



Leseprobe

Unsere Fachinhalte bieten Ihnen praxisnahe Lösungen, wertvolle Tipps und direkt anwendbares Wissen für Ihre täglichen Herausforderungen.

- ✓ **Praxisnah und sofort umsetzbar:** Entwickelt für Fach- und Führungskräfte, die schnelle und effektive Lösungen benötigen.
- ✓ **Fachwissen aus erster Hand:** Inhalte von erfahrenen Expertinnen und Experten aus der Berufspraxis, die genau wissen, worauf es ankommt.
- ✓ **Immer aktuell und verlässlich:** Basierend auf über 30 Jahren Erfahrung und ständigem Austausch mit der Praxis.

Blättern Sie jetzt durch die Leseprobe und überzeugen Sie sich selbst von der Qualität und dem Mehrwert unseres Angebots!

le oft beide Rechtsbereiche gleichzeitig tangieren. Der EDSA empfiehlt eine engere Verzahnung der Regulatoren, z. B. durch zentrale Kontaktstellen, um eine kohärente Durchsetzung des Rechts zu gewährleisten und den wirtschaftlichen Kontext bei Datenschutzbewertungen besser zu berücksichtigen.

Checkliste: Was Unternehmen tun müssen

- ☐ **Rechtsgrundlage identifizieren:** Welche Rechtsgrundlage ist für die Datenverarbeitung geeignet?
- ☐ **Anonymisierung sicherstellen:** Einsatz von robusten Anonymisierungstechniken
- ☐ **Datensicherheit gewährleisten:** Implementierung von technischen und organisatorischen Maßnahmen
- ☐ **Transparenz schaffen:** Information der betroffenen Personen über die Datenverarbeitung
- ☐ **Dokumentation führen:** Dokumentation aller Schritte und Maßnahmen
- ☐ **Mit Aufsichtsbehörden zusammenarbeiten:** bei Bedarf Beratung einholen und Prüfungen ermöglichen

6.5.3 KI-Verordnung (AI Act) im Überblick

Mit der am 01.08.2024 in Kraft getretenen KI-Verordnung (auch KI-Gesetz oder AI Act genannt)⁸ hat die Europäische Kommission den ersten Rechtsrahmen zur KI weltweit vorgelegt. Das Ziel ist, sicherzustellen, dass KI-Systeme, die auf dem EU-Markt in Verkehr gebracht und in der Union verwendet werden, sicher sind und die Grundrechte sowie Werte der EU wahren. Es soll auch Investitionen und Innovationen im KI-Bereich in Europa anregen.

 Tipp

Die Anforderungen aus dem AI Act sind bis Mitte 2027 umzusetzen und treten abschnittsweise in Kraft. Trotzdem empfiehlt es sich für Unternehmen, sich bereits jetzt mit den für sie relevanten

⁸ Vgl. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202401689 (zuletzt aufgerufen am: 05.02.2026).

Vorgaben der Verordnung zu beschäftigen und zu überprüfen, ob der ggf. bereits erfolgte bzw. geplante Einsatz von KI-Systemen im Unternehmen den Vorgaben aus dem AI Act genügen würde.

Grundsätzlicher Aufbau der KI-Verordnung

Der AI Act folgt einem risikobasierten Ansatz und kategorisiert KI-Systeme in verschiedene Risikoklassen, für die jeweils spezifische Regelungen gelten:

Unannehmbares Risiko

KI-Systeme mit der Klasse unannehmbares Risiko werden vollständig verboten. Dazu gehören

- Systeme zur Manipulation des menschlichen Verhaltens,
- Social-Scoring-Systeme,
- biometrische Echtzeit-Fernidentifikation im öffentlichen Raum (mit wenigen Ausnahmen).

Hohes Risiko

Klassifizierte Hochrisiko-KI-Systeme wie KI

- in kritischer Infrastruktur,
- in Bildung und Berufsausbildung,
- in Beschäftigung und Personalmanagement,
- im Bereich Strafverfolgung und
- KI in Migrations- und Grenzkontrolle.

Systeme müssen vor der Markteinführung eine Konformitätsbewertung durchlaufen und unterliegen strengen Dokumentations-, Überwachungs- und Qualitätsanforderungen.

