48. Jahrgang

datenschutz-berater.de

DSB 09/2024

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

ISSN 0170-7256

dfv Mediengruppe

Dr. Thomas Schwenke

Einführung KI-Verordnung: Grundlagen, Begriffe und Pflichtenkatalog

Mit der KI-Verordnung der EU (abgekürzt „KI-VO", englisch: „AI Act") hat die Europäische Union eine Vorreiterrolle bei der Regulierung der Entwicklung und Nutzung Künstlicher Intelligenz übernommen. Die Verordnung betrifft als produktbezogenes Gesetz, bis auf die persönliche Nutzung, alle Akteure, die KI einsetzen oder entwickeln, seien es Unternehmen, Selbständige oder Behörden. Die Bedeutung der KI-VO wird unter anderem durch die hohen Sanktionen unterstrichen, die für Anbieter von KI-Systemen bis zu 35 Millionen Euro oder bis zu 7 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist, betragen können.

Zweck und Notwendigkeit der KI-VO

Die KI-VO regelt umfassend die Entwicklung, den Vertrieb und den Einsatz von Künstlicher Intelligenz innerhalb der Europäischen Union. Ihr Hauptziel besteht darin, vertrauenswürdige KI-Systeme zu fördern und gleichzeitig ein sicheres sowie innovationsfreundliches Umfeld zu gewährleisten. Dabei soll die KI-VO den typischen Risiken der KI-Nutzung begegnen, zu denen insbesondere Diskriminierung und Bias, Datenschutzverletzungen, Sicherheitsrisiken, Verlust menschlicher Autonomie, Mangel an Transparenz sowie Fehlfunktionen und Fehler zählen.

Die KI-VO umfasst Regelungen, die für alle Arten von KI gelten (beispielsweise die Verpflichtung zur Sicherstellung einer KI-Kompetenz gemäß Art. 4 KI-VO), ebenso wie strenge Vorschriften für Hochrisiko-KI-Systeme, etwa im Beschäftigungskontext, und Verbote für bestimmte KI-Praktiken wie das Social Scoring.

Definition von KI-Systemen und KI-Modellen

Die KI-VO stützt sich auf die OECD-Definition von KI und versteht darunter ein maschinengestütztes, autonomes System, das nach Einführung anpassungsfähig ist und Eingaben zu Vorhersagen, Inhalten, Empfehlungen oder Entscheidungen verarbeitet, die physische oder virtuelle Umgebungen beeinflussen können.

Statt allgemein von „KI" zu sprechen, verwendet die KI-VO den spezifischen Begriff „KI-System", um die konkrete Anwendung und deren Auswirkungen auf Menschen und Umwelt zu betonen.

Zusätzlich verwendet die KI-VO den Begriff „KI-Modell" (z. B. im Art. 3 Nr. 63), der sich auf den Algorithmus bezieht, der durch Training die Denkweise einer KI formt und ihre Arbeitsweise bestimmt. Beispiele dafür sind Large Language Models (LLMs) wie „GPT", „LLAMA" oder „Claude", die als Grundlage für KI-Systeme wie ChatGPT oder Microsofts Copilot dienen.

Risikokategorien und Klassifikationen

Die KI-VO basiert auf einer differenzierten Risikobetrachtung und unterteilt den Einsatz von KI in verschiedene Risikokategorien:

