ÖSTERREICHISCHE FMA·FINANZMARKTAUFSICHT

FMA-FORUM:

NEXT LEVEL TECH@INSURANCE: VU / PK / BVK

Aufsicht über Versicherungsunternehmen, Pensionskassen und Betriebliche Vorsorgekassen

Wien, 23. April 2026

ÖSTERREICHISCHE FMA · FINANZMARKTAUFSICHT

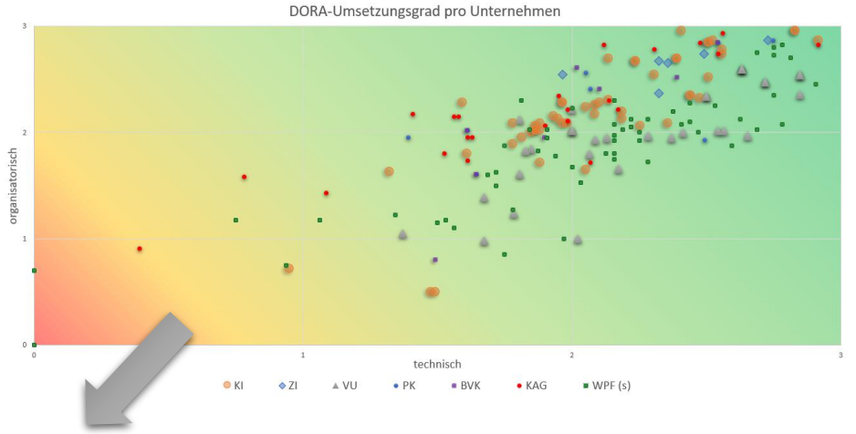
NEXT LEVEL TECH:

