Verordnung zur Regulierung eigenständiger Technologien:

KI-Verordnung (AI Act) soll Kompetenzen stärken

Geregelt wird in der Künstliche Intelligenz-Verordnung (KI-VO) der Umgang mit potentiell sehr gefährlicher Technik, wie in der FAZ vom 05.08.24 zu lesen war. KI begegnet uns überall, und jeder sollte wissen, bzw. lernen, wie damit umzugehen ist.

Definition laut KI-VO

KI ist eine autonome und deshalb nicht beherrschbare Technik, die sich ohne menschliches Zutun verändern kann. Es geht in der Verordnung um den Schutz natürlicher Personen vor der Technik.
Software, die nur nach bestimmten Mustern sucht und diese auswertet, ist keine KI nach dieser Verordnung, da die Fähigkeit zur eigenständigen Veränderung fehlt.
KI-Modelle und **KI-Systeme** fallen unter die KI-VO. Ein KI-Modell ist ein riesiger Datenpool, aus dem ein KI-System seine Informationen bezieht. Hier wird von der Technik nach Informationen jeder Art (Text, Bild, Ton) gesucht. Es gibt KI-Modelle für spezielle Bereiche und auch für allgemeine Anfragen (General Purpose AI). Chat GPT ist z. B. ein allgemeines Modell, hier werden Aufgaben gelöst, die in den verschiedensten Situationen entstehen. Es werden Texte zu bestimmten Themen verfasst, und entsprechend mit Fotos und Graphiken versehen. Durch die Software werden Inhalte generiert, die nicht mehr von menschlich erzeugten Ergebnissen unterschieden werden können.

Zweck der KI-VO

Durch die KI-VO soll sichergestellt werden, dass die KI-Systeme *„sicher, transparent, ethisch, unparteiisch und unter menschlicher Kontrolle sind."* Auch wenn die Inhalte in Drittländern erstellt werden, aber in der EU verfügbar sind, fallen sie unter die KI-VO.

Geltungsbereich der KI-VO

Die KI-VO gilt für alle, die KI im beruflichen Kontext benutzen. Der Nutzer wird zum Betreiber im Sinne der Verordnung, wenn er z. B. auf der Unternehmenswebseite einen Sprachbot oder einen Textbot einsetzt, der mit dem Kunden kommuniziert. Auch wenn Sie Bilder mit Hilfe der KI für Publikationen erstellen, werden Sie zum Betreiber der KI.
Betreiben bedeutet, ebenfalls analog zur Nutzung von Maschinen, ein KI-System zu benutzen. Das Verwenden des Hilfsmittels ist im Rechtssinn ein Betreiben und der Nutzer wird somit zum Betreiber. Die Nutzung im privaten Bereich fällt nicht unter die Verordnung. Zu beachten ist allerdings, wenn ein Mitarbeiter (mit Erlaubnis des Chefs) auf seinem privaten Smartphone ChatGPT oder eine andere KI-Anwendung installiert hat und diese dann im Büro nutzt, wird die Nutzung beruflich und fällt unter die KI-VO. Dies ist analog zu sehen mit dem menschlichen Schreiben eines Textes auf einem privaten Gerät mit privater Software und beruflichem Inhalt. Dieser Text ist auch nicht privat.

Pflichten der KI-Verwender

Nutzer eines KI-Systems im beruflichen Kontext müssen die Vorgaben der KI-VO beachten. Da diese sehr komplex sind, sollte nicht gewartet werden, bis die Verordnung in Kraft tritt, sondern Sie sollten schon jetzt tätig werden. Zu beginnen ist mit einer **Sensibilisierung der Mitarbeiter** (und der Geschäftsführung) für die **Chancen** und **Risiken** der KI-Nutzung. Einzelne Daten sind oft nur einfache Fakten, das Zusammenführen von verschiedenen Datenquellen und das Verarbeiten großer Datenmengen kann aber weitergehende Informationen erstellen, die missbraucht werden können. Auch können die Ergebnisse ungenau oder sogar falsch sein, wenn die Fragestellungen für die Verarbeitung nicht korrekt sind. Deshalb ist eine menschliche Plausibilitätsprüfung unverzichtbar.

