Insurance News Blog

By PwC Deutschland | 08.01.2025

Regulierung von KI im Finanzsektor: Bericht der Bank für Internationalen Zahlungsausgleich thematisiert aktuelle Entwicklungen und Herausforderungen

Das Papier diskutiert bestehende Risiken rund um Modelle und Datenschutz sowie neue Risiken durch Halluzinationen und Anthropomorphismen bei GenAI. Ein skizzierter Underwriting-Use-Case unterstreicht die Bedeutung für Versicherer und Aktuar:innen.

Ein Mitte Dezember veröffentlichter Bericht der Bank für Internationalen Zahlungsausgleich (BIZ) diskutiert die Chancen und Risiken der künstlichen Intelligenz (KI) im Finanzsektor. Während der Einsatz von KI Effizienz und Einblicke verspricht, warnt der Bericht gleichzeitig davor, dass schlechte Governance, undurchsichtige Entscheidungsfindung und übermäßiges Vertrauen in Drittanbieter Finanzinstitute verwundbar machen könnten.

Der BIZ-Bericht identifiziert mehrere kritische Herausforderungen, denen Anwender im Finanzdienstleistungsbereich beim Einsatz von KI-Technologien gegenüberstehen. Diese Herausforderungen ergeben sich aus einem doppelten Druck: zum einen aus dem Bedarf, Innovationen zu managen, und zum anderen der Notwendigkeit eines robusten Risikomanagements. Dies wird durch die beobachtbare rasche Ausweitung von KI-Anwendungsfällen im Allgemeinen sowie in den Abläufen bei Banken, Versicherungen und weiteren Finanzdienstleistern im Speziellen forciert. Dabei scheinen die Unternehmen noch zögerlich bei kundenorientierten Dienstleistungen und risikoreichen Aktivitäten, während mit generativer KI bei Aspekten rund um die betriebliche Effizienz und die Steigerung der Produktivität der Mitarbeiter:innen bereits umfangreich experimentiert werde.

Das Dokument verweist darauf, dass sich KI-Anwendungsfälle grundsätzlich auf verschiedenen Ebenen klassifizieren lassen, etwa in Bezug auf die Wertschöpfungskette des Unternehmens, Jobfunktionen, Risikotypen/-stufen oder Arten von KI-Algorithmen. Abhängig vom Geschäftsmodell – nicht nur im Vergleich zwischen Banken-, Versicherungs- sowie weiteren Finanzdienstleistungssektoren, sondern auch innerhalb der einzelnen Sektoren – können dabei verschiedene dieser Use Cases von Bedeutung sein und damit in unterschiedlicher Form die Transformation der Sektoren sowie der darin agierenden Unternehmen vorantreiben. Entsprechend heben die Autor:innen hervor, dass die mit den Fortschritten einhergehenden Risiken betrachtet werden müssen und damit auch aufsichtliche Aufmerksamkeit bedürfen.

Der Bericht fasst sektorübergreifend KI-spezifische Leitplanken zusammen, die bereits in einigen Jurisdiktionen in Kraft sind oder entwickelt werden. Diese umfassen die folgenden Dimensionen:

- **Transparenz und Nachvollziehbarkeit**: Der Bericht unterscheidet zwischen interner Transparenz, die sich auf die Erklärbarkeit, Interpretierbarkeit und Überprüfbarkeit von KI-Modellen bezieht. Dabei bedarf es einer angemessenen Dokumentation des Designs, der Prozesse und der verwendeten Daten sowie bezüglich Erklärbarkeit und Interpretierbarkeit die Beantwortung der Frage nach dem „Wie“ bzw. dem „Warum““ einer Entscheidung, die das KI-System getroffen hat. Die externe Transparenz betrifft die Darstellung gegenüber dem Kunden, d.h. Offenlegung gegenüber Kunden, wenn diese mit KI interagieren, sie betreffende Verwendung KI-gesteuerter Entscheidungen sowie den Folgen von KI-gesteuerten Entscheidungen.
- **Governance und Rechenschaftspflicht**: Der Einsatz von KI-Anwendungen erfordert die Festlegung klarer Rollen und Verantwortlichkeiten sowie die letztendliche Verantwortung des Vorstands bzw. der Geschäftsleitung eines Finanzinstituts. KI-Richtlinien legen Mindestanforderung an die Dokumentation der Funktionsweise des KI-Modells sowie der zugehörigen Prozesse und Kontrollen sowie an weitere Schlüsselelemente (z.B. Modelländerungen inkl. Versionierung und

Ablage des Modellcodes, Audit-Protokolle sowie Details zur Nutzung von Daten) fest. Ein besonderer Fokus liegt dabei auf der Rolle des menschlichen Eingreifens, dabei werden Konzepte wie "Human-in-the-Loop" (menschliches Eingreifen in den Entscheidungszyklus der KI), "Human-on-the-Loop" (menschliches Eingreifen während des Designzyklus und anschließender Überprüfungen) und neuerdings "Human-in-Control" (Vorrang des Menschen bei kritischen Entscheidungen) hervorgehoben