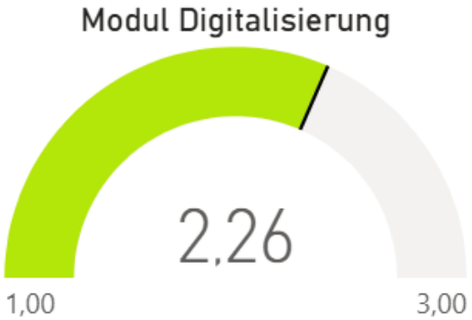
ERWARTUNGSHALTUNG & FOKUS DER AUFSICHT

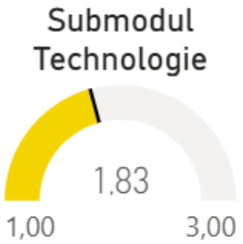
JUDr. Stanislava Saria, PhD

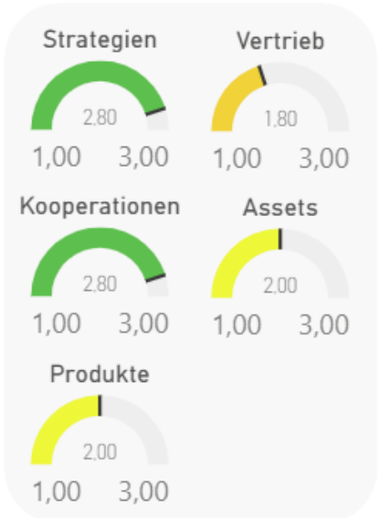
Wien, 23. April 2026

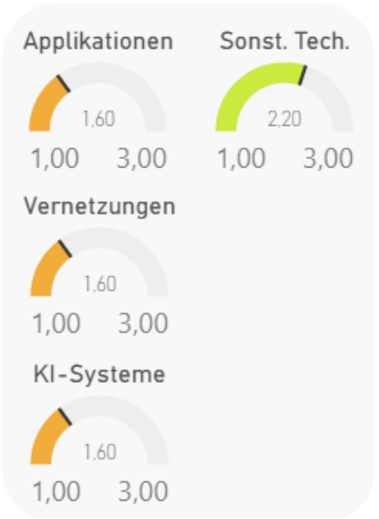
360°-VIEW AUF DAS DIGITALE RISIKOPROFIL

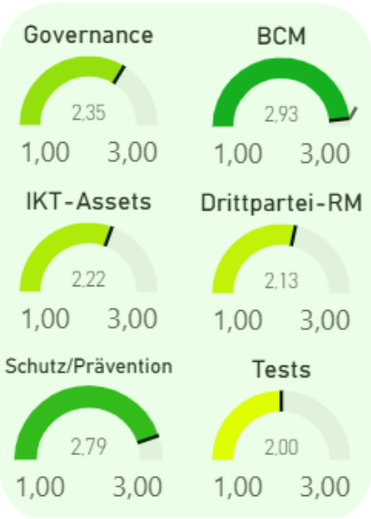












AI-BASIERTE SYSTEME **STARK IM WACHSEN**

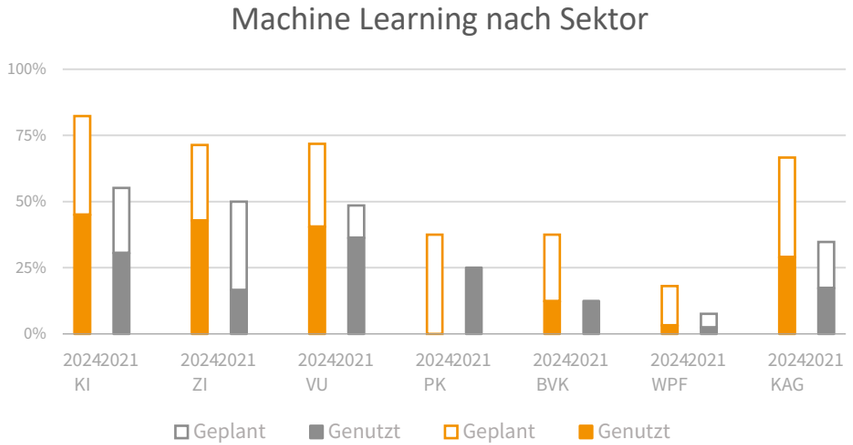
→ SEIT 2018 SUKZESSIVER ANSTIEG ENTLANG DER GESAMTEN WERTSCHÖPFUNGSKETTE

- Je **mehr digitale Technologien** ein Unternehmen insgesamt einsetzt, desto häufiger macht es sich auch die künstliche Intelligenz zu Nutze.

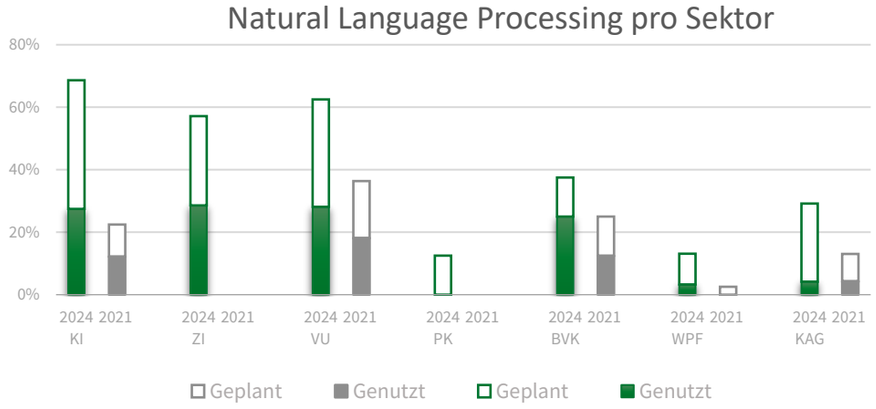
- **AI-basierte Systeme** stellen starke Wachstumsgebiete dar. Die 2021 kommunizierten Ausbaupläne wurden über alle Sektoren hinweg erfüllt.

- Auffallend hoch sind die **Ausbaupläne in allen Sektoren**: Bis 2027 wollen ¾ der KI, ZI, VU aber auch KAG Machine Learning-Techniken einsetzen. Ähnlich ambitioniert sind die Ausbaupläne bei Natural Language Processing**:** Bis 2027 streben KI, ZI und VU einen Nutzungsgrad von weit über 50% an.

- **Machine Learning:** Mehr als ¼ der Beaufsichtigten nutzt bereits ML in ihrer Geschäftstätigkeit.
  - Vorreiter beim Einsatz von maschinellem Lernen sind KI (45 %), ZI (43 %) und VU (41 %).
  - Die Haupteinsatzgebiete sind **Ratingsysteme, Fraud Analytics**, Unterstützung in den Bereichen **IT, Verwaltung** und **Marketing**.



