

Die rechtlich-abgesicherte Arbeit mit KI in der Kita ab dem 02. August 2026!

Ein präziser Leitfaden für Kita-Träger und pädagogisches Personal zur rechtskonformen Umsetzung der EU-KI-Verordnung (AI Act)

RISIKOKLASSIFIZIERUNG & VERBOTE IM KITA-ALLTAG



VERBOTEN

Verbotene KI-Praktiken (Art. 5)

- Emotionserkennung, biometrische Identifizierung und manipulative Systeme sind in Bildungsstätten seit Februar 2025 strikt untersagt.



Hochrisiko-Systeme im Fokus

- Systeme zur Bewertung von Lernergebnissen oder Platzvergabe gelten als hochriskant und erfordern striktes Risikomanagement.

02.08.2026



Transparenzpflicht ab 02.08.2026

- KI-generierte Inhalte (Texte, Bilder, Deepfakes) müssen ab diesem Datum zwingend als solche gekennzeichnet werden.



REGULATORISCHE MEILENSTEINE

02. FEB. 2025

Verbote & KI-Kompetenz

Verbot von Emotionserkennung;
Schulungspflicht für alle
Mitarbeitenden aktiv.



02. AUG. 2026

Transparenzpflichten

Kennzeichnungspflicht für
KI-Inhalte (Texte/Bilder) und
Chatbot-Offenlegung.



02. DEZ. 2027

Hochrisiko-Anforderungen

Volle Compliance-Pflicht für
digitale Bewertungs- und
Analyseplattformen

OPERATIVE UMSETZUNG & COMPLIANCE-CHECKLISTE



Pflicht zum Aufbau von KI-Kompetenz (Art. 4)

Träger müssen nachweislich sicherstellen,
dass alle Mitarbeitenden Chancen, Risiken
und Grenzen von KI verstehen.



Datenschutz als zentrale Leitplanke

Keine Eingabe personenbezogener Daten
(Namen, Fotos, Entwicklungsberichte) in
öffentliche KI-Tools ohne AV-Vertrag.



Human-in-the-Loop Prinzip

KI darf nur unterstützen; pädagogische
Entscheidungen und Diagnostik müssen
immer durch eine Fachkraft erfolgen.

Rechtssichere KI in der Kita: Der Fahrplan bis August 2026

Die **EU-KI-Verordnung (AI Act)** reguliert den Einsatz künstlicher Intelligenz basierend auf einem risikobasierten Ansatz. Während Verbote bereits seit Februar 2025 gelten, rückt am 02. August 2026 die verbindliche Transparenzpflicht in den Fokus, bevor 2027 strenge Regeln für Hochrisiko-Systeme folgen.

Zeitplan & Risikoklassen: Was gilt wann?



Risikoklassifizierung für den Kita-Alltag

Unannehmbar (Streng Verboten)	Hochrisiko (Erlaubt ab 2027, Zertifizierungspflicht)	Begrenzt (Erlaubt mit Transparenzhinweis)
Beispiele: - Emotionserkennung bei Kindern - Social Scoring	Beispiele: KI-Sprachstandsanalyse zur Förderzuweisung	Beispiele: - ChatGPT für Elternbriefe - Bildgeneratoren

Der 3-Phasen-Plan zur Compliance



Die rechtlich-abgesicherte Arbeit mit KI in der Kita

ab dem 02. August 2026

1. Strategische Einordnung:

Der Stichtag 02. August 2026 im Kontext der KI-Governance

Der 02. August 2026 markiert für Kindertageseinrichtungen den verbindlichen Übergang von einer Phase der explorativen Erprobung hin zu einem strikten regulatorischen Aufsichtsregime. Während erste Verbote bereits seit Februar 2025 gelten, tritt mit diesem Datum die volle operative Überwachung durch die nationalen Behörden in Kraft.

In Deutschland fungiert die Bundesnetzagentur (BNetzA) als zentrale Anlaufstelle, während das Bundesamt für Sicherheit in der Informationstechnik (BSI) wesentliche Durchsetzungs- und Prüfungsaufgaben übernimmt.

Für Kita-Träger bedeutet dies, dass informelle „Schatten-KI“ nicht länger geduldet werden kann; jedes System muss bis zu diesem Stichtag einer formalen Prüfung unterzogen worden sein, um den Anforderungen der Marktüberwachung standzuhalten.

Die folgende Übersicht konkretisiert die Meilensteine basierend auf dem EU AI Act und dem Digital Omnibus (Mai 2026):

Stichtag	Meilenstein Regulatorische Anforderung	/Strategischer Fokus für Kitas
02. Februar 2025	Inkrafttreten Art. 4 & 5 (EU AI Act)	Verbot inakzeptabler Praktiken (z. B. Emotionserkennung); Beginn der Unterstützungspflicht für KI-Kompetenz.
02. August 2025	GPAI-Regulierung (Art. 51 ff.)	Spezielle Regeln für General Purpose AI (z. B. ChatGPT); Einführung von Governance-Strukturen für Basismodelle.

02. August 2026	Transparenzpflichten (Art. 50)	Verbindliche Kennzeichnungspflicht für Chatbots und KI-Inhalte; Start der aktiven Aufsicht durch BNetzA und BSI.
02. Dezember 2027	Hochrisiko-Systeme (Anhang III)	Volle Compliance-Pflicht für Systeme zur Leistungsbewertung und Personalvorauswahl (durch Digital Omnibus verschoben).
02. August 2028	Hochrisiko-Systeme (Anhang I)	Compliance für KI als Sicherheitskomponente in Produkten (z. B. vernetztes Spielzeug).

Diese chronologische Planung ist jedoch nur das formale Gerüst; entscheidend für die Rechtssicherheit ist die inhaltliche Risikobewertung der eingesetzten Systeme.

2. Die Risikoklassifizierung in der Kita-Praxis: Zwischen Verbot und Hochrisiko

Der EU AI Act folgt einem risikobasierten Ansatz, bei dem die regulatorische Last direkt mit dem Gefahrenpotenzial korreliert. Eine fehlerhafte Einordnung der Tools kann für Träger existenzbedrohend sein:

Verstöße gegen verbotene Praktiken werden mit Bußgeldern von bis zu 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes sanktioniert.

Die Anwendungen im Kita-Alltag sind wie folgt zu kategorisieren:

- **Verbotene Praktiken (Art. 5):**

Seit Februar 2025 ist die Emotionserkennung in Bildungseinrichtungen und am Arbeitsplatz strikt untersagt. Systeme, die darauf abzielen, Gefühlszustände von Kindern oder Personal zu analysieren (z. B. zur Disziplinierung), sind verboten. Durch den Digital Omnibus 2026 wurde zudem das Verbot von KI-Anwendungen zur Erstellung nicht-einvernehmlicher intimer Inhalte (Deepfakes/KI-Pornografie) verschärft. Ein kritischer Aspekt für den Kinderschutz.

- **Hochrisiko-Systeme (Anhang III):**

Hierunter fallen KI-Systeme zur Personalvorauswahl (Recruiting) oder zur Leistungsbewertung von Fachkräften. Diese unterliegen strengen Dokumentationspflichten und menschlicher Aufsicht. Obwohl die Durchsetzung durch den Digital Omnibus auf Dezember 2027 verschoben wurde, müssen die technischen Weichenstellungen jetzt erfolgen.

- **Begrenztes Risiko (Art. 50):**

Gängige Chatbots (z. B. zur Elternkommunikation) erfordern ab August 2026 absolute Transparenz. Nutzer müssen unmissverständlich wissen, dass sie mit einer KI interagieren. KI-generierte Texte oder Bilder müssen manipulationssicher gekennzeichnet werden.

Die korrekte Klassifizierung ist die Basis für die operative Sicherheit, erfordert jedoch zwingend eine entsprechende Qualifizierung des Personals.

3. Die KI-Kompetenzpflicht nach Art. 4: Qualifizierungszwang für pädagogische Fachkräfte

KI-Kompetenz („AI Literacy“) ist keine optionale Fortbildung, sondern seit Februar 2025 eine strategische Notwendigkeit. Zwar hat der Digital Omnibus die Pflicht dahingehend modifiziert, dass Betreiber (Deployer) Literacy-Bemühungen lediglich „unterstützen“ müssen, statt das Ergebnis zu „garantieren“.

Aus Sicht der Haftungsprävention bleibt meine Empfehlung jedoch klar:

Nur eine nachweisbare Qualifizierung schützt die Geschäftsführung vor dem Vorwurf der Organisations- und Aufsichtspflichtverletzung.

Das Anforderungsprofil für „KI-Kompetenz in der Kita“ folgt dem AI Literacy Framework:

1. **Umgang mit KI:**

Erkennen von KI-Anwendungen und kritische Einordnung technischer Grenzen (Halluzinationen).

2. **Gestalten mit KI:**

Kompetente Steuerung von Systemen durch Prompt-Engineering unter Wahrung von Fairness und Urheberrecht.

3. **Verwalten von KI:**

Bewusste Entscheidung, welche Aufgaben delegiert werden und wo die pädagogische Letztentscheidung liegen muss.

4. **Entwickeln von KI:**

Grundverständnis der Funktionsweise, um soziale und ethische Auswirkungen (Bias) bewerten zu können.

KI-Kompetenz bildet somit die notwendige Bedingung für den rechtssicheren Umgang mit sensiblen Daten.

4. Datenschutz und DSGVO: Schutzschild für die „Perspektive Kind“

Die besondere Schutzwürdigkeit von Kinderdaten gemäß DSGVO trifft auf die oft intransparente Architektur globaler KI-Modelle. Im Sinne der Hamburger Bildungsleitlinien („Perspektive Kind“) muss das Kindeswohl auch im digitalen Raum das Primat bilden.

Um den Grundrechtsschutz zu gewährleisten, gilt für öffentliche KIs folgende „Negative-Liste“:

- Eingabe von Klarnamen oder Geburtsdaten ist strikt untersagt.
- Eingabe sensibler Entwicklungsberichte oder Beobachtungsnotizen in öffentliche Modelle ist verboten.
- Upload von Fotos oder Videos ohne KI-spezifische Einwilligung ist unzulässig.

Als rechtssichere Alternative müssen spezialisierte, DSGVO-konforme Lösungen wie z. B. KITALINO genutzt werden. Diese bieten durch den Standortvorteil „Hosting in Germany“ und die strikte Einhaltung europäischer Standards maximale Sicherheit. Entscheidende technische Merkmale sind hierbei die **Zwei-Faktor-Authentifizierung** und eine TLS-Verschlüsselung nach Bankenstandard, die den Schutz vor unbefugtem Zugriff garantieren. Diese Datenschutzparameter fließen unmittelbar in die Grundrechte-Folgenabschätzung ein.

5. Die Grundrechte-Folgenabschätzung (FRIA) nach Art. 27

Die FRIA (Fundamental Rights Impact Assessment) ist ein präventives Compliance-Instrument für Hochrisiko-Systeme. Verpflichtet sind Einrichtungen des öffentlichen Rechts sowie private Anbieter, die öffentliche Dienste (wie Erziehung und Bildung) erbringen.

Schritt-für-Schritt-Anleitung zur Umsetzung der FRIA:

1. **Verfahrensbeschreibung:** Zweckbestimmung und Einbindung in den Kita-Alltag.
2. **Zeitraum:** Dokumentation der Nutzungsdauer und -häufigkeit.
3. **Betroffene Personen:** Identifikation vulnerabler Gruppen (insbesondere Kinder).
4. **Schadensrisiken:** Analyse potenzieller Diskriminierung oder Beeinträchtigung der Privatsphäre.
5. **Menschliche Aufsicht:** Festlegung der Kontrollinstanzen entsprechend der Betriebsanleitungen.
6. **Minimierungsmaßnahmen:**

Implementierung von Schutzvorkehrungen und internen Richtlinien.

Das neu geschaffene Büro für Künstliche Intelligenz (AI Office) wird hierfür einen standardisierten Fragebogen/Muster bereitstellen, was den Prozess für Kita-Leitungen erheblich vereinfacht. Die Ergebnisse sind der Marktüberwachungsbehörde zu melden.

6. Operative Roadmap: Implementierungsschritte bis zum 02. August 2026

Die Kita-Leitung agiert als strategischer „Betreiber“ (Deployer).

Proaktives Handeln vor dem Stichtag im August 2026 ist die einzige Versicherung gegen Bußgelder.

5-Punkte-Aktionsplan:

1. **KI-Inventar:**

Erfassung aller genutzten Tools (inkl. Übersetzungs-Apps und Bildgeneratoren).

2. **Risiko-Audit:**

Dokumentierte Einstufung jedes Systems gemäß Art. 5, Anhang III oder Art. 50.

3. **Governance-Struktur:**

Erstellung verbindlicher Richtlinien und Etablierung eines Beschwerdemechanismus nach Art. 27.

4. **Schulungs-Rollout:**

Durchführung und Dokumentation zertifizierter Team-Schulungen (LMS-gestützt).

5. **Monitoring-Prozess:** Kontinuierliche Überprüfung der KI-Outputs auf Bias und sachliche Korrektheit.

Diese strukturierte Einführung wandelt regulatorischen Druck in operative Exzellenz um.

7. Fazit und Handlungsempfehlung

Künstliche Intelligenz bietet enorme Potenziale zur Entlastung von Administration und Dokumentation. Dennoch gilt: KI ist ein Werkzeug, kein Ersatz für pädagogische Expertise und die menschliche Bindung zum Kind. Rechtssicherheit ab August 2026 erfordert jetzt strategisches Investment.

Kern-Appelle an die Kita-Leitungen:

- **Identifizieren Sie bis August 2026 Ihr gesamtes KI-Inventar und stellen Sie sicher, dass keine verbotenen Praktiken oder unmarkierten Chatbots im Einsatz sind.**
- **Garantieren Sie die KI-Kompetenz Ihres Teams durch nachweisbare Qualifizierungen, um persönliche Haftungsrisiken der Geschäftsführung zu minimieren.**
- **Nutzen Sie für sensible pädagogische Daten ausschließlich spezialisierte Lösungen mit Zwei-Faktor-Authentifizierung und europäischem Hosting.**
- **Da Kitas unter föderale Landesgesetze und ggf. konfessionelle Datenschutzvorschriften (z. B. das kirchliche Gesetz über den Datenschutz, KDG) fallen, sollten Sie im Einleitungssatz der Richtlinie die konkrete Rechtsgrundlage Ihrer Einrichtung (z. B. das Landes-Kita-Gesetz) ergänzen.**
- **Koordinieren Sie diese Schritte eng mit Ihrem Träger und nutzen Sie spezialisierte Fachberatung, um die KI-Transformation rechtssicher und zum Wohl der Kinder zu gestalten.**

Für KI-Schulungen und weitere Fragen stehe ich Ihnen zur Verfügung:

Matthias Reithmann

matthias.reithmann@querhandeln.de oder info@neurokita.de

<https://www.querhandeln.de> oder <https://neurokita.de>

Mobil und WhatsApp: 0176 / 83 13 17 62

P.S.: Dieser Bericht wurde mit Unterstützung von <https://notebooklm.google.com> erstellt.

Checkliste 1: Fristen- und Umsetzungsfahrplan (Aktualisiert durch KI-Omnibus)

Diese Tabelle fasst die verbindlichen Stichtage für Kitas als Betreiber (Deployer) zusammen, angepasst an die neuesten Fristverlängerungen.

Stichtag / Frist	Regulatorischer Meilenstein für die Kita	Konkrete Aufgaben für Träger & Leitung (Check)
02. Februar 2025	Geltung der Verbote & KI-Kompetenzpflicht	Strikter Stopp aller KI-Systeme zur Emotionserkennung oder sozialen Bewertung. Start der gesetzlichen Schulungspflicht (Aufbau von KI-Kompetenz) für das gesamte pädagogische Personal.
02. August 2026	Transparenzpflichten bei geringem/begrenztem Risiko	KI-generierte Bilder, Texte (z. B. Elternbriefe) oder Chatbot-Interaktionen müssen ab jetzt klar als maschinell erstellt gekennzeichnet werden.
02. Dezember 2026	Übergangsfrist für Altsysteme (Digital Omnibus)	Sicherstellen, dass auch ältere, bereits genutzte KI-Systeme nun die Transparenz- und Kennzeichnungspflichten vollständig erfüllen.
02. Dezember 2027	Hochrisiko-Systeme (Bildung, Anhang III) – Frist verschoben	Volle Compliance bei Software zur automatisierten Bewertung oder Diagnostik von Kindern. Träger muss Registrierungen, Risikomanagement und EU-Konformitätserklärungen des Anbieters prüfen.

Checkliste 2: Akteurs-Matrix (Rechte & Pflichten im Kita-Alltag)

Die rechtliche Verantwortung ist streng nach Rollen verteilt. Diese Matrix dient der klaren Aufgabenabgrenzung.

Akteursgruppe	Kernrechte (Gesetzlicher Anspruch)	Operative & Ethische Pflichten (To-Dos)
Träger (Deployer)	Einholung technischer Konformitätsnachweise von Software-Anbietern.	IT-Sicherheit & DSGVO-/KDG-konforme Infrastruktur stellen. Regelmäßige KI-Kompetenz-Schulungen organisieren (Art. 4).
Kita-Leitung	Fachliche Beratung durch staatliche / kirchliche Aufsichtsbehörden einholen.	Einhaltung der verbotenen Praktiken (z.B. keine Emotionserkennung) überwachen. Interne Notfall- und Freigabeprozesse etablieren.
Päd. Fachkräfte	Recht auf Nutzung geprüfter, sicherer Dienstgeräte und angemessene Fortbildungszeit.	Human-in-the-Loop: Die pädagogische Endentscheidung immer beim Menschen belassen. Strikte Datensparsamkeit; keine echten Kindernamen in KI eingeben.
Eltern / Familie	Recht auf Aufklärung und Anfechtung von algorithmischen Urteilen.	Schriftliche Einwilligung zur Datenverarbeitung (bei Kindern unter 16) erteilen oder verweigern.
Kinder	Schutz vor kognitiver Verhaltensmanipulation und informationelle Selbstbestimmung.	<i>Kinder sind Träger von Schutzrechten; die Pflicht zur Umsetzung liegt vollständig bei den Erwachsenen.</i>

Checkliste 3: Der operative 4-Phasen-Zyklus für den KI-Einsatz

Der Einsatz von KI in der Kita muss einem strukturierten Qualitätsmanagement folgen.

Phase	Maßnahmen / Aufgaben im Kita-Alltag	Erledigt?
1. Vorbereitung	Bestandsaufnahme: Erstellung eines lückenlosen KI-Inventars aller genutzten Tools. Risikoanalyse: Gegebenenfalls Datenschutz-Folgenabschätzung (DSFA) bei sensiblen Tools durchführen. Freigabe: Einholen von Elterneinwilligungen und Durchführung der Kompetenzschulungen (Art. 4).	[]
2. Durchführung	Anonymisierung: Strikte Vermeidung personenbezogener Daten in Prompts (z.B. „Kind A“ statt echtem Namen). Prüfung: Plausibilitätsprüfung aller KI-Texte und Ergebnisse durch die Fachkraft. Transparenz: Klarer Hinweis auf KI-Nutzung setzen (z. B. unter Elternbriefen).	[]
3. Nachbereitung	Datensäuberung: Datenschutzkonforme Löschung aller temporären Chat-Verläufe und Daten auf den Endgeräten. Dokumentation: Erbrachte Schulungsnachweise in das zentrale Träger-Verzeichnis eintragen.	[]
4. Evaluation	Monitoring: Regelmäßige Teambesprechung zu Fehlerquoten, „Halluzinationen“ und pädagogischem Mehrwert. Anpassung: Überarbeitung des internen KI-Leitfadens basierend auf neuen Praxiserfahrungen.	[]

Checkliste 4: Der schnelle 5-Fragen-Compliance-Check für neue Software

Bevor eine Kita-Leitung oder pädagogische Fachkraft ein neues digitales Tool (wie Portfolio-Generatoren oder Übersetzer) einsetzt, müssen diese 5 Fragen mit **"Ja"** beantwortet werden.

