European AI ACT (KI-Verordnung)

Thema	Inhalt	Artikel
Gesetzgeber	EU-Kommission	
Offizielle Bezeichung	**VERORDNUNG (EU) 2024/1689 (EU AI Act)**	
Quelle	https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401689	
Kurzbeschreibung	Der AI Act (Artificial Intelligence Act) ist der erste umfassende Rechtsrahmen der Europäischen Union zur Regulierung von künstlicher Intelligenz. Ziel ist es, sichere, transparente und vertrauenswürdige KI-Systeme zu fördern und gleichzeitig Risiken für Grundrechte und Sicherheit zu minimieren. In den 27 Mitgliedstaaten der EU soll Rechtssicherheit bei der Entwicklung und Nutzung von KI geschaffen werden, indem zentrale Anforderungen für die Entwicklung und den Einsatz von KI-Systemen festgelegt werden. In der EU verwendete KI-Systeme sollen dadurch sicher, transparent, ethisch vertretbar und unvoreingenommen (no bias / no misleading information) entwickelt und genutzt werden.	
Inkrafttreten auf EU-Ebene	01.08.24	
Nationale Gültigkeit ab	01.08.2024 **Anmerkung:** Beim AI Act handelt es sich um eine Verordung, daher ist kein nationales Umsetzungsgesetz notwendig, wie es bei einer Richtlinie (Directive) der Fall wäre. Der AI Act ist direkt gültig und für alle EU-Mitgliedsstaaten anzuwenden. Die Anwendung des AI Act kann dennoch die Erlassung weiterer Gesetze oder Gesetzesanpassungen auf nationaler Ebene erforderlich machen, beispielsweise um Anforderungen klarer oder granularer für betroffene Anwendungsbereiche zu regeln. Stand Ende Januar 2025 dauern die Abstimmungen zum nationalen Durchführungsgesetz in Deutschland noch an.	
Anwendungsbereich / betroffene Interessengruppen	1. Anbieter von KI-Systemen (Art. 3, Nr. 3) sowie deren Bevollmächtigte (Art. 3, Nr. 5) 2. Betreiber von KI-Systemen (Art. 3, Nr. 4) 3. Einführer (Art. 3, Nr. 6) 4. Händler (Art. 3, Nr. 7) 5. Produkthersteller (Art. 2, Abs. 1e) 6. Nachgelagerte Anbieter (Art.3, Nr. 68) 7. Nationale Aufsichtsbehörden 8. Komission / EU-Aufsichtbehörden 9. Betroffene Personen (Art. 2, Abs. 1g)	Anwendungsbereich (Art. 2) Begriffsbestimmungen (Art. 3)
Zentrale Inhalte / Anforderungen	**I) Risikobasierter Ansatz:** KI-Systeme müssen anhand ihres inhärenten Risikos bewertet und in vier Risikoklassen klassifiziert werden (inakzeptables Risiko, hohes Risiko, begrenztes Risiko und minimales Risiko). Je höher das inhärente Risiko eines KI-Systems, desto strenger sind die Vorgaben. KI-Praktiken mit inakzeptablem Risiko sind in der Union verboten (Art. 5). Für Systeme mit hohem Risiko (Hochrisiko-KI-Systeme) gelten die strengsten Pflichten und Anforderungen. Darüber hinaus legt der AI Act spezifische Pflichten für verschiedene Akteure entlang der KI-Wertschöpfungskette fest. <u>Die Anforderungen lassen sich in folgende Kategorien unterteilen:</u> - Anforderungen an Kompetenz und Aufsicht - Anforderungen an das Risikomanagement - Anforderungen an Qualität, Resilienz und Cybersicherheit - Anforderungen an Dokumentation, Transparenz und Überwachung - Inormations- und Meldepflichten - Bewertungsverfahren und Einstufungsvorschriften - Daten und Datenqualität **II) Spezielle Anforderungen gemäß Risikoklasse:** Hochrisiko-KI-Systeme gemäß Art. 6 und Anhang III müssen eine Reihe von Anforderungen erfüllen, um für den EU-Markt zugelassen zu werden. Hierzu zählen Anforderungen an das Risiko- und Qualitätsmanagement, die Datenqualität, Transparenz und Erklärbarkeit, Dokumentation sowie Resilienz. Darüber hinaus gelten für verschiedene Akteure entlang der KI-Wertschöpfungskette spezifische Pflichten, wie etwa eine Grundrechte-Folgenabschätzung