

Insurance News Blog

By PwC Deutschland | 04.12.2023

# AI Governance in der Versicherungsbranche

**Regulierung in den Startlöchern – jetzt eine einheitliche und wirksame  
AI Governance etablieren**

Im Zeitalter des digitalen Wandels ist der Begriff „Künstliche Intelligenz“ (KI) omnipräsent und KI-basierte Systeme werden von Versicherungsunternehmen zunehmend eingesetzt. Von allgemeiner Prozessoptimierung, über intelligent gesteuerte und dunkelverarbeitete Schadenabwicklungsprozesse bis hin zu KI-Chatbots für den Kundensupport – die **Einsatzmöglichkeiten von KI** im Versicherungsbereich sind so vielfältig wie die hieraus wachsenden Herausforderungen. Einen Überblick über den Einsatz von KI im deutschen Finanzsektor – und insbesondere für Versicherungen - gibt unsere **Marktstudie** (PwC, September 2023, Konstantinos Dagianis, Franziska Hecker, Sounia Arbib). Welche Anforderungen sich aus der Nutzung von KI bei Versicherungsunternehmen ergeben können, ist Gegenstand nachfolgender Betrachtungen.

## Risikoeinstufungen von KI

Für Versicherer rücken die KI-bezogenen Anforderungen, die sich aus den aktuellen aufsichtsrechtlichen Regulierungen und den bevorstehenden Gesetzesverabschiedungen ergeben, immer mehr in den Fokus. Wie diesbezügliche Vorgaben und Empfehlungen konkret aussehen werden, ist zum aktuellen Zeitpunkt noch unklar. Das Ziel ist jedoch eindeutig: die Verwendung von Künstlicher Intelligenz, genauer KI-Systemen, soll künftig strikt reguliert werden. Mit ihrem **Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz** (EU AI Act) hat die Europäische Kommission im April 2021 den Grundstein für eine europaweite Regulierung von Künstlicher Intelligenz gelegt. Derzeit befindet sich das Gesetzgebungsverfahren im Trilog und könnte in den nächsten Monaten verabschiedet werden.

Der EU AI Act zielt darauf ab, KI technologie-neutral und uniform zu definieren und einen sicheren, transparenten und fairen Einsatz von KI-Systemen zu gewährleisten. Zusätzlich sollen Regeln zur verpflichtenden Einstufung von KI-Anwendungen in verschiedene Risikostufen die adäquate Analyse und Kontrolle von Risiken ermöglichen. In der aktuellen Entwurfsfassung sieht der risikobasierte Ansatz vier Kategorien vor:

- **Unacceptable risk:** KI-Systeme, die als eindeutige Bedrohung für die Sicherheit, den Lebensunterhalt und die Rechte des Menschen angesehen werden
- **High risk:** KI-Systeme, die einen negativen Einfluss auf die Sicherheit und die Rechte des Menschen haben und daher vor Markteintritt strengen Auflagen unterworfen werden
- **Limited risk:** KI-Systeme mit Transparenzpflichten
- **Minimal risk:** KI-Systeme mit minimalem oder gar keinem Risiko

In Abhängigkeit der Risikoeinstufung eines KI-Systems gelten unterschiedlich umfangreiche Anforderungen.

## Regulierung von KI in der Versicherungsbranche

Während der EU AI Act die Ver- und Anwendung von KI branchenweit reguliert, sind für Versicherungsunternehmen überdies sowohl bereits bestehende branchenspezifische Gesetze als auch etwaige zusätzliche Anforderungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zwingend

zu beachten. Mit ihrem *Prinzipienpapier für die Verwendung von Algorithmen in Entscheidungsprozessen* hat die BaFin einen ersten Einblick in vorläufige Überlegungen zu möglichen Mindestanforderungen für den Einsatz von KI gegeben. Grundlegend werden drei Prinzipienarten definiert:

### **1. Übergeordnete Prinzipien:**

- a. Klare Verantwortung der Geschäftsleitung
- b. Adäquates Risiko- und Auslagerungsmanagement
- c. Vermeidung systematischer Verzerrungen (Bias)
- d. Beachtung von bestehenden, gesetzlich untersagten Differenzierungen

### **2. Spezifische Prinzipien für die Entwicklungsphase:**

- a. Datenstrategie und -governance
- b. Einhaltung der Datenschutzregeln
- c. Sicherstellung korrekter, robuster und reproduzierbarer Ergebnisse
- d. Dokumentation zur internen und externen Nachvollziehbarkeit
- e. Angemessene Validierungsprozesse
- f. Verwendung relevanter Daten zur Kalibrierung und Validierung

### **3. Spezifische Prinzipien für die Anwendung:**

- a. Regelmäßige Validierung und stetige Kontrolle durch den Menschen
- b. Intensive Freigabe- und Feedbackprozesse
- c. Etablierung von Notfallmaßnahmen
- d. Laufende Validierung, übergeordnete Evaluation und entsprechende Anpassung

Diese Prinzipien sind keinesfalls komplett neu. Viele davon sind bereits aus anderen Zusammenhängen bekannt, wie etwa der faire und ethische Gebrauch von Daten der Kunden in der allgemeinen Datenverarbeitung. Zusätzlich zu den gesetzlichen und aufsichtsrechtlichen Anforderungen an KI müssen bei dessen Integration in der Versicherungsbranche auch versicherungsspezifische Regelungen Beachtung finden, wie beispielsweise die in der Versicherungsvertriebsrichtlinie (IDD) verankerte Produktüberwachung und -governance (POG). Demnach müssen Versicherungsunternehmen interne Verfahren und Kontrollen implementieren, um sicherzustellen, dass Versicherungsprodukte den Bedürfnissen der Kunden entsprechen und ordnungsgemäß vertrieben werden. Dies schließt die Produktentwicklung, -überwachung und -bewertung ein.

