KI in Versicherungsunternehmen – Chancen nutzen, Risiken managen

Versicherungsunternehmen können durch den Einsatz von künstlicher Intelligenz (KI) ihre Prozesse erheblich effizienter gestalten. Gleichzeitig gelten für den Finanzsektor besondere Compliance-Vorgaben. Neben allgemeinen Regelungen wie der „MaGo“, „DORA“ und „IDD“ müssen auch KI-spezifische Anforderungen, etwa aus dem AI Act oder den BaFin-Prinzipien zu Big Data und KI, berücksichtigt werden. Darüber hinaus arbeiten die Gesetzgeber und Aufsichtsbehörden kontinuierlich an der Weiterentwicklung der KI-Regulierung. Die daraus resultierenden rechtlichen Risiken sollten sorgfältig gemanagt werden. Ein zentraler Aspekt in diesem Zusammenhang ist der Aufbau einer effektiven KI-Governance.

Use Cases: So können Versicherungsunternehmen mit KI effizienter werden

Die Anwendungsmöglichkeiten von KI in Versicherungsmöglichkeiten sind vielfältig. Beispiele sind:

- Kundenkommunikation: Ein Sprachdialogsystem ermöglicht die automatisierte Bearbeitung von Kundenanliegen über Telefon und Chat, indem es die Identität des Kunden überprüft und das Anliegen präzise erkennt.
- Schadenbewertung und Betrugserkennung: Eine KI analysiert Schadensbilder, schätzt die Reparaturkosten und reduziert manuelle Prüfungen, wodurch der Prozess der Schadensregulierung schneller und effizienter wird. Dabei identifiziert die KI Anomalien in den Schadensmeldungen, nutzt externe Datenquellen zur Überprüfung und hilft, Versicherungsbetrug zu verhindern.
- Personalisierte Versicherungsangebote: Eine KI erstellt maßgeschneiderte Versicherungsempfehlungen basierend auf Kundenprofilen, Bedürfnissen und Risikofaktoren.
- Compliance-Prüfung von Vertragsdokumenten: Eine KI erkennt regulatorische Abweichungen, vergleicht Verträge mit geltenden Standards und minimiert somit Compliance-Risiken.
- Katastrophenmodellierung: Eine KI simuliert Naturkatastrophenszenarien, verbessert die Risikobewertung und ermöglicht eine genauere Kalkulation von Prämien.

Das regelt der AI Act

Beim Einsatz von KI ist insbesondere der im August 2024 in Kraft getretene AI Act zu beachten. Der AI Act der EU teilt KI in Risikogruppen ein. Je höher das Risiko einer Anwendung ist, desto höher sind die Anforderungen und Pflichten. Verboten sind nach dem AI Act KI-Systeme, die ein nicht hinnehmbares Risiko darstellen. Dazu zählen KI-Systeme, die dazu bestimmt sind, menschliches Verhalten unterschwellig nachteilig zu beeinflussen sowie biometrische Kategorisierungen in sensiblen Bereichen. KI-Systeme, die die Kreditwürdigkeit oder die Inanspruchnahme von Kranken- und Lebensversicherungen bewerten, sind nach dem AI Act mit einem hohen Risiko verbunden. Auch KI im Bewerbermanagement und in der Produktsicherheit wird häufig dazu gezählt. An Hochrisiko-KI-Systeme stellt der AI Act besonders hohe Anforderungen. Diese betreffen vor allem die Qualität der Datengrundlage, die Sicherheit, den Betrieb und die Dokumentation und Überwachung durch den Menschen sowie das Qualitäts- und Risikomanagement.