für Betreiber von Hochrisiko-KI-Systemen. Für KI-Modelle mit allgemeinem Verwendungszweck, z. B. die GPT-Modelle von OpenAI, (Art.51) gelten lediglich Transparenz- und Informationspflichten (z. B. Meldung schwerwiegender Fälle) **III) Regulierung und Durchsetzung:** Die Verordnung sieht die Einrichtung nationaler Aufsichtsbehörden vor, die die Einhaltung der Vorschriften überwachen und Verstöße ahnden sollen. Zudem wird ein europäisches KI-Gremium geschaffen, das die Koordination zwischen den Mitgliedstaaten erleichtern soll, sowie ein Büro für künstliche Intelligenz, über das die Kommission die Sachkenntnis und Fähigkeiten der Union auf dem Gebiet der KI entwickelt. Auf nationaler Ebene wird eine zuständige Marktüberwachungsbehörde per Durchführungsgesetz benannt. Zum Stand 31.01.2025 ist diese noch nicht bekannt. In Ausschüssen wurde die Bundesnetzagentur diskutiert.	Präambel (7)-(10) Einstufung (Art.6, Art. 51, Art.52, Anhang III) Risikomanagementsystem (Art.9) Daten und Datenverwaltung (Art.10) Technische Dokumentation (Art.11, Anhang I, Anhnang IV) Aufzeichnungspflichten (Art.12) Informationspflichten (Art.13) Menschliche Aufsicht (Art. 14) Genauigeit, Robustheit und Cybersicherheit (Art.15) Grundrechte-Folgenabschätzung (Art.27) Transparenzpflichten (Art.50)
Hinweise für Finanzinstitute	Die zuständigen Behörden für die Beaufsichtigung und Durchsetzung von Rechtsvorschriften im Finanzsektor sollen auch für die Überwachung der KI-Systeme in diesem Bereich verantwortlich sein. Diese Behörden erhalten umfassende Befugnisse zur Durchsetzung der Verordnung, einschließlich Marktüberwachungsaktivitäten, die in bestehende Aufsichtsmechanismen integriert werden können. Um Kohärenz und Gleichbehandlung im Finanzsektor zu gewährleisten, werden einige Anbieterpflichten in bestehende Verfahren integriert und begrenzte Ausnahmen für bestimmte Finanzinstitute in Betracht gezogen. **Hochrisiko-Systeme in der Finanzbranche** KI-Systeme, die in der Kreditwürdgkeitsprüfng und Bonitätsbewertung zum Einsatz kommen, klassifiziert der AI Act als Hochrsiko-Systeme. Im Bereich der Versicherungen sind Systeme zur Risikobewertung und Preisbildung von Lebens- und krankenversicherungen als Hochrisiko-Systeme klassifiziert. Für Finanzdientleister ergeben sich dementsprechend strenge Anforderungen und Pflichten, deren Nichteinhaltung wesentliche reputationelle und finanzielle Risiken nach sich ziehen kann.	Präambel (158) Anhang III
Anwendungsfristen und Termine	**Anwendungsfristen** **2. Februar 2025:** - Inkrafttreten der allgemeinen Bestimmungen sowie Art. 4 (KI-Kompetenz) und Art. 5 (Verbotene KI-Praktiken) **2. August 2025:** - Inkrafttreten der Bestimmungen über notifizierte Stellen und die Leitungsstruktur - Inkrafttreten der Pflichten für KI-Modelle mit allgemeinem Verwendungszweck - Inkrafttreten der Bestimmungen über Sanktionen **2. August 2026:** - Vollständiges Inkrafttreten der Verordnung - Einsatzbereitschaft der Infrastruktur für die Leitung und das Konformitätsbewertungssystem - Mitgliedsstaaten tragen dafür Sorge, dass mindestens ein KI-Reallabor eingerichtet und einsatzbereit ist **2. August 2027:** - Inkrafttreten von Einstufungsvorschriften für Hochrisiko-KI-Systeme gemäß Art. 6 Abs. 1 - Inkrafttreten von Anforderungen für KI-Modelle mit allgemeinem Verwendungszweck, die vor dem 2. August 2025 in Verkehr gebracht wurden **Termine** **2. November 2024:** - Mitgliedsstaaten müsssen Behörden/öffentlichen Stellen benennen, in einer öffentlichen Liste verfügbar machen und der Komission