Insurance News Blog

By PwC Deutschland | 20. Mai 2025

Open Insurance, FiDA und Künstliche Intelligenz – ein paar Gedanken

Unsicherheiten aus sich ausbreitenden Einsatz von KI und kommenden Datenaustausch im Versicherungsbereich gesamthaft adressieren, um Akzeptanz für Open Insurance zu fördern

Nicht zuletzt angesichts der von Technologisierung und Digitalisierung getriebenen Veränderungswucht der letzten Jahre strebt die Europäische Union den Ausbau der Datenwirtschaft an, damit der globale Anteil hieran dem wirtschaftlichen Gewicht des europäischen Wirtschaftsraums entspricht. Dies gilt auch für einen die digitalisierte Versicherungswelt einschließenden Finanzdienstleistungssektor: Hier soll mit der FiDA-Regulierung ein einheitlicher Rechtsrahmen für den Zugang zu Finanzdaten geschaffen werden (vgl. **unsere Ausführungen hier**, dort finden Sie auch unser FiDA Whitepaper zum Download!). In unserer aktuellen Webcast-Reihe zu „**FiDA für die Versicherungsbranche**“ kam dabei auch die Frage nach Anwendungsfällen von Künstlicher Intelligenz im FiDA-Kontext auf, daher skizzieren wir im Folgenden dieses Thema, um Impulse für eine weitergehende Diskussion zu setzen.

Die FiDA-Verordnung spannt den Rahmen für den kommenden Datenaustausch im Versicherungsbereich und adressiert in diesem Zusammengang die Rechte und Pflichten von Dateninhabern und Datennutzern. Damit gehen notwendige technischen Anpassungen einher, um zukünftig den Austausch relevanter Daten in Echtzeit über eine Schnittstelle zwischen den Dateninhabern und Datennutzern zu ermöglichen. Gleichzeitig gilt es, mit strategischen Erwägungen den über einen minimale Compliance hinausgehenden Nutzen aus der Regulierung zu erfassen. Bei entsprechenden Use Cases zur Verarbeitung der Daten kann der Einsatz Künstlicher Intelligenz eine Rolle spielen – sowohl auf Seiten der Dateninhaber als auch Datennutzer.

Anforderungen und Regelungen zum Austausch relevanter Daten

Das Sammeln und Weitergeben von Daten über Versicherungspolicen oder andere versicherungsbezogene Daten kann sensible Informationen z.B. über die Gesundheit, Sexualität und politische Ansichten oder andere persönliche Details einer Person offenbaren. Diesem Risiko begegnet die FiDA-Regulierung einerseits mit einem reduzierten Scope – das Krankenversicherungsgeschäft ist nach aktuellem Stand (vor den im April gestarteten und noch laufenden Trilogverhandlungen) komplett außen vor, ebenso von Lebensversicherungsunternehmen vertriebene Risikoleben- und Berufsunfähigkeitsversicherungen – und andererseits mit der engen Verknüpfung an Vorschriften für die Verarbeitung personenbezogener Daten, wie sie insbesondere in der Datenschutz-Grundverordnung (DSGVO) adressiert sind, und dem ab September 2025 anzuwendenden Data Act für nicht-personenbezogene Daten.

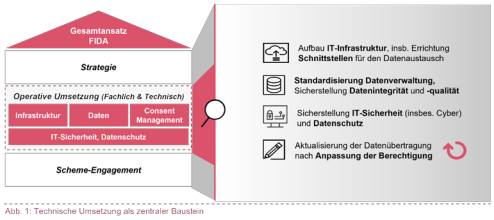

Abb. 1: Technische Umsetzung als zentraler Baustein

Der Gesamtansatz bei der FiDA-Umsetzung kann anhand der drei Dimensionen Strategie, Operative Umsetzung und Scheme-Engagement erfolgen. Dabei ist die technische Umsetzung ein zentraler Baustein, der sich einerseits in bei der Implementierung sowie andererseits für den laufenden Betrieb zu

berücksichtigende Aspekte untergliedern lässt (vgl. Abb. 1). Für den Erstaufsatz sind dabei insbesondere eine relevante IT-Infrastruktur zum Datentransport von den Quellsystemen zur aufzusetzenden Scheme-Schnittstelle in Echtzeit und der zugehörigen Datenaufbereitung, ein adäquates Datenmanagement sowie stabile und sichere Prozesse und Anwendungen relevant. Dem Consent Management kommt eine bedeutende Rolle zu, da hier der Endkunde seine Zugriffsberechtigungen jederzeit steuern kann – bei Einschränkung oder Widerruf muss entsprechend die Datenverarbeitung eingeschränkt bzw. die bis dato verfügbaren Daten ggf. gelöscht werden.