Prüfkriterium (Compliance)	Leitfrage für die Kita-Leitung	Status
1. Datensparsamkeit	Kann die KI-Anwendung sinnvoll betrieben werden, ohne dass echte Namen, Fotos oder sensible Entwicklungsdetails von Kindern eingegeben werden müssen?	☐ Ja / ☐ Nein
2. Serverstandort	Werden die eingegebenen Daten ausschließlich auf Servern innerhalb der Europäischen Union (EU) verarbeitet?	☐ Ja / ☐ Nein
3. Rechtssicherheit	Liegt ein gültiger Auftragsverarbeitungsvertrag (AVV) gemäß DSGVO oder dem kirchlichen Datenschutz (KDG) vor?	☐ Ja / ☐ Nein
4. Dateneigentum	Sichert der Anbieter vertraglich zu, dass unsere Kita-Daten nicht zum zukünftigen Training des KI-Modells verwendet werden?	☐ Ja / ☐ Nein
5. Risikoausschluss	Ist sichergestellt, dass das System keine automatisierten Entscheidungen über Kinder fällt und keine Emotionen/Verhalten biometrisch analysiert?	☐ Ja / ☐ Nein

*(Hinweis: Sobald eine Frage mit **"Nein"** beantwortet wird, darf das Tool für pädagogische Kernaufgaben und sensible Daten **nicht genutzt werden**, bis der Träger bzw. Datenschutzbeauftragte eine Einzelfallprüfung vorgenommen hat.)*

Quellen:

Risikoklasse / Kategorie	Beispiele für KI-Systeme	Wichtigste Anforderungen & Pflichten	Gültigkeitsbeginn / Frist	Sanktionen bei Verstößen	Verantwortliche Akteure	Quelle
Unannehmbares Risiko (Verboten)	Manipulative Techniken, Ausnutzung von Vulnerabilität (z.B. Alter, Behinderung, soziale Lage), Social Scoring, Emotionserkennung am Arbeitsplatz/Bildung (außer medizinisch/Sicherheit), biometrische Kategorisierung nach sensiblen Merkmalen.	Verbot des Inverkehrbringens, der Inbetriebnahme und der Verwendung. Prüfung auf wesentliche Verhaltensänderung und drohende erhebliche Schäden (Art. 5).	2. Februar 2025	Wirksame, verhältnismäßige und abschreckende Geldbußen (Art. 99), abhängig von Art, Schwere und Dauer des Verstoßes.	Anbieter, Betreiber (Deployer), Einführer, Händler.	[1]
Hohes Risiko (Hochrisiko-KI-Systeme)	KI als Medizinprodukt (z.B. Therapieplanung, Krisenintervention), Zugang zu Sozialleistungen (SGB VIII/XII), Bildungszulassung, Bewerbermanagement (HR-Software), Emotionserkennung (sofern nicht verboten).	Risikomanagementsystem (Art. 9), Daten-Governance (Art. 10), technische Dokumentation (Art. 11), menschliche Aufsicht (Art. 14), Genauigkeit & Cybersicherheit (Art. 15), Grundrechtefolgenabschätzung (Art. 27).	2. August 2026 (für Anhang III); 2. August 2027 (für Produkte unter Anhang I)	Erhebliche Geldbußen nach nationalen Umsetzungsvorschriften.	Anbieter (Softwarehersteller) und Betreiber (professionelle Nutzer/Einrichtungen).	[1]
Spezifisches Transparenzrisiko	Chatbots (Interaktion mit Menschen), Deepfakes, KI-generierte Texte (für öffentliche Informationen), Emotionserkennungssysteme.	Offenlegungspflicht: Information, dass man mit KI interagiert; Kennzeichnung von künstlich erzeugten Inhalten/Deepfakes (Art. 50).	2. August 2026	Bußgeldbewehrt bei Nicht-Einhaltung der Transparenzvorgaben.	Anbieter und Betreiber.	[1]

		Barrierefreiheit der Information.				
Minimales Risiko / Alle KI-Systeme	Spam-Filter, KI-gestützte Dokumentation ohne wesentlichen Einfluss auf Entscheidungen (z.B. sprachliche Korrektur), Onboarding-Bots für reines Wissensmanagement.	Sicherstellung der KI-Kompetenz der Mitarbeitenden (Art. 4). Freiwillige Einhaltung von Verhaltenskodizes möglich.	2. Februar 2025 (KI-Kompetenzpflicht)	Aufsichtsrechtliche Maßnahmen bei mangelnder Qualifizierung.	Alle Anbieter und Betreiber (professionelle Nutzer).	[1]
Unannehmbares Risiko (Verbotene Praktiken)	Social Scoring durch Staaten, biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum (mit Ausnahmen), kognitive Verhaltensmanipulation.	Vollständiges Verbot des Inverkehrbringens, der Inbetriebnahme oder der Verwendung dieser Praktiken in der EU.	Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist).	Anbieter und Betreiber (Deployer) innerhalb der EU.	Inferred
Hohes Risiko (High-Risk AI)	KI in der Bildung (z.B. Prüfungsbewertung), Beschäftigung/HR (z.B. Software zur Lebenslaufauswertung), kritische Infrastruktur, Strafverfolgung.	Konformitätsbewertung, Risikomanagementsystem, Daten-Governance, technische Dokumentation, menschliche Aufsicht, Grundrechtfolgenabschätzung (Art. 27).	August 2026 (allgemein) / August 2027 (für in Anhang I genannte Produkte); Digital Omnibus Anpassung 2026.	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Hauptpflichten) und Betreiber (Überwachung/Nutzung gemäß Anweisung).	Inferred
Begrenztes Risiko (Transparenzpflichten)	Chatbots (z.B. ChatGPT-basierte Kundensupport-Bots), Deepfakes, Emotionserkennungssysteme.	Transparenzpflichten: Nutzer müssen informiert werden, dass sie mit einer KI interagieren; Kennzeichnung von KI-generierten Inhalten.	August 2026 (24 Monate nach Inkrafttreten).	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und in bestimmten Fällen Betreiber (Kennzeichnungspflicht).	Inferred
Minimales Risiko	KI-gestützte Videospiele, Spam-Filter, einfache administrative KI-Tools in Kitas (ohne Profiling).	Keine spezifischen gesetzlichen Auflagen über bestehende Gesetze hinaus;	August 2024 (unmittelbar anwendbar).	Keine spezifischen Sanktionen unter dem AI Act (nur allgemeines Recht).	Anbieter.	Inferred

		freiwillige Verhaltenskodizes werden empfohlen.				
General Purpose AI (GPAI) / Basismodelle	Große Sprachmodelle (LLMs) wie GPT-4, Claude, Gemini.	Bereitstellung technischer Dokumentation, Zusammenarbeit mit Behörden, bei systemischem Risiko: Modellbewertung, Cybersicherheit.	August 2025 (12 Monate nach Inkrafttreten).	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter von GPAI-Modellen.	Inferred
Spezifische Pflicht: KI-Schulung (Art. 4)	Alle KI-Systeme im professionellen Kontext (z.B. Kita-Personal, Verwaltungsangestellte).	Anbieter und Betreiber müssen sicherstellen, dass ihr Personal über ein ausreichendes Maß an KI-Kompetenz verfügt (AI Literacy).	Februar 2025 (6 Monate nach Inkrafttreten).	Verhältnismäßige Sanktionen durch nationale Aufsichtsbehörden.	Anbieter und Betreiber (Deployer).	Inferred
Unannehmbares Risiko (Verbotene Praktiken)	Manipulative Techniken, Social Scoring, biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum, Emotionserkennung am Arbeitsplatz/Bildung, nicht einvernehmliche sexualisierte Deepfakes	Vollständiges Verbot des Inverkehrbringens und der Nutzung im EU-Binnenmarkt; Ausnahmen nur für eng definierte Strafverfolgungszwecke.	Seit dem 2. Februar 2025 (Verbot gilt bereits)	Bis zu 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes	Anbieter und Betreiber	[2]
Hohes Risiko (Anhang III - Grundrechte)	KI-Tools für Bewerbungsprozesse (HR), Bewertung von Lernergebnissen (Bildung), Kreditwürdigkeitsprüfung, kritische Infrastruktur (Strom/Wasser), Strafverfolgung	Risikomanagementsystem (Art. 9), Datenqualitätsstandards (Art. 10), technische Dokumentation (Art. 11), menschliche Aufsicht (Art. 14), Grundrechtefolgenabschätzung (Art. 27)	Verschoben auf den 2. Dezember 2027 (durch Digital Omnibus 2026)	Bis zu 15 Mio. Euro oder 3 % des weltweiten Jahresumsatzes	Anbieter (Hauptpflichten), Betreiber (Prüf- und Überwachungspflichten)	[2]

Hohes Risiko (Anhang I - Regulierte Produkte)	KI als Sicherheitskomponente in Spielzeug, Maschinen, Fahrzeugen oder medizinischen Geräten	Konformitätsbewertungsverfahren durch Dritte; Erfüllung sektorspezifischer Sicherheitsanforderungen und AI Act Pflichten.	Verschieben auf den 2. August 2028 (durch Digital Omnibus 2026)	Bis zu 15 Mio. Euro oder 3 % des weltweiten Jahresumsatzes	Produkthersteller / Anbieter	[2]
Begrenztes Risiko / Transparenzrisiko	Chatbots, Deepfakes, KI-generierte Texte/Bilder/Videos	Transparenzpflichten: Kennzeichnung von KI-Inhalten (maschinenlesbar), Information der Nutzer über KI-Interaktion (Art. 50).	2. August 2026 (Anbieter von Inhalten teils bis 2. Dez. 2026 laut Omnibus)	Bis zu 15 Mio. Euro oder 3 % des weltweiten Jahresumsatzes	Anbieter und Betreiber	[2]
Minimales Risiko	Spam-Filter, KI-gestützte Videospiele	Keine gesetzlichen Auflagen; Empfehlung zur Einhaltung freiwilliger Verhaltenskodizes.	2. August 2026	Keine spezifischen Sanktionen (außer bei allgemeinen Verstößen gegen Auskunftspflichten)	Anbieter und Betreiber	[2]
KI mit allgemeinem Verwendungszweck (GPAI)	Große Sprachmodelle (LLMs) wie ChatGPT (OpenAI)	Technische Dokumentation, Zusammenfassung der Trainingsdaten, Einhaltung des Urheberrechts; bei systemischem Risiko zusätzlich Risikomanagement.	2. August 2025 (GPAI-Regeln allgemein)	Bis zu 15 Mio. Euro oder 3 % des weltweiten Jahresumsatzes	Anbieter von GPAI-Modellen	[2]
KI-Schulungspflicht (Art. 4)	Alle KI-Systeme (unabhängig von der Risikoklasse)	Arbeitgeberpflicht zur KI-Kompetenzvermittlung: Mitarbeiter müssen über Kenntnisse verfügen, um KI-Systeme sachkundig und sicher einzusetzen.	Seit dem 2. Februar 2025 (durch Omnibus konkretisiert auf Unterstützungspflicht)	Geldbußen bei Nichteinhaltung allgemeiner Vorschriften (bis 15 Mio. € / 3 %)	Anbieter und Betreiber (Arbeitgeber)	[2]
Unannehmbares Risiko (Verboten)	Manipulative Techniken, Ausnutzung von Schwächen (Kinder, Ältere), Social Scoring,	Vollständiges Verbot der Nutzung im EU-Binnenmarkt gemäß Artikel 5. Ausnahmen	Seit dem 2. Februar 2025.	Bis zu 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer).	[3]

	biometrische Echtzeit-Fernidentifizierung (öffentliche Räume), Emotionserkennung am Arbeitsplatz/Schule.	nur für eng definierte Strafverfolgungszwecke.				
Hohes Risiko (Hochrisiko-KI)	Kritische Infrastruktur (Strom, Wasser), Personalmanagement (HR-Software für Bewerbungen), Bildung (Bewertung von Lernergebnissen), Kreditwürdigkeitsprüfung, Justiz, biometrische Fernidentifizierung.	Risikomanagementsystem (Art. 9), Datenqualitätsstandards (Art. 10), technische Dokumentation (Art. 11), menschliche Aufsicht (Art. 14), Grundrechte-Folgenabschätzung (Art. 27), KI-Schulungspflicht (Art. 4).	2. August 2026 (Anhang III) bzw. 2. August 2027 (Anhang I). Durch Digital Omnibus 2026: Verschiebung für Anhang III auf 2. Dez. 2027 und Anhang I auf 2. Aug. 2028.	Bis zu 15 Mio. Euro oder 3 % des weltweiten Jahresumsatzes.	Anbieter, Betreiber, Einführer, Händler.	[3]
Begrenztes Risiko (Transparenz)	Chatbots, Deepfakes, KI-generierte Texte/Bilder/Videos, Emotionserkennung (außerhalb verbotener Bereiche).	Transparenzpflichten: Nutzer müssen informiert werden, dass sie mit einer KI interagieren; KI-Inhalte müssen als solche gekennzeichnet sein (Art. 50).	2. August 2026. Durch Digital Omnibus 2026: Neue Frist für Anbieter zur Kennzeichnung synthetischer Inhalte am 2. Dez. 2026.	Bis zu 15 Mio. Euro oder 3 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber.	[3]
Minimales Risiko	Spamfilter, KI-gestützte Videospiele.	Keine spezifischen gesetzlichen Auflagen über bestehendes Recht hinaus. Freiwillige Einhaltung von Verhaltenskodizes wird empfohlen.	2. August 2026.	Keine spezifischen Sanktionen unter dem AI Act, sofern keine anderen Gesetze verletzt werden.	Anbieter.	[3]
KI mit allgemeinem Verwendungszweck (GPAI)	Große Sprachmodelle (LLMs) wie ChatGPT (GPAI mit systemischem Risiko).	Technische Dokumentation, Zusammenfassung der Trainingsdaten, Einhaltung des Urheberrechts. Bei	2. August 2025.	Bis zu 15 Mio. Euro oder 3 % des weltweiten Jahresumsatzes.	Anbieter von GPAI-Modellen.	[3]

		systemischem Risiko zusätzlich: Risikomanagement, Meldung schwerer Vorfälle.				
Verbotene KI-Praktiken (Art. 5)	Kognitive Verhaltensmanipulation, Ausnutzung von Schwachstellen, Social Scoring, biometrische Fernidentifizierung in Echtzeit, Emotionserkennung am Arbeitsplatz/Bildungseinrichtunge n, anlassloses Scraping von Gesichtsbildern.	Vollständiges Verbot des Inverkehrbringens, der Inbetriebnahme oder der Verwendung dieser Praktiken in der EU.	2. Februar 2025	Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist). (Inferred)	Anbieter und Betreiber (Deployer)	[4]
Hochrisiko-KI-Systeme (Anhang III & I)	Rekrutierung/Personalmanageme nt, Kreditwürdigkeitsprüfung, Bildung/Berufsbildung, Strafverfolgung, kritische Infrastrukturen.	Konformitätsbewertungen, Risikomanagementsysteme, Daten-Governance, technische Dokumentation, menschliche Aufsicht, Grundrechtefolgenabschätzun g (Art. 27).	2. Dezember 2027 (Anhang III) / 2. August 2028 (Anhang I - Produkte) gemäß Digital Omnibus 2026.	Bußgelder von bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes. (Inferred)	Anbieter (Primärpflichten) und Betreiber (Einhaltung der Nutzungsbedingungen/Ü berwachung).	[4]
KI-Systeme mit spezifischen Transparenzrisiken	Chatbots, Deepfakes, KI-generierte Texte/Bilder.	Offenlegungspflicht (Nutzer müssen wissen, dass sie mit KI interagieren), Kennzeichnung von KI-Inhalten (Watermarking).	August 2026	Nicht explizit im Text (gesetzlicher Rahmen bis zu 1,5 % des Umsatzes möglich). (Inferred)	Anbieter und Betreiber	[4]
Allzweck-KI-Modelle (GPAI)	Große Sprachmodelle (LLMs) wie GPT-4.	Bereitstellung technischer Dokumentation, Zusammenarbeit mit der Kommission, Zusammenfassungen von Trainingsdaten; bei	2. August 2025	Nicht im Quelltext spezifiziert. (Inferred)	Anbieter von GPAI- Modellen	[4]

		systemischem Risiko: Modellbewertungen und Cybersicherheit.				
Alle Risikostufen (KI-Schulungspflicht Art. 4)	Alle im professionellen Kontext genutzten Systeme (z. B. ChatGPT am Arbeitsplatz).	Sicherstellung der KI-Kompetenz (AI Literacy) bei Personal, das KI bedient; Verständnis der Funktionsweise und Risiken.	2. Februar 2025 (Aufsicht durch Marktüberwachung ab August 2026)	Verhältnismäßige Bußgelder je nach Mitgliedstaat. (Inferred)	Anbieter und Betreiber (Pflicht verbleibt bei Organisationen laut Digital Omnibus)	[4]
Unannehmbares Risiko (Verboten)	Social Scoring durch Staaten, biometrische Fernidentifizierung in Echtzeit (Öffentlicher Raum), manipulative Techniken zur Verhaltensbeeinflussung, Ausnutzung von Schwachstellen.	Vollständiges Verbot des Einsatzes innerhalb der EU (Art. 5).	Februar 2025 (6 Monate nach Inkrafttreten).	Bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer).	Inferred
Hochrisiko-KI	KI in der Bildung, HR-Software (Recruiting), Kreditwürdigkeitsprüfung, kritische Infrastrukturen, Strafverfolgung, Migrationskontrolle.	KI-Schulungspflicht (Art. 4), Qualitätsmanagementsystem, technisches Dossier, Risikomanagement, Grundrechtfolgenabschätzung (Art. 27).	August 2026 (24 Monate); für Bestands-IT (Digital Omnibus) teils bis 2027/2030.	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Hauptpflichten), Betreiber (Deployer) (Überwachung & Meldung).	Inferred
KI mit spezifischen Transparenzrisiken	Chatbots (z.B. ChatGPT), Deepfakes, Emotionserkennungssysteme.	Offenlegungspflicht (Nutzer müssen wissen, dass sie mit KI interagieren), Kennzeichnung von KI-generierten Inhalten.	August 2026 (24 Monate).	Bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und teils Betreiber.	Inferred
Minimales Risiko	KI-gestützte Videospiele, Spam-Filter.	Keine spezifischen gesetzlichen Auflagen über bestehendes Recht hinaus; freiwillige Verhaltenskodizes möglich.	August 2026.	Keine spezifischen Bußgelder unter dem AI Act.	Anbieter.	Inferred

