risControl daily

Künstliche Intelligenz, aber sicher.

Kommentar von Rechtsanwalt Mag. Stephan Novotny, AFPA-Lotse

6. Februar 2025, 5:19

Ab 2. 2. 2025: KI-Systeme für bestimmte Anwendungen verboten. „Verpflichtung zur KI-Kompetenz“. Hohe Strafen drohen.

Glaubt man Medien-Berichten, dann wird **sich KI zu einem Schlüsselthema in der Finanz- und Versicherungswelt** entwickeln. Wie schnell das passieren kann, zeigt die Nutzung von Systemen wie ChatGPT in den letzten Monaten. Dennoch wissen sehr viele Marktteilnehmer noch nicht oder nicht ausreichend genug, **welche Anwendungen** in unseren Branchen möglich sein könnten und was die **EU-KI-Verordnung verbietet bzw. welche Auflagen** sie für die nicht verbotenen Anwendungen vorschreibt. Besonders auf **nötige Ausbildungen** für alle, die KI einsetzen (wollen), möchten wir ganz dringend hinweisen.

Was ist die KI-Verordnung und warum ist sie wichtig?

Fakt ist: Das Thema der Künstlichen Intelligenz (KI) wird in unserem Alltag immer präsenter. Aber mit all den Möglichkeiten, die sie bietet – etwa die Automatisierung von Arbeitsprozessen, personalisierte digitale Assistenten – gehen auch erhebliche Herausforderungen einher. Genau an dieser Stelle setzt die KI-Verordnung der Europäischen

Union an: Sie soll einen **rechtlichen Rahmen schaffen**, der Risiken minimiert, während gleichzeitig Innovationen nicht ausgebremst werden.

Die KI-Verordnung wurde am 12. Juli 2024 veröffentlicht und ist **bereits zum Teil am 1. August 2024 in Kraft getreten.** Es handelt sich um eine europäische Verordnung, welche im Rahmen eines ordentlichen Gesetzgebungsverfahren von der Europäischen Kommission in Zusammenarbeit mit dem Europäischen Parlament und dem Ministerrat (Rat der EU) erlassen wurde. Nachdem die KI-Verordnung **Einstufungen von „kein Risiko" bis „inakzeptables Risiko" vorgenommen** hat, wird sie stufenweise eingeführt, orientiert an diesem System. Den Anfang machen diejenigen Systeme, die verboten werden sollen und bis 2027 soll die gesamte Verordnung gelten.

Kategorisierung von KI-Systemen

Da die KI-Verordnung einen **risikobasierten Ansatz** verfolgt, werden KI-Systeme in Zukunft entsprechend ihrem Risikopotential kategorisiert. "Risiko" im Sinne des AI Acts ist die Kombination aus der Wahrscheinlichkeit des Eintritts eines Schadens und der Schwere dieses Schadens (Artikel 3). Es wird **zwischen folgenden Stufen unterschieden:** minimales bzw. kein Risiko, begrenztes Risiko, hohes Risiko und inakzeptables Risiko. Während jene KI-Systeme mit minimalem bzw. keinem Risiko keine spezifischen Pflichten erfüllen müssen, werden den AnbieterInnen und BetreiberInnen von **jenen mit „begrenztem" Risiko Transparenzpflichten auferlegt.** Gemäß Artikel 50 AI Act fallen darunter folgende Systeme: Solche, die mit natürlichen Personen interagieren, Bild-, Audio-, Text- oder Videoinhalte erzeugen oder manipulieren sowie Systeme zur biometrischen Kategorisierung und Emotionserkennung.

Im Vergleich dazu erfordert die Kategorie der **Hochrisiko-KI-Systeme die Einhaltung bestimmter Anforderungen.** In die Stufe des inakzeptablen Risikos fallen und sind **daher verboten** beispielsweise KI-Systeme, die das menschliche Verhalten manipulieren, um den freien Willen des Menschen zu umgehen sowie solche, die eingesetzt werden, um die Schwächen von Menschen auszunutzen.

