ULF SCHMITT & PARTNER mbB
STEUERBERATER
RECHTSANWALT

EU AI Act: Künstliche Intelligenz im Unternehmen

Mandanten-Informationen

EU AI Act: Künstliche Intelligenz im Unternehmen

Inhalt

Editorial

Die technischen Möglichkeiten aus einem Einsatz Künstlicher Intelligenz („KI" oder in englischer Sprache „AI") entwickeln sich rasant, die Einsatzmöglichkeiten sind vielfältig, der Fantasie wenig Grenzen gesetzt.

Auch Unternehmen setzen KI in verstärktem Maße bereits ein, integrieren diese in ihre Arbeitsabläufe; KI unterstützt, bereitet vor und teils werden ganze, bislang von Menschen vorgenommene Arbeitsschritte bei der Herstellung von Produkten oder der Abarbeitung von Dienstleistungen durch KI ersetzt.

Der Einsatz künstlicher Intelligenz war bislang weitgehend ungeregelt. Nun haben die EU-Mitgliedstaaten im Mai 2024 den sog. „EU AI Act" verabschiedet und beschlossen. Dieser gilt als das erste weltweite KI-Gesetz und diese Verordnung ist, von einigen Ausnahmen abgesehen, 24 Monate nach dem Inkrafttreten auch von Unternehmen anzuwenden. Diese Mandanten-Info dient als erste Orientierung für Führungskräfte[1] in Unternehmen, die sich mit diesem Themenkomplex auseinandersetzen müssen.

[1] In dieser Publikation wird aus Gründen der besseren Lesbarkeit in der Regel das generische Maskulinum verwendet. Die verwendete Sprachform bezieht sich auf alle Menschen, hat ausschließlich redaktionelle Gründe und ist wertneutral.

Ulf Schmitt & Partner mbB, E.T.A.-Hoffmann-Str. 3, 96047 Bamberg,

Telefon: 0951 980 440, Telefax: 0951 980 4450

E-Mail: info@steuerkanzlei-schmitt.de, Internet: www.steuerkanzlei-schmitt.de

1 Der EU AI Act

Der Einsatz künstlicher Intelligenz im Alltag bietet sowohl erhebliche Chancen als auch Risiken.

Durch die frühzeitige Einbindung von KI kann eine zukunftsorientierte Gestaltung des Alltags – im privaten und beruflichen Umfeld – ermöglicht werden. KI kann in vielen Bereichen unterstützen; für die Wirtschaft ist der Einsatz von KI in jedem Fall geboten, um auch im internationalen Vergleich wettbewerbsfähig zu bleiben. Denn die Konkurrenz im Ausland setzt KI überall dort ein, wo es sinnvoll und vorteilhaft ist

Am 21.05.2024 hat der Rat der Europäischen Union den sog. EU AI Act, zu Deutsch KI-Verordnung, verabschiedet. Die Verordnung (EU) 2024/1689[2] wurde am 12.07.2024 im Amtsblatt der Europäischen Union veröffentlicht und ist seit dem 01.08.2024 in Kraft. Anwendung findet die Verordnung nach einer Übergangszeit von 24 Monaten im August 2026, wobei einige Vorschriften bereits früher anwendbar sein werden: *Ab Februar 2025* sind bereits die KI-Systeme der höchsten Risikostufe („unannehmbares Risiko") verboten. *Ab August 2025* greifen zudem bereits die Vorschriften für KI-Modelle mit allgemeinem Verwendungszweck – General Purpose AI Models (GPAI). Der größte Teil der KI-Verordnung gilt jedoch erst *ab dem 02.08.2026*.[3]

Im Kern beinhaltet der AI Act Regelungen über die Verhinderung des Missbrauchs von KI-Anwendungen. Dabei sollen bei der Verwendung künstlicher Intelligenz auf der einen Seite die Grundrechte der Betroffenen und zugleich auf der anderen Seite die Freiheiten von Wissenschaft und Wirtschaft gewahrt werden. Die Entwicklung und Einführung sicherer und vertrauenswürdiger KI-Systeme im EU-Binnenmarkt soll gestärkt werden.[4]

Die gegenläufigen Interessen sind in einen ausgewogenen Ausgleich miteinander zu bringen.

2 EU AI Act vom 12.07.2022 im EU-Amtsblatt mit weiteren Nachweisen, https://t1p.de/081wm (Stand: 03.12.2024).

3 V gl. Florian Stark , AI-Act: Die wichtigsten Fragen zur KI-Verordnung, https://t1p.de/bzr70 (Stand: 03.12.2024) ; Von Welser , die KI-Verordnung – ein Überblick über das weltweit erste Regelwerk für künstliche Intelligenz, GRUR-Praxis 2024, 485.

4 Von Welser , Die KI-Verordnung – ein Überblick über das weltweit erste Regelwerk für künstliche Intelligenz, GRUR-Praxis 2024, 485; Möller-Klapperich , Die neue KI-Verordnung der EU, N JW 2024, 337.

1.1 Ziele

Zusammengefasst verfolgt die KI-Verordnung vier konkrete und klar formulierte Ziele:

- **Schutz der EU-Grundrechte,**
- **Stärkung des Vertrauens in KI,**
- **Förderung von Innovation,**
- **Risikoschutz.**

1.2 Persönlicher Anwendungsbereich

Der persönliche Anwendungsbereich der KI-Verordnung (KI-VO), geregelt in Art. 2 KI-VO, umfasst sowohl **Anwender** als auch **Anbieter** von KI-Systemen.

Konkret nennt die Vorschrift:

- Anbieter, die in der Union KI-Systeme in Verkehr bringen oder in Betrieb nehmen,
- Betreiber von KI-Systemen mit Sitz oder Aufenthalt in der Union,
- Anbieter und Betreiber von KI-Systemen mit Sitz oder Aufenthalt in einem Drittland, wenn die KI-Systeme in der Union verwendet werden,
- Einführer und Händler von KI-Systemen,
- Produkthersteller, die KI-Systeme mit ihren Produkten verwenden,
- Bevollmächtigte von Anbietern außerhalb der Union,
- betroffene Personen innerhalb der Union.