KI-Kompetenz

Artikel 4 der KI-VO schreibt vor, dass jeder der KI beruflich nutzt, KI-Kompetenz besitzen und vermitteln muss. Es sind also nicht nur Unternehmen betroffen, sondern auch einzelne Mitarbeiter. **Der Nachweis dieser Kompetenzen ist ab dem 02.02.2025 verpflichtend.**
KI-Kompetenz bedeutet, z.B. folgende Fragen sicher beantworten zu können:

- Was ist ein KI-System?
- Was bedeutet Autonomie von KI?
- Warum kann KI nicht denken und trotzdem mit mir sprechen?
- Welche Nutzung von KI-Systemen ist gefahrlos möglich?
- Was bedeutet *„prompten"*, und wie geht das?
- Wie behalte ich als Mensch die Kontrolle über das Werkzeug KI?
- Was bedeutet der Einsatz von KI im beruflichen Alltag?
- Wo kann mir die Technik helfen, wo nicht?

Hinweis: Sie sollten prüfen, ob und wenn ja welche Software in ihrem Unternehmen KI nutzt. Dies können Sie über Software-Asset-Management-Systeme für Lizenzprüfungen machen oder im Lizenzordner sehen.

Unterschiedliche Vorgaben

Es gibt **allgemeine**, von jedermann einsetzbare **Systeme**, wie z.B. ChatGPT oder das Übersetzungsprogramm Deepl, die zu den General Purpose AI gehören, und natürlich auch **Hochrisikosysteme**, die sehr spezialisiert sind und mit besonders schützenswerten Daten arbeiten. Diese können aus den unterschiedlichsten Bereichen kommen: Gesundheitsdaten, Wirtschaftsdaten, Finanzdaten. Hier müssen von den Herstellern klare Dokumentationen erfolgen, sowohl, was die Herstellung als auch, was die Nutzung dieser Systeme angeht.
Die Vorgaben für die Nutzung (Kap. 3 KI-VO, Art. 29 und 52) werden durch die KI-VO konkretisiert:
Ab **02.02.2025** gelten Verbote einzelner Praktiken im Bereich der künstlichen Intelligenz (Art. 5 KI-VO).

- Unterschwellige, den Betroffenen unbewusste wesentliche Verhaltensbeeinflussung mit Schadenspotential,
- Einsatz von KI-Systemen zur Ausnutzung von Schwächen oder Schutzbedürftigkeit von Personen aufgrund von Alter oder geistiger Behinderung zu einer wesentlichen Verhaltensbeeinflussung, die dadurch Schadenspotential haben,
- KI-Systeme zum Scoring der Vertrauenswürdigkeit von Personen auf der Basis von Daten zu sozialem Verhalten oder persönlicher Eigenschaften oder Persönlichkeitsmerkmalen mit Folgen der zusammenhanglosen, ungerechtfertigten oder unverhältnismäßigen Schlechterstellung oder Benachteiligung (*„China-Social Scoring"*),
- KI-Einsatz zur Personenidentifizierung (z.B. Gesichtserkennung) in öffentlich zugänglichen Räumen für die Strafverfolgung, soweit nicht unbedingt erforderlich, um potentielle Opfer von Straftaten zu suchen, vermisste Kinder zu finden, zur Abwehr von unmittelbar personengefährdenden Terroranschlägen oder der Verfolgung bestimmter Straftaten.

Risikobasierter Ansatz

Durch die KI-VO werden drei Kategorien von Risiken berücksichtigt:

1) risikolos und erlaubt
2) hochriskant und nur unter strengen Bedingungen zulässig und
3) verboten

Ad 1) GPAI wie ChatGPT werden auch von der KI-VO erfasst. Aber wenn der Zweck der Anwendung nicht als hochriskant von der Verordnung angesehen wird, kann die Anwendung ohne Einschränkung genutzt werden. Diese Anwendungen stellen dann kein oder ein sehr geringes Risiko für Rechte und Freiheiten der Menschen dar.