General Purpose AI Models (GPAI)	Große Sprachmodelle (LLMs) mit systemischen Risiken.	Dokumentationspflichten, Einhaltung des Urheberrechts, bei systemischem Risiko: Modellbewertungen und Cybersicherheitstests.	August 2025 (12 Monate).	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Modellanbieter.	Inferred
Unannehmbares Risiko (Verbotene Praktiken)	Echtzeit-Biometrie im öffentlichen Raum, Social Scoring durch Behörden, Emotionserkennung am Arbeitsplatz/Bildungswesen, manipulative Techniken zur Verhaltensbeeinflussung.	Vollständiges Verbot der Inbetriebnahme oder Nutzung innerhalb der EU; Ausnahmen nur bei strengen Voraussetzungen für Strafverfolgung (Art. 5).	Februar 2025 (6 Monate nach Inkrafttreten)	Bis zu 35 Mio. € oder 7 % des weltweiten Vorjahresumsatzes.	Anbieter (Provider), Betreiber (Deployer), Einführer und Händler.	Inferred
Hohes Risiko (High-Risk)	HR-Software (Bewerberfilter), Bildung (Bewertung von Prüfungen), Kritische Infrastrukturen, Biometrie, Kreditwürdigkeitsprüfung, Rechtspflege.	Konformitätsbewertung, Risikomanagementsystem (Art. 9), Daten-Governance, technische Dokumentation, menschliche Aufsicht, Grundrechte-Folgenabschätzung (Art. 27) für öffentliche Stellen/Banken.	August 2026 (für Anhang III) bzw. August 2027 (für Produktsicherheit); Digital Omnibus 2026 Anpassungen beachten.	Bis zu 15 Mio. € oder 3 % des weltweiten Vorjahresumsatzes.	Anbieter (Hauptverantwortung), Betreiber (Überwachungspflichten), notifizierte Stellen.	Inferred
Begrenztes Risiko (Transparenzpflichten)	Chatbots (z.B. ChatGPT-Schnittstellen), Deepfakes, KI-generierte Texte (LLMs), Bildgeneratoren.	Offenlegungspflicht: Nutzer müssen wissen, dass sie mit einer KI interagieren; Kennzeichnung von KI-Inhalten (Art. 50); KI-Schulungspflicht für Personal (Art. 4).	August 2026 (allgemeine Anwendung)	Bis zu 7,5 Mio. € oder 1 % des weltweiten Vorjahresumsatzes.	Anbieter und Betreiber (hinsichtlich Kennzeichnung).	Inferred
Minimales Risiko	KI-gestützte Videospiele, Spam-Filter, KI-gesteuerte	Keine spezifischen gesetzlichen Auflagen über bestehendes Recht	August 2026	Keine spezifischen Bußgelder nach AI Act;	Anbieter und Betreiber.	Inferred

	Bestandsverwaltung in Kitas/Büros.	(DSGVO/KDG) hinaus; Einhaltung von freiwilligen Verhaltenskodizes empfohlen.		jedoch DSGVO-Sanktionen möglich.		
GPAI (General Purpose AI / Basismodelle)	Große Sprachmodelle (z.B. GPT-4, Gemini, Claude), Bild-Modelle (Midjourney).	Erstellung technischer Dokumentation, Zusammenarbeit mit dem KI-Büro, Zusammenfassungen über Trainingsdaten; Modelle mit systemischem Risiko: Modellbewertungen und Cybersicherheitspflichten.	August 2025 (12 Monate nach Inkrafttreten)	Bis zu 15 Mio. € oder 3 % des weltweiten Vorjahresumsatzes.	Anbieter von Basismodellen.	Inferred
Unannehmbares Risiko (Verbotene Praktiken)	Social Scoring, biometrische Fernidentifizierung in Echtzeit im öffentlichen Raum (mit Ausnahmen), KI zur kognitiven Verhaltensmanipulation.	Vollständiges Verbot des Inverkehrbringens, der Inbetriebnahme oder der Verwendung dieser Systeme in der EU.	Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter, Betreiber (Deployer), Importeure, Händler	Inferred
Hochrisiko-KI-Systeme	HR-Software (Bewerbersauswahl), Bildung (Bewertung von Prüfungen), Kreditwürdigkeitsprüfung, kritische Infrastrukturen.	Risikomanagementsystem, Daten-Governance, technische Dokumentation, Protokollierung (Logging), menschliche Aufsicht, Konformitätsbewertung, Grundrechtefolgenabschätzung (Art. 27).	August 2026 (allgemein) / August 2027 (für in EU-Rechtsakten geregelte Produkte); Digital Omnibus Anpassungen beachten.	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Hauptverantwortung), Betreiber (u.a. Überwachung im Betrieb, Meldepflichten).	Inferred
Spezifische Transparenzrisiken	Chatbots (z.B. ChatGPT), Deepfakes, KI-generierte Texte/Bilder.	Kennzeichnungspflicht (Nutzer müssen wissen, dass sie mit einer KI interagieren), Kennzeichnung von Deepfakes und KI-generierten Inhalten.	August 2026 (24 Monate nach Inkrafttreten).	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer).	Inferred

General-Purpose AI (GPAI) / Basismodelle	Große Sprachmodelle (LLMs) mit systemischem Risiko.	Technische Dokumentation, Zusammenfassungen über Trainingsdaten, Zusammenarbeit mit dem KI-Büro; bei systemischem Risiko zusätzlich Modellbewertungen und Cybersicherheit.	August 2025 (12 Monate nach Inkrafttreten).	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter von GPAI-Modellen.	Inferred
Minimales Risiko	Spam-Filter, KI-gestützte Videospiele.	Keine spezifischen gesetzlichen Pflichten über bestehendes Recht hinaus; freiwillige Verhaltenskodizes werden empfohlen. KI-Schulungspflicht (Art. 4) für Personal.	August 2024 (unmittelbar anwendbar für KI-Schulungspflicht).	Allgemeine Haftungsregeln.	Anbieter und Betreiber (Deployer).	Inferred
Verbotene Praktiken	Biometrische Identifizierung in Echtzeit im öffentlichen Raum (mit Ausnahmen), Social Scoring, manipulative KI zur Verhaltensbeeinflussung.	Absolutes Nutzungsverbot innerhalb der EU aufgrund unannehmbarer Risiken für die Grundrechte.	Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer)	[5]
Hohes Risiko (High-Risk)	HR-Software (Recruiting, Bewerberauswahl), Leistungsanalysen am Arbeitsplatz, Schichtplanung, Kreditwürdigkeitsprüfung, Bildungswesen.	Risikomanagementsystem, Daten-Governance, technische Dokumentation, Konformitätsbewertung, Grundrechtfolgenabschätzung (Art. 27).	August 2026 (24 Monate nach Inkrafttreten; für Produkte mit Drittprüfung 36 Monate)	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Primärpflichten) und Betreiber (Überwachungspflichten)	[5]
Begrenztes Risiko (Transparenz)	Chatbots im Recruiting, Deepfakes, Emotionserkennungssysteme.	Transparenzpflichten: Nutzer müssen informiert werden, dass sie mit einer KI interagieren;	August 2025 (12 Monate nach Inkrafttreten)	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber	[5]

		Kennzeichnungspflicht für KI-Inhalte.				
Minimales Risiko	Spam-Filter, KI-gestützte Videospiele.	Keine spezifischen gesetzlichen Auflagen, freiwillige Verhaltenskodizes werden empfohlen.	August 2024 (Inkrafttreten)	Keine spezifischen Sanktionen im Rahmen der KI-Verordnung.	Anbieter	[5]
Allgemeine Anforderungen (Horizontale Pflichten)	Alle KI-Systeme im beruflichen Kontext.	KI-Schulungspflicht (Art. 4): Sicherstellung der KI-Kompetenz bei Mitarbeitern, die KI bedienen.	Februar 2025 (6 Monate nach Inkrafttreten)	Einstufung als sonstige Verstöße gegen die Verordnung.	Dienstgeber / Betreiber (Deployer)	[5]
Unannehmbares Risiko (Verboten)	Systeme zur Manipulation von Menschen, Social Scoring, emotionale Beeinflussung	Verbot dieser Praktiken, da sie eine Bedrohung für die Grundrechte darstellen	Sofortige Gültigkeit (Verordnung gilt direkt)	Nicht im Quellmaterial spezifiziert	Träger der Sozialen Arbeit / Anbieter	[6]
Hohes Risiko	Einsatz in Gesundheit, Bildung, Beschäftigung (z.B. automatisierte Hilfeplanung)	Strenge Anforderungen: Transparenz, menschliche Kontrolle (Human-in-the-Loop), Risikomanagement, Dokumentation	Schulungspflicht seit Februar 2025	Nicht im Quellmaterial spezifiziert	Anbieter und Betreiber (Deployer)	[6]
Begrenztes Risiko	Chatbots, KI-generierte Inhalte (Texte, Bilder, Videos)	Transparenzpflicht: Information der Nutzer über KI-Interaktion, Kennzeichnungspflicht für KI-Inhalte	August 2024 (Inkrafttreten) / Schulungspflicht Feb 2025	Nicht im Quellmaterial spezifiziert	Betreiber / Träger	[6]
Minimales Risiko	Einfache Textvorschläge, Spamfilter	Keine spezifischen gesetzlichen Pflichten	Nicht im Quellmaterial spezifiziert	Nicht im Quellmaterial spezifiziert	Nicht im Quellmaterial spezifiziert	[6]
Unannehmbares Risiko (Verboten)	Manipulation von Menschen (psychologische Tricks), Social Scoring, Gesichtserkennung in	Vollständiges Verbot des Inverkehrbringens und der Nutzung. Leitlinien der	02.02.2025 (Verbot tritt in Kraft)	Bis zu 35 Mio. € oder 7 % des weltweiten Vorjahresumsatzes.	Anbieter und Betreiber	[7]

	Echtzeit (Öffentlicher Raum), biometrische Kategorisierung (sensible Merkmale), Emotionserkennung am Arbeitsplatz/Schule.	Kommission (Februar 2025) präzisieren Grenzen.				
Hohes Risiko (Hochrisiko-KI)	HR-Software (Bewerbersauswahl), Kreditwürdigkeitsprüfung, medizinische Bilderkennung, autonomes Fahren, kritische Infrastrukturen (Strom/Verkehr), KI in Bildung/Prüfungen.	Risikomanagementsystem (Art. 9), Datenverwaltung (Art. 10), technische Dokumentation (Art. 11), menschliche Aufsicht (Art. 14), KI-Kompetenzpflicht für Mitarbeiter (Art. 4), Grundrechtefolgenabschätzung (implizit über Art. 27).	01.08.2026 (allgemein); 01.08.2027 (für Anhang I Produkte); 31.12.2030 (IT- Großsysteme).	Bis zu 15 Mio. € oder 3 % des weltweiten Vorjahresumsatzes.	Anbieter (Hauptpflichten), Betreiber (Deployer), Einführer, Händler.	[7]
Begrenztes Risiko / Transparenz	Chatbots (Kundenservice), KI- generierte Inhalte (Bilder, Audios, Videos), Deepfakes.	Transparenzpflichten: Nutzer müssen erkennen, dass sie mit KI interagieren; Kennzeichnung von KI- generierten Inhalten (maschinenlesbar).	02.08.2026 (spezielle Kennzeichnungspflichten für synthetische Inhalte).	Bis zu 15 Mio. € oder 3 % des weltweiten Vorjahresumsatzes.	Anbieter und Betreiber	[7]
Minimales Risiko	Spamfilter, Rechtschreibkorrektur, KI-gestützte Videospiele.	Keine gesetzlichen Verpflichtungen; Empfehlung zur Einhaltung freiwilliger Verhaltenskodizes.	01.08.2024 (Inkrafttreten)	Keine direkten Sanktionen mangels Pflichten (außer bei Rollenwechsel).	Anbieter und Betreiber	[7]
GPAI (General Purpose AI)	Virtuelle Assistenten, Sprachmodelle (LLMs), Modelle mit systemischem Risiko (>10 ²⁵ FLOPs).	Technische Dokumentation, Urheberrechts-Compliance, Zusammenfassung der Trainingsdaten. Bei systemischem Risiko	01.08.2025 (allgemein); 02.08.2027 (für Bestandsmodelle).	Bis zu 15 Mio. € oder 3 % des weltweiten Vorjahresumsatzes.	Anbieter von GPAI- Modellen	[7]

		zusätzlich: Risikomanagement und Meldepflichten.				
Unannehmbares Risiko (Verbotene Praktiken)	Social Scoring, manipulative kognitive Beeinflussung, Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen	Vollständiges Verbot des Einsatzes in der EU (Art. 5). Spezifisch im Bildungsbereich: Verbot von Systemen zur Analyse von Emotionen (Gesicht/Stimme) bei Schülern/Kindern.	2. Februar 2025	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (je nachdem, was höher ist).	Anbieter und Betreiber (Deployer)	[8]
Hochrisiko-KI	Systeme zur Zulassung/Zuweisung zu Bildungseinrichtungen, Bewertung von Lernergebnissen (Grading), Erkennung von Prüfungsbetrug	Strenge Qualitäts-, Dokumentations- und Aufsichtsstandards; Grundrechte-Folgenabschätzung (Art. 27); Human-in-the-Loop (Art. 14); Konformitätsbewertung.	2. August 2027 (Vollständige Geltung für eingebettete Systeme)	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (primär), Betreiber (Compliance-Überwachung)	[8]
Begrenztes Risiko (Transparenzpflichten)	Generative KI, Chatbots (z. B. ChatGPT, Telli), Deepfakes, Bildgeneratoren	Transparenzpflicht (Art. 50): Nutzer müssen wissen, dass sie mit KI interagieren; Kennzeichnung von KI-generierten Inhalten (Deepfakes).	2. August 2026 (Allgemeine Transparenzregeln)	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Kennzeichnungspflicht)	[8]
Minimales Risiko	Spam-Filter, KI-gestützte Rechtschreibprüfung, einfache administrative Tools (Dienstplanung ohne Profiling)	Keine zusätzlichen gesetzlichen Auflagen über bestehende Gesetze (z. B. DSGVO) hinaus; freiwillige Verhaltenskodizes.	1. August 2024 (Inkrafttreten der VO)	Keine spezifischen AI Act Sanktionen, sofern keine anderen Rechte (DSGVO) verletzt werden.	Betreiber	[8]

Allzweck-KI-Modelle (GPAI)	Basismodelle wie GPT-4, Claude, Gemini	Erstellung technischer Dokumentationen; Bereitstellung von Informationen für nachgeschaltete Anbieter; Einhaltung des EU-Urheberrechts.	2. August 2025	Spezifische Bußgeldrahmen für GPAI-Anbieter durch das EU AI Office.	Anbieter von GPAI-Modellen	[8]
Sektorübergreifende Pflicht (KI-Kompetenz)	Alle KI-Anwendungen im beruflichen Kontext	Art. 4: Pflicht für Arbeitgeber, sicherzustellen, dass Mitarbeitende (Lehrkräfte, Erzieher), die KI nutzen, über ausreichende Kompetenz verfügen.	2. Februar 2025	Aufsichtsrechtliche Maßnahmen und mögliche Bußgelder durch nationale Behörden.	Träger (Betreiber/Deployer)	[8]
Zeitliche Roadmap (Meilensteine)	Gesamtregulierung (Digital Omnibus 2026 Berücksichtigung)	Schrittweise Einführung: Verbote (6 Mo.), GPAI (12 Mo.), Transparenz (24 Mo.), Hochrisiko (36 Mo.).	2024 bis 2027	Gestaffelt je nach Inkrafttreten der jeweiligen Artikel.	EU-Mitgliedstaaten, AI Office, Nationale Aufsichtsbehörden	[8]
Inakzeptables Risiko (Verbotene Praktiken)	Manipulative Techniken zur Verhaltensbeeinflussung, Ausnutzung von Vulnerabilitäten (Alter, Behinderung), Social Scoring, Echtzeit-Biometrie in öffentlich zugänglichen Räumen, Emotionserkennung in Bildungseinrichtungen.	Vollständiges Verbot der Anwendung; Schutz der Grundrechte und der menschlichen Selbstbestimmung (Art. 5).	02.02.2025 (6 Monate nach Inkrafttreten)	Nicht im Detail in der Quelle spezifiziert (Bußgeldrahmen allgemein Teil des AI Acts).	Anbieter und Betreiber (Deployer).	[9]
Hohes Risiko (Hochrisiko-KI)	KI zur Bewertung von Schülerleistungen, Notenfindung, Identifikation von	Risikomanagement, Qualitätssicherung, hochwertige Datensätze (Art. 26), Transparenz, menschliche	02.08.2026 (Generell) / 02.08.2027 (für bestimmte regulierte Produkte).	Nicht im Detail in der Quelle spezifiziert.	Anbieter (Hauptpflichten) und Betreiber (Aufsicht und Dateneingabe).	[9]

