

VERBOTEN, RISKANT ODER UNBEDENKLICH?

Wie der AI-Act künstliche Intelligenz sortiert und was das für Unternehmen bedeutet

Bereits seit 2018 ist mit der Datenschutz-Grundverordnung (DSGVO) ein EU-Gesetz in Kraft, das den Schutz personenbezogener Daten regelt. Die DSGVO soll sicherstellen, dass Unternehmen, Behörden und Organisationen mit Namen, E-Mail-Adressen, Bildern, Standortdaten und anderen heiklen Informationen verantwortungsvoll umgehen.

Mit dem AI-Act ist seit 1. August 2024 eine weitere Verordnung hinzugekommen, die Spielregeln für den Einsatz von künstlicher Intelligenz vorgibt. Ziel dieses weltweit ersten Regelwerks für künstliche Intelligenz ist, Risiken von KI einzudämmen, Innovation aber dennoch zu ermöglichen.

Erste Pflichten und KI-Kompetenz

Der AI-Act greift etappenweise: Schon seit 2. Februar 2025 sind bestimmte KI-Anwendungen in der EU verboten. Darunter fallen etwa manipulative KI-Anwendungen, die Menschen täuschen oder auch „Social-Scoring“-Praktiken, wie sie in China eingesetzt werden, um das Verhalten von Bürgerinnen und Bürgern zu

bewerten und zu sanktionieren. Zusätzlich müssen Unternehmen schon jetzt nachweisen können, dass Mitarbeitende, KI nutzen, entsprechend geschult sind – Stichwort „KI-Kompetenz“.

Einer, der den Umsetzungsprozess genau beobachtet, ist Michael Pachinger von der Rechtsanwaltskanzlei Saxinger. Pachinger ist Experte für Rechtsmaterien wie den AI-Act und die DSGVO und berät zahlreiche Unternehmen und Organisationen. Sein Eindruck: Verbotene KI-Praktiken sind in österreichischen Betrieben bislang ohnehin weniger verbreitet. Schwieriger ist jedoch der Nachweis der KI-Kompetenz. „Das Problem ist: Was ist KI-Kompetenz? Zunächst ein gewisses Bewusstsein, ob überhaupt KI-Tools eingesetzt werden. Dann braucht es Schulungen und die Sensibilisierung der Mitarbeitenden, die erkennen: Hier müssen wir achtgeben, weil relevante KI enthalten sein könnte“, erläutert Pachinger.

Hochrisiko-KI und Transparenz

Neben dem Verbot bestimmter KI-Praktiken nimmt der AI-Act auch eine Ab-

stufung zwischen unbedenklichen und hochriskanten KI-Anwendungen vor. Rechtsanwalt Pachinger: „Als hochriskant gilt beispielsweise der Bereich des Personalmanagements, aber auch etwa das Bewerten von Leistungen von Mitarbeitenden durch KI-Systeme. Unbedenklich wären zum Beispiel Spamfilter, aber spannend wird’s bei bestimmten KI-Systemen, wie Chatbots, die Texte, Inhalte oder Videos generieren und verändern. Daran könnten sich unter Umständen Transparenzpflichten knüpfen, wenn diese Deepfakes beinhalten und veröffentlicht werden sollen“, betont Pachinger und bezieht sich mit sogenannten Deepfakes auf Bilder, Video- oder Audioaufnahmen, die von einer KI erzeugt oder verändert wurden, wirklichen Personen, Gegenständen etc. ähneln und fälschlicherweise als echt erscheinen. Die diesbezüglichen Transparenzpflichten treten mit 2. August 2026 in Kraft, zeitgleich mit weiteren Anordnungen des AI-Acts.

KI im Personalmanagement

Besonders im Personalmanagement sieht Michael Pachinger Handlungsbe-

Diese vier Praxistipps gibt Rechtsanwalt Michael Pachinger Unternehmen, die KI einsetzen (wollen):

1. Kennen Sie Ihr KI-Tool und wissen Sie, dass Sie KI einsetzen.
2. Setzen Sie sich von Beginn des Projekts an mit den Prämissen des Einsatzes und rechtlichen Vorgaben auseinander.
3. Sehen Sie es als laufenden Prozess und nicht einmaliges Handeln.
4. Prüfen Sie den Einsatz von KI sorgfältig, aber nicht allein, sondern nehmen Sie Ihre Vertragspartner/KI-Anbieter in die Pflicht!



darf, da der Einsatz von KI in diesem Bereich vielerorts zur gängigen Praxis geworden ist. „Im HR-Bereich wird KI eingesetzt, weil es aus Effizienzgründen einen großen Mehrwert bietet. KI-Systeme, die Lebensläufe filtern oder Kandidatinnen und Kandidaten bewerten, sparen zwar Zeit, werden aber vom AI-Act als Hochrisikobereich definiert und entsprechende Pflichten werden auferlegt. Das heißt aber nicht automatisch, dass man derartige Tools nicht verwenden darf“, so Pachinger.