Einsatz von KI-Anwendungen im Rahmen von Use Cases

Technische Umsetzung und strategische Erwägungen haben gegenseitigen Einfluss. Bei der Anpassung an der IT-Landschaft sollten Bedarfe aus potenziellen Use Cases reflektiert werden. Dies ist insbesondere für Datennutzer relevant, wenn Daten übernommen und dann für Dienstleistungen genutzt werden.

Zwar macht FiDA allgemeine Vorgaben zum Datenaustausch und den Rollen von Dateninhabern und Datennutzern, zu konkreten Anwendungsfeldern schweigt sich der Regulator jedoch aus. Im Herbst 2024 veröffentlichte zwar EIOPA die **Ergebnisse eines unabhängig von der FiDA-Entwicklung konsultierten Anwendungsfalls** in Form eines „Insurance Dashboards“ – auch dieser eher allgemeine Use Case.geht allerdings nicht auf KI-Anwendungen ein.

Daneben verweist der Entwurf in seiner Begründung explizit auf die weiteren regulatorischen Anforderungen zu Datenschutz und -governance der DSGVO, den Data Act sowie zur digitalen operationellen Resilienz im Finanzsektor (DORA). Daneben steht der AI Act, der die KI-Anwendung industrieunabhängig reguliert. Im risikobasierten Ansatz der europäischen Regulierung in den High-Risk-Bereich fallende versicherungsspezifische Anwendungsfälle im Pricing und Underwriting von Kranken- und Lebensversicherung dürften bis auf Einzelfälle im Graubereich aufgrund des oben erwähnten Ausschlusses aus dem FiDA-Scope ohnehin nicht relevant sein. Für darüber hinausgehende Use Cases sind insbesondere die Vorgaben des AI Act zu beachten, zudem spielt hier die Kundenfreigabe eine Rolle: nur bei expliziter Freigabe – in diesem Fall neben dem Datenaustausch zwischen Dateninhaber und Datennutzer auch explizit für die KI-Verarbeitung für die angefragte Dienstleistung.

Absicherungserwägungen rund um den KI-Einsatz und Software-as-a-Service-Anwendungen

Die oben erwähnte IT-Sicherheit spielt bei der Berücksichtigung von KI-Anwendungen zur Aufbereitung und Weiterverarbeitung erhaltener Daten als Grundlage von Dienstleistungsangeboten eine bedeutende Rolle. Rund um die KI-Anwendung ist eine entsprechende Governance zu entwickeln und zu etablieren, die sich in die übergreifende Strategie einbettet (vgl. Abb. 2). Dabei gilt es laufende dynamische Entwicklungen zu berücksichtigen, mit Agentic AI haben sich KI-Modelle erst in jüngerer Vergangenheit nochmals stark weiterentwickelt (vgl. hierzu **dieses aktuelle Whitepaper**).

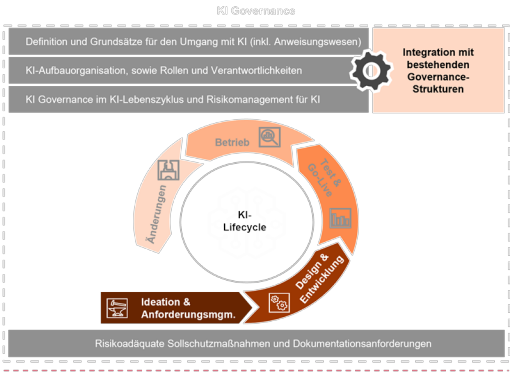

Abb. 2: Grundschema KI-Governance

Im Falle des Rückgriffs auf von externen Dritten angebotenen Anwendungen und Softwarelösungen sind Maßnahmen zu treffen, die das Drittparteienrisiko reflektieren. Dabei sollten sich Unternehmen bei spezialisierten Anbietern insbesondere Konzentrationsrisiken sowie möglichen Unsicherheiten bewusst sein, die aus schnell aufeinander folgenden Veröffentlichungen von Produkten, Produktvarianten oder neuen Komponenten ohne umfassende integrierte oder standardmäßig aktivierte Sicherheitsmaßnahmen auf Seiten des Anbieters entstehen können.