Desweiteren sind bei der Entwicklung und dem Betrieb von KI-Anwendungen die Anforderungen der VAIT (Versicherungsaufsichtliche Anforderungen an die IT) der BaFin umzusetzen. Das schließt eine Berücksichtigung in der IT-Strategie, die Aufnahme in den Informationsverbund und damit die Steuerung der Risiken im Informationsrisikomanagement und Informationssicherheitsmanagement mit ein. Dies ergibt sich nicht nur für KI-Systeme, die On-Premise entwickelt und betrieben werden, es ist vielmehr auch in der Dienstleistersteuerung zu beachten, sofern durch den Dienstleister KI-Anwendungen genutzt werden. Mit Blick auf den Digital Operational Resilience Act (DORA) der EU wird dies noch an Bedeutung deutlich zunehmen.

## Auswirkungen der KI-Regulierung auf Versicherungsunternehmen

Für die Versicherungsindustrie ergeben sich aus den dargestellten Anforderungen weitreichende Konsequenzen. Gemäß **Anhang III** des europäischen Regulierungsentwurfs in der Fassung des Europäischen Rats werden **KI-Systeme, die bei Lebens- und Krankenversicherungen für die Risikobewertung in Bezug auf natürliche Personen und die Preisbildung verwendet werden sollen, als hoch riskant eingestuft**. Die Klassifizierung als Hochrisiko-KI-System könnte wiederum zu zusätzlich unabsehbar hohen zeitlichen und monetären Aufwänden führen. Gemäß EU AI Act ist beim Einsatz von hoch riskanter KI beispielsweise ein KI-eigenes Risikomanagement obligatorisch, die Einführung einer Data Governance so gut wie unvermeidbar und eine technische Dokumentation dieser Systeme notwendig. Zusätzlich wird gefordert, dass Hochrisiko-KI-Systeme so konzipiert und entwickelt werden müssen, dass Menschen sie überwachen können. Dies erfordert wiederum Weiterbildungsmaßnahmen, um die erforderliche technische Expertise überhaupt aufbauen zu können.

Versicherungsunternehmen sind deshalb gefordert sicherzustellen, dass KI-Anwendungen stets ethisch, transparent und im Einklang mit den regulatorischen Anforderungen arbeiten. Hierfür ist eine sorgfältige Integration von KI unter Berücksichtigung gesetzlicher Bestimmungen und bspw. einer robusten POG unabdingbar. Das Vertrauen der Kunden zu stärken und rechtliche Risiken zu minimieren kann letztlich nur durch eingehaltene Datenschutzbestimmungen, Fairness, erklärbare Entscheidungen, regulatorische Compliance und transparente Kundenkommunikation gelingen. Somit ist eine einheitliche und wirksame AI Governance in der Versicherungsbranche notwendig, die allen Entwicklern und Anwendern von KI-Anwendungen bekannt ist und konsequent umgesetzt wird.

## Rechtzeitige Vorbereitung auf die bevorstehende KI-Regulierung

Der EU AI Act steht vor der Tür und damit möglicherweise weitreichende zusätzliche Anforderungen an zahlreiche Funktionen im Versicherungsunternehmen (wie bspw. die Risikomanagementfunktion, die Informationssicherheit oder Aktuarien, die KI in ihren Modellen verwenden). **Damit Versicherungsunternehmen für die bevorstehende Regulierung von KI gut vorbereitet sind, gilt es, sich frühzeitig und ganzheitlich mit AI Governance zu befassen**. Hierbei unterstützen wir gerne, indem wir ein einheitliches Verständnis über die Begriffsdefinition und Transparenz über aktuelle und mögliche zukünftige Anforderungen und die Situation in Ihrem Unternehmen schaffen. Wir begleiten Sie bei der Inventarisierung Ihrer KI-Anwendungen anhand eines entwickelten KI-Fragebogens, bei der Umsetzung der Anforderungen mittels eines auf Ihre Bedürfnisse abgestimmten Regelwerks sowie beim Aufbau und der Etablierung eines Regelprozesses zur Sicherstellung einer angemessenen AI Governance. Für bereits eingesetzte KI-Systeme evaluieren wir die "Readiness" im Hinblick auf den EU AI Act und unterstützen bei der Umsetzung und Erfüllung der regulatorischen Anforderungen an den vertrauenswürdigen KI-Einsatz.

[Laufende Updates zum Thema erhalten Sie über das regulatorische Horizon Scanning in unserer Recherche-Applikation PwC Plus. Lesen Sie hier mehr über die Möglichkeiten und Angebote.](#)

[Zu weiteren PwC Blogs](#)

## Keywords

Artificial Intelligence (AI), Digitalisierung, Prozesse, Versicherungsmarkt

## Contact



**David Richter**

Köln

[david.richter@pwc.com](mailto:david.richter@pwc.com)