die Maßnahme gerechtfertigt ist, und schlägt, falls erforderlich, weitere geeignete Maßnahmen vor.

(5) Die Kommission teilt ihren Beschluss unverzüglich den betroffenen Mitgliedstaaten und den jeweiligen Akteuren mit. Sie unterrichtet auch die übrigen Mitgliedstaaten.

I. Worum geht es?

Artikel 82 regelt Fälle, in denen ein KI-System zwar alle Vorschriften der KI-VO erfüllt und formal konform ist, aber trotzdem ein Risiko für Menschen oder öffentliche Interessen darstellt. Die Norm stellt damit eine Artikel "Sicherheitsnetz" dar: Auch bei vollständiger Rechtskonformität darf ein gefährliches KI-System nicht einfach weiterlaufen. Ziel ist es, den Schutz von Gesundheit, Sicherheit, Grundrechten und öffentlichem Interesse auch über die bloße Normkonformität hinaus sicherzustellen.

II. Detailkommentar

A. Feststellung eines Risikos

- **Marktüberwachungsbehörde**: Sie prüft, ob trotz Konformität ein Risiko vorliegt. Grundlage dafür ist die Prüfung nach Artikel 79 KI-VO.
- **Konsultationspflicht**: Vor einer Entscheidung muss die Behörde die zuständige nationale Fachbehörde einbinden (Artikel 77 KI-VO Absatz 1).
- **Risikobereich**: Betroffen sind Gesundheit, Sicherheit, Grundrechte oder sonstige öffentliche Interessen. Damit ist der Anwendungsbereich sehr weit.

Beispiel: *Ein KI-System zur Kreditbewertung ist formal konform, stellt sich aber in der Praxis als diskriminierend gegenüber bestimmten Personengruppen heraus. Die Behörde muss einschreiten.*

B. Maßnahmen der Akteure

- **Pflicht zur Korrektur**: Der Anbieter oder ein anderer relevanter Akteur (zB Importeur) muss das Risiko beseitigen.
- **Fristsetzung**: Die Behörde legt eine Frist fest, bis wann die Korrekturmaßnahmen erfolgen müssen.
- **Geltung für alle Systeme**: Die Korrektur betrifft nicht nur das einzelne Produkt, sondern alle bereits auf dem Markt befindlichen betroffenen Systeme.

Beispiel: *Ein KI-gestütztes Diagnosesystem für Ärzte zeigt in seltenen Fällen falsche Warnmeldungen an, die Patienten verunsichern. Der Anbieter muss ein Software-Update für alle Geräte ausspielen.*

C. Informationspflichten der Mitgliedstaaten

- **Meldung an die Kommission**: Sobald ein Risiko festgestellt wird, muss der betroffene Mitgliedstaat die Kommission und die anderen Mitgliedstaaten informieren.
- **Inhalt der Meldung**: Erforderlich sind ua Identifikationsdaten des Systems, Angaben zur Lieferkette, Beschreibung des Risikos und der ergriffenen Maßnahmen.

Beispiel: *Ein Mitgliedstaat stellt Sicherheitsmängel bei einem KI-basierten Robotiksystem fest und informiert die EU-Organe, damit auch andere Staaten gewarnt sind.*

D. Rolle der Kommission

- **Konsultation und Prüfung**: Die Kommission prüft gemeinsam mit den Mitgliedstaaten und den betroffenen Akteuren, ob die Maßnahmen gerechtfertigt sind.
- **Entscheidungskompetenz**: Sie entscheidet, ob die Maßnahmen bleiben, geändert oder aufgehoben werden sollen.
- **Vorgeschlagene Maßnahmen**: Falls nötig, kann die Kommission zusätzliche Maßnahmen auf EU-Ebene anstoßen.

Beispiel: *Die Kommission bestätigt eine nationale Maßnahme und empfiehlt allen Mitgliedstaaten, den Verkauf des Systems bis zur Fehlerbehebung zu stoppen.*

E. Besondere Aspekte

- **Verhältnis zur Konformität**: Auch ein konformes System kann gefährlich sein. Artikel 82 zeigt, dass Sicherheit Vorrang vor reiner Normkonformität hat.

- **Breiter Risikobegriff**: Nicht nur körperliche Gefahren, sondern auch Grundrechtsverstöße (zB Diskriminierung) sind umfasst.
- **Europäische Koordination**: Nationale Alleingänge sollen vermieden werden, indem die Kommission koordiniert.

III. Zusammenfassung

Risikofeststellung	Auch konforme Systeme können gefährlich sein, Prüfung durch Marktüberwachungsbehörden
Pflichten der Akteure	Anbieter müssen Korrekturmaßnahmen für alle betroffenen Systeme umsetzen
Informationspflichten	Mitgliedstaaten müssen Kommission und andere Staaten informieren
Rolle der Kommission	Prüfung und Koordination, ggf. EU-weite Maßnahmen
Schwerpunkt	Schutz von Gesundheit, Sicherheit, Grundrechten und öffentlichen Interessen über Konformität hinaus

Artikel 83 KI-VO

Formale Nichtkonformität

(1) Wenn die Marktüberwachungsbehörde eines Mitgliedstaats eine der folgenden Nichtkonformitäten feststellt, fordert sie den jeweiligen Anbieter auf, diese binnen einer Frist, die sie vorgeben kann, zu beheben:

a) die CE-Kennzeichnung wurde unter Verstoß gegen Artikel 48 angebracht;

b) es wurde keine CE-Kennzeichnung angebracht;

c) es wurde keine EU-Konformitätserklärung gemäß Artikel 47 ausgestellt;

d) es wurde keine EU-Konformitätserklärung gemäß Artikel 47 ordnungsgemäß ausgestellt;

e) es wurde keine Registrierung in der EU-Datenbank gemäß Artikel 71 vorgenommen;

f) es wurde kein Bevollmächtigter — sofern erforderlich — ernannt;

g) es ist keine technische Dokumentation verfügbar.

(2) Besteht die Nichtkonformität nach Absatz 1 weiter, so ergreift die Marktüberwachungsbehörde des betreffenden Mitgliedstaats geeignete und verhältnismäßige Maßnahmen, um die Bereitstellung des Hochrisiko-KI-Systems auf dem Markt zu beschränken oder zu verbieten oder um dafür zu sorgen, dass es unverzüglich zurückgerufen oder vom Markt genommen wird.

I. Worum geht es?

Artikel 83 regelt, wie die Behörden vorgehen, wenn ein Anbieter von KI-Systemen bestimmte formale Pflichten nicht erfüllt. Es geht also nicht um technische Mängel des Systems selbst, sondern um fehlende Unterlagen oder Kennzeichnungen. Ziel ist es, die Einhaltung der Verwaltungs- und Nachweispflichten sicherzustellen, damit Transparenz und Kontrolle gewährleistet sind.

II. Detailkommentar

A. Ausgangspunkt

- **Formale Mängel**: Gemeint sind Fehler wie fehlende Kennzeichnung, fehlende Erklärungen oder unvollständige Dokumentation.
- **Abgrenzung**: Es geht nicht um funktionale oder sicherheitsrelevante Defekte, sondern um Verstöße gegen Dokumentations- und Kennzeichnungspflichten.

B. Typische Fälle

1. CE-Kennzeichnung

- **Pflicht**: Jedes Hochrisiko-KI-System muss eine CE-Kennzeichnung tragen, die die Konformität bestätigt.
- **Fehlerfälle**: Entweder wird sie gar nicht angebracht oder falsch angebracht.

Beispiel: *Ein Anbieter verkauft ein KI-System ohne CE-Zeichen, obwohl es verpflichtend wäre.*

2. EU-Konformitätserklärung

- **Pflicht**: Der Anbieter muss eine Konformitätserklärung **nach** Artikel 47 KI-VO ausstellen.
- **Fehlerfälle**: Erklärung fehlt völlig oder ist fehlerhaft erstellt.

Beispiel: *Ein Unternehmen legt nur eine unvollständige Konformitätserklärung vor, die zentrale Angaben wie den Geltungsbereich nicht enthält.*

3. Registrierung in EU-Datenbank

- **Pflicht**: Hochrisiko-KI-Systeme müssen in einer zentralen EU-Datenbank registriert sein (Artikel 71 KI-VO).
- **Fehlerfall**: Anbieter überspringt diesen Schritt.

Beispiel: *Ein Start-up bringt eine neue KI-Software auf den Markt, ohne sie in die Datenbank einzutragen.*

4. Bevollmächtigter

- **Pflicht**: Wenn Anbieter außerhalb der EU sitzen, müssen sie einen Bevollmächtigten in der EU benennen.
- **Fehlerfall**: Keiner

Beispiel: *Ein US-Unternehmen vertreibt KI-Systeme in der EU, ohne einen Ansprechpartner in der EU zu benennen*.

5. Technische Dokumentation

- **Pflicht**: Anbieter müssen eine technische Dokumentation bereithalten.
- **Fehlerfall**: Dokumentation ist nicht vorhanden oder unzugänglich.

Beispiel: B*ei einer Marktüberprüfung kann der Hersteller keine technischen Unterlagen vorlegen*.

C. Rechtsfolgen

1. Aufforderung zur Nachbesserung

- **Erstes Mittel**: Die Marktüberwachungsbehörde fordert den Anbieter auf, den Mangel zu beheben.
- **Fristsetzung**: Die Behörde legt eine Frist fest.

2. Folgen bei Untätigkeit

- Wenn der Anbieter nicht reagiert, darf die Behörde weitere Maßnahmen ergreifen.
- **Mögliche Maßnahmen**:
    - Beschränkung der Bereitstellung,
    - Verbot des Inverkehrbringens,
    - Rückruf oder Entfernung vom Markt.

Beispiel: *Ein Hersteller ignoriert wiederholt Aufforderungen zur Nachbesserung – die Behörde verbietet den Vertrieb seines KI-Systems.*

D. Besonderheiten

- **Verhältnismäßigkeit**: Maßnahmen der Behörden müssen angemessen sein, also nur so weit gehen, wie nötig.
- **Fokus auf Hochrisiko-Systeme**: Artikel 83 betrifft vor allem Hochrisiko-KI-Systeme, weil für diese strenge formale Anforderungen gelten.

III. Zusammenfassung

Ziel	Sicherstellung der formalen Pflichten wie CE-Kennzeichnung, Erklärungen, Registrierung
Typische Verstöße	Fehlende/fehlerhafte CE-Kennzeichnung, keine oder unvollständige EU-Konformitätserklärung, fehlende Registrierung, kein Bevollmächtigter, keine technische Dokumentation
Vorgehen der Behörden	Aufforderung zur Nachbesserung mit Fristsetzung 2. Bei Untätigkeit: Beschränkung, Verbot, Rückruf oder Marktentzug
Grundsatz	Maßnahmen müssen verhältnismäßig sein

Artikel 84 KI-VO

Unionsstrukturen zur Unterstützung der Prüfung von KI

(1) Die Kommission benennt eine oder mehrere Unionsstrukturen zur Unterstützung der Prüfung von KI, die die Aufgaben gemäß Artikel 21 Absatz 6 der Verordnung (EU) 2019/1020 im KI-Bereich wahrnehmen.

(2) Unbeschadet der in Absatz 1 genannten Aufgaben leisten die Unionsstrukturen zur Unterstützung der Prüfung von KI auf Anfrage des KI-Gremiums, der Kommission oder der Marktüberwachungsbehörden auch unabhängige technische oder wissenschaftliche Beratung.

I. Worum geht es?

Artikel 84 KI-VO regelt die Einrichtung besonderer Unionsstrukturen, die die Prüfung und Bewertung von KI-Systemen unterstützen sollen. Ziel ist es, eine europaweit einheitliche Expertise bereitzustellen, damit Marktüberwachungsbehörden, die Kommission und das KI-Gremium bei technischen und wissenschaftlichen Fragen zur KI-VO fachlich unterstützt werden. Damit wird eine zentrale Fachkompetenz geschaffen, die die Umsetzung der KI-VO erleichtert und die Qualität von Prüfungen verbessert.

II. Detailkommentar

A. Einrichtung von Unionsstrukturen

- **Benennung durch die Kommission**: Die Europäische Kommission entscheidet, welche Einrichtungen oder Stellen als „Unionsstrukturen" eingesetzt werden.
- **Mehrere Strukturen möglich**: Es kann eine einzige Stelle oder ein Netzwerk aus verschiedenen Einrichtungen sein.
- **Anknüpfungspunkt zu Verordnung (EU) 2019/1020**: Die Unionsstrukturen übernehmen im Bereich KI dieselben Aufgaben, die dort für andere Produktprüfungen festgelegt sind (zB Unterstützung der Marktüberwachung durch technische Prüfungen).

Beispiel: *Die Kommission könnte ein bestehendes europäisches Forschungsinstitut für KI-Sicherheit als Unionsstruktur ernennen, das dann technische Prüfungen von Hochrisiko-KI-Systemen vornimmt.*

B. Aufgabenbereich

1. Unterstützung nach Artikel 21 Absatz 6 VO 2019/1020

- Diese Vorschrift sieht vor, dass bestimmte Unionsstrukturen die Arbeit nationaler Marktüberwachungsbehörden durch Prüfungen und Gutachten ergänzen.
- Im KI-Bereich bedeutet das: Die Strukturen können KI-Systeme technisch testen, analysieren und bewerten.

2. Beratungsfunktion

- **Adressaten**: KI-Gremium, Kommission, Marktüberwachungsbehörden.
- **Inhalt**: Technische oder wissenschaftliche Beratung, unabhängig von politischen oder wirtschaftlichen Interessen.
- **Anlass**: Auf Anfrage, d.h. nur wenn die Institutionen eine konkrete Frage oder einen Bedarf haben.

Beispiel: *Eine Marktüberwachungsbehörde ist unsicher, ob ein KI-System, das Bewerbungsunterlagen sortiert, unter die Hochrisiko-Kategorie fällt. Sie kann die Unionsstruktur um ein wissenschaftliches Gutachten bitten.*

C. Besonderheiten

- **Unabhängigkeit**: Die Beratung muss neutral und fachlich fundiert sein, um Vertrauen zu schaffen.
- **Flexibilität**: Die Kommission kann die Strukturen dynamisch anpassen (zB bei neuen technischen Entwicklungen).
- **Koordinierungsfunktion**: Die Strukturen erleichtern die Zusammenarbeit zwischen den Mitgliedstaaten und verhindern widersprüchliche nationale Bewertungen.

Beispiel: *Ein Mitgliedstaat bewertet ein KI-System als Hochrisiko, ein anderer nicht. Die Unionsstruktur kann eine einheitliche Einschätzung geben, um Konflikte zu lösen.*

III. Zusammenfassung

Einrichtung	Die Kommission benennt eine oder mehrere Unionsstrukturen zur Prüfung von KI.
Aufgaben	Unterstützung nach Artikel 21 Absatz 6 VO 2019/1020 sowie Beratung bei technischen und wissenschaftlichen Fragen.
Adressaten	KI-Gremium, Kommission, Marktüberwachungsbehörden.
Ziel	Einheitliche, unabhängige Expertise für die Anwendung der KI-VO.

Artikel 85 KI-VO

Recht auf Beschwerde bei einer Marktüberwachungsbehörde

Unbeschadet anderer verwaltungsrechtlicher oder gerichtlicher Rechtsbehelfe kann jede natürliche oder juristische Person, die Grund zu der Annahme hat, dass gegen die Bestimmungen dieser Verordnung verstoßen wurde, bei der betreffenden Marktüberwachungsbehörde Beschwerden einreichen.

Gemäß der Verordnung (EU) 2019/1020 werden solche Beschwerden für die Zwecke der Durchführung von Marktüberwachungstätigkeiten berücksichtigt und nach den einschlägigen von den Marktüberwachungsbehörden dafür eingerichteten Verfahren behandelt.

I. Worum geht es?

Artikel 85 KI-VO gibt jeder Person – also sowohl Privatpersonen als auch Unternehmen – das Recht, bei einer Marktüberwachungsbehörde Beschwerde einzulegen, wenn sie einen Verstoß gegen die Verordnung vermuten. Ziel ist es, einen einfachen und niederschwelligen Zugang zu schaffen, damit mögliche Verstöße gegen die KI-VO erkannt und verfolgt werden können. Dieses Recht besteht zusätzlich zu anderen möglichen Rechtswegen (zB Klagen vor Gerichten). Ein Recht, Abhilfemaßnahmen vom mutmaßlichen Verletzer zu fordern, erhält man durch diese Regelung aber nicht.

II. Detailkommentar

A. Adressatenkreis

- **Natürliche Personen**: Jede Privatperson kann Beschwerde erheben, auch ohne persönlich betroffen zu sein. Es reicht der begründete Verdacht auf einen Verstoß.
- **Juristische Personen**: Auch Unternehmen, Verbände oder Organisationen dürfen Beschwerde einlegen.
- **Kein Erfordernis der Betroffenheit**: Anders als bei vielen klassischen Rechtsmitteln ist keine persönliche Rechtsverletzung nötig. Schon der Verdacht genügt.

Beispiel: *Ein Verbraucher entdeckt, dass ein Online-Dienst ein KI-System nutzt, das möglicherweise nicht den Transparenzpflichten entspricht. Auch wenn er selbst nicht direkt betroffen ist, darf er Beschwerde einreichen.*

B. Gegenstand der Beschwerde

- **Verstöße gegen die KI-VO**: Jede Form der Nichtbeachtung, egal ob es sich um Hochrisiko-KI-Systeme oder andere Pflichten handelt.
- **Bezug zur Marktüberwachung**: Beschwerden werden im Rahmen der Marktüberwachung berücksichtigt. Dies bedeutet, dass die Behörden prüfen, ob ein Verstoß vorliegt und ggf. Maßnahmen einleiten.

Beispiel: *Ein Start-up meldet, dass ein Konkurrent sein KI-System ohne vorgeschriebene Konformitätsbewertung vertreibt.*

C. Verfahren

- **Verweis auf Verordnung (EU) 2019/1020**: Diese regelt die allgemeine Marktüberwachung in der EU und legt fest, wie Beschwerden behandelt werden.
- **Verfahren nach nationalem Recht**: Jede Marktüberwachungsbehörde hat eigene Verfahren, die eingehalten werden müssen.
- **Berücksichtigungspflicht**: Die Behörde muss jede Beschwerde prüfen, kann aber im Rahmen ihres Ermessens entscheiden, ob und wie sie weiter vorgeht.

Beispiel: *Eine NGO reicht eine Beschwerde gegen den Einsatz einer Gesichtserkennungssoftware im öffentlichen Raum ein. Die Behörde prüft, ob das System tatsächlich den Hochrisiko-Vorgaben entspricht.*

D. Verhältnis zu anderen Rechtsbehelfen

- **Unbeschadet anderer Rechtswege**: Das Beschwerderecht ergänzt andere Rechtsmittel wie gerichtliche Klagen oder verwaltungsrechtliche Anträge.

- **Parallel möglich**: Eine Person kann gleichzeitig Beschwerde bei der Behörde einlegen und vor Gericht gehen.

III. Zusammenfassung

Beschwerderecht	Jede natürliche oder juristische Person kann Beschwerde einlegen.
Kein Betroffenheitserfordernis	Es genügt, wenn ein Verstoß vermutet wird.
Bezug zur Marktüberwachung	Beschwerden werden von den Behörden im Rahmen ihrer Überwachung geprüft.
Verfahren	Behandlung nach nationalen Vorschriften und EU-Verordnung 2019/1020.
Zusätzlich zu anderen Rechtswegen	Beschwerden schließen andere Klagen oder Rechtsbehelfe nicht aus.

IV. Quellenverzeichnis

- Erwägungsgründe 159, 160 KI-VO (EU) 2024/1689

Artikel 86 KI-VO

Recht auf Erläuterung der Entscheidungsfindung im Einzelfall

(1) Personen, die von einer Entscheidung betroffen sind, die der Betreiber auf der Grundlage der Ausgaben eines in Anhang III aufgeführten Hochrisiko-KI-Systems, mit Ausnahme der in Nummer 2 des genannten Anhangs aufgeführten Systeme, getroffen hat und die rechtliche Auswirkungen hat oder sie in ähnlicher Artikel erheblich auf eine Weise beeinträchtigt, die ihrer Ansicht nach ihre Gesundheit, ihre Sicherheit oder ihre Grundrechte beeinträchtigt, haben das Recht, vom Betreiber eine klare und aussagekräftige Erläuterung zur Rolle des KI-Systems im Entscheidungsprozess und zu den wichtigsten Elementen der getroffenen Entscheidung zu erhalten.

(2) Absatz 1 gilt nicht für die Verwendung von KI-Systemen, bei denen sich Ausnahmen von oder Beschränkungen der Pflicht nach dem genannten Absatz aus dem Unionsrecht oder dem nationalen Recht im Einklang mit dem Unionsrecht ergeben.

(3) Dieser Artikel gilt nur insoweit, als das Recht gemäß Absatz 1 nicht anderweitig im Unionsrecht festgelegt ist.

I. Worum geht es?

Dieser Artikel gibt betroffenen Personen das Recht, eine **Erläuterung** zu erhalten, wenn eine für sie wichtige Entscheidung mithilfe eines Hochrisiko-KI-Systems getroffen wird. Ziel ist es, die Entscheidungsfindung **nachvollziehbar** und **transparent** zu machen. Die Norm stellt damit eine wichtige Schnittstelle zwischen technischer KI-Nutzung und dem Schutz der Grundrechte dar.

II. Detailkommentar

A. Anwendungsbereich

- **Betroffene Personen**: Gemeint sind alle Personen, die von einer Entscheidung eines Betreibers eines Hochrisiko-KI-Systems unmittelbar betroffen sind.

- **Voraussetzungen**: Die Entscheidung muss entweder rechtliche Wirkung entfalten (zB Ablehnung eines Antrags) oder die Person erheblich beeinträchtigen (zB Auswirkungen auf Gesundheit oder Berufschancen).
- **Ausgeschlossene Systeme**: KI-Systeme aus Anhang III KI-VO Nr 2 (kritische Infrastruktur) sind nicht erfasst.

Beispiel: *Eine Bank lehnt auf Grundlage eines KI-gestützten Kreditbewertungssystems einen Kredit ab. Die betroffene Person kann eine Erläuterung verlangen, wie das System in die Entscheidung eingeflossen ist.*

B. Inhalt der Erläuterung

- **Rolle des KI-Systems**: Es muss erklärt werden, welchen Beitrag das KI-System im Entscheidungsprozess hatte (zB Empfehlung, automatische Entscheidung, unterstützende Analyse).
- **Wesentliche Elemente**: Es sind die Schlüsselfaktoren darzustellen, die zur Entscheidung geführt haben (zB bestimmte Risikoparameter oder Datenpunkte).
- **Klar und aussagekräftig**: Die Erklärung muss verständlich und nachvollziehbar sein, nicht nur technisch oder abstrakt. Die betroffene Person muss durch diese Erläuterung ihre Rechte ausüben können.

Beispiel: *Eine Behörde teilt einer Bewerberin mit, dass ein KI-System ihr Qualifikationsprofil anhand bestimmter Kriterien bewertet hat und diese Kriterien die Entscheidung beeinflusst haben.*

C. Ausnahmen und Beschränkungen

- **Rechtsgrundlagen**: Wenn Unionsrecht oder nationales Recht im Einklang mit Unionsrecht Einschränkungen oder Ausnahmen vorsieht, entfällt die Pflicht zur Erläuterung.
- **Schutzinteressen**: Dies kann insbesondere im Bereich der öffentlichen Sicherheit oder der Strafverfolgung relevant sein.

D. Verhältnis zu anderem Unionsrecht

- **Subsidiarität**: Das Recht auf Erläuterung nach Artikel 86 gilt nur dann, wenn es nicht bereits durch andere EU-Vorschriften geregelt ist (zB Datenschutz-Grundverordnung).

E. Besonderheiten

- **Abgrenzung zu Transparenzpflichten**: Während viele Transparenzpflichten ex ante bestehen (zB Information über Funktionsweise des Systems), knüpft Artikel 86 an eine konkrete individuelle Entscheidung an.
- **Stärkung der Grundrechte**: Die Norm schützt insbesondere die Rechte auf effektiven Rechtsschutz und informationelle Selbstbestimmung.

III. Zusammenfassung

Anwendungsbereich	Betroffene Personen bei Entscheidungen durch Hochrisiko-KI-Systeme (außer kritische Infrastruktur)
Voraussetzung	Entscheidung mit rechtlicher Wirkung oder erheblicher Beeinträchtigung
Anspruch	Klare und aussagekräftige Erläuterung zur Rolle des KI-Systems und den wesentlichen Entscheidungselementen
Ausnahmen	Einschränkungen durch Unions- oder nationales Recht möglich
Verhältnis	Gilt nur subsidiär, wenn kein anderer EU-Rechtsakt bereits ein entsprechendes Recht vorsieht

IV. Quellenverzeichnis

- Erwägungsgründe 159, 160 KI-VO (EU) 2024/1689

Artikel 87 KI-VO

Meldung von Verstößen und Schutz von Hinweisgebern

Für die Meldung von Verstößen gegen diese Verordnung und den Schutz von Personen, die solche Verstöße melden, gilt die Richtlinie (EU) 2019/1937.

I. Worum geht es?

Dieser Artikel stellt klar, dass für die Meldung von Verstößen gegen die KI-VO und den Schutz von Hinweisgebern die Regeln der sogenannten **Whistleblower-Richtlinie** (Richtlinie (EU) 2019/1937) gelten. Damit wird ein einheitlicher Schutzstandard geschaffen. Personen, die Verstöße melden, sollen keine Nachteile erleiden und rechtlich abgesichert sein.

II. Detailkommentar

A. Bezug zur Whistleblower-Richtlinie

- **Direkter Verweis**: Artikel 87 verweist vollständig auf die Whistleblower-Richtlinie. Es gibt keine zusätzlichen Vorschriften innerhalb der KI-VO.
- **Schutzbereich**: Erfasst werden Personen, die Verstöße gegen die KI-VO melden, zB Mitarbeiter eines Unternehmens oder auch externe Personen.
- **Rechtsfolgen**: Hinweisgeber genießen Schutz vor Repressalien wie Kündigung, Diskriminierung oder sonstigen Benachteiligungen.

Beispiel: *Ein Mitarbeiter eines Softwareunternehmens meldet anonym, dass sein Arbeitgeber ein KI-System ohne die vorgeschriebene Konformitätsbewertung auf den Markt bringt. Der Mitarbeiter darf deswegen nicht entlassen oder beruflich benachteiligt werden.*

B. Adressaten und Verfahren

- **Adressaten**: Die Meldung kann sich an interne Stellen (zB Compliance-Abteilungen), an Behörden oder auch an die Öffentlichkeit richten – jeweils nach den Vorgaben der Richtlinie.

- **Meldestellen**: Unternehmen ab einer bestimmten Größe sind verpflichtet, interne Meldesysteme einzurichten.
- **Anwendungsbereich**: Die Regelung gilt unabhängig davon, ob es sich um Hochrisiko-KI oder um andere Verstöße handelt.

Beispiel: *Eine NGO deckt auf, dass ein KI-System zur biometrischen Überwachung ohne gesetzliche Grundlage eingesetzt wird. Auch die NGO-Mitarbeiter, die den Verstoß melden, sind geschützt.*

C. Besonderheiten

- **Keine Sonderregeln in der KI-VO**: Artikel 87 ergänzt die KI-VO nicht um eigene Vorgaben, sondern verweist vollständig auf die bestehende Richtlinie.
- **Systematische Einordnung**: Der Artikel steht am Ende der Verordnung, da er eine Querschnittsregelung darstellt, die für alle Verstöße gilt.

III. Zusammenfassung

Schutzstandard	Es gilt die Whistleblower-Richtlinie 2019/1937
Geschützte Personen	Hinweisgeber von Verstößen gegen die KI-VO
Schutzumfang	Verbot von Repressalien, Recht auf Anonymität, rechtliche Absicherung
Anwendungsbereich	Alle Verstöße gegen die KI-VO, unabhängig vom Bereich

IV. Quellenverzeichnis

- Erwägungsgrund 172 KI-VO (EU) 2024/1689

Artikel 88 KI-VO

Durchsetzung der Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

(1) Die Kommission verfügt unter Berücksichtigung der Verfahrensgarantien nach Artikel 94 über ausschließliche Befugnisse zur Beaufsichtigung und Durchsetzung von Kapitel V. Unbeschadet der Organisationsbefugnisse der Kommission und der Aufteilung der Zuständigkeiten zwischen den Mitgliedstaaten und der Union auf der Grundlage der Verträge überträgt die Kommission dem Büro für Künstliche Intelligenz die Durchführung dieser Aufgaben.

(2) Unbeschadet des Artikels 75 Absatz 3 können die Marktüberwachungsbehörden die Kommission ersuchen, die in diesem Abschnitt festgelegten Befugnisse auszuüben, wenn es erforderlich und verhältnismäßig ist, um die Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung zu unterstützen.

I. Worum geht es?

Artikel 88 regelt die Durchsetzung der Vorschriften für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck. Er legt fest, dass die Aufsicht zentral bei der EU-Kommission liegt, die diese Aufgabe wiederum an das Büro für Künstliche Intelligenz überträgt. Nationale Marktüberwachungsbehörden können zwar unterstützen, haben aber in diesem speziellen Bereich keine Hauptzuständigkeit.

II. Detailkommentar

A. Zentrale Zuständigkeit der Kommission

- **Exklusive Befugnisse**: Nur die Kommission ist für die Durchsetzung der Regeln in Kapitel V verantwortlich. Nationale Behörden haben hier keine eigene Durchsetzungsbefugnis.
- **Büro für Künstliche Intelligenz**: Die praktische Durchführung übernimmt dieses spezialisierte EU-Gremium. Es verfügt über Fachwissen und fungiert faktisch wie eine Marktüberwachungsbehörde.

- **Verfahrensgarantien**: Die Kommission muss dabei stets die Vorgaben aus Artikel 94 KI-VO beachten, die Schutzrechte wie Anhörung und Rechtsmittel sichern.

Beispiel: *Ein großer Anbieter bringt ein KI-Modell heraus, das von vielen Unternehmen weiterverwendet wird. Bei einem Verdacht auf Regelverstöße ist ausschließlich die Kommission zuständig, nicht die nationale Behörde.*

B. Zusammenarbeit mit Marktüberwachungsbehörden

- **Antragsrecht**: Nationale Behörden können die Kommission ersuchen, tätig zu werden. Dies ist jedoch nur bei **Erforderlichkeit und Verhältnismäßigkeit** vorgesehen.
- **Unterstützungsfunktion**: Die nationalen Stellen bleiben zuständig für KI-Systeme allgemein. Sie können sich aber an die Kommission wenden, wenn sie ohne deren Mitwirkung nicht weiterkommen.
- **Praxisrelevanz**: Dadurch wird verhindert, dass nationale Behörden in Fällen ohne ausreichenden Zugang zu Modell-Informationen blockiert sind.

Beispiel: *Eine nationale Behörde untersucht ein hochriskantes KI-System, das auf einem allgemeinen Modell basiert. Da sie keinen Zugriff auf die Modellinformationen hat, bittet sie die Kommission um Unterstützung.*

C. Besonderheiten

- **Vermeidung von Doppelzuständigkeiten**: Die klare Abgrenzung soll sicherstellen, dass es keine widersprüchlichen Entscheidungen zwischen nationaler und europäischer Ebene gibt.
- **Synergieeffekte**: Die Zentralisierung beim Büro für Künstliche Intelligenz bündelt Expertise und sorgt für eine einheitliche Anwendung des Rechts.
- **Subsidiäre Rolle der Mitgliedstaaten**: Nationale Behörden bleiben wichtig, spielen aber eine ergänzende Rolle und greifen nur ein, wenn die Kommission Unterstützung braucht oder von ihnen darum gebeten wird.

III. Zusammenfassung

Zuständigkeit	Exklusiv bei der EU-Kommission
Durchführung	Büro für Künstliche Intelligenz
Rolle der Mitgliedstaaten	Unterstützend, auf Antrag
Ziel	Einheitliche Aufsicht, Vermeidung von Doppelzuständigkeiten

IV. Quellenverzeichnis

- Erwägungsgründe 161, 162 KI-VO (EU) 2024/1689

Artikel 89 KI-VO

Überwachungsmaßnahmen

(1) Zur Wahrnehmung der ihr in diesem Abschnitt übertragenen Aufgaben kann das Büro für Künstliche Intelligenz die erforderlichen Maßnahmen ergreifen, um die wirksame Umsetzung und Einhaltung dieser Verordnung durch Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, einschließlich der Einhaltung genehmigter Praxisleitfäden, zu überwachen.

(2) Nachgelagerte Anbieter haben das Recht, eine Beschwerde wegen eines Verstoßes gegen diese Verordnung einzureichen. Eine Beschwerde ist hinreichend zu begründen und enthält mindestens Folgendes:

a) die Kontaktstelle des Anbieters des betreffenden KI-Modells mit allgemeinem Verwendungszweck;

b) eine Beschreibung der einschlägigen Fakten, die betreffenden Bestimmungen dieser Verordnung und die Begründung, warum der nachgelagerte Anbieter der Auffassung ist, dass der Anbieter des KI-Modells mit allgemeinem Verwendungszweck gegen diese Verordnung verstoßen hat;

c) alle sonstigen Informationen, die der nachgelagerte Anbieter, der die Anfrage übermittelt hat, für relevant hält, gegebenenfalls einschließlich Informationen, die er auf eigene Initiative hin zusammengetragen hat.

I. Worum geht es?

Artikel 89 regelt die **Überwachungsmaßnahmen** für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck. Das Büro für Künstliche Intelligenz erhält Befugnisse, um die Einhaltung der Verordnung sicherzustellen. Zudem wird ein **Beschwerderecht für nachgelagerte Anbieter** geschaffen, die von einem möglichen Verstoß betroffen sind. Ziel ist es, Transparenz, Kontrolle und effektive Durchsetzung auf Unionsebene zu gewährleisten.

II. Detailkommentar

A. Befugnisse des Büros für Künstliche Intelligenz

- **Überwachungsbefugnis**: Das Büro darf alle notwendigen Maßnahmen ergreifen, um sicherzustellen, dass Anbieter von KI-Modellen mit allgemeinem Verwendungszweck die Vorschriften einhalten.
- **Umsetzung und Einhaltung**: Die Befugnis umfasst die Kontrolle der Anwendung von genehmigten Praxisleitfäden.
- **Unionsebene**: Das Büro wirkt als zentrale Aufsichtsbehörde, um parallele nationale Zuständigkeiten zu vermeiden und einheitliche Standards sicherzustellen.

Beispiel: *Ein Anbieter bringt ein neues Sprachmodell auf den Markt. Das Büro für Künstliche Intelligenz kann prüfen, ob die vorgeschriebenen Sicherheitsmaßnahmen und Transparenzpflichten eingehalten werden.*

B. Beschwerderecht nachgelagerter Anbieter

1. **Recht auf Beschwerde**: Nachgelagerte Anbieter können eine Beschwerde einreichen, wenn sie der Ansicht sind, dass ein Anbieter gegen die Verordnung verstößt.
2. **Formale Anforderungen**: Die Beschwerde muss begründet sein und mindestens folgende Angaben enthalten:
    - **Kontaktstelle**: Angaben zum Anbieter des KI-Modells.
    - **Fakten und Rechtsgrundlage**: Darstellung der relevanten Tatsachen, benannte Vorschriften und Begründung des Verstoßes.
    - **Zusätzliche Informationen**: Weitere von dem nachgelagerten Anbieter für relevant erachtete Angaben, auch solche, die er selbst recherchiert hat.