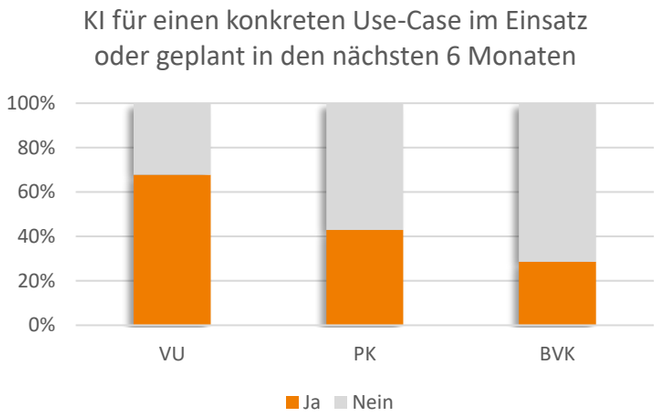
- **Natural Language Processing** hat seit 2021 an Bedeutung gewonnen.
  - In den Sektoren KI, ZI, VU und BVK beträgt der Nutzungsgrad bereits über 20%
  - Insb. **Chatbots** bei der Kundenkommunikation eingesetzt.

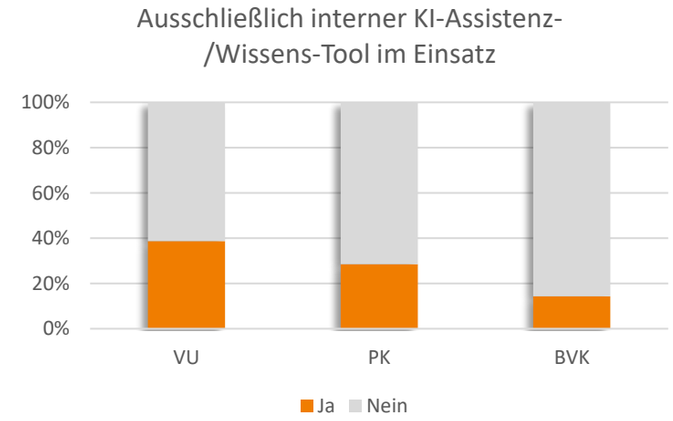


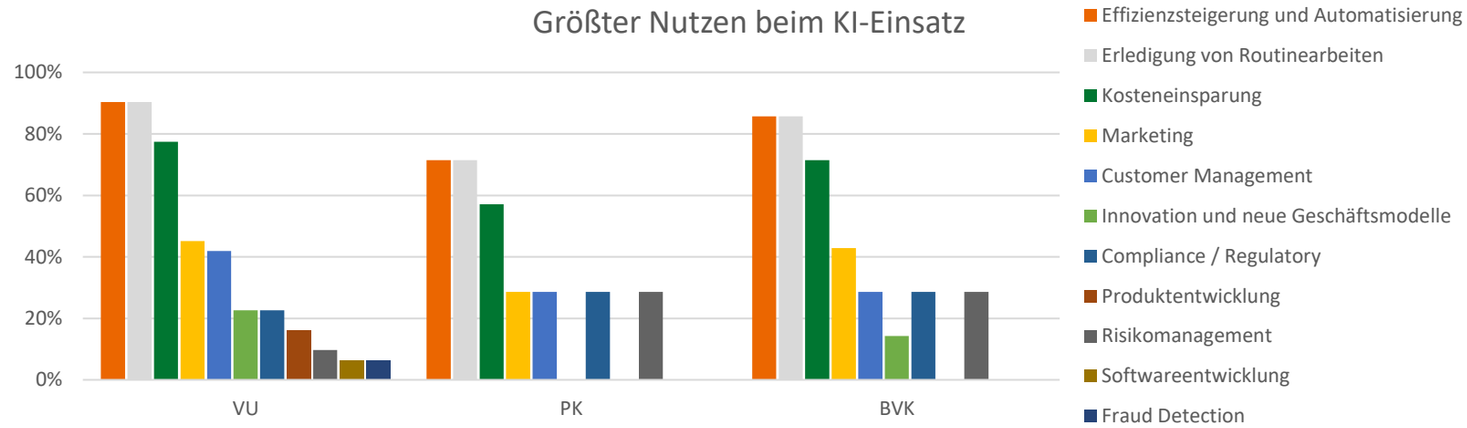
Q, FMA Austrian Digital Finance Landscape 2024

