Die KI-Verordnung

Beitrag der Rechtsinformationsstelle von ORCA.nrw

25.11.2024

Abstract

Am 2. August 2024 ist die KI-Verordnung (VO (EU) 2024/1689) in Kraft getreten. Dieser Beitrag soll einen ersten Überblick über das Regelungsinstrument der KI-Verordnung bieten. Hierbei werden die Zielsetzung sowie der Anwendungsbereich und die entsprechenden Pflichten dargestellt.

Informationen zur Rechtsinformationsstelle von ORCA.nrw unter
https://www.orca.nrw/oer/oer-erstellen/rechtsinformation/

I. Ziel und Gegenstand der Verordnung

Die KI-VO ist ein spezielles Produktsicherheitsgesetz, das nicht an die Anwendung anknüpft, sondern die KI und die „Produkthersteller“ selbst. Hierzu versucht die Verordnung einen Rechtsrahmen für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und Verwendung von KI-Systemen herzustellen. Ziel ist dabei die Minimierung von Risiken und die Erzeugung eines einheitlich hohes Schutzniveaus sowie die Verhinderung von schädlichen Auswirkungen von KI-Systemen, während gleichzeitig vertrauenswürdige KI-Systeme gefördert und die Innovation unterstützt werden soll (Art. 1 Abs. 1 KI-VO). Hierzu regelt die KI-VO insbesondere das Inverkehrbringen, die Inbetriebnahme sowie die Verwendung von KI-Systemen und stellt Verbote bestimmter Praktiken auf. Kern der Verordnung sind dabei die Pflichten für die verschiedenen Akteure in Bezug auf General Purpose KI und Hochrisiko-KI, die auf einem risikobasieren Ansatz beruht.

II. Anwendungsbereich, Art. 2 KI-VO

Art. 2 KI-VO bestimmt den Anwendungsbereich der Verordnung, sprich wen die später dargestellten Pflichten treffen sollen. In persönlicher Hinsicht sind hierbei verschiedene Akteure Adressaten der Verordnung, in sachlicher Hinsicht muss ein KI-Modell mit allgemeinem Verwendungszweck vorliegen, sog. General Purpose KI.

1. Akteure (Persönlicher Anwendungsbereich)

Die wichtigsten Akteure der KI-VO sind die Anbieter und Betreiber. Daneben werden weitere Akteure wie Einführer, Händler, Produkthersteller und Bevollmächtigte von Anbietern definiert.

Art. 2 Abs. 1 lit. a): Anbieter ist nach der Verordnung eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, 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 das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich.

Art. 2 Abs. 2 lit. b): Betreiber ist eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet (Art. 3 Nr. 4 KI-VO).

Hochschulen können in den Anwendungsbereich der KI-VO fallen, wenn sie als Anbieter oder Betreiber zu klassifizieren sind. Das ist insbesondere bei der Entwicklung eigener KI – solange diese nicht rein intern zur Forschung genutzt wird – denkbar.

2. KI-Systeme (Sachlicher Anwendungsbereich)

Die KI-VO greift, wenn ein KI-System i.S.d. KI-VO vorliegt. Ein solches ist nach Art. 3 Nr. 1 KI-VO *„ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder*

virtuelle Umgebungen beeinflussen können“. Wobei diese Definition aus Sicht des Zwecks der KI-VO gesehen werden muss und daher keine abschließende oder gar technische Definition einer KI ist.

Die KI-VO sortiert KI-Systemen mit unterschiedlichem Risiko unterschiedliche Pflichten zu, wobei zwischen vier Kategorien von KI-Systemen unterschieden wird:

Zunächst die **verbotene KI-Systeme** i.S.d. Art. 5 der KI-VO. Sie zeichnen sich vor allem durch eine klare Bedrohung von Grundrechten aus. Solche Systeme liegen z.B. bei unzulässigen Beeinflussungen, Manipulationen, Täuschungen, Diskriminierung, Social Scoring, Profiling, Gesichtserkennungen oder ähnliche Praktiken vor (Art. 5 KI-VO). Das Verbot dieser KI-Systeme gilt ab dem **02.05.2025** (Art. 113 lit. a) KI-VO).