	Lernschwierigkeiten, Systeme für Zulassungsverfahren.	Aufsicht, Grundrechte-Folgenabschätzung (Art. 27).				
Begrenztes Risiko	KI-gestützte Chatbots zur Beantwortung von Schülerfragen, Deepfakes, Emotionserkennung (außerhalb der Verbote).	Transparenzpflichten (Art. 50): Nutzer müssen informiert werden, dass sie mit einer KI interagieren (z.B. durch KI-Logo).	02.08.2026	Nicht im Detail in der Quelle spezifiziert.	Anbieter und Betreiber.	[9]
Minimales / Kein Risiko	KI-gestützte Spam-Filter, KI in der Schulverwaltung für einfache Prozesse ohne Einfluss auf Grundrechte.	Keine spezifischen zusätzlichen gesetzlichen Verpflichtungen über bestehendes Recht hinaus; Förderung von Verhaltenskodizes.	02.08.2026	Keine spezifischen Sanktionen (weitgehend unreguliert).	Betreiber / Nutzer.	[9]
KI-Kompetenz (AI Literacy - Art. 4)	Gilt für alle KI-Systeme unabhängig von der Risikoklasse.	Sicherstellung eines ausreichenden Maßes an KI-Kompetenz beim Personal; Schulungs- und Fortbildungspflichten für Betreiber (Schulen).	02.02.2025	Nicht im Detail in der Quelle spezifiziert.	Anbieter und Betreiber (z.B. Schulleitung/Schulträger).	[9]
Unannehmbares Risiko (Verbotene Praktiken)	Social Scoring durch Behörden, biometrische Fernidentifizierung in Echtzeit im öffentlichen Raum (mit Ausnahmen), kognitive Verhaltensmanipulation.	Vollständiges Nutzungsverbot innerhalb der EU aufgrund des hohen Missbrauchspotenzials und des Verstoßes gegen Grundwerte.	Februar 2025 (6 Monate nach Inkrafttreten)	Bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer)	[10]
Hohes Risiko (High-Risk AI)	KI in der Bildung (Bewertung von Prüfungen), HR-Software (Recruiting), kritische Infrastruktur, Kreditwürdigkeitsprüfung, biometrische Identifizierung.	KI-Schulungspflicht (Art. 4), Grundrechtfolgenabschätzung (Art. 27), Qualitäts- und Risikomanagementsysteme,	August 2026 (24 Monate); für eingebettete Produkte (Digital Omnibus) teils bis August 2027.	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Hauptpflichten) und Betreiber (Überwachungspflichten)	[10]

		menschliche Aufsicht, technische Dokumentation.				
Begrenztes Risiko (Transparenzpflichten)	Chatbots (z. B. ChatGPT im Basiseinsatz), Deepfakes, Emotionserkennungssysteme.	Offenlegungspflicht: Nutzer müssen informiert werden, dass sie mit einer KI interagieren; Kennzeichnung von KI-generierten Inhalten.	August 2026 (allgemein), GPAI-Modelle bereits ab August 2025.	Bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und in spezifischen Fällen Betreiber	[10]
Minimales Risiko	KI-gestützte Videospiele, Spam- Filter, Inventar-Optimierung.	Keine spezifischen gesetzlichen Auflagen über bestehendes Recht (z. B. DSGVO) hinaus; freiwillige Verhaltenskodizes werden empfohlen.	August 2026	Keine spezifischen Bußgelder nach KI- Verordnung, sofern keine anderen Gesetze verletzt werden.	Anbieter	[10]
Verbotene Praktiken	Social Scoring durch staatliche Stellen, biometrische Fernidentifizierung in Echtzeit im öffentlichen Raum (mit Ausnahmen), kognitive Verhaltensmanipulation.	Vollständiges Verbot der Nutzung und Bereitstellung dieser Systeme innerhalb der EU aufgrund unannehmbarer Risiken für die Grundrechte.	Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter (Provider) und Betreiber (Deployer)	[Inferred]
Hohes Risiko (High-Risk)	HR-Software (Bewerberscreening), KI in der Bildung (Bewertung von Prüfungen), Kreditwürdigkeitsprüfung, Biometrie, kritische Infrastrukturen.	Risikomanagementsystem, Daten-Governance, technische Dokumentation, menschliche Aufsicht, Grundrechtfolgenabschätzung (Art. 27), KI-Schulungspflicht (Art. 4).	August 2026 (24 Monate); für Produkte mit EU- Sicherheitsvorschriften (Digital Omnibus) bis August 2027.	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Hauptverantwortung), Betreiber (Einhaltung der Nutzungsvorgaben)	[10-15, Inferred]
Begrenztes Risiko (Transparenzpflichten)	Chatbots (z. B. ChatGPT), Deepfakes, Emotionserkennungssysteme.	Offenlegungspflicht: Nutzer müssen informiert werden, dass sie mit einer KI	August 2026 (allgemein); GPAI-Modelle bereits ab August 2025.	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des	Anbieter und Betreiber	[5, 54, Inferred]

		interagieren; Kennzeichnung von KI-generierten Inhalten.		weltweiten Jahresumsatzes.		
Minimales Risiko	Spam-Filter, KI-gestützte Videospiele, Bestandsmanagementsysteme.	Keine spezifischen gesetzlichen Pflichten über bestehendes Recht hinaus; freiwillige Verhaltenskodizes werden empfohlen.	August 2026 (24 Monate)	Nicht spezifisch definiert (allgemeine Haftung).	Anbieter	[Inferred]
Verbotene Praktiken / Unannehmbares Risiko	Nicht explizit im Quelltext aufgeführt (gemäß AI Act: Social Scoring, biometrische Fernidentifizierung in Echtzeit).	Vollständiges Verbot des Einsatzes dieser Systeme innerhalb der EU.	6 Monate nach Inkrafttreten (Februar 2025).	Bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (Inferred).	Anbieter und Betreiber (Deployer).	[11]
Hochrisiko-KI-Systeme (HRAIS) - Kontextabhängig	Kritische Infrastruktur, Bildung, Strafverfolgung, HR-Software (Einstellung).	Konformitätsbewertung, technisches Dokumentationsmanagement, Qualitätsmanagementsystem (QMS), menschliche Aufsicht, Grundrechtfolgenabschätzungen (Art. 27).	Gemäß Digital Omnibus: 6 Monate nach Verfügbarkeit der technischen Standards (Backstop: 2. Dezember 2027).	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes (Inferred).	Anbieter (Provider) und Betreiber (Deployer).	[11]
Hochrisiko-KI-Systeme (HRAIS) - Sicherheitskomponenten	KI als Sicherheitskomponente in Produkten (Annex I), z. B. Medizinprodukte oder Fahrzeuge.	Einhaltung sektorspezifischer Sicherheitsvorschriften und AI Act Anforderungen; Post-Market-Monitoring.	Gemäß Digital Omnibus: 12 Monate nach Verfügbarkeit der Standards (Backstop: 2. August 2028).	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes (Inferred).	Anbieter (Produkthersteller).	[11]
Transparenzpflichten / Generative KI	Chatbots, Deepfakes, Bildgeneratoren (GenAI).	Kennzeichnung von KI-Inhalten (Watermarking), Offenlegung der Interaktion mit KI; KI-Schulungspflicht (Art. 4) nun als Empfehlung.	August 2026; Übergangsfrist für Watermarking bis 2. Februar 2027 für Bestandssysteme.	Nicht explizit im Text (typischerweise bis zu 7,5 Mio. EUR oder 1,5 % Umsatz - Inferred).	Anbieter und Betreiber.	[11]

Allgemeine KI-Modelle (GPAI)	Basis-Modelle (Foundation Models) wie GPT-4.	Technische Dokumentation, Zusammenfassung von Trainingsdaten, Urheberrechtseinhaltung; bei systemischem Risiko: Modellbewertungen.	12 Monate nach Inkrafttreten (August 2025).	Überwachung durch das zentrale EU AI Office.	Anbieter von GPAI-Modellen.	[11]
Minimales / Geringes Risiko	Spam-Filter, KI-gestützte Videospiele.	Keine spezifischen gesetzlichen Auflagen; freiwillige Verhaltenskodizes.	August 2024 (Inkrafttreten).	Keine direkten Sanktionen unter dem AI Act.	Anbieter.	[11]
Unannehmbares Risiko (Verbotene Praktiken)	Unterschwellige Beeinflussung, Ausnutzung von Schutzbedürftigkeit, biometrische Kategorisierung, Social Scoring, biometrische Echtzeit-Fernidentifizierung, Gesichtserkennungsdatenbanken, KI-Nudification-Apps	Vollständiges Nutzungsverbot; Pflicht zur Einstellung der Nutzung; Schulung der Mitarbeiter im Umgang mit KI (Art. 4)	02. Februar 2025	Bis zu 35 Mio. € oder 7 % des weltweiten Jahresumsatzes (für KMU gilt der niedrigere Betrag)	Anbieter und Betreiber	[12]
Hohes Risiko (Hochrisiko-KI)	Kritische Infrastrukturen, Bildung/Berufsbildung, Personalmanagement (HR-Software), Zugang zu privaten/öffentlichen Diensten, Strafverfolgung, Migration, Rechtspflege, medizinische Geräte, autonomes Fahren	Risikomanagementsystem, technische Dokumentation, Transparenz, menschliche Aufsicht, Grundrechte-Folgenabschätzung (Art. 27), Datenschutz-Folgenabschätzung, CE-Kennzeichnung, EU-Konformitätserklärung	02. Dezember 2027 (Anhang III - durch Digital Omnibus verschoben); 02. August 2028 (in Produkten integriert)	Bis zu 15 Mio. € oder 3 % des Jahresumsatzes	Primär Anbieter, teilweise Betreiber (Deployer)	[12]
Begrenztes Risiko	KI-Chatbots, Deepfakes, KI-Emotionserkennung, Systeme zur	Spezifische Transparenzpflichten (Art. 50): Kennzeichnungspflicht für KI-	02. August 2026	Bis zu 15 Mio. € oder 3 % des Jahresumsatzes	Anbieter und Betreiber	[12]

	Erzeugung synthetischer Inhalte (Audio, Bild, Video)	Inhalte, Information der Nutzer über Interaktion mit einer KI				
Minimales Risiko	Suchalgorithmen, Computerspiele, Spam-Filter	Keine spezifischen gesetzlichen Auflagen über bestehendes Recht hinaus; freiwillige Verhaltenskodizes möglich	02. August 2026	Nicht explizit aufgeführt (allgemeine Bestimmungen)	Anbieter	[12]
GPAI (KI-Modelle mit allgemeinem Verwendungszweck)	Große Sprachmodelle (LLMs) wie GPT (OpenAI), Claude (Anthropic)	Technische Dokumentation, Zusammenfassung der Trainingsdaten, Copyright-Compliance, Einhaltung des GPAI Code of Practice	02. August 2025 (Verpflichtungen für Anbieter)	Bis zu 15 Mio. € oder 3 % des Jahresumsatzes	Anbieter von GPAI-Modellen	[12]
Unannehmbares Risiko (Verboten)	Social Scoring, Emotionserkennung an Arbeitsplätzen und Bildungseinrichtungen, schädliche KI-basierte Manipulation und Täuschung.	Vollständiges Verbot des Inverkehrbringens und der Nutzung innerhalb der EU (Art. 5).	Februar 2025 (6 Monate nach Inkrafttreten).	Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber.	[13]
Hohes Risiko	Bewertung von Prüfungsergebnissen, Zulassungsverfahren (Bildung), KI-Sicherheitskomponenten in kritischen Infrastrukturen, Justizverwaltung.	Konformitätsbewertungsverfahren, Risikomanagementsystem, Grundrechte-Folgenabschätzung (Art. 27), menschliche Aufsicht, Dokumentation.	August 2026 (allgemein) bzw. August 2027 für KI als Sicherheitskomponente.	Bußgelder von bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer).	[13]
Begrenztes Risiko / Transparenzrisiko	Chatbots, Deepfakes, Generierung synthetischer Inhalte (Audio, Bild, Video, Text).	Transparenzpflichten (Art. 50): Kennzeichnung von KI-Interaktionen und	August 2026 (24 Monate nach Inkrafttreten).	Bußgelder von bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und gewerbliche Nutzer.	[13]

		synthetischen Inhalten (Deepfakes).				
Geringes / Minimales Risiko	Spam-Filter, KI-gestützte Videospiele.	Keine spezifischen gesetzlichen Auflagen; freiwillige Verhaltenskodizes möglich.	August 2026.	Keine spezifischen Bußgelder für diese Klasse vorgesehen.	Anbieter.	[13]
KI-Kompetenz (Horizontale Pflicht)	Alle KI-Systeme im beruflichen Kontext (z. B. Einsatz von bwGPT an Hochschulen).	KI-Schulungspflicht (Art. 4): Sicherstellung von technischem, regulatorischem und anwendungsspezifischem Wissen beim Personal.	2. Februar 2025.	Aufsichtsrechtliche Maßnahmen und Bußgelder je nach Kontext.	Anbieter und Betreiber (Arbeitgeber/Einrichtungen).	[13]
Unannehmbares Risiko (Verbotene Praktiken)	Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen; biometrische Kategorisierung nach sensiblen Attributen; Social Scoring; kognitive Verhaltensmanipulation.	Vollständiges Verbot des Inverkehrbringens, der Inbetriebnahme oder der Nutzung innerhalb der EU (Art. 5). Ausnahmen nur für eng definierte medizinische oder sicherheitsrelevante Zwecke.	Februar 2025 (6 Monate nach Inkrafttreten).	Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Vorjahresumsatzes (je nachdem, welcher Betrag höher ist).	Anbieter und Betreiber (Deployer).	[14, 15]
Hohes Risiko (Hochrisiko-KI-Systeme)	KI für Rekrutierung/HR-Software (Bewerberfilterung); Bewertung von Lernergebnissen; Kreditwürdigkeitsprüfung; biometrische Fernidentifizierung; Management kritischer Infrastrukturen (Wasser, Gas, Strom).	Risikomanagementsystem (Art. 9); Daten-Governance (Art. 10); technische Dokumentation (Art. 11); menschliche Aufsicht (Art. 14); Grundrechtfolgenabschätzung (Art. 27); Registrierung in EU-Datenbank.	August 2026 (allgemein); August 2027 für Systeme, die als Sicherheitskomponenten in bereits regulierten Produkten dienen.	Bußgelder von bis zu 15 Mio. EUR oder 3 % des weltweiten Vorjahresumsatzes.	Anbieter, Importeure, Händler und Betreiber (Deployer).	[14]
Allgemeine KI-Modelle (GPAI)	Große Sprachmodelle (LLMs) wie GPT-4, sofern sie als Basis für verschiedene Anwendungen	Erstellung technischer Dokumentation; Bereitstellung von	August 2025 (12 Monate nach Inkrafttreten); Anpassungsfristen für	Bußgelder von bis zu 15 Mio. EUR oder 3 % des weltweiten	Anbieter von GPAI-Modellen.	[14]

	dienen; Modelle mit systemischem Risiko bei hoher Rechenleistung.	Informationen für nachgeschaltete Anbieter; Einhaltung des Urheberrechts; bei systemischem Risiko zusätzlich: Modellbewertungen und Cybersicherheit.	bereits am Markt befindliche Modelle bis 2027.	Vorjahresumsatzes (Art. 101).		
Geringes / Minimales Risiko & Transparenzpflichten	Chatbots; Deepfakes; KI-generierte Texte (zur Information der Öffentlichkeit); Spam-Filter; KI-gestützte Videospiele.	Transparenzpflichten (Art. 50): Kennzeichnungspflicht (Nutzer müssen wissen, dass sie mit einer KI interagieren); AI Literacy Pflicht für Personal (Art. 4).	Februar 2025 (AI Literacy gemäß Art. 4); August 2026 (Transparenzregeln).	Bußgelder von bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Vorjahresumsatzes.	Anbieter und Betreiber (Deployer).	[14, 15]
Unannehmbares Risiko (Verbotene Praktiken)	Social Scoring, Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen, schädliche KI-basierte Manipulation und Täuschung	Vollständiges Verbot des Inverkehrbringens, der Inbetriebnahme oder der Verwendung solcher Systeme in der EU.	Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (Inferred)	Anbieter, Betreiber (Deployer)	[16]
Hohes Risiko (High-Risk)	KI-Systeme zur Bewertung von Prüfungsergebnissen (Bildung), Zugang zum Berufsleben (HR-Software), kritische Infrastrukturen, Justizverwaltung	KI-Schulungspflicht (Art. 4), Konformitätsbewertungsverfahren, Risikomanagementsystem, Grundrechtefolgenabschätzung (Art. 27) (Inferred)	August 2026 (24 Monate) / 2027 für Produkte mit Sicherheitskomponenten (Digital Omnibus)	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes (Inferred)	Anbieter, Betreiber (z.B. Hochschulen, Unternehmen)	[16]
Begrenztes Risiko	Chatbots (z.B. Findus One), Deepfakes, Generierung synthetischer Inhalte (Audio, Bild, Video, Text)	Transparenzpflichten (Art. 50): Kennzeichnungspflicht für KI-Interaktionen und synthetische Inhalte; KI-	August 2026 (allgemeine Transparenzpflichten)	Bußgelder bei Nichteinhaltung der Transparenzvorgaben (Inferred)	Anbieter (Kennzeichnung), Betreiber (Information der Nutzer)	[16, 17]

		Schulungspflicht für Personal (Art. 4).				
Geringes / Minimales Risiko	Spamfilter, KI-gestützte Videospiele	Keine spezifischen gesetzlichen Auflagen über bestehendes Recht hinaus; freiwillige Verhaltenskodizes werden empfohlen.	August 2026 (Inferred)	Keine spezifischen Sanktionen im AI Act vorgesehen (Inferred)	Anbieter	[16]
KI-Kompetenz (Art. 4)	Gilt für alle KI-Systeme (einschließlich bwGPT, Findus One)	Verpflichtende Schulung des Personals; Sicherstellung von technischem, regulatorischem und anwendungsspezifischem Wissen.	2. Februar 2025	Aufsichtsrechtliche Maßnahmen bei mangelnder Schulung (Inferred)	Anbieter und Betreiber (Deployer)	[16, 17]
Verbotene Praktiken	Social Scoring durch Staaten, biometrische Fernidentifizierung in Echtzeit im öffentlichen Raum (mit Ausnahmen), kognitive Verhaltensmanipulation.	Vollständiges Verbot des Inverkehrbringens, der Inbetriebnahme oder der Verwendung innerhalb der EU.	Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer)	[18]
Hochrisiko-KI-Systeme	KI zur Bewertung von Schülerleistungen (ITS/AIS), HR-Software für Bewerberauswahl, Kreditwürdigkeitsprüfung, kritische Infrastrukturen.	KI-Schulungspflicht (Art. 4), Grundrechtfolgenabschätzung (Art. 27), Risikomanagementsystem, Daten-Governance, technische Dokumentation, menschliche Aufsicht.	August 2026 (allgemein); August 2027 für KI als Sicherheitskomponente in Produkten.	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Hauptpflichten) und Betreiber (Einhaltung der Nutzungsvorgaben)	[18]
Spezifische Transparenzrisiken (GPAI)	Chatbots (ChatGPT), Deepfakes, KI-generierte Texte (Formulierungshilfen), Bildgeneratoren.	Offenlegung, dass Inhalte KI-generiert sind; Kennzeichnungspflicht für Deepfakes; Zusammenfassung	August 2025 (12 Monate für General Purpose AI)	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter von Modellen mit allgemeinem Verwendungszweck	[18]

		urheberrechtlich geschützter Trainingsdaten.				
Minimales / Geringes Risiko	Spam-Filter, KI-gestützte Videospiele, einfache Inventar-Software.	Keine spezifischen gesetzlichen Auflagen über bestehendes Recht (DSGVO) hinaus; freiwillige Verhaltenskodizes werden empfohlen.	August 2026 (vollständige Anwendbarkeit)	Keine spezifischen KI-Act-Sanktionen (nur allgemeine Gesetze wie DSGVO).	Anbieter	[18]
Unannehmbares Risiko (Verbotene Praktiken)	Systeme zur Ausnutzung von Schwachstellen aufgrund des Alters (Art. 5); Social Scoring; biometrische Fernidentifizierung in Echtzeit.	Vollständiges Verbot des Inverkehrbringens, der Inbetriebnahme oder der Verwendung solcher Systeme in der EU.	Februar 2025 (6 Monate nach Inkrafttreten)	Bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter (Provider) und Betreiber (Deployer).	[19]
Hohes Risiko (High-Risk)	KI im Bildungswesen (z. B. Prüfungsbewertung), HR-Software (Rekrutierung), kritische Infrastrukturen, Strafverfolgung.	Risikomanagementsystem (Art. 9); Grundrechte-Folgenabschätzung (Art. 27); Daten-Governance; technische Dokumentation; menschliche Aufsicht.	August 2026 (24 Monate nach Inkrafttreten); Digital Omnibus 2026 Anpassungen für bestehende Systeme.	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Hauptpflichten), Importeure, Händler und Betreiber (Überwachungspflichten)	[19]
KI mit spezifischen Transparenzrisiken	Chatbots, Deepfakes, Emotionserkennungssysteme, KI-generierte Inhalte.	Offenlegungspflicht (Nutzer müssen wissen, dass sie mit KI interagieren); Kennzeichnung von Deepfakes (Watermarking).	August 2026 (24 Monate nach Inkrafttreten).	Bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber.	[19]
Minimales Risiko / Allgemeines Risiko	Spam-Filter, KI-gestützte Videospiele, einfache Inventar-Software.	KI-Schulungspflicht (Art. 4) für Personal; Einhaltung freiwilliger Verhaltenskodizes.	August 2024 (Art. 4 KI-Schulungspflicht gilt bereits kurz nach Inkrafttreten).	Verhältnismäßige Geldbußen je nach Schweregrad und nationaler Umsetzung.	Betreiber (Deployer) bezüglich der Mitarbeiterschulung.	[19, 20]