Der in der Verordnung enthaltene Pflichtenkatalog unterscheidet insbesondere zwischen Anbietern und Betreibern, sodass eine entsprechende Abgrenzung von besonderer Wichtigkeit ist.

1.2.1 Anbieter

Der Begriff des „Anbieters" wird in Art. 3 Nr. 3 KI-VO wie folgt definiert:

***„Anbieter** ist 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."*

1.2.2 Betreiber

Den Begriff des „Betreibers" definiert Art. 3 Nr. 4 KI-VO wie folgt:

*„**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".*

Mithin genügt bereits das eigenverantwortliche Einsetzen eines KI-Systems zum Begründen der Betreibereigenschaft. Betreiber können beispielsweise Arbeitgeber sein, wenn sie KI-Systeme im HR-Bereich einsetzen. Sofern sie jedoch die Zweckbestimmung eines KI-Systems verändern oder eine andere wesentliche Veränderung am KI-System vornehmen, können sie vom Betreiber zum Anbieter werden.

1.3 Sachlicher Anwendungsbereich

Maßgebend für den Umfang des sachlichen Anwendungsbereichs ist die Definition des „KI-Systems" in Art. 3 Nr. 1 KI-VO:

***„KI-System** bezeichnet ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und nach seiner Betriebsaufnahme anpassungsfähig sein kann. Es kann aus den erhaltenen Eingaben für explizite oder implizite Ziele ableiten, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können."*

Diese Definition soll KI-Systeme von herkömmlichen Softwaresystemen und Programmierungsansätzen abgrenzen; ein KI-System zeichnet sich in besonderer Weise dadurch aus, dass es die Fähigkeit zum „Ableiten" hat, was durch Techniken wie maschinelles Lernen ermöglicht wird. Das System lernt also selbstständig dazu, indem es Daten sammelt.

1.4 Räumlicher Anwendungsbereich

Die Verordnung gilt räumlich nicht nur bezogen auf Anbieter/ Betreiber aus der Europäischen Union (EU), sondern auch für KI-Systeme, die Auswirkungen auf die EU haben.[5] So nennt die Vorschrift ausdrücklich auch Adressaten, die Sitz oder Aufenthalt in einem Drittland haben, sofern die KI-Systeme in der Union verwendet werden.

1.5 Risikobasierter Ansatz

Das mit dem AI Act aufgesetzte Regelwerk verfolgt einen risikobasierten Ansatz.[6] Die Vorgaben, das heißt die Anforderungen und Pflichten, sind demnach umso strenger, je höher das Risiko der Rechtsverletzung oder Gefährdung von Rechten durch die KIAnwendung eingestuft wird.

Der AI Act ordnet KI-Anwendungen drei Risikokategorien zu:

- geringes/minimales Risiko,
- hohes Risiko,
- unannehmbares Risiko.

Eine besondere Herausforderung liegt für Unternehmen in dem Umgang mit der KI der mittleren Gruppe (Hochrisiko-KI).

1.5.1 Unannehmbares Risiko (verbotene Praktiken)

Das unannehmbare Risiko ist die höchste Risikostufe des AI Acts. KI-Systeme, die in diese Risikogruppe eingestuft werden, dürfen laut Art. 5 KI-VO **nicht** in Verkehr gebracht, in Betrieb genommen oder anderweitig verwendet werden. Diese KI-Systeme werden also von der EU als so gefährlich eingestuft, dass sie **gänzlich verboten werden**.

5 Woesch/Vogt , Die KI-Verordnung – Die digitale Zukunft im Finanzsektor BKR 2024, 689.

6 Von Welser , Die KI-Verordnung – ein Überblick über das weltweit erste Regelwerk für künstliche Intelligenz, GRUR-Praxis 2024, 485; Möller-Klapperich , Die neue KI-Verordnung der EU, NJ 2024, 337.

Die Einstufung in die Kategorie des höchsten Risikos erfolgt zusammenfassend dann, wenn wesentliche Rechtsgüter der betroffenen Personen verletzt oder gefährdet werden – es handelt sich um KI-Systeme, die etwa negativen Einfluss auf die Meinungsbildung/Entscheidungsfähigkeit von Personen nehmen oder die Persönlichkeitsrechte im Hinblick auf persönliche Daten gefährden oder diskriminierend sind.

Konkret benennt Art. 5 KI-VO Anwendungen, bei denen ein unannehmbares Risiko zu bejahen ist und legt fest, dass KI-Systeme verboten sind,

- die dazu bestimmt sind, menschliches Verhalten nachteilig zu verändern, indem Personen unterschwellig beeinflusst werden oder absichtlich manipulative oder täuschende Techniken verwendet werden (vgl. Art. 5 Abs. 1 lit. a KI-VO),
- welche die Vulnerabilität oder die Schutzbedürftigkeit natürlicher Personen, etwa aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation ausnutzen (vgl. Art. 5 Abs. 1 lit. b KI-VO),
- zum Zweck des „Social Scoring", z. B. Systeme, derer sich Behörden zum Zweck der Bewertung oder zur Klassifizierung der Vertrauenswürdigkeit natürlicher Personen in öffentlich zugänglichen Räumen bedienen,
- die ausschließlich auf der Grundlage des Profiling das Risiko bewerten, dass eine natürliche Person eine Straftat begeht (Art. 5 Abs. 1 lit. d KI-VO),
- die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern (Art. 5 Abs. 1 lit. e KI-VO),
- die zur Ableitung von Emotionen einer natürlichen Person am Arbeitsplatz und in Bildungseinrichtungen verwendet werden, außer dies erfolgt aus medizinischen oder aus Sicherheitsgründen (Art. 5 Abs. 1 lit. f KI-VO),
- die der biometrischen Kategorisierung von Personen dienen, um deren Rasse, ihre politischen Einstellungen, ihre Gewerkschaftszugehörigkeit, ihre religiösen oder weltanschaulichen Überzeugungen, ihr Sexualleben oder ihre sexuelle Ausrichtung zu erschließen oder abzuleiten (Art. 5 Abs. 1 lit. g KI-VO),

- die zur biometrischen Echtzeit-Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen von Strafverfolgungsbehörden eingesetzt werden (Art. 5 Abs. 1 lit. h KI-VO). Eine Ausnahme besteht nur dann, wenn dies im Hinblick auf konkret formulierte Ziele unbedingt erforderlich ist – beispielsweise zur Abwendung einer unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen. Die Ausnahme kann beispielsweise bei der Suche nach vermissten Personen greifen.