Beispiel: *Ein Unternehmen nutzt ein KI-Modell für juristische Textanalyse. Es stellt fest, dass wichtige Sicherheitsinformationen fehlen. Es reicht beim Büro für Künstliche Intelligenz eine Beschwerde mit den entsprechenden Nachweisen ein.*

C. Besonderheiten

- **Doppelte Schutzfunktion**: Zum einen wird die Einhaltung durch das Büro überwacht, zum anderen haben betroffene Marktteilnehmer ein eigenes Beschwerderecht.
- **Systematische Verknüpfung**: Artikel 89 ergänzt die Aufgabenverteilung zwischen Union und Mitgliedstaaten, wie sie in den Erwägungsgründen beschrieben wird.
- **Zielsetzung der Norm**: Ziel ist die Sicherstellung einer **effektiven Kontrolle**, gerade bei Modellen, die weitreichende Auswirkungen auf viele Sektoren haben können.

III. Zusammenfassung

Zuständige Behörde	Büro für Künstliche Intelligenz (Unionsebene)
Befugnisse	Überwachung, Kontrolle, Maßnahmen zur Umsetzung
Beschwerderecht	Nachgelagerte Anbieter können begründete Beschwerden einreichen
Mindestangaben bei Beschwerde	Kontaktstelle, Fakten und Rechtsgrundlage, zusätzliche Infos
Ziel	Einheitliche, effektive Aufsicht über KI-Modelle mit allgemeinem Verwendungszweck

IV. Quellenverzeichnis

- Erwägungsgründe 161, 162 KI-VO (EU) 2024/1689

Artikel 90 KI-VO

Warnungen des wissenschaftlichen Gremiums vor systemischen Risiken

(1) Das wissenschaftliche Gremium kann dem Büro für Künstliche Intelligenz eine qualifizierte Warnung übermitteln, wenn es Grund zu der Annahme hat, dass

a) ein KI-Modell mit allgemeinem Verwendungszweck ein konkretes, identifizierbares Risiko auf Unionsebene birgt oder

b) ein KI-Modell mit allgemeinem Verwendungszweck die Bedingungen gemäß Artikel 51 erfüllt.

(2) Aufgrund einer solchen qualifizierten Warnung kann die Kommission über das Büro für Künstliche Intelligenz und nach Unterrichtung des KI-Gremiums die in diesem Abschnitt festgelegten Befugnisse zur Beurteilung der Angelegenheit ausüben. Das Büro für Künstliche Intelligenz unterrichtet das KI-Gremium über jede Maßnahme gemäß den Artikeln 91 bis 94.

(3) Eine qualifizierte Warnung ist hinreichend zu begründen und enthält mindestens Folgendes:

a) die Kontaktstelle des Anbieters des betreffenden KI-Modells mit allgemeinem Verwendungszweck mit systemischem Risiko;

b) eine Beschreibung der einschlägigen Fakten und der Gründe für die Warnung durch das wissenschaftliche Gremium;

c) alle sonstigen Informationen, die das wissenschaftliche Gremium für relevant hält, gegebenenfalls einschließlich Informationen, die es auf eigene Initiative hin zusammengetragen hat.

I. Worum geht es?

Artikel 90 regelt, wie das wissenschaftliche Gremium die Kommission und das Büro für Künstliche Intelligenz auf mögliche systemische Risiken durch KI-Modelle mit allgemeinem Verwendungszweck aufmerksam machen kann. Kernidee ist, dass unabhängige Fachleute Risiken frühzeitig erkennen und diese in Form einer „qualifizierten Warnung“ weiterleiten. Damit soll sichergestellt werden, dass gefährliche Entwicklungen rechtzeitig überprüft und gegebenenfalls Maßnahmen ergriffen werden.

II. Detailkommentar

A. Rolle des wissenschaftlichen Gremiums

- **Unabhängigkeit**: Das Gremium besteht aus Sachverständigen, die auf Basis von Fachwissen im KI-Bereich ausgewählt werden und unabhängig arbeiten.
- **Unterstützung der Kommission**: Es dient als Frühwarnsystem, um das Büro für Künstliche Intelligenz bei seiner Überwachungsarbeit zu unterstützen.
- **Expertise**: Entscheidungen und Warnungen basieren auf wissenschaftlichen und technischen Einschätzungen.

Beispiel: *Ein Team von Experten stellt fest, dass ein weit verbreitetes Sprachmodell bestimmte falsche medizinische Empfehlungen ausgibt, die sich schnell über Europa verbreiten könnten. Das Gremium könnte daraufhin eine qualifizierte Warnung aussprechen.*

B. Voraussetzungen einer qualifizierten Warnung

- **Risiko auf Unionsebene**: Es muss ein konkretes, identifizierbares Risiko für die gesamte EU bestehen (zB Sicherheit, Gesundheit, Grundrechte).
- **Systemisches Risiko**: Alternativ kann eine Warnung erfolgen, wenn das Modell die Kriterien für ein systemisches Risiko erfüllt **(**Artikel 51 KI-VO).

Beispiel: *Ein Bildgenerierungsmodell produziert systematisch diskriminierende Darstellungen bestimmter Gruppen. Das Gremium erkennt, dass dies europaweit das Vertrauen in KI untergräbt und spricht eine Warnung aus.*

C. Verfahren und Folgen

- **Adressat**: Die Warnung geht an das Büro für Künstliche Intelligenz.
- **Folgen**: Die Kommission kann daraufhin Untersuchungen oder andere Maßnahmen nach Artikel 91 KI-VO ff einleiten.

- **Informationspflicht**: Das Büro muss das KI-Gremium über alle ergriffenen Maßnahmen informieren.

Beispiel: *Nach einer Warnung über ein Modell, das für Desinformationskampagnen missbraucht wird, startet die Kommission eine Untersuchung und fordert zusätzliche Informationen vom Anbieter an.*

D. Inhalt einer qualifizierten Warnung

- **Kontaktstelle des Anbieters**: Damit die Behörden den Anbieter direkt erreichen können.
- **Beschreibung der Fakten und Gründe**: Klare Darstellung, warum eine Gefahr angenommen wird.
- **Zusätzliche Informationen**: Alle relevanten Daten, auch solche, die das Gremium selbst gesammelt hat.

Beispiel: *Die Warnung enthält eine Analyse mit dokumentierten Fehlfunktionen, Kontaktdaten des Anbieters und eine technische Begründung, warum das Modell Risiken birgt.*

E. Besonderheiten

- **Frühwarnmechanismus**: Artikel 90 ist ein präventives Instrument, bevor ein Schaden entsteht.
- **Systemische Dimension**: Die Regelung zielt nicht auf Einzelfälle, sondern auf Risiken, die eine Wirkung für die gesamte EU entfalten können.
- **Transparenz und Begründung**: Jede Warnung muss nachvollziehbar begründet sein, um willkürliche Eingriffe zu verhindern.

III. Zusammenfassung

Adressat	Warnungen gehen an das Büro für Künstliche Intelligenz
Voraussetzungen	Risiko auf EU-Ebene oder systemisches Risiko

Folgen	Kommission kann Untersuchungen/ Maßnahmen ergreifen
Inhalt	Anbieter-Kontakt, Begründung, zusätzliche Infos
Zweck	Frühwarnung vor gefährlichen Entwicklungen durch KI-Modelle

IV. Quellenverzeichnis

- Erwägungsgründe 151, 163 KI-VO (EU) 2024/1689

Artikel 91 KI-VO

Befugnis zur Anforderung von Dokumentation und Informationen

(1) Die Kommission kann den Anbieter des betreffenden KI-Modells mit allgemeinem Verwendungszweck auffordern, die vom Anbieter gemäß den Artikeln 53 und 55 erstellte Dokumentation oder alle zusätzlichen Informationen vorzulegen, die erforderlich sind, um die Einhaltung dieser Verordnung durch den Anbieter zu beurteilen.

(2) Vor der Übermittlung des Informationsersuchens kann das Büro für Künstliche Intelligenz einen strukturierten Dialog mit dem Anbieter des KI-Modells mit allgemeinem Verwendungszweck einleiten.

(3) Auf hinreichend begründeten Antrag des wissenschaftlichen Gremiums kann die Kommission ein Informationsersuchen an einen Anbieter eines KI-Modells mit allgemeinem Verwendungszweck richten, wenn der Zugang zu Informationen für die Wahrnehmung der Aufgaben des wissenschaftlichen Gremiums gemäß Artikel 68 Absatz 2 erforderlich und verhältnismäßig ist.

(4) In dem Auskunftsersuchen sind die Rechtsgrundlage und der Zweck des Ersuchens zu nennen, anzugeben, welche Informationen benötigt werden, eine Frist für die Übermittlung der Informationen zu setzen, und die Geldbußen für die Erteilung unrichtiger, unvollständiger oder irreführender Informationen gemäß Artikel 101 anzugeben.

(5) Der Anbieter des betreffenden KI-Modells mit allgemeinem Verwendungszweck oder sein Vertreter stellt die angeforderten Informationen bereit. Im Falle juristischer Personen, Gesellschaften oder — wenn der Anbieter keine Rechtspersönlichkeit besitzt — die Personen, die nach Gesetz oder Satzung zur Vertretung dieser Personen befugt sind, stellen die angeforderten Informationen im Namen des Anbieters des betreffenden KI-Modells mit allgemeinem Verwendungszweck zur Verfügung. Ordnungsgemäß bevollmächtigte Rechtsanwälte können Informationen im Namen ihrer Mandanten erteilen. Die Mandanten bleiben jedoch in vollem Umfang dafür verantwortlich, dass die erteilten Auskünfte vollständig, sachlich richtig oder nicht irreführend sind.

I. Worum geht es?

Artikel 91 regelt die Befugnis der Europäischen Kommission, von Anbietern von KI-Modellen mit allgemeinem Verwendungszweck bestimmte

Dokumentationen und Informationen zu verlangen. Ziel ist es, die Einhaltung der KI-VO zu überwachen und sicherzustellen. Der Artikel schafft damit eine zentrale Aufsichts- und Kontrollkompetenz auf Unionsebene.

II. Detailkommentar

A. Adressatenkreis

- **Anbieter von KI-Modellen**: Gemeint sind Anbieter von sogenannten KI-Modellen mit allgemeinem Verwendungszweck. Das sind Modelle, die in verschiedenen Anwendungsfeldern einsetzbar sind und nicht nur auf einen bestimmten Zweck zugeschnitten sind.
- **Vertreter**: Falls der Anbieter nicht in der EU ansässig ist, kann die Kommission den in der Union benannten Vertreter adressieren.

B. Befugnisse der Kommission

1. **Anforderung von Dokumentation**: Die Kommission darf die nach Artikel 53 KI-VO und Artikel 55 KI-VO erstellten Unterlagen einfordern.
2. **Zusätzliche Informationen**: Neben den standardisierten Dokumentationen können weitere Informationen verlangt werden, wenn diese für die Bewertung der Einhaltung notwendig sind.
3. **Dialog vor Anforderung**: Bevor ein formelles Auskunftsersuchen gestellt wird, kann das Büro für Künstliche Intelligenz einen „strukturierten Dialog“ mit dem Anbieter beginnen, um Informationen auf kooperativem Wege zu erhalten.

Beispiel: *Die Kommission vermutet, dass ein Sprachmodell gegen Transparenzpflichten verstößt. Vor einer formellen Anfrage organisiert das Büro für Künstliche Intelligenz zunächst ein Gespräch mit dem Anbieter, um Unklarheiten auszuräumen.*

C. Rolle des wissenschaftlichen Gremiums

- **Begründeter Antrag**: Auch das wissenschaftliche Gremium kann indirekt ein Auskunftsersuchen auslösen, wenn es selbst für seine Aufgaben Informationen benötigt.
- **Kommission als Filter**: Das Ersuchen läuft immer über die Kommission, die das Begehren prüft und formalisiert.

D. Formale Anforderungen an das Auskunftsersuchen

- **Rechtsgrundlage**: Das Schreiben muss sich auf die entsprechende Norm berufen.
- **Zweck**: Der konkrete Anlass und das Ziel der Anfrage müssen genannt werden.
- **Klarheit**: Es ist anzugeben, welche Informationen konkret benötigt werden.
- **Fristsetzung**: Die Kommission muss eine angemessene Frist festlegen.
- **Sanktionserwähnung**: Es ist auf die drohenden Geldbußen nach Artikel 101 KI-VO hinzuweisen.

Beispiel: *Die Kommission fordert die Offenlegung der Trainingsdatenkategorien eines Modells an. Das Schreiben nennt Artikel 91 als Grundlage, erklärt den Zweck der Überprüfung, listet die konkret benötigten Dokumente auf und setzt eine Frist von vier Wochen. Zudem wird auf mögliche Bußgelder hingewiesen.*

E. Pflichten des Anbieters

- **Unmittelbare Bereitstellung**: Der Anbieter oder sein Vertreter muss die geforderten Informationen zur Verfügung stellen.
- **Verantwortlichkeit**: Auch wenn ein Anwalt bevollmächtigt wird, bleibt der Anbieter verantwortlich für die Richtigkeit und Vollständigkeit der Angaben.

- **Vertretungsregelung**: Juristische Personen oder Gesellschaften müssen die Auskünfte durch ihre gesetzlichen Vertreter erteilen.

F. Besonderheiten

- **Zentrale Aufsicht**: Durch Artikel 91 wird die Überwachung von KI-Modellen mit allgemeinem Verwendungszweck bewusst auf Unionsebene gebündelt. Dies soll verhindern, dass nationale Behörden unterschiedlich agieren.
- **Schutz vor Missbrauch**: Das Verfahren ist durch klare formale Vorgaben (Rechtsgrundlage, Zweck, Frist, Sanktionen) eingehegt, um Transparenz und Rechtssicherheit für die Anbieter zu gewährleisten.

III. Zusammenfassung

Zuständigkeit	Kommission kann Informationen von Anbietern von KI-Modellen verlangen
Vorverfahren	Büro für Künstliche Intelligenz kann strukturierten Dialog führen
Auslöser	Eigeninitiative der Kommission oder Antrag des wissenschaftlichen Gremiums
Formvorgaben	Rechtsgrundlage, Zweck, konkrete Angaben, Frist, Hinweis auf Sanktionen
Pflicht des Anbieters	Unverzügliche und vollständige Bereitstellung; Anwalt möglich, Verantwortung bleibt beim Anbieter

IV. Quellenverzeichnis

- Erwägungsgründe 161, 162 KI-VO (EU) 2024/1689

Artikel 92 KI-VO

Befugnis zur Durchführung von Bewertungen

(1) Das Büro für Künstliche Intelligenz kann nach Konsultation des KI-Gremiums Bewertungen des betreffenden KI-Modells mit allgemeinem Verwendungszweck durchführen, um

a) die Einhaltung der Pflichten aus dieser Verordnung durch den Anbieter zu beurteilen, wenn die gemäß Artikel 91 eingeholten Informationen unzureichend sind, oder

b) systemische Risiken auf Unionsebene von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko zu ermitteln, insbesondere im Anschluss an eine qualifizierte Warnung des wissenschaftlichen Gremiums gemäß Artikel 90 Absatz 1 Buchstabe a.

(2) Die Kommission kann beschließen, unabhängige Sachverständige zu benennen, die in ihrem Namen Bewertungen durchführen, einschließlich aus dem gemäß Artikel 68 eingesetzten wissenschaftlichen Gremium. Die für diese Aufgabe benannten unabhängigen Sachverständigen erfüllen die in Artikel 68 Absatz 2 umrissenen Kriterien.

(3) Für die Zwecke des Absatzes 1 kann die Kommission über API oder weitere geeignete technische Mittel und Instrumente, einschließlich Quellcode, Zugang zu dem betreffenden KI-Modell mit allgemeinem Verwendungszweck anfordern.

(4) In der Anforderung des Zugangs sind die Rechtsgrundlage, der Zweck und die Gründe für die Anforderung zu nennen und die Frist für die Bereitstellung des Zugangs zu setzen und die Geldbußen gemäß Artikel 101 für den Fall, dass der Zugang nicht bereitgestellt wird, anzugeben.

(5) Die Anbieter des betreffenden KI-Modells mit allgemeinem Verwendungszweck oder seine Vertreter stellen die angeforderten Informationen zur Verfügung. Im Falle juristischer Personen, Gesellschaften oder — wenn der Anbieter keine Rechtspersönlichkeit besitzt — die Personen, die nach Gesetz oder ihrer Satzung zur Vertretung dieser Personen befugt sind, stellen den angeforderten Zugang im Namen des Anbieters des betreffenden KI-Modells mit allgemeinem Verwendungszweck zur Verfügung.

(6) Die Kommission erlässt Durchführungsrechtsakte, in denen die detaillierten Regelungen und Voraussetzungen für die Bewertungen,

einschließlich der detaillierten Regelungen für die Einbeziehung unabhängiger Sachverständiger, und das Verfahren für deren Auswahl festgelegt werden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

(7) Bevor es den Zugang zu dem betreffenden KI-Modell mit allgemeinem Verwendungszweck anfordert, kann das Büro für Künstliche Intelligenz einen strukturierten Dialog mit dem Anbieter des KI-Modells mit allgemeinem Verwendungszweck einleiten, um mehr Informationen über die interne Erprobung des Modells, interne Vorkehrungen zur Vermeidung systemischer Risiken und andere interne Verfahren und Maßnahmen, die der Anbieter zur Minderung dieser Risiken ergriffen hat, einzuholen.

I. Worum geht es?

Artikel 92 regelt die Befugnisse des Büros für Künstliche Intelligenz und der Kommission zur Durchführung von Bewertungen von KI-Modellen mit allgemeinem Verwendungszweck. Ziel ist es, die Einhaltung der Pflichten zu überwachen und systemische Risiken frühzeitig zu erkennen. Der Artikel schafft klare Verfahren, wie und unter welchen Voraussetzungen das Büro oder die Kommission Zugriff auf KI-Modelle nehmen dürfen.

II. Detailkommentar

A. Zweck der Bewertungen

- **Kontrolle der Pflichten**: Bewertungen können durchgeführt werden, wenn Informationen nach Artikel 91 KI-VOnicht ausreichen, um die Einhaltung der Pflichten des Anbieters zu beurteilen.
- **Ermittlung systemischer Risiken**: Bewertungen dienen auch dazu, potenzielle Gefahren für den Binnenmarkt oder die Gesellschaft zu erkennen, insbesondere wenn das wissenschaftliche Gremium eine qualifizierte Warnung ausspricht.

Beispiel: *Ein Anbieter liefert nur unvollständige technische Unterlagen. Das Büro für Künstliche Intelligenz kann daher eine Bewertung verlangen, um sicherzustellen, dass Sicherheitsstandards eingehalten werden.*

B. Beteiligung unabhängiger Sachverständiger

- **Benennung durch die Kommission**: Die Kommission kann unabhängige Experten beauftragen, auch aus dem wissenschaftlichen Gremium nach Artikel 68 KI-VO.
- **Anforderungen**: Experten müssen die in Artikel 68 Absatz 2 genannten Kriterien erfüllen, insbesondere Unabhängigkeit und Fachkompetenz.

Beispiel: *Bei der Prüfung eines großen Sprachmodells zieht die Kommission externe Wissenschaftler hinzu, um technische Aspekte wie Training und Datenquellen zu bewerten.*

C. Zugang zum KI-Modell

- **Technische Mittel**: Zugang kann über API, andere Schnittstellen oder in Ausnahmefällen auch durch Einsicht in den Quellcode verlangt werden.
- **Rechtsgrundlage und Transparenz**: In der Anforderung müssen Rechtsgrundlage, Zweck, Gründe, Frist und mögliche Geldbußen angegeben werden.
- **Verpflichtung des Anbieters**: Anbieter bzw. ihre gesetzlichen Vertreter müssen den Zugang bereitstellen.

Beispiel: *Die Kommission fordert API-Zugang, um die Funktionsweise eines Bildgenerierungsmodells zu überprüfen. Der Anbieter muss den Zugang innerhalb einer gesetzten Frist ermöglichen.*

D. Verfahren und Durchführungsrechtsakte

- **Detailregelungen**: Die Kommission erlässt Durchführungsrechtsakte, die Verfahren, Auswahl der Sachverständigen und konkrete Abläufe regeln.
- **Rechtssicherheit**: Diese Akte schaffen Einheitlichkeit und verhindern willkürliche Entscheidungen.

E. Dialog mit Anbietern

- **Vorbereitender Austausch**: Bevor Zugang zum Modell verlangt wird, kann ein strukturierter Dialog mit dem Anbieter erfolgen.
- **Inhalt des Dialogs**: Informationen über interne Tests, Risikovermeidungsmaßnahmen und Verfahren zur Risikominderung.

Beispiel: *Vor einer formellen Bewertung bittet das Büro für Künstliche Intelligenz den Anbieter um ein Gespräch über dessen interne Prüfverfahren, um eine einvernehmliche Lösung zu finden.*

F. Besonderheiten

- **Unionsebene statt nationale Ebene**: Artikel 92 konkretisiert die Kompetenzverteilung zwischen EU und Mitgliedstaaten. Die Aufsicht über KI-Modelle mit allgemeinem Verwendungszweck liegt zentral bei der Kommission und dem Büro für Künstliche Intelligenz.
- **Systemische Risiken im Fokus**: Anders als bei Hochrisiko-KI-Systemen steht hier die Abwehr von übergreifenden Gefahren (zB Auswirkungen großer Sprachmodelle auf Informationsökosysteme) im Vordergrund.

III. Zusammenfassung

Zweck der Bewertung	Kontrolle der Pflichten oder Erkennung systemischer Risiken
Beteiligte	Büro für Künstliche Intelligenz, Kommission, unabhängige Sachverständige
Zugang	API, technische Mittel, ggf. Quellcode; mit Begründung und Fristsetzung
Pflicht des Anbieters	Bereitstellung von Zugang und Informationen
Verfahren	Durchführungsrechtsakte regeln Details und Expertenernennung
Besonderheit	Zentralisierte Aufsicht auf Unionsebene, Fokus auf systemische Risiken

IV. Quellenverzeichnis

- Erwägungsgründe 161, 162 KI-VO (EU) 2024/1689

Artikel 93 KI-VO

Befugnis zur Aufforderung zu Maßnahmen

(1) Soweit erforderlich und angemessen, kann die Kommission die Anbieter auffordern,

a) geeignete Maßnahmen zu ergreifen, um die Verpflichtungen gemäß den Artikeln 53 und 54 einzuhalten;

b) Risikominderungsmaßnahmen durchzuführen, wenn die gemäß Artikel 92 durchgeführte Bewertung zu ernsthaften und begründeten Bedenken hinsichtlich eines systemischen Risikos auf Unionsebene geführt hat;

c) die Bereitstellung des Modells auf dem Markt einzuschränken, es zurückzunehmen oder zurückzurufen.

(2) Vor der Aufforderung zu einer Maßnahme kann das Büro für Künstliche Intelligenz einen strukturierten Dialog mit dem Anbieter des KI-Modells mit allgemeinem Verwendungszweck einleiten.

(3) Wenn der Anbieter des KI-Modells mit allgemeinem Verwendungszweck im Rahmen des strukturierten Dialogs gemäß Absatz 2 Verpflichtungszusagen zur Durchführung von Risikominderungsmaßnahmen, um einem systemischen Risiko auf Unionsebene zu begegnen, anbietet, kann die Kommission diese Verpflichtungszusagen durch einen Beschluss für bindend erklären und feststellen, dass es keinen weiteren Anlass zum Handeln gibt.

I. Worum geht es?

Artikel 93 KI-VO gibt der Kommission ein zentrales Instrument zur Durchsetzung der Verordnung. Sie kann Anbieter von KI-Modellen mit allgemeinem Verwendungszweck auffordern, bestimmte Maßnahmen zu ergreifen. Das Ziel ist es, Risiken für die Union frühzeitig zu mindern und die Einhaltung der Pflichten sicherzustellen. Die Norm dient somit als Eingriffsbefugnis, wenn andere Aufsichtsmaßnahmen nicht ausreichen.

II. Detailkommentar

A. Adressaten

- **Anbieter von KI-Modellen mit allgemeinem Verwendungszweck**: Nur sie können von Maßnahmen betroffen sein, da hier besondere Risiken für die gesamte Union bestehen.

B. Arten von Maßnahmen

- **Sicherstellung der Pflichterfüllung**: Die Kommission kann Anbieter anweisen, ihre Verpflichtungen nach Artikel 53 KI-VO und Artikel 54 KI-VOeinzuhalten. Diese betreffen Transparenz- und Dokumentationspflichten.
- **Risikominderungsmaßnahmen**: Wenn eine Bewertung nach Artikel 92 KI-VO ernsthafte und begründete Bedenken zu einem systemischen Risiko aufzeigt, darf die Kommission konkrete Gegenmaßnahmen verlangen.
- **Marktintervention**: Reicht dies nicht aus, kann die Kommission die Bereitstellung des Modells einschränken, es zurücknehmen oder zurückrufen.

Beispiel: *Eine Kommissionsevaluierung ergibt, dass ein Sprachmodell manipulative Desinformation in großem Umfang ermöglicht. Der Anbieter kann aufgefordert werden, zusätzliche Sicherheitsfilter einzubauen oder im Extremfall das Modell zurückzuziehen.*

C. Verfahren

- **Strukturierter Dialog**: Vor einer formellen Maßnahme kann das Büro für Künstliche Intelligenz einen Dialog mit dem Anbieter führen. Dies dient der Klärung und freiwilligen Einigung.
- **Verpflichtungszusagen**: Macht der Anbieter konkrete Zusagen zu Risikominderungsmaßnahmen, kann die Kommission diese für bindend erklären. Damit entfällt weiterer Handlungsbedarf.

Beispiel: *Ein Anbieter verpflichtet sich, ein unabhängiges Monitoring-System einzurichten. Die Kommission erkennt dies als ausreichend an und verzichtet auf zusätzliche Auflagen.*

D. Systematische Einordnung

- **Zusammenhang mit Artikel 92 KI-VO**: Maßnahmen setzen regelmäßig eine vorgängige Bewertung durch das Büro für Künstliche Intelligenz voraus.
- Die unterstützende Rolle des wissenschaftlichen Gremiums und die Kompetenzen des Büros für KI werden verdeutlicht. Die Kommission erhält damit fachlich fundierte Entscheidungsgrundlagen.

E. Besonderheiten

- **Verhältnismäßigkeit**: Maßnahmen müssen erforderlich und angemessen sein. Das schützt Anbieter vor überzogenen Eingriffen.
- **Kooperationsansatz**: Vorrang hat die einvernehmliche Lösung durch Dialog und Zusagen. Zwangsmaßnahmen sind das letzte Mittel.

III. Zusammenfassung

Ziel	Absicherung der Pflichterfüllung und Risikominderung bei KI-Modellen mit allgemeinem Verwendungszweck
Maßnahmen	Aufforderung zur Pflichterfüllung, Risikominderung, Markteinschränkungen bis Rückruf
Verfahren	Strukturierter Dialog und Möglichkeit verbindlicher Zusagen vor formellen Eingriffen
Schutzmechanismen	Erforderlichkeit, Angemessenheit und Verfahrensrechte sichern Anbieter ab

IV. Quellenverzeichnis

- Erwägungsgründe 163, 164 KI-VO (EU) 2024/1689

Artikel 94 KI-VO

Verfahrensrechte der Wirtschaftsakteure des KI-Modells mit allgemeinem Verwendungszweck

Unbeschadet der in dieser Verordnung enthaltenen spezifischeren Verfahrensrechte gilt für die Anbieter des KI-Modells mit allgemeinem Verwendungszweck Artikel 18 der Verordnung (EU) 2019/1020 sinngemäß.

I. Worum geht es?

Artikel 94 regelt die **Verfahrensrechte der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck**. Der Artikel stellt klar, dass diese Anbieter die gleichen grundlegenden Rechte genießen wie Wirtschaftsakteure in anderen regulierten Bereichen. Grundlage dafür ist Artikel 18 der Verordnung (EU) 2019/1020 (Marktüberwachungsverordnung), der nun sinngemäß Anwendung findet. Ziel ist es, ein faires Verfahren zu garantieren, wenn Behörden Maßnahmen ergreifen – etwa bei der Untersuchung möglicher Verstöße oder der Einschränkung des Modells.

II. Detailkommentar

A. Bezug zu Artikel 18 Marktüberwachungsverordnung

- **Sinngemäße Anwendung**: Die Vorschriften des Artikel 18 gelten nicht wortwörtlich, sondern werden an den Kontext der KI-VO angepasst. Gemeint sind die gleichen Schutzmechanismen: Transparenz, rechtliches Gehör und Information über Rechtsmittel.
- **Adressaten**: Nur Anbieter von KI-Modellen mit allgemeinem Verwendungszweck sind geschützt. Für andere Wirtschaftsakteure gelten die jeweils einschlägigen Regelungen.

B. Wesentliche Verfahrensrechte

1. **Begründungspflicht:** Jede Maßnahme oder Entscheidung des KI-Büros oder anderer zuständiger Behörden muss eine klare rechtliche Grundlage nennen. Dies schützt Anbieter vor willkürlichen Eingriffen.

2. **Mitteilungspflicht:** Entscheidungen müssen den betroffenen Anbietern unverzüglich mitgeteilt werden, verbunden mit Informationen zu möglichen Rechtsmitteln und Fristen.
3. **Rechtliches Gehör:** Bevor eine Maßnahme ergriffen wird, muss dem Anbieter Gelegenheit zur Stellungnahme gegeben werden. Die Frist beträgt mindestens zehn Arbeitstage.
4. **Ausnahme Dringlichkeit:** In Eilfällen – etwa bei gravierenden Risiken für öffentliche Sicherheit oder Gesundheit – kann eine Maßnahme sofort ergehen. In diesem Fall muss das Gehör so schnell wie möglich nachgeholt werden.

Beispiel: *Das KI-Büro plant, ein KI-Modell mit allgemeinem Verwendungszweck wegen systemischer Risiken vom Markt zu nehmen. Vor der Entscheidung erhält der Anbieter mindestens zehn Tage Zeit, um schriftlich Stellung zu nehmen. Nur wenn eine akute Gefahr für Cybersicherheit vorliegt, darf die Maßnahme sofort erfolgen.*

C. Verhältnis zu speziellen Verfahrensrechten der KI-VO

- Artikel 94 stellt klar, dass diese allgemeinen Verfahrensrechte zusätzlich gelten. Spezifischere Rechte innerhalb der KI-VO bleiben unberührt.
- **Schutzgedanke**: Damit soll sichergestellt werden, dass Anbieter mindestens die Garantien des allgemeinen Marktüberwachungsrechts erhalten, ergänzt durch besondere Schutzmechanismen der KI-VO.

D. Besonderheiten im Kontext von KI-Modellen mit allgemeinem Verwendungszweck

- **Risikoorientierung**: Der Artikel ist eingebettet in die Überwachung von Modellen mit potenziell systemischen Risiken. Behörden haben weitreichende Eingriffsbefugnisse (bis hin zu Rückruf oder Marktbeschränkung). Daher ist ein robuster Rechtsschutz notwendig.
- **Europäische Ebene**: Zuständig ist das EU-Amt für Künstliche Intelligenz, nicht nationale Marktüberwachungsbehörden. Dies hebt den supranationalen Charakter hervor.

III. Zusammenfassung

Geltung	Artikel 18 MarktüberwachungsVO gilt sinngemäß für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck
Rechte	Begründung, Mitteilung, rechtliches Gehör, Information über Rechtsmittel
Ausnahmen	Sofortmaßnahmen bei Dringlichkeit; Anhörung nachzuholen
Verhältnis	Ergänzend zu spezifischen Verfahrensrechten der KI-VO
Besonderheit	Zuständig ist das EU-KI-Amt, nicht nationale Behörden

IV. Quellenverzeichnis

- Erwägungsgründe 163, 164 KI-VO (EU) 2024/1689
- Artikel 18 VO (EU) 2019/1020

Artikel 95 KI-VO

Verhaltenskodizes für die freiwillige Anwendung bestimmter Anforderungen

(1) Das Büro für Künstliche Intelligenz und die Mitgliedstaaten fördern und erleichtern die Aufstellung von Verhaltenskodizes, einschließlich damit zusammenhängender Governance-Mechanismen, mit denen die freiwillige Anwendung einiger oder aller der in Kapitel III Abschnitt 2 genannten Anforderungen auf KI-Systeme, die kein hohes Risiko bergen, gefördert werden soll, wobei den verfügbaren technischen Lösungen und bewährten Verfahren der Branche, die die Anwendung dieser Anforderungen ermöglichen, Rechnung zu tragen ist.

(2) Das Büro für Künstliche Intelligenz und die Mitgliedstaaten erleichtern die Aufstellung von Verhaltenskodizes in Bezug auf die freiwillige Anwendung spezifischer Anforderungen auf alle KI-Systeme, einschließlich durch Betreiber, auf der Grundlage klarer Zielsetzungen sowie wesentlicher Leistungsindikatoren zur Messung der Erfüllung dieser Zielsetzungen, einschließlich unter anderem folgender Elemente:

a) in den Ethik-Leitlinien der Union für eine vertrauenswürdige KI enthaltene anwendbare Elemente;

b) Beurteilung und Minimierung der Auswirkungen von KI-Systemen auf die ökologische Nachhaltigkeit, einschließlich im Hinblick auf energieeffizientes Programmieren, und Techniken, um KI effizient zu gestalten, zu trainieren und zu nutzen;

c) Förderung der KI-Kompetenz, insbesondere der von Personen, die mit der Entwicklung, dem Betrieb und der Nutzung von KI befasst sind;

d) Erleichterung einer inklusiven und vielfältigen Gestaltung von KI-Systemen, unter anderem durch die Einsetzung inklusiver und vielfältiger Entwicklungsteams und die Förderung der Beteiligung der Interessenträger an diesem Prozess;

e) Bewertung und Verhinderung der negativen Auswirkungen von KI-Systemen auf schutzbedürftige Personen oder Gruppen schutzbedürftiger Personen, einschließlich im Hinblick auf die Barrierefreiheit für Personen mit Behinderungen, sowie auf die Gleichstellung der Geschlechter.

(3) Verhaltenskodizes können von einzelnen KI-System-Anbietern oder -Betreibern oder von Interessenvertretungen dieser Anbieter oder Betreiber oder von beiden aufgestellt werden, auch unter Einbeziehung von

Interessenträgern sowie deren Interessenvertretungen einschließlich Organisationen der Zivilgesellschaft und Hochschulen. Verhaltenskodizes können sich auf ein oder mehrere KI-Systeme erstrecken, um ähnlichen Zweckbestimmungen der jeweiligen Systeme Rechnung zu tragen.

(4) Das Büro für Künstliche Intelligenz und die Mitgliedstaaten berücksichtigen die besonderen Interessen und Bedürfnisse von KMU, einschließlich Startups, bei der Förderung und Erleichterung der Aufstellung von Verhaltenskodizes.

I. Worum geht es?

Der Artikel 95 regelt die Möglichkeit, dass freiwillige **Verhaltenskodizes** für KI-Systeme entwickelt werden können, die kein hohes Risiko bergen. Ziel ist es, ethische, nachhaltige und inklusive Standards über das Mindestmaß der Verordnung hinaus zu fördern. Diese Kodizes sollen Leitlinien für verantwortungsvollen Umgang mit KI darstellen und die Verbreitung vertrauenswürdiger KI in der EU stärken.

II. Detailkommentar

A. Zielrichtung der Norm

- **Freiwilligkeit**: Es handelt sich nicht um verpflichtende Regeln, sondern um freiwillige Selbstverpflichtungen der Anbieter oder Betreiber.
- **Förderung durch Behörden**: Das Büro für Künstliche Intelligenz und die Mitgliedstaaten unterstützen die Aufstellung solcher Kodizes.
- **Übertragung von Hochrisiko-Standards**: Bestimmte Anforderungen, die für Hochrisiko-KI gelten, sollen freiwillig auch auf Systeme mit geringerem Risikopotenzial angewandt werden.