übermitteln **2. Mai 2025:** - Vorlage der Verhaltenskodizes für die freiwillige Anwendung bestimmter Anforderungen - Veröffentlichung von Praxisleitfäden zur ordnungsgemäßen Anwendung der Verordnung unter Berücksichtigung internationaler Ansätze **2. August 2025** - Benennung von nationalen Aufsichtsbehörden, die die Durchführung der Verordnung auf nationaler Ebene überwachen - Veröffentlichung von Leitlinien zur Meldung schwerwiegender Vorfälle **2. Februar 2026:** - Veröffentlichung von Leitlinien zur praktischen Umsetzung und Durchführung der Verordnung **Zusätzlich sollten die Mitgliedstaaten vor dem 2. August 2026:** - Vorschriften über Sanktionen festlegen und der Kommission mitteilen - Sicherstellen, dass diese Sanktionen ordnungsgemäß und wirksam umgesetzt werden	Präambel (179) Anbieterpflichten (Art. 53ff) Praxisleitfäden (Art. 56) Nationale Behörden (Art. 70, Art.77) Meldung Vorfälle (Art. 73) Verhaltenskodizes (Art. 95) Leitlinien (Art. 96) Bereits in Umlauf gebrachte Systeme mit allgemeinem Verwedungszweck (Art. 111) Inkrafttreten und Geltungsbeginn (Art. 113)
Sicherstellung geeigneter Kompetenzen	Unter KI-Kompetenz versteht der Gesetzgeber die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen ermöglichen, unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten dieser Verordnung, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden. 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.	KI-Kompetenz (Art.4)
Normen	**Normungsaufträge** Die Komission vergibt Normungsaufträge gemäß Verordnung Nr. 1025/2012 (Artikel 10) zur Erstellung harmonisierter Normen durch Normungsorganisationen. **Aktuelle Normen:** ISO/IEC 42001:2023 **Normungsorganisationen:** Deuschland: DIN, DKE; Europa: CEN, CENELEC, ETSI; International: ISO, IEC, IEEE, ITU	Harmonisierte Normen (Art.40)
Sanktionen	1) Bei Missachtung des Verbots der in Artikel 5 genannten KI-Praktiken werden Geldbußen von **bis zu 35 000 000 €** oder — im Falle von Unternehmen — von **bis zu 7 % des gesamten weltweiten Jahresumsatzes** des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist. 2) Für Verstöße gegen Akteure oder notifizierte Stellen geltende Bestimmungen (mit Ausnahme der in Artikel 5 genannten) werden Geldbußen von **bis zu 15 000 000 €** oder — im Falle von Unternehmen — von **bis zu 3 % des gesamten weltweiten Jahresumsatzes** des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist. 3) 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 €** oder — im Falle von Unternehmen — von **bis zu 1 % des gesamten weltweiten Jahresumsatzes** des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher Betrag höher ist. **Geldbußen für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (Art. 101)** 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 € verhängen, je nachdem, welcher Betrag höher ist. **HINWEIS:** Im Falle von KMU, einschließlich Start-up-Unternehmen, gilt für jede in diesem Artikel genannte Geldbuße der jeweils niedrigere Betrag aus den in 1)-3) genannten Prozentsätzen oder Summen.	Sanktionen (Art. 99, Art.100, Art. 101)

European AI ACT (KI-Verordnung)

Thema	Inhalt	Artikel