1.5.2 Hohes Risiko

KI-Systeme der Risikokategorie „hoch" – auch Hochrisiko-KISysteme genannt (vgl. Art. 6 KI-VO) – sind solche, die ein hohes Risiko für die Gesundheit und die Sicherheit natürlicher Personen darstellen oder geeignet sind, deren Grundrechte bzw. Grundfreiheiten zu bedrohen.

In Betracht kommt insbesondere die Verletzung der folgenden Grundrechte bzw. Grundfreiheiten:

- Würde des Menschen,
- Achtung des Privat- und Familienlebens,
- Schutz personenbezogener Daten,
- Freiheit der Meinungsäußerung,
- Informationsfreiheit,
- Versammlungs- und Vereinigungsfreiheit.

Entsprechend enthält Art. 6 Abs. 3 KI-VO auch die Bestimmung, dass KI-Systeme dann nicht als hochriskant gelten, wenn sie kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte natürlicher Personen beinhalten, indem sie unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflussen.

Die Einstufung als Hochrisiko-KI-System kann sich entweder aus dem Produkt selbst oder aus dem Anwendungsbereich ergeben.

1.5.3 Anforderungen an Hochrisiko-KI-Systeme

An Hochrisiko-KI-Systeme werden durch den AI Act entsprechend hohe Anforderungen gestellt. Insgesamt macht die Kategorie der Hochrisiko-KI-Systeme den wichtigsten Teil und den Schwerpunkt der KI-Verordnung aus. Die Anforderungen für Hochrisiko-KISysteme sind in Abschnitt 2 der Verordnung festgelegt.

Im Einzelnen werden an Hochrisiko-KI-Systeme die folgenden Anforderungen gestellt:

- **Einrichtung eines Risikomanagementsystems**

  Für Hochrisiko-KI-Systeme ist ein Risikomanagementsystem einzurichten, welches kontinuierlich zu pflegen ist (vgl. Art. 9 KI-VO). Im Rahmen dessen müssen bekannte und vorhersehbare Risiken für Gesundheit, Sicherheit oder für Grundrechte Betroffener ermittelt und analysiert sowie anschließend abgeschätzt und bewertet werden. Zur Bewältigung dieser Risiken müssen geeignete und gezielte Risikomanagementmaßnahmen ergriffen werden.

- **Daten-Governance (KI-Aufsicht)**

  Des Weiteren sind bei Hochrisiko-KI-Systemen bestimmte Regelungen in Bezug auf verwendete Daten zu beachten. Sofern Techniken eingesetzt werden, bei denen KI-Modelle mit Daten trainiert werden, müssen Trainings-, Validierungs- und Testdatensätze entwickelt werden, die bestimmten Qualitätskriterien entsprechen (Art. 10 KI-VO). Es gelten in diesem Zusammenhang spezifische Daten-Governance- und Datenverwaltungsverfahren.

  Die KI-Aufsicht ist insgesamt auf unterschiedliche Behörden und Gremien verteilt, darunter ein KI-Büro der EU-Kommission, ein KI-Gremium, ein Beratungsforum, ein wissenschaftliches Gremium sowie auf Ebene der Mitgliedstaaten jeweils eine notifizierende Behörde und eine Marktüberwachungsbehörde.

- **Technische Dokumentation**

  Bevor Hochrisiko-KI-Systeme in Verkehr gebracht oder in Betrieb genommen werden, muss eine technische Dokumentation erstellt werden, die auf dem neuesten Stand zu halten ist. Diese soll sicherstellen und belegen, dass die nach Abschnitt 2 der Verordnung geltenden Anforderungen an Hochrisiko-KI-Systeme eingehalten werden. Für kleine und mittlere Unternehmen sowie Start-Ups besteht die Möglichkeit, für die technische Dokumentation ein vereinfachtes Formular zu verwenden, welches von der Europäischen Kommission bereitgestellt wird.

- **Aufzeichnungspflichten**

  Gemäß Art. 12 KI-VO bestehen zudem bestimmte Aufzeichnungspflichten im Zusammenhang mit Hochrisiko-KI-Systemen. Es ist eine Protokollierung, d. h. die automatische Aufzeichnung von Ereignissen während des gesamten Lebenszyklus des Systems, erforderlich.

- **Transparenzpflichten**

  Überdies sind im Zusammenhang mit der Verwendung von Hochrisiko-KI-Systemen Transparenzpflichten zu beachten, die in Art. 13 KI-VO normiert sind. Konkrete Vorgaben fehlen jedoch; nach dem Verordnungstext muss lediglich die Transparenz in einer geeigneten Art und in einem angemessenen Maß gewährleistet sein. Zudem müssen u.a. Betriebsanleitungen für die KI-Systeme bereitgestellt werden, die ein festgelegtes Mindestmaß von Informationen enthalten.

- **Menschliche Aufsicht**

  Hochrisiko-KI-Systeme müssen gem. Art. 14 KI-VO derart konzipiert sein, dass sie während der Dauer ihrer Verwendung durch Menschen beaufsichtigt werden können. Dies soll explizit die Risiken für Gesundheit, Sicherheit und Grundrechte Betroffener minimieren. Aufsichtsmaßnahmen müssen entsprechend der Höhe des jeweils bestehenden Risikos vorgenommen werden und dem Grad der Autonomie und dem Kontext der Nutzung des Systems angemessen sein.