Begrenztes Risiko

Für bestimmte KI-Systeme mit der Klasse begrenztes Risiko gelten Transparenzpflichten. Dies betrifft z. B. Chatbots, Deepfakes und Emotionserkennungssysteme.

Minimales oder kein Risiko

Die meisten KI-Anwendungen fallen in diese Kategorie und unterliegen keinen spezifischen Regelungen. Zusätzlich enthält die Verordnung spezielle Vorgaben für KI-Modelle mit allgemeinem Verwendungszweck (General Purpose AI).

Die KI-Verordnung legt außerdem Pflichten für verschiedene Akteure wie Anbieter, Nutzer und Importeure fest und sieht Aufsichts- und Durchsetzungsmechanismen vor:

- **Anbieter von KI-Systemen:** Dies umfasst Unternehmen, die KI-Systeme entwickeln, auf den Markt bringen oder in Betrieb nehmen, unabhängig davon, ob sie inner- oder außerhalb der EU ansässig sind.
- **Nutzer von KI-Systemen:** Hierzu zählen Unternehmen und Organisationen, die KI-Systeme in ihrer beruflichen Tätigkeit einsetzen.
- **Importeure und Vertreiber:** Unternehmen, die KI-Systeme in die EU einführen oder innerhalb der EU vertreiben, fallen ebenfalls unter den AI Act.
- **Hersteller von Produkten:** Wenn ein Produkt ein KI-System als Sicherheitskomponente verwendet, muss der Hersteller die Anforderungen der KI-Verordnung erfüllen.

Übergangsfristen

Es gibt unterschiedliche Übergangsfristen der einzelnen Regelungen des AI Acts, die je nach Risikokategorie der KI-Systeme gelten:

- **Verbotene KI-Systeme:** Die Verbote für inakzeptable Risiken gelten nach sechs Monaten nach Inkrafttreten der Verordnung, also seit dem 01.02.2025.
- **GPAI-Modelle:** Die Anforderungen für KI-Modelle mit allgemeinem Verwendungszweck (GPAI) sind seit dem 01.08.2025 gültig.

 Tipp

GPAI-Modelle (General Purpose AI Models)⁹ weisen folgende Hauptmerkmale auf:

- Sie besitzen eine erhebliche allgemeine Verwendbarkeit und können ein breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen.
- Sie können in eine Vielzahl von nachgelagerten KI-Systemen oder -Anwendungen integriert werden.
- Typischerweise werden sie auf Basis enormer Datenmengen trainiert.

GPAI-Modelle wie GPT-5, DALL-E, Google BERT oder Midjourney 5.2 stellen aufgrund ihrer Flexibilität und Leistungsfähigkeit einen wesentlichen Bestandteil der KI-Wertschöpfungskette dar. Ihre Regulierung im AI Act zielt darauf ab, potenzielle Risiken zu adressieren und gleichzeitig Innovation zu ermöglichen:

- GPAI-Modelle werden in solche mit und ohne systemisches Risiko unterschieden.
 - Anbieter von GPAI-Modellen müssen bestimmte Pflichten erfüllen, wie z. B. das Erstellen technischer Dokumentation und die Bereitstellung von Informationen für nachgelagerte Anbieter.
 - Für GPAI-Modelle mit systemischem Risiko gelten zusätzliche Anforderungen wie Modellbewertungen und Risikominierungsmaßnahmen.
-
- **Hochrisiko-KI-Systeme in Annex II des AI Acts:** Deren Anforderungen werden 24 Monate nach Inkrafttreten der Verordnung, also ab dem 01.08.2026 gültig sein.
 - **Hochrisiko-KI-Systeme in Annex I des AI Acts:** Die Anforderungen für Hochrisiko-KI-Systeme aus Annex I sind 36 Monate nach Inkrafttreten der Verordnung und damit ab dem 01.08.2027 umzusetzen.

⁹ Leitlinien und Praxishilfen der Bundesnetzagentur dazu sind abrufbar unter: www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/3_Modelle/start.html?r=1 (zuletzt aufgerufen am: 05.02.2026).