Ad 2) Hochriskant sind Anwendungen, die z.B. dazu dienen, Lernergebnisse zu verfälschen oder Arbeitsbedingungen zu beeinflussen. Ebenso Anwendungen im Gesundheitsbereich und der Justiz.

Jeder, der KI benutzt, muss also immer abwägen, ob die Verwendung der KI evtl. hochriskant ist. Hier darf nicht davon ausgegangen werden, welche positiven Effekte der Einsatz hat, sondern es muss auch bedacht werden, was an Rechtsverletzungen möglich ist. Zahlreiche Rechtsvorschriften können durch den Einsatz von KI verletzt werden: Datenschutzrecht, Urheberrecht, Markenrecht, Grundrechte der Menschen.

Ad 3) Verbotene Aktionen durch KI sind zum Beispiel die Eingabe geheimer Daten von Forschungsprojekten oder die Eingabe von nichtöffentlichen Betriebszahlen, um hieraus dann Berechnungen erstellen zu lassen. KI lernt nämlich durch die Daten, die ihr zur Verfügung gestellt werden, so dass solche Eingaben durchaus an die Öffentlichkeit kommen können. Ebenfalls verboten ist es in Deutschland, Menschen durchgängig zu scannen und zu klassifizieren, um dann weitere Maßnahmen zu ergreifen. Auch wenn es im Falle von Straftaten wichtig sein könnte, auf solches Social Scoring zurückzugreifen, würden hier überwiegend unbescholtene Bürger überwacht, was unserem Freiheitsbild entgegen läuft und deshalb verboten ist.

Sanktionen

Bei Verstößen gegen die KI-VO werden – wenn die VO umgesetzt wurde – je nach Schwere des Vergehens Bußgelder in nicht unerheblicher Höhe fällig. Es gilt: Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein, aber die Interessen von kleinen und mittleren Unternehmen, inklusive Start-up-Unternehmen, einschl. deren wirtschaftliches Überleben berücksichtigen (Art. 99 Abs.1). Vorgesehen sind je nach Art und Schwere des Verstoßes Geldbußen, die im Extremfall Millionen betragen können.

Verwaltung – KI-Amt der EU

Das KI-Amt wird eine Schlüsselrolle bei der Umsetzung des europäischen KI-Gesetzes spielen und ein innovatives EU-Ökosystem für vertrauenswürdige KI fördern. Das Amt wurde offiziell am 16. Juni 2024 eingerichtet.

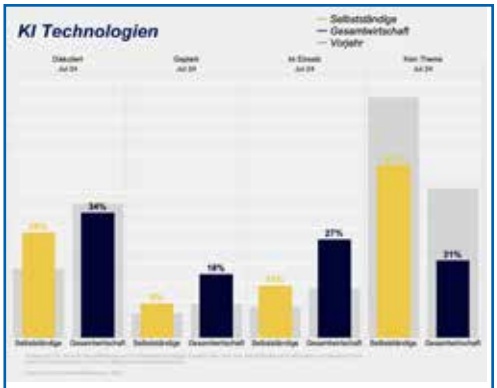
140 Mitarbeiter sollen unter wissenschaftlicher Leitung die Entwicklung von KI so beeinflussen, dass der gesellschaftliche und wirtschaftliche Nutzen bei Risikominimierung gesteigert wird. Auch ist das Amt an der Durchsetzung der KI-VO beteiligt. Momentan werden Leitlinien erarbeitet, die den Umgang mit KI-Systemen konkretisieren sollen.

Die EU-Mitgliedsstaaten müssen bis zum **2. August 2025** ein **Durchführungsgesetz** erlassen, in dem u.a. *„Allgemeine Marktüberwachungsbehörden"* benannt werden.