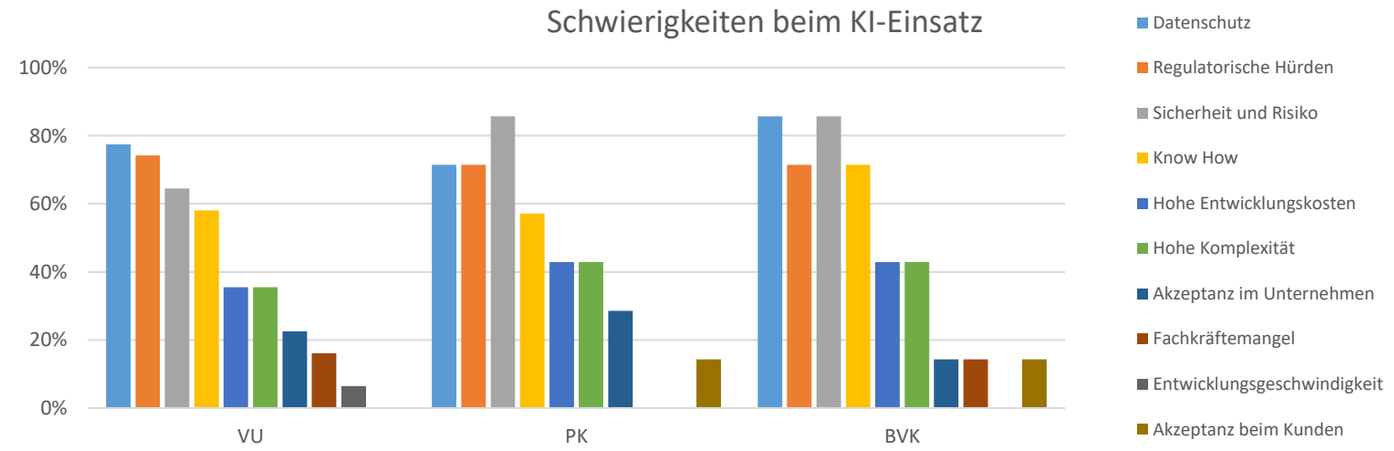
AI-SYSTEME: AKTUELLER EINSATZ

→ MEHR ALS ⅔ DER VU SETZT KI FÜR **KONKRETE USE CASES** IM GESCHÄFTSBETRIEB EIN





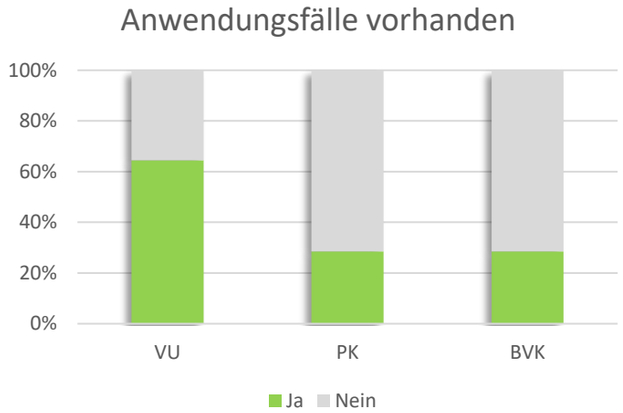


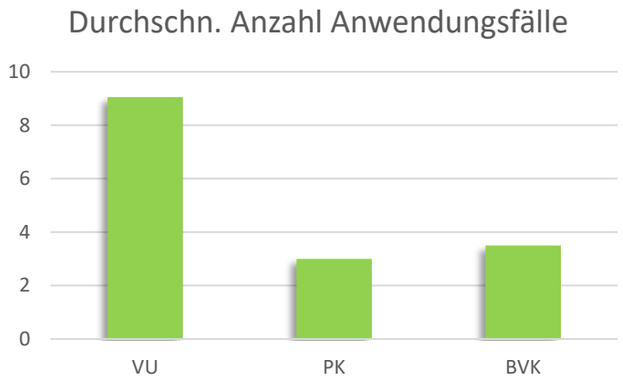


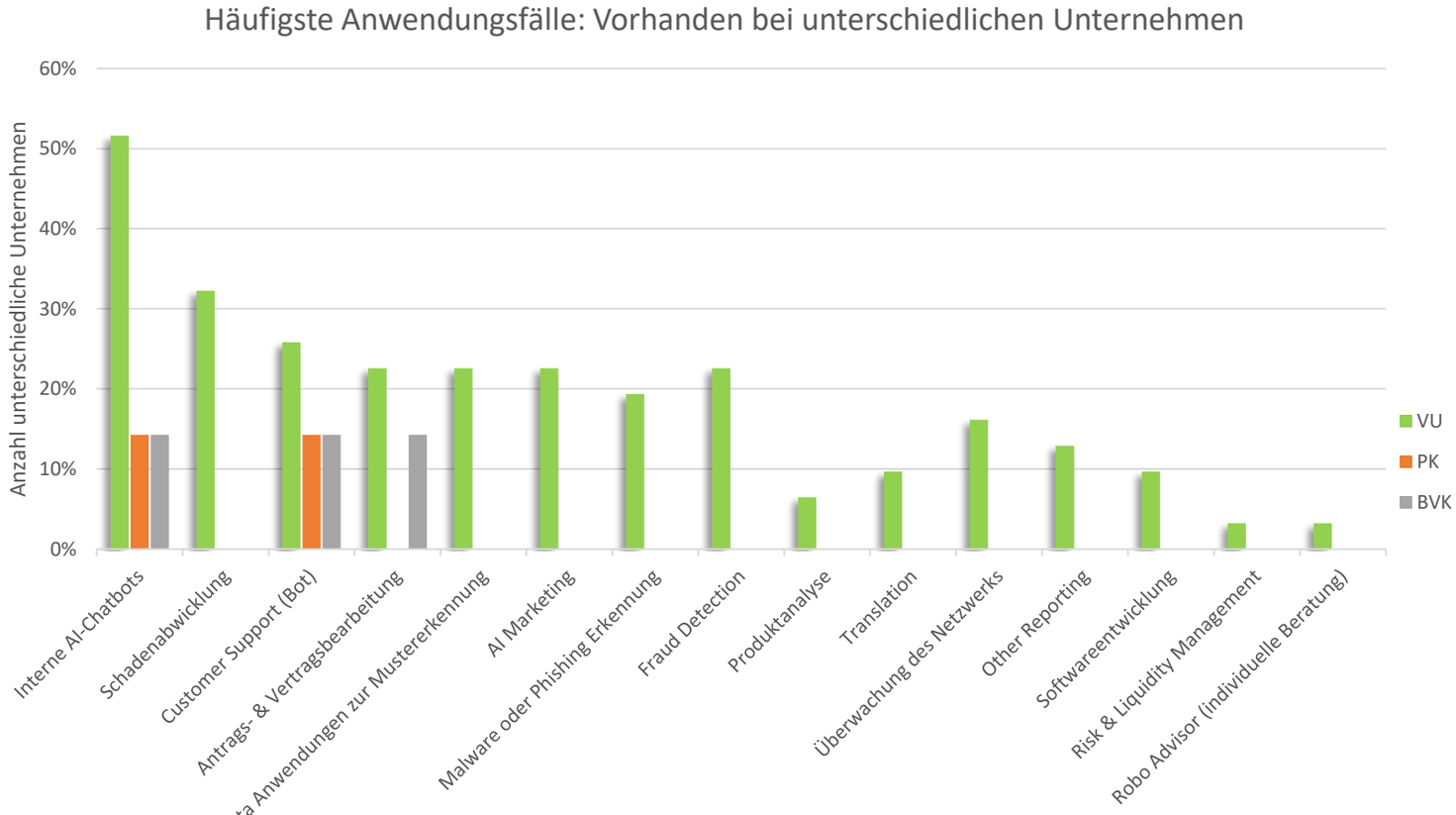
Q, FMA-Erhebung, April 2026: Marktabdeckung von 100% in allen Sektoren (VU/PK/BVK)

AI-SYSTEME: ANWENDUNGSFÄLLE

→ MEHR ALS ½ DER VU NUTZT INTERNE **AI-CHATBOTS**; IN DER **SCHADENABWICKLUNG** SETZT BEREITS ⅓ DER VU AUF AI;
BEI DER POLIZZIERUNG, VERTRAGSABWICKLUNG UND FRAUD DETECTION IST ES ¼ DER VU







Q, FMA-Erhebung, April 2026: Marktabdeckung von 100% in allen Sektoren (VU/PK/BVK)