KI-Governance-Grundsätze der EIOPA

Die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung („EIOPA“) hat Governance-Grundsätze speziell für KI festlegt. Die zentralen Prinzipien der EIOPA sind:

1. Prinzip der Verhältnismäßigkeit: Der Einsatz von KI muss an die Art, den Umfang und die Komplexität der Aktivitäten von Versicherungsunternehmen angepasst werden.
2. Prinzip der Fairness und Nichtdiskriminierung: KI darf keine diskriminierenden Ergebnisse liefern und grundsätzlich niemandem den Zugang zu Versicherungen verweigern.
3. Prinzip der Transparenz und Erklärbarkeit: Versicherungsunternehmen müssen sicherzustellen, dass die Funktionsweise von KI-Systemen sowie deren Ergebnisse transparent und so weit wie möglich erklärbar sind.
4. Prinzip der menschlichen Aufsicht: Ein Mensch muss die Funktionsweise eines KI-basierten Systems in jeder Phase überwachen.
5. Prinzip der Daten-Governance und Aufzeichnung: Die von KI-Systemen verwendeten Daten müssen genau, vollständig und angemessen sein und einer sicheren Umgebung gespeichert werden.
6. Prinzip der Robustheit und Leistung: Ein robustes und effizientes System arbeitet zuverlässig und verursacht keine Schäden – sowohl in technischer als auch in ethischer Hinsicht.
7. EIOPA eröffnet Konsultationsverfahren zu KI Governance und Risikomanagement

Als Reaktion auf den AI Act hat die EIOPA am 12. Februar 2025 ein Konsultationsverfahren eröffnet, in dem sie um Rückmeldung zu ihrer Stellungnahme zu Governance und Risikomanagement im Bereich der künstlichen Intelligenz bittet. Rückmeldungen werden noch bis zum 12. Mai 2025 angenommen.

In der Stellungnahme werden die Erwartungen der EIOPA in Bezug auf die Grundsätze der Unternehmensführung und des Risikomanagements dargelegt, die Versicherungsunternehmen anwenden sollten, um einen verantwortungsvollen Einsatz von KI-Systemen in bestimmten Anwendungsfällen zu gewährleisten. Diese Grundsätze umfassen unter anderem:

- Anwendung eines risikobasierten und verhältnismäßigen Ansatzes während des gesamten Lebenszyklus von KI-Systemen,
- Handeln auf der Grundlage von Fairness und ethischen Grundsätzen im besten Interesse der Verbraucher:innen,
- eine klare Definition der Rollen und Zuständigkeiten der Verantwortlichen,
- die Fähigkeit, die Ergebnisse von KI-Systemen verständlich zu erklären,
- die Umsetzung einer soliden Datenmanagementpolitik und
- eine angemessene und ordnungsgemäße Dokumentation und Aufzeichnung.

Der Umgang der BaFin mit künstlicher Intelligenz

Die BaFin hat KI bisher im Rahmen bestehender Aufsichtsprozesse oder aus gegebenem Anlass überprüft. Dabei differenziert sie nicht zwischen menschlichen und KI-Entscheidungsprozessen, sondern betrachtet den Entscheidungsprozess als Ganzes. Auch sie hat Prinzipien formuliert:

- Die klare Verantwortung liegt bei der Geschäftsleitung.
- Werden Anwendungen von einem Dienstleister bezogen, muss die Geschäftsleitung ein effektives Auslagerungs- bzw. Ausgliederungsmanagement einrichten. Hierbei sind Verantwortungs-, Berichts- und Kontrollstrukturen klar festzulegen.
- Bei Algorithmen-basierten Entscheidungsprozessen muss ein Bias, also die systematische Verzerrung von Ergebnissen, vermieden werden.
- Für einige Finanzdienstleistungen ist zudem gesetzlich festgelegt, dass bestimmte Merkmale nicht zur Differenzierung – also zur Risiko- und Preiskalkulation – herangezogen werden dürfen. Konditionen dürfen nicht auf Basis solcher Merkmale gestaltet werden, um Diskriminierung zu vermeiden.

Zusätzlich hat die BaFin spezifische Prinzipien für die Entwicklungsphase sowie die Anwendung von KI aufgestellt.