- Unannehmbares Risiko – Verbotene KI-Praktiken: KI-Praktiken, die als unannehmbar risikoreich eingestuft werden, sind vollständig verboten. Hierzu zählen etwa KI-Anwendungen, die Menschen manipulieren oder kriminelles Verhalten aufgrund persönlicher Merkmale vorhersagen.
- Hohes Risiko – KI-Systeme, die ein hohes Risiko darstellen, unterliegen strengen Vorschriften. Diese umfassen Anforderungen an die Datenqualität, Dokumentation und Transparenz sowie regelmäßige Prüfungen und Überwachungen. Beispiele hierfür sind KI-Systeme im Gesundheitswesen für Diagnosezwecke oder zur Beurteilung von Bewerbern und Beschäftigten.
- KI-Systeme mit begrenztem Risiko – Systeme mit begrenztem Risiko müssen spezifische Transparenzanforderungen erfüllen. Benutzer müssen darüber informiert werden, dass sie mit einer KI interagieren, und in der Lage sein, deren Entscheidungen nachzuvollziehen. Beispiele hierfür sind Chatbots im Kundensupport oder Deepfakes.
- KI-Systeme mit minimalem Risiko – Für KI-Anwendungen, die ein minimales Risiko darstellen, gelten, abgesehen von der Pflicht zur Sicherstellung einer KI-Kompetenz, keine spezifischen regulatorischen Anforderungen. Dies betrifft etwa KI-Anwendungen zur Spamerkennung oder deren Einsatz in Videospielen.
- KI-Modelle mit allgemeinem Verwendungszweck – Diese Modelle, die für eine Vielzahl von Anwendungen genutzt werden und je nach Einsatzbereich in alle vorgenannten Kategorien fallen können, unterliegen spezifischen Anforderungen, um ihre Sicherheit und Zuverlässigkeit sicherzustellen. Dies umfasst Maßnahmen zur Gewährleistung der Robustheit, Genauigkeit und Fairness der Modelle sowie klare Vorgaben zur Transparenz und Nachvollziehbarkeit der Entscheidungen. Beispiele sind generative Sprachmodelle wie GPT-4.0 oder Claude 3.5.

Anwendungsbereich der KI-VO

Die KI-VO gilt – ähnlich wie die Datenschutz-Grundverordnung (DSGVO) – gem. Art. 2 KI-VO nicht nur für KI, die in der EU entwickelt, vermarktet und eingesetzt wird, sondern auch dann, wenn der KI-Output in der EU Auswirkungen hat.

Die Akteure – Wer die KI-VO beachten muss

Die KI-VO müssen praktisch alle Personen, Unternehmen oder Behörden beachten, die KI-Systeme und Modelle entwickeln, vertreiben oder einsetzen. Der Unterschied besteht im Umfang der Pflichten, die auf die einzelnen Akteure zukommen (Art. 3 Nr. 3-7 KI-VO):

- Anbieter – „Anbieter" ist jedermann, sei es eine einzelne Person, ein Unternehmen oder eine Behörde, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder in Betrieb nimmt. Beispiel: OpenAI (ChatGPT), Google (Gemini).
- Einführer – Einführer führen KI-Systeme aus Nicht-EU-Ländern in die EU ein. Sie müssen überprüfen, ob die importierten Systeme den europäischen Vorschriften entsprechen, und sicherstellen, dass diese Systeme ordnungsgemäß dokumentiert und rechtskonform sind. Wer insbesondere Hochrisiko-KI-Systeme von KI-Systemen, die von Nicht-EU-Anbietern angeboten werden, in der EU/EWR zur Verfügung stellt, muss sicherstellen, dass die Anbieter die gleichen wie für EU-Anbieter geltenden Pflichten erfüllen (z. B. dass das Konformitätsbewertungsverfahren gemäß Art. 43 KI-VO durchgeführt wurde und entsprechende Dokumentation vorhanden ist, Art. 23 KI-VO).
- Händler – Händler vertreiben KI-Systeme innerhalb der EU. Händler müssen entsprechend Art. 24 KI-VO prüfen, ob KI-Systeme außerhalb der EU/EWR mit der erforderlichen CE-Kennzeichnung versehen sind und ob eine Kopie der in Art. 47 genannten EU-Konformitätserklärung und Betriebsanleitungen beigefügt ist.
- Betreiber – Als „Betreiber" werden alle bezeichnet, die ein KI-System in eigener Verantwortung verwenden, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet. Betreiber müssen die Systeme gemäß den Anweisungen des Anbieters nutzen, die Sicherheitsstandards einhalten, die Leistung der Systeme überwachen und bei Problemen die entsprechenden Behörden informieren.
- Bevollmächtigte – „Bevollmächtigte" sind EU-ansässige Vertreter eines Nicht-EU-Anbieters eines KI-Systems oder eines KI-Modells, die für die Anbieter die Pflichten der KI-VO wahrnehmen.