Ineinandergreifen von DSGVO und AI Act

■ Neu

Die Risikobewertung nach dem AI Act kennzeichnet nicht automatisch die Betrachtung aller Risiken in Bezug auf Datenschutz. Aus diesem Grund empfiehlt sich ein schrittweises Vorgehen.

Am Anfang jeder KI-Anwendung muss, wie bei der Erstellung des Verarbeitungsverzeichnisses, der Zweck der Anwendung klar beschrieben sein. Die Zweckdefinition ist ausschlaggebend für die Risikobewertung.

Tipp

Umfangreiche KI-Modelle können zu unterschiedlichen Zwecken eingesetzt werden. ChatGPT zur Unterstützung von Marketingtexten für LinkedIn oder Werbeanzeigen birgt sicherlich ein geringeres Risiko als die Nutzung von ChatGPT in der Personalentwicklung.

Aus diesem Grund ist es zwingend, die Bewertung nicht auf ein IT- bzw. KI-System zu forcieren, sondern auf den Zweck der Datenverarbeitung. Hier gelten sehr ähnliche Regeln wie bei der Erstellung des Verarbeitungsverzeichnisses. Das IT-System ist „nur“ die ausführende Instanz, der Zweck der Verarbeitung kennzeichnet die Risiken.

Ist der Zweck beschrieben, kann eine Risikoklassifizierung nach dem AI Act erfolgen¹⁰. Die Verordnung gibt verschiedene Zweckklassen vor. Je nach zutreffendem Einsatzgebiet entscheidet sich, von welcher Risikoklasse nach dem AI Act man spricht. Bei dieser Einstufung erfolgt aber keine Bewertung hinsichtlich der verarbeiteten Daten für diesen Zweck. Werden keine personenbezogenen Daten oder sogar besonders schützenswerte Daten verarbeitet, wird hier nicht gefragt. Daher ist es notwendig, nach dieser Risiko-

¹⁰ Vgl. <https://regina-stoiber.com/risikoklassifizierung-nach-dem-ai-act-ki-verordnung/ki-klassifizierung-ki-risikoklasse-ermitteln-self-check/> (zuletzt aufgerufen am: 05.02.2026).

klassifizierung auch zu bewerten, ob eine Datenschutz-Folgenabschätzung notwendig ist.

6.5.4 KI-Kompetenz

Seit dem 02.02.2025 gibt es eine spezielle Vorgabe zur Vermittlung von KI-Kompetenz: Gemäß Art. 4 AI Act müssen Anbieter und Betreiber von KI-Systemen ab diesem Datum sicherstellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit KI-Systemen arbeiten, über ein ausreichendes Maß an KI-Kompetenz verfügen. Diese umfasst dabei

- ein Grundverständnis der Funktionsweise von KI,
- Kenntnisse über Chancen und Risiken von KI-Systemen,
- Fähigkeiten zum verantwortungsvollen Umgang mit KI sowie
- grundlegende Kenntnisse über die Regelungen des AI Acts.

Tipp

Der genaue Umfang der erforderlichen Kompetenz richtet sich nach der Art des KI-Systems, dem technischen Wissen der Mitarbeitenden und dem Nutzungskontext. Unternehmen können die KI-Kompetenz durch verschiedene Maßnahmen vermitteln, u. a. durch interne Schulungen oder Workshops, qualifizierte externe E-Learning-Kurse, Erstellung eines Schulungsplans oder durch Implementierung eines Verhaltenskodex für den Umgang mit KI.

6.5.5 Regelungen im Unternehmen zum KI-Einsatz

■ Neu

Sehr häufig hört man von der Empfehlung, eine KI-Richtlinie im Unternehmen einzuführen. Die Bezeichnung „KI-Richtlinie“ ist sehr generisch und schießt in den meisten Fällen über das Ziel hinaus. Viele neu erstellte KI-Richtlinien erweisen sich als unzureichend

Bestelloptionen



Datenschutz 2026

Sie haben Fragen zum Produkt oder benötigen Unterstützung bei der Bestellung? Unser Kundenservice ist für Sie da:

☎ 08233 / 381-123 (Mo - Do 7:30 - 17:00 Uhr, Fr 7:30 - 15:00 Uhr)

✉ service@forum-verlag.com

Oder bestellen Sie bequem über unseren Online-Shop:

Jetzt bestellen