BaFin stellt neuen Entwurf der MaGo vor

Im Januar 2025 hat die BaFin den Entwurf des überarbeiteten Rundschreibens „Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen unter Solvabilität II (MaGo für SII-VU)“ veröffentlicht. Das Konsultationsverfahren wurde am 26. Februar 2025 abgeschlossen. Es ist jedoch noch nicht bekannt, wann mit der Veröffentlichung eines endgültigen Entwurfs zu rechnen ist. In dem veröffentlichten Entwurf formuliert die BaFin Anforderungen an die Aufbau- und Ablauforganisation für automatisierte Geschäftsabläufe. Der Entwurf sieht vor, dass automatisierte Geschäftsabläufe wie die Risikozeichnung, die Schadens- und Leistungsbearbeitung sowie die Bestandsverwaltung angemessen gesteuert, überwacht und dokumentiert werden. Dabei sind die Identifizierbarkeit, Nachvollziehbarkeit und Qualitätssicherung dieser Prozesse sowie regelmäßige unabhängige Bewertungen im Einklang mit dem Risikoprofil sicherzustellen.

Der aktuelle Entwurf der MaGo enthält keine genaue Definition für automatisierte Geschäftsabläufe. Es bleibt daher unklar, wann die Anforderungen dieses Kapitels anzuwenden sind. Ein ähnlicher Begriff findet sich in der DSGVO, nämlich die automatisierte Entscheidung. Vergleicht man diese Begriffe, spricht vieles dafür, dass die Anforderungen der MaGo bereits bei jedem automatisierten Geschäftsablauf erfüllt werden könnten, unabhängig davon, ob eine Entscheidung gegenüber einer versicherten Person getroffen wird. Eine so weit gefasste Auslegung würde jedoch dazu führen, dass nahezu alle durch moderne Technologien unterstützten Geschäftsprozesse unter den Begriff fallen würden.

Rechtsfolgen von Verstößen der Geschäftsorganisation

Rechtsverstöße führen zu Sanktionen und Mängeln bei IT-Sicherheit und Resilienz und begründen ebenfalls Risiken. Gemäß § 301 VAG kann die Aufsichtsbehörde bei bestimmten Abweichungen des Risikoprofils oder der Geschäftsorganisation einen Kapitalaufschlag auf die Solvabilitätskapitalanforderung für ein Versicherungsunternehmen festsetzen.

Auch DORA sieht Sanktionen für Versicherungsunternehmen vor. Gemäß Artikel 50 DORA sind hohe Geldstrafen oder Einschränkungen im Geschäftsbetrieb möglich.

Sonstige KI-relevante Haftungsrisiken

Haftungsrisiken können sich nicht nur aus Vorschriften zur Geschäftsorganisation ergeben. Der Einsatz von KI betrifft viele rechtliche Querschnittsbereiche, die auf den ersten Blick nicht unmittelbar etwas mit KI oder Geschäftsorganisation zu tun haben. Ein Verstoß gegen solche Vorschriften kann einen Beseitigungs- und Unterlassungsanspruch oder sogar einen Schadensersatzanspruch begründen. Nichtsdestotrotz muss die Geschäftsorganisation auch solche Haftungsrisiken berücksichtigen. Generell sind beim Einsatz von KI zu beachten:

- In der Kundenbetreuung müssen Benachteiligungen ausgeschlossen werden. Hier ist das Allgemeine Gleichbehandlungsgesetz (AGG) zu beachten. Dieses untersagt eine Benachteiligung aus Gründen der „Rasse“, der ethnischen Herkunft, wegen des Geschlechts, der Religion, einer Behinderung, des Alters oder der sexuellen Identität.
- Für die Verarbeitung personenbezogener und sensibler Daten sind die Vorschriften der DSGVO zu beachten. Hier unterliegen insbesondere automatisierte Entscheidungen besonderen Einschränkungen.

