

Regulatorik:

Zwischen Innovation und Compliance

Versicherungsforen-**Themendossier**

Nr. 15/2026

17. August 2026

im
Dossier

Warum Geldwäscheprävention mehr denn je Thema der Versicherer ist

DORA – IT-Governance und Prozesse als Grundlage digitaler operativer Resilienz

Solvency II im Wandel: Neue Möglichkeiten für die strategische Asset-Allokation

Versicherungsforen **THEMENDOSSIER**

Eine Publikation der

 **Versicherungs**foren Leipzig

KI-Compliance in der Versicherungswirtschaft: RegTech schafft den Ausweg

von Rüdiger Lang, Consileon

Warum der EU AI Act strukturellen Handlungsbedarf erzeugt und wie technologiegestützte Compliance-Lösungen den Aufwand beherrschbar machen:

Viele Versicherungsunternehmen haben in den vergangenen zwei Jahren bemerkenswerte Fortschritte beim Einsatz Künstlicher Intelligenz gemacht. Copilot- oder ChatGPT-Lizenzen wurden ausgerollt, im Schadenmanagement werden erste Automatisierungslösungen produktiv genutzt, HR-Abteilungen erproben KI-gestützte Recruiting-Tools. Parallel dazu haben zahlreiche Häuser begonnen, ihre Belegschaft zu sensibilisieren, KI-Führerschein und interne Schulungsformate sind vielerorts entstanden.

Das Ergebnis ist ein verbreitetes Muster: KI ist im Unternehmen angekommen, aber ohne übergreifende Steuerung. Die Governance-Frage wurde vertagt.

Der EU AI Act trifft Versicherungen an mehreren Stellen

Mit dem EU AI Act, dessen Kernpflichten für Hochrisiko-KI-Systeme ab August 2026 grei-

fen, ändert sich die Ausgangslage grundlegend. Entscheidend ist dabei eine Unterscheidung, die in der Praxis häufig übersehen wird: Der Act reguliert nicht primär Technologien, sondern Verwendungszwecke.

Ein und dieselbe Software kann je nach Einsatzszenario regulatorisch irrelevant oder hochriskant sein. Microsoft Copilot etwa ist als Produktivitätswerkzeug grundsätzlich unkritisch. Wird es jedoch im HR-Bereich eingesetzt, um Bewerbungsunterlagen vorzusortieren oder Leistungsbeurteilungen zu unterstützen, fällt dieser Use Case unter Annex III des AI Act mit der Folge substanzieller Compliance-Pflichten.

Für Versicherungsunternehmen gilt das in besonderem Maße. Annex III klassifiziert KI-Systeme explizit als hochriskant, wenn sie bei der Risikobewertung und Tarifierung im Bereich Kranken- oder Lebensversicherungen eingesetzt werden, Entscheidungen über Leistungsauszahlungen unterstützen oder zur Betrugserkennung mit direkten Konsequenzen für Versicherungsnehmer beitragen. Das betrifft keine Randphänomene, sondern Kernprozesse der Branche.

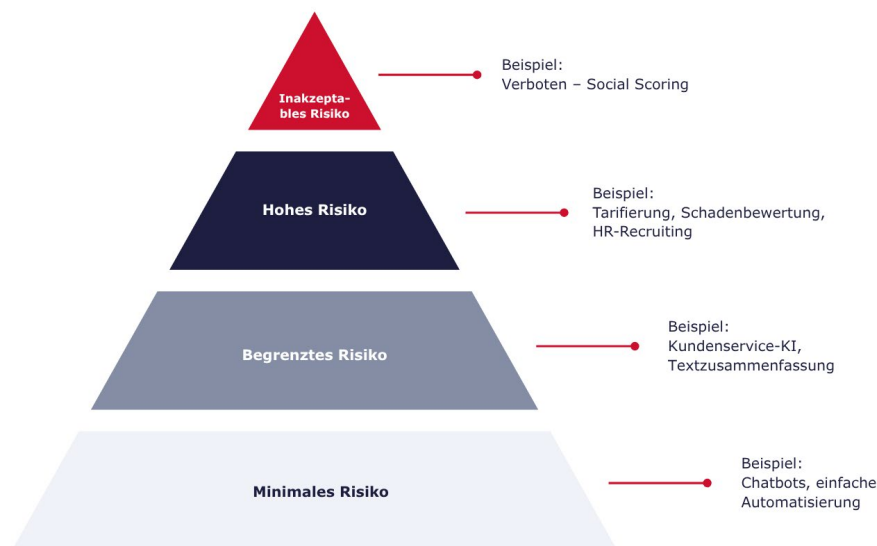


Abbildung 1: Risikosysteme

Was auf Versicherungen konkret zukommt

Die Pflichten, die der AI Act Deployern von Hochrisiko-Systemen auferlegt, sind umfangreich und werden in ihrer operativen Konsequenz noch vielfach unterschätzt.