Diese Rollen und Abgrenzungen können jedoch fließend sein und sich überschneiden. So kann ein Unternehmen, das zunächst eine fremde KI-Software lediglich betreibt, zum Anbieter werden, wenn es diese weiterentwickelt und auf dem Markt bereitstellt.

Nutzung von KI durch Privatpersonen

Die KI-VO gilt nicht für den Betrieb von KI-Systemen im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit. Gemeint ist damit eine KI-Nutzung, die in Entsprechung zu der sog. „Haushaltsausnahme" im Art. 2 Abs. 2 lit. c DSGVO Dritte nicht beeinträchtigt und auf einen engen persönlichen und nicht-öffentlichen Personenkreis beschränkt ist.

Verbotene KI-Praktiken

Die KI-VO verbietet das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das zu folgenden Zwecken eingesetzt wird oder die genannten Wirkungen hat (Art. 5 KI-VO)

- Erhebliche Schäden verursachende Verhaltensänderung und Entscheidungsbeeinflussung – Untersagt werden KI-Praktiken, die das Verhalten einer Person oder einer Gruppe so wesentlich verändern, dass sie Entscheidungen treffen, die ihnen erheblichen Schaden zufügen könnten. Verboten ist hierbei insbesondere die a) Unterschwellige Beeinflussung, d. h. der Einsatz von Techniken der unterschwelligen Beeinflussung oder absichtlich manipulativer oder täuschender Techniken sowie b) die Ausnutzung von Schwächen oder Schutzbedürftigkeit, d. h. die gezielte Ansprache von Personen oder Gruppen aufgrund von Alter, Behinderung oder sozialer und wirtschaftlicher Situation.
- Soziale Bewertung („Social Scoring") – KI-Systeme zur Bewertung von Personen oder Gruppen über einen bestimmten Zeitraum basierend auf ihrem Sozialverhalten oder persönlichen Eigenschaften, wenn dies zu ungerechtfertigter Benachteiligung führt.
- Vorhersage krimineller Aktivitäten – KI-Systeme zur Bewertung oder Vorhersage des Risikos, dass eine Person eine Straftat begeht, basierend auf Profiling und Persönlichkeitsmerkmalen.
- Gesichtserkennungsdatenbanken – KI-Systeme, die Gesichtserkennungsdatenbanken durch ungezieltes Auslesen von Bildern aus dem Internet oder Überwachungskameras erstellen oder erweitern.
- Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen – KI-Systeme zur Ableitung von Emotionen am Arbeitsplatz oder in Bildungseinrichtungen, außer sie werden aus medizinischen oder sicherheitstechnischen Gründen eingesetzt.
- Biometrische Überwachung – Verboten ist die biometrische Identifizierung in der Öffentlichkeit zu Strafverfolgungszwecken, außer in konkreten Gefahrenlagen.
- Biometrische Kategorisierung – KI-Systeme, die Personen auf Grundlage biometrischer Daten kategorisieren, um Rückschlüsse auf Rasse, politische Meinungen, Ge-

werkschaftszugehörigkeit, religiöse Überzeugungen, Sexualleben oder sexuelle Orientierung zu ziehen.

In der unternehmerischen Praxis sind die Verbote insbesondere im Personalmanagement (z. B. Emotionserkennung) oder im Marketing (unterschwellige Beeinflussung und Ausnutzen von Schwächen) von Relevanz. Beschäftigte, die in diesen Bereichen tätig sind, sollten in jedem Fall über diese Verbote informiert und auf deren Einhaltung verpflichtet werden.

Hochrisiko-KI-Systeme

Das Meiste der Pflichten in der KI-VO betreffen sog. „Hochrisiko-KI-Systeme".