Beispiel: *Ein Start-up entwickelt eine Sprachlern-App (kein Hochrisiko-System) und beschließt, freiwillig strengere Transparenzpflichten einzuhalten, um das Vertrauen der Nutzer zu stärken.*

B. Inhalte der Verhaltenskodizes

1. **Ethik-Leitlinien**: Bezugnahme auf die europäischen Ethik-Leitlinien für vertrauenswürdige KI. Ethik meint insbesondere Fairness (Vermeidung diskriminierender Ergebnisse oder algorithmischer Bias), Transparenz (Nachvollziehbarkeit von Prozessen und Entscheidungen) und Verantwortlichkeit (klare Zuweisung von Verantwortlichkeiten für Entwicklung, Einsatz und Folgen)
2. **Nachhaltigkeit**: Maßnahmen zur Senkung des Energieverbrauchs und für umweltfreundliches Training und Betrieb von KI.
3. **KI-Kompetenz**: Schulung von Entwicklern, Betreibern und Nutzern im verantwortungsvollen Umgang mit KI.
4. **Inklusion und Vielfalt**: Förderung diverser Entwicklungsteams und Beteiligung verschiedener Interessengruppen.
5. **Schutz vulnerabler Gruppen**: Vermeidung negativer Auswirkungen auf Menschen mit Behinderungen, Kinder oder andere besonders schutzbedürftige Gruppen.

Beispiel: *Ein Unternehmen verpflichtet sich in seinem Kodex, bei der Entwicklung einer Recruiting-Software stets Teams mit Geschlechterparität einzusetzen und mögliche Diskriminierung im Algorithmus zu prüfen.*

C. Beteiligte Akteure

- **Aufsteller**: Anbieter, Betreiber, deren Verbände oder auch Hochschulen und Zivilgesellschaft.
- **Adressaten**: Verhaltenskodizes können für einzelne Systeme oder ganze Produktgruppen erstellt werden.
- **Mitwirkung**: Breite Einbindung von Stakeholdern wie Gewerkschaften oder Verbraucherschutzorganisationen ist erwünscht.

Beispiel: *Eine Branchenvereinigung für Chatbot-Entwickler erstellt gemeinsam mit Verbraucherschutzverbänden einen Kodex zur Transparenz bei der Kommunikation mit Kunden.*

D. Besonderheiten für KMU

- **Berücksichtigung spezieller Interessen**: KMU und Start-ups sollen durch das Büro für Künstliche Intelligenz besonders unterstützt werden.
- **Praxisnähe**: Verhaltenskodizes müssen so gestaltet sein, dass sie für kleine Unternehmen handhabbar bleiben.

Beispiel: *Ein kleines KI-Start-up erhält von einer nationalen Behörde Vorlagen und Tools, um einen eigenen freiwilligen Kodex effizient zu entwickeln.*

III. Zusammenfassung

Ziel	Förderung freiwilliger Standards für nicht-hochriskante KI-Systeme
Instrument	Verhaltenskodizes, unterstützt von Büro für Künstliche Intelligenz und Mitgliedstaaten
Inhalte	Ethik, Nachhaltigkeit, KI-Kompetenz, Inklusion, Schutz vulnerabler Gruppen
Beteiligte	Anbieter, Betreiber, Verbände, Hochschulen, Zivilgesellschaft
Besonderheit	Berücksichtigung von KMU und Start-ups

IV. Quellenverzeichnis

- Erwägungsgründe 165, 166 KI-VO (EU) 2024/1689

Artikel 96 KI-VO

Leitlinien der Kommission zur Durchführung dieser Verordnung

(1) Die Kommission erarbeitet Leitlinien für die praktische Umsetzung dieser Verordnung, die sich insbesondere auf Folgendes beziehen:

a) die Anwendung der in den Artikeln 8 bis 15 und in Artikel 25 genannten Anforderungen und Pflichten;

b) die in Artikel 5 genannten verbotenen Praktiken;

c) die praktische Durchführung der Bestimmungen über wesentliche Veränderungen;

d) die praktische Umsetzung der Transparenzpflichten gemäß Artikel 50;

e) detaillierte Informationen über das Verhältnis dieser Verordnung zu den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften der Union sowie zu anderen einschlägigen Rechtsvorschriften der Union, auch in Bezug auf deren kohärente Durchsetzung;

f) die Anwendung der Definition eines KI-Systems gemäß Artikel 3 Nummer 1.

Wenn die Kommission solche Leitlinien herausgibt, widmet sie den Bedürfnissen von KMU einschließlich Start-up-Unternehmen, von lokalen Behörden und von den am wahrscheinlichsten von dieser Verordnung betroffenen Sektoren besondere Aufmerksamkeit.

Die Leitlinien gemäß Unterabsatz 1 dieses Absatzes tragen dem allgemein anerkannten Stand der Technik im Bereich KI sowie den einschlägigen harmonisierten Normen und gemeinsamen Spezifikationen, auf die in den Artikeln 40 und 41 Bezug genommen wird, oder den harmonisierten Normen oder technischen Spezifikationen, die gemäß den Harmonisierungsrechtsvorschriften der Union festgelegt wurden, gebührend Rechnung.

(2) Auf Ersuchen der Mitgliedstaaten oder des Büros für Künstliche Intelligenz oder von sich aus aktualisiert die Kommission früher verabschiedete Leitlinien, wenn es als notwendig erachtet wird.

I. Worum geht es?

Artikel 96 regelt die Leitlinien, die die Europäische Kommission zur praktischen Umsetzung der KI-VO herausgibt. Diese Leitlinien sollen sicherstellen, dass die Vorgaben der Verordnung einheitlich und praxisnah angewendet werden. Sie dienen als Orientierung für Unternehmen, Behörden und andere betroffene Akteure. Besonderes Augenmerk wird auf kleine und mittlere Unternehmen (KMU) gelegt, da diese oft weniger Ressourcen für die Umsetzung komplexer Vorschriften haben.

II. Detailkommentar

A. Zweck der Leitlinien

- **Orientierungshilfe**: Die Leitlinien helfen Anbietern, Betreibern und Behörden, die Vorgaben der KI-VO praktisch anzuwenden.
- **Kohärenz**: Sie sorgen dafür, dass die Verordnung europaweit einheitlich umgesetzt wird.
- **Rechtsklarheit**: Sie reduzieren Unsicherheiten bei der Auslegung unbestimmter Begriffe und Vorgaben.

B. Inhalte der Leitlinien

1. **Anforderungen und Pflichten**: Praktische Hinweise zur Umsetzung der in Artikel 8 KI-VO ff sowie Artikel 25 KI-VOgeregelten Pflichten (zB Datenqualität, Risikomanagement, Transparenz).
2. **Verbotene Praktiken**: Konkretisierung, wie die in Artikel 5 KI-VO aufgeführten Verbote in der Praxis zu verstehen sind.
3. **Wesentliche Veränderungen**: Erläuterung, wann eine wesentliche Änderung vorliegt und welche Folgen dies hat.
4. **Transparenzpflichten**: Hinweise zur Umsetzung von Artikel 50 KI-VO(zB Nutzerhinweise bei KI-Interaktion).
5. **Verhältnis zu anderem Recht**: Darstellung, wie die KI-VO mit bestehenden EU-Harmonisierungsrechtsvorschriften (Anhang I KI-VO) und anderen Rechtsakten zusammenspielt.

6. **Definition von KI-Systemen**: Konkretisierung der in Artikel 3 KI-VO Nr 1 enthaltenen Definition.

Beispiel: *Ein KMU entwickelt eine Sprachassistenz-Software. Mithilfe der Leitlinien erfährt das Unternehmen, wie es Transparenzpflichten praktisch erfüllt, etwa durch einen klaren Hinweis an den Nutzer, dass er mit einem KI-System interagiert.*

C. Besonderer Fokus auf KMU und Start-ups

- **Unterstützung kleiner Unternehmen**: Leitlinien berücksichtigen die begrenzten Ressourcen von KMU und Start-ups.
- **Pragmatische Umsetzung**: Vorgaben sollen nicht überfordern, sondern praktikable Lösungen bieten.

Beispiel: *Ein Start-up im Gesundheitsbereich erhält durch die Leitlinien vereinfachte Beispiele, wie Risikomanagementsysteme schlank und effektiv umgesetzt werden können.*

D. Stand der Technik und Normen

- **Technische Orientierung**: Die Leitlinien müssen den aktuellen Stand der Technik im KI-Bereich berücksichtigen.
- **Normenbezug**: Harmonisierten Normen und Spezifikationen (Artikel 40 KI-VO und Artikel 41 KI-VO) wird Rechnung getragen.

E. Aktualisierung der Leitlinien

- **Flexibilität**: Die Kommission kann Leitlinien jederzeit aktualisieren.
- **Anlassbezogen**: Auf Antrag der Mitgliedstaaten oder des KI-Büros oder von sich aus.

Beispiel: *Wenn sich ein neuer technischer Standard zur Erklärbarkeit von KI durchsetzt, aktualisiert die Kommission die Leitlinien entsprechend.*

F. Systematischer Zusammenhang

- **Artikel 96 als sogenanntes„Soft Law“**: Leitlinien sind keine verbindlichen Rechtsakte, haben aber faktisch große Bedeutung.
- **Unterstützung von freiwilligen Initiativen**: Erwägungsgründe 165 und 166 betonen zusätzlich die Rolle freiwilliger Kodizes und Sicherheitsstandards auch bei Nicht-Hochrisiko-Systemen.

III. Zusammenfassung

Ziel	Praktische Umsetzung der KI-VO erleichtern
Adressaten	Unternehmen (bes. KMU), Behörden, betroffene Sektoren
Inhalte	Anforderungen, Verbote, wesentliche Änderungen, Transparenz, Verhältnis zu anderem Recht, KI-Definition
Besonderheit	Leitlinien sind flexibel, orientieren sich am Stand der Technik, werden regelmäßig aktualisiert
Bedeutung	Hoher Praxiswert, auch wenn rechtlich nicht bindend

IV. Quellenverzeichnis

- Erwägungsgründe 165, 166 KI-VO (EU) 2024/1689

Artikel 97 KI-VO

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die in Artikel 6 Absätze 6 und 7, Artikel 7 Absätze 1 und 3, Artikel 11 Absatz 3, Artikel 43 Absätze 5 und 6, Artikel 47 Absatz 5, Artikel 51 Absatz 3, Artikel 52 Absatz 4 sowie Artikel 53 Absätze 5 und 6 genannte Befugnis zum Erlass delegierter Rechtsakte wird der Kommission für einen Zeitraum von fünf Jahren ab 1. August 2024 übertragen. Die Kommission erstellt spätestens neun Monate vor Ablauf des Zeitraums von fünf Jahren einen Bericht über die Befugnisübertragung. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widersprechen einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.

(3) Die Befugnisübertragung gemäß Artikel 6 Absätze 6 und 7, Artikel 7 Absätze 1 und 3, Artikel 11 Absatz 3, Artikel 43 Absätze 5 und 6, Artikel 47 Absatz 5, Artikel 51 Absatz 3, Artikel 52 Absatz 4 sowie Artikel 53 Absätze 5 und 6 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in jenem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem darin angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung niedergelegten Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der nach Artikel 6 Absatz 6 oder 7, Artikel 7 Absatz 1 oder 3, Artikel 11 Absatz 3, Artikel 43 Absatz 5 oder 6, Artikel 47 Absatz 5, Artikel 51 Absatz 3, Artikel 52 Absatz 4 sowie Artikel 53 Absatz 5 oder 6 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung jenes Rechtsakts an das Europäische Parlament und den Rat

Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

I. Worum geht es?

Artikel 97 regelt, unter welchen Bedingungen die Europäische Kommission befugt ist, sogenannte **delegierte Rechtsakte** zu erlassen. Dabei handelt es sich um Rechtsakte, mit denen die Kommission bestimmte technische oder organisatorische Details der KI-VO anpassen darf. Der Artikel legt fest, für welche Vorschriften die Befugnis gilt, wie lange sie dauert, wie das Europäische Parlament und der Rat diese Befugnis kontrollieren können und wie das Verfahren im Detail abläuft. Ziel ist es, die KI-VO flexibel an neue Entwicklungen anpassen zu können, ohne jedes Mal das gesamte Gesetzgebungsverfahren eröffnen zu müssen.

II. Detailkommentar

A. Umfang der Befugnisübertragung

- **Kommission erhält Befugnis**: Die Kommission darf in bestimmten Bereichen ergänzende oder präzisierende Regeln erlassen.
- **Betroffene Vorschriften**: Die Befugnis bezieht sich ua auf Regelungen zur Risikoeinstufung (Artikel 6 KI-VO und Artikel 7 KI-VO), zu Technischer Dokumentation (Artikel 11 KI-VO), zum Konformitätsbewertungsverfahren (Artikel 43 KI-VO), zu EU-Konformitätserklärung (Artikel 47 KI-VO), zu Einstufung von KI-Modellen mit allgemeinem Verwendungszweck (Artikel 51 KI-VO), zu Verfahren (Artikel 52 KI-VO) und zu Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (Artikel 53 KI-VO).
- **Technischer Anpassungsbedarf**: Gerade in dynamischen Bereichen wie KI ist es wichtig, flexibel reagieren zu können, etwa bei neuen Technologien oder Risiken.

Beispiel: *Wenn sich herausstellt, dass ein neuer KI-Anwendungsfall erhebliche Risiken birgt, kann die Kommission mittels delegiertem Rechtsakt festlegen, dass er in den Hochrisikobereich fällt.*

B. Dauer und Verlängerung der Befugnis

- **Grundzeitraum**: Die Befugnis gilt zunächst fünf Jahre ab 1. August 2024.
- **Stillschweigende Verlängerung**: Ohne Widerspruch verlängert sich die Befugnis automatisch um weitere fünf Jahre.
- **Berichtspflicht**: Die Kommission muss neun Monate vor Ablauf berichten, wie sie die Befugnis genutzt hat.

C. Kontrolle durch Parlament und Rat

- **Widerrufsrecht**: Sowohl Parlament als auch Rat können die Befugnis jederzeit widerrufen. Dann endet die Befugnis ab Veröffentlichung im Amtsblatt.
- **Einwendungsrecht**: Nach Erlass eines delegierten Rechtsakts haben Parlament und Rat drei Monate Zeit, Einwände zu erheben. Auf Wunsch kann diese Frist auf sechs Monate verlängert werden.
- **Rechtsfolgen**: Ohne Einwand tritt der Rechtsakt in Kraft. Bestehende Rechtsakte bleiben auch bei späterem Widerruf gültig.

Beispiel: *Die Kommission erlässt einen delegierten Rechtsakt zur Anpassung der Hochrisiko-Definition. Das Parlament hält dies für zu weitgehend und legt Einspruch ein – der Rechtsakt tritt nicht in Kraft.*

D. Beteiligung von Sachverständigen

- **Mitgliedstaaten eingebunden**: Vor Erlass konsultiert die Kommission Experten der Mitgliedstaaten.

E. Besonderheiten

- **Vertrauensvolle Zusammenarbeit**: Es wird betont, dass bei Ausübung der Befugnisse Vertraulichkeit und Schutz sensibler Informationen zu wahren sind.
- **Abgrenzung**: Delegierte Rechtsakte dienen der Ergänzung und Änderung nicht-wesentlicher Vorschriften. Sie unterscheiden sich von Durchführungsrechtsakten, die nur die Anwendung im Detail regeln.

III. Zusammenfassung

Befugnis	Kommission darf delegierte Rechtsakte erlassen
Dauer	fünf Jahre ab 1. August 2024, automatische Verlängerung
Kontrolle	Parlament und Rat können widerrufen oder Einwände erheben
Verfahren	Konsultation von Sachverständigen, Übermittlung an Parlament und Rat
Besonderheit	Schutz vertraulicher Informationen und Rechte

IV. Quellenverzeichnis

- Erwägungsgrund 167 KI-VO (EU) 2024/1689

Artikel 98 KI-VO

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr 182/2011.

I. Worum geht es?

Artikel 98 regelt das **Ausschussverfahren**, mit dem die Kommission bei der Durchführung der KI-VO unterstützt wird. Es handelt sich um ein Standardinstrument der EU, um Mitgliedstaaten in die Entscheidungsprozesse einzubeziehen. Kern ist, dass die Kommission nicht völlig frei handelt, sondern ein Ausschuss der Mitgliedstaaten über bestimmte Maßnahmen mitentscheidet.

II. Detailkommentar

A. Funktion des Ausschusses

- **Unterstützung der Kommission**: Die Kommission erhält bei wichtigen Durchführungsmaßnahmen Unterstützung durch einen Ausschuss.
- **Einbindung der Mitgliedstaaten**: Jeder Mitgliedstaat entsendet Vertreter. Dadurch ist die gemeinsame Kontrolle gewährleistet.
- **Ziel**: Einheitliche Umsetzung der KI-VO in allen Mitgliedstaaten.

Beispiel: *Wenn die Kommission technische Standards für die Risikobewertung von KI-Systemen festlegt, berät und stimmt der Ausschuss mit.*

B. Rechtsgrundlage

- **Verweisung auf Verordnung (EU) Nr 182/2011**: Dieses Regelwerk beschreibt, wie Ausschüsse die Kommission kontrollieren.

- **Artikel 5 dieser Verordnung**: Legt das „Prüfverfahren“ fest, also ein Verfahren, bei dem die Mitgliedstaaten in einem Ausschuss abstimmen. Die Kommission ist an das Ergebnis gebunden.

Beispiel: *Die Kommission will eine Liste verbotener KI-Anwendungen ergänzen. Ohne Zustimmung des Ausschusses kann dies nicht beschlossen werden.*

C. Bedeutung für die Praxis

- **Rechtsstaatlichkeit**: Die Kommission wird durch die Mitgliedstaaten kontrolliert. Das verhindert einseitige Entscheidungen.
- **Einheitlichkeit**: Mitgliedstaaten bringen ihre Perspektive ein, damit die Regelungen in ganz Europa gleichermaßen anwendbar sind.
- **Vertrauen**: Durch die gemeinsame Entscheidungsfindung wird das Vertrauen in die Umsetzung der KI-VO gestärkt.

Beispiel: *Ein Mitgliedstaat hat besondere Sicherheitsbedenken bei einer KI-Anwendung. Diese werden im Ausschuss diskutiert und können in die Entscheidung einfließen.*

D. Besonderheiten

- **Zusammenarbeit und Vertraulichkeit**: Erwägungsgrund 167 betont, dass die Zusammenarbeit der Behörden vertraulich und respektvoll ablaufen muss. Vertrauliche Geschäftsdaten oder Sicherheitsinteressen dürfen nicht offengelegt werden.
- **Breite Aufgaben**: Der Ausschuss entscheidet nicht nur über technische Details, sondern auch über Fragen der Sicherheit, Transparenz und Rechtsdurchsetzung.

III. Zusammenfassung

Ausschussverfahren	Kommission wird von einem Ausschuss der Mitgliedstaaten unterstützt
Rechtsgrundlage	Verordnung (EU) Nr 182/2011, insbesondere Artikel 5 (Prüfverfahren)

Ziel	Einheitliche Umsetzung, Kontrolle und Vertrauen
Besonderheiten	Vertraulichkeit, Schutz sensibler Daten, Einbindung der Mitgliedstaaten

IV. Quellenverzeichnis

- Erwägungsgrund 167 KI-VO (EU) 2024/1689
- Artikel 5 VO (EU) 2011/182

Artikel 99 KI-VO

Sanktionen

(1) Entsprechend den Vorgaben dieser Verordnung erlassen die Mitgliedstaaten Vorschriften für Sanktionen und andere Durchsetzungsmaßnahmen, zu denen auch Verwarnungen und nichtmonetäre Maßnahmen gehören können, die bei Verstößen gegen diese Verordnung durch Akteure Anwendung finden, und ergreifen alle Maßnahmen, die für deren ordnungsgemäße und wirksame Durchsetzung notwendig sind, wobei die von der Kommission gemäß Artikel 96 erteilten Leitlinien zu berücksichtigen sind. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Sie berücksichtigen die Interessen von KMU, einschließlich Start-up-Unternehmen, sowie deren wirtschaftliches Überleben.

(2) Die Mitgliedstaaten teilen der Kommission die Vorschriften für Sanktionen und andere Durchsetzungsmaßnahmen gemäß Absatz 1 unverzüglich und spätestens zum Zeitpunkt ihres Inkrafttretens mit und melden ihr unverzüglich etwaige spätere Änderungen.

(3) Bei Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken werden Geldbußen von bis zu 35 000 000 EUR oder — im Falle von Unternehmen — von bis zu 7 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

(4) Für Verstöße gegen folgende für Akteure oder notifizierte Stellen geltende Bestimmungen, mit Ausnahme der in Artikel 5 genannten, werden Geldbußen von bis zu 15 000 000 EUR oder — im Falle von Unternehmen — von bis zu 3 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist:

a) Pflichten der Anbieter gemäß Artikel 16;

b) Pflichten der Bevollmächtigten gemäß Artikel 22;

c) Pflichten der Einführer gemäß Artikel 23;

d) Pflichten der Händler gemäß Artikel 24;

e) Pflichten der Betreiber gemäß Artikel 26;

f) für notifizierte Stellen geltende Anforderungen und Pflichten gemäß Artikel 31, Artikel 33 Absätze 1, 3 und 4 bzw. Artikel 34;

g) Transparenzpflichten für Anbieter und Betreiber gemäß Artikel 50.

(5) Werden notifizierten Stellen oder zuständigen nationalen Behörden auf deren Auskunftsersuchen hin falsche, unvollständige oder irreführende Informationen bereitgestellt, so werden Geldbußen von bis zu 7 500 000 EUR oder — im Falle von Unternehmen — von bis zu 1 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist.

(6) Im Falle von KMU, einschließlich Start-up-Unternehmen, gilt für jede in diesem Artikel genannte Geldbuße der jeweils niedrigere Betrag aus den in den Absätzen 3, 4 und 5 genannten Prozentsätzen oder Summen.

(7) Bei der Entscheidung, ob eine Geldbuße verhängt wird, und bei der Festsetzung der Höhe der Geldbuße werden in jedem Einzelfall alle relevanten Umstände der konkreten Situation sowie gegebenenfalls Folgendes berücksichtigt:

a) Artikel, Schwere und Dauer des Verstoßes und seiner Folgen, unter Berücksichtigung des Zwecks des KI-Systems sowie gegebenenfalls der Zahl der betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

b) ob demselben Akteur bereits von anderen Marktüberwachungsbehörden für denselben Verstoß Geldbußen auferlegt wurden;

c) ob demselben Akteur bereits von anderen Behörden für Verstöße gegen das Unionsrecht oder das nationale Recht Geldbußen auferlegt wurden, wenn diese Verstöße auf dieselbe Handlung oder Unterlassung zurückzuführen sind, die einen einschlägigen Verstoß gegen diese Verordnung darstellt;

d) Größe, Jahresumsatz und Marktanteil des Akteurs, der den Verstoß begangen hat;

e) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie etwa unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste;

f) Grad der Zusammenarbeit mit den zuständigen nationalen Behörden, um den Verstoß abzustellen und die möglichen nachteiligen Auswirkungen des Verstoßes abzumildern;

g) Grad an Verantwortung des Akteurs unter Berücksichtigung der von ihm ergriffenen technischen und organisatorischen Maßnahmen;

h) Artikel und Weise, wie der Verstoß den zuständigen nationalen Behörden bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Akteur den Verstoß gemeldet hat;

i) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

j) alle Maßnahmen, die der Akteur ergriffen hat, um den Schaden, der den betroffenen Personen zugefügt wird, zu mindern.

(8) Jeder Mitgliedstaat erlässt Vorschriften darüber, in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(9) In Abhängigkeit vom Rechtssystem der Mitgliedstaaten können die Vorschriften über Geldbußen je nach den dort geltenden Regeln so angewandt werden, dass die Geldbußen von den zuständigen nationalen Gerichten oder von sonstigen Stellen verhängt werden. Die Anwendung dieser Vorschriften in diesen Mitgliedstaaten muss eine gleichwertige Wirkung haben.

(10) Die Ausübung der Befugnisse gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem nationalen Recht, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(11) Die Mitgliedstaaten erstatten der Kommission jährlich Bericht über die Geldbußen, die sie in dem betreffenden Jahr gemäß diesem Artikel verhängt haben, und über damit zusammenhängende Rechtsstreitigkeiten oder Gerichtsverfahren.

I. Worum geht es?

Artikel 99 regelt die Sanktionen bei Verstößen gegen die KI-VO. Er legt fest, welche Bußgelder drohen, welche Maßstäbe für deren Höhe gelten und wie Mitgliedstaaten das Sanktionssystem auszugestalten haben. Ziel ist es, Verstöße wirksam, verhältnismäßig und abschreckend zu ahnden.

Gleichzeitig sollen insbesondere KMU und Start-ups geschützt werden, indem ihre Interessen bei der Festlegung der Sanktionen berücksichtigt werden.

II. Detailkommentar

A. Rolle der Mitgliedstaaten

- **Regelungskompetenz**: Mitgliedstaaten sind verpflichtet, eigene Vorschriften über Sanktionen zu erlassen und deren Durchsetzung sicherzustellen.
- **Flexibilität**: Neben Geldbußen sind auch nichtmonetäre Maßnahmen wie Verwarnungen vorgesehen.
- **Verpflichtung zur Mitteilung**: Sanktionen müssen der Kommission gemeldet werden, ebenso spätere Änderungen.

B. Arten und Höhe der Sanktionen

1. Verbotene KI-Praktiken

- Bis zu 35 Mio EUR oder 7 % des weltweiten Jahresumsatzes.

Beispiel: *Ein Unternehmen setzt ein KI-System zur „sozialen Bewertung" von Bürgern ein. Dies ist nach Artikel 5 verboten und kann mit den Höchstbußen geahndet werden.*

2. Pflichtverletzungen von Akteuren und notifizierten Stellen

- Bis zu 15 Mio EUR oder 3 % des weltweiten Umsatzes.
- **Betroffen**: Anbieter, Bevollmächtigte, Einführer, Händler, Betreiber und notifizierte Stellen.

Beispiel: *Ein Händler bringt ein KI-System auf den Markt, ohne die vorgeschriebene CE-Kennzeichnung zu prüfen.*

3. Fehl- oder Falschinformationen gegenüber Behörden

- Bis zu 7,5 Mio EUR oder 1 % des weltweiten Umsatzes.

Beispiel: *Ein Anbieter übermittelt absichtlich unvollständige Dokumentation an die Marktüberwachungsbehörde.*

4. Besonderheit für KMU und Start-ups

- Hier gilt stets der niedrigere Betrag (absolute Zahl oder Umsatzanteil).
- Dies schützt kleine Unternehmen vor übermäßigen finanziellen Belastungen.

C. Kriterien für die Bußgeldbemessung

- **Artikel, Schwere, Dauer**: Je gravierender der Verstoß, desto höher die Sanktion.
- **Wiederholungstäter**: Frühere Verstöße erhöhen das Strafmaß.
- **Unternehmensgröße**: Marktanteil und Umsatz werden berücksichtigt.
- **Zusammenarbeit mit Behörden**: Mildernd, wenn der Akteur aktiv bei der Aufklärung hilft.
- **Vorsatz oder Fahrlässigkeit**: Vorsätzliche Verstöße wiegen schwerer.
- **Schadensminderung**: Eigenständige Maßnahmen zur Begrenzung des Schadens wirken bußgeldmindernd.

Beispiel: *Ein Anbieter meldet einen eigenen Verstoß frühzeitig und arbeitet eng mit der Behörde zusammen. Dadurch kann das Bußgeld reduziert werden.*

D. Behörden und öffentliche Stellen

- Mitgliedstaaten bestimmen, in welchem Umfang Geldbußen auch gegen Behörden oder öffentliche Stellen verhängt werden.
- Unterschiedliche nationale Systeme sind zulässig, solange die Wirkung gleichwertig bleibt.

E. Verfahrensgarantien

- **Rechtsschutz**: Jede Sanktion unterliegt unions- und nationalrechtlichen Garantien, insbesondere gerichtlicher Überprüfbarkeit.
- **Jährliche Berichte**: Mitgliedstaaten müssen der Kommission über verhängte Geldbußen berichten.

F. Besonderheiten

- **Doppelbestrafung**: Ein Verstoß darf nicht mehrfach für denselben Sachverhalt sanktioniert werden.
- **Transparenzpflicht**: Kommission erhält Überblick über nationale Sanktionen und Entwicklungen.

III. Zusammenfassung

Verbotene KI-Praktiken	Bis 35 Mio EUR oder 7 % des Umsatzes
Pflichtverletzungen (Anbieter, Händler etc.)	Bis 15 Mio EUR oder 3 % des Umsatzes
Falsche Informationen an Behörden	Bis 7,5 Mio EUR oder 1 % des Umsatzes
KMU/Start-ups	Jeweils der niedrigere Betrag
Kriterien der Bemessung	Schwere, Dauer, Vorsatz/Fahrlässigkeit, Unternehmensgröße, Zusammenarbeit

IV. Quellenverzeichnis

- Erwägungsgründe 143, 168, 169 KI-VO (EU) 2024/1689

Artikel 100 KI-VO

Verhängung von Geldbußen gegen Organe, Einrichtungen und sonstige Stellen der Union

(1) Der Europäische Datenschutzbeauftragte kann gegen Organe, Einrichtungen und sonstige Stellen der Union, die in den Anwendungsbereich dieser Verordnung fallen, Geldbußen verhängen. Bei der Entscheidung, ob eine Geldbuße verhängt wird, und bei der Festsetzung der Höhe der Geldbuße werden in jedem Einzelfall alle relevanten Umstände der konkreten Situation sowie Folgendes gebührend berücksichtigt:

a) Artikel, Schwere und Dauer des Verstoßes und dessen Folgen, unter Berücksichtigung des Zwecks des betreffenden KI-Systems sowie gegebenenfalls der Zahl der betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

b) Grad der Verantwortung des Organs, der Einrichtung oder der sonstigen Stelle der Union unter Berücksichtigung der von diesem bzw. dieser ergriffenen technischen und organisatorischen Maßnahmen;

c) alle Maßnahmen, die das Organ, die Einrichtung oder die sonstige Stelle der Union zur Minderung des von den betroffenen Personen erlittenen Schadens ergriffen hat;

d) das Maß der Zusammenarbeit mit dem Europäischen Datenschutzbeauftragten bei der Behebung des Verstoßes und der Minderung seiner möglichen nachteiligen Auswirkungen, einschließlich der Befolgung von Maßnahmen, die der Europäische Datenschutzbeauftragte dem Organ, der Einrichtung oder der sonstigen Stelle der Union im Hinblick auf denselben Gegenstand zuvor bereits auferlegt hatte;

e) ähnliche frühere Verstöße des Organs, der Einrichtung oder der sonstigen Stelle der Union;

f) Artikel und Weise, wie der Verstoß dem Europäischen Datenschutzbeauftragten bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang das Organ, die Einrichtung oder die sonstige Stelle der Union den Verstoß gemeldet hat;

g) der Jahreshaushalt des Organs, der Einrichtung oder der sonstigen Stelle der Union.

(2) Bei Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken werden Geldbußen von bis zu 1 500 000 EUR verhängt.

(3) Bei Nichtkonformität des KI-Systems mit in dieser Verordnung festgelegten Anforderungen oder Pflichten, mit Ausnahme der in Artikel 5 festgelegten, werden Geldbußen von bis zu 750 000 EUR verhängt.

(4) Bevor der Europäische Datenschutzbeauftragte Entscheidungen nach dem vorliegenden Artikel trifft, gibt er dem Organ, der Einrichtung oder der sonstigen Stelle der Union, gegen das bzw. die sich das von ihm geführte Verfahren richtet, Gelegenheit, sich zum Vorwurf des Verstoßes zu äußern. Der Europäische Datenschutzbeauftragte stützt seine Entscheidungen nur auf die Elemente und Umstände, zu denen sich die betreffenden Parteien äußern können. Beschwerdeführer, soweit vorhanden, müssen in das Verfahren eng einbezogen werden.

(5) Die Verteidigungsrechte der betroffenen Parteien werden während des Verfahrens in vollem Umfang gewahrt. Vorbehaltlich der legitimen Interessen von Einzelpersonen oder Unternehmen im Hinblick auf den Schutz ihrer personenbezogenen Daten oder Geschäftsgeheimnisse haben die betroffenen Parteien Anspruch auf Einsicht in die Unterlagen des Europäischen Datenschutzbeauftragten.

(6) Das Aufkommen aus den nach diesem Artikel verhängten Geldbußen trägt zum Gesamthaushalt der Union bei. Die Geldbußen dürfen nicht den wirksamen Betrieb des Organs, der Einrichtung oder der sonstigen Stelle der Union beeinträchtigen, dem bzw. der die Geldbuße auferlegt wurde.

(7) Der Europäische Datenschutzbeauftragte macht der Kommission jährlich Mitteilung über die Geldbußen, die er nach Maßgabe dieses Artikels verhängt hat, und über die von ihm eingeleiteten Rechtsstreitigkeiten oder Gerichtsverfahren.

I. Worum geht es?

Artikel 100 regelt die Möglichkeit, dass der Europäische Datenschutzbeauftragte (EDSB) Geldbußen gegen Organe, Einrichtungen und sonstige Stellen der Europäischen Union verhängt, wenn diese gegen die KI-VO verstoßen. Damit schafft die Norm ein spezielles Sanktionsinstrument innerhalb der EU selbst. Ziel ist es, die Einhaltung der

Vorgaben sicherzustellen und Verstöße wirksam, verhältnismäßig und abschreckend zu ahnden.

II. Detailkommentar

A. Zuständigkeit und Adressaten

- **Zuständigkeit EDSB**: Der Europäische Datenschutzbeauftragte kann Geldbußen nach Artikel 100 verhängen.
- **Adressatenkreis**: Nur Organe, Einrichtungen und sonstige Stellen der Union. Private Unternehmen oder Mitgliedstaaten fallen nicht hierunter.

Beispiel: *Die Europäische Kommission nutzt ein KI-System zur Entscheidungsunterstützung, das gegen Artikel 5 verstößt. Hier könnte der EDSB eine Geldbuße verhängen.*

B. Höhe der Geldbußen

- **Verstöße gegen Artikel 5 KI-VO**: Geldbuße bis zu 1.500.000 EUR.
- **Andere Verstöße**: Geldbuße bis zu 750.000 EUR.
- **Grundprinzip**: Bußgeld darf den wirksamen Betrieb der betroffenen Stelle nicht gefährden.

Beispiel: *Ein EU-Organ verwendet ein verbotenes KI-System (Artikel 5). Der EDSB kann bis zu 1,5 Mio. EUR verhängen.*

C. Bemessungskriterien

- **Artikel, Schwere, Dauer**: Entscheidend sind Ausmaß und Folgen des Verstoßes.
- **Verantwortungsgrad**: Welche organisatorischen oder technischen Maßnahmen wurden ergriffen?
- **Schadensminderung**: Wurden Maßnahmen getroffen, um den Schaden für Betroffene zu reduzieren?

- **Kooperationsbereitschaft**: Zusammenarbeit mit dem EDSB wirkt bußgeldmindernd.
- **Vorverstöße**: Frühere Verstöße erhöhen die Sanktion.
- **Meldeverhalten**: Selbstanzeige oder Verschweigen spielt eine Rolle.
- **Jahreshaushalt**: Finanzkraft des Organs begrenzt die Bußgeldhöhe.