Vom Branchenverband Bitkom gibt es Leitfäden zum Umgang mit KI. Sie können diese in der Geschäftsstelle bekommen
E-Mail: claudia.koch@zhh.de.

Fazit

Auch wenn es noch bis Sommer 2026 dauert, bis die Regelungen der KI-VO umgesetzt werden müssen, sollten Sie nicht solange warten. Die Vorbereitungen erfordern Zeit, Geld und Gewöhnung. Je



Umfrage des ifo Instituts im Auftrag von Jimdo (Internetdienstleister) – KI in Klein- und Kleinstunternehmen Handwerkszeitung vom 15.08.2024

häufiger die Regeln in der Praxis angewendet werden, desto leichter wird die Entscheidung, ob der Einsatz erlaubt ist.

Derzeit wird überall von KI gesprochen, in Nachrichtentexten im Internet liest man immer häufiger den Hinweis *„erstellt mit Hilfe von künstlicher Intelligenz"*. Die tatsächlichen Nutzerzahlen sehen aber anders aus: Bei Rolf Becker ist zu lesen, dass erst 13 Prozent der Unternehmen KI einsetzen, weitere 33 Prozent es erst planen oder darüber sprechen. Hier wird schon regulierend eingegriffen, obwohl der Nutzerkreis noch recht überschaubar ist. Einerseits gut, da es sich um eine Technologie handelt, die recht schnell missbraucht werden kann (Stichwort Fake News in Wort und Bild), aber andererseits können diese Regulatorien innovative Ideen einschränken.

Im September hat in Zusammenarbeit mit dem Mittelstand-Digital Zentrum Handel ein vielbeachtetes Online-Seminar zum Thema Prompting stattgefunden.

Auf dem 8. PVH-Kongress in Köln am 14.03.2025 werden wir uns ausführlich mit dem Thema KI befassen und es aus verschiedenen Blickwinkeln betrachten.

Mehr Informationen hierzu in der Geschäftsstelle: gf@zhh.de.

Quellen: u.a.
RA Rolf Becker, Rechtstipp August 2024 ECC-Rechtstipp; Haufe, verschiedene Seiten; FAZ

Timetable

KI-VO ist am **01. August 2024** in Kraft getreten und wird nun schrittweise umgesetzt.

Ab **02. Februar 2025** muss sichergestellt sein, dass jeder, der KI im beruflichen Kontext und eigener Verantwortung nutzt, über ausreichende KI-Kompetenz verfügt. Hier muss für die Weiterbildung der Betroffenen gesorgt werden.

Ab **02. Februar 2025** sind auch verschiedene Nutzungen von KI verboten: es darf keine indirekte Beeinflussung durch KI stattfinden, keine soziale Bewertung oder das Hervorrufen von Emotionen. Wer durch KI z.B. die Zufriedenheit in der Belegschaft oder die Prüfungsangst der Azubis erfragen will, der beeinflusst evtl. das Verhalten der Mitarbeiter.

Bis zum **02. August 2025** muss seitens des Staates eine Leitungsstruktur erstellt werden und Verfahren zur Überwachung der KI-VO installiert sein. Die Bundesnetzagentur könnte die verantwortliche Behörde werden. Interessiert sind allerdings auch die Datenschutzbehörden.

Ab dem **02. August 2026** gilt die KI-VO in weiteren Teilen: Nun müssen besondere Anforderungen an Transparenz, Datenqualität und vieles mehr erfüllt werden. Besonders betroffen sind Systeme, die zur Erstellung von Inhalten wie Texten, Bildern, Videos oder Musik genutzt werden. Hier muss grundsätzlich kenntlich gemacht werden, dass KI benutzt wurde. Verantwortliche Nutzer der KI müssen sicherstellen, dass die Betriebsanleitung beachtet wird und dass es eine menschliche Aufsicht über den Betrieb der KI gibt.