Anwendungsbereich und regulierte Subjekte

Die KI-Verordnung gilt für alle KI-Systeme, die innerhalb der EU oder des EWR-Raums in Betrieb genommen oder in den Verkehr gebracht werden. Ein **Unternehmenssitz innerhalb dieses Gebiets ist dabei nicht erforderlich.** Entscheidend für die Anwendung der Verordnung ist nicht nur die Inbetriebnahme und das Inverkehrbringen von KI-Systemen, sondern auch die Nutzung der Ergebnisse, die diese Systeme liefern.

In Artikel 3 der Verordnung werden die **relevanten Akteure genauer definiert.** Neben dem „Anbieter", an den sich die Verordnung primär richtet, werden auch „Bereitsteller", „Bevollmächtigter", „Importeur", „Händler" und „Betreiber" genannt. Die genaue Unterscheidung dieser Kategorien ist von Bedeutung, da je nach Rolle unterschiedliche Anforderungen erfüllt werden müssen.

Während **Anbieter** aktiv an der Entwicklung von KI-Systemen mitwirken oder bestehende Modelle in eigene Produkte integrieren, die dann unter ihrem Namen vertrieben werden, setzt ein **Betreiber** KI-Systeme lediglich zur internen Anwendung ein.

Als Importeure gelten jene, die aus einem Drittland stammende KI-Systeme einführen. Und Unternehmen, die weder Anbieter noch Betreiber oder Importeure sind, aber dennoch Teil der Lieferkette eines KI-Systems sind, das auf dem EU-Markt bereitgestellt wird, könnten unter die Kategorie der **Händler** fallen.

Auswirkungen auf Unternehmen

Zwar erscheint die Zeitspanne bis zur Durchsetzung des AI-Acts lange, sie ist jedoch sehr umfassend. Daher gilt: je früher sich Unternehmen mit den Anforderungen der Verordnung befassen, desto besser. Wer frühzeitig eine Bestandsaufnahme der eingesetzten KI-Systeme vornimmt und mit der Umsetzung beginnt, hat bessere Chancen den Anforderungen rechtzeitig zu entsprechen.
Besonders Anbieter von Hochrisiko-KI-Systemen sollten sich umgehend mit der Verordnung auseinandersetzen und ihre Systeme entsprechend anpassen. Auch jene Unternehmen, die **bereitgestellte KI-Systeme nutzen** und nicht in die Kategorie der „Anbieter“ fallen, **sollten frühzeitig** mit der Bestandsaufnahme ihrer eingesetzten Systeme **beginnen.** Durch die frühzeitige Implementierung der erforderlichen Maßnahmen können Unternehmen sich einen Wettbewerbsvorteil verschaffen.

Verpflichtende Schulungen zur KI im Versicherungsvertrieb

Ab Anfang Februar 2025 sind im Versicherungsvertrieb Personen, die mit der Entwicklung oder dem Betrieb von KI-Systemen betraut sind, sowie diejenigen, die KI-Systeme einsetzen, verpflichtet, an Schulungen teilzunehmen. Dies ergibt sich aus Artikel 4 des AI-Acts. Dabei fehlen jedoch noch genaue Angaben zur Art der Schulung sowie zur Frage, ob diese intern oder extern durchgeführt werden muss.

Die knapp bevorstehenden nächsten Schritte

Wie bereits zu Beginn erwähnt, wird die Verordnung nach und nach eingeführt. Ab 2. Februar 2025 sind zunächst Technologien, welche als „inakzeptables Risiko“ eingestuft werden, verboten. Sechs Monate später, also am 2. August 2025 greifen dann die Bestimmungen für jene KI-Systeme, die unter „begrenztes Risiko“ fallen. Ab 2. August 2026 werden schließlich alle Regeln der KI-Verordnung vollständig wirksam.

Wofür kann KI eingesetzt werden und wofür darf man das künftig nicht?