Unakzeptables Risiko (Verbotene Praktiken)	Schädliche Manipulation, Social Scoring, biometrische Echtzeit-Fernidentifizierung, Emotionserkennung in Bildungseinrichtungen oder am Arbeitsplatz.	Vollständiges Verbot des Inverkehrbringens und der Nutzung innerhalb der EU (Art. 5). Schutz der Grundrechte und Vermeidung manipulativer Praktiken.	02. Februar 2025 (Verbot tritt 6 Monate nach Inkrafttreten in Kraft).	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist).	Anbieter (Provider) und Betreiber (Deployer).	[21]
Hohes Risiko (High-Risk)	KI zur Bewertung von Lernleistungen (Noten), Systeme zur Zulassungsentscheidung, Überwachung von Schülerverhalten bei Prüfungen, HR-Software für Rekrutierung.	Strenge Auflagen: Konformitätsbewertung, Risikomanagementsystem, Daten-Governance, technische Dokumentation, menschliche Aufsicht (Human Oversight) und Grundrechtfolgenabschätzung (Art. 27).	02. August 2026 (allgemeine Anwendung); für in Produkte eingebettete Systeme bis 02. August 2027.	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Hauptverantwortung) und Betreiber (Einhaltung der Nutzungsvorgaben).	[21, 22]
Begrenztes Risiko / Transparenz	Chatbots (z.B. Kundensupport), Deepfakes, generative KI-Tools (z.B. ChatGPT für allgemeine Texte).	Transparenzpflichten: Nutzer müssen informiert werden, dass sie mit einer KI interagieren. Kennzeichnung von KI-generierten Inhalten.	02. August 2025 (Regeln für General-Purpose AI / GPAI).	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und teils Betreiber (hinsichtlich Kennzeichnung).	[21, 22]
Minimales Risiko	KI-gestützte Rechtschreibprüfung, automatische Übersetzungen (DeepL), Spam-Filter, Videospiele mit KI-Gegnern.	Keine spezifischen gesetzlichen Zusatzanforderungen über bestehendes Recht hinaus. Freiwillige Verhaltenskodizes möglich.	Ab Inkrafttreten (weitgehend unreguliert).	Keine spezifischen Sanktionen unter dem AI Act, sofern keine anderen Rechte (z.B. DSGVO) verletzt werden.	Anbieter.	[21, 22]
KI-Kompetenz & Schulung	Alle im Bildungsbereich eingesetzten Systeme (IServ, MS 365 Copilot, Moodle-Plugins).	KI-Schulungspflicht (Art. 4): Mitarbeiter in Bildungseinrichtungen müssen	02. Februar 2025 (Inkrafttreten der Schulungspflicht).	Abhängig von nationaler Aufsicht und Schwere der	Betreiber (Deployer) / Schulleitungen / Träger.	[21, 22]

(Sektorübergreifend/Bildung)		fachkundig geschult werden, um Chancen und Risiken zu verstehen (KI-Literacy).		Vernachlässigung der Sorgfaltspflicht.		
Unannehmbares Risiko (Verbotene Praktiken)	KI-Systeme, die Schwachstellen aufgrund des Alters (Kinder) ausnutzen; biometrische Fernidentifizierung; Social Scoring.	Vollständiges Verbot des Inverkehrbringens und der Inbetriebnahme dieser Systeme in der EU.	6 Monate nach Inkrafttreten (ca. Februar 2025).	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer).	[23]
Hochrisiko-KI-Systeme	KI im Bildungswesen (z.B. Prüfungsbewertung); HR-Software (Recruiting); kritische Infrastrukturen; medizinische Geräte.	Strenge Risikomanagementsysteme; Grundrechtefolgenabschätzung (Art. 27); Konformitätsbewertungsverfahren; Dokumentationspflichten.	24 bis 36 Monate nach Inkrafttreten (Roadmap 2026/2027; teils angepasst durch Digital Omnibus).	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Primär Anbieter; spezifische Überwachungspflichten für Betreiber (Deployer).	[23, 24]
Spezifische Transparenzrisiken	Chatbots; Deepfakes; Emotionserkennungssysteme.	Offenlegungspflicht (Nutzer müssen wissen, dass sie mit KI interagieren); Kennzeichnungspflicht (Watermarking) für Deepfakes.	Ab 2026 (allgemeine Anwendung der meisten Bestimmungen).	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und Nutzer/Betreiber.	[23]
Alle KI-Systeme (Allgemeine Pflicht)	Jede Art von KI-Software in Organisationen.	KI-Schulungspflicht gemäß Art. 4 (KI-Kompetenz für Personal sicherstellen); Verknüpfung mit Datenschutzschulungen empfohlen.	Bereits hohe praktische Relevanz (unmittelbare Vorbereitung erforderlich).	Verhältnismäßige Sanktionen je nach Schweregrad der Vernachlässigung der Sorgfaltspflicht.	Anbieter und Betreiber (Arbeitgeber).	[24]
Inakzeptables Risiko (Verbotene Praktiken)	Nicht explizit im Text (allgemein: Social Scoring, biometrische Fernidentifizierung im öffentlichen Raum)	Vollständiges Verbot der Nutzung und des Inverkehrbringens innerhalb der EU.	Ab 2. Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (Inferred)	Anbieter und Betreiber (Deployer)	[25, 26]

Hohes Risiko (Hochrisiko-KI)	Systeme zur Leistungsbewertung oder Lernanalyse in Schulen, HR-Software, KI im Gesundheitswesen (Diagnose)	Strenge Anforderungen an Transparenz, Datenqualität, Dokumentation; Grundrechtefolgenabschätzung (Art. 27); Konformitätsbewertungsverfahren.	Vollständige Umsetzung bis 2026 (Digital Omnibus Anpassungen)	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes (Inferred)	Anbieter (Hauptpflichten) und Betreiber (Überwachung/Meldepflichten)	[25, 26]
Geringes / Minimales Risiko & Spezifische Transparenz	Chatbots, generative KI, KI-basierte Lernempfehlungen, einfache Filter	Transparenzpflichten (Nutzer müssen wissen, dass sie mit KI interagieren); Kennzeichnungspflicht für KI-generierte Inhalte.	Ab August 2026 (allgemeine Anwendung)	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes (Inferred)	Anbieter und Betreiber (Deployer)	[25, 26]
Alle Risikoklassen (KI-Schulungspflicht)	Alle KI-Anwendungen im beruflichen/behördlichen Kontext (z.B. Office-KI, Schul-KI)	KI-Kompetenz (Art. 4): Maßnahmen zur Sicherstellung eines ausreichenden Maßes an AI Literacy beim Personal; Dokumentation der Schulungen.	Ab 2. Februar 2025	Haftungsrisiken im Schadensfall bei Nachweis mangelnder Kompetenz; behördliche Bußgelder möglich.	Anbieter und Betreiber (Unternehmen, Behörden, Bildungseinrichtungen)	[25, 26]
GPAI (KI-Modelle mit allgemeinem Verwendungszweck)	Basismodelle (Foundation Models) wie GPT-Varianten	Technische Dokumentation, Urheberrechtsvorgaben, Zusammenfassungen von Trainingsdaten.	Ab August 2025 (12 Monate nach Inkrafttreten)	Spezifische Bußgelder für Modell-Anbieter (Inferred)	Anbieter von KI-Modellen	[25, 26]
Unannehmbares Risiko (Verbotene Praktiken)	Nicht explizit im Quelltext aufgeführt (allgemeine Kategorie des AI Act)	Vollständiges Verbot der Nutzung und Bereitstellung dieser Systeme innerhalb der EU.	Februar 2025 (6 Monate nach Inkrafttreten am 01.08.2024)	Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Vorjahresumsatzes (je nachdem, welcher Betrag höher ist).	Anbieter und Betreiber (Deployer)	[27]

Hohes Risiko (Hochrisiko-KI)	KI in der Bildung (z. B. Bewertung von Prüfungen), HR-Software (Rekrutierung), Biometrie, kritische Infrastrukturen.	Risikomanagementsystem, Daten-Governance, technische Dokumentation, menschliche Aufsicht, Grundrechtefolgenabschätzung (Art. 27).	August 2026 (24 Monate nach Inkrafttreten); für bestimmte Produkte August 2027 (36 Monate).	Bußgelder von bis zu 15 Mio. EUR oder 3 % des weltweiten Vorjahresumsatzes.	Anbieter (Hauptpflichten) und Betreiber (u. a. Überwachung, Art. 4 Schulungspflicht).	[27]
Begrenztes Risiko (Transparenzpflichten)	Chatbots (z. B. ChatGPT), Deepfakes, Emotionserkennungssysteme.	Transparenzpflichten: Nutzer müssen informiert werden, dass sie mit einer KI interagieren; Kennzeichnung von KI-generierten Inhalten.	August 2026 (allgemeine Anwendung), teils früher für GPAI-Modelle (August 2025).	Bußgelder von bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Vorjahresumsatzes.	Anbieter und Betreiber	[27, 28]
Minimales Risiko / Kein Risiko	Spam-Filter, KI-gestützte Videospiele, administrative Übersetzungstools (z. B. DeepL für Routine).	Keine spezifischen gesetzlichen Pflichten; freiwillige Verhaltenskodizes werden empfohlen. KI-Schulungspflicht (Art. 4) gilt dennoch für Personal.	August 2026 (allgemeine Anwendung).	Keine direkten Sanktionen, sofern keine anderen gesetzlichen Verstöße (z. B. DSGVO) vorliegen.	Anbieter und Betreiber	[27, 28]
Spezifische Pflicht: KI-Kompetenz (Art. 4)	Alle KI-Systeme (einschließlich ChatGPT-Nutzung in Organisationen).	Pflicht zur Sicherstellung der KI-Kompetenz/Schulung des Personals, das KI-Systeme im Auftrag des Betreibers nutzt.	Februar 2025 (6 Monate nach Inkrafttreten gemäß Leitlinien zur KI-Kompetenz).	Einstufung als allgemeiner Verstoß gegen Bestimmungen des AI Act; Bußgelder je nach Schweregrad.	Betreiber (Deployer) / Arbeitgeber (auch gemeinnützige Träger).	[27, 28]
Unannehmbares Risiko (Verbotene Praktiken)	Nicht-konsensuale intime Bilder/Videos (Nudifiers), Kindesmissbrauchsmaterial (CSAM).	Vollständiges Verbot der Bereitstellung und Nutzung; Anbieter müssen vorausschaubare Missbrauchsrisiken bei Design und Einsatz bewerten und	2. Februar 2025 (allgemein); Übergangsfrist für das neue Nudifier/CSAM-Verbot bis 2. Dezember 2026.	Nicht im Detail in der Quelle genannt (Bußgeldrahmen im EU AI Act vorgesehen).	Anbieter (Providers).	[29]

		technische Schutzmaßnahmen implementieren (Art. 5).				
Hohes Risiko (Hochrisiko-KI-Systeme - Anhang III)	Rekrutierung (HR-Software), Kreditwürdigkeitsprüfung, Strafverfolgung, Bildung (Prüfungssysteme), Grenzmanagement.	Konformitätsbewertungen, Risikomanagementsysteme, Grundrechtfolgenabschätzun gen (Art. 27), Transparenzpflichten.	2. Dezember 2027 (durch Digital Omnibus verschoben).	Durchsetzung durch EU AI Office und nationale Behörden; Befugnis zur Verhängung von Bußgeldern.	Anbieter und Betreiber (Deployer).	[29]
Hohes Risiko (Hochrisiko-KI in regulierten Produkten - Anhang I)	Medizinprodukte, Maschinen, Fahrzeuge, Spielzeug.	Einhaltung der KI-Act- Anforderungen integriert in bestehende sektorale Sicherheitsvorschriften; Vermeidung von Doppelregulierung.	2. August 2028 (durch Digital Omnibus verschoben).	Sektorale Sanktionen kombiniert mit KI-Act- Befugnissen des AI Office.	Anbieter der Produkte.	[29]
Transparenzrisiko / Spezifische Transparenzpflichten	Chatbots, KI-generierte Inhalte (Texte, Bilder).	Offenlegung der Interaktion mit KI; Wasserzeichenpflicht für KI-generierte Inhalte (Art. 50 Abs. 2).	2. August 2026; 4- monatige Schonfrist für Wasserzeichen bei Bestandssystemen bis 2. Dezember 2026.	Untersuchungsbefugnisse und Sanktionen durch das EU AI Office.	Anbieter und teilweise Betreiber.	[29]
Allgemeine Pflichten (KI-Kompetenz)	Alle KI-Systeme am Arbeitsplatz/in Schulen.	KI-Schulungspflicht (Art. 4): Unterstützung der Mitarbeiter beim Erwerb von KI- Kompetenz (aufgeweichte Anforderung).	2. Februar 2025.	Überwachung durch nationale Behörden.	Anbieter und Betreiber (Deployer).	[29]
General-Purpose AI (GPAI)	Große Sprachmodelle (LLMs) wie GPT.	Dokumentationspflichten, Zusammenarbeit mit dem EU AI Office.	2. August 2025.	Exklusive Zuständigkeit des EU AI Office für Bußgelder und Inspektionen.	Anbieter von GPAI- Modellen.	[29]
Unannehmbares Risiko (Verbotene Praktiken)	Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen,	Striktes Verbot der Nutzung, Bereitstellung und	Seit dem 2. Februar 2025 (unmittelbar geltendes Verbot).	Bußgelder von bis zu 35 Mio. € oder 7 % des	Anbieter (Provider) und Betreiber (Deployer).	[30]

	biometrisches Face-Scraping, Social Scoring, kognitive Verhaltensmanipulation.	Inverkehrbringung solcher Systeme innerhalb der EU.		weltweiten Vorjahresumsatzes.		
Hohes Risiko (High-Risk AI)	KI zur Bewertung von Lernergebnissen, automatisierte Kitaplatzvergabe, Sprachstandsanalysen zur Förderzuweisung, HR-Software für Rekrutierung.	Risikomanagementsystem, Daten-Governance, technische Dokumentation, Protokollierung (Logging), menschliche Aufsicht, Konformitätsbewertung und Grundrechtefolgenabschätzung (Art. 27).	Verschieben auf den 2. Dezember 2027 (durch Digital Omnibus 2026; ursprünglich August 2026).	Bußgelder von bis zu 15 Mio. € oder 3 % des Umsatzes.	Primär Anbieter (Zertifizierung), aber auch Betreiber (Überwachung, Meldepflichten).	[30]
Begrenztes Risiko / Transparenzrisiko	Chatbots (z. B. ChatGPT), KI-Bildgeneratoren, Deepfakes, Systeme zur Interaktion mit Menschen.	Transparenzpflichten nach Art. 50: Nutzer müssen wissen, dass sie mit einer KI interagieren; Kennzeichnung von KI-generierten Inhalten.	2. August 2026 (Content-Marking für Altsysteme bis 2. Dezember 2026).	Bußgelder von bis zu 7,5 Mio. € oder 1,5 % des Umsatzes.	Anbieter und Betreiber (hinsichtlich der Kennzeichnungspflicht).	[30]
Minimales Risiko	Spam-Filter, KI-gestützte Videospiele, Rechtschreibprüfung, administrative Übersetzungen (ohne Datenspeicherung).	Keine spezifischen gesetzlichen Pflichten unter dem AI Act; Einhaltung allgemeiner Standards (DSGVO) und freiwillige Verhaltenskodizes.	Keine spezifische Frist (Anwendung allgemeiner Gesetze bereits gültig).	Keine Sanktionen direkt nach dem AI Act, jedoch nach DSGVO bei Datenschutzverstößen.	Anbieter und Betreiber.	[30]
KI-Kompetenz (Horizontalpflicht)	Gilt für alle KI-Systeme (Art. 4).	KI-Schulungspflicht für Personal: Personal, das KI einsetzt, muss über notwendige Kenntnisse zur Funktionsweise und Risikobewertung verfügen.	2. Februar 2025 (Einführungsphase läuft bereits).	Aufsichtsrechtliche Maßnahmen und Haftungsrisiken bei Fehlbedienung.	Anbieter und Betreiber (Arbeitgeberpflicht).	[30]

Unannehmbares Risiko / Verbotene Praktiken	Social Scoring (Bürgerbewertung), Gesichtserkennung im öffentlichen Raum (mit Ausnahmen), Emotionserkennung am Arbeitsplatz/Bildungseinrichtungen, manipulative Systeme (z.B. sprachgesteuertes Spielzeug), Ausnutzung von Schwächen (z.B. Robo-Calls gegen Senioren).	Striktes Verbot der Anwendung; Ausnahmen für Sicherheitsbehörden nur bei schweren Straftaten wie Terrorismus oder Menschenhandel unter strengen Auflagen.	Seit Anfang Februar 2025 (Wochenende vor dem 03.02.2025).	Nicht im Detail in der Quelle (Inferred: Bis zu 7 % des weltweiten Jahresumsatzes oder 35 Mio. Euro nach EU AI Act).	Anbieter und Betreiber (Unternehmen, Polizei, Sicherheitsbehörden).	[31]
Hohes Risiko (High-Risk)	KI in der Bildung (z.B. Bewertung von Prüfungen), HR-Software, kritische Infrastrukturen, Biometrie.	Einhaltung strenger Standards für Sicherheit, Transparenz und Ethik; Daten-Governance; Rechenschaftspflicht; menschliche Aufsicht; Konformitätsbewertungsverfahren.	Vollständig anwendbar ab August 2026 (Digital Omnibus Anpassungen beachtet).	Nicht im Detail in der Quelle (Inferred: Bis zu 3 % des weltweiten Jahresumsatzes oder 15 Mio. Euro).	Anbieter (Entwickler) und Deployer (Nutzer/Einsetzende Unternehmen).	[31, 32]
KI mit allgemeinem Verwendungszweck (GPAI) / Transparenzrisiko	Chatbots, Deepfakes, leistungsfähige Sprachmodelle.	Offenlegungspflicht (Nutzer müssen wissen, dass sie mit einer KI interagieren), Kennzeichnung von KI-generierten Inhalten, Dokumentationspflichten für technische Details.	August 2025 (Transparenzregeln); GPAI-Modelle teils früher/gestaffelt.	Nicht im Detail in der Quelle (Inferred: Bis zu 3 % des weltweiten Jahresumsatzes).	Anbieter von Modellen und Betreiber von Schnittstellen.	[31, 32]
Minimales Risiko	Spam-Filter, KI-gestützte Videospiele.	Keine spezifischen gesetzlichen Auflagen über bestehende Gesetze hinaus; freiwillige Verhaltenskodizes werden empfohlen (KI-	August 2026 (allgemeine Anwendung).	Keine spezifischen Bußgelder für diese Klasse, sofern keine anderen Rechte verletzt werden.	Anbieter.	[31, 32]