- Das Urhebergesetz sieht vor, dass urheberrechtlich geschützte Trainingsdaten nur mit Einwilligung oder im Rahmen der Text-und-Data-Mining-Schranke verwendet werden dürfen. Der Output darf keine urheberrechtlich geschützten Werke enthalten.
- Weitere Verpflichtungen für den Einsatz von KI können sich aus dem Vertriebsrecht ergeben. Zum Beispiel muss eine angemessene Beratung unter Berücksichtigung der Bedürfnisse und Wünsche der Kund:innen stattfinden.

Ein Verstoß gegen diese Vorschriften kann nicht nur eine Haftung des Versicherungsunternehmens gegenüber den geschädigten Personen begründen. Im Innenverhältnis ist der Vorstand verpflichtet, nicht gegen Satzung, Gesetz oder Treuepflichten zu verstoßen. Das ergibt sich aus § 23 Abs. 1 S. 2 VAG, § 93 Abs. 1 S. 1 AktG. Im Übrigen ist von einer Pflicht des Vorstands zur Einführung einer Compliance-Organisation auszugehen. Verstößt der Vorstand gegen diese Pflichten, kann auch er sich schadensersatzpflichtig machen.

Voraussetzungen für eine KI-Governance: Datenmanagement und Strategie

Nach § 23 Abs. 1 VAG müssen Versicherungsunternehmen über eine Geschäftsorganisation verfügen, die sowohl die regulatorischen Vorgaben als auch eine solide und umsichtige Leitung des Unternehmens gewährleistet. Eine gute Governance sollte Chancen nutzen und Risiken mindern.
Voraussetzung für eine funktionierende KI-Governance ist dabei auch, dass ein sinnvolles Datenmanagement etabliert wird. Ebenso wichtig ist der Aufbau einer KI-Strategie. Kernelemente einer KI-Strategie sind strategische Leitplanken zu KI sowie KI-Ziele, die sich aus den Unternehmenszielen ableiten. Außerdem sollte die KI-Strategie Standards und Frameworks festlegen, an denen sich das Versicherungsunternehmen orientiert.

Aufbau einer erfolgreichen KI-Governance

Eine KI-Governance sollte klare, anpassungsfähige KI-Richtlinien und Governance-Strukturen enthalten, die Datenschutz, Transparenz, kontinuierliche Modellaktualisierungen und ein verantwortungsbewusstes Risikomanagement gewährleisten.

Im ersten Schritt sollten Unternehmen ihre spezifischen KI-Risiken beschreiben und in Risikokategorien einstufen.

Im zweiten Schritt werden KI-Richtlinien verfasst und kommuniziert. Sie spezifizieren organisatorische und technische Maßnahmen, eine Data Governance, Wesentlichkeitskriterien und die Verbindlichkeit von KI-Entscheidungen.
Im dritten Schritt wird die Ablauforganisation aufgebaut. Prozesse mit Einsatz von KI sowie Maßnahmen und Kontrollen werden definiert. Es wird ein Inventar von KI-Anwendungen und KI-Modellen erstellt. Qualitätsmaßen und Prüfpfade für Entscheidungen sowie Erklärbarkeitsschemata werden festgelegt.

Im selben Schritt sollte neben der Ablauforganisation auch die Aufbauorganisation errichtet werden. Diese sollte zunächst festgelegt und schriftlich fixiert werden. Außerdem sollten relevante Einheiten und Gremien verortet und die fachliche Kompetenz aufgebaut werden. Außerdem sollten Rollenprofile erstellt und die einzelnen Einheiten voneinander separiert werden.

Autoren:

Dr. Frank Püttgen, Partner, KPMG Law Rechtsanwaltsgesellschaft mbH

Dr. Fabian Bohnert, Director, KPMG AG Wirtschaftsprüfungsgesellschaft

Dr. Martin Köhler, Senior Manager, KPMG AG Wirtschaftsprüfungsgesellschaft

Ansprechpartner:

Dr. Frank Püttgen
Tel: +49 221 2716891414
fpuettgen@kpmg-law.com