Große Hoffnungen werden vielerorts in die **Kundenansprache mittels Chatbots** gesetzt. Gemeint sind hier nicht die „ersten Anfangs-Tools“, an denen Kunden verzweifeln, sondern moderne Versionen, bei denen man nicht mehr realisiert, dass man in Wirklichkeit mit einer „Maschine spricht“. Hier erwarten sich die Verantwortlichen, dass am Anfang zumindest einfache und immer wieder zum gleichen Thema gestellte Fragen rasch beantwortet werden können, ohne dass ein menschlicher Berater eingreifen müsste. **Im Bankbereich könnten typische Bereiche** etwa die Sperre einer Kundenkarte oder Bestellung einer neuen

Kreditkarte sein oder die Frage, wo man Formular XY findet, um irgendwas bekannt zu geben usw. In einem Profil-Bericht berichtete Susanne Zach von der Wirtschaftsprüfungsgesellschaft EY davon, dass in einer Investment-Bank ein Chatbot Kundenanfragen derart gut beantwortet, dass nicht nur **80 Arbeitsstunden pro Monat eingespart** werden konnten, sondern sich die **Kundenzufriedenheit um 15 %** erhöht hatte. Außerdem bedeutet das, dass das Unternehmen dieses Service rund um die Uhr anbieten kann.
Solche Anwendungen werden **auch künftig erlaubt sein,** da hier wohl wenig Risiko für Kunden zu erwarten ist. Allerdings muss man die User, die solche Chatbots nutzen, künftig darauf hinweisen, dass Sie mit einem Chatbot „sprechen" (Kennzeichnungs- und Transparenzpflicht).

Ebenso **unproblematisch werden wohl KI-Anwendungen** sein, mit denen Bürotätigkeiten automatisiert werden. Etwa das automatische Transkribieren (also das Abschreiben von Gesprochenem) von Telefonkonferenzen, soferne beim Start der Konferenz der Datenschutzhinweis gegeben wurde, dass die Sitzung aufgezeichnet wird.

Hilfreich werden KI-Systeme auch sein, **um in Echtzeit in einer Unmenge an Daten „ungewöhnliche Muster" zu erkennen und mögliche Betrugsversuche zu verhindern**. Darin ist die KI den Menschen weit überlegen und erzielt z.B. in der Krebsvorsorge schon bemerkenswerte Erfolge, weil Krebs schon im Frühstadium erkannt werden kann, lange bevor der Arzt einen Verdacht gehegt hätte. Auf unsere Branchen umgelegt, könnte also die KI erkennen, dass (nach Vergleich mit historischen Daten) vom Konto eines Kunden unüblich viel Geld abgebucht wird oder die Bankomat-Karte im Ausland genutzt wird, obwohl der Kunde kurz vorher im Supermarkt in Wien eingekauft hat. Und löst sofort Alarm aus.

Problematischer sind KI-Anwendungen, die z.B. entscheiden, ob jemand **kreditwürdig ist oder nicht.** Oder dank „machine learning" vorhersagen, mit welcher Wahrscheinlichkeit der Kunde und zu welchem Zinssatz er das Angebot annimmt. Im oben zitierten Profil-Beitrag berichtet Kilian Verweyen von der Unternehmensberatung KPMG davon, dass die KI aus Fakten wie Alter, Nutzung von Vergleichsplattformen (deutet auf Preissensibilität hin), verwendetes Endgerät (Apple-Kunden gelten als wenig preissensibel) etc. den **Zinssatz individuell anpasst.** Ein Phänomen, das Konsumentenschützer in den letzten Jahren schon bei Flug- oder Hotelbuchung kritisierten.
Das große Problem hierbei ist, dass man **nicht weiß, warum die KI zu einer Entscheidung gekommen** ist und man darauf vertrauen muss, dass die KI die Fehler einsieht und selbst daraus lernt. Das ist der EU jedoch zu unsicher. Daher fordert die EU, dass auf den Einsatz der KI transparent hingewiesen wird und dass man u.a. einen **menschlichen Kontakt angeben muss**, mit dem man das erhaltene Angebot besprechen kann.

Unter welchen Bedingungen etwa **Kreditscoring-Systeme** von Banken künftig erlaubt sind – beinhalten möglicherweise hohes Risiko für Kunden – wird sich zeigen. Laut KPMG-Berater Verweyen zählt die EU den Zugang zu Krediten zur Grundversorgung der Bürger. Man solle daher „Vorsicht walten lassen und die Anforderungen des AI Acts genau prüfen".

