MENOLD BEZLER

10 Fragen und Antworten zur KI-Verordnung (KI-VO)

1 Was ist die KI-Verordnung?

Die KI-Verordnung (**KI-VO**, auch **AI Act)** ist ein europäisches Gesetz zur Regulierung von künstlicher Intelligenz (KI). Noch handelt es sich dabei nur um einen Entwurf. Wenn die KI-VO in Kraft tritt, wird es sich aber um das **weltweit erste KI-Gesetz** handeln.

2 Wann kommt die KI-Verordnung?

Das Gesetzgebungsverfahren befindet sich in der letzten Verfahrensphase, dem sog. Trilog. In diesem verhandeln Rat, Kommission und EU-Parlament über die finale Version der Verordnung. Eine politische Einigung wird vor Ende des Jahres angestrebt. Die KI-VO könnte dann Anfang 2024 offiziell verabschiedet werden.

3 Wen betrifft die KI-Verordnung?

Die Verordnung richtet sich vor allem an **Anbieter**, die KI-Systeme (unabhängig von ihrem Sitz) **in der Union in Verkehr bringen oder in Betrieb nehmen** sowie an **Nutzer**, die i**n der EU niedergelassen sind oder ihren Sitz in der EU** haben. Nutzer ist dabei grundsätzlich jeder, der ein KI-System unter seiner Aufsicht einsetzt. Es wurde aber vorgeschlagen, die außerberufliche Nutzung aus dieser Definition auszuklammern. Wenn Anbieter oder Nutzer sich in einem **Drittland** befinden, der von der KI erzeugte **Output aber in der Union verwendet** werden soll, soll die Verordnung ebenfalls Anwendung finden.

Weiterhin wird sich die Verordnung voraussichtlich auch auf Importeure und Händler von KI-Systemen erstrecken, sowie auf Produkthersteller, die eine KI zusammen mit ihrem Produkt in Verkehr bringen oder in Betrieb nehmen. Details hierzu bleiben abzuwarten.

Wie ist die KI-Verordnung aufgebaut?

Die KI-VO verfolgt im Kern einen **risikobasierten Ansatz:** Sie differenziert zwischen KI-Systemen, die ein unannehmbares Risiko, ein hohes Risiko oder ein geringes bzw. minimales Risiko darstellen und stellt je nach Risikoklasse unterschiedliche Anforderungen. Für KI-Anbieter und -Nutzer ist die Risikoeinstufung somit entscheidend für die Pflichten, die sie nach der KI-VO erfüllen müssen. Darüber hinaus werden allgemeine Regelung getroffen, die für alle Risikoklassen gelten. Der hintere Teil der KI VO regelt zudem umfassend die Überwachung und Umsetzung der Verordnung.

Was sind KI-Systeme mit „unannehmbarem Risiko“ und was gilt für diese?

KI, die ein **unannehmbares Risiko** für Grundrechte oder Werte der Union darstellt, soll **verboten** werden. Hierzu zählen z.B. Systeme, die Personen unterschwellig dazu manipulieren, andere Menschen zu schädigen oder bestimmte KI-Systeme im Bereich der Strafverfolgung. Die verbotenen Systeme dürften für die meisten Unternehmen **keine praktische Bedeutung** haben.

Was sind KI-Systeme mit „hohem Risiko“ und was gilt für diese?

Der Schwerpunkt der Verordnung liegt auf der Regulierung von KI-Systemen mit **hohem Risiko**. Das sind KI-Systeme, von denen eine **besondere Gefahr für Gesundheit, Sicherheit oder Grundrechte** befürchtet wird. Die Einstufung als hochriskant richtet sich vor allem nach dem **Anhang III** zur KI-VO, der die hochriskanten Systeme auflistet. Hierzu gehören z.B. KI-Systeme, die zur biometrischen Identifizierung von Personen, in kritischen Infrastrukturen wie dem Straßenverkehr, bei Bewerbungsverfahren oder bei Kreditwürdigkeitsentscheidungen eingesetzt werden. Die Liste in Anhang III soll künftig von der Kommission **ergänzt und überarbeitet** werden können.

An Hochrisiko-KI wird eine **Vielzahl besonderer Anforderungen** gestellt. Hierzu zählen z.B. Dokumentations- und Informationspflichten, Qualitätsanforderungen an Test- und Trainingsdaten und die Gewährleistung einer menschlichen Aufsicht. Hochrisiko-KI-Anbieter müssen sich zudem einem Konformitätsbewertungsverfahren unterziehen. Auch wurde zuletzt die Dokumentation des ökologischen Fußabdrucks und die Einhaltung bestimmter Umweltstandards gefordert.

Was gilt für übrige KI-Systeme?

An KI-Systeme mit **geringem Risiko** – d.h. solche Systeme, die **weder verboten noch hochriskant** sind – werden im Wesentlichen nur **Transparenzanforderungen** gestellt. Der Endnutzer soll hier bei bestimmten KI-Systemen wissen, dass er es mit einer KI bzw. einem von einer KI erzeugtem Output zu tun hat. Deep Fakes oder intelligente Chatbots wie Chat-GPT müssen sich danach künftig deutlich als solche zu erkennen geben.