		Schulungspflicht Art. 4 gilt allgemein).				
Verbotene KI-Praktiken	Social Scoring, biometrische Fernidentifizierung in Echtzeit im öffentlichen Raum (mit Ausnahmen), manipulative Systeme, Ausnutzung von Schwachstellen.	Vollständiges Verbot des Inverkehrbringens, der Inbetriebnahme oder der Nutzung dieser Systeme innerhalb der EU.	Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer)	[33]
Hochrisiko-KI-Systeme (Anhang III & II)	Rechenschaftspflichtige Systeme in Bildung (Notenvergabe), Beschäftigung (Recruiting, Beförderung, Überwachung), kritische Infrastruktur, Strafverfolgung.	Risikomanagementsystem, Daten-Governance, technische Dokumentation, Protokollierung (Logging), Transparenz, menschliche Aufsicht, Grundrechtefolgenabschätzung (Art. 27).	2. August 2026 (Ursprünglich); durch Digital Omnibus auf 2. Dezember 2027 verschoben (für bestimmte Kategorien).	Bußgelder von bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Providers) und Betreiber (Deployers)	[33]
KI mit spezifischem Transparenzrisiko	Chatbots (z.B. ChatGPT), Deepfakes, Emotionserkennungssysteme.	Offenlegungspflicht (Nutzer müssen wissen, dass sie mit einer KI interagieren), Kennzeichnung von KI-generierten Inhalten.	August 2026 (24 Monate nach Inkrafttreten)	Bußgelder von bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und teilweise Betreiber	[33]
Allgemeine Anforderungen (Horizontal)	Alle KI-Systeme im Anwendungsbereich.	KI-Schulungspflicht für Personal (Art. 4): Sicherstellung eines angemessenen Maßes an KI-Kompetenz bei Mitarbeitern.	Februar 2025 (6 Monate nach Inkrafttreten)	Verhältnismäßige Sanktionen je nach Schweregrad und Unternehmensgröße.	Anbieter und Betreiber (Deployer)	[33, 34]
Minimales Risiko	Spam-Filter, KI-gestützte Videospiele.	Keine spezifischen gesetzlichen Verpflichtungen;	August 2026 (24 Monate nach Inkrafttreten)	In der Regel keine Sanktionen, sofern keine	Anbieter	[33]

		freiwillige Verhaltenskodizes werden empfohlen.		anderen Rechte verletzt werden.		
Unannehmbares Risiko (Verboten)	Systeme zur kognitiven Verhaltensmanipulation, ungezieltes Auslesen von Gesichtsbildern (Social Scoring), biometrische Fernidentifizierung in Echtzeit im öffentlichen Raum.	Vollständiges Verbot der Anwendung und des Inverkehrbringens innerhalb der EU.	Februar 2025 (6 Monate nach Inkrafttreten)	Bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer)	[35]
Hohes Risiko (High-Risk)	HR-Software (Bewerbermanagement), KI in der Bildung (Bewertung von Prüfungen), Kreditwürdigkeitsprüfung, kritische Infrastrukturen, Biometrie.	Risikomanagementsystem, Daten-Governance, technische Dokumentation, Transparenz, menschliche Aufsicht, Grundrechtfolgenabschätzung (Art. 27) für öffentliche Stellen.	August 2026 (24 Monate nach Inkrafttreten); für im Digital Omnibus geregelte Bestands-IT teils bis 2027/2030.	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Hauptpflichten) und Betreiber (Überwachung/Nutzung gemäß Anleitung)	[35]
Spezifisches Transparenzrisiko	Chatbots (z.B. ChatGPT), Deepfakes, Emotionserkennungssysteme.	Offenlegungspflicht: Nutzer müssen informiert werden, dass sie mit einer KI interagieren; Kennzeichnung von KI-generierten Inhalten.	August 2025 (12 Monate nach Inkrafttreten)	Bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber	[35]
Allgemeine Anforderungen (Horizontal)	Alle KI-Systeme im Unternehmen.	KI-Schulungspflicht (Art. 4): Sicherstellung von KI-Kompetenz bei Mitarbeitern, die Systeme bedienen; technische, rechtliche und ethische Kenntnisse.	Februar 2025 (bereits gültig gemäß Art. 4)	Aktuell nicht direkt bußgeldbehaftet (laut IHK Hannover), aber Haftungsrisiken im Schadensfall.	Alle Akteure (Anbieter, Betreiber, Händler, Importeure)	[35]
Minimales Risiko / Kein Risiko	Spam-Filter, KI-gestützte Videospiele, Inventar-Management-Tools.	Keine spezifischen gesetzlichen Auflagen;	August 2024 (Inkrafttreten)	Keine spezifischen Sanktionen gemäß AI Act.	Anbieter	[35]

		freiwillige Verhaltenskodizes werden empfohlen.				
Verbotene KI-Praktiken (Art. 5) / Inakzeptables Risiko	Social Scoring durch staatliche Stellen, manipulative KI, biometrische Echtzeit-Fernüberwachung im öffentlichen Raum, Emotionserkennung am Arbeitsplatz/Bildungseinrichtungen, ungezielte biometrische Auswertung, Erstellung nicht-einvernehmlicher intimer Inhalte.	Vollständiges Verbot der Inverkehrbringung, Inbetriebnahme und Nutzung in der EU.	2. Februar 2025	Bis zu 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes.	Anbieter, Betreiber (Deployer), Importeure und Händler.	[36]
Hochrisiko-KI-Systeme (Anhang III - Eigenständige Systeme)	Personalwesen (Bewerbersauswahl, Leistungsbeurteilung), Bildung (Zulassung, Benotung), biometrische Fernidentifizierung, kritische Infrastruktur, Kreditvergabe, Strafverfolgung, Migration, Justiz.	Konformitätsbewertung, technische Dokumentation, Risikomanagementsystem, Datenqualitätsstandards, menschliche Aufsicht, Grundrechtfolgenabschätzung (Art. 27), Registrierung in EU-Datenbank.	2. Dezember 2027 (verschoben durch Digital Omnibus 2026 von Aug 2026).	Bis zu 15 Mio. Euro oder 3 % des weltweiten Jahresumsatzes.	Primär Anbieter; Betreiber (Deployer) bezüglich Überwachung und Nutzung.	[36]
Hochrisiko-KI-Systeme (Anhang I - Sicherheitskomponenten)	Medizinprodukte, Maschinen, Spielzeug, Aufzüge, Fahrzeuge, Schutzausrüstungen (Produkte unter EU-Harmonisierungsvorschriften).	Einhaltung der sektoralen Sicherheitsanforderungen plus spezifische KI-Anforderungen; Konformitätsbewertung durch Dritte erforderlich.	2. August 2028 (verschoben durch Digital Omnibus 2026 von Aug 2027).	Bis zu 15 Mio. Euro oder 3 % des weltweiten Jahresumsatzes.	Anbieter/Hersteller.	[36, 37]
Begrenztes Risiko / Transparenzpflichten (Art. 50)	Chatbots, Deepfakes, KI-generierte Texte, Bilder, Audio oder Videos.	Offenlegungspflicht (Kennzeichnung als KI-Interaktion oder KI-generierter Inhalt), Deepfakes müssen als solche markiert sein.	2. August 2026	Bußgeldrahmen für allgemeine Verstöße (gestaffelt).	Anbieter und Betreiber (Deployer).	[36]

KI-Schulungspflicht / KI-Kompetenz (Art. 4)	Gilt für alle KI-Systeme (z.B. ChatGPT, MS Copilot), sofern sie beruflich genutzt werden.	Unternehmen müssen sicherstellen, dass Personal, das KI nutzt oder entwickelt, über ausreichende Kompetenz verfügt (KI-Literacy).	2. Februar 2025	Verstoß gegen allgemeine Pflichten; Haftungsrisiken für die Geschäftsführung.	Alle Unternehmen (Anbieter und Betreiber), unabhängig von der Größe.	[36]
General Purpose AI (GPAI) / Basismodelle	LLMs wie GPT-4 (Modelle mit oder ohne systemisches Risiko).	Technische Dokumentation, Urheberrechts-Compliance, bei systemischem Risiko: Modellbewertungen, Cybersicherheitstests, Überwachungspflichten.	2. August 2025	Spezifische Sanktionen für GPAI-Anbieter.	Anbieter von GPAI-Modellen.	[36, 37]
Minimales Risiko	Spam-Filter, KI-gestützte Videospiele, Empfehlungssysteme, einfache Textoptimierung.	Keine gesetzlichen Auflagen; Empfehlung von freiwilligen Verhaltenskodizes (Codes of Conduct).	Bereits zulässig; keine spezifische Frist.	Keine.	Anbieter.	[36, 37]
Unannehmbares Risiko (Verbotene Praktiken)	Kognitive Verhaltensmanipulation von Personen oder schutzbedürftigen Gruppen (z. B. KI-gesteuertes Spielzeug, das gefährliches Verhalten fördert); Social Scoring; biometrische Fernidentifizierung in Echtzeit.	Vollständiges Verbot des Inverkehrbringens, der Inbetriebnahme oder der Verwendung dieser Systeme in der EU aufgrund des unannehmbaren Risikos für die Sicherheit und die Grundrechte.	Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist).	Anbieter (Provider) und Betreiber (Deployer).	[38]
Hohes Risiko (High-Risk)	Systeme im Bildungswesen (z. B. Bewertung von Prüfungsleistungen, Zulassungsverfahren); HR-Software (Rekrutierung); kritische	Risikomanagementsystem; Daten-Governance; technische Dokumentation; Transparenz; menschliche Aufsicht; Genauigkeit; Grundrechte-	August 2026 (24 Monate nach Inkrafttreten) / August 2027 für Produkte mit Konformitätsbewertung durch Dritte.	Bußgelder von bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Hauptverantwortung für Konformität) und Betreiber (Einhaltung der Nutzungsvorgaben).	[38]

	Infrastrukturen; Biometrie; Rechtspflege.	Folgenabschätzung (Art. 27) für bestimmte Akteure.				
Spezifisches Transparenzrisiko	Chatbots; Deepfakes (KI-generierte Bilder/Videos/Audios); Emotionserkennungssysteme.	Offenlegungspflicht: Nutzer müssen informiert werden, dass sie mit einer KI interagieren; Deepfakes müssen als künstlich erzeugt oder manipuliert gekennzeichnet werden (Labeling/Metadaten).	August 2026 (24 Monate nach Inkrafttreten).	Bußgelder von bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und Nutzer, die solche Inhalte erstellen/verbreiten.	[38]
Allgemeine Anforderungen (Horizontal)	Alle KI-Systeme im Anwendungsbereich des Gesetzes.	KI-Schulungspflicht (Art. 4): Personal, das KI-Systeme betreibt, muss über angemessene Kenntnisse verfügen (AI Literacy).	Februar 2025 (6 Monate nach Inkrafttreten).	Verhältnismäßige Sanktionen je nach nationaler Umsetzung und Schwere des Verstoßes.	Anbieter und Betreiber (Deployer).	[39]
Minimales Risiko	Spam-Filter; KI-gestützte Videospiele (ohne manipulative Absicht).	Keine spezifischen gesetzlichen Verpflichtungen über bestehendes Recht hinaus; freiwillige Verhaltenskodizes werden empfohlen.	August 2024 (unmittelbar nach Inkrafttreten möglich).	Keine spezifischen Bußgelder nach dem AI Act.	Anbieter.	[38]
Unannehmbares Risiko (Verbotene Praktiken)	Predictive Policing (Vorausschauende Polizeiarbeit), Social Scoring, biometrische Fernidentifizierung in Echtzeit (mit Ausnahmen).	Vollständiges Verbot des Inverkehrbringens und der Inbetriebnahme innerhalb der EU.	Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer)	[40]
Hohes Risiko (High-Risk)	HR-Software (Rekrutierung), Bildung (Bewertung von Prüfungen),	Risikomanagementsystem, Daten-Governance, technische Dokumentation, menschliche	Dezember 2027 (durch Digital Omnibus um 15	Bußgelder von bis zu 15 Mio. EUR oder 3 % des	Anbieter (Primärpflichten) und	[40]

	Kreditwürdigkeitsprüfung, kritische Infrastrukturen, Biometrie.	Aufsicht, Grundrechtefolgenabschätzung (Art. 27), KI-Schulungspflicht (Art. 4).	Monate von August 2026 verschoben)	weltweiten Jahresumsatzes.	Betreiber (Deployer - z.B. FRIAs)	
Spezifisches Transparenzrisiko	Chatbots, Deepfakes, Emotionserkennungssysteme, KI-generierte Texte.	Offenlegungspflicht: Nutzer müssen informiert werden, dass sie mit einer KI interagieren; Kennzeichnung von KI-Inhalten.	August 2026 (24 Monate nach Inkrafttreten)	Bußgelder von bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer)	[40]
Minimales Risiko	KI-gestützte Videospiele, Spam-Filter, einfache Algorithmen ohne sicherheitsrelevante Auswirkungen.	Keine spezifischen gesetzlichen Auflagen über bestehendes Recht hinaus; freiwillige Verhaltenskodizes werden empfohlen.	August 2026 (24 Monate nach Inkrafttreten)	Keine spezifischen Sanktionen gemäß KI-Gesetz (allgemeines Recht gilt).	Anbieter	[40]
General Purpose AI (GPAI) / Basismodelle	Large Language Models (LLMs) wie GPT-4, wenn sie für allgemeine Zwecke eingesetzt werden.	Technische Dokumentation, Einhaltung des Urheberrechts, Zusammenfassungen von Trainingsdaten; bei systemischem Risiko zusätzliche Modellbewertungen.	August 2025 (12 Monate nach Inkrafttreten)	Bußgelder von bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter von GPAI-Modellen	[40]
Verbotene Praktiken	Emotionserkennung oder Stimmungsanalyse von Kindern/Beschäftigten (Kamera/Mikrofon), Social Scoring (z.B. Einstufung als Risikokind), manipulative Systeme zur Verhaltenssteuerung,	Absolutes Nutzungsverbot gemäß Art. 5 EU AI Act; Schutzpflichten gegenüber Kindern verhindern Systeme, die Menschen klassifizieren oder überwachen	Verbot tritt 6 Monate nach Inkrafttreten in Kraft (ca. Februar 2025)	Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (Inferred)	Anbieter und Betreiber (Deployer / Träger)	[41]

	biometrische Auswertungen (Gesichtserkennung/Profiling)					
Hochrisiko-KI	Systeme für Zugangssteuerung, Leistungsbewertung, Verhaltensüberwachung, KI in Bildung oder Personalmanagement (HR-Software)	Grundrechtefolgenabschätzung (Art. 27), Konformitätsbewertung, menschliche Aufsicht, hohe Genauigkeit und Cybersicherheit, Risikomanagementsystem	Anforderungen greifen i.d.R. nach 36 Monaten (2027), für Bestandsysteme im öffentlichen Bereich ggf. früher (Omnibus 2026)	Bußgelder von bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes (Inferred)	Anbieter (Hauptpflichten) und Betreiber (Einhaltung der Nutzungsvorgaben)	[41]
Begrenztes Risiko / Transparenz	Chatbots (z.B. ChatGPT), Deepfakes, generative KI zur Texterstellung	KI-Schulungspflicht für Personal (Art. 4), Kennzeichnungspflicht von KI-Inhalten, Transparenzhinweise für Nutzer	Transparenzpflichten nach 12 bis 24 Monaten (2025/2026)	Bußgelder von bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes (Inferred)	Anbieter und Betreiber (Träger der Einrichtung)	[41]
Minimales Risiko	KI-gestützte Portfolioarbeit (Lerngeschichten), Erstellung von Elternbriefen, Übersetzungen, Inspiration für Spiele (ohne Personenbezug)	KI-Kompetenz der Anwender (Art. 4), Datenschutzkonformität (DSGVO), menschliche Überprüfung der Ergebnisse (Vermeidung von Halluzinationen)	KI-Kompetenzpflicht (Art. 4) gilt ab Februar 2025	Bei Missachtung der Sorgfaltspflichten vor allem zivilrechtliche Haftung oder DSGVO-Bußgelder	Pädagogische Fachkräfte und Kitaleitung (Betreiber)	[41, 42]
Verbotene Praktiken (Art. 5)	Emotionserkennung oder Stimmungsanalyse (Kamera/Mikrofon), Social Scoring, automatisierte Einstufung von Kindern/Eltern (z.B. "Risikokind"), manipulative Systeme, biometrische Auswertungen (Gesichtserkennung/Profiling)	Absolutes Nutzungsverbot für Systeme, die Kinder oder Beschäftigte bewerten, einordnen, überwachen oder deren Verhalten unbemerkt manipulativ steuern.	Verbot gilt 6 Monate nach Inkrafttreten (Februar 2025)	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (je nachdem, was höher ist)	Anbieter und Betreiber (Deployer)	[43]

Hochrisiko-KI	Systeme für Zugangssteuerung, Leistungsbewertung, Verhaltensüberwachung, KI zur Bewertung von Bildungsabschlüssen oder zur Steuerung des Bildungszugangs	Strenge Auflagen: Grundrechtefolgenabschätzung (Art. 27), Qualitätsmanagement, Risikomanagementsystem, detaillierte technische Dokumentation, menschliche Aufsicht.	Gültig nach 24 Monaten (August 2026); für Produkte unter EU-Harmonisierungsvorschriften nach 36 Monaten (August 2027)	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes	Anbieter (Primärpflichten) und Betreiber (Einhaltung der Nutzungsvorgaben)	[43]
Geringes / Minimales Risiko	Textentwürfe für Elterninfos, Übersetzungen, Inspiration für Spiele/Projekte (z.B. ChatGPT ohne Personenbezug), KI-gestützte Transkription (z.B. für HAVASE-Verfahren)	KI-Kompetenzpflicht (Art. 4): Schulung der Mitarbeitenden; Kennzeichnungspflicht bei Interaktion mit KI; menschliche Prüfung der Ergebnisse (Haftung).	KI-Kompetenz (Art. 4) gilt ab Februar 2025; Transparenzpflichten ab August 2026	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes bei Falschangaben	Betreiber (Kitas/Träger), Anbieter	[43, 44]
KI-Kompetenz (Art. 4) - Allgemeine Pflicht	Alle im professionellen Kontext genutzten KI-Systeme	Personal muss KI verstehen und kritisch hinterfragen können; Nachweis durch Schulungen (Datenschutz-Basics, No-Go-Daten, Prompt-Regeln, Dokumentation).	Gilt ab 02. Februar 2025	Aufsichtsrechtliche Maßnahmen und Bußgelder je nach nationaler Ausgestaltung	Träger der Einrichtung / Arbeitgeber (Sicherstellung der Befähigung)	[43]
Unannehmbares Risiko (Verbotene Praktiken)	KI-gestützte kognitive Verhaltensmanipulation, ungezieltes Auslesen von Gesichtsbildern (Social Scoring), biometrische Fernidentifizierung in Echtzeit (mit Ausnahmen).	Striktes Verbot der Anwendung innerhalb der EU aufgrund des hohen Gefährdungspotenzials für Grundrechte.	Februar 2025 (6 Monate nach Inkrafttreten)	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer).	[45]
Hohes Risiko (High-Risk)	Systeme für Zulassung/Zulassung zu Bildungseinrichtungen, Bewertung von Lernergebnissen,	Konformitätsbewertung, Risikomanagementsystem, Daten-Governance, technische	August 2026 (für im Anhang III gelistete Systeme); August 2027	Bußgelder bis zu 15 Mio. EUR oder 3 % des	Anbieter (Hauptpflichten), Betreiber	[45]