Beispiel: *Ein EU-Amt meldet selbstständig einen Verstoß und ergreift sofort Abhilfemaßnahmen. Dies führt zu einer geringeren Geldbuße.*

D. Verfahrensrechte

- **Anhörungspflicht**: Betroffene Stelle muss Gelegenheit zur Stellungnahme erhalten.
- **Verteidigungsrechte**: Voller Schutz, einschließlich Akteneinsicht.
- **Beteiligung von Beschwerdeführern**: Falls vorhanden, müssen diese eng eingebunden werden.

Beispiel: *Ein EU-Organ wird vor Erlass einer Geldbuße angehört und erhält Einsicht in die Verfahrensunterlagen.*

E. Haushaltsrechtliche Besonderheiten

- **Verwendung der Geldbußen**: Fließen in den Gesamthaushalt der Union.
- **Betriebsfähigkeitsschutz**: Geldbuße darf nicht die Funktionsfähigkeit des betroffenen Organs gefährden.

F. Berichtspflicht

Jährliche Mitteilungspflicht: Der EDSB informiert die Kommission über verhängte Bußgelder und eingeleitete Verfahren.

III. Zusammenfassung

Zuständig	EDSB
Adressaten	EU-Organe, Einrichtungen, sonstige Stellen
Kriterien	Schwere, Dauer, Verantwortung, Kooperation, Vorverstöße, Haushalt
Höhe	1,5 Mio. EUR (Artikel 5 KI-VO), sonst 750.000 EUR
Verfahren	Anhörung, Verteidigungsrechte, Einbeziehung Beschwerdeführer
Verwendung	Gesamthaushalt der EU
Bericht	Jährlich an die Kommission

IV. Quellenverzeichnis

- Erwägungsgründe 168, 169 KI-VO (EU) 2024/1689

Artikel 101 KI-VO

Geldbußen für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

(1) Die Kommission kann gegen Anbieter von KI-Modellen mit allgemeinem Verwendungszweck Geldbußen von bis zu 3 % ihres gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr oder 15 000 000 EUR verhängen, je nachdem, welcher Betrag höher ist, wenn sie feststellt, dass der Anbieter vorsätzlich oder fahrlässig

a) gegen die einschlägigen Bestimmungen dieser Verordnung verstoßen hat;

b) der Anforderung eines Dokuments oder von Informationen gemäß Artikel 91 nicht nachgekommen ist oder falsche, unvollständige oder irreführende Informationen bereitgestellt hat;

c) einer gemäß Artikel 93 geforderten Maßnahme nicht nachgekommen ist;

d) der Kommission keinen Zugang zu dem KI-Modell mit allgemeinem Verwendungszweck oder dem KI-Modell mit allgemeinem Verwendungszweck mit systemischem Risiko gewährt hat, um eine Bewertung gemäß Artikel 92 durchzuführen.

Bei der Festsetzung der Höhe der Geldbuße oder des Zwangsgelds wird der Artikel, der Schwere und der Dauer des Verstoßes sowie den Grundsätzen der Verhältnismäßigkeit und der Angemessenheit gebührend Rechnung getragen. Die Kommission berücksichtigt außerdem Verpflichtungen, die gemäß Artikel 93 Absatz 3 oder in den einschlägigen Praxisleitfäden nach Artikel 56 gemacht wurden.

(2) Vor der Annahme einer Entscheidung nach Absatz 1 teilt die Kommission dem Anbieter des KI-Modells mit allgemeinem Verwendungszweck ihre vorläufige Beurteilung mit und gibt ihm Gelegenheit, Stellung zu nehmen.

(3) Die gemäß diesem Artikel verhängten Geldbußen müssen wirksam, verhältnismäßig und abschreckend sein.

(4) Informationen über gemäß diesem Artikel verhängte Geldbußen werden gegebenenfalls dem KI-Gremium mitgeteilt.

(5) Der Gerichtshof der Europäischen Union hat die unbeschränkte Befugnis zur Überprüfung der Entscheidungen der Kommission über die

Festsetzung einer Geldbuße gemäß diesem Artikel. Er kann die verhängte Geldbuße aufheben, herabsetzen oder erhöhen.

(6) Die Kommission erlässt Durchführungsrechtsakte mit detaillierten Regelungen und Verfahrensgarantien für die Verfahren im Hinblick auf den möglichen Erlass von Beschlüssen gemäß Absatz 1 dieses Artikels. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 98 Absatz 2 genannten Prüfverfahren erlassen.

I. Worum geht es?

Artikel 101 regelt die Geldbußen für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck. Die Kommission kann empfindliche Strafen verhängen, wenn Anbieter gegen ihre Pflichten verstoßen. Ziel ist es, die Einhaltung der Verordnung wirksam durchzusetzen und gleiche Wettbewerbsbedingungen zu schaffen.

II. Detailkommentar

A. Adressaten

- **Anbieter von KI-Modellen mit allgemeinem Verwendungszweck**: Nur sie können nach Artikel 101 sanktioniert werden. Anbieter anderer KI-Systeme fallen unter die allgemeine Sanktionsregelung der Mitgliedstaaten.

B. Voraussetzungen für Geldbußen

- **Vorsatz oder Fahrlässigkeit**: Geldbußen setzen ein schuldhaftes Verhalten voraus. Reine technische Fehler ohne Verschulden sind nicht erfasst.
- **Verstöße gegen einschlägige Bestimmungen**: Dazu zählen alle Pflichten aus der KI-VO, die speziell Anbieter von allgemeinen KI-Modellen betreffen.
- **Nichtbefolgung von Auskunfts- und Mitwirkungspflichten**: Artikel 91 KI-VO verpflichtet zur Bereitstellung von Dokumenten und

Informationen. Unvollständige oder falsche Angaben sind bußgeldbewehrt.

- **Missachtung von Maßnahmen nach Artikel 93 KI-VO**: Die Kommission kann bestimmte Abhilfemaßnahmen anordnen. Werden diese ignoriert, droht eine Sanktion.
- **Verweigerung des Zugangs zu Modellen**: Nach Artikel 92 KI-VOkann die Kommission ein Modell prüfen. Anbieter müssen Zugang gewähren, sonst riskieren sie eine Geldbuße.

Beispiel: *Ein Anbieter verweigert der Kommission Einsicht in die Trainingsdaten seines Modells. Dies stellt einen klaren Verstoß dar und kann mit Geldbuße belegt werden.*

C. Höhe der Geldbußen

- **Obergrenze**: Bis zu 3 % des weltweiten Jahresumsatzes oder 15 Mio. EUR, je nachdem, was höher ist. Diese Regel soll sicherstellen, dass auch große Unternehmen spürbar sanktioniert werden können.
- **Bemessungskriterien**: Artikel, Schwere, Dauer des Verstoßes, Verhältnismäßigkeit und Angemessenheit. Besonderheiten kleiner Anbieter (zB Start-ups) sind zu berücksichtigen (vgl Erwägungsgrund 168).
- **Leitfäden und Verpflichtungen**: Selbst eingegangene Verpflichtungen (zB nach Artikel 93 KI-VO Absatz 3) werden bei der Bewertung berücksichtigt.

Beispiel: *Ein Start-up verletzt eine Dokumentationspflicht. Wegen der geringen Unternehmensgröße und der kurzen Dauer des Verstoßes könnte die Kommission eine geringere Geldbuße verhängen.*

D. Verfahren

1. **Anhörung**: Vor einer Entscheidung muss die Kommission ihre vorläufige Einschätzung mitteilen und dem Anbieter Gelegenheit zur Stellungnahme geben. Damit wird das rechtliche Gehör gewahrt.

2. **Wirksamkeit, Verhältnismäßigkeit, Abschreckung**: Geldbußen müssen so ausgestaltet sein, dass sie Verstöße verhindern, aber nicht übermäßig belasten.
3. **Mitteilung an das KI-Gremium**: Informationen über verhängte Bußgelder werden weitergegeben, um Transparenz und Koordination zu sichern.
4. **Rechtskontrolle durch den EuGH**: Der Gerichtshof hat volle Überprüfungsbefugnis. Er kann Geldbußen aufheben, herabsetzen oder sogar erhöhen.
5. **Durchführungsrechtsakte**: Die Kommission erlässt zusätzliche Detailregeln zum Verfahren (zB Fristen, Anhörungsrechte).

E. Besonderheiten

- **Unionsweite Harmonisierung**: Anders als bei anderen KI-Systemen sind hier nicht die Mitgliedstaaten zuständig, sondern die Kommission selbst. Dies unterstreicht die besondere Bedeutung von KI-Modellen mit allgemeinem Verwendungszweck.
- **Starker Abschreckungscharakter**: Die hohe Bußgeldobergrenze ähnelt der DSGVO und zeigt, dass Verstöße als schwerwiegend gelten.

III. Zusammenfassung

Adressaten	Anbieter von KI-Modellen mit allgemeinem Verwendungszweck
Tatbestände	Verstöße gegen Pflichten, fehlende Auskünfte, Missachtung von Maßnahmen, verweigerter Zugang
Schuld	Vorsatz oder Fahrlässigkeit erforderlich
Höhe	Bis 3 % Umsatz oder 15 Mio EUR (höherer Wert maßgeblich)
Kriterien	Artikel, Schwere, Dauer, Verhältnismäßigkeit, KMU-Berücksichtigung
Verfahren	Anhörung, Mitteilung ans KI-Gremium, volle Kontrolle durch EuGH

Besonderheit	Zentrale Zuständigkeit der Kommission, hohe Abschreckungskraft

IV. Quellenverzeichnis

- ErwGr 168, 169 KI-VO (EU) 2024/1689

Artikel 102 KI-VO

Änderung der Verordnung (EG) Nr 300/2008

In Artikel 4 Absatz 3 der Verordnung (EG) Nr 300/2008 wird folgender Unterabsatz angefügt:

„Beim Erlass detaillierter Maßnahmen, die technische Spezifikationen und Verfahren für die Genehmigung und den Einsatz von Sicherheitsausrüstung betreffen, bei der auch Systeme der künstlichen Intelligenz im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates zum Einsatz kommen, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

I. Worum geht es?

Artikel 102 KI-VO ergänzt die bestehende Verordnung (EG) Nr 300/2008 über die Sicherheit der Zivilluftfahrt. Es wird klargestellt, dass beim Einsatz von KI-Systemen in Sicherheitsausrüstungen für Flughäfen und Flugzeuge die in der KI-VO vorgesehenen Anforderungen für Hochrisiko-KI-Systeme beachtet werden müssen. Ziel ist die einheitliche Anwendung der KI-VO auch in diesem besonders sensiblen Sicherheitsbereich.

II. Detailkommentar

A. Einbindung der KI-VO in die Luftsicherheit

- **Klarstellung**: Die Luftsicherheitsverordnung (EG) Nr 300/2008 regelt Maßnahmen zum Schutz der Zivilluftfahrt vor Angriffen und Gefahren. Durch Artikel 102 wird diese Verordnung mit der KI-VO verknüpft.
- **Konkretisierung**: Sobald KI-Systeme in Sicherheitsausrüstungen eingesetzt werden – etwa bei Körperscannern, Gepäckkontrollen oder Zugangskontrollsystemen – müssen die besonderen Anforderungen für Hochrisiko-KI-Systeme nach Kapitel III Abschnitt 2 KI-VO berücksichtigt werden.
- **Folge**: Hersteller und Betreiber solcher Systeme müssen die KI-VO bei der Entwicklung, Zulassung und Anwendung zwingend einhalten.

Beispiel: *Ein Hersteller entwickelt ein KI-gestütztes Körperscannersystem, das automatisch gefährliche Gegenstände erkennt. Bei der Zulassung des Geräts muss nicht nur das Luftsicherheitsrecht erfüllt werden, sondern auch die Anforderungen der KI-VO, wie etwa Risikomanagement, Datenqualität und Transparenz.*

B. Verhältnis zu bestehenden Verfahren

- **Ergänzung, keine Ablösung**: Die bestehenden Zulassungs- und Prüfverfahren nach der Luftsicherheitsverordnung bleiben bestehen. Sie werden jedoch um die KI-spezifischen Anforderungen erweitert.
- **Systematische Auslegung**: Dies verhindert, dass KI-Systeme als „Sonderfall" behandelt werden, und sorgt für Kohärenz mit den anderen sektoralen Rechtsakten, die im Erwägungsgrund 49 aufgezählt sind.

Beispiel: *Ein Zugangskontrollsystem mit Gesichtserkennung am Flughafen muss nicht nur nach Luftsicherheitsrecht genehmigt werden, sondern auch die KI-VO-Anforderungen erfüllen, etwa die Überprüfung auf diskriminierungsfreie Datenverwendung.*

C. Besonderheiten

- **Sicherheitskritische Systeme**: Gerade im Bereich der Luftsicherheit bestehen besonders hohe Anforderungen, da Fehler oder Manipulationen gravierende Folgen haben könnten.
- **Zusätzliche Sensibilisierung**: Artikel 102 betont daher ausdrücklich, dass die KI-VO-Anforderungen nicht übersehen werden dürfen, wenn KI-Systeme Teil der Sicherheitsinfrastruktur werden.

III. Zusammenfassung

Einbindung	Verknüpfung der Luftsicherheitsverordnung mit der KI-VO
Anwendungsfall	KI-Systeme in Sicherheitsausrüstungen für Flughäfen und Flugzeuge

Pflicht	Anforderungen nach Kapitel III Abschnitt 2 KI-VO müssen eingehalten werden
Verhältnis	Ergänzung der bestehenden Verfahren, keine Ersetzung

IV. Quellenverzeichnis

- Erwägungsgrund 49 KI-VO (EU) 2024/1689
- Artikel 4 VO (EG) 2008/300

Artikel 103 KI-VO

Änderung der Verordnung (EU) Nr 167/2013

In Artikel 17 Absatz 5 der Verordnung (EU) Nr 167/2013 wird folgender Unterabsatz angefügt:

„Beim Erlass delegierter Rechtsakte nach Unterabsatz 1, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

I. Worum geht es?

Artikel 103 KI-VO ergänzt die bestehende Verordnung (EU) Nr 167/2013 über die Genehmigung und Marktüberwachung von land- und forstwirtschaftlichen Fahrzeugen. Es wird klargestellt, dass beim Erlass von delegierten Rechtsakten, die sich auf KI-Systeme als Sicherheitsbauteile beziehen, die Anforderungen der KI-VO für Hochrisiko-KI-Systeme zu berücksichtigen sind. Ziel ist es, die sektorale Fahrzeugregulierung mit den allgemeinen Vorgaben der KI-VO zu verknüpfen.

II. Detailkommentar

A. Einbindung der KI-VO in die Fahrzeugregulierung

- **Grundgedanke**: Die Verordnung (EU) Nr 167/2013 regelt die Genehmigungsvoraussetzungen für land- und forstwirtschaftliche Fahrzeuge. Durch Artikel 103 wird sie mit den Anforderungen der KI-VO verknüpft.
- **Klarstellung**: Sobald in sicherheitsrelevanten Fahrzeugbauteilen – zB Bremssysteme, Lenkung oder Sensoren – KI-Systeme integriert werden, gelten zusätzlich die besonderen Anforderungen der KI-VO.
- **Folge**: Die Kommission muss bei der Ausarbeitung delegierter Rechtsakte die Vorgaben zu Hochrisiko-KI-Systemen aus Kapitel III Abschnitt 2 der KI-VO berücksichtigen.

Beispiel: *Ein Hersteller entwickelt ein KI-gestütztes Bremssystem für Traktoren, das automatisch Gefahren erkennt und den Bremsvorgang einleitet. Bei der Genehmigung müssen sowohl die Vorgaben der Fahrzeugverordnung als auch die KI-VO-Anforderungen – etwa zu Datenqualität, Risikomanagement und Transparenz – erfüllt werden.*

B. Verhältnis zu bestehenden Verfahren

- **Ergänzung, keine Ersetzung**: Die bisherigen Zulassungsverfahren der Verordnung (EU) Nr 167/2013 bleiben bestehen, werden jedoch durch die KI-VO-Anforderungen erweitert.
- **Systematische Auslegung**: Damit wird gewährleistet, dass KI-Systeme nicht als Sonderfall behandelt werden, sondern in die bestehende Fahrzeugregulierung integriert sind.

Beispiel: *Ein KI-gestütztes Sensorsystem zur Stabilitätskontrolle muss die Prüfungen nach dem Fahrzeugrecht durchlaufen und zugleich die KI-VO-Anforderungen nachweisen.*

C. Besonderheiten

- **Sicherheitsrelevante Systeme**: Gerade bei Fahrzeugen, die im öffentlichen Straßenverkehr oder bei Arbeiten mit hohem Gefahrenpotenzial eingesetzt werden, ist die Zuverlässigkeit der KI-Systeme besonders kritisch.
- **Risikominimierung**: Artikel 103 betont die Notwendigkeit, die KI-VO-Anforderungen zwingend einzubeziehen, um Risiken für Fahrer, Passanten und Umwelt zu reduzieren.

III. Zusammenfassung

Einbindung	Verknüpfung der Fahrzeugverordnung (EU) Nr 167/2013 mit der KI-VO
Anwendungsfall	KI-Systeme in sicherheitsrelevanten Bauteilen von Land- und Forstfahrzeugen
Pflicht	Anforderungen nach Kapitel III Abschnitt 2 KI-VO müssen berücksichtigt werden

Verhältnis	Ergänzung der bestehenden Verfahren, keine Ersetzung

IV. Quellenverzeichnis

- Erwägungsgrund 49 KI-VO (EU) 2024/1689
- Artikel 17 VO (EU) 2013/167

Artikel 104 KI-VO

Änderung der Verordnung (EU) Nr 168/2013

In Artikel 22 Absatz 5 der Verordnung (EU) Nr 168/2013 wird folgender Unterabsatz angefügt:

„Beim Erlass delegierter Rechtsakte nach Unterabsatz 1, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

I. Worum geht es?

Artikel 104 KI-VO ergänzt die Verordnung (EU) Nr 168/2013, die die Genehmigung und Marktüberwachung von zwei- oder dreirädrigen und vierrädrigen Fahrzeugen regelt. Es wird klargestellt, dass beim Erlass delegierter Rechtsakte für KI-Systeme, die als Sicherheitsbauteile dieser Fahrzeuge eingesetzt werden, die besonderen Anforderungen an Hochrisiko-KI-Systeme nach Kapitel III Abschnitt 2 KI-VO zu berücksichtigen sind. Ziel ist die einheitliche Einbindung der KI-VO in den Bereich der Fahrzeugsicherheit.

II. Detailkommentar

A. Einbindung der KI-VO in das Fahrzeugrecht

- **Klarstellung**: Die Verordnung (EU) Nr 168/2013 enthält technische Anforderungen und Verfahren für Fahrzeuge. Durch Artikel 104 wird ausdrücklich festgelegt, dass auch die KI-VO zu berücksichtigen ist, wenn KI-Systeme sicherheitsrelevante Bauteile darstellen.
- **Konkretisierung**: Sobald KI-Systeme für sicherheitsrelevante Funktionen wie Bremsen, Stabilitätskontrollen oder Kollisionsvermeidung genutzt werden, greifen die Hochrisiko-Vorgaben der KI-VO.
- **Folge**: Hersteller solcher Systeme müssen zusätzlich zu den bestehenden fahrzeugrechtlichen Vorschriften auch die KI-spezifischen Anforderungen erfüllen.

Beispiel: *Ein Hersteller entwickelt ein KI-gestütztes Antiblockiersystem (ABS), das nicht nur das Blockieren der Räder verhindert, sondern auch lernfähig auf unterschiedliche Straßenbedingungen reagiert. Für die Zulassung müssen sowohl die Vorgaben des Fahrzeugrechts als auch die Anforderungen der KI-VO, zB Risikomanagement und Transparenz, eingehalten werden.*

B. Verhältnis zu bestehenden Verfahren

- **Ergänzung, keine Ablösung**: Die bisherigen Verfahren der Fahrzeugverordnung bleiben bestehen, sie werden durch die KI-Vorgaben erweitert.
- **Systematische Einordnung**: Damit wird sichergestellt, dass KI-Systeme nicht losgelöst betrachtet werden, sondern nahtlos in das bestehende Fahrzeugzulassungsrecht eingebettet sind.

Beispiel: *Ein Fahrzeugsensor mit KI-Funktionalität zur Hinderniserkennung muss sowohl die fahrzeugrechtlichen Sicherheitsprüfungen bestehen als auch die KI-VO-Anforderungen erfüllen, insbesondere hinsichtlich Datenqualität und menschlicher Aufsicht.*

C. Besonderheiten

- **Sicherheitskritischer Bereich**: Gerade bei Fahrzeugen hängt die Sicherheit unmittelbar vom fehlerfreien Funktionieren technischer Systeme ab. Der Einsatz von KI erfordert daher besonders strenge Anforderungen.
- **Harmonisierung**: Artikel 104 sorgt dafür, dass für alle sicherheitsrelevanten Fahrzeug-KI-Systeme einheitliche Standards gelten, unabhängig von nationalen Unterschieden.

III. Zusammenfassung

Einbindung	Verknüpfung der Fahrzeugverordnung (EU) Nr 168/2013 mit der KI-VO
Anwendungsfall	KI-Systeme als Sicherheitsbauteile in Fahrzeugen

Pflicht	Anforderungen nach Kapitel III Abschnitt 2 KI-VO müssen berücksichtigt werden
Verhältnis	Ergänzung bestehender Verfahren, keine Ersetzung

IV. Quellenverzeichnis

- Erwägungsgrund 49 KI-VO (EU) 2024/1689
- Artikel 22 VO (EU) 2013/168

Artikel 105 KI-VO

Änderung der Richtlinie 2014/90/EU

In Artikel 8 der Richtlinie 2014/90/EU wird folgender Absatz angefügt:

„(5) Bei Systemen der künstlichen Intelligenz, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates handelt, berücksichtigt die Kommission bei der Ausübung ihrer Tätigkeiten nach Absatz 1 und bei Erlass technischer Spezifikationen und Prüfnormen nach den Absätzen 2 und 3 die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen.

I. Worum geht es?

Artikel 105 KI-VO ergänzt die Richtlinie 2014/90/EU über Schiffsausrüstung. Er stellt klar, dass die Kommission bei technischen Vorgaben für Sicherheitsbauteile mit KI-Systemen die Anforderungen an Hochrisiko-KI nach Kapitel III Abschnitt 2 KI-VO berücksichtigen muss. Ziel ist eine einheitliche Anwendung der KI-VO im Bereich der maritimen Sicherheit.

II. Detailkommentar

A. Einbindung der KI-VO in die Schiffsausrüstung

- **Klarstellung**: Die Richtlinie 2014/90/EU regelt die Anforderungen an Schiffsausrüstung, die für die Sicherheit auf See entscheidend ist. Mit Artikel 105 wird nun die Brücke zur KI-VO geschlagen.
- **Konkretisierung**: Sobald KI-Systeme als Sicherheitsbauteile in Schiffsausrüstung eingebaut sind – etwa in Navigationssystemen oder Kollisionswarnsystemen – gelten zusätzlich die Anforderungen der KI-VO.
- **Folge**: Hersteller und Betreiber solcher Systeme müssen nicht nur die Schifffahrtsvorschriften, sondern auch die speziellen Hochrisiko-Anforderungen für KI-Systeme einhalten.

Beispiel: *Ein Hersteller entwickelt ein KI-gestütztes Radarsystem, das automatisch Kurskorrekturen bei drohenden Kollisionen berechnet. Bei der Zulassung muss sowohl das Schifffahrtsrecht eingehalten werden als auch die KI-VO, etwa Anforderungen an Datenqualität und Transparenz.*

B. Verhältnis zu bestehenden Verfahren

- **Ergänzung, keine Ersetzung**: Die bestehenden Prüf- und Zertifizierungsmechanismen der Schiffsausrüstungsrichtlinie bleiben bestehen. Sie werden lediglich um die KI-Anforderungen erweitert.
- **Systematische Einordnung**: Damit wird sichergestellt, dass KI nicht isoliert, sondern kohärent im Rahmen des maritimen Sicherheitsrechts berücksichtigt wird.

Beispiel: *Ein automatisiertes Steuerungssystem auf einem Schiff muss die Zertifizierung nach Schifffahrtsrecht durchlaufen. Kommt KI zum Einsatz, sind zusätzlich die KI-VO-Anforderungen, etwa ein Risikomanagementsystem, einzuhalten.*

C. Besonderheiten

- **Sicherheitskritische Systeme**: Fehler oder Manipulationen in der Schifffahrt können katastrophale Folgen haben. Daher ist die ausdrückliche Berücksichtigung der KI-VO hier besonders wichtig.
- **Technische Spezifikationen**: Die Kommission muss bei Normen und Standards für Schiffsausrüstung die KI-VO-Anforderungen zwingend berücksichtigen. Damit wird einheitlicher Schutz auf hoher See gewährleistet.

III. Zusammenfassung

Einbindung	Schiffsausrüstungsrichtlinie wird mit der KI-VO verknüpft
Anwendungsfall	KI-Systeme als Sicherheitsbauteile in Schiffsausrüstung
Pflicht	Anforderungen nach Kapitel III Abschnitt 2 KI-VO müssen eingehalten werden

Verhältnis	Ergänzung bestehender Verfahren, keine Ersetzung

IV. Quellenverzeichnis

- Erwägungsgrund 49 KI-VO (EU) 2024/1689
- Artikel 8 RL (EU) 2014/90

Artikel 106 KI-VO

Änderung der Richtlinie (EU) 2016/797

In Artikel 5 der Richtlinie (EU) 2016/797 wird folgender Absatz angefügt:

„(12) Beim Erlass von delegierten Rechtsakten nach Absatz 1 und von Durchführungsrechtsakten nach Absatz 11, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

I. Worum geht es?

Artikel 106 KI-VO ergänzt die Eisenbahnrichtlinie (EU) 2016/797. Er stellt sicher, dass beim Erlass von Rechtsakten für KI-Systeme, die als Sicherheitsbauteile im Eisenbahnsektor eingesetzt werden, die Anforderungen der KI-VO für Hochrisiko-KI-Systeme beachtet werden. Ziel ist die kohärente Einbindung der KI-VO in die Sicherheitsregeln des europäischen Eisenbahnrechts.

II. Detailkommentar

A. Einbindung der KI-VO in das Eisenbahnrecht

- **Verknüpfung**: Die Richtlinie (EU) 2016/797 regelt die Interoperabilität des Eisenbahnsystems in der Union. Durch Artikel 106 wird diese mit der KI-VO verknüpft.
- **Konkretisierung**: Sobald KI-Systeme als Sicherheitsbauteile im Eisenbahnbereich eingesetzt werden – etwa in Bremssystemen, Signaltechnik oder automatisierten Steuerungseinheiten – müssen die speziellen Anforderungen für Hochrisiko-KI-Systeme nach Kapitel III Abschnitt 2 KI-VO berücksichtigt werden.
- **Folge**: Hersteller und Betreiber solcher Systeme müssen neben den eisenbahnrechtlichen Vorschriften auch die KI-VO zwingend einhalten.

Beispiel: *Ein Hersteller entwickelt ein KI-gestütztes Signalsystem, das automatisch Zugbewegungen steuert. Bei der Zulassung muss neben den eisenbahnrechtlichen Anforderungen auch die KI-VO beachtet werden, etwa hinsichtlich Risikomanagement, Datenqualität und Transparenz.*

B. Verhältnis zu bestehenden Verfahren

- **Ergänzung, keine Ersetzung**: Die bestehenden Genehmigungs- und Konformitätsbewertungsverfahren nach dem Eisenbahnrecht bleiben erhalten. Sie werden jedoch um die KI-spezifischen Vorgaben erweitert.
- **Systematische Auslegung**: Dies sorgt dafür, dass KI-Systeme nicht isoliert betrachtet, sondern in das bestehende Sicherheitsgefüge integriert werden.

Beispiel: *Ein automatisiertes Bremssystem für Züge wird nicht nur nach eisenbahnrechtlichen Kriterien geprüft, sondern zusätzlich auf die Einhaltung der KI-VO-Anforderungen wie Robustheit und Nachvollziehbarkeit.*

C. Besonderheiten

- **Sicherheitskritische Bedeutung**: Der Eisenbahnverkehr ist ein besonders sensibler Bereich, da Fehlfunktionen unmittelbar Menschenleben gefährden können.
- **Zusätzliche Absicherung**: Artikel 106 verdeutlicht, dass KI-Systeme in diesem Bereich den hohen Standards der KI-VO genügen müssen und diese nicht hinter sektoralen Vorschriften zurücktreten.

III. Zusammenfassung

Einbindung	KI-VO wird in das Eisenbahnrecht integriert
Anwendungsfall	KI-Systeme als Sicherheitsbauteile im Schienenverkehr
Pflicht	Anforderungen nach Kapitel III Abschnitt 2 KI-VO müssen eingehalten werden

Verhältnis	Ergänzung der bestehenden eisenbahnrechtlichen Verfahren, keine Ersetzung

IV. Quellenverzeichnis

- Erwägungsgrund 49 KI-VO (EU) 2024/1689
- Artikel 5 RL (EU) 2016/797

Artikel 107 KI-VO

Änderung der Verordnung (EU) 2018/858

In Artikel 5 der Verordnung (EU) 2018/858 wird folgender Absatz angefügt:

„(4) Beim Erlass delegierter Rechtsakte nach Absatz 3, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

I. Worum geht es?

Artikel 107 KI-VO ergänzt die Verordnung (EU) 2018/858, die den Rahmen für die Genehmigung und Marktüberwachung von Kraftfahrzeugen bildet. Neu ist, dass beim Erlass von delegierten Rechtsakten, die sich auf KI-Systeme in sicherheitsrelevanten Fahrzeugbauteilen beziehen, zwingend die Anforderungen aus Kapitel III Abschnitt 2 KI-VO berücksichtigt werden müssen. Damit wird eine klare Verbindung zwischen dem Fahrzeugrecht und den Vorschriften für Hochrisiko-KI-Systeme hergestellt.

II. Detailkommentar

A. Einbindung der KI-VO in das Fahrzeugrecht

- **Verknüpfung mit Sicherheitsbauteilen**: Die Verordnung (EU) 2018/858 regelt, wie Fahrzeuge und deren sicherheitsrelevante Bauteile genehmigt werden. Artikel 107 stellt klar, dass KI-Systeme in solchen Bauteilen denselben hohen Anforderungen wie andere Hochrisiko-KI-Systeme unterliegen.
- **Rechtsangleichung**: Damit wird verhindert, dass für sicherheitsrelevante Fahrzeugkomponenten mit KI-Technologie parallele, widersprüchliche Vorgaben entstehen.

Beispiel: *Ein KI-gestütztes Notbremsassistenzsystem fällt als sicherheitsrelevantes Bauteil unter die Fahrzeugverordnung. Bei der Genehmigung müssen die Vorgaben der KI-VO – etwa Risikomanagement, Datenqualität oder Transparenzpflichten – beachtet werden.*

B. Verhältnis zu bestehenden Verfahren

- **Ergänzende Anforderungen**: Die bestehenden Genehmigungsverfahren im Fahrzeugrecht bleiben unverändert. Neu ist nur, dass zusätzlich die KI-VO-Anforderungen verpflichtend einbezogen werden müssen.
- **Systematische Auslegung**: Artikel 107 folgt dem in Erwägungsgrund 49 beschriebenen Prinzip, sektorale Rechtsakte um KI-spezifische Anforderungen zu ergänzen, ohne die bisherigen Prüf- und Aufsichtsmechanismen auszuschalten.

Beispiel: *Ein KI-basiertes Lenksystem muss weiterhin die klassischen Fahrzeugsicherheitsprüfungen bestehen, zusätzlich aber die Anforderungen der KI-VO erfüllen, etwa durch eine Dokumentation der Trainingsdaten.*

C. Besonderheiten

- **Sicherheitskritischer Bereich**: Da es hier um Verkehrssicherheit geht, können Fehler von KI-Systemen direkt zu Unfällen mit erheblichen Folgen führen.
- **Stärkung der Rechtssicherheit**: Durch die ausdrückliche Erwähnung in Artikel 107 wird klargestellt, dass die KI-VO nicht neben, sondern innerhalb der bestehenden Fahrzeugvorschriften gilt.

III. Zusammenfassung

Bereich	Inhalt
Einbindung	Verknüpfung der Fahrzeugverordnung mit der KI-VO
Anwendungsfall	KI-Systeme in sicherheitsrelevanten Fahrzeugbauteilen
Pflicht	Anforderungen nach Kapitel III Abschnitt 2 KI-VO müssen eingehalten werden
Verhältnis	Ergänzung der bestehenden Verfahren, keine Ersetzung

IV. Quellenverzeichnis

- Erwägungsgrund 49 KI-VO (EU) 2024/1689
- Artikel 5 VO (EU) 2018/858

Artikel 108 KI-VO

Änderungen der Verordnung (EU) 2018/1139

Die Verordnung (EU) 2018/1139 wird wie folgt geändert:

1.In Artikel 17 wird folgender Absatz angefügt:

„(3) Unbeschadet des Absatzes 2 werden beim Erlass von Durchführungsrechtsakten nach Absatz 1, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates handelt, die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr 300/2008, (EU) Nr 167/2013, (EU) Nr 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (ABl. L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).“ "

2.In Artikel 19 wird folgender Absatz angefügt:

„(4) Beim Erlass delegierter Rechtsakte nach den Absätzen 1 und 2, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.“

3.In Artikel 43 wird folgender Absatz angefügt:

„(4) Beim Erlass von Durchführungsrechtsakten nach Absatz 1, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.“

4.In Artikel 47 wird folgender Absatz angefügt:

„(3) Beim Erlass delegierter Rechtsakte nach den Absätzen 1 und 2, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 handelt,

werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt."

5.In Artikel 57 wird folgender Unterabsatz angefügt:

„Beim Erlass solcher Durchführungsrechtsakte, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt."

6.In Artikel 58 wird folgender Absatz angefügt:

„(3) Beim Erlass delegierter Rechtsakte nach den Absätzen 1 und 2, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt."

I. Worum geht es?

Artikel 108 KI-VO ändert die bestehende Verordnung (EU) 2018/1139 über die Luftfahrt. Die Änderungen stellen sicher, dass bei allen Rechtsakten, die sich auf KI-Systeme in der Luftfahrt beziehen, die speziellen Anforderungen der KI-VO für Hochrisiko-KI-Systeme berücksichtigt werden. Damit wird die Luftfahrtregulierung mit der KI-VO verzahnt.

II. Detailkommentar

A. Einbindung der KI-VO in die Luftfahrt

- **Klarstellung**: Die Verordnung (EU) 2018/1139 regelt die Sicherheit in der Zivilluftfahrt, etwa bei der Zulassung von Flugzeugen oder deren Bauteilen. Artikel 108 ergänzt diese Regeln um einen Verweis auf die KI-VO.
- **Verknüpfung mit KI-VO**: Sobald in der Luftfahrt KI-Systeme als Sicherheitsbauteile verwendet werden, müssen die Anforderungen des Kapitel III Abschnitt 2 KI-VO eingehalten werden.

- **Praxisbezug**: Dies gilt insbesondere für Systeme, die sicherheitskritische Funktionen übernehmen, zB automatische Flugsicherung oder Wartungsdiagnosen.

Beispiel: *Ein Hersteller entwickelt ein KI-gestütztes Triebwerksüberwachungssystem, das potenzielle Ausfälle frühzeitig erkennt. Bei der Genehmigung des Systems muss nicht nur die Luftfahrtsicherheitsverordnung berücksichtigt werden, sondern auch die Pflichten der KI-VO, etwa Risikomanagement, Dokumentation und Transparenz.*

B. Verhältnis zu bestehenden Verfahren

- **Ergänzung, nicht Ersatz**: Die bestehenden Zulassungs- und Aufsichtsverfahren in der Luftfahrt bleiben bestehen. Sie werden lediglich durch die KI-VO ergänzt.
- **Systematische Einordnung**: Damit wird ein Gleichlauf mit anderen sektoralen Regelungen hergestellt, wie in Erwägungsgrund 49 vorgesehen.