- **Genauigkeit, Robustheit und Cybersicherheit**

  Zuletzt ist bestimmt, dass Hochrisiko-KI-Systeme derart konzipiert und entwickelt sind, dass über ihren gesamten Lebenszyklus hinweg ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit gewährleistet ist. Es soll erreicht werden, dass Hochrisiko-KI-Systeme möglichst widerstandsfähig gegenüber Fehlern, Störungen – auch Manipulation durch Dritte – und Unstimmigkeiten werden, insbesondere wenn Interaktionen mit natürlichen Personen stattfinden.

1.5.4 Geringes/Minimales Risiko

In die Risikokategorie geringes/minimales Risiko fallen grundsätzlich alle KI-Systeme, die nicht in die Kategorien „hohes" oder „unannehmbares" Risiko fallen (vgl. Art. 95 KI-VO). Beispiele für KI-Systeme mit minimalem Risiko sind etwa Spamfilter.[7]

Die Anforderungen in dieser Risikokategorie sind entsprechend weniger streng.

Anbieter von KI-Systemen der geringen Risikogruppe sollen jedoch dazu angeregt werden, die Anforderungen der höheren Risikogruppe freiwillig zu befolgen. Hierzu können etwa Verhaltenskodizes durch die Unternehmen erstellt werden (Art. 95 KI-VO).

1.5.5 General Purpose AI Models (GPAI)

Über die Kategorisierung in den drei Risikostufen hinaus beinhaltet der AI Act auch Regelungen für KI-Systeme mit allgemeinem Verwendungszweck, sog. General Purpose AI (GPAI). Hierbei handelt es sich um KI-Anwendungen, die grundsätzlich unterschiedlichen Zwecken dienen. Sie können selbstständige Systeme oder auch integrative Bestandteile anderer KI-Anwendungen sein. Beispiele für GPAI-Modelle sind insbesondere die großen Sprachmodelle (Large Language Models – LLM) wie GPT-4.o (Open AI), Google Gemini, Llama 3.1 (Meta) oder Luminous (Aleph Alpha).

Die Trennschärfe der Definition aus Art. 3 Nr. 63 KI-VO („KI-Modell mit allgemeinem Verwendungszweck") ist derzeit noch unklar.

Grundsätzlich werden diese Systeme in die dritte (geringe) Risikokategorie eingestuft, sodass für sie auch die Transparenzpflichten aus Art. 50 KI-VO gelten.

Der AI Act beinhaltet auch für die allgemeinen GPAI-Modelle einige Anforderungen, etwa die Bereitstellung technischer Unterlagen und Gebrauchsanweisungen, die Beachtung des Urheberrechts oder auch die Zusammenfassung der für das Training verwendeten Inhalte.

Pflichten der Anbieter von KI-Modellen mit allgemeinem Verwendungszweck sind in Art. 53 KI-VO der Verordnung geregelt.

[7] Von Welser , Die KI-Verordnung – ein Überblick über das weltweit erste Regelwerk für künstliche Intelligenz, GRUR-Praxis 2024, 485.

Anbieter von GPAI-Modellen mit systematischem Risiko haben überdies noch – entsprechend des hier höheren Risikos – weitergehende Pflichten zu beachten. Diese sind in Art. 55 KI-VO normiert. Konkret werden den Anbietern der GPAI-Modelle, zusätzlich zu den Anforderungen an GPAI-Modelle im Allgemeinen, die folgenden Pflichten auferlegt:

- Durchführung von Modellbewertungen mit standardisierten Protokollen und Instrumenten, die dem Stand der Technik entsprechen,
- Bewertung und Minderung möglicher systematischer Risiken einschließlich ihrer Ursachen, die sich aus der Entwicklung, dem Inverkehrbringen oder der Verwendung der GPAIs ergeben,
- sammeln von Informationen über schwerwiegende Vorfälle und Erfassen möglicher Abhilfen,
- Gewährleistung eines angemessenen Maßes an Cybersicherheit und einer physischen Infrastruktur des Modells.

1.6 Pflichten im Zusammenhang mit KI-Systemen

Aus dem dritten Abschnitt der KI-Verordnung folgt, dass insbesondere Anbietern und Betreibern von KI-Systemen, aber auch anderen Adressaten der Verordnung unterschiedliche Pflichten auferlegt werden. Wie schon aus der Kategorisierung der KI-Systeme in den Risikostufen ersichtlich wird, richten sich die Anforderungen jeweils nach der Höhe des Risikos.

Insgesamt haben Anbieter von KI-Systemen weitreichendere Pflichten aus der KI-Verordnung als beispielsweise Betreiber.[8]

In bestimmten Fällen werden jedoch Händler, Einführer, Betreiber und sonstige Dritte wie Anbieter behandelt, so dass für sie ebenfalls die nach Art. 16 KI-VO für Anbieter normierten Pflichten gelten. Es gelten entsprechende Verantwortlichkeiten entlang der KI-Wertschöpfungskette. Diese Fälle sind in Art. 25 KI-VO bestimmt. Zu bejahen ist ein solcher Fall, wenn die Beteiligten

- ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System mit ihrem eigenen Namen oder Handelsmarke versehen, ohne dass eine abweichende Pflichtenverteilung vertraglich vereinbart wird,

[8] Woesch/Vogt , Die KI-Verordnung – Die digitale Zukunft im Finanzsektor BKR 2024, 689.

- eine wesentliche Veränderung eines Hochrisiko-KI-Systems vornehmen, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, sofern es weiterhin als Hochrisiko-KI-System einzustufen ist,
- die Zweckbestimmung eines Hochrisiko-KI-Systems derart verändern, dass es danach als hochriskant einzustufen ist.

1.7 Allgemeine Pflichten unabhängig von der Risikostufe

1.7.1 KI-Kompetenz

Unabhängig von der Klassifizierung der KI-Systeme innerhalb der jeweiligen Risikogruppen existieren für Anbieter und Betreiber allgemeine Pflichten, namentlich die KI-Kompetenz nach Art. 4 KI-VO.

Demnach haben Anbieter und Betreiber von KI-Systemen Maßnahmen zu ergreifen, um sicherzustellen, 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. Hierzu gehören technische Kenntnisse, Erfahrungen, Ausbildung und Schulungen.