Zunächst braucht jedes Hochrisiko-System eine vollständige technische Dokumentation: Zweck, Funktionsweise, eingesetzte Daten, Leistungsgrenzen, bekannte Risiken. Diese Dokumentation muss aktuell gehalten werden, jede wesentliche Änderung am System zieht eine Aktualisierungspflicht nach sich. Hinzu kommt die Pflicht zur Konformitätsbewertung vor dem produktiven Einsatz sowie zur Registrierung in der EU-Datenbank für KI-Systeme.

Im laufenden Betrieb sind Logging und Auditierbarkeit sicherzustellen: Systeme müssen so konfiguriert sein, dass relevante Ereignisse protokolliert und bei Anfragen von Aufsichtsbehörden wie der BaFin nachvollzogen werden können. Parallel dazu sind Betroffene, also etwa Antragsteller oder Versicherungsnehmer, über den Einsatz von KI bei sie betreffenden Entscheidungen zu informieren. Und schließlich muss menschliche Aufsicht über automatisierte Entscheidungen nicht nur konzeptionell vorgesehen, sondern nachweisbar gewährleistet sein.

Projiziert man diese Anforderungen auf eine realistische Systemlandschaft, wird der Aufwand greifbar: Eine mittelgroße Versicherung, die KI in Tarifierung, Schadensbearbeitung, HR und Kundenservice einsetzt, hat schnell

sechs bis zehn potenzielle Hochrisiko-Systeme im Betrieb, jedes mit eigenem Dokumentations-, Bewertungs- und Überwachungszyklus. Allein die initiale Dokumentation eines einzelnen Systems kann mehrere Personenwochen erfordern, wenn sie manuell erarbeitet wird. Multipliziert mit der Systemzahl und dem laufenden Aktualisierungsbedarf entsteht ein dauerhafter operativer Aufwand, der mit klassischen Compliance-Ressourcen kaum zu stemmen ist.

Das eigentliche Problem: fehlende Übersicht

Bevor all das greift, muss eine grundlegende Frage beantwortet sein: Welche KI-Systeme sind überhaupt im Einsatz? In Unternehmen mit dezentralem KI-Wildwuchs – und das betrifft einen erheblichen Teil der mittelgroßen Versicherungsbranche – ist diese Frage oft

nicht verlässlich zu beantworten. Fachbereiche beschaffen eigenständig, IT hat keinen vollständigen Überblick, Compliance war bislang nicht systematisch eingebunden.

Ohne vollständiges KI-Inventar ist keine Risikoklassifizierung möglich. Ohne Klassifizierung lässt sich nicht bestimmen, welche Systeme unter den AI Act fallen. Und ohne diese Grundlage bleibt jede Compliance-Maßnahme lückenhaft – unabhängig davon, wie viele Führerscheine ausgestellt wurden.

RegTech als Antwort auf strukturelle Komplexität

Genau hier liegt der Ansatzpunkt für technologiegestützte Compliance-Lösungen – kurz RegTech. Statt manuelle Prüfprozesse hochzuskalieren, setzen moderne Plattformen auf KI-gestützte Automatisierung: Regulatorische

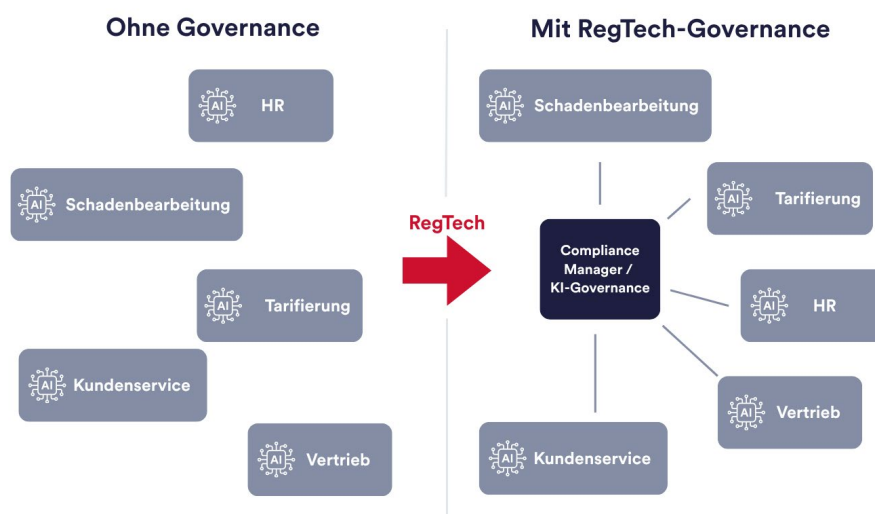


Abbildung 2: Governance-System

Anforderungen werden kontinuierlich überwacht und auf Relevanz bewertet (Regulatory Watch), interne Dokumente, Prozessbeschreibungen und Verträge automatisch gegen das aktuelle Regelwerk abgeglichen und identifizierte Lücken in strukturierte Handlungsempfehlungen überführt.