Beispiel: *Ein KI-gestütztes Autopilotensystem wird wie bisher nach Luftfahrtrecht geprüft. Zusätzlich müssen aber auch die KI-VO-Anforderungen eingehalten werden, zB die Überprüfung auf diskriminierungsfreie Trainingsdaten.*

C. Besonderheiten

- **Sicherheitsrelevante Systeme**: Gerade in der Luftfahrt haben Fehler oder Manipulationen von KI-Systemen gravierende Folgen.
- **Hohe Standards**: Artikel 108 verdeutlicht daher, dass bei allen delegierten Rechtsakten oder Durchführungsrechtsakten die Anforderungen der KI-VO verbindlich zu berücksichtigen sind.

III. Zusammenfassung

Einbindung	Verknüpfung der Luftfahrtverordnung mit der KI-VO
Anwendungsfall	KI-Systeme als Sicherheitsbauteile in der Luftfahrt
Pflicht	Einhaltung der Anforderungen nach Kapitel III Abschnitt 2 KI-VO
Verhältnis	Ergänzung bestehender Luftfahrtsverfahren, keine Ersetzung

IV. Quellenverzeichnis

- Erwägungsgrund 49 KI-VO (EU) 2024/1689
- VO (EU) 2018/1139

Artikel 109 KI-VO

Änderung der Verordnung (EU) 2019/2144

In Artikel 11 der Verordnung (EU) 2019/2144 wird folgender Absatz angefügt:

„(3) Beim Erlass von Durchführungsrechtsakten nach Absatz 2, die sich auf Systeme der künstlichen Intelligenz beziehen, bei denen es sich um Sicherheitsbauteile im Sinne der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates handelt, werden die in Kapitel III Abschnitt 2 jener Verordnung festgelegten Anforderungen berücksichtigt.

I. Worum geht es?

Artikel 109 KI-VO ergänzt die Verordnung (EU) 2019/2144 über die allgemeine Sicherheit von Kraftfahrzeugen. Er stellt klar, dass beim Erlass von Durchführungsrechtsakten für KI-Systeme, die als sicherheitsrelevante Bauteile in Fahrzeugen eingesetzt werden, die Anforderungen der KI-VO berücksichtigt werden müssen. Damit wird gewährleistet, dass die Vorgaben für Hochrisiko-KI-Systeme auch in der Fahrzeug-Sicherheitsregulierung verbindlich zur Anwendung kommen.

II. Detailkommentar

A. Einbindung der KI-VO in die Fahrzeugsicherheit

- **Verknüpfung mit Fahrzeugrecht**: Die Verordnung (EU) 2019/2144 legt Rahmenbedingungen für die Typgenehmigung und Sicherheit von Kraftfahrzeugen fest. Durch Artikel 109 wird dieses Regelwerk mit den Anforderungen der KI-VO verknüpft.
- **Klarstellung für KI-Sicherheitsbauteile**: Sobald KI-Systeme als Sicherheitsbauteile in Fahrzeugen eingesetzt werden – etwa bei automatischen Notbremsassistenten, Spurhaltesystemen oder Fahrerüberwachungssystemen – müssen die Anforderungen der KI-VO für Hochrisiko-KI-Systeme eingehalten werden.
- **Praktische Wirkung**: Hersteller dürfen solche KI-Systeme nur dann in Verkehr bringen, wenn sie zusätzlich zu den fahrzeugrechtlichen Vorgaben auch die Vorgaben der KI-VO erfüllen.

Beispiel: *Ein Hersteller entwickelt ein KI-gestütztes Notbremssystem, das automatisch auf Fußgänger reagiert. Bei der Typgenehmigung des Fahrzeugs muss nicht nur die Fahrzeugsicherheitsverordnung eingehalten werden, sondern auch die Anforderungen der KI-VO, wie zB Risikomanagement, Datenqualität und Transparenz.*

B. Verhältnis zu bestehenden Verfahren

- **Ergänzende Anwendung**: Die bestehenden Verfahren zur Typgenehmigung und Konformitätsbewertung im Fahrzeugrecht bleiben bestehen, werden jedoch um die KI-Anforderungen ergänzt.
- **Systematische Auslegung**: Dies verhindert Doppelstrukturen oder Rechtsunsicherheiten und sorgt dafür, dass KI-Systeme nicht als Sonderfall ohne klare Regulierung behandelt werden.

Beispiel: *Ein Fahrerassistenzsystem mit KI-basierter Spurwechselkontrolle muss weiterhin nach Fahrzeugrecht geprüft werden. Zusätzlich müssen die Vorgaben der KI-VO, wie die Vermeidung diskriminierender Trainingsdaten, nachgewiesen werden.*

C. Besonderheiten

- **Sicherheitskritischer Einsatz**: Fehler in KI-Sicherheitsbauteilen können unmittelbar Leben und Gesundheit gefährden. Daher ist die ausdrückliche Verknüpfung mit der KI-VO von besonderer Bedeutung.
- **Sektorübergreifende Kohärenz**: Durch Artikel 109 wird die Einheitlichkeit der KI-VO auch im Bereich der Fahrzeugsicherheit sichergestellt, analog zu den anderen sektoralen Anpassungen (vgl Erwägungsgrund 49).

III. Zusammenfassung

Einbindung	Verknüpfung der Fahrzeug-Sicherheitsverordnung mit der KI-VO

Anwendungsfall	KI-Systeme als sicherheitsrelevante Bauteile in Fahrzeugen
Pflicht	Anforderungen nach Kapitel III Abschnitt 2 KI-VO müssen eingehalten werden
Verhältnis	Ergänzung der bestehenden Genehmigungsverfahren, keine Ablösung

IV. Quellenverzeichnis

- Erwägungsgrund 49 VO (EU) 2019/2144
- Artikel 11 VO (EU) 2019/2144

Artikel 110 KI-VO

Änderung der Richtlinie (EU) 2020/1828

In Anhang I der Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates wird die folgende Nummer angefügt:

„68. Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr 300/2008, (EU) Nr 167/2013, (EU) Nr 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)“

I. Worum geht es?

Artikel 110 KI-VO ergänzt die Richtlinie (EU) 2020/1828 über Verbandsklagen zum Schutz der Kollektivinteressen von Verbrauchern. Die KI-VO wird in den Anhang dieser Richtlinie aufgenommen. Damit wird sie zu einem der Rechtsakte, bei deren Verletzung Verbraucherverbände Verbandsklagen erheben können.

II. Detailkommentar

A. Einbindung in die Richtlinie (EU) 2020/1828

- **Richtlinie 2020/1828**: Diese regelt das Instrument der Verbandsklage, mit dem Verbraucherverbände Verstöße gegen bestimmte EU-Rechtsakte vor Gericht bringen können.
- **Neue Aufnahme**: Durch Artikel 110 wird die KI-VO in den Katalog der durchsetzbaren Rechtsakte aufgenommen.
- **Folge**: Verbraucherverbände können gegen Unternehmen klagen, wenn diese die Anforderungen der KI-VO verletzen, etwa bei Transparenz- oder Sicherheitsvorschriften für KI-Systeme.

Beispiel: *Ein Anbieter bringt ein KI-System zur Kreditwürdigkeitsprüfung auf den Markt, ohne die vorgeschriebenen Transparenzpflichten einzuhalten. Ein Verbraucher kann individuell nur schwer dagegen*

vorgehen. Dank der Änderung durch Artikel 110 können nun Verbraucherverbände eine Verbandsklage erheben, um die Einhaltung der KI-VO durchzusetzen.

B. Stärkung des Verbraucherschutzes

- **Kollektiver Rechtsschutz**: Verbraucher sind oft von KI-Systemen betroffen, ohne selbst Einfluss auf deren Funktionsweise zu haben.
- **Effektive Durchsetzung**: Durch die Möglichkeit der Verbandsklage wird gewährleistet, dass Verstöße gegen die KI-VO nicht nur theoretisch, sondern auch praktisch sanktioniert werden können.
- **Systematische Auslegung**: Die Aufnahme in die Richtlinie zeigt, dass die KI-VO nicht nur technische, sondern auch verbraucherschutzrechtliche Wirkung entfalten soll.

C. Besonderheiten

- **Schlussbestimmungen**: Artikel 110 ist Teil der Schlussbestimmungen und dient vor allem der rechtssystematischen Verknüpfung.
- **Keine inhaltliche Neuerung**: Der Artikel schafft keine neuen materiellen Pflichten, sondern sorgt für die Durchsetzbarkeit bestehender Regeln der KI-VO über das Instrument der Verbandsklage.

III. Zusammenfassung

Einbindung	KI-VO wird in den Katalog der Verbandsklagen nach der Richtlinie (EU) 2020/1828 aufgenommen
Anwendungsfall	Verbraucherverbände können bei Verstößen gegen die KI-VO klagen
Wirkung	Stärkung des Verbraucherschutzes und effektive Durchsetzung der KI-VO
Besonderheit	Formale Ergänzung, keine materiellen Neuerungen

IV. Quellenverzeichnis

- Anhang I RL (EU) 2020/1828

Artikel 111 KI-VO

Bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme und bereits in Verkehr gebrachte KI-Modelle mit allgemeinem Verwendungszweck

(1) Unbeschadet der Anwendung des Artikels 5 gemäß Artikel 113 Absatz 3 Buchstabe a werden KI-Systeme, bei denen es sich um Komponenten von IT-Großsystemen handelt, die mit den in Anhang X aufgeführten Rechtsakten eingerichtet wurden und vor dem 2. August 2027 in Verkehr gebracht oder in Betrieb genommen wurden, bis zum 31. Dezember 2030 mit dieser Verordnung in Einklang gebracht.

Die in dieser Verordnung festgelegten Anforderungen werden bei der Bewertung jedes IT-Großsystems, das mit den in Anhang X aufgeführten Rechtsakten eingerichtet wurde, berücksichtigt, wobei die Bewertung entsprechend den Vorgaben der jeweiligen Rechtsakte und bei Ersetzung oder Änderung dieser Rechtsakte erfolgt.

(2) Unbeschadet der Anwendung des Artikels 5 gemäß Artikel 113 Absatz 3 Buchstabe a gilt diese Verordnung für Betreiber von Hochrisiko-KI-Systemen — mit Ausnahme der in Absatz 1 des vorliegenden Artikels genannten Systeme —, die vor dem 2. August 2026 in Verkehr gebracht oder in Betrieb genommen wurden, nur dann, wenn diese Systeme danach in ihrer Konzeption erheblich verändert wurden. In jedem Fall treffen die Anbieter und Betreiber von Hochrisiko-KI-Systemen, die bestimmungsgemäß von Behörden verwendet werden sollen, die erforderlichen Maßnahmen für die Erfüllung der Anforderungen und Pflichten dieser Verordnung bis zum 2. August 2030.

(3) Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, die vor dem 2. August 2025 in Verkehr gebracht wurden, treffen die erforderlichen Maßnahmen für die Erfüllung der in dieser Verordnung festgelegten Pflichten bis zum 2. August 2027.

I. Worum geht es?

Artikel 111 regelt die Übergangsbestimmungen für KI-Systeme und KI-Modelle, die bereits vor dem allgemeinen Anwendungsbeginn der KI-VO in Verkehr gebracht oder in Betrieb genommen wurden. Ziel ist es, Rechtssicherheit zu schaffen, eine schrittweise Anpassung zu ermöglichen

und Marktstörungen zu vermeiden. Grundsätzlich gilt die Verordnung für bestehende Systeme nur eingeschränkt oder erst nach Ablauf bestimmter Übergangsfristen.

II. Detailkommentar

A. IT-Großsysteme

- **Besonderheit IT-Großsysteme**: KI-Systeme, die Teil von großen, durch EU-Rechtsakte geregelten IT-Systemen sind, müssen bis spätestens 31. Dezember 2030 mit der KI-VO in Einklang gebracht werden.
- **Anknüpfung an andere Rechtsakte**: Die Bewertung dieser Systeme erfolgt im Rahmen der jeweiligen Spezialgesetze, die in Anhang X KI-VO aufgelistet sind.
- **Ziel**: Gewährleistung von Kontinuität und Rechtskonformität in komplexen, europaweit eingesetzten IT-Infrastrukturen.

Beispiel: *Ein KI-System zur biometrischen Identifizierung ist Bestandteil eines EU-weiten Dateninformationssystems. Obwohl es bereits vor 2027 eingesetzt wurde, muss es bis 2030 die Anforderungen der KI-VO erfüllen.*

B. Hochrisiko-KI-Systeme

- **Grundsatz**: Hochrisiko-KI-Systeme, die vor dem 2. August 2026 auf den Markt gebracht oder in Betrieb genommen wurden, müssen die Vorgaben der KI-VO nur dann erfüllen, wenn sie danach erheblich verändert werden.
- **Ausnahme bei Behördennutzung**: Hochrisiko-Systeme, die von Behörden eingesetzt werden, müssen in jedem Fall bis spätestens 2. August 2030 die Anforderungen der KI-VO einhalten – unabhängig von späteren Änderungen.
- **Begriffsklärung**: „Erhebliche Veränderung“ ist gleichbedeutend mit „wesentliche Änderung“, dh wenn sich die Konzeption oder Zweckbestimmung eines Systems grundlegend wandelt.

Beispiel: *Eine Behörde nutzt ein KI-System zur automatisierten Kreditwürdigkeitsprüfung. Auch wenn das System unverändert bleibt, muss es bis 2030 an die Vorgaben der KI-VO angepasst werden.*

C. KI-Modelle mit allgemeinem Verwendungszweck

- **Pflicht zur Anpassung**: Anbieter von allgemeinen KI-Modellen (zB Sprachmodelle), die vor dem 2. August 2025 in Verkehr gebracht wurden, müssen bis spätestens 2. August 2027 alle Pflichten der KI-VO erfüllen.
- **Praktische Bedeutung**: Betroffen sind insbesondere große Basismodelle, die vielfach in anderen Systemen integriert werden.

Beispiel: *Ein Unternehmen bringt 2024 ein Sprachmodell auf den Markt. Dieses Modell muss bis spätestens 2027 an die Pflichten der KI-VO angepasst werden.*

D. Besonderheiten

- **Schutz der Kontinuität**: Bestehende Systeme sollen nicht abrupt vom Markt verschwinden.
- **Freiwillige Voranpassung**: Anbieter werden ermutigt, die Vorgaben bereits während der Übergangsphase einzuhalten, auch wenn dies noch nicht verpflichtend ist.

III. Zusammenfassung

Bereich	Stichtag	Anpassungspflicht
IT-Großsysteme	bis 31. Dezember 2030	Vollständige Anpassung erforderlich
Hochrisiko-KI-Systeme (außer IT-Großsysteme)	ab 2. August 2026	Nur bei erheblicher Veränderung verpflichtend; bei Behördennutzung bis 02. August 2030 zwingend

KI-Modelle mit allgemeinem Verwendungszweck	bis 2. August 2027	Anpassung zwingend erforderlich

IV. Quellenverzeichnis

- Erwägungsgründe 177, 178 KI-VO (EU) 2024/1689

Artikel 112 KI-VO

Bewertung und Überprüfung

(1) Die Kommission prüft nach Inkrafttreten dieser Verordnung und bis zum Ende der Befugnisübertragung gemäß Artikel 97 einmal jährlich, ob eine Änderung der Liste in Anhang III und der Liste der verbotenen Praktiken im KI-Bereich gemäß Artikel 5 erforderlich ist. Die Kommission übermittelt die Ergebnisse dieser Bewertung dem Europäischen Parlament und dem Rat.

(2) Bis zum 2. August 2028 und danach alle vier Jahre bewertet die Kommission Folgendes und erstattet dem Europäischen Parlament und dem Rat Bericht darüber:

a) Notwendigkeit von Änderungen zur Erweiterung bestehender Bereiche oder zur Aufnahme neuer Bereiche in Anhang III:

b) Änderungen der Liste der KI-Systeme, die zusätzliche Transparenzmaßnahmen erfordern, in Artikel 50;

c) Änderungen zur Verbesserung der Wirksamkeit des Überwachungs- und Governance-Systems.

(3) Bis zum 2. August 2029 und danach alle vier Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Bewertung und Überprüfung dieser Verordnung vor. Der Bericht enthält eine Beurteilung hinsichtlich der Durchsetzungsstruktur und der etwaigen Notwendigkeit einer Agentur der Union zur Lösung der festgestellten Mängel. Auf der Grundlage der Ergebnisse wird diesem Bericht gegebenenfalls ein Vorschlag zur Änderung dieser Verordnung beigefügt. Die Berichte werden veröffentlicht.

(4) In den in Absatz 2 genannten Berichten wird insbesondere auf folgende Aspekte eingegangen:

a) Sachstand bezüglich der finanziellen, technischen und personellen Ressourcen der zuständigen nationalen Behörden im Hinblick auf deren Fähigkeit, die ihnen auf der Grundlage dieser Verordnung übertragenen Aufgaben wirksam zu erfüllen;

b) Stand der Sanktionen, insbesondere der Bußgelder nach Artikel 99 Absatz 1, die Mitgliedstaaten bei Verstößen gegen diese Verordnung verhängt haben;

c)angenommene harmonisierte Normen und gemeinsame Spezifikationen, die zur Unterstützung dieser Verordnung erarbeitet wurden;

d)Zahl der Unternehmen, die nach Inkrafttreten dieser Verordnung in den Markt eintreten, und wie viele davon KMU sind.

(5) Bis zum 2. August 2028 bewertet die Kommission die Arbeitsweise des Büros für Künstliche Intelligenz und prüft, ob das Büro für Künstliche Intelligenz mit ausreichenden Befugnissen und Zuständigkeiten zur Erfüllung seiner Aufgaben ausgestattet wurde, und ob es für die ordnungsgemäße Durchführung und Durchsetzung dieser Verordnung zweckmäßig und erforderlich wäre, das Büro für Künstliche Intelligenz und seine Durchsetzungskompetenzen zu erweitern und seine Ressourcen aufzustocken. Die Kommission übermittelt dem Europäischen Parlament und dem Rat einen Bericht über ihre Bewertung.

(6) Bis zum 2. August 2028 und danach alle vier Jahre legt die Kommission einen Bericht über die Überprüfung der Fortschritte bei der Entwicklung von Normungsdokumenten zur energieeffizienten Entwicklung von KI-Modellen mit allgemeinem Verwendungszweck vor und beurteilt die Notwendigkeit weiterer Maßnahmen oder Handlungen, einschließlich verbindlicher Maßnahmen oder Handlungen. Dieser Bericht wird dem Europäischen Parlament und dem Rat vorgelegt und veröffentlicht.

(7) Bis zum 2. August 2028 und danach alle drei Jahre führt die Kommission eine Bewertung der Folgen und der Wirksamkeit der freiwilligen Verhaltenskodizes durch, mit denen die Anwendung der in Kapitel III Abschnitt 2 festgelegten Anforderungen an andere KI-Systeme als Hochrisiko-KI-Systeme und möglicherweise auch zusätzlicher Anforderungen an andere KI-Systeme als Hochrisiko-KI-Systeme, auch in Bezug auf deren ökologische Nachhaltigkeit, gefördert werden soll.

(8) Für die Zwecke der Absätze 1 bis 7 übermitteln das KI-Gremium, die Mitgliedstaaten und die zuständigen nationalen Behörden der Kommission auf Anfrage unverzüglich die gewünschten Informationen.

(9) Bei den in den Absätzen 1 bis 7 genannten Bewertungen und Überprüfungen berücksichtigt die Kommission die Standpunkte und Feststellungen des KI-Gremiums, des Europäischen Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen.

(10) Die Kommission legt erforderlichenfalls geeignete Vorschläge zur Änderung dieser Verordnung vor und berücksichtigt dabei insbesondere

technologische Entwicklungen, die Auswirkungen von KI-Systemen auf die Gesundheit und Sicherheit und auf die Grundrechte und die Fortschritte in der Informationsgesellschaft.

(11) Als Orientierung für die in den Absätzen 1 bis 7 genannten Bewertungen und Überprüfungen entwickelt das Büro für Künstliche Intelligenz ein Ziel und eine partizipative Methode für die Bewertung der Risikoniveaus anhand der in den jeweiligen Artikeln genannten Kriterien und für die Einbeziehung neuer Systeme in

a) die Liste gemäß Anhang III, einschließlich der Erweiterung bestehender Bereiche oder der Aufnahme neuer Bereiche in diesen Anhang;

b) die Liste der verbotenen Praktiken gemäß Artikel 5; und

c) die Liste der KI-Systeme, die zusätzliche Transparenzmaßnahmen erfordern, in Artikel 50.

(12) Eine Änderung dieser Verordnung im Sinne des Absatzes 10 oder entsprechende delegierte Rechtsakte oder Durchführungsrechtsakte, die sektorspezifische Rechtsvorschriften für eine unionsweite Harmonisierung gemäß Anhang I Abschnitt B betreffen, berücksichtigen die regulatorischen Besonderheiten des jeweiligen Sektors und die in der Verordnung festgelegten bestehenden Governance-, Konformitätsbewertungs- und Durchsetzungsmechanismen und -behörden.

(13) Bis zum 2. August 2031 nimmt die Kommission unter Berücksichtigung der ersten Jahre der Anwendung der Verordnung eine Bewertung der Durchsetzung dieser Verordnung vor und erstattet dem Europäischen Parlament, dem Rat und dem Europäischen Wirtschafts- und Sozialausschuss darüber Bericht. Auf Grundlage der Ergebnisse wird dem Bericht gegebenenfalls ein Vorschlag zur Änderung dieser Verordnung beigefügt, der die Struktur der Durchsetzung und die Notwendigkeit einer Agentur der Union für die Lösung festgestellter Mängel betrifft.

I. Worum geht es?

Artikel 112 legt fest, wie die Kommission die Verordnung regelmäßig bewertet und überprüft. Ziel ist es, sicherzustellen, dass die KI-VO auch in Zukunft wirksam bleibt und an technologische Entwicklungen angepasst wird. Dazu sind feste Fristen, Prüfaufgaben und Berichtspflichten

vorgesehen. Im Kern geht es also um die **Dynamik und Weiterentwicklung** der Verordnung.

II. Detailkommentar

A. Jährliche Überprüfung

- **Prüfung von Anhang III KI-VO und Verboten**: Die Kommission prüft jährlich, ob die Liste der Hochrisiko-KI-Systeme (Anhang III KI-VO) oder die Liste verbotener Praktiken (Artikel 5 KI-VO) angepasst werden muss.
- **Transparenzpflicht**: Ergebnisse gehen an Parlament und Rat, um demokratische Kontrolle sicherzustellen.

Beispiel: *Eine neue KI-Technologie im Bildungsbereich entwickelt sich rasant und könnte künftig als Hochrisiko gelten. Die Kommission prüft, ob eine Aufnahme in Anhang III notwendig ist.*

B. Vierjährliche Überprüfung

- **Anhang III KI-VO**: Notwendigkeit von Änderungen oder Erweiterungen.
- **Transparenzpflichten**: Anpassung der Liste in Artikel 50 KI-VO.
- **Governance-System**: Prüfung, ob die Überwachung effektiv funktioniert.

Beispiel: *Wenn die Marktüberwachungsbehörden überlastet sind, könnte die Kommission Änderungen am Governance-System vorschlagen.*

C. Umfassende Evaluationsberichte

- **Erster Bericht 2029**, danach alle vier Jahre.
- **Inhalte**: Beurteilung der Durchsetzungsstruktur, mögliche Notwendigkeit einer EU-Agentur.
- **Veröffentlichung**: Transparenz gegenüber Öffentlichkeit und Institutionen.

D. Schwerpunkte in den Berichten

- **Ressourcen der Behörden**: Sind sie personell, finanziell und technisch so ausgestattet, dass eine wirksame Durchsetzung der Verordnung gewährleistet ist?
- **Sanktionen**: Werden Bußgelder verhängt und wirken sie?
- **Normen und Standards**: Welche Instrumente existieren hier bereits?
- **Marktentwicklung**: Zahl der neuen Unternehmen, Anteil von KMU.

E. Büro für Künstliche Intelligenz

- **Überprüfung bis 2028**: Ob es genügend Befugnisse und Ressourcen hat.
- **Mögliche Erweiterung**: Kompetenzen und Ausstattung können ausgebaut werden.

F. Spezifische Themenfelder

- **Energieeffizienz von KI**: Bis 2028 und danach alle vier Jahre Bewertung von Standards.
- **Verhaltenskodizes**: Alle drei Jahre Prüfung, wie wirksam freiwillige Standards sind.

Beispiel: *Ein freiwilliger Kodex zur umweltfreundlichen KI-Nutzung zeigt Wirkung. Die Kommission prüft, ob er verbindlich werden sollte.*

G. Informationspflichten

- **Zuarbeit**: Mitgliedstaaten, Behörden und das KI-Gremium müssen auf Anfrage Informationen liefern.
- **Einbindung**: Auch externe Stellen und Institutionen werden berücksichtigt.

H. Anpassungsmöglichkeiten

- **Technologische Entwicklung**: Anpassungen erfolgen bei neuen Risiken.
- **Sektorenspezifische Regeln**: Besondere Gegebenheiten einzelner Branchen werden berücksichtigt.

I. Langfristige Evaluierung

- **2031**: Große Überprüfung der Durchsetzung, evtl. Vorschlag für eine eigene EU-Agentur.

III. Zusammenfassung

Thema	Zeitpunkt	Inhalt
Jährliche Prüfung	jährlich	Anhang III KI-VOund Verbote (Artikel 5 KI-VO)
Erste große Überprüfung	2028	Anhang III, Transparenzpflichten, Governance
Umfassender Bericht	2029, alle vier Jahre	Durchsetzung, Agentur-Frage, Veröffentlichung
Büro für Künstliche Intelligenz	2028	Prüfung Befugnisse, evtl. Ausbau
Energieeffizienz	2028, alle vier Jahre	Normen für KI-Modelle
Verhaltenskodizes	2028, alle drei Jahre	Wirksamkeit freiwilliger Standards
Langfristige Durchsetzung	2031	Struktur, mögliche neue Agentur

IV. Quellenverzeichnis

- Erwägungsgründe 162, 164, 165, 174 KI-VO (EU) 2024/1689

Artikel 113 KI-VO

Inkrafttreten und Geltungsbeginn

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

Sie gilt ab dem 2. August 2026.

Jedoch:

a) Die Kapitel I und II gelten ab dem 2. Februar 2025;

b) Kapitel III Abschnitt 4, Kapitel V, Kapitel VII und Kapitel XII sowie Artikel 78 gelten ab dem 2. August 2025, mit Ausnahme des Artikels 101;

c) Artikel 6 Absatz 1 und die entsprechenden Pflichten gemäß dieser Verordnung gelten ab dem 2. August 2027.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Brüssel am 13. Juni 2024.

Im Namen des Europäischen Parlaments

Die Präsidentin

R. METSOLA

Im Namen des Rates

Der Präsident

M. MICHEL

I. Worum geht es?

Dieser Artikel regelt das **Inkrafttreten und den zeitlich gestaffelten Geltungsbeginn** der KI-VO. Er legt fest, ab wann die Verordnung insgesamt und in einzelnen Teilen Anwendung findet. Ziel ist es, einerseits den Betroffenen ausreichend Vorbereitungszeit einzuräumen, andererseits besonders dringliche Vorschriften früher in Kraft zu setzen.

II. Detailkommentar

A. Grundsatz

- **Inkrafttreten**: Die KI-VO tritt am 20. Tag nach Veröffentlichung im Amtsblatt in Kraft. Dies ist ein rein formaler Vorgang, ab dem die Verordnung existiert, jedoch noch nicht vollständig gilt.
- **Allgemeiner Geltungsbeginn**: Ab dem 2. August 2026 gilt die Verordnung in ihrer Gesamtheit, soweit keine Ausnahmen vorgesehen sind.

B. Staffelung der Anwendung

1. Früherer Beginn ab 2. Februar 2025

- **Kapitel I und II**: Diese enthalten die allgemeinen Vorschriften, Definitionen und Verbote unzulässiger KI-Praktiken. Ihre frühzeitige Anwendung dient dem Schutz vor besonders hohen Risiken.
- **Begründung**: Verbotene Praktiken mit „unannehmbarem Risiko" sollen bereits so früh wie möglich untersagt werden.

2. Beginn ab 2. August 2025

- **Kapitel III Abschnitt 4**: Regelt die Konformitätsbewertung für Hochrisiko-KI-Systeme.
- **Kapitel V**: Betrifft KI-Modelle mit allgemeinem Verwendungszweck.
- **Kapitel VII**: Errichtet die Leitungs- und Koordinierungsstrukturen (zB Büro für Künstliche Intelligenz).
- **Kapitel XII**: Regelt Sanktionen und deren Umsetzung.
- Artikel 78 KI-VO: Vertraulichkeit
- **Begründung**: Die Infrastruktur für Aufsicht und Kontrolle soll frühzeitig arbeitsfähig sein, damit die volle Anwendung der KI-VO 2026 gesichert ist.

3. Späterer Beginn ab 2. August 2027

- **Artikel 6 KI-VO Absatz 1**: Enthält die Kriterien zur Einstufung von Hochrisiko-KI-Systemen.
- **Entsprechende Pflichten**: Alle Vorschriften, die sich aus dieser Einstufung ergeben, werden damit erst ein Jahr nach dem allgemeinen Geltungsbeginn wirksam.
- **Begründung**: Anbieter sollen genügend Zeit haben, ihre Systeme an die komplexen Anforderungen anzupassen.

C. Besonderheiten

- **Unmittelbare Geltung**: Wie jede Verordnung ist die KI-VO in allen Mitgliedstaaten unmittelbar anwendbar, ohne dass nationale Umsetzungsgesetze erforderlich sind.
- **Übergangscharakter**: Die gestaffelte Anwendung soll ein Gleichgewicht schaffen zwischen Schutzinteressen und praktischer Umsetzbarkeit.
- **Sanktionssystem**: Damit Verstöße ab Geltungsbeginn wirksam geahndet werden können, verpflichtet Erwägungsgrund 179 die Mitgliedstaaten, ihre Sanktionen bis August 2025 festzulegen.

III. Zusammenfassung

Zeitpunkt	Regelungsinhalt
20. Tag nach Veröffentlichung	Inkrafttreten (formales Bestehen der Verordnung)
2. Februar 2025	Kapitel I und II (Verbote, allgemeine Bestimmungen)
2. August 2025	Kapitel III Abschnitt 4, Kapitel V, VII, XII; Artikel 78 KI-VO (Aufsicht, Konformitätsbewertung, GPAI, Sanktionen)
2. August 2026	Allgemeiner Geltungsbeginn der Verordnung
2. August 2027	Artikel 6 KI-VO Absatz 1 und darauf basierende Pflichten (Hochrisiko-KI)

IV. Quellenverzeichnis

- Erwägungsgrund 179 KI-VO (EU) 2024/1689

Anhang I KI-VO

Liste der Harmonisierungsrechtsvorschriften der Union

Abschnitt A — Liste der Harmonisierungsrechtsvorschriften der Union auf der Grundlage des neuen Rechtsrahmens

1.Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (ABl. L 157 vom 9.6.2006, S. 24)

2.Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates vom 18. Juni 2009 über die Sicherheit von Spielzeug (ABl. L 170 vom 30.6.2009, S. 1)

3.Richtlinie 2013/53/EU des Europäischen Parlaments und des Rates vom 20. November 2013 über Sportboote und Wassermotorräder und zur Aufhebung der Richtlinie 94/25/EG (ABl. L 354 vom 28.12.2013, S. 90)

4.Richtlinie 2014/33/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über Aufzüge und Sicherheitsbauteile für Aufzüge (ABl. L 96 vom 29.3.2014, S. 251)

5.Richtlinie 2014/34/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten für Geräte und Schutzsysteme zur bestimmungsgemäßen Verwendung in explosionsgefährdeten Bereichen (ABl. L 96 vom 29.3.2014, S. 309)

6.Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG (ABl. L 153 vom 22.5.2014, S. 62)

7.Richtlinie 2014/68/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Druckgeräten auf dem Markt (ABl. L 189 vom 27.6.2014, S. 164)

8. Verordnung (EU) 2016/424 des Europäischen Parlaments und des Rates vom 9. März 2016 über Seilbahnen und zur Aufhebung der Richtlinie 2000/9/EG (ABl. L 81 vom 31.3.2016, S. 1)

9. Verordnung (EU) 2016/425 des Europäischen Parlaments und des Rates vom 9. März 2016 über persönliche Schutzausrüstungen und zur Aufhebung der Richtlinie 89/686/EWG des Rates (ABl. L 81 vom 31.3.2016, S. 51)

10. Verordnung (EU) 2016/426 des Europäischen Parlaments und des Rates vom 9. März 2016 über Geräte zur Verbrennung gasförmiger Brennstoffe und zur Aufhebung der Richtlinie 2009/142/EG (ABl. L 81 vom 31.3.2016, S. 99)

11. Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr 178/2002 und der Verordnung (EG) Nr 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (ABl. L 117 vom 5.5.2017, S. 1)

12. Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (ABl. L 117 vom 5.5.2017, S. 176)

Abschnitt B — Liste anderer Harmonisierungsrechtsvorschriften der Union

13. Verordnung (EG) Nr 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72)

14. Verordnung (EU) Nr 168/2013 des Europäischen Parlaments und des Rates vom 15. Januar 2013 über die Genehmigung und Marktüberwachung von zwei- oder dreirädrigen und vierrädrigen Fahrzeugen (ABl. L 60 vom 2.3.2013, S. 52)

15. Verordnung (EU) Nr 167/2013 des Europäischen Parlaments und des Rates vom 5. Februar 2013 über die Genehmigung und Marktüberwachung von land- und forstwirtschaftlichen Fahrzeugen (ABl. L 60 vom 2.3.2013, S. 1)

16. Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates vom 23. Juli 2014 über Schiffsausrüstung und zur Aufhebung der Richtlinie 96/98/EG des Rates (ABl. L 257 vom 28.8.2014, S. 146)

17. Richtlinie (EU) 2016/797 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Interoperabilität des Eisenbahnsystems in der Europäischen Union (ABl. L 138 vom 26.5.2016, S. 44)

18. Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr 715/2007 und (EG) Nr 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG (ABl. L 151 vom 14.6.2018, S. 1)

19. Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EG) Nr 78/2009, (EG) Nr 79/2009 und (EG) Nr 661/2009 des Europäischen Parlaments und des Rates sowie der Verordnungen (EG) Nr 631/2009, (EU) Nr 406/2010, (EU) Nr 672/2010, (EU) Nr 1003/2010, (EU) Nr 1005/2010, (EU) Nr 1008/2010, (EU) Nr 1009/2010, (EU) Nr 19/2011, (EU) Nr 109/2011, (EU) Nr 458/2011, (EU) Nr 65/2012, (EU) Nr 130/2012, (EU) Nr 347/2012, (EU) Nr 351/2012, (EU) Nr 1230/2012 und (EU) 2015/166 der Kommission (ABl. L 325 vom 16.12.2019, S. 1)

20. Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr 2111/2005, (EG) Nr 1008/2008, (EU) Nr 996/2010, (EU) Nr 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr 552/2004 und (EG) Nr 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr 3922/91 des Rates (ABl. L 212

vom 22.8.2018, S. 1), insoweit die Konstruktion, Herstellung und Vermarktung von Luftfahrzeugen gemäß Artikel 2 Absatz 1 Buchstaben a und b in Bezug auf unbemannte Luftfahrzeuge sowie deren Motoren, Propeller, Teile und Ausrüstung zur Fernsteuerung betroffen sind

I. Worum geht es?

Anhang I enthält eine Auflistung jener **Rechtsakte zur Angleichung nationaler Regelungen** die für die Einstufung von Hochrisiko-KI-Systemen nach Artikel 6 KI-VO maßgeblich sind. Er stellt damit die Verbindung zwischen der KI-VO und bereits bestehenden sektorspezifischen Rechtsakten her, die strenge Sicherheits- und Marktüberwachungsregeln vorsehen. Auf diese Weise wird klargestellt, in welchen Produktkategorien KI-Anwendungen automatisch als Hochrisikosysteme gelten, weil sie in ohnehin stark regulierten Bereichen eingesetzt werden.