Definitiv verboten sind KI-Systeme, die „social scoring" betreiben, wie man es aus China immer wieder hört. Dort soll wünschenswertes Verhalten belohnt (Gesetzestreue, soziales Engagement, pünktliche Rückzahlung von Krediten etc.) und unerwünschtes Verhalten (Falschparken, bei Rot über die Ampel gehen, Zahlungsverstoß, etc.) sanktioniert werden (kein Zugang zu Flügen, Uni, Jobs, Krediten usw.). Das ist in der EU definitiv verboten, weil es als Verstoß gegen die EU-Grundwerte gilt.

Natürlich wird auch der **Wertpapierbereich durch KI verändert** werden. Allerdings weisen Christian Lenz und Fabian Schinerl von der Kanzlei Brandl Talos in einem Beitrag im FondsProfessionell darauf hin, dass die strengen Anforderungen von MiFID-2 auch weiterhin einzuhalten sind. Gemeint ist, dass **bei Anlageberatung und Portfolioverwaltung** die Dienstleister immer im besten Kundeninteresse handeln müssen und bei der Beratung z.B. die finanzielle Situation des Kunden, seine Risikobereitschaft, Kenntnisse und Erfahrungen, seine Anlageziele und Nachhaltigkeitspräferenzen einbeziehen müssen. Und das Produkt muss umfassend und verständlich erklärt werden (Chancen / Risiken, Kosten usw.).

Und Lenz/Schinerl verweisen auf eine **Stellungnahme der ESMA**, der Europäischen Wertpapieraufsicht, wonach durch den Einsatz von KI die Bestimmungen von MiFID-2 nicht umgangen werden können. Egal, ob KI oder Mitarbeiter: **Der Dienstleister haftet für deren Fehler.** Daher müssen Banken und Wertpapierdienstleister ihre Kunden über den Einsatz und die Rolle der KI im Anlageentscheidungsprozess informieren und zwar klar, fair und nicht irreführend. Auch im „normalen" Kontakt müssen die Kunden darauf hingewiesen werden, wenn Chatbots oder andere KI-basierte automatisierte Systeme eingesetzt werden.

ESMA fordert erhöhte Sorgfalt /Kompetenz bei KI-Anwendungen
Dienstleister, die KI zur Information der Anleger über Anlageprodukte einsetzen, haben dabei erhöhte Sorgfalt walten zu lassen, um das gleiche Maß an Qualitätsstandards zu gewährleisten, wie bei einer rein analogen Dienstleistung. Konkret bedeutet dies laut Lenz/Schinerl, dass strenge Kontrollen vorzusehen sind, um vorab (ex ante) die Richtigkeit der gelieferten und genutzten Informationen sicherzustellen. Außerdem müssen regelmäßig Ex-post-Kontrollen durchgeführt werden, um alle Prozesse zu überwachen und zu bewerten, bei denen Informationen direkt oder indirekt über KI-gesteuerte Mechanismen - bereitgestellt werden.
Damit sollen die MiFID-2-Verpflichtungen eingehalten und Anleger vor unrichtigen oder irreführenden Informationen über Anlageprodukte und -dienstleistungen geschützt werden.

Wichtig: Wie bereits anfangs (im Versicherungsbereich beschrieben) sind auch im Wertpapierbereich **Schulungen nötig:** Die Mitarbeiter sind über die operativen Aspekte der KI, potenzielle Risiken, ethische Überlegungen und regulatorische Auswirkungen zu schulen, so Lenz/Schinerl.

Fakt ist: Die KI-Anwendungen haben immer die **Verwendung von großen Datenmengen als Basis.** Also sind hier auch sehr viele Datenschutzfragen zu berücksichtigen. Zwar ist der KI /AI act verabschiedet worden, der einige Eckpflöcke einschlägt. Aber viele Fragen werden sich erst exakt klären lassen, sobald eine aussagekräftige Rechtsprechung vorliegt.
Foto: Mag. Stephan Novotny ©Stephan Huger