Gap-Analysen, die manuell Wochen dauern würden, lassen sich so in Stunden durchführen. Änderungen im Regelwerk werden frühzeitig erkannt, bevor sie zur Compliance-Lücke werden. Reporting-Funktionen erzeugen auditfähige Nachweise, die gegenüber Aufsichtsbehörden oder internen Revisionen vorgelegt werden können – ohne mühsame manuelle Aufbereitung.

Lösungen wie der Consileon Compliance Manager adressieren genau diese Anforderungen für regulatorische Rahmenwerke wie DORA, MaRisk und NIS-2. Ein spezifisches Modul für den EU AI Act befindet sich in Entwicklung.

Strukturelle Antworten statt punktueller Maßnahmen

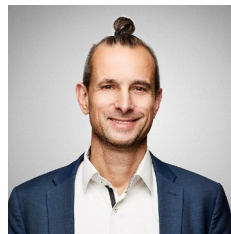
Was Versicherungsunternehmen jetzt brauchen, ist keine weitere Schulungsoffensive, sondern eine strukturierte Antwort auf drei Fragen: Was setzen wir ein? Was davon ist regulatorisch relevant? Wer ist dafür verantwortlich?

Das erfordert funktionsübergreifende Zusammenarbeit zwischen IT, Recht, Compliance und den jeweiligen Fachbereichen – und eine

Governance-Struktur, die KI nicht als IT-Thema behandelt, sondern als unternehmensweite Managementaufgabe. RegTech-Lösungen können dabei den operativen Aufwand erheblich reduzieren. Sie ersetzen jedoch nicht die strategische Entscheidung, das Thema ernsthaft anzugehen.

Seit dem 2. August 2026 ist beim EU AI Act vor allem die Transparenzpflicht (Art. 50) wirksam. Wer jetzt mit dem Inventar beginnt, hat noch die Chance, strukturiert vorzugehen. Wer wartet, wird unter Druck dokumentieren – und das sieht man den Ergebnissen dann meistens an.

Autor



Rüdiger Lang

Principal

Consileon Business Consultancy GmbH

Mehr zu Consileon:

<https://www.consileon.de/>

Über den Autor:

Rüdiger Lang ist Principal bei der Consileon Business Consultancy GmbH und verantwortet dort den Bereich KI-Beratung. Er begleitet Unternehmen aus Finanzdienstleistung und Versicherung bei der strategischen Einführung und Governance von KI-Systemen.

IMPRESSUM

Autoren des vorliegenden Themendossiers

Anna-Lena Erhard et al.

E Anna-Lena.Erhard@versicherungsforen.net

Diese Publikation wurde nach den Grundprinzipien des [Redaktionskodex der Versicherungsforen Leipzig](http://www.versicherungsforen.net/redaktionskodex) verfasst: www.versicherungsforen.net/redaktionskodex

Feedback zum vorliegenden Themendossier

Wenn Sie uns Ihre Meinung mitteilen möchten, würde uns das sehr freuen. Vielleicht gibt es ja ein spezielles Thema, über das Sie im Themendossier einmal lesen möchten? Haben Sie weitere Fragen und Anregungen oder Anlass zur Kritik? In jedem Fall freuen wir uns über eine Nachricht von Ihnen.

Bitte senden Sie Ihre Kommentare an

Anna-Lena Erhard | T +49 341 98988-223 | E Anna-Lena.Erhard@versicherungsforen.net

Abonnement des Versicherungsforen-Themendossiers

Aufgrund der Partnerschaft Ihres Unternehmens mit den Versicherungsforen Leipzig steht Ihnen das Abonnement des Versicherungsforen-Themendossiers unternehmensweit zur Verfügung! Gern können Sie deshalb weitere Empfänger aus Ihrem Haus registrieren lassen. Nutzen Sie dazu einfach unser Anmeldeformular unter www.versicherungsforen.net/themendossier.

Eine Übersicht über alle Partnerunternehmen finden Sie unter www.versicherungsforen.net/partner.

Abbestellen des Versicherungsforen-Themendossiers

Sie wollen das Themendossier in Zukunft nicht mehr empfangen? Senden Sie einfach eine E-Mail mit dem Betreff „unsubscribe Themendossier“ an kontakt@versicherungsforen.net.

Versicherungsforen-Newsletter

Wenn Sie regelmäßig per E-Mail über Aktualisierungen im Bereich „Wissen“ auf www.versicherungsforen.net, Veröffentlichungen, gegenwärtige Veranstaltungen sowie Nachrichten aus unserem Partnernetzwerk informiert werden möchten, können Sie sich auf www.versicherungsforen.net/newsletter anmelden. Diesen Service bieten wir auch für Nicht-Partnerunternehmen kostenfrei an.

© 2026 Versicherungsforen Leipzig GmbH

Ein Unternehmen der LF Gruppe | Hainstraße 16 | 04109 Leipzig |

T +49 341 98988-0 | F +49 341 98988-9199 | E kontakt@versicherungsforen.net | I www.versicherungsforen.net

Geschäftsführung: Justus Lücke, Jens Ringel | Amtsgericht Leipzig HRB 25803

USt-IdNr.: DE268226821