Vorliegen eines Hochrisiko-KI-Systems

Zum einem wird ein KI-System als Hochrisiko eingestuft, wenn es ein Produkt oder eine Sicherheitskomponente eines Produkts ist, die unter EU-Harmonisierungsvorschriften fallen, wie z. B. medizinische Geräte, industrielle Maschinen, Spielzeug, Flugzeuge oder Autos (Art. 6 Abs. 1 i. V. m. Anhang I KI-VO). Gemäß Art. 6 Abs. 2 KI-VO wird ein KI-System zudem als Hochrisiko eingestuft, wenn es in einem der in Anhang III gelisteten „hochriskanten" Einsatzbereiche verwendet wird. Zu diesen gehören:

- Biometrie: Biometrische Fernidentifizierung (z. B. Gesichtserkennung in öffentlichen Bereichen), biometrische Kategorisierung (sofern nicht nach Art. 45 KI-VO verboten), und Emotionserkennung, z. B. am Arbeitsplatz.
- Kritische Infrastruktur: Verwaltung und Betrieb kritischer digitaler Infrastruktur, z. B. Straßenverkehr, Wasser-, Gas-, Wärme- oder Stromversorgung.
- Bildung: Zulassung und Bewertung in Bildungseinrichtungen.
- Beschäftigung und Personalmanagement: Einstellungen, Beförderungen und Kündigungen, z. B. KI-gestützte Bewerberauswahl.
- Grundlegende Dienste: Kreditwürdigkeitsprüfungen und Risikobewertungen bei Versicherungen.
- Strafverfolgung: Einsatz von Lügendetektoren und Vorhersage zukünftiger Straftaten.
- Migration und Grenzkontrolle: Prüfung von Asyl- und Visumanträgen sowie Sicherheitsrisikobewertungen.
- Rechtspflege und Demokratie: Analyse von Beweismitteln und Überwachung von Wahldaten.

Anforderungen an Anbieter von Hochrisiko-KI-Systemen

Wird der Einsatz eines KI-Systems durch die KI-VO als Hochrisiko-KI-System eingestuft, sind für dessen Anbieter zahlreiche Pflichten zu beachten (Art. 6 bis 49 KI-VO):

- Risikomanagementsystem (Art. 9 KI-VO)
- Datengovernance und Datenmanagement (Art. 10 KI-VO)
- Technische Dokumentation und Protokollierung (Art. 11, 12 KI-VO)
- Transparenzanforderungen (Art. 13 KI-VO)
- Menschliche Aufsicht (Art. 14 KI-VO)
- Genauigkeit, Robustheit und Cybersicherheit (Art. 15 KI-VO)
- Korrekturmaßnahmen und Informationspflichten (Art. 20 KI-VO)
- Konformitätsbewertung (Art. 43 KI-VO)
- Zertifizierung und CE-Kennzeichnung (Art. 49 KI-VO).

Anforderungen an Betreiber von Hochrisiko-KI-Systemen

In der Praxis erstellen oder bieten nur wenige Unternehmen selbst Hochrisiko-KI-Systeme an. Häufiger beziehen sie derartige Leistungen, wie etwa biometrische Systeme, von spezialisierten Anbietern. Als Betreiber eines solchen KI-Systems obliegt es ihnen nicht, die Grundlagen des Systems zu prüfen. Jedoch sind bestimmte Pflichten im Rahmen der Implementierung und des Betriebs des KI-Systems zu erfüllen (Art. 26 KI-VO):

- Verwendung entsprechend der Betriebsanleitung und technische sowie organisatorische Sicherheitsmaßnahmen
- Kompetente Aufsicht (KI-Beauftragte)
- Datenkontrolle entsprechend Zweckbestimmung
- Überwachung und Berichterstattung
- Protokollaufbewahrung
- Information der Arbeitnehmer
- Registrierungspflichten
- Datenschutz-Folgenabschätzung.

