

Pflichten als Anbieter eines KI-Systems nach der KI-Verordnung

Was Anbieter von KI-Systemen nach der KI-Verordnung jetzt beachten müssen

Mit der europäischen KI-Verordnung (KI-VO) erhalten Unternehmen, die KI-Systeme entwickeln oder entwickeln lassen und unter dem eigenen Namen/unter der eigenen Marke in Verkehr bringen oder in Betrieb nehmen, einen klaren rechtlichen Rahmen. Für den sog. Anbieter des KI-Systems hängen Umfang und Tiefe der Pflichten maßgeblich davon ab, in welche Risikokategorie das jeweilige KI-System fällt: Verbotene KI-Praktiken, Hochrisiko-KI-Systeme, KI-Systeme mit Transparenzrisiken oder KI-Systeme mit lediglich minimalen Risiken.

Dieses Infoschreiben ordnet die Rolle des Anbieters nach der KI-VO ein, zeigt die wesentlichen Pflichtenkreise nach der KI-VO auf und macht deutlich, warum Rollenprüfung und Risikoklassifizierung zentrale Voraussetzungen für eine belastbare KI-Compliance sind. Wegen der Umsetzungsfristen der jeweiligen Pflichten verweisen wir auf unsere Handlungshilfe „Die KI-Verordnung nach dem KI-Omnibus“.

1 Wer ist Anbieter eines KI-Systems?

Die KI-VO versteht unter einem „Anbieter“ (Art. 3 Nr. 3 KI-VO) jede natürliche oder juristische Person, Behörde oder sonstige Stelle, die

- ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und
- dieses KI-System unter eigenem Namen oder eigener Marke in Verkehr bringt oder in Betrieb nimmt – entgeltlich oder unentgeltlich.

Wesentlich ist damit nicht nur die technische Entwicklung, sondern insbesondere der Marktauftritt: Wer gegenüber Kundinnen, Kunden oder Beschäftigten als „eigener“ KI-Anbieter erscheint, kann in die Anbieterrolle nach der KI-VO geraten – auch wenn zugrundeliegende KI-Modelle (also die eigentlichen technischen Herzstücke) von Dritten stammen.

Praxisbeispiele:

- Ein Unternehmen entwickelt ein eigenes KI-System zur Qualitätskontrolle in der Produktion, versieht es mit dem eigenen Markennamen und vertreibt es an andere Unternehmen: Das Unternehmen ist Anbieter dieses KI-Systems.
- Ein Unternehmen integriert externe KI-APIs (z. B. von großen Cloud-Anbietern) in eine eigene Kundenplattform und vermarktet diese Plattform als „eigene KI-Lösung“: Auch hier kann eine Anbieterrolle bestehen, obwohl das KI-Modell nicht selbst entwickelt wurde.
- Ein Unternehmen lizenziert eine „White-Label“-Lösung und nimmt das KI-System mit der unternehmenseigenen Marke/ dem unternehmenseigenen Logo in Betrieb. In dieser Konstellation werden die Fallstricke besonders deutlich, da sogar das bloße Anbringen des eigenen Logos ausreichen kann, um in die Rolle des Anbieters zu schlüpfen.

Im Regelfall tritt ein Unternehmen als Anbieter immer dann auf, wenn es ein KI-System aktiv in den Markt bringt oder im eigenen Namen bereitstellt.

2 Wonach richten sich die Anbieter-Pflichten?

Die KI-VO folgt einem risikobasierten Ansatz. Je mehr Risiken vom Einsatz eines KI-Systems ausgehen (können), desto mehr Compliance-Anforderungen müssen beachtet werden. Für Anbieter von KI-Systemen ist daher in jedem Einzelfall zu unterscheiden, in welche Risikoklasse das jeweilige KI-System fällt:

- Verbotene KI-Praktiken (Art. 5 KI-VO) – keine Pflichten, da verboten;
- Hochrisiko-KI-Systeme (Art. 6 KI-VO i. V. m. Anhängen I und III) – umfangreicher Pflichtenkatalog;
- KI-Systeme mit Transparenzrisiken (Art. 50 KI-VO) – einzelfallbezogene Pflichten;
- KI-Systeme mit minimalen Risiken – keine gesonderten Pflichten.

Darüber hinaus gibt es organisationsbezogene Vorgaben (unabhängig von der Risikoklasse), die v.a. die Förderung der KI-Kompetenz nach Art. 4 KI-VO adressieren und in jedem Fall Teil des Pflichtenprogramms sind.