Querbezüge zu DORA	**Risikomanagement** AI Act: - Klassifizierung von KI-Systemen in vier Risikoklassen sowie Implementierung eines Risikomanagement-Frameworks für Hochrisiko-KI-Systeme DORA: - Aufbau eines IKT-Risikomanagement-Frameworks, insb. IKT-Assetmanagement **IT- und Cybersicherheit** AI Act: - Anforderungen an Robustheit, Genauigkeit und Cybersicherheit zum Schutz vor Angriffen und Manipulationen, insb. für Hochrisiko-KI-Systeme DORA: - Anforderungen an die Überwachung und Kontrolle von IKT-Assets, insb. kritische oder wichtige Funktionen **Drittanbieter und Lieferketten** AI Act: - Verteilung klarer Verantwortlichkeiten entlang der KI-Wertschöpfungskette (Anbieter, Betreiber, Händler, etc.) DORA: - Anforderungen an das Management von (kritischen) IKT-Drittanbietern **Dokumentationspflichten, Meldepflichten und Transparenzanforderungen** AI Act: - Anforderungen an technische Dokumentationen und Aufzeichnungspflichten (Protokolle) - Meldung von Fehlfunktionen, Risiken und Änderungen an bestehenden KI-Modellen oder -Systemen sowie Meldung von schwerwiegenden Vorfällen an die Behörden - Transparenzanforderungen bzgl. verwendeter Daten sowie Einsatz von KI-Systemen gegenüber Nutzern und der Aufsicht - Aufbau EU-Datenbank über eingesetzte Hochrisiko-KI-Systeme DORA: - Pflicht zur Dokumentation von IKT-Risiken und schwerwiegenden IKT-bezogenen Vorfällen - Pflicht zur Meldung von IKT-Vorfällen und Informationen über IKT-Drittdienstleister an die Behörden - Transparenzanforderungen bzgl. IKT-Drittanbietern sowie IKT-Vorfällen gegenüber der Aufsicht - Aufbau eines Informationsregisters über IKT-Drittdienstleistungen	
Querbezüge zu DSGVO	**Transparenz** AI Act: - Information an die Nutzer über KI-Interaktionen DSGVO: - Informationen über Datenverarbeitung (Art. 13-14 DSGVO) **Dokumentationspflicht** AI Act: - Risiko- und Konformitätsbewertungen sowie -erklärungen für Hochrisikosysteme DSGVO: - Verzeichnis von Verarbeitungstätigkeiten - Risikobewertung, wenn die Verarbeitung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt **Risikobasierter Ansatz** AI Act: - Klassifizierung nach vier Risikostufen (unannehmbar, hoch, begrenzt, minimal) DSGVO: - Unterscheidung der personenbezogenen Daten nach Datenkategorien (personenbezogene und besondere personenbezogene Daten) **Technische und organisatorische Maßnahmen ("TOMs")** AI Act: - TOMs für Hochrisikosysteme DSGVO: - Einrichtung von TOMs, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten **Datenbezogene Prinzipien** AI Act: - (Indirekte) Zweckbindung über verschiedene Artikel (Art. 5 verbotene KI-Praktiken, Art. 8 Anforderungen an Hochrisiko-KI-Systeme, Art. 53 Pflichten für Anbieter allgemeiner KI-Modelle) DSGVO: - Daten dürfen nur für vorab definierte Zwecke genutzt werden	
Assoziierte Verordnungen	Verordnung (EU) 2023/2854 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung Verordnung (EU) 2023/988 über die allgemeine Produktsicherheit Verordnung (EU) 2022/2065 über einen Binnenmarkt für digitale Dienste Verordnung (EU) 2022/868 über europäische Daten-Governance Verordnung (EU) 2019/881 über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik Verordnung (EU) 2019/1020 über Marktüberwachung und die Konformität von Produkten Verordnung (EU) 2018/1725 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten Verordnung (EU) 2013/526 für Netz- und Informationssicherheit (ENISA) Verordnung (EU) 2013/1024 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank Verordnung (EU) 2013/575 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen Verordnung (EU) 2012/1025 zur europäischen Normung Verordnung (EU) 2011/182 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren Verordnung (EG) Nr. 765/2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten (CE-Kennzeichnung) Richtline 2001/95/EG über die allgemeine Produktsicherheit -> Anforderungen für KI-Systeme, die in Produkten verwendet werden, z.B. Flugzeuge, Autos, medizinische Produkte, Sielsachen, etc.	