Anforderungen an Entwickler von KI-Modellen mit allgemeinem Verwendungszweck

KI-Modelle mit allgemeinem Verwendungszweck sind vielseitige Modelle, die in verschiedenen Anwendungen genutzt werden können, wie z. B. GPT-4 für Textgenerierung, Übersetzung und Fragenbeantwortung. Da mit diesen KI-Modellen betriebene KI-Systeme generell in alle Risikokategorien der KI-VO fallen können, enthält die KI-VO spezielle Regeln, die bereits deren Entwickler beachten müssen (Art. 51-56 KI-VO).

Transparenzanforderungen an alle KI-Systeme

Auch wenn der Einsatz eines KI-Systems weder eine verbotene KI-Praxis darstellt noch es sich um ein Hochrisiko-KI-System handelt, sind dennoch die für alle KI-Systeme geltenden Pflichten zu beachten (Art. 50 KI-VO).

Transparenzpflichten bei Interaktion

Anbieter von KI-Systemen müssen sicherstellen, dass natürliche Personen informiert werden, wenn sie mit einem KI-System interagieren, es sei denn, dies ist offensichtlich.

Kennzeichnung von KI-Ergebnissen

Anbieter von KI-Systemen müssen sicherstellen, dass Ausgaben des KI-Systems in einem maschinenlesbaren Format gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind. Alle KI-Ergebnisse müssen in den Meta-Daten als solche gekennzeichnet werden.

Kennzeichnungspflicht bei Deepfakes

Als „Deepfakes" bezeichnet die KI-VO (Art. 3 Nr. 60 KI-VO), „einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde." Deepfakes sind also Bilder oder Videos, die dann entstehen, wenn Sie von der KI verlangen, dass die Ergebnisse fotorealistisch oder „wie echt" erscheinen sollen. Dabei ist es nicht erforderlich, dass mit Deepfakes eine Täuschungs- oder Irreführungsabsicht verfolgt wird. Deepfakes müssen immer als KI-Erzeugnisse gekennzeichnet werden (Art. 50 Abs. 4 KI-VO). Ansonsten droht ein Bußgeld (Art. 99 Abs. 4 lit. g KI-VO) und falls reale Personen abgebildet werden bei abträglichen Deepfakes eine Strafbarkeit wegen Verleumdung (§ 187 StGB).

Pflicht zur KI-Kompetenz

Die Gesetzgebung fordert generell die Sicherstellung der KI-Kompetenz (Art. 4 KI-VO), verstanden als das Zusammenspiel von Fähigkeiten, Kenntnissen und Verständnis (Art. 3 Nr. 56 KI-VO), um KI-Systeme sachkundig einzusetzen. Dies umfasst auch das Bewusstsein für Chancen, Risiken und mögliche Schäden durch KI. Vor der Einführung von KI in einer Organisation muss sichergestellt werden, dass Mitarbeiter die nötigen Kenntnisse besitzen. Anderenfalls haften verantwortliche Personen, wie Geschäftsführer, persönlich.

Verhältnis der KI-VO zur DSGVO

Die KI-VO und die DSGVO ergänzen sich, da sie unterschiedliche, aber verknüpfte Aspekte der Nutzung von KI-Systemen regeln (Art. 2 Abs. 7 KI-VO). Solange keine Hochrisiko-KI-Systeme eingesetzt werden, bleibt die DSGVO für Betreiber meist zentral. KI-Systeme, die personenbezogene Daten verarbeiten, sollten im Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO erfasst werden. Betroffene Personen müssen in den Datenschutzhinweisen gemäß Art. 12 Abs. 1, 13 und 14 DSGVO über die Anbieter von KI-Systemen als Datenempfänger informiert werden.

Sanktionen bei Verstoß gegen die KI-VO

Die KI-VO sieht ein dreistufiges Sanktionskonzept vor, das abhängig von der Schwere des Verstoßes verschiedene Bußgelder vorsieht (Art. 99 Abs. 3 bis 5 KI-VO). Dabei wird die Höhe der Sanktionen im Verhältnis zur Größe und dem Umsatz des betroffenen Unternehmens bestimmt, wobei die Sanktionen sowohl abschreckend wirken als auch eine gewisse Angemessenheit wahren sollen.