- **Verlässlichkeit und Solidität**: Durchführung regelmäßiger unabhängiger Tests oder weiterer Validierungstätigkeiten, um zu bestätigen, dass ein KI-Modell wie vorgesehen funktioniert. Dazu gehören Genauigkeit, Robustheit und Zuverlässigkeit. Diese sollten vom Vorgehen für traditionelle Modelle bekannt sein, jedoch soll der Minimierung potenzieller negativer Auswirkungen Vorrang eingeräumt werden. Hierzu wird die Rolle des menschlichen Eingreifens in Fällen betont, in denen KI-Modelle Fehler möglicherweise nicht erkennen oder korrigieren können.
- **Fairness, Ethik und Sicherheit**: Zwei Dimensionen bezüglich Fairness werden hervorgehoben. Einerseits soll KI nichtdiskriminierend sein, dabei werden bezüglich Voreingenommenheit als Hauptkategorien systemisch, rechnerisch und statistisch sowie menschlich-kognitiv hervorgehoben. Andererseits bezieht sich die verfahrensrechtliche Fairness auf die Fairness innerhalb des Entscheidungsprozesses. Ethik ist weiter gefasst als Fragen der Fairness und umfasst den Schutz der Privatsphäre und den Datenschutz, Nichtdiskriminierung und Gleichberechtigung, Vielfalt, Integration und soziale Gerechtigkeit. Hier verweist der Bericht darauf, dass bereits einige Regulierungsbehörden eine Reihe von Maßnahmen vor dem Einsatz von KI-Anwendungen erfordern, da ethische Fragestellungen abhängig von der jeweiligen Jurisdiktion und gesellschaftlichen Erwartungen sind und somit übergreifende Richtlinien und Kodizes zur Nutzung und Weiterverarbeitung von Daten eine kritische Auseinandersetzung anstoßen sollen. Bezüglich Sicherheit wird betont, dass viele KI-Vorgaben und Leitfäden als Anforderung darstellen, dass KI-Systeme so eingesetzt werden müssen, dass sie keinen Schaden anrichten oder Menschenrechte verletzen. Teilweise wurden in einzelnen Staaten bereits Aufsichtsbehörden mit einem expliziten Mandat zur entsprechenden Überwachung der Einhaltung regulatorischer Daten- und KI-Vorgaben ausgestattet.
- **Datenschutz und -sicherheit**: KI-Anwendungen arbeiten im Spannungsfeld großer Datenmengen für die Erzielung zuverlässiger und solider Ergebnisse in Verbindung mit fairen und ethischen Erwartungen und dem Schutz personenbezogener Daten wie Identität, Standort und Gewohnheiten von Personen. Insbesondere können KI-Systeme eingesetzt werden, um Menschen etwa durch Deepfakes und psychologisches Profiling zu manipulieren. Parallel verweist der Bericht auf eine wachsende Abhängigkeit der Unternehmen von KI-Systemen und eine zunehmende Anfälligkeit für Cyberangriffe. In Übereinstimmung mit geltenden datenbezogenen Gesetzen und Verordnungen ist daher typischerweise die Zustimmung des Einzelnen zur Erhebung, Nutzung und Speicherung personenbezogener Daten erforderlich, die EU-Vorgaben verlangen darüber hinaus ein strenges Verfahren zur Erkennung und Korrektur von Verzerrungen bei besonderen Kategorien personenbezogener Daten (z.B. bezüglich ethnischer Herkunft, religiösen Überzeugungen,

Gesundheit/biometrischen Daten und sexueller Orientierung). Daher müssen KI-Systeme auch technisch in der Lage sein, Vertraulichkeit, Integrität und Verfügbarkeit im Falle einer Störung, einschließlich schwerwiegender Verletzungen der Cybersicherheit, aufrechterhalten zu können. Zudem fordert der Bericht eine entsprechende Organisation des internen Risikomanagements, teilweise ist bereits eine Berichtspflicht zu derartigen Vorfällen gegenüber staatlichen Behörden vorgesehen.

- **Verbraucherschutz und KI-Kenntnisse/Bewusstsein**: Die externe Rechenschaftspflicht, einschließlich der Forderung nach geeigneten Rechtsmitteln für Verbraucher, wird ebenfalls im Bericht hervorgehoben. Zudem sollen Unternehmen vor Einführung von KI-Systemen und danach während des laufenden Betriebs Sensibilisierungs- und/oder Schulungsmaßnahmen für ihre Mitarbeiter:innen durchführen, in denen insbesondere auch Auswirkungen auf gefährdete Gruppen reflektiert werden.
- **Sonstiges**: Weitere relevante Aspekte sieht der Bericht im Umgang mit geistigem Eigentum (z.B. Einholung geeigneter Lizenzen oder Genehmigungen für die Nutzung von Trainingsdaten, ordnungsgemäße Nennung der Urheber von urheberrechtlich geschütztem Material und eine transparente Erläuterung, wie KI-Systeme mit urheberrechtlich geschützten Inhalten umgehen), Nachhaltigkeitserwägungen angesichts benötigter leistungsstarker Rechenkapazitäten und einem damit einhergehenden erhöhten Energiebedarf, internationaler Interoperabilität vor dem Hintergrund verschiedener regulatorischer Rahmenwerke und Ethikerwartungen sowie Partnerschaften zwischen öffentlichem und privatem Sektor angesichts einer teilweise beobachteten engen Zusammenarbeit zwischen Regierung, Industrie, Wissenschaft und verschiedenen Vertretern der Zivilgesellschaft.