8 Was gilt für vielseitig einsetzbare Systeme wie Chat-GPT?

Der intelligente Chatbot Chat-GPT ist vielseitig einsetzbar und lässt sich daher theoretisch allen Risikoklassen zuordnen: Er könnte zur verbotenen Manipulation von Menschen oder als Komponente eines Hochrisiko-Systems oder „unkritisch" als digitaler Assistent im Kundenservice, z.B. beim Onlinehandel eingesetzt werden. Chat-GPT ist damit nicht per se „gefährlich", könnte aber für verbotene oder hochriskante Praktiken verwendet werden.

Der Ministerrat hat daher vorgeschlagen, eine Regelung für sog. **General Purpose AI** einzuführen, d.h. für KI, die keinen spezifischen, sondern lediglich einen „allgemeinen" Anwendungszweck verfolgt und daher vielseitig einsetzbar ist. Wird diese KI in einem hochriskanten Bereich oder als Komponente einer Hochrisiko-KI eingesetzt, soll sie insbesondere die Anforderungen an Hochrisiko-KI erfüllen müssen. Außerdem müssen Anbieter von General Purpose AI bestimmte Informationen über die KI bereitstellen.

Das EU-Parlament hat weiter vorgeschlagen, auch sog. **Foundation Models** als Unterform der General Purpose AI zu adressieren. Darunter versteht es KI-Modelle, die auf einer breiten Datenbasis in großem Umfang trainiert wurden, auf einen allgemeinen Output ausgelegt sind und an eine Vielzahl spezieller Aufgaben weiter angepasst werden können. Der Unterschied zu der General Purpose AI liegt nach der Definition des Parlaments vorallem in den verwendeten Trainingsdaten. Chat-GPT wäre als solches Foundation Model einzuordnen, da es mit Daten aus dem gesamten Internet trainiert wurde. Das Parlament hat strengere Anforderungen für Foundation Models vorgeschlagen, insb. hinsichtlich Daten, Dokumentation und Transparenz.

9 Was droht bei Verstößen gegen die Verordnung?

Bei Verordnungsverstößen drohen **erhebliche Sanktionen.** Der Vorschlag des Ministerrats bedroht einen Verstoß – ähnlich wie die DSGVO – mit Bußgeldern von bis zu **30 Millionen Euro bzw. 6 % des weltweiten Jahresumsatzes**. Das Parlament hat vorgeschlagen, diese Bußgelder sogar auf 40 Millionen Euro bzw. 7 % des Jahresumsatzes zu erhöhen.

10 Wie geht es weiter und was ist zu tun?

Der Rahmen der Verordnung mit ihrem risikobasierten Ansatz scheint festzustehen. Politisch umstritten ist dagegen, welche KI-Systeme wegen ihres unannehmbaren Risikos verboten werden sollen sowie die **Liste der Hochrisiko-KI-Systeme**. Auch Details zu den einzelnen Anforderungen an Hochrisiko-KI-Anbieter und -Nutzer werden noch debattiert. Bis Jahresende dürfte aber mit einer Einigung zu rechnen sein. Da es sich um eine Verordnung handelt, werden die Regelungen **unmittelbar in allen EU-Mitgliedsstaaten gelten**, ohne dass es einer Umsetzung durch ein nationales Gesetz bedarf. Spätestens bis zum Ablauf der sog. Schonfrist, die voraussichtlich **zwei Jahre** betragen wird, müssen Betroffene die Anforderungen der KI-VO umgesetzt haben. Daher sollten sich Unternehmen, die KI-Systeme anbieten oder nutzen und dabei mit dem EU-Markt in Berührung kommen frühzeitig mit der KI-VO auseinandersetzen und prüfen, ob sie unter den Anwendungsbereich der Verordnung fallen und welche Pflichten sie künftig umsetzen müssen.

Autorin: Jessica Hawighorst

Unser Team aus dem Bereich IT- / Internet- und Datenschutzrecht

Dr. Jörg Schneider-Brodtmann, LL. M
Partner, Rechtsanwalt
joerg.schneider-brodtmann
@menoldbezler.de
Tel.: +49 711 86040 350

Dr. Carsten Ulbricht M.C.L.
Partner, Rechtsanwalt
carsten.ulbricht@menoldbezler.de
Tel.: +49 711 86040 025

Carolin Nemec, LL.M. (UCC)
Rechtsanwältin
carolin.nemec@menoldbezler.de
Tel.: +49 711 86040 791

Varinia Iber
Rechtsanwältin,
Fachanwältin für IT Recht
varinia.iber@menoldbezler.de
Tel.: +49 711 86040 025

Jessica Hawighorst
Rechtsanwältin
jessica.hawighorst@menoldbezler.de
Tel.: +49 711 86040 760