Kapitel III befasst sich sodann mit den **Hochrisiko-KI-Systemen**. Hochrisiko-KI sind KI-Systeme, die sich – allgemein gesagt – potenziell negativ auf die Sicherheit und Grundrecht von Personen auswirken können. Art. 6 KI-VO listet hierfür die genaueren Kriterien und verweist auf die Anhänge I und III. Auch an Hochschulen können unter Umständen Hochrisiko-KI zum Einsatz kommen. Relevant erscheint hierbei insbesondere nach Art. 6 Abs. 2 KI-VO i.V.m. Anhang III Nr. 3. Dieser legt fest, dass es sich bei KI-Systemen, welche die allgemeine und berufliche Bildung betreffen, von einer Hochrisiko-KI ausgegangen werden kann.

Als drittes bestehen **KI-Systeme mit begrenztem Risiko**, für welche nur begrenze Vorschriften bestehen. Damit sind die Systeme gemeint, die unter die KI-VO fallen, allerdings weder Hochrisiko-KI-Systeme noch verbotene KI-Systeme sind. Fällt ein KI-System gänzlich aus dem Anwendungsbereich der KI-VO, so ist es ein **System mit minimalem Risiko**. Dieses wird zwar von KI-VO nicht erwähnt, ist allerdings in der Literatur als vierte Kategorie anerkannt.

Neben diesen vier Risikostufen kennt die KI-VO noch die **KI-Modelle mit allgemeinem Verwendungszweck**, sog. General Purpose KI in Kapitel V der Verordnung (Art. 51 ff. KI-VO). Hierbei handelt es sich um solche KI-Modelle, die als allgemeines Modell eine Grundlage für speziellere KI-Systeme bilden können. Hierunter fallen vor allem die Large Language Models (LLM) wie z.B. ChatGPT. Sollten Hochschulen entsprechende KI-Modelle entwickeln und auf den Markt bringen, so können hieraus Anbieterpflichten (s.u.) erwachsen. In den meisten Fällen werden die Hochschulen in Bezug auf die General Purpose KI wohl maximal als Betreiber in Betracht kommen, diese Treffen die Anbieterpflichten nicht.

III. Pflichten der KI-Verordnung

Nur weil ein Hochrisiko-KI-System vorliegt, heißt das nicht, dass dieses KI-System nicht mehr verwendet werden darf! Die KI-VO knüpft die weitere Verwendung jedoch an die Einhaltung gewisser Pflichten.

So schreibt Art. 4 KI-VO vor, dass die Anbieter und Betreiber von KI-Systemen Maßnahmen ergreifen zu haben, die sicherstellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind über ein ausreichendes Maß an „KI-Kompetenz“ verfügen. Ob zu diesen „anderen Personen“ auch Studierende zählen kann an dieser Stelle noch nicht abschließend gesagt werden. Auch die Frage nach der Art der Maßnahmen zur Erzeugung der KI-Kompetenz kann noch nicht beantwortet werden, denkbar wären aber z.B. regelmäßige Schulungen.

Die Pflichten bzgl. der General Purpose KI (wie LLM) treffen allein den Anbieter und nicht den Betreiber. So müssen die Anbieter eine umfangreiche Dokumentation zur Verfügung stellen. Hat die entsprechende General Purpose KI auch ein systemisches Risiko, so treten die Pflichten der Art. 55, 56 KI-VO hinzu. Weitere Pflichten der KI-VO sind die sog. Compliance- und Transparenzpflichten für die Anbieter nach Art. 53 und 55 KI-VO.

IV. Fristen

Art. 113 KI-VO bestimmt, dass die Verordnung grundsätzlich ab dem 2. August 2026 zu gelten beginnt. Hiervon werden jedoch Ausnahmen gemacht, so sollen die allgemeinen Vorschriften und die Vorschriften zu den verbotenen KI-Systemen ab dem 2. Februar 2025 gelten, die Regeln für die General Purpose KI ab dem 2. August 2025 und für die Hochrisiko-KI am 2. August 2026 bzw. am 2. August 2027.