Im Folgenden bricht der Bericht diese Dimensionen anhand einer als Use Case diskutierten Kredit- und Versicherungsprüfung vertieft herunter. KI könne beim Underwriting unterstützen, da in kürzerer Zeit umfangreiche und teilweise auch unstrukturiert vorliegende Daten für eine risikoadäquate Entscheidungsfindung herangezogen werden können, eine bessere Kundenerfahrung erreicht werde und damit insgesamt auch Kapazitäten ausweiten – und somit zunehmend auch in den aufsichtlichen Fokus rücken. Dabei wird darauf verwiesen, dass einige der oben genannten Dimensionen bereits in der Vergangenheit bei traditionellen Modellen angewendet und insbesondere damit auch im Fokus regulatorischer Vorgaben standen und in jüngerer Zeit zunehmend ein prinzipienorientierter Ansatz mit dem Fokus auf eine angemessenes Risikomanagement und angemessene Kontrollen bei der Geschäftstätigkeit verfolgt wird, der im Licht einer zunehmenden KI-Anwendung sich auch auf technologische Aspekte ausweiten muss. Dabei zeigt sich global (noch) ein uneinheitliches Bild, inwiefern die KI-Anwendung spezifisch für die Finanzdienstleistungsbranche reguliert werden muss. Transparenz und Nachvollziehbarkeit werden als zentrale Anliegen für den Use Case identifiziert, da es sich um einen Anwendungsfall mit hohem Risiko handelt. Der Bericht unterstreicht, dass Entscheidungsträger:innen ein klares Verständnis der Funktionsweise von KI-Systemen benötigen, um sicherzustellen, dass ihre Ergebnisse mit den regulatorischen Erwartungen und der Risikobereitschaft der Institutionen übereinstimmen und zugleich die Anforderungen an Fairness und Nichtdiskriminierung sowie Erklärbarkeit

erfüllt sind.

Ein Mangel an Erklärbarkeit von KI-Modellen kann ein erhöhtes Modellrisiko zur Folge haben, denn KI-Modelle – insbesondere generative KI-Systeme – arbeiten oft als Blackbox, so dass es schwierig ist, ihre Ergebnisse zu überprüfen oder zu verstehen, wie bestimmte Entscheidungen zustande gekommen sind. Daher wird insbesondere der Aufbau von KI-Expertise und -Fähigkeiten gefordert. Im Zuge der Weiterentwicklung von KI-Technologien müssen die Unternehmen sicherstellen, dass ihre Teams in der Lage sind, die Komplexität der Systeme einzuordnen und zu managen. Ein Mangel an technischen Kenntnissen auf Führungsebene könnte zudem zu unzureichender Wahrnehmung der Leitungs- und Überwachungsfunktion und ineffektiver Risikominderung führen. Der Bericht macht auch auf datenbezogene Risiken aufmerksam, die durch die zunehmende Abhängigkeit von Drittanbietern für KI-Modelle und Cloud-basierte Dienste noch verschärft werden. Diese externen Beziehungen bieten zwar Skalierbarkeit und Kosteneffizienz, bringen aber auch Schwachstellen wie Datenschutzverletzungen und Anbieterbindung mit sich und erfordern ein entsprechendes Third-Party-Risikomanagement

Sie haben Fragen zur KI-Anwendung und der diesbezüglichen Governance sowie dem entsprechenden Upskilling in Ihrem Unternehmen? Profitieren Sie von unserer umfassenden sektorübergreifenden Expertise in der Regulierung von Finanzinstituten und Versicherungsunternehmen, die insbesondere neben traditionellem Modellrisikomanagement auch Aspekte der IT-Governance rund um VAIT und DORA sowie die KI-Governance umfasst. Gehen Sie gerne auf mich und meine Kolleg:innen von Governance, Risk and Compliance Insurance zu, wenn Sie Interesse an diesem Themengebiet haben. Wir freuen uns auf den Austausch mit Ihnen!

Keywords

Aktuar, Artificial Intelligence (AI), Datenanalyse, Datenschutz, Digitalisierung, Model Risk, Prozesse, Versicherungsmarkt

Contact

Tilmann Schmidt

München

tilmann.schmidt@pwc.com