Den Begriff „KI-Kompetenz" definiert Art. 3 Nr. 56 KI-VO wie folgt:

*„**KI-Kompetenz** ist die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden."*

Anbieter und Betreiber müssen also dafür sorgen, dass grundlegende Konzepte und Fähigkeiten über KI-Systeme und ihre Funktionsweise sowie ihrer Risiken und Vorteile vermittelt werden. Dies kann durch regelmäßige Schulungen und Fortbildungen für Mitarbeiter geschehen.

1.7.2 Urheberrecht

Die KI-Verordnung enthält selbst keine Regelungen zum Urheberrecht, verpflichtet jedoch die Anbieter von KI-Systemen und KI-Modellen zur Einhaltung der bestehenden EU-Regelungen zum Urheberrecht. Dies führt dazu, dass beispielsweise urheberrechtsverletzender Output zusätzlich über die KI-Verordnung sanktioniert werden kann.

1.8 Pflichten der Anbieter von Hochrisiko-KI-Systemen

Welche Pflichten den Anbietern von Hochrisiko-KI-Systemen konkret auferlegt werden, wird in Art. 16 KI-VO geregelt.

Einerseits haben Anbieter von Hochrisiko-KI-Systemen **alle generellen** Anforderungen aus Abschnitt 2 der Verordnung zu erfüllen. Darüber hinaus treffen Anbieter die folgenden Pflichten:

- Angabe des Namens/Handelsnamens/Handelsmarke sowie einer Kontaktanschrift,
- Einführung eines Qualitätsmanagementsystems,
- Aufbewahrung der Dokumentation,
- Aufbewahrung automatisch erzeugter Protokolle,
- vor dem Inverkehrbringen oder der Inbetriebnahme muss das KI-System einem Konformitätsbewertungsverfahren unterzogen werden, eine Konformitätserklärung ist auszustellen nebst einer CE-Kennzeichnung,
- Erfüllen der Registrierungspflichten nach Art. 49 KI-VO,
- Ergreifen erforderlicher Korrekturmaßnahmen und Bereit-stellung erforderlicher Informationen nach Art. 20 KI-VO,
- Nachweisbarkeit der Erfüllung der Anforderungen aus Abschnitt 2 der KI-Verordnung gegenüber Behörden,
- Erfüllen der Barrierefreiheitsanforderungen nach den Richtlinien[9] (EU) 2016/2012 und (EU) 2019/882,
- Beobachtung des KI-Systems nach Inverkehrbringen (Art. 72 KI-VO),
- Meldung schwerwiegender Vorfälle bei Marktüberwachungsbehörden (Art. 73 KI-VO).

[9] EU-Richtlinie (EU) 2016/2012 vom 26.10.2016, https://t1p.de/slto0 (Stand: 03.12.2024); EU-Richtlinie (EU) 2019/882 vom 17.04.2019, h ttps://t1p.de/ejz77 (Stand: 03.12.2024).

1.9 Pflichten der Einführer von Hochrisiko-KI-Systemen

Einführer von Hochrisiko-KI-Systemen haben nach Art. 23 KI-VO die Pflicht, das KI-System vor dem Inverkehrbringen daraufhin zu überprüfen, ob es den Anforderungen der Verordnung entspricht. Dies betrifft aber nicht alle Anforderungen, sondern nur die Überprüfung hinsichtlich

- der Durchführung des Konformitätsbewertungsverfahrens nach Art. 43 KI-VO durch den Anbieter,
- der Erstellung der technischen Dokumentation nach Art. 11 KI-VO und Anhang IV durch den Anbieter,
- dem Vorhandensein der CE-Kennzeichnung und ob die EU-Konformitätserklärung sowie die erforderliche Betriebsanleitung beigefügt sind und
- ob der Anbieter einen Bevollmächtigten benannt hat.

1.10 Pflichten der Händler beim Handel mit Hochrisiko-KI-Systemen

Auch Personen, die Handel mit Hochrisiko-KI-Systemen betreiben, werden durch die KI-Verordnung gewisse Pflichten auferlegt. Sie müssen – neben anderem – vor der Bereitstellung auf dem Markt zunächst prüfen, ob die erforderliche CE-Kennzeichnung, die EU-Konformitätserklärung sowie die Betriebsanleitung vorliegen. Überdies müssen Händler sicherstellen, dass Anbieter sowie Einführer ihre Pflicht zur Angabe von Kontaktdaten erfüllt haben sowie ein Qualitätsmanagementsystem nach Art. 17 KI-VO vorhanden ist.

1.11 Pflichten der Betreiber von Hochrisiko-KI-Systemen

Ein Großteil der praxisrelevanten Fälle betrifft Unternehmen, die Hochrisiko-KI-Systeme einsetzen, mithin Unternehmen als Betreiber solcher Systeme.

In Art. 26 KI-VO sind die Pflichten der Betreiber von HochrisikoKI-Systemen festgelegt. Betreiber haben einen deutlich geringeren Pflichtenkatalog zu befolgen als Anbieter.

Konkret gelten die folgenden Pflichten:

- Treffen geeigneter technischer und organisatorischer Maßnahmen, um sicherzustellen, dass KI-Systeme entsprechend der beigefügten Betriebsanleitungen verwendet werden,