Relevante Artikel: Artikel 6 KI-VO(Klassifizierung), Artikel 43 KI-VO ff (Konformitätsbewertun, Bescheinigungen und Registrierung) sowie alle Hochrisikovorschriften.

II. Detailkommentar

A. Struktur des Anhangs

- **Abschnitt A (Neuer Rechtsrahmen)**: Hier finden sich jene Vorschriften, die auf dem sogenannten „New Legislative Framework“ (NLF) beruhen. Dazu zählen klassische Produktsektoren wie **Spielzeug**, **Medizinprodukte** oder **Gasgeräte**.
- **Abschnitt B (Sonstige Rechtsvorschriften)**: Hier sind zusätzliche Sektoren aufgelistet, die nicht vollständig unter den NLF fallen, aber dennoch strenge Sicherheitsanforderungen haben, etwa **Zivilluftfahrt**, **Kraftfahrzeuge** oder **Eisenbahnsysteme**.

B. Detaillierte Liste relevanter Sektoren

- **Maschinen** (Richtlinie 2006/42/EG): Deckt Industrieanlagen und Produktionsmaschinen ab, bei denen KI-Steuerungen sicherheitsrelevant sein können.
- **Spielzeug** (Richtlinie 2009/48/EG): Betrifft zB interaktive, KI-gesteuerte Kinderspielzeuge mit potenziellen Sicherheitsrisiken.
- **Sportboote und Wassermotorräder** (Richtlinie 2013/53/EU): Relevanz bei automatisierten Steuerungen oder Assistenzsystemen.
- **Aufzüge und Sicherheitsbauteile für Aufzüge** (Richtlinie 2014/33/EU): KI kann hier zB Steuerung oder Notfallfunktionen betreffen.
- **Geräte und Schutzsysteme für explosionsgefährdete Bereiche** (Richtlinie 2014/34/EU): KI-basierte Steuerungen können Sicherheitsrisiken in sensiblen Umgebungen beeinflussen.
- **Funkanlagen** (Richtlinie 2014/53/EU): Einschließlich smarter Kommunikationsgeräte mit sicherheitskritischen Funktionen.
- **Druckgeräte** (Richtlinie 2014/68/EU): KI-Anwendungen könnten Druckregelung oder Überwachungssysteme betreffen.
- **Seilbahnen** (Verordnung (EU) 2016/424): Relevanz bei automatisierten Steuerungs- und Notfallsystemen.
- **Persönliche Schutzausrüstungen** (Verordnung (EU) 2016/425): KI-basierte Funktionen wie intelligente Helme oder Sensorik.
- **Geräte zur Verbrennung** (Verordnung (EU) 2016/426): KI-gestützte Steuerungen zur Sicherheit in Haushalten oder Industrie.
- **Medizinprodukte** (Verordnung (EU) 2017/745): Umfasst KI-gestützte Diagnose- und Therapiesysteme.
- **In-vitro-Diagnostika** (Verordnung (EU) 2017/746): Relevanz für KI-gestützte Labortests und Diagnosesoftware.
- **Zivilluftfahrt-Sicherheit** (Verordnung (EG) Nr 300/2008): Sicherheitsrelevante Systeme im Bereich Flughäfen und Flugzeuge.

- **Zwei-, drei- und vierrädrige Fahrzeuge** (Verordnung (EU) Nr 168/2013): Automatisierte Steuerung und Assistenzsysteme in Motorrädern oder Quads.
- **Land- und forstwirtschaftliche Fahrzeuge** (Verordnung (EU) Nr 167/2013): KI-basierte Assistenzsysteme in Traktoren oder Mähdreschern.
- **Schiffsausrüstung** (Richtlinie 2014/90/EU): ZB automatische Navigations- oder Sicherheitssysteme.
- **Eisenbahnsysteme** (Richtlinie (EU) 2016/797): Einsatz von KI für Steuerung, Signalisierung oder Sicherheit.
- **Kraftfahrzeuge und Anhänger** (Verordnung (EU) 2018/858): KI in automatisierten Fahrsystemen.
- **Fahrzeugsicherheit und Insassenschutz** (Verordnung (EU) 2019/2144): KI-gestützte Sicherheitssysteme wie Notbremsassistenten.
- **Zivilluftfahrt** (Verordnung (EU) 2018/1139): KI-Anwendungen in Flugzeugen, Drohnen und deren Steuerung.

III. Zusammenfassung

Hochrisiko-Voraussetzung	Produkt fällt unter einen der in Anhang I genannten Rechtsakte und unterliegt einem externen Konformitätsbewertungsverfahren
Abschnitt A & B	Unterteilung in NLF-basierte Vorschriften (klassische Produktregeln) und sonstige Vorschriften (zB Luftfahrt, Fahrzeuge).
Ziel	Schutz von Gesundheit und Sicherheit durch klare Schnittstelle zwischen Produktrecht und KI-VO.

Anhang II KI-VO

Liste der Straftaten gemäß Artikel 5 KI-VO Absatz 1 Unterabsatz 1 Buchstabe h Ziffer iii

Straftaten gemäß Artikel 5 Absatz 1 Unterabsatz 1 Buchstabe h Ziffer iii:

- *Terrorismus,*
- *Menschenhandel,*
- *sexuelle Ausbeutung von Kindern und Kinderpornografie,*
- *illegaler Handel mit Drogen oder psychotropen Stoffen,*
- *illegaler Handel mit Waffen, Munition oder Sprengstoffen,*
- *Mord, schwere Körperverletzung,*
- *illegaler Handel mit menschlichen Organen oder menschlichem Gewebe,*
- *illegaler Handel mit nuklearen oder radioaktiven Substanzen,*
- *Entführung, Freiheitsberaubung oder Geiselnahme,*
- *Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen,*
- *Flugzeug- oder Schiffsentführung,*
- *Vergewaltigung,*
- *Umweltkriminalität,*
- *organisierter oder bewaffneter Raub,*
- *Sabotage,*
- *Beteiligung an einer kriminellen Vereinigung, die an einer oder mehreren der oben genannten Straftaten beteiligt ist.*

I. Worum geht es?

Anhang II enthält die Auflistung jener **Straftaten von besonderer Schwere**, bei denen der Einsatz von **biometrischen Echtzeit-**

Fernidentifizierungssystemen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken ausnahmsweise zulässig ist. Damit stellt der Anhang eine **Ausnahmebestimmung** zum in Artikel 5 KI-VOverankerten Verbot solcher Systeme dar: Nur im Zusammenhang mit den dort genannten Delikten darf die ansonsten verbotene Praxis angewandt werden. In allen anderen Fällen bleibt ihr Einsatz untersagt.

Relevante Artikel: Artikel 5 KI-VO Absatz 1 lit h Z iii

II. Detailkommentar

A. Inhaltliche Reichweite

- **Abschließende Aufzählung**: Die im Anhang II genannten Straftaten bilden eine feste Liste. Nur diese Straftaten sind erfasst, nicht vergleichbare oder verwandte Delikte.
- **Schwerkriminalität**: Es handelt sich überwiegend um besonders gravierende Delikte, die hohes Unrecht darstellen und internationale Dimensionen haben (zB Terrorismus, Menschenhandel).
- **EU-weite Angleichung nationaler Regelungen**: Durch die Liste wird ein gemeinsamer Standard geschaffen, der unabhängig von nationalen Strafrechtsunterschieden gilt.

Beispiel: *Ein KI-System, das vorhersagen soll, ob eine Person künftig einen einfachen Diebstahl begeht, fällt nicht unter Artikel 5 lit h Ziff iii, da Diebstahl nicht in der Liste des Anhangs II enthalten ist.*

B. Einteilung der Straftaten

1. Straftaten gegen die Allgemeinheit

- Terrorismus, Sabotage, Umweltkriminalität
- **Charakter**: Gefahren für öffentliche Sicherheit und Ordnung

2. Straftaten gegen die körperliche Unversehrtheit

- Mord, schwere Körperverletzung, Vergewaltigung

- **Charakter**: Schutz des Lebens und der physischen Integrität

3. Straftaten gegen die persönliche Freiheit

- Entführung, Freiheitsberaubung, Geiselnahme, Flugzeug- oder Schiffsentführung
- **Charakter**: Schutz individueller Selbstbestimmung

4. Straftaten im Bereich organisierter Kriminalität

- Menschenhandel, Drogenhandel, Waffenhandel, Organhandel, Kinderpornografie, organisierter oder bewaffneter Raub
- **Charakter**: Transnationale Strukturen, wirtschaftliche Dimension, hohe Professionalität

5. Internationale Verbrechen

- Straftaten im Zuständigkeitsbereich des Internationalen Strafgerichtshofs
- **Charakter**: Schwere Verletzungen internationalen Rechts

C. Besonderheiten

- **Straftaten mit internationalem Bezug**: Viele genannte Delikte stehen in engem Zusammenhang mit internationalem Strafrecht (zB Rom-Statut des IStGH). Dadurch wird deutlich, dass die KI-VO über rein nationale Delikte hinausblickt.
- **Abgrenzung zu minderschweren Straftaten**: Straftaten wie Betrug oder einfacher Diebstahl sind bewusst nicht aufgenommen, um eine Überdehnung der Regelung zu vermeiden.

III. Zusammenfassung

Charakter der Delikte	Schwerste Kriminalität mit hoher Gefährdungslage
Typische Bereiche	Terrorismus, organisierte/transnationale Kriminalität, Völkerrechtsverbrechen
Schutzzweck	Öffentliche Sicherheit, Leben und Gesundheit, persönliche Freiheit
Besonderheit	Abschließende Liste – keine Ausdehnung auf minderschwere Straftaten

Anhang III KI-VO

Hochrisiko-KI-Systeme gemäß Artikel 6 KI-VO Absatz 2

Als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 gelten die in folgenden Bereichen aufgeführten KI-Systeme:

1. Biometrie, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

a) biometrische Fernidentifizierungssysteme.

Dazu gehören nicht KI-Systeme, die bestimmungsgemäß für die biometrische Verifizierung, deren einziger Zweck darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt, verwendet werden sollen;

b) KI-Systeme, die bestimmungsgemäß für die biometrische Kategorisierung nach sensiblen oder geschützten Attributen oder Merkmalen auf der Grundlage von Rückschlüssen auf diese Attribute oder Merkmale verwendet werden sollen;

c) KI-Systeme, die bestimmungsgemäß zur Emotionserkennung verwendet werden sollen.

2. Kritische Infrastruktur: KI-Systeme, die bestimmungsgemäß als Sicherheitsbauteile im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur, des Straßenverkehrs oder der Wasser-, Gas-, Wärme- oder Stromversorgung verwendet werden sollen

3. Allgemeine und berufliche Bildung

a) KI-Systeme, die bestimmungsgemäß zur Feststellung des Zugangs oder der Zulassung oder zur Zuweisung natürlicher Personen zu Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung verwendet werden sollen;

b) KI-Systeme, die bestimmungsgemäß für die Bewertung von Lernergebnissen verwendet werden sollen, einschließlich des Falles, dass diese Ergebnisse dazu dienen, den Lernprozess natürlicher Personen in Einrichtungen oder Programmen aller Ebenen der allgemeinen und beruflichen Bildung zu steuern;

c) KI-Systeme, die bestimmungsgemäß zum Zweck der Bewertung des angemessenen Bildungsniveaus, das eine Person im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und

beruflichen Bildung erhalten wird oder zu denen sie Zugang erhalten wird, verwendet werden sollen;

d)KI-Systeme, die bestimmungsgemäß zur Überwachung und Erkennung von verbotenem Verhalten von Schülern bei Prüfungen im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung verwendet werden sollen.

4.Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit

a)KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere um gezielte Stellenanzeigen zu schalten, Bewerbungen zu sichten oder zu filtern und Bewerber zu bewerten;

b)KI-Systeme, die bestimmungsgemäß für Entscheidungen, die die Bedingungen von Arbeitsverhältnissen, Beförderungen und Kündigungen von Arbeitsvertragsverhältnissen beeinflussen, für die Zuweisung von Aufgaben aufgrund des individuellen Verhaltens oder persönlicher Merkmale oder Eigenschaften oder für die Beobachtung und Bewertung der Leistung und des Verhaltens von Personen in solchen Beschäftigungsverhältnissen verwendet werden soll.

5.Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen:

a)KI-Systeme, die bestimmungsgemäß von Behörden oder im Namen von Behörden verwendet werden sollen, um zu beurteilen, ob natürliche Personen Anspruch auf grundlegende öffentliche Unterstützungsleistungen und -dienste, einschließlich Gesundheitsdiensten, haben und ob solche Leistungen und Dienste zu gewähren, einzuschränken, zu widerrufen oder zurückzufordern sind;

b)KI-Systeme, die bestimmungsgemäß für die Kreditwürdigkeitsprüfung und Bonitätsbewertung natürlicher Personen verwendet werden sollen, mit Ausnahme von KI-Systemen, die zur Aufdeckung von Finanzbetrug verwendet werden;

c)KI-Systeme, die bestimmungsgemäß für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Fall von Lebens- und Krankenversicherungen verwendet werden sollen;

d)KI-Systeme, die bestimmungsgemäß zur Bewertung und Klassifizierung von Notrufen von natürlichen Personen oder für die Entsendung oder

Priorisierung des Einsatzes von Not- und Rettungsdiensten, einschließlich Polizei, Feuerwehr und medizinischer Nothilfe, sowie für Systeme für die Triage von Patienten bei der Notfallversorgung verwendet werden sollen.

6. Strafverfolgung, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

a) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden oder in deren Namen zur Bewertung des Risikos einer natürlichen Person, zum Opfer von Straftaten zu werden, verwendet werden sollen;

b) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden als Lügendetektoren oder ähnliche Instrumente verwendet werden sollen;

c) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur Bewertung der Verlässlichkeit von Beweismitteln im Zuge der Ermittlung oder Verfolgung von Straftaten verwendet werden sollen;

d) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur Bewertung des Risikos, dass eine natürliche Person eine Straftat begeht oder erneut begeht, nicht nur auf der Grundlage der Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 oder zur Bewertung persönlicher Merkmale und Eigenschaften oder vergangenen kriminellen Verhaltens von natürlichen Personen oder Gruppen verwendet werden sollen;

e) KI-Systeme, die bestimmungsgemäß von Strafverfolgungsbehörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Unterstützung von Strafverfolgungsbehörden zur Erstellung von Profilen natürlicher Personen gemäß Artikel 3 Absatz 4 der Richtlinie (EU) 2016/680 im Zuge der Aufdeckung, Ermittlung oder Verfolgung von Straftaten verwendet werden sollen.

7.Migration, Asyl und Grenzkontrolle, soweit ihr Einsatz nach einschlägigem Unionsrecht oder nationalem Recht zugelassen ist:

a)KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder Organen, Einrichtungen und sonstigen Stellen der Union als Lügendetektoren verwendet werden sollen oder ähnliche Instrumente;

b)KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union zur Bewertung eines Risikos verwendet werden sollen, einschließlich eines Sicherheitsrisikos, eines Risikos der irregulären Einwanderung oder eines Gesundheitsrisikos, das von einer natürlichen Person ausgeht, die in das Hoheitsgebiet eines Mitgliedstaats einzureisen beabsichtigt oder eingereist ist;

c)KI-Systeme, die bestimmungsgemäß von zuständigen Behörden oder in deren Namen oder von Organen, Einrichtungen und sonstigen Stellen der Union verwendet werden sollen, um zuständige Behörden bei der Prüfung von Asyl- und Visumanträgen sowie Aufenthaltstiteln und damit verbundenen Beschwerden im Hinblick auf die Feststellung der Berechtigung der den Antrag stellenden natürlichen Personen, einschließlich damit zusammenhängender Bewertungen der Verlässlichkeit von Beweismitteln, zu unterstützen;

d)KI-Systeme, die bestimmungsgemäß von oder im Namen der zuständigen Behörden oder Organen, Einrichtungen und sonstigen Stellen der Union, im Zusammenhang mit Migration, Asyl oder Grenzkontrolle zum Zwecke der Aufdeckung, Anerkennung oder Identifizierung natürlicher Personen verwendet werden sollen, mit Ausnahme der Überprüfung von Reisedokumenten.

8.Rechtspflege und demokratische Prozesse

a)KI-Systeme, die bestimmungsgemäß von einer oder im Namen einer Justizbehörde verwendet werden sollen, um eine Justizbehörde bei der Ermittlung und Auslegung von Sachverhalten und Rechtsvorschriften und bei der Anwendung des Rechts auf konkrete Sachverhalte zu unterstützen, oder die auf ähnliche Weise für die alternative Streitbeilegung genutzt werden sollen;

b)KI-Systeme, die bestimmungsgemäß verwendet werden sollen, um das Ergebnis einer Wahl oder eines Referendums oder das Wahlverhalten

natürlicher Personen bei der Ausübung ihres Wahlrechts bei einer Wahl oder einem Referendum zu beeinflussen. Dazu gehören nicht KI-Systeme, deren Ausgaben natürliche Personen nicht direkt ausgesetzt sind, wie Instrumente zur Organisation, Optimierung oder Strukturierung politischer Kampagnen in administrativer oder logistischer Hinsicht.

I. Worum geht es?

Anhang III enthält die Auflistung jener KI-Systeme, die nach Artikel 6 KI-VO Absatz 2 automatisch als **Hochrisiko-KI-Systeme** gelten. Der Anhang legt konkrete Anwendungsbereiche fest, in denen KI aufgrund ihres erheblichen Einflusses etwa auf Grundrechte, Sicherheit und Vertrauen als besonders risikoreich eingestuft wird

Relevante Artikel: Artikel 6 KI-VO (Einstufungsvorschriften für Hochrisiko-KI-Systeme), Artikel 7 KI-VO (Änderungen des Anhangs III)), Artikel 43 KI-VO ff (Konformitätsbewertung, Bescheinigungen und Registrierung) sowie alle diesbezüglich impliziten Hochrisikovorschriften

II. Detailkommentar

A. Biometrie

- **Biometrische Fernidentifizierung**: Systeme zur Identifikation auf Distanz, zB Gesichtserkennung im öffentlichen Raum.
- **Kategorisierung nach sensiblen Merkmalen**: KI, die Personen etwa nach Hautfarbe, Religion oder sexueller Orientierung einteilt. Besonders risikobehaftet, da Diskriminierung droht.
- **Emotionserkennung**: Systeme, die Gefühle anhand von Gesichtsausdruck, Stimme oder Körpersprache bewerten. Risiko von Fehlinterpretationen und massiver Grundrechtseingriffe.

Beispiel: *Eine Stadt setzt KI-gestützte Kameras ein, die nicht nur Personen identifizieren, sondern auch deren Stimmung („aggressiv“/„ruhig“) einschätzen sollen.*

B. Kritische Infrastruktur

- **Digitale Infrastruktur**: zB Systeme zur Steuerung von Servernetzen oder Cloud-Sicherheit.
- **Verkehrssysteme**: Einsatz im Straßenverkehr, zB bei autonomen Fahrzeugen.
- **Energie- und Wasserversorgung**: KI zur Überwachung oder Steuerung von Netzen.

Beispiel: *Ein KI-System reguliert die Stromzufuhr in einem Versorgungsnetz und entscheidet automatisch über Lastverteilung.*

C. Bildung

- **Zugang und Zulassung**: KI zur Steuerung von Aufnahmeprüfungen oder Bewerbungen.
- **Bewertung von Lernergebnissen**: zB automatische Korrektur von Prüfungen.
- **Bestimmung des Bildungsniveaus**: KI, die entscheidet, ob Schüler auf eine bestimmte Schule wechseln dürfen.
- **Überwachung bei Prüfungen**: Systeme, die Betrugsversuche erkennen sollen.

Beispiel: *Eine Universität nutzt KI, um Online-Prüfungen zu überwachen und auffälliges Verhalten automatisch zu melden.*

D. Beschäftigung & Arbeitswelt

- **Einstellung und Auswahl**: Algorithmen zur Vorauswahl von Bewerbern.
- **Arbeitsbedingungen und Kündigungen**: KI, die Entscheidungen über Beförderung oder Entlassung vorbereitet.
- **Überwachung von Mitarbeitern**: zB Systeme zur Leistungsbewertung oder Verhaltensanalyse.

Beispiel: *Ein Unternehmen nutzt KI, um Bewerbungen automatisch zu filtern und Kandidaten mit geringer Eignung auszuschließen.*

E. Grundlegende Dienste

- **Öffentliche Leistungen**: KI zur Entscheidung über Anspruch auf Sozialhilfe oder Gesundheitsleistungen.
- **Kreditwürdigkeit**: Systeme, die Kreditrisiken von Personen bewerten.
- **Versicherungen**: KI zur Risikobewertung und Preisbildung in der Lebens- und Krankenversicherung.
- **Not- und Rettungsdienste**: Systeme zur Klassifizierung von Notrufen und Zuteilung von Einsatzkräften.

Beispiel: *Ein Krankenhaus verwendet KI, um bei Massenunfällen Patienten automatisch nach Dringlichkeit einzustufen (Triage).*

F. Strafverfolgung

- **Opferrisiko-Bewertung**: Einschätzung, ob Personen besonders gefährdet sind.
- **Lügendetektoren**: KI, die Wahrheit oder Lüge anhand von Sprache, Mimik oder Gestik beurteilen soll.
- **Beweisbewertung**: Einschätzung von Verlässlichkeit von Beweisen.
- **Rückfallprognosen**: Bewertung der Wahrscheinlichkeit erneuter Straftaten.
- **Profilbildung**: Erstellung von Profilen natürlicher Personen zur Aufklärung von Straftaten.

Beispiel: *Die Polizei nutzt KI, um anhand von Daten über frühere Delikte Rückfallrisiken einzelner Personen einzuschätzen.*

G. Migration, Asyl und Grenzkontrolle

- **Lügendetektoren an Grenzen**: zB Systeme zur Befragung von Asylsuchenden.
- **Risikobewertung**: Einschätzung von Gefahren wie Terrorismus oder Krankheit.
- **Unterstützung bei Asylverfahren**: KI zur Bewertung der Glaubwürdigkeit von Dokumenten oder Aussagen.
- **Identifizierung**: Systeme zur Gesichtserkennung oder Abgleich biometrischer Daten.

Beispiel: *Eine Grenzbehörde setzt KI ein, um bei Visumanträgen automatisch die Plausibilität von Angaben zu prüfen.*

H. Justiz und Demokratie

- **Justizunterstützung**: Systeme, die Richter bei Entscheidungen unterstützen.
- **Wahlen und Referenden**: KI zur Beeinflussung von Wahlentscheidungen. Ausgenommen sind nur administrative Hilfen.

Beispiel: *Eine Plattform setzt KI-gestützte Tools ein, die personalisierte politische Werbung so zuschneiden, dass sie direkt das Wahlverhalten beeinflussen.*

III. Zusammenfassung

Bereich	Beispiele	Zentrale Risiken
Biometrie	Gesichtserkennung, Emotionserkennung	Grundrechte, Diskriminierung
Kritische Infrastruktur	Energie, Verkehr	Sicherheit, Versorgungsausfälle
Bildung	Prüfungsaufsicht, Aufnahmeverfahren	Fairness, Chancengleichheit
Beschäftigung	Bewerberauswahl, Mitarbeiterüberwachung	Diskriminierung, Arbeitsplatzverlust

Grundlegende Dienste	Sozialleistungen, Kredite, Versicherungen	Soziale Teilhabe, wirtschaftliche Benachteiligung
Strafverfolgung	Lügendetektoren, Rückfallprognosen	Freiheit, Datenschutz
Migration & Asyl	Risikobewertung, Identitätsprüfung	Menschenrechte, Diskriminierung
Justiz & Demokratie	Richterassistenz, Wahlbeeinflussung	Rechtsstaat, Demokratie

Anhang IV KI-VO

Technische Dokumentation gemäß Artikel 11 KI-VO Absatz 1

Die in Artikel 11 Absatz 1 genannte technische Dokumentation muss mindestens die folgenden Informationen enthalten, soweit sie für das betreffende KI-System von Belang sind:

1.Allgemeine Beschreibung des KI-Systems, darunter

a)Zweckbestimmung, Name des Anbieters und Version des Systems mit Angaben dazu, in welcher Beziehung sie zu vorherigen Versionen steht;

b)gegebenenfalls Interaktion oder Verwendung des KI-Systems mit Hardware oder Software, einschließlich anderer KI-Systeme, die nicht Teil des KI-Systems selbst sind;

c)Versionen der betreffenden Software oder Firmware und etwaige Anforderungen in Bezug auf Aktualisierungen der Versionen;

d)Beschreibung aller Formen, in denen das KI-System in Verkehr gebracht oder in Betrieb genommen wird, zum Beispiel in Hardware eingebettete Softwarepakete, Herunterladen oder API;

e)Beschreibung der Hardware, auf der das KI-System betrieben werden soll;

f)falls das KI-System Bestandteil von Produkten ist: Fotografien oder Abbildungen, die äußere Merkmale, die Kennzeichnungen und den inneren Aufbau dieser Produkte zeigen;

g)eine grundlegende Beschreibung der Benutzerschnittstelle, die dem Betreiber zur Verfügung gestellt wird;

h)Betriebsanleitungen für den Betreiber und gegebenenfalls eine grundlegende Beschreibung der dem Betreiber zur Verfügung gestellten Benutzerschnittstelle;

2.Detaillierte Beschreibung der Bestandteile des KI-Systems und seines Entwicklungsprozesses, darunter

a)Methoden und Schritte zur Entwicklung des KI-Systems, gegebenenfalls einschließlich des Einsatzes von durch Dritte bereitgestellten

vortrainierten Systemen oder Instrumenten, und wie diese vom Anbieter verwendet, integriert oder verändert wurden;

b) Entwurfsspezifikationen des Systems, insbesondere die allgemeine Logik des KI-Systems und der Algorithmen; die wichtigsten Entwurfsentscheidungen mit den Gründen und getroffenen Annahmen, einschließlich in Bezug auf Personen oder Personengruppen, bezüglich deren das System angewandt werden soll; hauptsächliche Einstufungsentscheidungen; was das System optimieren soll und welche Bedeutung den verschiedenen Parametern dabei zukommt; Beschreibung der erwarteten Ausgabe des Systems und der erwarteten Qualität dieser Ausgabe; die über mögliche Kompromisse in Bezug auf die technischen Lösungen, mit denen die in Kapitel III Abschnitt 2 festgelegten Anforderungen erfüllt werden sollen, getroffenen Entscheidungen;

c) Beschreibung der Systemarchitektur, aus der hervorgeht, wie Softwarekomponenten aufeinander aufbauen oder einander zuarbeiten und in die Gesamtverarbeitung integriert sind; zum Entwickeln, Trainieren, Testen und Validieren des KI-Systems verwendete Rechenressourcen;

d) gegebenenfalls Datenanforderungen in Form von Datenblättern, in denen die Trainingsmethoden und -techniken und die verwendeten Trainingsdatensätze beschrieben werden, einschließlich einer allgemeinen Beschreibung dieser Datensätze sowie Informationen zu deren Herkunft, Umfang und Hauptmerkmalen; Angaben zur Beschaffung und Auswahl der Daten; Kennzeichnungsverfahren (zum Beispiel für überwachtes Lernen) und Datenbereinigungsmethoden (zum Beispiel Erkennung von Ausreißern);

e) Bewertung der nach Artikel 14 erforderlichen Maßnahmen der menschlichen Aufsicht, mit einer Bewertung der technischen Maßnahmen, die erforderlich sind, um den Betreibern gemäß Artikel 13 Absatz 3 Buchstabe d die Interpretation der Ausgaben von KI-Systemen zu erleichtern;

f) gegebenenfalls detaillierte Beschreibung der vorab bestimmten Änderungen an dem KI-System und seiner Leistung mit allen einschlägigen Informationen zu den technischen Lösungen, mit denen

sichergestellt wird, dass das KI-System die einschlägigen in Kapitel III Abschnitt 2 festgelegten Anforderungen weiterhin dauerhaft erfüllt;

g) verwendete Validierungs- und Testverfahren, mit Informationen zu den verwendeten Validierungs- und Testdaten und deren Hauptmerkmalen; Parameter, die zur Messung der Genauigkeit, Robustheit und der Erfüllung anderer einschlägiger Anforderungen nach Kapitel III Abschnitt 2 sowie potenziell diskriminierender Auswirkungen verwendet werden; Testprotokolle und alle von den verantwortlichen Personen datierten und unterzeichneten Testberichte, auch in Bezug auf die unter Buchstabe f genannten vorab bestimmten Änderungen;

h) ergriffene Cybersicherheitsmaßnahmen;

3. Detaillierte Informationen über die Überwachung, Funktionsweise und Kontrolle des KI-Systems, insbesondere in Bezug auf Folgendes: die Fähigkeiten und Leistungsgrenzen des Systems, einschließlich der Genauigkeitsgrade bei bestimmten Personen oder Personengruppen, auf die es bestimmungsgemäß angewandt werden soll, sowie des in Bezug auf seine Zweckbestimmung insgesamt erwarteten Maßes an Genauigkeit; angesichts der Zweckbestimmung des KI-Systems vorhersehbare unbeabsichtigte Ergebnisse und Quellen von Risiken in Bezug auf Gesundheit und Sicherheit sowie Grundrechte und Diskriminierung; die nach Artikel 14 erforderlichen Maßnahmen der menschlichen Aufsicht, einschließlich der technischen Maßnahmen, die getroffen wurden, um den Betreibern die Interpretation der Ausgaben von KI-Systemen zu erleichtern; gegebenenfalls Spezifikationen zu Eingabedaten;

4. Darlegungen zur Eignung der Leistungskennzahlen für das spezifische KI-System;

5. Detaillierte Beschreibung des Risikomanagementsystems gemäß Artikel 9;

6. Beschreibung einschlägiger Änderungen, die der Anbieter während des Lebenszyklus an dem System vorgenommen hat;

7. Aufstellung der vollständig oder teilweise angewandten harmonisierten Normen, deren Fundstellen im Amtsblatt der Europäischen Union veröffentlicht wurden; falls keine solchen harmonisierten Normen angewandt wurden, eine detaillierte Beschreibung der Lösungen, mit denen die in Kapitel III Abschnitt 2 festgelegten Anforderungen erfüllt

werden sollen, mit einer Aufstellung anderer angewandter einschlägiger Normen und technischer Spezifikationen;

8. Kopie der EU-Konformitätserklärung gemäß Artikel 47;

9. Detaillierte Beschreibung des Systems zur Bewertung der Leistung des KI-Systems in der Phase nach dem Inverkehrbringen gemäß Artikel 72, einschließlich des in Artikel 72 Absatz 3 genannten Plans für die Beobachtung nach dem Inverkehrbringen

I. Worum geht es?

Die Funktion von Anhang IV liegt darin, präzise Vorgaben für die **technische Dokumentation** von Hochrisiko-KI-Systemen festzulegen. Diese Dokumentation ist nach Artikel 11 KI-VOAbsatz 1 zwingend erforderlich und dient als Nachweis, dass das KI-System die in Kapitel III Abschnitt 2 vorgesehenen Anforderungen einhält. Sie bildet die Grundlage für die Konformitätsbewertung (Artikel 43 KI-VO) und für die Beobachtung nach dem Inverkehrbringen (Artikel 72 KI-VO).

Relevanter Artikel: Artikel 11 KI-VO

II. Detailkommentar

A. Allgemeine Beschreibung des KI-Systems

- **Zweckbestimmung und Versionen**: Das System muss mit seiner vorgesehenen Nutzung, dem Anbieter und den Versionsangaben dokumentiert werden. So wird nachvollziehbar, wofür es entwickelt wurde und welche Änderungen gegenüber Vorgängerversionen bestehen.
- **Interaktion mit anderer Software/Hardware**: Es ist wichtig, Abhängigkeiten oder Schnittstellen zu anderen Systemen offenzulegen, zB wenn ein KI-Modul auf einer externen Plattform läuft.

- **Benutzerschnittstelle**: Eine grundlegende Beschreibung der Nutzeroberfläche stellt sicher, dass Bediener wissen, wie sie mit dem System interagieren können.

Beispiel: *Ein Sprachmodell, das in eine Kanzleisoftware eingebunden ist, muss nicht nur seine Funktion (Textgenerierung für Schriftsätze) dokumentieren, sondern auch die Interaktion mit Textverarbeitungsprogrammen.*

B. Beschreibung des Entwicklungsprozesses

- **Methoden und Schritte**: Offenlegung des Entwicklungswegs, inkl Nutzung von vortrainierten Modellen.
- **Entwurfsspezifikationen**: Beschreibung der Logik, Algorithmen, Zielgrößen und getroffenen Annahmen.
- **Systemarchitektur**: Darstellung der Software-Module und Rechenressourcen.
- **Datenanforderungen**: Herkunft, Umfang, Merkmale und Aufbereitung der Trainingsdaten.
- **Menschliche Aufsicht**: Darstellung der technischen Lösungen, die menschliche Kontrolle ermöglichen.
- **Vorab bestimmte Änderungen**: Angabe, welche Systemänderungen vorgesehen sind und wie die Anforderungen auch dann erfüllt bleiben.
- **Validierung und Tests**: Darstellung der Testmethoden, Testdaten und Ergebnisse.
- **Cybersicherheit**: Beschreibung getroffener Schutzmaßnahmen.

Beispiel: *Ein KI-System zur Betrugserkennung im Finanzsektor muss dokumentieren, welche Datenquellen (zB Transaktionsdaten) verwendet wurden, wie diese bereinigt wurden, welche Logik der Anomalieerkennung zugrunde liegt und mit welchen Testverfahren die Genauigkeit der Vorhersagen überprüft wurde.*

C. Überwachung, Funktionsweise und Kontrolle

- **Leistungsgrenzen**: Anbieter müssen Genauigkeit und Grenzen des Systems angeben.
- **Vorhersehbare Risiken**: Dokumentation möglicher unbeabsichtigter Effekte, zB diskriminierende Ergebnisse.
- **Menschliche Aufsicht**: Dokumentation der Maßnahmen zur Menschlichen Aufsicht nach Artikel 14 KI-VO. Es wird insbesondere eine Bewertung der technischen Maßnahmen verlangt, die erforderlich sind, um den Betreibern die Interpretation der Ausgaben des Systems zu erleichtern.

Beispiel: *Ein KI-System, das Bewerbungen vorsortiert, muss angeben, welche Vorkehrungen zur menschlichen Aufsicht getroffen wurden. Dazu gehört IV insbesondere, dass die Ausgaben so aufbereitet werden, dass Personalverantwortliche sie interpretieren können.*

D. Risikomanagement und Leistungsbewertung

- **Risikomanagementsystem**: Darstellung gemäß Artikel 9 KI-VO.
- **Leistungskennzahlen**: Nachweis, dass die Messgrößen geeignet sind, die Systemqualität zu prüfen.
- **Änderungen im Lebenszyklus**: Dokumentation aller späteren Anpassungen.
- **Harmonisierte Normen**: Auflistung der angewandten Normen oder alternativen Lösungen.
- **Konformitätserklärung**: Beifügung der EU-Konformitätserklärung.
- **Überwachung nach dem Inverkehrbringen**: Plan und Verfahren zur laufenden Kontrolle.