Für Unternehmen ist daher zu prüfen, ob Pflichten für Anbieter von Hochrisiko-KI-Systemen (Ziffer 3.) und/oder Pflichten für Anbieter von KI-Systemen mit Transparenzrisiken (Ziffer 4.) einschlägig sind und wie Pflichten für alle Anbieter von KI-Systemen (Ziffer 5.) umgesetzt werden können.

3 Pflichten für Anbieter von Hochrisiko-KI-Systemen

Sofern ein KI-System als Hochrisiko-KI-System eingestuft wird (z. B. KI als reguliertes Produkt oder Sicherheitsbauteil mit Dritt-Konformitätsbewertung nach Anhang I oder KI-Systeme in sensiblen Anwendungsbereichen nach Anhang III), gilt für Anbieter ein umfassender Pflichtenkatalog.

Kernpflichten für Anbieter von Hochrisiko-KI-Systemen sind insbesondere:

- **Risikomanagementsystem (Art. 9 KI-VO)**
Kontinuierlicher, iterativer Prozess zur Identifikation, Bewertung und Minimierung von Risiken über den gesamten Lebenszyklus des KI-Systems.
- **Datenqualität (Art. 10 KI-VO)**
Einsatz geeigneter Trainings-, Validierungs- und Testdaten mit klaren Qualitätskriterien (z. B. Repräsentativität, Fehlerarmut, Umgang mit Bias).
- **Technische Dokumentation (Art. 11 KI-VO)**
Erstellung vor Inverkehrbringen oder Inbetriebnahme; Nachweis, dass das KI-System sämtliche Anforderungen für Hochrisiko-KI erfüllt.
- **Protokollierung (Art. 12 KI-VO)**
Implementierung automatisierter Logging-Funktionen zur Rückverfolgbarkeit relevanter Ereignisse.
- **Bereitstellung von Informationen (Art. 13 KI-VO)**
Transparente Betriebsanleitungen und Nutzerinformationen, damit Betreiber die Ausgaben des Systems angemessen interpretieren können.
- **Menschliche Aufsicht (Art. 14 KI-VO)**
Sicherstellung, dass das Hochrisiko-KI-System wirksam durch natürliche Personen beaufsichtigt werden kann (geeignete Mensch-Maschine-Schnittstellen).
- **Genauigkeit, Robustheit, Cybersicherheit (Art. 15 KI-VO)**
Gewährleistung eines verlässlichen Betriebs mit angemessener Genauigkeit und Widerstandsfähigkeit gegenüber Fehlern und Manipulationen.
- **Einhaltung des Pflichtenkatalogs in Art. 16 KI-VO**
u.a. Qualitätsmanagementsystem (Art. 17 KI-VO), Aufbewahrung der Dokumentation (Art. 18 KI-VO), Protokolle (Art. 19 KI-VO), EU-Konformitätserklärung (Art. 47 KI-VO), CE-Kennzeichnung (Art. 48 KI-VO).

In der Praxis ist der Hochrisiko-Pflichtenkreis stark an das Produktregulierungsrecht (Produktsicherheit, CE-Kennzeichnung, Konformitätsbewertung) angelehnt; die KI-VO ergänzt diese Vorgaben spezifisch für KI-Systeme und fordert eine detaillierte Prüfung und

Umsetzung im Einzelfall. Ebenfalls ist es wichtig, darauf hinzuweisen, dass neben den spezifischen Pflichten für Anbieter von Hochrisiko-KI-Systemen auch die Pflichten aus Artikel 50 KI-VO für KI-Systeme mit Transparenzrisiken einschlägig sein können. Beide Pflichtenkreise schließen sich nicht gegenseitig aus, sondern können – in Abhängigkeit des jeweiligen KI-Systems – nebeneinanderstehen.

4 Pflichten für Anbieter von KI-Systemen mit Transparenzrisiken

Soweit ein wesentliches Risiko eines KI-Systems darin liegt, dass der Einsatz von KI oder der KI-Output für Nutzer nicht erkennbar ist, greifen Transparenz- und Kennzeichnungspflichten nach Art. 50 KI-VO.