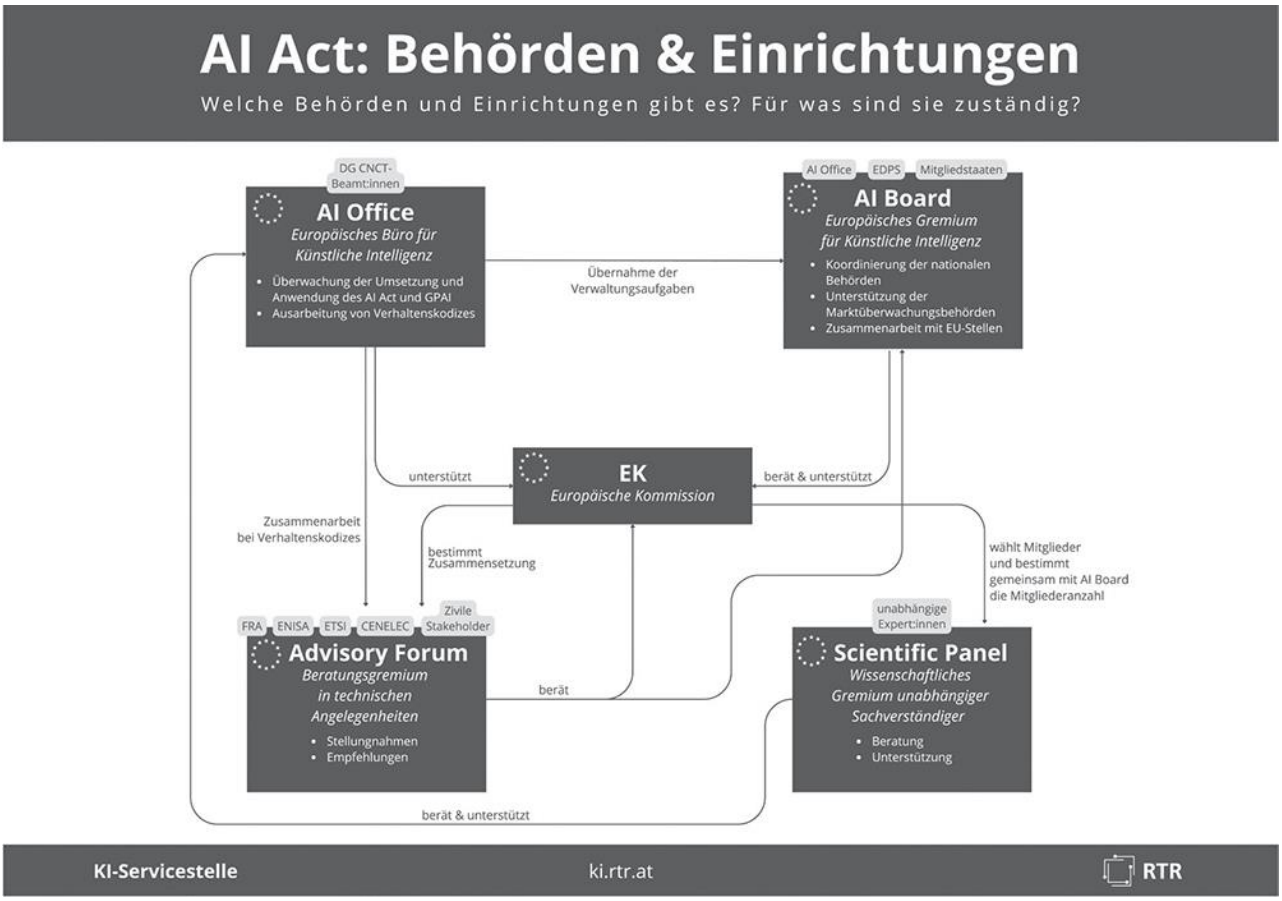
- Menschliche Aufsicht durch ausgewählte und kompetente natürliche Personen,
- Eingabedaten müssen der Zweckbestimmung des HochrisikoKI-Systems entsprechen und ausreichend repräsentativ sein,
- Überwachung des Betriebs des Hochrisiko-KI-Systems anhand der Betriebsanleitung und ggf. Informationsweitergabe an die Anbieter,
- Aufbewahrung automatisch erzeugter Protokolle,
- ggf. Information von Arbeitnehmern über die Verwendung von Hochrisiko-KI-Systemen,
- Registrierungspflichten nach Art. 49 KI-VO,
- Genehmigungspflicht bei Nutzung eines Hochrisiko-KI-Systems zur biometrischen Fernidentifizierung im Rahmen von Ermittlungen zur Strafverfolgung,
- ggf. Information natürlicher Personen, sofern diese der Nutzung eines Hochrisiko-KI-Systems unterliegen,
- Zusammenarbeit mit Behörden.

Darüber hinaus müssen Betreiber eines Hochrisiko-KI-Systems, sofern es sich um Einrichtungen des öffentlichen Rechts oder private Einrichtungen, die öffentliche Dienste erbringen, handelt, eine Prüfung der Auswirkungen auf Grundrechte Betroffener vornehmen. Hierzu muss eine Abschätzung vorgenommen werden, die u. a. analysiert wie, wann und wie häufig das KI-System genutzt wird, wer davon betroffen sein könnte oder ob es beispielsweise Schadensrisiken gibt. Die Anforderungen an die Grundrechte-Folgenabschätzung sind in Art. 27 KI-VO geregelt.

1.12 Anforderungen an die Mitgliedstaaten

Die EU-Mitgliedstaaten werden durch die KI-Verordnung verpflichtet, gewisse Maßnahmen zum Schutz vor den Gefahren bei dem Umgang mit KI-Systemen zu ergreifen und sind zu deren Weiterentwicklung verpflichtet.

Wie sich die Einrichtungen auf EU-Ebene nach der KI-Verordnung zusammenstellen und welche Aufgaben jeweils übernommen werden, wird nachfolgend skizziert:[10]



[10] Bild abrufbar unter: https://t1p.de/qe6t4 (Stand: 03.12.2024).

1.13 Sanktionen bei Verstößen gegen den EU AI Act

Der EU AI Act beinhaltet Sanktionen für den Fall, dass gegen die Anforderungen verstoßen wird. Verstöße können Geldbußen von bis zu 35 Mio. Euro oder bis zu 7 % des gesamten weltweiten Jahresumsatzes des vorherigen Geschäftsjahres des betroffenen Unternehmens zur Konsequenz haben.

Möglich ist neben Sanktionen in Form von Geldbußen auch das Aussprechen von Verwarnungen sowie von anderen nichtmonetären Maßnahmen.