Beispiel: *Ein Medizin-KI-System zur Bildauswertung muss laufend überprüft werden, ob neue Datenquellen die bisherige Genauigkeit verändern.*

III. Zusammenfassung

Bereich	Kernpunkt	Ziel
Allgemeine Beschreibung	Zweck, Version, Schnittstellen	Nachvollziehbarkeit
Entwicklungsprozess	Methoden, Architektur, Daten, Tests	Qualitätssicherung
Funktionsweise/Kontrolle	Grenzen, Risiken, menschliche Aufsicht	Sicherheit und Grundrechtsschutz
Risikomanagement	Systematische Risikoanalyse	Minimierung von Gefahren
Normen & Konformität	Bezug auf Standards und EU-Erklärung	Einheitliche Umsetzung
Überwachung	Post-Market-Plan	Laufende Kontrolle

Anhang V KI-VO

EU-Konformitätserklärung

Die EU-Konformitätserklärung gemäß Artikel 47 enthält alle folgenden Angaben:

1. *Name und Artikel des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen;*
2. *Name und Anschrift des Anbieters und gegebenenfalls seines Bevollmächtigten;*
3. *Erklärung darüber, dass der Anbieter die alleinige Verantwortung für die Ausstellung der EU-Konformitätserklärung gemäß Artikel 47 trägt;*
4. *Versicherung, dass das betreffende KI-System der vorliegenden Verordnung sowie gegebenenfalls weiteren einschlägigen Rechtsvorschriften der Union, in denen die Ausstellung der EU-Konformitätserklärung gemäß Artikel 47 vorgesehen ist, entspricht;*
5. *wenn ein KI-System die Verarbeitung personenbezogener Daten erfordert, eine Erklärung darüber, dass das KI-System den Verordnungen (EU) 2016/679 und (EU) 2018/1725 sowie der Richtlinie (EU) 2016/680 entspricht;*
6. *Verweise auf die verwendeten einschlägigen harmonisierten Normen oder sonstigen gemeinsamen Spezifikationen, für die die Konformität erklärt wird;*
7. *gegebenenfalls Name und Identifizierungsnummer der notifizierten Stelle, Beschreibung des durchgeführten Konformitätsbewertungsverfahrens und Identifizierungsnummer der ausgestellten Bescheinigung;*
8. *Ort und Datum der Ausstellung der Erklärung, den Namen und die Funktion des Unterzeichners sowie Angabe, für wen oder in wessen Namen diese Person unterzeichnet hat, eine Unterschrift.*

I. Worum geht es?

Anhang V legt fest, welche Inhalte zwingend in einer EU-Konformitätserklärung für KI-Systeme enthalten sein müssen. Die

Konformitätserklärung ist ein offizielles Dokument, mit dem der Anbieter bestätigt, dass sein KI-System die Anforderungen der KI-VO erfüllt.

Relevante Artikel: Artikel 47 KI-VO (EU-Konformitätserklärung), Artikel 43 KI-VO ff (Konformitätsbewertung, Bescheinigungen und Registrierung).

II. Detailkommentar

A. Identifizierung des KI-Systems

- **Name und Artikel**: Das KI-System muss klar bezeichnet werden. Auch die Artikel des Systems (zB Chatbot, Gesichtserkennungssystem) ist anzugeben.
- **Zusätzliche Angaben**: Seriennummern, Softwareversionen oder andere eindeutige Merkmale die die Rückverfolgbarkeit ermöglichen.

B. Angaben zum Anbieter

- **Name und Anschrift**: Der Anbieter (Hersteller) muss vollständig identifizierbar sein.
- **Bevollmächtigter**: Falls ein Vertreter innerhalb der EU tätig ist, sind dessen Angaben ebenfalls erforderlich.

C. Verantwortungserklärung

- **Alleinige Verantwortung**: Der Anbieter erklärt ausdrücklich, dass er für die Richtigkeit der Angaben verantwortlich ist. Dies schließt eine Haftung bei falschen oder fehlenden Informationen ein.

D. Einhaltung der Vorschriften

- **Verordnungskonformität**: Es ist zu bestätigen, dass das KI-System die Vorgaben der KI-VO erfüllt.

- **Weitere Rechtsakte**: Falls andere EU-Rechtsvorschriften gelten (zB Produktsicherheitsrichtlinien), müssen diese ebenfalls berücksichtigt werden.

E. Datenschutz

- **Pflicht zur Erklärung**: Wenn personenbezogene Daten verarbeitet werden, muss die Einhaltung der Datenschutzgrundverordnung (DSGVO (EU 2016/679)), der Verordnung 2018/1725 und der Richtlinie 2016/680 bestätigt werden.

F. Technische Standards

- **Verweis auf Normen**: Der Anbieter muss angeben, auf welche harmonisierten Normen oder gemeinsamen Spezifikationen er sich bei der Konformität stützt.

G. Rolle notifizierter Stellen

- **Beteiligung**: Wenn eine externe Prüfstelle beteiligt war, müssen deren Name und Identifikationsnummer angegeben werden.
- **Bescheinigung**: Auch die Artikel des Konformitätsbewertungsverfahrens und die Bescheinigungsnummer sind aufzuführen.

H. Formale Angaben

- **Ort und Datum**: Diese zeigen, wann und wo die Erklärung erstellt wurde.
- **Unterzeichner**: Name, Funktion und Unterschrift sind zwingend, damit die Erklärung rechtsverbindlich ist.

III. Zusammenfassung

Pflichtangabe	Inhalt
KI-System	Name, Artikel, Identifizierungsmerkmale

Anbieter	Name, Anschrift, Bevollmächtigter
Verantwortung	Erklärung der alleinigen Verantwortung
Vorschriften	Einhaltung KI-VO und anderer Rechtsakte
Datenschutz	Erklärung zur DSGVO- und Datenschutzkonformität
Normen	Verweis auf harmonisierte Standards
Notifizierte Stelle	Angaben bei externer Prüfung
Formalien	Ort, Datum, Name, Funktion, Unterschrift

Anhang VI KI-VO

Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle

1. Das Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle ist das Konformitätsbewertungsverfahren gemäß den Nummern 2, 3 und 4.

2. Der Anbieter überprüft, ob das bestehende Qualitätsmanagementsystem den Anforderungen des Artikels 17 entspricht.

3. Der Anbieter prüft die in der technischen Dokumentation enthaltenen Informationen, um zu beurteilen. ob das KI-System den einschlägigen grundlegenden Anforderungen in Kapitel III Abschnitt 2 entspricht.

4. Der Anbieter überprüft ferner, ob der Entwurfs- und Entwicklungsprozess des KI-Systems und seine Beobachtung nach dem Inverkehrbringen gemäß Artikel 72 mit der technischen Dokumentation im Einklang stehen.

I. Worum geht es?

Anhang VI beschreibt ein vereinfachtes Verfahren, mit dem ein Anbieter selbst prüfen kann, ob sein KI-System den Anforderungen der KI-VO entspricht. Dieses Verfahren wird „interne Kontrolle“ genannt, da keine externe Stelle (zB eine benannte Stelle) beteiligt ist. Das Verfahren ist insbesondere für Anbieter relevant, die nachweisen wollen, dass ihre Systeme die gesetzlichen Mindeststandards erfüllen, ohne dafür externe Prüfungen in Anspruch nehmen zu müssen.

Relevante Artikel: Artikel 17 KI-VO (QMS), Artikel 72 KI-VO (Beobachtung nach Inverkehrbringen), sowie die grundlegenden Anforderungen in Kapitel III Abschnitt 2.

II. Detailkommentar

A. Grundstruktur

- **Selbstprüfung**: Der Anbieter führt alle Prüfungen eigenständig durch. Dies bedeutet Eigenverantwortung und weniger externe Kontrolle.

- **Drei Kernbereiche**: QMS, technische Dokumentation und Entwicklungs- sowie Beobachtungsprozesse müssen überprüft werden.

B. QMS

- **Anforderung nach Artikel 17 KI-VO**: Der Anbieter muss ein QMS haben, das die Entwicklung, Prüfung und Überwachung des KI-Systems regelt.
- **Prüfpflicht**: Der Anbieter kontrolliert, ob sein System diese Anforderungen tatsächlich erfüllt.

Beispiel: *Ein Unternehmen, das ein Sprachassistenzsystem entwickelt, muss sicherstellen, dass sein internes Managementsystem klare Prozesse zur Datenqualität, Risikobewertung und Fehlerbehebung vorsieht.*

C. Technische Dokumentation

- **Inhalt**: Alle Informationen, die das KI-System betreffen, müssen dokumentiert sein.
- **Prüfung**: Der Anbieter gleicht die Dokumentation mit den grundlegenden Anforderungen der KI-VO ab (zB Sicherheit, Transparenz, Datenqualität).

Beispiel: *Ein Anbieter von KI-Software für Bewerbungsverfahren prüft, ob seine Unterlagen nachweisen, dass das System diskriminierungsfrei arbeitet*.

D. Entwicklungs- und Beobachtungsprozesse

- **Kohärenzprüfung**: Der Anbieter stellt sicher, dass der tatsächliche Entwicklungsprozess und die Überwachung nach Markteinführung mit der Dokumentation übereinstimmen.
- **Bezug zu Artikel 72 KI-VO**: Anbieter müssen Systeme auch nach dem Inverkehrbringen beobachten, um Probleme oder Risiken frühzeitig zu erkennen.

Beispiel: *Ein KI-System zur medizinischen Bildanalyse wird nach seiner Einführung regelmäßig überprüft. Stellt der Anbieter Abweichungen von den dokumentierten Qualitätsstandards fest, muss er diese korrigieren.*

III. Zusammenfassung

Prüffeld	Inhalt	Ziel
Qualitätsmanagement (Nr 2)	Prüfung nach Artikel 17 KI-VO	Sicherstellung funktionierender interner Abläufe
Technische Dokumentation (Nr 3)	Abgleich mit grundlegenden Anforderungen	Nachweis der Rechtskonformität
Entwicklungs- & Beobachtungsprozesse (Nr 4)	Übereinstimmung mit Dokumentation und Artikel 72 KI-VO	Laufende Sicherheit und Anpassung

Anhang VII KI-VO

Konformität auf der Grundlage einer Bewertung des Qualitätsmanagementsystems und einer Bewertung der technischen Dokumentation

1. Einleitung

Die Konformität auf der Grundlage einer Bewertung des Qualitätsmanagementsystems und einer Bewertung der technischen Dokumentation entspricht dem Konformitätsbewertungsverfahren gemäß den Nummern 2 bis 5.

2. Überblick

Das genehmigte Qualitätsmanagementsystem für die Konzeption, die Entwicklung und das Testen von KI-Systemen nach Artikel 17 wird gemäß Nummer 3 geprüft und unterliegt der Überwachung gemäß Nummer 5. Die technische Dokumentation des KI-Systems wird gemäß Nummer 4 geprüft.

3. Qualitätsmanagementsystem

3.1. Der Antrag des Anbieters muss Folgendes enthalten:

a) Name und Anschrift des Anbieters sowie, wenn der Antrag von einem Bevollmächtigten eingereicht wird, auch dessen Namen und Anschrift;

b) die Liste der unter dasselbe Qualitätsmanagementsystem fallenden KI-Systeme;

c) die technische Dokumentation für jedes unter dasselbe Qualitätsmanagementsystem fallende KI-System;

d) die Dokumentation über das Qualitätsmanagementsystem mit allen in Artikel 17 aufgeführten Aspekten;

e) eine Beschreibung der bestehenden Verfahren, mit denen sichergestellt wird, dass das Qualitätsmanagementsystem angemessen und wirksam bleibt;

f) eine schriftliche Erklärung, dass derselbe Antrag bei keiner anderen notifizierten Stelle eingereicht wurde.

3.2. Das Qualitätssicherungssystem wird von der notifizierten Stelle bewertet, um festzustellen, ob es die in Artikel 17 genannten Anforderungen erfüllt.

Die Entscheidung wird dem Anbieter oder dessen Bevollmächtigten mitgeteilt.

Die Mitteilung enthält die Ergebnisse der Bewertung des Qualitätsmanagementsystems und die begründete Bewertungsentscheidung.

3.3. Das genehmigte Qualitätsmanagementsystem wird vom Anbieter weiter angewandt und gepflegt, damit es stets angemessen und effizient funktioniert.

3.4. Der Anbieter unterrichtet die notifizierte Stelle über jede beabsichtigte Änderung des genehmigten Qualitätsmanagementsystems oder der Liste der unter dieses System fallenden KI-Systeme.

Die notifizierte Stelle prüft die vorgeschlagenen Änderungen und entscheidet, ob das geänderte Qualitätsmanagementsystem die unter Nummer 3.2 genannten Anforderungen weiterhin erfüllt oder ob eine erneute Bewertung erforderlich ist.

Die notifizierte Stelle teilt dem Anbieter ihre Entscheidung mit. Die Mitteilung enthält die Ergebnisse der Prüfung der Änderungen und die begründete Bewertungsentscheidung.

4. Kontrolle der technischen Dokumentation

4.1. Zusätzlich zu dem unter Nummer 3 genannten Antrag stellt der Anbieter bei der notifizierten Stelle seiner Wahl einen Antrag auf Bewertung der technischen Dokumentation für das KI-System, das er in Verkehr zu bringen oder in Betrieb zu nehmen beabsichtigt und das unter das unter Nummer 3 genannte Qualitätsmanagementsystem fällt.

4.2. Der Antrag enthält Folgendes:

a) den Namen und die Anschrift des Anbieters;

b) eine schriftliche Erklärung, dass derselbe Antrag bei keiner anderen notifizierten Stelle eingereicht wurde;

c) die in Anhang IV genannte technische Dokumentation.

4.3. Die technische Dokumentation wird von der notifizierten Stelle geprüft. Sofern es relevant ist und beschränkt auf das zur Wahrnehmung ihrer Aufgaben erforderliche Maß erhält die notifizierte Stelle uneingeschränkten Zugang zu den verwendeten Trainings-,

Validierungs- und Testdatensätzen, gegebenenfalls und unter Einhaltung von Sicherheitsvorkehrungen auch über API oder sonstige einschlägige technische Mittel und Instrumente, die den Fernzugriff ermöglichen.

4.4. Bei der Prüfung der technischen Dokumentation kann die notifizierte Stelle vom Anbieter weitere Nachweise oder die Durchführung weiterer Tests verlangen, um eine ordnungsgemäße Bewertung der Konformität des KI-Systems mit den in Kapitel III Abschnitt 2 festgelegten Anforderungen zu ermöglichen. Ist die notifizierte Stelle mit den vom Anbieter durchgeführten Tests nicht zufrieden, so führt sie gegebenenfalls unmittelbar selbst angemessene Tests durch.

4.5. Sofern es für die Bewertung der Konformität des Hochrisiko-KI-Systems mit den in Kapitel III Abschnitt 2 festgelegten Anforderungen notwendig ist, und nachdem alle anderen sinnvollen Möglichkeiten zur Überprüfung der Konformität ausgeschöpft sind oder sich als unzureichend erwiesen haben, wird der notifizierten Stelle auf begründeten Antrag Zugang zu den Trainingsmodellen und trainierten Modellen des KI-Systems, einschließlich seiner relevanten Parameter, gewährt. Ein solcher Zugang unterliegt dem bestehenden EU-Recht zum Schutz von geistigem Eigentum und Geschäftsgeheimnissen.

4.6. Die Entscheidung der notifizierten Stelle wird dem Anbieter oder dessen Bevollmächtigten mitgeteilt. Die Mitteilung enthält die Ergebnisse der Bewertung der technischen Dokumentation und die begründete Bewertungsentscheidung.

Erfüllt das KI-System die Anforderungen in Kapitel III Abschnitt 2, so stellt die notifizierte Stelle eine Unionsbescheinigung über die Bewertung der technischen Dokumentation aus. Diese Bescheinigung enthält den Namen und die Anschrift des Anbieters, die Ergebnisse der Prüfung, etwaige Bedingungen für ihre Gültigkeit und die für die Identifizierung des KI-Systems notwendigen Daten.

Die Bescheinigung und ihre Anhänge enthalten alle zweckdienlichen Informationen für die Beurteilung der Konformität des KI-Systems und gegebenenfalls für die Kontrolle des KI-Systems während seiner Verwendung.

Erfüllt das KI-System die in Kapitel III Abschnitt 2 festgelegten Anforderungen nicht, so verweigert die notifizierte Stelle die Ausstellung einer Unionsbescheinigung über die Bewertung der technischen

Dokumentation und informiert den Antragsteller darüber, wobei sie ihre Verweigerung ausführlich begründet.

Erfüllt das KI-System nicht die Anforderung in Bezug auf die verwendeten Trainingsdaten, so muss das KI-System vor der Beantragung einer neuen Konformitätsbewertung erneut trainiert werden. In diesem Fall enthält die begründete Bewertungsentscheidung der notifizierten Stelle, mit der die Ausstellung der Unionsbescheinigung über die Bewertung der technischen Dokumentation verweigert wird, besondere Erläuterungen zu den zum Trainieren des KI-Systems verwendeten Qualitätsdaten und insbesondere zu den Gründen für die Nichtkonformität.

4.7. Jede Änderung des KI-Systems, die sich auf die Konformität des KI-Systems mit den Anforderungen oder auf seine Zweckbestimmung auswirken könnte, bedarf der Bewertung durch die notifizierte Stelle, die die Unionsbescheinigung über die Bewertung der technischen Dokumentation ausgestellt hat. Der Anbieter informiert die notifizierte Stelle über seine Absicht, eine der oben genannten Änderungen vorzunehmen, oder wenn er auf andere Weise Kenntnis vom Eintreten solcher Änderungen erhält. Die notifizierte Stelle bewertet die beabsichtigten Änderungen und entscheidet, ob diese Änderungen eine neue Konformitätsbewertung gemäß Artikel 43 Absatz 4 erforderlich machen oder ob ein Nachtrag zu der Unionsbescheinigung über die Bewertung der technischen Dokumentation ausgestellt werden könnte. In letzterem Fall bewertet die notifizierte Stelle die Änderungen, teilt dem Anbieter ihre Entscheidung mit und stellt ihm, sofern die Änderungen genehmigt wurden, einen Nachtrag zu der Unionsbescheinigung über die Bewertung der technischen Dokumentation aus.

5. Überwachung des genehmigten Qualitätsmanagementsystems

5.1. Mit der unter Nummer 3 genannten Überwachung durch die notifizierte Stelle soll sichergestellt werden, dass der Anbieter sich ordnungsgemäß an die Anforderungen und Bedingungen des genehmigten Qualitätsmanagementsystems hält.

5.2. Zu Bewertungszwecken gewährt der Anbieter der notifizierten Stelle Zugang zu den Räumlichkeiten, in denen die Konzeption, die Entwicklung und das Testen der KI-Systeme stattfindet. Außerdem

übermittelt der Anbieter der notifizierten Stelle alle erforderlichen Informationen.

5.3. Die notifizierte Stelle führt regelmäßig Audits durch, um sicherzustellen, dass der Anbieter das Qualitätsmanagementsystem pflegt und anwendet, und übermittelt ihm einen Prüfbericht. Im Rahmen dieser Audits kann die notifizierte Stelle die KI-Systeme, für die eine Unionsbescheinigung über die Bewertung der technischen Dokumentation ausgestellt wurde, zusätzlichen Tests unterziehen.

I. Worum geht es?

Anhang VII beschreibt ein spezielles **Konformitätsbewertungsverfahren** für Hochrisiko-KI-Systeme. Es verbindet die Prüfung des **QMS** des Anbieters mit einer **Bewertung der technischen Dokumentation** des jeweiligen KI-Systems. Ziel ist es, sicherzustellen, dass Anbieter ihre Systeme nach festgelegten Standards entwickeln und betreiben und dass diese Systeme die Anforderungen der KI-VO erfüllen.

Relevante Artikel: Artikel 17 KI-VO (QMS), Artikel 43 KI-VO (Konformitätsbewertung), Artikel 44 KI-VO ff (Bescheinigungen und Registrierung).

II. Detailkommentar

A. Überblick

- **Kombination von Prüfungen**: Der Anhang legt fest, dass sowohl das interne QMS des Anbieters als auch die externe technische Dokumentation durch eine unabhängige Stelle geprüft werden.
- **Rolle der notifizierten Stelle**: Diese bewertet, genehmigt und überwacht das QMS und prüft die Dokumentation einzelner KI-Systeme.
- **Ergebnis**: Bei erfolgreicher Prüfung erhält der Anbieter eine **Unionsbescheinigung**; bei Mängeln wird sie verweigert.

B. QMS

1. Antrag des Anbieters

- **Identifikationsdaten**: Der Anbieter muss Name, Anschrift und ggf. Daten eines Bevollmächtigten angeben.
- **Systemübersicht**: Liste aller KI-Systeme, die unter das QMS fallen.
- **Technische Unterlagen**: Für jedes System sind die geforderten Dokumente einzureichen.
- **QMS-Dokumentation**: Nach Artikel 17 KI-VO müssen Verfahren zu Design, Entwicklung, Test, Risikomanagement etc. dargestellt werden.
- **Pflege und Wirksamkeit**: Verfahren zur Sicherstellung, dass das QMS aktuell und funktionsfähig bleibt.
- **Exklusivität**: Erklärung, dass derselbe Antrag nicht bei mehreren Stellen eingereicht wurde.

Beispiel: *Ein Anbieter von KI-basierten Kreditbewertungssystemen reicht einen Antrag ein, in dem er sowohl sein Risikomanagementhandbuch als auch die Liste aller geplanten Kreditbewertungsmodelle darlegt.*

2. Bewertung durch die notifizierte Stelle

- **Prüfung der Anforderungen**: Kontrolle, ob das QMS die in Artikel 17 KI-VO festgelegten Anforderungen erfüllt.
- **Mitteilung**: Schriftliche Entscheidung mit Begründung an den Anbieter.

3. Laufende Verpflichtung

- **Pflege**: Das genehmigte QMS muss dauerhaft angewendet werden.
- **Änderungen**: Jede Änderung muss der notifizierten Stelle gemeldet werden. Diese prüft, ob eine neue Bewertung nötig ist oder die Änderung ohne erneute Prüfung akzeptiert werden kann.

Beispiel: *Der Anbieter will ein neues Modul in seine KI-Software integrieren. Dies muss er der notifizierten Stelle melden, die prüft, ob dadurch die Risikobewertung betroffen ist.*

C. Kontrolle der technischen Dokumentation

1. Antrag auf Bewertung

- **Einreichung**: Separater Antrag bei einer notifizierten Stelle.
- **Inhalte**: Identifikationsdaten, Erklärung der Einmaligkeit, vollständige technische Dokumentation nach Anhang IV KI-VO.

2. Prüfung durch die notifizierte Stelle

- **Zugang zu Daten**: Bei Bedarf Zugriff auf Trainings-, Validierungs- und Testdatensätze (ggf über API, unter Wahrung von Sicherheits- und Geheimnisschutz).
- **Nachweise und Tests**: Zusätzliche Nachweise oder Tests können gefordert werden. Die Stelle darf auch eigene Tests durchführen.
- **Zugang zu Modellen**: In Ausnahmefällen können auch die trainierten Modelle und ihre Parameter verlangt werden, stets unter Wahrung von IP- und Geheimnisschutz.

Beispiel: *Eine notifizierte Stelle fordert Einsicht in die Trainingsdaten eines Gesichtserkennungssystems, um zu prüfen, ob die Daten frei von Diskriminierungsmustern sind.*

3. Entscheidung

- **Positive Entscheidung**: Ausstellung einer Unionsbescheinigung mit allen relevanten Daten.
- **Negative Entscheidung**: Verweigerung mit ausführlicher Begründung, insbesondere bei mangelhaften Trainingsdaten (in diesem Fall muss das System neu trainiert werden).

- **Änderungen**: Wesentliche Änderungen am KI-System müssen erneut geprüft werden, was zu einer neuen oder ergänzten Bescheinigung führt.

D. Überwachung des genehmigten QMS

- **Zweck**: Sicherstellung, dass der Anbieter das genehmigte QMS dauerhaft einhält.
- **Zugangsrechte**: Notifizierte Stelle hat Zugang zu Räumen und Informationen.
- **Audits**: Regelmäßige Audits durch die notifizierte Stelle; ggf zusätzliche Tests an bestehenden Systemen.

Beispiel: *Bei einem jährlichen Audit stellt die notifizierte Stelle fest, dass der Anbieter die Dokumentation für ein KI-System nicht aktualisiert hat. Sie fordert eine Nachbesserung.*

III. Zusammenfassung

Kernpunkt	Inhalt	Ergebnis
QMS-Antrag	Anbieter legt Dokumentation und Liste betroffener Systeme vor	Grundlage für Prüfung
Bewertung durch notifizierte Stelle	Prüfung auf Einhaltung von Artikel 17-Anforderungen	Genehmigung oder Ablehnung
Pflege & Änderungen	QMS muss aktuell gehalten, Änderungen gemeldet werden	Fortlaufende Gültigkeit
Technische Dokumentation	Vollständige Unterlagen, ggf. Zugang zu Daten/Modellen	Ausstellung oder Verweigerung einer Bescheinigung
Überwachung	Regelmäßige Audits und Nachprüfungen durch die notifizierte Stelle	Sicherstellung dauerhafter Konformität

Anhang VIII KI-VO

Bei der Registrierung des Hochrisiko-KI-Systems gemäß Artikel 49 bereitzustellende Informationen

Abschnitt A — Von Anbietern von Hochrisiko-KI-Systemen gemäß Artikel 49 Absatz 1 bereitzustellende Informationen

Für Hochrisiko-KI-Systeme, die gemäß Artikel 49 Absatz 1 zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem neuesten Stand gehalten:

1. der Name, die Anschrift und die Kontaktdaten des Anbieters;

2. bei Vorlage von Informationen durch eine andere Person im Namen des Anbieters: der Name, die Anschrift und die Kontaktdaten dieser Person;

3. gegebenenfalls der Name, die Anschrift und die Kontaktdaten des Bevollmächtigten;

4. der Handelsname des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen;

5. eine Beschreibung der Zweckbestimmung des KI-Systems und der durch dieses KI-System unterstützten Komponenten und Funktionen;

6. eine grundlegende und knappe Beschreibung der vom System verwendeten Informationen (Daten, Eingaben) und seiner Betriebslogik;

7. der Status des KI-Systems (in Verkehr/in Betrieb; nicht mehr in Verkehr/in Betrieb, zurückgerufen);

8. die Artikel, die Nummer und das Ablaufdatum der von der notifizierten Stelle ausgestellten Bescheinigung und gegebenenfalls Name oder Identifizierungsnummer dieser notifizierten Stelle;

9. gegebenenfalls eine gescannte Kopie der in Nummer 8 genannten Bescheinigung;

10. alle Mitgliedstaaten, in denen das KI-System in Verkehr gebracht, in Betrieb genommen oder in der Union bereitgestellt wurde;

11. eine Kopie der in Artikel 47 genannten EU-Konformitätserklärung;

12. elektronische Betriebsanleitungen; dies gilt nicht für Hochrisiko-KI-Systeme in den Bereichen Strafverfolgung oder Migration, Asyl und Grenzkontrolle gemäß Anhang III Nummern 1, 6 und 7;

13. Eine URL-Adresse für zusätzliche Informationen (fakultativ).

Abschnitt B — Von Anbietern von Hochrisiko-KI-Systemen gemäß Artikel 49 Absatz 2 bereitzustellende Informationen

Für KI-Systeme, die gemäß Artikel 49 Absatz 2 zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem neuesten Stand gehalten:

1. der Name, die Anschrift und die Kontaktdaten des Anbieters;

2. bei Vorlage von Informationen durch eine andere Person im Namen des Anbieters: Name, Anschrift und Kontaktdaten dieser Person;

3. gegebenenfalls der Name, die Anschrift und die Kontaktdaten des Bevollmächtigten;

4. der Handelsname des KI-Systems und etwaige zusätzliche eindeutige Angaben, die die Identifizierung und Rückverfolgbarkeit des KI-Systems ermöglichen;

5. eine Beschreibung der Zweckbestimmung des KI-Systems;

6. die Bedingung oder Bedingungen gemäß Artikel 6 Absatz 3, aufgrund derer das KI-System nicht als Hoch-Risiko-System eingestuft wird;

7. eine kurze Zusammenfassung der Gründe, aus denen das KI-System in Anwendung des Verfahrens gemäß Artikel 6 Absatz 3 nicht als Hoch-Risiko-System eingestuft wird;

8. der Status des KI-Systems (in Verkehr/in Betrieb; nicht mehr in Verkehr/in Betrieb, zurückgerufen)

9. alle Mitgliedstaaten, in denen das KI-System in der Union in Verkehr gebracht, in Betrieb genommen oder bereitgestellt wurde.

Abschnitt C — Von Betreibern von Hochrisiko-KI-Systemen gemäß Artikel 49 Absatz 3 bereitzustellende Informationen

Für Hochrisiko-KI-Systeme, die gemäß Artikel 49 Absatz 3 zu registrieren sind, werden folgende Informationen

bereitgestellt und danach auf dem neuesten Stand gehalten:

1. der Name, die Anschrift und die Kontaktdaten des Betreibers;

2. der Name, die Anschrift und die Kontaktdaten der Person, die im Namen des Betreibers Informationen übermittelt;

3. die URL des Eintrags des KI-Systems in der EU-Datenbank durch seinen Anbieter;

4. eine Zusammenfassung der Ergebnisse der gemäß Artikel 27 durchgeführten Grundrechte-Folgenabschätzung;

5. gegebenenfalls eine Zusammenfassung der im Einklang mit Artikel 35 der Verordnung (EU) 2016/679 oder Artikel 27 der Richtlinie (EU) 2016/680 gemäß Artikel 26 Absatz 8 der vorliegenden Verordnung durchgeführten Datenschutz-Folgenabschätzung.

I. Worum geht es?

Anhang VIII legt fest, welche Informationen bei der Registrierung von Hochrisiko-KI-Systemen in der EU-Datenbank bereitzustellen sind.

Relevante Artikel: Artikel 49 KI-VO (Registrierung), Artikel 47 KI-VO(EU-Konformitätserklärung), Artikel 27 KI-VO (Grundrechte-Folgenabschätzung), Artikel 26 KI-VO Absatz 8 (Verweis auf Datenschutz-Folgenabschätzungen).

II. Detailkommentar

A. Abschnitt A – Anbieter nach Artikel 49 KI-VO Absatz 1

1. Grundlegende Angaben

- **Name und Kontaktdaten**: Eindeutige Identifizierung des Anbieters.
- **Vertretungsperson**: Falls eine andere Person im Auftrag handelt, müssen deren Daten ebenfalls angegeben werden.
- **Bevollmächtigter**: Nur falls einer bestellt wurde.

2. Systemidentifikation

- **Handelsname und eindeutige Angaben**: Erleichtern die Rückverfolgbarkeit.
- **Zweckbestimmung**: Beschreibung, wofür das System eingesetzt werden soll.
- **Betriebslogik**: Kurze Darstellung, wie das System funktioniert und welche Daten es nutzt.

Beispiel: *Ein Anbieter registriert ein KI-System für die automatische Kreditwürdigkeitsprüfung. Er beschreibt, dass das System Daten wie Einkommen, Beschäftigungsstatus und Bonitätshistorie verarbeitet und die Betriebslogik auf maschinellem Lernen beruht.*

3. Status und Zertifizierung

- **Statusangabe**: Ob das System aktiv genutzt wird, nicht mehr im Verkehr ist oder zurückgerufen wurde.
- **Zertifizierungsangaben**: Artikel, Nummer und Ablaufdatum der Bescheinigung einer notifizierten Stelle.
- **Kopie der Bescheinigung**: Hochzuladen, sofern vorhanden.

4. Weitere Pflichten

- **Mitgliedstaatenangabe**: In welchen Ländern das System bereitgestellt wurde.
- **EU-Konformitätserklärung**: Kopie ist verpflichtend.
- **Betriebsanleitungen**: Elektronisch beizufügen, außer bei bestimmten sicherheitskritischen Bereichen (zB Strafverfolgung).

B. Abschnitt B – Anbieter nach Artikel 49 KI-VO Absatz 2

1. Grundlegende Angaben

- **Name, Anschrift, Kontaktdaten**: Identifizierung des Anbieters.

- **Vertretungsperson oder Bevollmächtigter**: Falls zutreffend.

2. Systembeschreibung

- **Handelsname und eindeutige Angaben**: Zur Rückverfolgbarkeit.
- **Zweckbestimmung**: Beschreibung des vorgesehenen Einsatzes.

3. Begründung für „Nicht-Hochrisiko"-Status

- **Bedingungen nach** Artikel 6 KI-VO **Absatz 3**: Darlegung, warum das System nicht als Hochrisiko eingestuft wurde.
- **Kurze Begründung**: Erläuterung der Entscheidung.

Beispiel: *Ein Chatbot für Kundendienst wird zunächst geprüft. Der Anbieter begründet, dass das System nicht in einem Anwendungsfeld des Anhangs III eingesetzt wird und daher nicht als Hochrisiko gilt.*

4. Statusangaben

- **Status**: Aktiv, inaktiv oder zurückgerufen.
- **Mitgliedstaaten**: Angabe, wo das System bereitgestellt wurde.

C. Abschnitt C – Betreiber nach Artikel 49 KI-VO Absatz 3

1. Identitätsangaben

- **Name und Kontaktdaten**: Klare Zuordnung des Betreibers.
- **Vertretungsperson**: Falls die Registrierung durch Dritte erfolgt.

2. Systembezug

- **URL des Eintrags in der EU-Datenbank**: Verknüpfung zum Anbieter-Eintrag.

3. Folgenabschätzungen

- **Grundrechte-Folgenabschätzung**: Zusammenfassung der Ergebnisse nach Artikel 27 KI-VO.
- **Datenschutz-Folgenabschätzung**: Falls nach DSGVO oder RL (EU) 2016/680 verpflichtend.

Beispiel: *Eine Behörde, die ein biometrisches KI-System einsetzt, muss eine Grundrechte-Folgenabschätzung vorlegen und zusätzlich eine Datenschutz-Folgenabschätzung, wenn sensible Daten verarbeitet werden.*

III. Zusammenfassung

Verpflichtete	Bereitzustellende Kerninformationen
Anbieter (Artikel 49 KI-VO Absatz 1)	Identität, Systemdaten, Zweck, Betriebslogik, Status, Zertifizierungen, Konformitätserklärung, Betriebsanleitungen
Anbieter (Artikel 49 Absatz 2)	Identität, Systemdaten, Zweck, Begründung für Nicht-Hochrisiko-Status, Status, Mitgliedstaaten
Betreiber (Artikel 49 Absatz 3)	Identität, Bezug zum EU-Eintrag, Grundrechte-Folgenabschätzung, ggf Datenschutz-Folgenabschätzung

Anhang IX KI-VO

Bezüglich Tests unter Realbedingungen gemäß Artikel 60 bei der Registrierung von in Anhang III aufgeführten Hochrisiko-KI-Systemen bereitzustellende Informationen

Bezüglich Tests unter Realbedingungen, die gemäß Artikel 60 zu registrieren sind, werden folgende Informationen bereitgestellt und danach auf dem aktuellen Stand gehalten:

1. *eine unionsweit einmalige Identifizierungsnummer des Tests unter Realbedingungen;*
2. *der Name und die Kontaktdaten des Anbieters oder zukünftigen Anbieters und der Betreiber, die an dem Test unter Realbedingungen teilgenommen haben;*
3. *eine kurze Beschreibung des KI-Systems, seine Zweckbestimmung und sonstige zu seiner Identifizierung erforderliche Informationen;*
4. *eine Übersicht über die Hauptmerkmale des Plans für den Test unter Realbedingungen;*
5. *Informationen über die Aussetzung oder den Abbruch des Tests unter Realbedingungen.*

I. Worum geht es?

Anhang IX regelt, welche **Informationen verpflichtend bereitgestellt werden müssen**, wenn ein **Test unter Realbedingungen** für ein Hochrisiko-KI-System (aus Anhang III KI-VO) gemäß Artikel 60 KI-VO registriert wird. Ziel ist es, Transparenz und Nachvollziehbarkeit zu sichern, indem zentrale Daten zum Test dokumentiert und aktuell gehalten werden.