	Prüfung des Bildungsniveaus, Erkennung verbotenen Verhaltens von Schülern, HR-Software (Recruiting).	Dokumentation, menschliche Aufsicht, Grundrechtefolgenabschätzung (Art. 27).	(vollständige Anwendung).	weltweiten Jahresumsatzes.	(Sorgfaltspflichten/Überwachung).	
Spezifisches Transparenzrisiko (u.a. Generative KI)	Chatbots (z.B. ChatGPT, Gemini, Claude), Deepfakes, KI-generierte Texte/Bilder.	Offenlegungspflicht (Nutzer müssen wissen, dass sie mit KI interagieren), Kennzeichnungspflicht für Deepfakes (Watermarking), KI-Schulungspflicht (Art. 4).	August 2025 (für GPAI-Modelle); Digital Omnibus Anpassung bis Juni 2026 für Indikatoren.	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter von GPAI-Modellen, Betreiber von KI-Systemen.	[45]
Minimales Risiko	KI-gestützte Videospiele, Spam-Filter, einfache pädagogische Roboter ohne KI (z.B. vorprogrammierte Nao-Roboter).	Keine spezifischen gesetzlichen Verpflichtungen unter dem AI Act, jedoch Einhaltung bestehender Gesetze (z.B. DSGVO); freiwillige Verhaltenskodizes empfohlen.	August 2024 (Inkrafttreten, keine Übergangsfrist erforderlich).	Keine direkten Sanktionen durch den AI Act, sofern keine anderen Rechte (DSGVO) verletzt werden.	Anbieter.	[45, 46]
Inakzeptables Risiko (Verbotene Praktiken)	Biometrische Kategorisierung (sensible Merkmale), ungezielte Gesichtserkennungs-Datenbanken, Emotionserkennung (Arbeitsplatz/Bildung), Manipulation, Social Scoring, NCII/CSAM-Generierung.	Nutzung muss eingestellt werden; Verbot von Systemen zur Verhaltensmanipulation oder Ausnutzung von Schwachstellen; Verbot von Nudifier-Apps und CSAM-Inhalten.	02.02.2025 (allgemeine Verbote); 02.12.2026 (spezifische NCII/CSAM-Verbote laut Digital Omnibus).	Bis zu 35 Mio. Euro oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer).	[47, 48]
Hochrisiko-KI-Systeme	KI in kritischen Infrastrukturen, Bildung, Personalwesen (HR-Software), Strafverfolgung, Grenzschutz, Finanzinstitutionen.	Grundrechtefolgenabschätzung (Art. 27), Konformitätsbewertung, CE-Kennzeichnung, Risikomanagement,	02.08.2026 (Standard); verschoben auf 02.12.2027 (Art. 6 Abs. 2); 02.08.2028 (Sektor-Gesetzgebung Annex I).	Abstufung je nach Schwere: 7,5 Mio. € / 1,5 % bis zu 15 Mio. € / 3 % (inferred based on hierarchy).	Anbieter, Betreiber (Deployer), Importeure.	[47, 48]

		technische Dokumentation, menschliche Aufsicht.				
KI mit allgemeinem Verwendungszweck (GPAI / Foundation Models)	Große Sprachmodelle (z.B. ChatGPT), generative KI für Texte oder Bilder.	Technische Dokumentation, EU-Urheberrechts-Compliance, Zusammenfassung der Trainingsdaten; bei systemischem Risiko zusätzlich Modelltests und Risikominimierung.	02.08.2025 (Dokumentationspflichten); 02.08.2026 (Transparenz für generative KI).	Strafen durch das EU KI-Büro (zentrale Durchsetzung).	Anbieter (Entwickler).	[47, 48]
Minimales Risiko / Spezifische Transparenz	Chatbots, Deepfakes, KI-generierte Texte (für öffentliches Interesse), Spam-Filter, Videospiele.	Kennzeichnungspflicht (Nutzer müssen wissen, dass sie mit KI interagieren), Kennzeichnung von synthetischen Inhalten (Deepfakes), maschinenlesbare Wasserzeichen.	02.08.2026; verschoben auf 02.12.2026 für Content-Marking (Digital Omnibus); Übergangsfrist für Bestands-Systeme bis 02.12.2026.	Bußgelder je nach Unternehmensgröße und Schwere (7,5 Mio. € / 1,5 % Basis).	Anbieter und Betreiber.	[47, 48]
Übergreifende Pflichten (KI-Kompetenz)	Alle im Unternehmen eingesetzten KI-Tools.	KI-Schulungspflicht (Art. 4): Mitarbeiter müssen im kompetenten Umgang mit KI nachweislich geschult werden.	02.02.2025.	Keine expliziten Strafbestimmungen direkt in der Verordnung für Art. 4 genannt.	Unternehmen (Arbeitgeber), Vertragspartner, Lieferanten.	[47]
Sonderregeln (SMEs & Mid-Caps)	KI-Anwendungen von Start-ups oder mittelständischen Unternehmen.	Erleichterte Dokumentation, prioritärer Zugang zu Reallaboren (Sandboxes), angepasste Bußgeldobergrenzen.	Reallabore müssen bis 02.08.2027 einsatzbereit sein.	Gedeckelte/verhältnismäßige Bußgelder.	KMU, Start-ups, Small Mid-Caps (bis 750 MA / 150 Mio. € Umsatz).	[48]
Unannehmbares Risiko (Verbotene Praktiken)	Systeme zur kognitiven Verhaltensmanipulation, Social Scoring durch Behörden,	Vollständiges Verbot der Nutzung und des	Februar 2025	Bußgelder bis zu 35 Mio. EUR oder 7 % des	Anbieter und Betreiber (Deployer)	[49]

	biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum (mit Ausnahmen).	Inverkehrbringens innerhalb der EU.		weltweiten Vorjahresumsatzes.		
Hohes Risiko (Hochrisiko-KI)	Systeme im Bildungssektor (z.B. Prüfungsbewertung), HR-Software (Rekrutierung), kritische Infrastrukturen, Kreditwürdigkeitsprüfung.	Konformitätsbewertung, Risikomanagementsystem, Daten-Governance, technische Dokumentation, menschliche Aufsicht, Grundrechtefolgenabschätzung (Art. 27).	August 2026 (für bestimmte Systeme bis 2027/2030)	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Vorjahresumsatzes.	Primär Anbieter (Konformität), Betreiber (ordnungsgemäße Nutzung & Aufsicht)	[49, 50]
Spezifisches Transparenzrisiko / GAI	Chatbots (z.B. ChatGPT), Deepfakes, Emotionserkennungssysteme.	Offenlegungspflicht (Kennzeichnung als KI), Kennzeichnung von generierten Inhalten, Zusammenfassung urheberrechtlich geschützter Trainingsdaten.	August 2025 (für GAI-Modelle)	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Vorjahresumsatzes.	Anbieter und Betreiber	[49]
Alle KI-Systeme (Horizontalpflicht)	Jede Art von KI-Anwendung, unabhängig von der Risikostufe (z.B. einfache Büro-KI, Übersetzungstools).	KI-Schulungspflicht / KI-Kompetenz (Art. 4): Sicherstellung ausreichender Kenntnisse bei Personal, das KI nutzt oder entwickelt.	2. Februar 2025	Rechtliche Konsequenzen bei Vorfällen aufgrund mangelnder Kompetenz; Einbettung in Compliance-Systeme.	Anbieter und Betreiber (inkl. Behörden)	[50]
Verbotene Praktiken / KI-Systeme	Manipulative Systeme (unbewusste Beeinflussung), Social Scoring (Verhaltensbewertung), Echtzeit-Gesichtserkennung, Analyse von Emotionen (in Schulen).	Absolutes Nutzungsverbot für diese Praktiken innerhalb der EU.	Verbot tritt 6 Monate nach Inkrafttreten in Kraft (Inferred: Februar 2025).	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (Inferred).	Anbieter und Betreiber (Deployer).	[51]

Hochrisiko-KI	Systeme zur Notengebung, Bewertung von Schülerleistungen, Empfehlungssysteme für Bildungswege, Prüfungsüberwachung, Betrugserkennung, Kreditwürdigkeitsprüfung (Finanzwesen), Versicherungsrisikobewertung.	Grundrechtefolgenabschätzung (Art. 27), systematische Risikobewertung (Art. 35 DSGVO), Dokumentation der Funktionsweise (Art. 12 & 29), KI-Schulungspflicht für Personal (Art. 4), menschliche Aufsicht.	Allgemein 24-36 Monate (Inferred: 2026/2027); Grundrechtefolgenabschätzung vor Inbetriebnahme erforderlich.	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes (Inferred).	Betreiber (Deployer) für Art. 27; Anbieter für technische Konformität.	[51, 52]
KI mit begrenztem Risiko	Chatbots (z. B. virtuelle Assistenten), Sprachübersetzer, Grammatikhilfen, KI-gestützte personalisierte Übungsvorschläge.	Transparenzpflichten (Art. 50): Nutzer müssen über die Interaktion mit einer KI informiert werden. Kennzeichnungspflicht für KI-generierte Inhalte.	Anwendung nach 24 Monaten (Inferred: August 2026).	Bußgelder bei Verstößen gegen Transparenzpflichten (Inferred).	Anbieter und Betreiber (Deployer).	[51]
KI mit minimalem Risiko	Rechtschreibkorrekturen (z. B. Grammarly, DeepL), einfache Tutorensysteme (ohne Langzeitdatenspeicherung).	Keine spezifischen gesetzlichen Auflagen über bestehendes Recht (z. B. DSGVO) hinaus; Empfehlung zur Information der Nutzer.	Unmittelbar bzw. ab Geltung des AI Acts.	Keine spezifischen AI Act Sanktionen vorgesehen.	Anbieter und Betreiber (Deployer).	[51]
Unannehmbares Risiko (Verbotene Praktiken)	KI zur Generierung von Darstellungen sexuellen Missbrauchs von Kindern (CSAM) oder nicht einvernehmlichen intimen Inhalten (NCIC).	Vollständiges Verbot des Inverkehrbringens, der Inbetriebnahme oder der Verwendung solcher Systeme in der EU.	02. Dezember 2026	Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (basierend auf Standardregelungen des AI Act).	Anbieter, Betreiber (Deployer), Importeure und Händler.	[53]
Hochrisiko-KI (Standalone / Annex III)	KI-Systeme im Bereich HR, Beschäftigung (z. B.	Konformitätsbewertung, Risikomanagementsystem, Daten-Governance, technische	02. Dezember 2027 (verschoben durch Digital Omnibus/AI Omnibus).	Bußgelder von bis zu 15 Mio. EUR oder 3 % des	Anbieter (Primärverantwortung) und Betreiber (Deployer)	[53]

	Bewerbermanagement), Bildung, Strafverfolgung oder Grenzschutz.	Dokumentation, Registrierung in EU-Datenbank (Art. 6/Annex III).		weltweiten Jahresumsatzes.	bezüglich der Nutzungsvorgaben.	
Hochrisiko-KI (Eingebettet in Produkte / Annex I)	KI-Funktionen in Medizinprodukten (MDR), Maschinen (Machinery Regulation), Spielzeug oder Fahrzeugen.	Erfüllung der sektoralen Sicherheitsregeln kombiniert mit AI Act Anforderungen; Dritte-Partei-Konformitätsbewertung.	02. August 2028 (verschoben durch Digital Omnibus/AI Omnibus).	Bußgelder je nach Schweregrad und Unternehmensgröße (bis zu 3 % des Umsatzes).	Anbieter der Produkte und Hersteller der Sicherheitskomponenten .	[53]
KI mit spezifischen Transparenzrisiken (Begrenztes Risiko)	Chatbots (z. B. ChatGPT, Google Gemini), generative KI für Audio/Bild/Video, Deepfakes.	Transparenzpflichten (Art. 50): Kennzeichnung von KI-Inhalten (Watermarking), Offenlegung der KI-Interaktion gegenüber Nutzern.	02. August 2026 (generell); 02. Dezember 2026 für Watermarking bei Altsystemen.	Bußgelder von bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter (für technische Kennzeichnung) und Betreiber (für Information der Nutzer).	[53, 54]
Minimales Risiko / Übergreifende Pflichten	KI-gestützte Tools zur Kita-Planung, Bastelideen-Generatoren, Sprachförder-Reime ohne Personenbezug.	KI-Schulungspflicht (Art. 4); Sicherstellung der KI-Kompetenz (AI Literacy); Einhaltung von Datenschutzvorgaben (GDPR).	02. August 2026 (Schulungspflicht/Kompetenz).	Reputationsverlust; DSGVO-Bußgelder bei unsachgemäßer Datenverarbeitung.	Anbieter und Betreiber (Deployer) zur Förderung der Mitarbeiterkompetenz.	[53, 54]
Inakzeptables Risiko (Verbotene Praktiken)	Gesichtserkennung im öffentlichen Raum in Echtzeit, Social Scoring, vorausschauende Polizeiarbeit, Emotionserkennung in Bildungseinrichtungen oder am Arbeitsplatz.	Vollständiges Verbot der Nutzung und Bereitstellung dieser Systeme innerhalb der EU.	Verbote gelten ab Februar 2025 (6 Monate nach Inkrafttreten).	Bußgelder von bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes (je nachdem, welcher Wert höher ist).	Anbieter und Betreiber (Deployer).	[55]
Hochrisiko-KI-Systeme	Systeme zur Bewertung von Lernergebnissen, Steuerung von Lernprozessen, Überwachung von Prüfungsbetrug, Beeinflussung von	Konformitätsbewertungsverfahren, Risikomanagementsystem, Grundrechtfolgenabschätzung (Art. 27), Daten-Governance,	Allgemeiner Gültigkeitsbeginn ab 2. August 2026; für bestimmte Produkte 2027.	Bußgelder von bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (primär) und Betreiber (Sorgfaltspflichten).	[55, 56]

	Wählern, HR-Software (impliziert durch Arbeitsplatzkontext).	technische Dokumentation und menschliche Aufsicht.				
KI-Modelle mit allgemeinem Verwendungszweck (GPAI) / Geringes Risiko	Large Language Models (LLM) wie ChatGPT, Microsoft Copilot, Google Gemini; Chatbots, Deepfakes.	Transparenzvorschriften: Nutzer müssen über KI-Interaktion informiert werden; Kennzeichnung von Deepfakes; Zusammenfassung von Trainingsdaten; Einhaltung des Urheberrechts; KI-Schulungspflicht (Art. 4).	KI-Schulungspflicht ab 2. Februar 2025; GPAI-Regeln ab August 2025.	Bußgelder von bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter (Hersteller) und gewerbliche Nutzer.	[55, 56]
Minimales Risiko	KI-gestützte Videospiele oder Spam-Filter.	Freiwillige Verhaltenskodizes; keine spezifischen gesetzlichen Auflagen über bestehendes Recht (z.B. DSGVO) hinaus.	2. August 2026.	Nicht explizit für diese Klasse definiert, sofern keine Grundrechtsverletzungen vorliegen.	Anbieter.	[55, 56]
Unannehmbares Risiko (Verbotene Praktiken)	KI zur Erzeugung von nicht einvernehmlichen intimen oder sexuellen Inhalten (Nudifier), CSAM (Child Sexual Abuse Material).	Vollständiges Verbot des Inverkehrbringens und der Nutzung solcher Praktiken innerhalb der EU.	Bereits wirksam (Verbot bestimmter Praktiken gilt unmittelbar).	Nicht explizit beziffert für diese Kategorie, jedoch nationale Bußgeldvorschriften bis zu 50.000 EUR (DE-Entwurf).	Anbieter, Betreiber, Importeure.	[57, 58]
Hochrisiko-KI (High-Risk)	HR-Software (Vorauswahl, Leistungsanalyse), Bildung (Prüfungsbewertung, Zulassung), Öffentliche Leistungen (Pflegeplanung, Jugendhilfe), Kritische Infrastruktur.	Risikomanagementsystem (Art. 17), Dokumentation, Datenqualität & Governance, menschliche Aufsicht, KI-Verzeichnis, Grundrechtfolgenabschätzung (Schnittstelle zu DSFA).	02.12.2027 (Stand-alone Systeme); 02.08.2028 (Eingebettete Produkte/Sicherheitskomponenten).	Bußgeldvorschriften bis zu 50.000 EUR (nationaler Entwurf DE).	Anbieter (Provider), Betreiber (Deployer).	[57, 58]

Begrenztes Risiko / Transparenz	Chatbots (ohne Entscheidungsfunktion), KI- generierte Inhalte.	Transparenzpflichten: Kennzeichnung von KI- generierten Inhalten; Information der Nutzer über Interaktion mit KI.	02.12.2026 (für Kennzeichnungspflichten von Bestands-Systemen).	Bußgeldvorschriften bis zu 50.000 EUR (nationaler Entwurf DE).	Anbieter, Betreiber.	[57, 58]
Minimales Risiko / Unkritisch	Unterstützende Lernsysteme ohne Bewertung, Text-Tools für Stellenausschreibungen (ohne Entscheidungsfunktion).	KI-Schulungspflicht (AI Literacy) für Mitarbeitende gemäß Art. 4; Einhaltung allgemeiner Rechtsrahmen (DSGVO).	Bereits heute wirksam (insbesondere AI Literacy Pflicht).	Allgemeine Haftung und nationale Bußgelder.	Anbieter, Betreiber.	[57]
KI-Modelle mit allgemeinem Verwendungszweck (GPAI)	ChatGPT, Claude, Co-Pilot.	Spezifische Transparenz- und Dokumentationspflichten; exklusive Aufsicht durch das EU AI Office.	Februar 2027 (Aufschub durch Digital Omnibus).	Nicht im Detail beziffert (Aufsicht durch EU AI Office).	Anbieter (GPAI-Provider).	[57]
Unvertretbares Risiko	KI-Systeme, die gegen EU-Werte verstoßen (z. B. Social Scoring, biometrische Fernidentifizierung in Echtzeit in öffentlich zugänglichen Räumen mit Ausnahmen).	Vollständiges Verbot des Einsatzes und Inverkehrbringens dieser Systeme innerhalb der EU.	02. Februar 2025 (6 Monate nach Inkrafttreten).	Bußgelder bis zu 35 Mio. EUR oder 7 % des weltweiten Vorjahresumsatzes (je nachdem, welcher Betrag höher ist).	Anbieter, Betreiber (Deployer), Importeure und Händler.	[59]
Hohes Risiko (Hochrisiko-KI)	Systeme zur Zulassung von Personen zu Bildungseinrichtungen, Benotung von Prüfungsleistungen, Bildungspotenzialanalyse (Art. 27), HR-Software für Rekrutierung, biometrische Identifizierung.	Konformitätsbewertung, Risikomanagementsystem, Daten-Governance, technische Dokumentation, menschliche Aufsicht, Grundrechtefolgenabschätzung (Art. 27) für öffentliche Stellen/Betreiber, KI- Schulungspflicht (Art. 4).	02. August 2027 (36 Monate nach Inkrafttreten für Systeme in Anhang II; für Anhang III teilweise früher ab 02. August 2026).	Bußgelder bis zu 15 Mio. EUR oder 3 % des weltweiten Vorjahresumsatzes.	Anbieter (Hauptverantwortung), Betreiber (Deployer - Überwachung & Meldung), Behörden.	[59]