Die Höchststrafe von bis zu 35 Mio. Euro oder 7 % des Jahresumsatzes ist bei einer Missachtung des Verbots von KI-Systemen der höchsten Risikostufe (unannehmbares Risiko) möglich. Es gilt im Einzelfall der höhere Betrag, dieser kann also auch über 35 Mio. Euro liegen.

Eine Geldbuße von bis zu 15 Mio. Euro oder, im Falle von Unternehmen, bis zu 3 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, kann für folgende Verstöße verhängt werden:

- Verstoß gegen Pflichten der Anbieter von Hochrisiko-KI-Systemen nach Art. 16 KI-VO und Bevollmächtigte der Anbieter nach Art. 22 KI-VO,
- Verstoß gegen Pflichten der Einführer nach Art. 23 KI-VO,
- Verstoß gegen Pflichten der Händler nach Art. 24 KI-VO,
- Verstoß gegen Pflichten der Betreiber von Hochrisiko-KISystemen nach Art. 26 KI-VO,
- Verstoß gegen bestimmte Anforderungen, die für notifizierende Stellen gelten (Art. 31 KI-VO),
- Verstoß gegen für Anbieter und Betreiber geltende Transparenzpflichten (Art. 50 KI-VO).

Bei der Bereitstellung falscher, unvollständiger oder irreführender Informationen durch notifizierende Stellen sind Geldbußen von bis zu 7,5 Mio. Euro oder 1 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres möglich.

Die Verordnung enthält einen Katalog von Kriterien, anhand derer zu entscheiden ist, ob eine Geldbuße verhängt wird. Zu berücksichtigen sind demnach z. B. Art, Schwere, Dauer und Folgen des Verstoßes unter Berücksichtigung des Zwecks des KI-Systems und der betroffenen Personen sowie des Schadensausmaßes, erschwerende oder mildernde Umstände im Einzelfall und andere Umstände.

1.14 Rechtsbehelfe

Zum Schutz der von der KI-Verordnung Betroffenen enthält die Verordnung eigene Rechtsbehelfe:

- Recht auf Beschwerde bei einer Marktüberwachungsbehörde (Art. 85 KI-VO) bei Verstößen gegen die Verordnung, dabei ist jede natürliche oder juristische Person beschwerdebefugt,
- Recht auf Erläuterung der Entscheidungsfindung (Art. 86 KI-VO) in Bezug auf rechtlich erhebliche Entscheidungen von Betreibern,
- Anwendung der Hinweisgeberrichtline (EU) 2019/1937 bei der Meldung von Verstößen; in Deutschland gilt hierfür seit 2023 das Hinweisgeberschutzgesetz (HinSchG).[11]

1.15 Umsetzung des EU AI Act in der Bundesrepublik Deutschland

Der EU AI Act muss von jedem Mitgliedstaat in nationales Recht umgesetzt werden, wobei den Mitgliedstaaten ein gewisser Gestaltungsspielraum zusteht.

Hierzu bleibt mit Stand heute (Dezember 2024) abzuwarten, wie diese Umsetzung erfolgt.

[11] Hinweisgeberschutzgesetz (HinSchG) vom 31.05.2023, BGBl. 2023 I, 140.

2 Der EU AI Act in der Praxis für Unternehmen und Unternehmer

Der EU AI Act hat – wie bereits angedeutet – praktische Auswirkungen auf Abläufe und Strukturen im Unternehmen.

Es wird nur wenige Unternehmen geben, die zukünftig **nicht** in der einen oder anderen Art und Weise künstliche Intelligenz einsetzen werden.

2.1 Vorprüfung

Generell sollte jedes Unternehmen vor dem Hintergrund des EU AI Acts unverzüglich eine Art Vorprüfung anstellen, die sich grob wie folgt darstellt:

1. Handelt es sich bei dem bereits eingesetzten oder konkret zur Verwendung beabsichtigten IT-System um ein KI-System im Sinne der KI-Verordnung?
2. Soll das KI-System bestimmungsgemäß in einem Hochrisikobereich eingesetzt werden oder wird es das bereits?
3. Greift eine der hierzu in der KI-Verordnung geregelten Ausnahmen?
4. Welche Regelungen greifen für das Unternehmen?

Man sollte sich generell die Frage stellen:

Ob und in welchem Maße haben Mitarbeiter im Unternehmen generell und auch speziell für den Betrieb der vom Unternehmen eingesetzten KI die notwendige **KI-Kompetenz**? Was müssen wir tun, um diese herzustellen?

Dies gilt gleichermaßen für Unternehmen sowie Behörden.

2.2 Regeln zur KI als Compliance-Thema

Die Einhaltung von Regelungen zum Einsatz von künstlicher Intelligenz ist natürlich ein Compliance-Thema.

Compliance kann als die allgemeine Verpflichtung verstanden werden, in einem Unternehmen dafür zu sorgen, dass gesetzliche Regeln und Auflagen eingehalten werden, damit auf diese Weise unerwartete Haftungen nicht drohen und auch strafrechtlich relevante Tatbestände nicht verwirklicht werden.

Gerade auch mittelständische Unternehmen sind darauf angewiesen, ein System der Regeleinführung, -beachtung und -überwachung einzuführen, um das Unternehmen vor Haftung zu schützen.

Hierdurch soll sichergestellt werden, dass das Unternehmen in Übereinstimmung mit gesetzlichen, behördlichen oder sonstigen Auflagen geführt und betrieben wird. Hierzu können auch Regeln gehören, die sich das Unternehmen (die Unternehmensführung) selbst setzt.

Das im Unternehmen eingerichtete System, durch welches Regeltreue sichergestellt werden soll, ist das sog. Compliance Management System, CMS.

2.3 Notwendige Maßnahmen beim Einsatz von KI im Unternehmen

Hat die Vorprüfung (→*Kapitel 2.1*) ergeben, dass im Unternehmen KI eingesetzt wird oder der Einsatz geplant ist, muss zwingend festgestellt und festgelegt werden, welche Regelungen für das Unternehmen gelten. Zudem ist im Rahmen des Compliance-Management-Systems festzulegen, wie die Einhaltung dieser Regelungen sichergestellt wird.