Während klassisch externe Interaktionsebenen wie Schnittstellen absichtlich architektonisch von den zentralen Backend-Systemen, Anwendungen und Daten eines Unternehmens getrennt sind, können durch moderne Nutzungsmodelle wie z.B. Software-as-a-Service diese strikten Trennungen aufgelöst werden. Bei korrekter Funktionsweise kann damit kosteneffizient die Produktivität erhalten und möglicherweise gesteigert werden, im Falle von Kompromittierungen ergeben sich jedoch signifikante Risiken durch den Zugriff auf vertrauliche Daten. Daher sollten entsprechende Sicherheitsmaßnahmen von den Unternehmen in den internen IT- und KI-Strategien sowie Risikokultur reflektiert werden und daraus abgeleitet den Weg in die hieraus herunter gebrochenen Arbeitsanweisungen und weiteren Vorgaben finden.

Scheme-Betreiber müssen daher darauf achten, dass in einem um das Scheme entstehenden Ökosystem eine vertrauenswürdige Integration ermöglicht wird und damit kontinuierliche Nachweise einfordern, dass Kontrollen und weitere Sicherheitsmaßnahmen effektiv funktionieren. Dies betrifft Dateninhaber und entsprechende Anwendungen insbesondere bei der Aufbereitung der relevanten Daten vor der Freigabe über die Schnittstelle gleichermaßen wie Datennutzer bei der Verarbeitung dieser Daten. Zudem sollte von diesen jeweils bei der Wahl von Drittanbietern – sowohl bei klassischen als auch integrierten Nutzungsmodellen – auf den Stellenwert geachtet werden, den diese Sicherheitsaspekten und zugehörigen risikomitigierenden Maßnahmen einräumen. Denn letztlich stehen die hieraus resultierenden Risiken im Verantwortungsbereich des jeweils hierauf zurückgreifenden Dateninhabers oder Datennutzers.

Die Integration muss neu gedacht werden, denn die vernetzte Welt braucht eine moderne Sicherheitsarchitektur, bei der auch KI-Risiken berücksichtigt werden. KI-Anwendungen reizen mit Automatisierung, Personalisierung und Effizienzsteigerung bei der Problemlösung – eine einfache

Handhabung sowie ein beobachtbarer Nutzen sind entsprechend zentrale Voraussetzung für eine Nutzung durch Endkunden. Gleichzeitig muss aber auch das Vertrauen in die Anwendung und den Umgang mit sensiblen Informationen geschaffen werden, damit eine hohe Akzeptanz erreicht wird. Verbindungen sichern, bevor leistungsstarke KI-Tools auf sensible Umgebungen und Daten losgelassen werden, wird damit zu einer zentralen Aufgabe.

Fazit

Die Anwendung von KI-Lösungen „in der Breite“ muss sich in der Versicherungswirtschaft – auch unabhängig von FiDA – noch etablieren. Die Regulierungsinitiative kann dabei als Beschleuniger datengetriebener Geschäftsmodelle und Dienstleistungsangebote im Finanzdienstleistungsbereich allgemein und im Versicherungssektor im Speziellen wirken, dies ist auch ein erklärtes Ziel der Initiative. Wenngleich Künstliche Intelligenz nicht explizit in den Entwürfen der Verordnung genannt ist, entwickeln sich mit wachsender Verfügbarkeit relevanter Daten KI-Anwendungsfälle auch im FiDA-Kontext, da durch die Regulierung standardisiert Daten bereitgestellt werden müssen. Dabei sollte schon im Zuge der technischen Implementierung und Anpassung an der bestehenden IT-Landschaft an die Flexibilität gedacht werden, um hier Prozesse und Anwendungen an ein dynamisches Umfeld adaptieren zu können. Gleichzeitig ist eine Sicherstellung von IT-Sicherheit nicht nur vor dem Hintergrund möglicher Cyberangriffe über integrierte Systeme und des adäquaten Datenschutzes essenziel – dies kann entscheidendes Kriterium bei der Wahl von Drittanbietern sein.

Sie haben Fragen zu Open Insurance, der FiDA-Regulierungsinitative und der Anwendung und Governance von Künstlicher Intelligenz im Versicherungsbereich? Kommen Sie gerne auf mich sowie meine Kolleg:innen aus **Actuarial Risk Modelling Services / GRC Insurance** bzw. **Technology and Process Risk** zu. Gemeinsam diskutieren wir mit Ihnen lösungsorientiert die Chancen und Herausforderungen.

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

Schlagwörter

Aktuar, Artificial Intelligence (AI), Datenanalyse, Datenschutz, Lebensversicherung, Risk Management Insurance, Schaden- und Unfallversicherung

Kontakt

Tilmann Schmidt
München
tilmann.schmidt@pwc.com