Begrenztes Risiko (Transparenzpflichten)	Chatbots (z. B. ChatGPT am Arbeitsplatz), Deepfakes, Emotionserkennungssysteme, KI-generierte Texte/Bilder.	Transparenzpflicht: Offenlegung, dass eine KI interagiert oder Inhalte erstellt hat (Kennzeichnungspflicht); KI-Schulungspflicht für Mitarbeiter (Art. 4).	02. August 2025 (für Transparenzpflichten und allgemeine KI-Modelle).	Bußgelder bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Vorjahresumsatzes.	Anbieter und Betreiber (Deployer).	[59]
KI-Modelle für allgemeine Zwecke (GPAI)	Basis-Modelle wie GPT-4, Llama, BERT (sofern nicht open-source ohne systemisches Risiko).	Technische Dokumentation, Zusammenfassung der Trainingsdaten, Einhaltung des Urheberrechts, bei systemischem Risiko zusätzlich Modellbewertung und Cybersicherheit.	02. August 2025 (Übergangsfrist für Bestandsmodelle bis 2026/2027 via Digital Omnibus).	Spezifische Bußgelder für Modell-Anbieter durch das EU-KI-Amt (bis zu 3 % des Umsatzes).	Anbieter von KI-Modellen.	[59]
Minimales Risiko	KI-gestützte Spam-Filter, KI-Funktionen in Videospielen.	Keine spezifischen gesetzlichen Verpflichtungen über geltendes Recht hinaus; freiwillige Verhaltenskodizes werden empfohlen.	02. Februar 2025 (Kapitel I & II gelten ab dann).	Keine Sanktionen spezifisch unter dem AI Act (außer allgemeine Rechtsverstöße).	Anbieter (freiwillig).	[59]
Inakzeptables Risiko (Verbotene Praktiken)	Social Scoring, Emotionserkennung am Arbeitsplatz/Bildung, biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum (Strafverfolgung), unterschwellige Beeinflussung, Ausnutzung vulnerabler Gruppen, Predictive Policing, Scraping von Gesichtsbildern.	Vollständiges Verbot der Nutzung innerhalb der EU; KI-Schulungspflicht (Art. 4) zur Sensibilisierung der Mitarbeiter.	02. Februar 2025 (6 Monate nach Inkrafttreten)	Bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer).	[60, 61]

Hohes Risiko (Hochrisiko-KI)	HR-Software (Bewerbersauswahl/Leistungsbewertung), Kreditwürdigkeitsprüfung, Bewertung in Bildungseinrichtungen, kritische Infrastrukturen (Energie, Verkehr), Medizinprodukte, Biometrische Identifikation.	Konformitätsbewertung, Risikomanagementsystem, Daten-Governance, technische Dokumentation, Protokollierung, menschliche Aufsicht, Grundrechtefolgenabschätzung (Art. 27).	August 2026 (allgemein) / August 2027 (für Produkte mit Sicherheitskomponenten /Anhang II).	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Hauptsächlich Anbieter (Compliance-Pflichten) und Betreiber (Überwachung/Nutzung).	[60, 61]
Begrenztes Risiko	Chatbots, Deepfakes, generative KI-Systeme zur Text- und Bildgenerierung, Emotionserkennung (außerhalb verbotener Bereiche).	Transparenzpflichten: Nutzer müssen informiert werden, dass sie mit einer KI interagieren; Kennzeichnungspflicht für KI-generierte Inhalte.	August 2026 (24 Monate nach Inkrafttreten).	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber.	[60, 61]
Minimales Risiko	Spam-Filter, KI-gestützte Videospiele, vorausschauende Wartung (Predictive Maintenance), interne Tools.	Keine spezifischen gesetzlichen Auflagen; Empfehlung zur freiwilligen Einhaltung von Verhaltenskodizes und ethischen Prinzipien.	August 2026 (theoretisch, da keine Pflichten bestehen).	Keine (da keine spezifischen Pflichten).	Anbieter und Betreiber.	[60, 61]
GPAI (KI-Modelle mit allgemeinem Verwendungszweck)	Große Sprachmodelle (LLMs) wie ChatGPT (OpenAI), Mistral, Aleph Alpha.	Technische Dokumentation, Zusammenfassung der Trainingsdaten, Einhaltung des Urheberrechts; bei systemischem Risiko zusätzlich Modellbewertungen und Red Teaming.	02. August 2025 (12 Monate nach Inkrafttreten).	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Entwickler von GPAI-Modellen.	[60, 61]
Verbotene Praktiken	Erstellung von CSAM (Darstellungen des sexuellen	Verbot des Inverkehrbringens und der Verwendung;	02.12.2026 für technische Schutzmaßnahmen.	Bußgeldrahmen laut EU AI Act (im Dokument nicht	Anbieter und Betreiber.	[62]

	Missbrauchs von Kindern), nicht-einvernehmliche sexuelle/intime Inhalte, 'Nudifier'-Apps.	Implementierung technischer Schutzmaßnahmen (Refusal Training, Output-Kontrollen, Inhaltsfilter).		spezifisch beziffert, aber als Sanktionen bei Verstößen adressiert).		
Hohes Risiko (Stand-alone)	Systeme in den Bereichen Beschäftigung (HR-Software), Bildung, kritische Infrastruktur, Strafverfolgung und Kreditwürdigkeitsprüfung (Annex III).	Konformitätsbewertung anhand harmonisierter Standards, Risikomanagement, Dokumentations- und Governance-Frameworks, Registrierung in EU-Datenbank.	02.12.2027 (verschoben durch Digital Omnibus).	Bußgeldrahmen laut EU AI Act (Allgemeine Erwähnung im Kontext der Compliance-Priorität).	Anbieter (Primärpflichten) und Betreiber (Deployer).	[62]
Hohes Risiko (Eingebettet in Produkte)	KI in Medizinprodukten, Spielzeug, Maschinen (Annex I). Hinweis: Maschinen-Produkte teilweise gezielt ausgenommen/delegierte Rechtsakte.	Einhaltung sektoraler Sicherheitsgesetze kombiniert mit KI-spezifischen Anforderungen (z.B. Gesundheitsschutz).	02.08.2028 (verschoben durch Digital Omnibus).	Sanktionen gemäß AI Act und sektoralen Produktvorschriften.	Anbieter der Produkte.	[62]
Spezielles Transparenzrisiko	KI-generierte Inhalte (Bilder, Audio, Video, Text), Chatbots.	Kennzeichnung KI-generierter Inhalte in maschinenlesbarem Format; Information der Nutzer über Interaktion mit KI.	02.08.2026 (Allgemein); 02.12.2026 (Grace Period für Kennzeichnung bei Bestands-Systemen).	Bußgelder bei Nicht-Kennzeichnung/Täuschung.	Anbieter.	[62]
Geringes / Minimales Risiko (Selbstbewertung)	KI-Systeme, die vom Anbieter als Nicht-Hochrisiko eingestuft wurden.	Registrierungspflicht in der EU-Datenbank (leichtgewichtiger Prozess), KI-Schulungspflicht (Art. 4), Datenverarbeitung zur Bias-Erkennung (optionaler Rechtsgrund).	02.08.2026 (Allgemeine Anwendung).	Verwaltungsstrafen bei fehlender Registrierung.	Anbieter (Registrierung) und Betreiber (Schulung).	[62]

General-Purpose AI (GPAI) / Modelle	Basismodelle, die für vielfältige Zwecke eingesetzt werden können; Modelle in sehr großen Online-Plattformen (DSA).	Aufsicht durch das KI-Amt (AI Office), Dokumentationspflichten, Kooperation mit nationalen Behörden.	02.08.2026 (Abhängig von spezifischen Modell-Fristen).	Überwachung und Sanktionierung durch das KI-Amt (AI Office).	Anbieter von GPAI-Modellen.	[62]
Verbotene Praktiken (Unannehmbares Risiko)	Biometrische Identifizierung in Echtzeit im öffentlichen Raum (mit Ausnahmen), Social Scoring, kognitive Verhaltensmanipulation, ungezieltes Auslesen von Gesichtsbildern (Scraping).	Vollständiges Verbot des Einsatzes und Inverkehrbringens innerhalb der EU.	Februar 2025 (6 Monate nach Inkrafttreten)	Bis zu 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber (Deployer)	[63, 64]
Hohes Risiko (Hochrisiko-KI)	Systeme in den Bereichen Bildung (z.B. Prüfungsbewertung), Beschäftigung (HR-Software, Recruiting), kritische Infrastrukturen, Strafverfolgung, Migration.	Risikomanagementsystem, Daten-Governance, technische Dokumentation, Protokollierung (Logging), menschliche Aufsicht, Genauigkeit, Cybersicherheit, Grundrechtefolgenabschätzung (Art. 27).	August 2026 (24 Monate); für Produkte unter EU-Harmonisierungsvorschriften: August 2027 (36 Monate)	Bis zu 15 Mio. EUR oder 3 % des weltweiten Jahresumsatzes.	Anbieter (Primärpflichten), Betreiber (Sicherstellung der bestimmungsgemäßen Verwendung, Überwachung)	[63, 64]
Begrenztes Risiko (Transparenzpflichten)	Chatbots (z.B. ChatGPT für Texte), Deepfakes, Emotionserkennungssysteme, KI-Bildgeneratoren.	Offenlegungspflicht: Nutzer müssen wissen, dass sie mit einer KI interagieren; Kennzeichnungspflicht für KI-generierte Inhalte (Watermarking).	August 2026 (Allgemeine Regelungen); GPAI-Modelle bereits ab Mai 2025	Bis zu 7,5 Mio. EUR oder 1,5 % des weltweiten Jahresumsatzes.	Anbieter und Betreiber	[63, 64]
Minimales Risiko	Spam-Filter, KI-gestützte Videospiele, administrative Hilfswerkzeuge ohne	Keine spezifischen gesetzlichen Pflichten über bestehendes Recht hinaus (z.B. DSGVO); freiwillige	August 2026	Allgemeine Sanktionen bei Nichteinhaltung bestehender Gesetze (z.B. DSGVO-Bußgelder).	Anbieter	[64]

	Personenbezug (z.B. Malvorlagen-Generatoren).	Verhaltenskodizes werden empfohlen.				
Allgemeine Anforderungen (Horizontal)	Alle KI-Systeme im Anwendungsbereich des Gesetzes.	KI-Schulungspflicht (Art. 4): Personal muss über ausreichende KI-Kompetenz verfügen; Einhaltung der DSGVO-Prinzipien (Datensparsamkeit, Zweckbindung).	Februar 2025 (Art. 4 Schulungspflicht)	Abhängig von der Schwere des Versäumnisses und der Risikoklasse des eingesetzten Systems.	Anbieter und Betreiber (insb. Arbeitgeber für Schulungen)	[63, 64]
Verbotene KI-Praktiken (Inferred)	Biometrische Kategorisierung, Social Scoring, kognitive Verhaltensmanipulation (Inferred)	Vollständiges Verbot des Inverkehrbringens und der Nutzung innerhalb der EU (Inferred)	Februar 2025 (6 Monate nach Inkrafttreten) (Inferred)	Bis zu 35 Mio. € oder 7 % des weltweiten Jahresumsatzes (Inferred)	Anbieter und Betreiber (Deployer) (Inferred)	Not in source
Hohes Risiko (High-Risk) (Inferred)	HR-Software zur Bewerberauswahl, KI in der Bildung (Bewertung), kritische Infrastrukturen (Inferred)	KI-Schulungspflicht (Art. 4), Grundrechtefolgenabschätzung (Art. 27), Risikomanagement, Daten-Governance (Inferred)	August 2026 (24 Monate nach Inkrafttreten); August 2027 für Anhang I Produkte (Inferred)	Bis zu 15 Mio. € oder 3 % des weltweiten Jahresumsatzes (Inferred)	Anbieter (Primärpflichten), Betreiber (Überwachungspflichten) (Inferred)	Not in source
Spezielles Transparenzrisiko (GPAI) (Inferred)	Chatbots (z.B. ChatGPT), Deepfakes, Emotionserkennung (Inferred)	Offenlegungspflicht (KI-Kennzeichnung), technische Dokumentation, Zusammenfassung von Trainingsdaten (Inferred)	August 2025 (12 Monate nach Inkrafttreten für GPAI-Modelle) (Inferred)	Bis zu 7,5 Mio. € oder 1,5 % des weltweiten Jahresumsatzes (Inferred)	Anbieter von Allzweck-KI-Modellen (GPAI) (Inferred)	Not in source
Minimales Risiko (Inferred)	Spam-Filter, KI-gestützte Videospiele (Inferred)	Keine spezifischen gesetzlichen Auflagen; freiwillige Verhaltenskodizes (Inferred)	August 2026 (allgemeine Anwendung) (Inferred)	Allgemeine Sanktionen bei Nichteinhaltung geltender EU-Gesetze (Inferred)	Anbieter (Inferred)	Not in source

-
- [1] Künstliche Intelligenz in der Sozialen Arbeit. Grundlagen für Theorie und Praxis - peDOCS
 - [2] AI Act: Regeln für Unternehmen beim Einsatz künstlicher Intelligenz - IHK München
 - [3] AI Act: Regeln für Unternehmen beim Einsatz künstlicher Intelligenz - IHK München
 - [4] Visions of the Machine and Standards of the Human — What the AI Act Really Asks of Us
 - [5] Seminare und Webinare zum Caritas Arbeitsrecht und AVR - Lambertus-Verlag
 - [6] Künstliche Intelligenz (KI) in der Kinder- und Jugendhilfe diakonischer Einrichtungen im Ev. Fachverband Kinder, Jugend und Fam - Diakonie Württemberg
 - [7] EU AI Act - IHK Frankfurt am Main
 - [8] Der EU AI Act in Bildungs- und Betreuungseinrichtungen: Eine wissenschaftliche Analyse regulatorischer Vorgaben, operativer Umsetzungspfade und pädagogischer Implikationen
 - [9] EU AI Act - Regelungen und mögliche Folgen der KI-Verordnung für Schule & Unterricht
 - [10] Handlungsempfehlung für die Bildungsverwaltung zum Umgang mit Künstlicher Intelligenz (KI) in schulischen Bildungsprozessen. - Kultusministerkonferenz (KMK)
 - [11] EU's Digital Omnibus offers AI regulatory relief, but questions remain - PwC
 - [12] AI Act: Das steht in der KI-Verordnung der EU - Lexware
 - [13] EU AI-Act/KI-Verordnung - Universität Tübingen
 - [14] Anhang III: Hochrisiko-KI-Systeme gemäß Artikel 6(2) - EU AI Act
 - [15] EU AI Act für Schulen · KI-Didaktik
 - [16] EU AI-Act/KI-Verordnung - Universität Tübingen
 - [17] Findus One von H24 - WGKD
 - [18] Rechtssicher handeln im digitalen Raum - GEW NRW
 - [19] AI Act has potential to transform children's online experience - 5Rights Foundation
 - [20] KI-Leitfaden – Prüfen und Bewerten - IQES
 - [21] From regulation to innovation: What the EU AI Act means for EdTech - FeedbackFruits
 - [22] EU AI Act: Was Bildungseinrichtungen jetzt wissen müssen - co.Tec GmbH
 - [23] EU AI Act enters into force: A crucial step for child protection - 5Rights Foundation
 - [24] Transparenzoffensive – Tätigkeitsbericht des KDSZ Bayern 2025 - Artikel 91
 - [25] EU AI Act: Wie wird Deutschland KI-kompetent? - KI-Campus
 - [26] KI-Wegweiser - Hopp Foundation
 - [27] Pflichten des EU AI Act - auch für gemeinnützige Träger - Der Paritätische Rheinland-Pfalz
 - [28] Transparenzoffensive „Kita-Qualität“ - Landtag NRW

-
- [29] EU AI Act Omnibus Agreement — Postponed High-Risk Deadlines and Other Key Changes
 - [30] Regulatorische Pflichten, zeitliche Verschiebungen und praktische Handlungsrahmen für Kindertageseinrichtungen unter dem EU AI Act ab August 2026
 - [31] "AI Act" - EU setzt Regeln für den Umgang mit Künstlicher Intelligenz in Kraft
 - [32] Germany AI in Education - International Trade Administration
 - [33] The Digital AI Omnibus: Proposed deferral of high risk AI obligations under the AI Act (update) - DLA Piper GENIE
 - [34] Germany: Recommendation for action on the use of artificial ...
 - [35] Verpflichtungen im AI-Act: KI-Kompetenzen im Unternehmen sichern - IHK Hannover
 - [36] EU AI Act: Was Unternehmen 2026 wissen und tun müssen - reteach
 - [37] Prüfung und Zertifizierung von KI in der Praxis: Herausforderungen und Lösungsansätze
 - [38] EU AI Act: How Well Does it Protect Children and Young People? - LCFI
 - [39] KI kann die Kita unterstützen - aber keine Fachkraft ersetzen - Stiftung Kinder forschen
 - [40] AI Omnibus: deregulation at the expense of fundamental rights - ECNL.org
 - [41] KI in Kitas rechtssicher nutzen: Regeln, Verbote, Praxis-Tipps - Kita Shield – Datenschutz und KI in der Kita
 - [42] Portfolioarbeit in Kitas mit Künstliche Intelligenz - ErzieherIn.de
 - [43] KI in Kitas rechtssicher nutzen: Regeln, Verbote, Praxis-Tipps - Kita Shield – Datenschutz und KI in der Kita
 - [44] Vorschulische Sprachstandsermittlung für alle Hamburger Kinder
 - [45] Children and generative AI - European Parliament
 - [46] Die turnende Rechenmaschine: Roboter im Hort
 - [47] AI Act: Pflichten für Unternehmen - WKO
 - [48] EU's Digital Omnibus on AI: 7 Key Changes You Need to Know - Orrick
 - [49] Künstliche Intelligenz im Bildungssektor: Auswirkungen des EU AI Act | Deloitte Deutschland
 - [50] Kompetenzaufbau gemäß Art. 4 AI Act (KI-VO) - BMDS
 - [51] Handlungsleitfaden für sicheren Einsatz von Ki in ... - evido-magazin
 - [52] Grundrechtefolgenabschätzung - ki-kanzlei.de
 - [53] EU Lawmakers Reach Provisional Agreement to Delay Key EU AI Act Obligations
 - [54] KI in der Kita - Praxisideen | Betzold Blog

-
- [55] AI Act bis Datenschutz: Welche Regelungen es für den KI-Einsatz an ...
 - [56] Infopaket Künstliche Intelligenz - Datenschutz in Sachsen-Anhalt
 - [57] AI Act August 2026: KI-Compliance jetzt richtig strukturieren - Althammer & Kill
 - [58] Digital Omnibus on AI | Legislative Train Schedule - European Parliament
 - [59] Welche Verpflichtungen ergeben sich aus dem AI-Act für Bildungseinrichtungen und Lehrende - Aktuelles - Wb-web.de
 - [60] EU AI Act: Risikoklassifizierung in der KI-Verordnung - trail - AI Governance
 - [61] FAQ: Die wichtigsten Fragen zur KI-Verordnung (AI-Act) - IHK Region Stuttgart
 - [62] EU AI Act unpacked #34: The final Digital Omnibus on AI - Key amendments to the AI Act and their impact on businesses active in the EU | Freshfields
 - [63] KI in der Kita rechtssicher und verantwortlich anwenden - Kitalino
 - [64] KI in der Kita rechtssicher und verantwortlich anwenden - Kitalino