Aus Sicht des Anbieters sind insbesondere relevant:

- **Interaktive KI-Systeme (Art. 50 Abs. 1 KI-VO)**
 - Wenn ein KI-System für die direkte Interaktion mit natürlichen Personen bestimmt ist, müssen Anbieter die Systeme so gestalten, dass betroffene Personen erkennen können, dass sie mit einem KI-System interagieren.
 - Der Hinweis muss klar, verständlich und bereits im Design verankert sein (z. B. Kennzeichnung „KI-Chatbot“, deutlich sichtbare Hinweise, akustische Signale bei Voicebots).
- **Synthetische Inhalte (Text, Bild, Audio, Video – Art. 50 Abs. 2 KI-VO)**
 - KI-Systeme, die synthetische Inhalte (Text, Bild, Audio, Video) erzeugen, müssen Outputs in einem maschinenlesbaren Format kennzeichnen und als künstlich erzeugt oder manipuliert erkennbar machen.
 - Die technische Lösung muss wirksam, interoperabel, robust und zuverlässig sein; empfohlen werden etwa Metadaten-Embedding, Wasserzeichen und Fingerprinting.
 - Ausnahmen können jedoch dann gelten, wenn das KI-System lediglich unterstützend tätig ist und Inhalte oder Semantik nicht wesentlich verändert (z. B. Formatkonvertierungen, Rechtschreibprüfungen, reine Komprimierungen).

Transparenzpflichten nach Art. 50 KI-VO können – wie bereits aufgezeigt – zusätzlich zu Hochrisiko-Pflichten gelten: Ein KI-System kann gleichzeitig Hochrisiko-System (z. B. im HR-Bereich) sein und Transparenzpflichten auslösen, wenn es synthetische Inhalte erzeugt oder direkte Nutzerinteraktionen umfasst.

5 Pflichten für alle Anbieter von KI-Systemen

Unabhängig davon, ob ein KI-System als Hochrisiko-System, als KI-System mit Transparenzrisiken oder als System mit minimalen Risiken eingestuft wird, gilt für regulierte

KI-Systeme stets die übergeordnete Pflicht aus Art. 4 KI-VO. Anbieter müssen geeignete Maßnahmen ergreifen, um ein ausreichendes Maß an KI-Kompetenz („AI literacy“) bei den Personen zu fördern, die KI-Systeme im Auftrag des Unternehmens entwickeln, betreiben oder nutzen. Maßgeblich ist dabei eine kontextbezogene Betrachtung: Berücksichtigt werden sollen insbesondere technische Vorkenntnisse, Berufserfahrung, Ausbildungsstand und der konkrete Nutzungskontext der eingesetzten KI-Systeme sowie die Personengruppen, auf die diese Systeme wirken.

Art. 4 KI-VO ist hierbei als organisatorische Förder- und Maßnahmenpflicht zu verstehen, nicht als individuelle Erfolgsgarantie. Unternehmen müssen ein angemessenes Kompetenzniveau durch passende Schulungs-, Informations- und Unterstützungsangebote ermöglichen, sind aber nicht verpflichtet, für jede einzelne Person einen bestimmten, konkret messbaren Grad an KI-Kompetenz „zu garantieren“. In der Praxis umfasst dies insbesondere ein Grundverständnis der Funktionsweise und Einsatzszenarien der verwendeten KI-Systeme, die Fähigkeit, Chancen und Risiken des KI-Einsatzes realistisch einzuschätzen, sowie grundlegende Kenntnisse der einschlägigen rechtlichen Rahmenbedingungen.

6 Handlungsempfehlung für Mitgliedsunternehmen

Mitgliedsunternehmen sollten für jedes geplante oder bereits eingesetzte KI-System zunächst systematisch prüfen und dokumentieren, ob sie in der Rolle des Anbieters im Sinne der KI-VO auftreten und welcher Risikoklasse das KI-System zuzuordnen ist. Auf dieser Grundlage lassen sich verbotene KI-Praktiken (Art. 5 KI-VO) frühzeitig ausschließen, Hochrisiko-Systeme nach Anhängen I und III identifizieren und die Transparenzpflichten nach Art. 50 KI-VO zuordnen. Eine interne Checkliste sowie ein standardisierter Freigabeprozess erleichtern es, die jeweiligen Pflichtenkreise strukturiert zu erfassen und die Umsetzung schrittweise zu planen.

Ansprechpartner

Dr. Sebastian Horlacher, LL.M.

Grundsatzabteilung Recht

Telefon 089-551 78-131

sebastian.horlacher@vbw-bayern.de

www.vbw-bayern.de

Marius Drabiniok

SKW Schwarz

Telefon 069-630-00-165

m.drabiniok@skwschwarz.de

In Kooperation mit



Hinweis:

Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.