Die Sanktionen gliedern sich wie folgt:

1. 35 Millionen Euro oder 7 % des weltweiten Jahresumsatzes, je nachdem, was höher ist – Dieses höchste Bußgeld droht, wenn verbotene KI-Systeme gemäß Art. 5 der KI-VO eingesetzt werden oder die Qualitätskriterien für verwendete Daten bei Hochrisiko-KI-Systemen gemäß Art. 10 der KI-VO nicht erfüllt werden.
2. 15 Millionen Euro oder 3 % des weltweiten Jahresumsatzes, je nachdem, was höher ist – Dieses Bußgeld wird beispielsweise fällig, wenn Hochrisiko-KI-Systeme ohne die erforderlichen technischen und organisatorischen Maßnahmen eingesetzt werden, keine KI-Beauftragten bestimmt werden oder Deepfakes nicht gekennzeichnet sind.
3. 7,5 Millionen Euro oder 1 % des weltweiten Jahresumsatzes, je nachdem, was höher ist – Diese Sanktion droht bei der Übermittlung falscher Informationen an die zuständigen Stellen oder Behörden.

Diese Sanktionen sind so ausgestaltet, dass sie je nach Schwere des Verstoßes angepasst werden können und dabei sowohl abschreckend wirken als auch die wirtschaftliche Leistungsfähigkeit der Sanktionsadressaten berücksichtigen.

Für kleine und mittlere Unternehmen (KMUs) sowie Start-Ups gilt gemäß Art. 99 Abs. 6 KI-VO, dass der jeweils niedrigere Betrag aus den in den Absätzen 3, 4 und 5 genannten Prozentsätzen oder Summen als Bußgeld verhängt wird.

Zuständige Behörden für die Durchsetzung der KI-VO

Die KI-Verordnung (KI-VO) etabliert einen umfassenden Ordnungsrahmen für eine einheitliche und koordinierte Umsetzung. Auf europäischer Ebene dienen das Europäische Amt für künstliche Intelligenz (zuständig für die Marktüberwachung von KI-Modellen mit allgemeinem Verwendungszweck), das Europäische Gremium für Künstliche Intelligenz, das Beratungsforum und ein wissenschaftliches Gremium unabhängiger Sachverständiger primär Beratungs- und Koordinierungszwecken. Auf nationaler Ebene muss jeder Mitgliedstaat eine Überwachungsbehörde benennen, um die Einhaltung der KI-VO sicherzustellen. In Deutschland ist die zuständige Behörde noch unklar, jedoch zeigen die Datenschutzbehörden Interesse an dieser Aufgabe.

Zeitliche Geltung der KI-VO

Die KI-VO trat am 2. August 2024 in Kraft und setzt verschiedene Umsetzungsfristen fest, insbesondere:

- 2. Februar 2025 – Verbot bestimmter KI-Praktiken; Nachweis KI-Kompetenz erforderlich.

- 2. August 2026 – Vollständige Wirksamkeit der KI-VO, einschließlich Vorschriften für Hochrisiko-KI-Systeme.
- 2. August 2027 – Inkrafttreten der Vorschriften für Hochrisiko-KI-Systeme gemäß Anhang I.

Fazit – Kombinierte Compliance mit KI-VO und DSGVO

Da KI zunehmend in alle Bereiche des Geschäftslebens integriert wird, ist die Prüfung der KI-VO ebenso notwendig wie die der DSGVO. Die Prüfung kann oft mit der DSGVO beginnen, da deren Einhaltung in der Regel auch die Anforderungen der KI-VO erfüllt. Es ist jedoch zu beachten, dass nicht alle nach der KI-VO erlaubten Verfahren automatisch DSGVO-konform sind.

Autor: **Dr. Thomas Schwenke, LL.M. commercial (Auckland), Dipl.FinWirt (FH), ist Rechtsanwalt in Berlin, berät international Unternehmen im Marketing- sowie Datenschutzrecht, podcastet unter Rechtsbelehrung.com und ist Betreiber der Plattform Datenschutz-Generator.de.**