Hier kann in folgenden Schritten vorgegangen werden:

- Unternehmensanalyse/Unternehmensstrategie zu KI (→*Kapitel 2.3.1*).
- Finden und Festlegen der geltenden Regeln für KI (→*Kapitel 2.3.2*).
- Kommunikation im Unternehmen, Mitarbeiterschulung, Unternehmensführung (→*Kapitel 2.3.3*).

2.3.1 Unternehmensanalyse/Unternehmensstrategie zu KI

Abteilungen, die möglicherweise mit KI in Berührung kommen oder diese einsetzen, sollten im Rahmen von Workshops möglichst viele Mitarbeiter einbeziehen, um folgende Fragen zu beantworten:

- In welchen Bereichen setzen wir KI bereits ein?
- Wo könnten wir KI noch einsetzen, und wo wäre dies wünschenswert?
- Scheuen sich die Mitarbeiter, auf KI zurückzugreifen, und warum?

2.3.2 Finden und Festlegen der geltenden Regeln für KI

Nachdem in Rahmen der Unternehmensanalyse ermittelt wurde, wo KI bereits eingesetzt wird und wo sie zukünftig eingesetzt werden soll, müssen die verschiedenen Einsatzarten gemäß den in den vorstehenden Kapiteln beschriebenen Regelungen des EU AI Acts überprüft werden.

Dabei wird zunächst geklärt, ob und in welchem Umfang HochrisikoKI genutzt wird und es ist sicherzustellen, dass keine verbotene KI zum Einsatz kommt.

Anschließend werden betriebsinterne Regelwerke erstellt, die es den Mitarbeitern ermöglichen, KI regelkonform einzusetzen.

2.3.3 Kommunikation im Unternehmen, Mitarbeiterschulung, Unternehmensführung

Sobald das Regelwerk für den Einsatz von Künstlicher Intelligenz auf Management- und Unternehmensführungsebene erstellt wurde, muss es im Unternehmen kommuniziert werden. Die Mitarbeiter sind entsprechend zu schulen, um sicherzustellen, dass sie die Regelungen zum Einsatz von KI verstehen und einhalten.

Darüber hinaus sollte das Unternehmen eine Strategie entwickeln, die den zukünftigen Umgang mit dem Einsatz von KI generell festlegt und die Haltung der Unternehmensführung dazu klärt.

2.4 Überblick: Prozess „KI im Unternehmen“

Der folgende Überblick über verschiedene Fragestellungen kann als Vorlage für einen unternehmensinternen Prozess zum Thema „KI im Unternehmen“ dienen:

Mehr als Digitalisierung von Prozessen: KI verändert das Arbeiten in den Unternehmen grundsätzlich und wirft viele Fragen auf

Unternehmensstrategie	Recht & Compliance	Unternehmenskommunikation
▪ Warum setzt das Unternehmen bereits KI ein? ▪ Wo könnte KI noch zum Einsatz kommen? ▪ Was macht der Wettbewerb? ▪ Wer kümmert sich um das Thema KI im Unternehmen – technologisch und strategisch?	▪ Was sind die rechtlichen Rahmenbedingungen - für KI schon im Einsatz? - für KI, die kommt? ▪ Wo könnten wir den Wettbewerb angreifen? ▪ Welche internen Regeln setzen wir uns? ▪ Welchen Einfluss hat KI auf unseren Nachhaltigkeitsbericht und unsere Compliance-Statuten?	▪ Warum brauchen wir KI? ▪ Warum macht uns KI keine Angst? ▪ Für welche Aufgaben und wie können wir KI sinnvoll nutzen? ▪ Welches Know-How brauchen wir dafür? ▪ Welche Regeln gilt es zu beachten? ▪ Wie verändert KI unsere Unternehmenskultur und unser Selbstverständnis (KI als Teil unseres Leitbildes/Wertesystems), wie gehen wir verantwortungsvoll mit KI um?

2.5 Überblick: KI im Unternehmen – Aufgaben und handelnde Personen

Die Auseinandersetzung mit dem Thema „KI im Unternehmen" ist ein Prozess, der die Einbindung nahezu aller Unternehmensbereiche erfordert, da der Einsatz von KI das Unternehmen und die Geschäftstätigkeit nachhaltig verändern wird.

Eine erste Übersicht über die Kernaufgaben und die wesentlichen Beteiligten gibt die folgende Darstellung:

Aufgaben und handelnde Personen

Ist-Analyse/Audit	**Kommunikationsstrategie/-umsetzung**	**Rechtliche Regelwerke/Compliance**
▪ Audit-Workshop mit Top-Management und ausgewählten Führungskräften - Status-Quo und Ausblick KI - Blockade/Schwierigkeiten ▪ Führungskräfte einschl. Geschäftsführung ▪ Abteilungsleiter ▪ KI-Beauftragter (sollte solch eine Stelle geschaffen werden?)	▪ Entwicklung Kommunikationsstrategie KI & digitale Transformation ▪ Entwicklung Inhalte (Digital-Story) ▪ Einbindung verantwortungsvoller Umgang mit KI in Unternehmenskultur: - Wie beeinflusst KI unser Miteinander, unsere Werte, unser Selbstverständnis, unser Kundenverhältnis? ▪ Führungskräftekommunikation und Coaching ▪ Regelkommunikation Transformationsprozess KI Kommunikationsabteilung mit HR oder externe Berater	▪ Anpassung des Compliance Management Systems ▪ Festlegung rechtlicher Rahmenbedingungen ▪ Anbindung an Meldestelle HinSchG ▪ Schulung KI-Mitarbeiter ▪ Wirtschaftsanwälte Unternehmensberater im Bereich IT/Prozesse ▪ Steuerberater/WB für Nachhaltigkeitsberichte ▪ Wirtschaftsstrafverteidiger

Ulf Schmitt & Partner mbB, E.T.A.-Hoffmann-Str. 3, 96047 Bamberg,

Telefon: 0951 980 440, Telefax: 0951 980 4450

E-Mail: info@steuerkanzlei-schmitt.de, Internet: www.steuerkanzlei-schmitt.de