Relevante Artikel: Artikel 60 KI-VO (Tests unter Realbedingungen).

II. Detailkommentar

A. Identifikationsnummer

- **Eindeutige Kennung**: Jeder Test erhält eine unionsweit einmalige Identifikationsnummer.

- **Zweck**: Sicherstellung der Nachverfolgbarkeit und Vermeidung von Doppelungen.

Beispiel: *Ein Test zur Erprobung eines KI-Systems zur Bewerberauswahl erhält die Nummer „EU-RT-2026-000123“. Damit ist der Test in der gesamten Union eindeutig erfasst.*

B. Angaben zu Anbietern und Betreibern

- **Name und Kontaktdaten**: Sowohl der Anbieter (oder zukünftige Anbieter) als auch die Betreiber müssen mit ihren Daten erfasst werden.
- **Zweck**: Ermöglicht die direkte Kontaktaufnahme und Verantwortlichkeitsklärung.

Beispiel: *Ein KI-Hersteller in Deutschland testet sein System in Zusammenarbeit mit einem Krankenhaus in Spanien. Beide werden mit Namen, Adresse und E-Mail registriert.*

C. Beschreibung des KI-Systems

- **Kurzbeschreibung**: Darstellung, worum es sich bei dem KI-System handelt.
- **Zweckbestimmung**: Angabe, für welchen Einsatz das System vorgesehen ist.
- **Weitere Identifikationsinformationen**: zB Versionsnummer oder technische Merkmale.

Beispiel: *Das System dient der automatisierten Analyse von Röntgenbildern, Version 3.2, mit Fokus auf Erkennung von Lungenentzündungen.*

D. Übersicht des Testplans

- **Hauptmerkmale**: Darstellung der geplanten Vorgehensweise.
- **Transparenz**: Dritte sollen nachvollziehen können, wie der Test strukturiert ist.

Beispiel: *Der Testplan sieht die Auswertung von 5.000 Fällen über einen Zeitraum von sechs Monaten vor, wobei eine Vergleichsgruppe von Ärzten parallel bewertet.*

E. Angaben zu Abbruch oder Aussetzung

- **Pflicht zur Aktualisierung**: Wenn ein Test ausgesetzt oder abgebrochen wird, muss dies gemeldet werden.
- **Sicherheitsaspekt**: Dient der Aufklärung über mögliche Probleme oder Risiken während des Tests.

Beispiel: *Ein Test wird abgebrochen, weil sich während der Durchführung unerwartete Datenschutzprobleme zeigen.*

III. Zusammenfassung

Pflichtinformation	**Zweck**
Identifikationsnummer	Eindeutige Erfassung und Nachverfolgbarkeit
Anbieter & Betreiber	Verantwortlichkeiten klarstellen
Beschreibung des Systems	Zweck und Identifikation
Übersicht des Testplans	Transparenz über Vorgehen
Angaben zu Abbruch/Aussetzung	Aufklärung über Probleme

Anhang X KI-VO

Rechtsvorschriften der Union über IT-Großsysteme im Raum der Freiheit, der Sicherheit und des Rechts

1. Schengener Informationssystem

a) Verordnung (EU) 2018/1860 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger (ABl. L 312 vom 7.12.2018, S. 1)

b) Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr 1987/2006 (ABl. L 312 vom 7.12.2018, S. 14)

c) Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56)

2. Visa-Informationssystem

a) Verordnung (EU) 2021/1133 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Änderung der Verordnungen (EU) Nr 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 und (EU) 2019/818 hinsichtlich der Festlegung der Voraussetzungen für den Zugang zu anderen Informationssystemen der EU für Zwecke des Visa-Informationssystems (ABl. L 248 vom 13.7.2021, S. 1)

b) Verordnung (EU) 2021/1134 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Änderung der Verordnungen (EG) Nr 767/2008, (EG) Nr 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 und (EU) 2019/1896 des Europäischen Parlaments und des Rates und zur Aufhebung der Entscheidung 2004/512/EG und des Beschlusses 2008/633/JI des Rates

zum Zwecke der Reform des Visa-Informationssystems (ABl. L 248 vom 13.7.2021, S. 11)

3. Eurodac

Verordnung (EU) 2024/1358 des Europäischen Parlaments und des Rates vom 14. Mai 2024 über die Einrichtung von Eurodac für den Abgleich biometrischer Daten zum Zwecke der effektiven Anwendung der Verordnungen (EU) 2024/1315 und (EU) 2024/1350 des Europäischen Parlaments und des Rates und der Richtlinie 2001/55/EG des Rates und zur Feststellung der Identität illegal aufhältiger Drittstaatsangehöriger und Staatenloser und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnungen (EU) 2018/1240 und (EU) 2019/818 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnung (EU) Nr 603/2013 des Europäischen Parlaments und des Rates (ABl. L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj)

4. Einreise-/Ausreisesystem

Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr 767/2008 und (EU) Nr 1077/2011 (ABl. L 327 vom 9.12.2017, S. 20)

5. Europäisches Reiseinformations- und -genehmigungssystem

a) Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr 1077/2011, (EU) Nr 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226 (ABl. L 236 vom 19.9.2018, S. 1)

b) Verordnung (EU) 2018/1241 des Europäischen Parlaments und des Rates vom 12. September 2018 zur Änderung der Verordnung (EU) 2016/794

für die Zwecke der Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) (ABl. L 236 vom 19.9.2018, S. 72)

6. Europäisches Strafregisterinformationssystem über Drittstaatsangehörige und Staatenlose

Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726 (ABl. L 135 vom 22.5.2019, S. 1)

7. Interoperabilität

a) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27)

b) Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816 (ABl. L 135 vom 22.5.2019, S. 85).

I. Worum geht es?

Anhang X enthält die Rechtsgrundlagen für die wichtigsten unionsweiten Informationssysteme im Bereich Migration, Grenzkontrolle, Strafverfolgung und Sicherheit. Diese Systeme sind besonders sensibel, da sie große Mengen personenbezogener und biometrischer Daten verarbeiten. Wird KI in diesem Kontext eingesetzt, gelten strengste Vorgaben für Hochrisiko-Systeme.

Relevante Artikel: Artikel 6 KI-VO (Einstufungsvorschriften für Hochrisiko-KI-Systeme), **Artikel 43 KI-VO** (Konformitätsbewertung) und Artikel 84 KI-VO (Unionsstrukturen zur Unterstützung der Prüfung von KI).

II. Detailkommentar

A. Schengener Informationssystem (SIS)

- **Mehrere Teilbereiche**: Rückkehr illegal aufhältiger Personen, Grenzkontrollen und polizeiliche/judizielle Zusammenarbeit.
- **Kernfunktion**: Speicherung und Abruf von Informationen über Personen und Sachen für Sicherheits- und Grenzschutzbehörden.
- **Risiko**: KI-gestützte Analysen können Fehlalarme oder diskriminierende Treffer erzeugen.

Beispiel*: Eine KI schlägt vor, dass eine Person auf einer SIS-Fahndungsliste auftaucht, obwohl es sich um eine Namensähnlichkeit handelt.*

B. Visa-Informationssystem (VIS)

- **Zweck**: Verwaltung von Daten für Visaerteilungen und Abgleich mit anderen EU-Datenbanken.
- **Ergänzende Regelungen**: Zugang auch für Sicherheitsbehörden.
- **Risiko**: Automatisierte Entscheidungen über Visa können Grundrechte verletzen.

Beispiel: *Ein Algorithmus lehnt einen Visumantrag ab, ohne dass ein menschlicher Prüfer den Fall noch einmal betrachtet.*

C. Eurodac

- **Funktion**: Abgleich biometrischer Daten von Staatenlosen und Drittstaatsangehörigen.
- **Zweck**: Erleichterung der VO (EU) 603/2013 und Unterstützung bei Strafverfolgung.

- **Risiko**: Falschzuordnungen durch fehlerhafte KI-Biometrie können gravierende Folgen haben.

Beispiel: *Ein Asylbewerber wird aufgrund eines fehlerhaften Fingerabdruck-Matches einem falschen Mitgliedstaat zugeordnet.*

D. Einreise-/Ausreisesystem (EES)

- **Zweck**: Speicherung von Ein- und Ausreisedaten an EU-Außengrenzen.
- **Besonderheit**: Enthält auch Daten über abgelehnte Einreisen.
- **Risiko**: KI-gestützte Mustererkennung kann Reisende zu Unrecht als „auffällig" markieren.

Beispiel: *Ein Vielreisender wird durch eine KI als verdächtig eingestuft, nur weil er häufig zwischen EU und Drittstaaten pendelt.*

E. ETIAS (Europäisches Reiseinformations- und -genehmigungssystem)

- **Zweck**: Vorabprüfung von Drittstaatsangehörigen, die visumfrei in die EU reisen wollen.
- **Datenumfang**: Erfasst Reise- und Sicherheitsdaten.
- **Risiko**: Automatisierte Risikobewertungen können diskriminierend wirken.

Beispiel: *Eine KI verweigert die Reisegenehmigung, weil sie Daten falsch mit einer Sicherheitsdatenbank verknüpft.*

F. ECRIS-TCN (Europäisches Strafregister für Drittstaatsangehörige und Staatenlose)

- **Zweck**: Zentrale Übersicht, in welchem Mitgliedstaat Strafregistereinträge bestehen.
- **Risiko**: KI-gestützte Suchverfahren könnten falsche Treffer liefern.

Beispiel: *Eine Person wird bei einem Strafverfahren fälschlich als vorbestraft eingestuft, weil die KI einen gleichnamigen Datensatz zuordnet.*

G. Interoperabilität

- **Rahmenverordnungen**: Schaffen die Grundlage für die Verknüpfung der genannten Systeme.
- **Zweck**: Effizienterer Datenaustausch zwischen verschiedenen Bereichen (Grenzen, Visa, Asyl, Polizei).
- **Risiko**: Durch KI können Querverbindungen entstehen, die zu Überwachung oder Fehlerketten führen.

Beispiel: *Eine KI verknüpft Daten aus ETIAS und SIS, wodurch eine Person fälschlich als Sicherheitsrisiko eingestuft wird.*

III. Zusammenfassung

System	Zweck	Risiko bei KI-Einsatz
SIS	Fahndung & Grenzkontrolle	Fehlalarme, Diskriminierung
VIS	Visaerteilung	Automatisierte Ablehnung
Eurodac	Fingerabdruck-Abgleich	Falschzuordnung
EES	Ein- und Ausreisedaten	Falsche Risikoeinstufung
ETIAS	Reisegenehmigung	Diskriminierende Bewertungen
ECRIS-TCN	Strafregisterauskünfte	Falsche Zuordnung
Interoperabilität	Verknüpfung von Systemen	Fehlerketten, Überwachung

Anhang XI KI-VO

Technische Dokumentation gemäß Artikel 53 Absatz 1 Buchstabe a — technische Dokumentation für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

Abschnitt 1

Von allen Anbietern von KI-Modellen mit allgemeinem Verwendungszweck bereitzustellende Informationen

Die in Artikel 53 Absatz 1 Buchstabe a genannte technische Dokumentation muss mindestens die folgenden Informationen enthalten, soweit es anhand der Größe und des Risikoprofils des betreffenden Modells angemessen ist:

1.Eine allgemeine Beschreibung des KI-Modells einschließlich

a)der Aufgaben, die das Modell erfüllen soll, sowie der Artikel und des Wesens der KI-Systeme, in die es integriert werden kann;

b) die anwendbaren Regelungen der akzeptablen Nutzung;

c) das Datum der Freigabe und die Vertriebsmethoden;

d) die Architektur und die Anzahl der Parameter;

e)die Modalität (zum Beispiel Text, Bild) und das Format der Ein- und Ausgaben;

f) die Lizenz.

2.Eine ausführliche Beschreibung der Elemente des Modells gemäß Nummer 1 und relevante Informationen zum Entwicklungsverfahren, einschließlich der folgenden Elemente:

a)die technischen Mittel (zum Beispiel Betriebsanleitungen, Infrastruktur, Instrumente), die für die Integration des KI-Modells mit allgemeinem Verwendungszweck in KI-Systeme erforderlich sind;

b)die Entwurfsspezifikationen des Modells und des Trainingsverfahrens einschließlich Trainingsmethoden und -techniken, die wichtigsten Entwurfsentscheidungen mit den Gründen und getroffenen Annahmen; gegebenenfalls, was das Modell optimieren soll und welche Bedeutung den verschiedenen Parametern dabei zukommt;

c)gegebenenfalls Informationen über die für das Trainieren, Testen und Validieren verwendeten Daten, einschließlich der Artikel und Herkunft

der Daten und der Aufbereitungsmethoden (zum Beispiel Bereinigung, Filterung usw.), der Zahl der Datenpunkte, ihres Umfangs und ihrer Hauptmerkmale; gegebenenfalls die Artikel und Weise, wie die Daten erlangt und ausgewählt wurden, sowie alle anderen Maßnahmen zur Feststellung, ob Datenquellen ungeeignet sind, und Methoden zur Erkennung ermittelbarer Verzerrungen;

d)die für das Trainieren des Modells verwendeten Rechenressourcen (zum Beispiel Anzahl der Gleitkommaoperationen), die Trainingszeit und andere relevante Einzelheiten im Zusammenhang mit dem Trainieren;

e) bekannter oder geschätzter Energieverbrauch des Modells.

Wenn der Energieverbrauch des Modells nicht bekannt ist, kann für Buchstabe e der Energieverbrauch auf Informationen über die eingesetzten Rechenressourcen gestützt werden.

Abschnitt 2

Zusätzliche von Anbietern von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko bereitzustellende Informationen

1.Eine ausführliche Beschreibung der Prüfstrategien, einschließlich der Prüfungsergebnisse, auf der Grundlage öffentlich verfügbarer Prüfprotokolle und -instrumente oder anderer Prüfmethoden. Die Prüfstrategien umfassen Prüfkriterien und -metrik sowie die Methodik zur Ermittlung von Einschränkungen.

2.Gegebenenfalls eine ausführliche Beschreibung der Maßnahmen, die ergriffen wurden, um interne und/oder externe Angriffstests durchzuführen (zum Beispiel Red Teaming), Modellanpassungen, einschließlich Ausrichtung und Feinabstimmung.

3.Gegebenenfalls eine ausführliche Beschreibung der Systemarchitektur, aus der hervorgeht, wie Softwarekomponenten aufeinander aufbauen oder einander zuarbeiten und in die Gesamtverarbeitung integriert sind.

I. Worum geht es?

Anhang XI legt fest, welche Informationen Anbieter von KI-Modellen mit allgemeinem Verwendungszweck in ihrer technischen Dokumentation bereitstellen müssen. Ziel ist es, Transparenz, Nachvollziehbarkeit und

Sicherheit zu gewährleisten. Für Modelle mit systemischem Risiko gelten zusätzliche, erweiterte Dokumentationspflichten.

Relevante Artikel: Artikel 53 KI-VO (Pflichten der Anbieter von Modellen mit allgemeinem Verwendungszweck), Artikel 55 KI-VO (Pflichten der Anbieter von Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko)

II. Detailkommentar

A. Grundanforderungen an die technische Dokumentation

1. Allgemeine Beschreibung des Modells

- **Aufgaben und Einsatzmöglichkeiten**: Anbieter müssen die Aufgaben des Modells sowie die Artikel und das Wesen der KI-Systeme, in die es integriert werden kann, angeben.
- **Nutzungsregeln**: Es ist festzuhalten, welche Anwendungen erlaubt sind und welche ausgeschlossen werden sollen.
- **Zeitpunkt und Verbreitung**: Dokumentiert werden das Freigabedatum und die Vertriebswege des Modells.
- **Architektur und Parameter**: Angaben zur technischen Struktur und zur Anzahl der Modellparameter sind erforderlich.
- **Modalität**: Erfasst werden die Artikel der Eingaben und Ausgaben (zB Text, Bild) und deren Format.
- **Lizenz**: Anbieter müssen die rechtliche Grundlage der Nutzung (zB Open Source oder kommerziell) angeben.

Beispiel: *Ein Sprachmodell, das für Textgenerierung vorgesehen ist, muss klarstellen, dass es nicht für medizinische Diagnosen genutzt werden darf.*

2. Beschreibung des Entwicklungsverfahrens

- **Technische Mittel**: Beschrieben werden muss, welche Infrastruktur und Hilfsmittel für die Integration des Modells notwendig sind.

- **Entwurfsspezifikationen**: Dazu gehören Informationen zu Trainingsmethoden, Designentscheidungen und zugrunde liegenden Annahmen.
- **Datenbasis**: Soweit verfügbar, Angaben über Artikel, Herkunft, Aufbereitung und Auswahl der Trainings- und Testdaten.
- **Rechenressourcen**: Dokumentation der eingesetzten Rechenleistung, Trainingsdauer und sonstiger technischer Parameter.
- **Energieverbrauch**: Bekannte oder geschätzte Angaben zum Energiebedarf des Modells.

Beispiel: *Ein Bildklassifikationsmodell müsste darlegen, dass es auf Millionen von Fotos aus frei zugänglichen Datenbanken trainiert wurde und während des Trainings hohe Rechenressourcen verbrauchte.*

B. Zusätzliche Anforderungen bei systemischem Risiko

1. Prüfstrategien

- **Testmethoden**: Anbieter müssen Prüfungen dokumentieren, etwa durch anerkannte Protokolle oder eigene Verfahren.
- **Kriterien und Metriken**: Klarheit darüber, nach welchen Maßstäben das Modell bewertet wurde.

Beispiel: *Ein besonders einflussreiches Sprachmodell könnte durch externe Prüfungen getestet werden, um Vorurteile oder Sicherheitslücken zu identifizieren.*

2. Angriffstests und Anpassungen

- **Red Teaming**: Gezielte Tests zur Aufdeckung von Schwachstellen sind zu dokumentieren.
- **Feinabstimmungen**: Informationen zu nachträglichen Anpassungen des Modells, insbesondere zur Ausrichtung auf bestimmte Zwecke, müssen vorliegen.

Beispiel: *Ein Anbieter dokumentiert, dass sein Modell mit Angriffstests auf Falschinformationen geprüft und anschließend nachtrainiert wurde.*

3. Systemarchitektur

- **Softwareintegration**: Offenlegung, wie die einzelnen Softwarekomponenten zusammenarbeiten und in die Gesamtstruktur eingebettet sind.

Beispiel: *Ein Anbieter erklärt, dass das Modell Teil einer größeren Plattform ist, die auch Datenvorverarbeitung und Sicherheitsfilter umfasst.*

III. Zusammenfassung

Bereich	**Pflichtinhalte**
Allgemeine Beschreibung	Aufgabenbereich, Nutzungsregeln, Freigabedatum, Architektur, Modalität der Ein- und Ausgaben, Lizenz
Entwicklungsverfahren	Technische Mittel, Entwurfsspezifikationen, Datenbasis, Rechenressourcen, Energieverbrauch
Zusätzliche Pflichten bei systemischem Risiko	Prüfstrategien und Ergebnisse, Angriffstests und Anpassungen, detaillierte Systemarchitektur

Anhang XII KI-VO

Transparenzinformationen gemäß Artikel 53 Absatz 1 Buchstabe b — technische Dokumentation für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck für nachgelagerte Anbieter, die das Modell in ihr KI-System integrieren

Die in Artikel 53 Absatz 1 Buchstabe b genannten Informationen enthalten mindestens Folgendes:

1.eine allgemeine Beschreibung des KI-Modells einschließlich

a)der Aufgaben, die das Modell erfüllen soll, sowie der Artikel und des Wesens der KI-Systeme, in die es integriert werden kann;

b) die anwendbaren Regelungen der akzeptablen Nutzung;

c) das Datum der Freigabe und die Vertriebsmethoden;

d)gegebenenfalls wie das Modell mit Hardware oder Software interagiert, die nicht Teil des Modells selbst ist, oder wie es zu einer solchen Interaktion verwendet werden kann;

e)gegebenenfalls die Versionen der einschlägigen Software im Zusammenhang mit der Verwendung des KI-Modells mit allgemeinem Verwendungszweck;

f) die Architektur und die Anzahl der Parameter;

g)die Modalität (zum Beispiel Text, Bild) und das Format der Ein- und Ausgaben;

h) die Lizenz für das Modell.

2.Eine Beschreibung der Bestandteile des Modells und seines Entwicklungsprozesses, einschließlich

a)die technischen Mittel (zum Beispiel Betriebsanleitungen, Infrastruktur, Instrumente), die für die Integration des KI-Modells mit allgemeinem Verwendungszweck in KI-Systeme erforderlich sind;

b)Modalität (zum Beispiel Text, Bild usw.) und Format der Ein- und Ausgaben und deren maximale Größe (zum Beispiel Länge des Kontextfensters usw.);

c)gegebenenfalls Informationen über die für das Trainieren, Testen und Validieren verwendeten Daten, einschließlich der Artikel und Herkunft der Daten und der Aufbereitungsmethoden.

I. Worum geht es?

Anhang XII legt fest, welche Transparenzinformationen Anbieter von KI-Modellen mit allgemeinem Verwendungszweck bereitstellen müssen. Diese Informationen sind für nachgelagerte Anbieter gedacht, die das Modell in eigene KI-Systeme integrieren. Ziel ist es, eine nachvollziehbare und sichere Nutzung zu gewährleisten.

Relevante Artikel: Artikel 53 KI-VO (Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck)

II. Detailkommentar

A. Allgemeine Beschreibung des KI-Modells

- **Aufgaben und Einsatzmöglichkeiten**: Anbieter müssen die Aufgaben des Modells sowie die Artikel und das Wesen der KI-Systeme angeben, in die es integriert werden kann. Dadurch erhalten nachgelagerte Anbieter die notwendigen Informationen, um das Modell sachgerecht in eigene Systeme einzubinden.
- **Regeln der Nutzung**: Vorgaben zur akzeptablen Nutzung (zB keine Nutzung für rechtswidrige Inhalte) müssen offengelegt werden. So werden Missbrauchsrisiken reduziert.
- **Freigabedatum und Vertrieb**: Angaben zum Zeitpunkt der Veröffentlichung und zu den Verbreitungswegen (zB Open Source, Lizenzmodell) sichern Transparenz.
- **Interaktionen mit fremder Software/Hardware**: Informationen, wie das Modell mit anderer Technik kombiniert werden kann oder muss, erleichtern die Integration.
- **Softwareversionen**: Wenn bestimmte Versionen von Software nötig sind, müssen diese klar benannt werden.

- **Architektur und Parameterzahl**: Grundlegende Angaben zum technischen Aufbau und zur Größe des Modells helfen bei der technischen Einschätzung.
- **Modalität und Formate**: Ob Text, Bild oder andere Eingaben und Ausgaben verarbeitet werden, muss klar ersichtlich sein.
- **Lizenz**: Die rechtlichen Rahmenbedingungen der Nutzung (zB Open-Source-Lizenz, kommerzielle Lizenz) sind verbindlich anzugeben.

Beispiel: *Ein Sprachmodell, das zur Textgenerierung dient, muss angeben, dass es Texte verarbeiten und generieren kann, nur mit bestimmten Softwarebibliotheken funktioniert und unter einer Creative-Commons-Lizenz genutzt werden darf.*

B. Beschreibung des Modells und Entwicklungsprozesses

- **Technische Mittel für die Integration**: Anbieter müssen auflisten, welche Hilfsmittel oder Anleitungen notwendig sind, damit Dritte das Modell korrekt in ihre Systeme einbauen können.
- **Modalität, Formate und Größenbeschränkungen**: Es müssen auch Beschränkungen angegeben werden, zB wie lang der Eingabetext maximal sein darf.
- **Daten für Training, Test und Validierung**: Falls relevant, sind Artikel, Herkunft und Aufbereitung der verwendeten Daten offenzulegen. Das soll Transparenz über mögliche Vorurteile oder Qualitätsgrenzen schaffen.

Beispiel: *Ein Bildklassifikationsmodell gibt an, dass es für Eingaben in JPEG-Format mit einer maximalen Auflösung von 1024x1024 Pixeln ausgelegt ist und mit einem Datensatz aus öffentlich zugänglichen Bildern trainiert wurde.*

III. Zusammenfassung

Bereich	Kernanforderungen	Nutzen für Nachgelagerte

Allgemeine Modellbeschreibung	Aufgaben, Nutzungsvorgaben, Architektur, Modalitäten, Lizenz	Verstehen, wofür und wie das Modell genutzt werden darf
Technische Angaben	Anleitungen, Softwareanforderungen, Eingabe-/Ausgabeformate	Erleichterung der Integration in eigene Systeme
Entwicklungsinformationen	Trainingsdaten (Artikel, Herkunft, Aufbereitung)	Bewertung von Qualität und möglichen Verzerrungen

Anhang XIII KI-VO

Kriterien für die Benennung von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko gemäß Artikel 51

Um festzustellen, ob ein KI-Modell mit allgemeinem Verwendungszweck über Fähigkeiten oder eine Wirkung verfügt, die den in Artikel 51 Absatz 1 Buchstabe a genannten gleichwertig sind, berücksichtigt die Kommission folgende Kriterien:

a) die Anzahl der Parameter des Modells;

b)die Qualität oder Größe des Datensatzes, zum Beispiel durch Tokens gemessen;

c)die Menge der für das Trainieren des Modells verwendeten Berechnungen, gemessen in Gleitkommaoperationen oder anhand einer Kombination anderer Variablen, wie geschätzte Trainingskosten, geschätzter Zeitaufwand für das Trainieren oder geschätzter Energieverbrauch für das Trainieren;

d)die Ein- und Ausgabemodalitäten des Modells, wie Text-Text (Große Sprachmodelle), Text-Bild, Multimodalität, Schwellenwerte auf dem Stand der Technik für die Bestimmung der Fähigkeiten mit hoher Wirkkraft für jede Modalität und die spezifische Artikel der Ein- und Ausgaben (zum Beispiel biologische Sequenzen);

e)die Benchmarks und Beurteilungen der Fähigkeiten des Modells, einschließlich unter Berücksichtigung der Zahl der Aufgaben ohne zusätzliches Training, der Anpassungsfähigkeit zum Erlernen neuer, unterschiedlicher Aufgaben, des Grades an Autonomie und Skalierbarkeit sowie der Instrumente, zu denen es Zugang hat;

f)ob es aufgrund seiner Reichweite große Auswirkungen auf den Binnenmarkt hat — davon wird ausgegangen, wenn es mindestens 10 000 in der Union niedergelassenen registrierten gewerblichen Nutzern zur Verfügung gestellt wurde;

g) die Zahl der registrierten Endnutzer.

I. Worum geht es?

Anhang XIII beschreibt die Kriterien, nach denen die Kommission feststellt, ob ein KI-Modell mit allgemeinem Verwendungszweck ein systemisches Risiko aufweist. Dabei geht es um besonders leistungsfähige Modelle, deren Fähigkeiten oder Wirkungen so weitreichend sind, dass sie in erheblichem Umfang Grundrechte, Gesundheit oder Sicherheit beeinträchtigen können.

Relevante Artikel: Artikel 51 KI-VO (systemisches Risiko), Artikel 52 KI-VO (Verfahren).

II. Detailkommentar

A. Grundidee

- **Systemisches Risiko**: Es geht um Modelle, die aufgrund ihrer Fähigkeiten oder Reichweite den Binnenmarkt oder die Gesellschaft in großem Maßstab beeinflussen können.
- **Zentrale Rolle der Kommission**: Die Entscheidung, ob ein Modell dieses Risiko aufweist, trifft die Kommission anhand der in Anhang XIII genannten Kriterien.

B. Kriterien im Einzelnen

1. Modellgröße (a)

Anzahl der Parameter: Je mehr Parameter, desto komplexer und potenziell mächtiger ist das Modell. Viele Parameter deuten auf hohe Rechenleistung und Lernfähigkeit hin.

Beispiel: *Ein Sprachmodell mit mehreren hundert Milliarden Parametern kann selbstständig Texte in vielen Sprachen verfassen und dadurch enorme Reichweite entfalten.*

2. Datensätze (b)

Qualität und Größe: Entscheidend ist nicht nur die Menge, sondern auch die Vielfalt und Repräsentativität der Trainingsdaten.

Beispiel: *Ein Modell, das auf Milliarden von Texten aus dem Internet trainiert ist, kann ein breites Wissen simulieren, birgt aber auch die Gefahr von Fehlinformationen.*

3. Rechenaufwand (c)

Trainingsressourcen: Anzahl der Berechnungen, Kosten, Zeit oder Energieverbrauch zeigen, wie groß der technische Aufwand für das Modell ist.

Beispiel: *Ein Modell, dessen Training Millionen Euro kostet und mehrere Wochen auf Supercomputern läuft, gilt als besonders leistungsstark.*

4. Ein- und Ausgabemodalitäten (d)

Vielfalt der Modalitäten: Modelle können Texte, Bilder, Sprache oder biologische Daten verarbeiten. Multimodale Modelle sind besonders mächtig.

Beispiel: *Ein Modell, das Text versteht und gleichzeitig Bilder erzeugen kann, eröffnet neue, weitreichende Einsatzmöglichkeiten.*

5. Leistungsfähigkeit (e)

Benchmarks und Tests: Entscheidend sind die Fähigkeiten, ohne zusätzliches Training viele Aufgaben zu lösen, die Lernfähigkeit für neue Aufgaben sowie die Autonomie und Skalierbarkeit.

Beispiel: *Ein Modell, das ohne weiteres Training sowohl juristische Texte analysieren als auch Code schreiben kann, gilt als hochgradig anpassungsfähig.*

6. Marktverbreitung – Gewerbliche Nutzer (f)

10.000 gewerbliche Nutzer: Wird ein Modell von so vielen Unternehmen in der EU genutzt, geht der Gesetzgeber automatisch von hoher Marktrelevanz aus.

Beispiel: *Ein KI-Textgenerator, der in tausenden europäischen Firmen im Kundenservice eingesetzt wird, hat großen Einfluss auf den Binnenmarkt.*

7. Marktverbreitung – Endnutzer (g)

Zahl der registrierten Nutzer: Auch eine sehr hohe Zahl an Privatnutzern kann auf ein systemisches Risiko hinweisen.

Beispiel: *Ein Chatbot mit Millionen aktiver Nutzer in der EU kann gesellschaftlich relevante Auswirkungen haben, zB auf öffentliche Meinung.*

C. Systematische Einordnung

- **Anhang XIII ergänzt Artikel 51 KI-VO**: Er macht die abstrakten Vorgaben konkret und gibt der Kommission objektive Kriterien an die Hand.
- **Zielsetzung der Norm**: Schutz des Binnenmarkts und der Gesellschaft vor unkontrollierten Risiken besonders mächtiger KI-Modelle.

III. Zusammenfassung

Kriterium	Bedeutung	Beispiel
Parameterzahl	Größe und Komplexität des Modells	Milliarden Parameter = große Leistungsfähigkeit
Datensatzgröße	Umfang und Qualität der Trainingsdaten	Internetweite Textbasis
Rechenaufwand	Kosten, Energie, Dauer des Trainings	Wochenlange Supercomputer-Nutzung
Modalitäten	Artikel der Eingaben/Ausgaben	Text, Bild, Audio, multimodal
Leistungsfähigkeit	Benchmarks, Anpassungsfähigkeit, Autonomie	Vielseitige Aufgabenlösungen

Marktverbreitung	Ab 10.000 gewerbliche Nutzer in der EU	Breiter Einsatz in Firmen
Endnutzerzahl	Reichweite im Alltag	Millionen von Chatbot-Nutzern

Dokumentation der Vorgehensweise zur Erstellung des Kommentars zur KI-VO

1. Ausgangspunkt und Ziel

Die erläuternde Darstellung der KI-Verordnung (KI-VO) wurde mit dem Ziel erstellt, die komplexen juristischen Vorgaben in verständlicher Sprache für juristische Laien und nichtspezialisierte Jurist:innen unter Verwendung generativer KI aufzubereiten. Der Fokus lag auf Klarheit, Prägnanz und systematischer Struktur.

2. Grundlage der Arbeit

Als methodische Basis diente ein festgelegter Masterprompt, der die Rolle, Zielgruppe, zulässigen Quellen und das gewünschte Ausgabeformat definierte. Der Masterprompt wurde im Zuge intensiver fachlicher Abstimmungen und Diskussionen wiederholt angepasst, strukturell verfeinert und inhaltlich weiterentwickelt. Die inhaltliche Überprüfung und rechtliche Bewertung der Ergebnisse erfolgen auf Grundlage juristischer Fachkenntnisse und juristischer Arbeitsweise.

- Quellenbasis: ausschließlich der Artikeltext der KI-Verordnung, die Erwägungsgründe und – soweit vorhanden – Leitlinien der EU-Kommission. Externe Literatur oder Kommentare wurden bewusst ausgeschlossen, um eine eigenständige und quellentreue Auslegung sicherzustellen. Zentraler Bezugspunkt war der Artikeltext, mit dem Ziel diesen eigenständig von der KI auslegen zu lassen.
- Methodik der Auslegung: zunächst Wortlaut, dann systematische Einordnung im Gesamtzusammenhang, bei Bedarf teleologische Auslegung (Sinn & Zweck der KI-Verordnung).
- Verwendetes Modell: ChatGPT-5 (Stand August 2025).

3. Struktur der Kommentare

Jeder Artikel wurde nach einem einheitlichen Schema kommentiert:

- Artikelnummer & Volltext
- I. Worum geht es? – kurze Kernaussage des Artikels

- II. Detailkommentar – differenzierte Erläuterung mit Untergliederung
- III. Zusammenfassung – komprimierte Übersicht
- IV. Quellenverzeichnis – Nennung der verwendeten Erwägungsgründe/Leitlinien

4. Review-Prozess

Alle automatisch erzeugten Kommentierungen wurden durch Jurist:innen auf Plausibilität und Richtigkeit überprüft.

- Ergebnis: Rund 95 % der Texte waren direkt verwendbar.
- Änderungen: Bei Korrekturbedarf, wurde der jeweilige Abschnitt neu gepromptet. Eine manuelle Änderung hat nicht stattgefunden.
- Dadurch blieb die inhaltliche Linie konsistent und die Überarbeitungen minimal.

5. Technische Umsetzung

Für die einheitliche Formatierung in wurde ein Makros-Skript (MS WORD) entwickelt, das automatisch die korrekten Überschriften, Listen, Tabellen und Formatierungen einfügt. Dadurch konnte der Formatierungsaufwand stark reduziert und die Einheitlichkeit über alle Artikel hinweg gewährleistet werden.

6. Ergebnis

Das Ergebnis ist eine vollständige, klar strukturierte und erläuterte Darstellung der KI-VO, die sowohl juristisch präzise als auch für Laien und nichtspezialisierte Jurist:innen verständlich ist. Die Vorgehensweise kombiniert KI-gestützte Texterstellung, juristische Fachprüfung und automatisierte Formatierung, was eine effiziente und qualitativ hochwertige Erstellung ermöglicht hat.