Bei Chatbots oder Deepfakes gehe es nicht nur um Warnhinweise nach außen, wenn ein Unternehmen KI einsetzt, erläutert Pachinger. „Intern muss man vor allem die Funktionalitäten analysieren und dokumentieren. Je nach konkretem Einsatz und Risikolage sind entsprechende Maßnahmen zu setzen, zum Beispiel auch zu kommunizieren: Achtung, KI-generiert.“

Doch der AI-Act hat diesbezüglich noch eine weitere Konsequenz: „Aus Unternehmenssicht ist auch wichtig, dass man prüft, wie ein KI-System zum Einsatz kommt, welche Auswirkungen es hat be-

ziehungsweise haben kann und wie man damit umgeht. Es ist entscheidend, zu wissen: Besteht eine Kontrolle durch natürliche Personen? Gibt es eine menschliche Aufsicht, wie es im AI-Act heißt? Sprich, wird der KI-Output analysiert und überwacht?“ Das Um und Auf in Unternehmen sei es laut Pacher jetzt, zu analysieren und einzelfallbasiert zu prüfen, wo sich welche Pflichten ergeben. Das könne mitunter komplex sein.

Risiko und Strafen

Immer wieder werden EU-Regulierungen als praxisfern, zu komplex und oftmals auch zu unbestimmt kritisiert. Michael Pachinger sieht das beim AI-Act differenzierter: „Ich betrachte die unbestimmten Gesetzesbegriffe durchaus auch als Chance, die Unternehmen eine gewisse Flexibilität bietet.“ Man habe aus der Umsetzung der Datenschutz-Grundverordnung gelernt, so Pachinger: „Viele ‚Lessons Learned‘ aus der DSGVO können jetzt herangezogen werden. Bestes Beispiel ist der sogenannte risikobasierte Ansatz. Das heißt: Maßnahmen sind von Unternehmen ge-

zielt dort und in dem Ausmaß zu setzen, wo und wie die Risikolage es verlangt. Augenmaß ist gefragt, sodass zum Beispiel Sicherheitsmaßnahmen nicht überdimensional vorgesehen werden. Eine Einzelfallanalyse für die konkrete Anwendung kann hier oft viel Aufwand ersparen und dennoch zeigen, dass man die erforderliche und angemessene Sorgfalt walten lässt. Insofern lässt der AI-Act, ähnlich wie schon die DSGVO, Eigenverantwortung zu“, resümiert Pachinger.

Und die Strafen? Sie sind drastisch, aber abhängig vom Grad der Verantwortung. Verstöße können mit bis zu 35 Millionen Euro oder 7 Prozent des weltweiten Umsatzes geahndet werden, je nach Schweregrad des Verstoßes. Was ist also teurer: Es richtig zu machen oder nichts zu tun? Pachinger: „Am teuersten kann es werden, wenn man gar nichts tut und keinerlei Vorkehrungen nachweisen kann. Punktgenaue Analysen, ausgehend von einem guten Datenmanagement und einer zweckgebundenen Risikobewertung, sind eine sinnvolle und rechtssichere Vorgangsweise“, empfiehlt Pachinger.

ENTGELTICHE EINSCHALTUNG

Abweichungen in juristischen Dokumenten sicher beherrschen

Künstliche Intelligenz erkennt textuelle und semantische Unterschiede auf einen Blick.

KOALaw von RISC Software GmbH vergleicht Dokumente automatisiert mit Fokus auf textuelle und semantische Unterschiede. Die Analyse erfolgt präzise, nachvollziehbar und in Echtzeit, was die Entscheidungsfindung erheblich beschleunigt. Entwickelt und betrieben in Österreich.



Abweichungen sofort erkennen

Textuell & semantisch – nachvollziehbar



Sicher & rechtskonform

Betrieb in Österreich, EU-Recht



Integrierbar und skalierbar

Schnittstellen nach Bedarf

Mehr Informationen
und Use Cases:

<https://www.risc-software.at/koalaw/>