Saria, FMA

AI-ACT: REGULATORISCHE EINBETTUNG

→ AI-ACT BETRIFFT ALLE UNTERNEHMEN, DIE KI-SYSTEME INNERHALB DER EU BETREIBEN ODER BEREITSTELLEN

	AI-Act	Solvency II / IDD	DORA
Fokus:	Produktbezogene cross-sektorale Regulierung für (bestimmte) im AI-Act definierte **KI-Systeme und -Modelle**	Technologieneutrale sektorale Anforderungen an Beaufsichtigte iZm der **Erbringung regulierter Tätigkeiten**	cross-sektorale Regulierung für Finanzunternehmen iZm der **Erbringung regulierter Tätigkeiten**
Ziele:	Grundrechte, Gesundheit, Sicherheit	Versichertenschutz, Finanzmarktstabilität	Aufrechterhaltung einer hohen digitalen operationalen Resilienz
Scope:	▪ **KI-Systeme** und -Modelle ▪ **Anbieter** (die KI-Systeme in der EU in Verkehr bringen o. in Betrieb nehmen) ▪ **Nutzer** von KI-Systemen innerhalb der EU inkl. natürlicher Personen	▪ Lebens- / Nichtlebensversicherung ▪ Rückversicherung	▪ **IKT-Assets** ▪ **IKT-Dienstleistungen**, dh digitale Dienste und Daten-dienste, die über **IKT-Systeme** dauerhaft bereitgestellt werden
Folge:	Sofern KI-Systeme / -Modelle in den Anwendungsbereich des AIA fallen, sind (zusätzliche) regulatorische Anforderungen zu beachten => umfassende KI-Governance, die die Risiken über den gesamten Lebenszyklus hinweg beherrschbar und transparent macht (**risikobasierter Ansatz**)	▪ Allgemeine Anforderungen an Governance inkl. Risikomanagement ▪ Vertriebsvorschriften der IDD	umfassende Vorgaben für das IKT-Risiko-Management
Auslagerung:	Verwendung **externer KI-Systeme** kann zu einer Auslagerung gemäß § 109 VAG führen		

VERWENDET MEIN UNTERNEHMEN „AI" ?

AI-Definition (Art 3 (1) iVm ErwGr 12 AIA)	**EK-Leitlinien zur Definition eines KI-Systems** C(2025) 5053 final
▪ **Maschinengestütztes System**	▪ Der Begriff „maschinengestützt" bezieht sich auf die Tatsache, dass KI-Systeme mithilfe von Maschinen entwickelt und auf Maschinen betrieben werden.
▪ **Autonomie**	▪ „mit verschiedenen Graden der Autonomie" bedeutet, dass KI-Systeme **bis zu einem gewissen Grad unabhängig von menschlichem Zutun agieren** können und in der Lage sind, ohne menschliches Eingreifen zu arbeiten. ➢ **Nicht umfasst** sind Systeme, die ausschließlich für den Betrieb unter vollständigem, manuellem Zutun und Eingreifen des Menschen konzipiert sind.
▪ **Anpassungsfähigkeit**	▪ „das nach seiner Betriebsaufnahme anpassungsfähig sein kann" bezieht sich auf die **Lernfähigkeit, durch die sich das Verhalten des KI-Systems während seiner Verwendung verändern kann**. Das neue Verhalten des angepassten KI-Systems kann bei denselben Eingaben gegenüber dem vorherigen KI-System zu anderen Ausgaben führen.
▪ **Ziele des KI-Systems**	▪ „für explizite oder implizite Ziele ableitet" bedeutet, dass KI-Systeme so ausgelegt sind, dass sie mit einem oder mehreren expliziten oder impliziten Zielen betrieben werden können. Diese Ziele können sich unter Umständen vom Zweck (= nach außen gerichtetem Kontext, in welchem das KI-System eingesetzt werden soll) unterscheiden.
▪ **Ableiten**	▪ Diese Fähigkeit bezieht sich auf 1) den Prozess der **Erzeugung von Ausgaben** (zB Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen), die physische und digitale Umgebungen beeinflussen können sowie auf 2) die Fähigkeit der **Ableitung von Modellen und/oder Algorithmen** aus Eingaben oder Daten. Die Fähigkeit eines KI-Systems, abzuleiten, geht über die einfache Datenverarbeitung hinaus, indem Lern-, Schlussfolgerungs- und Modellierungsprozesse ermöglicht werden. ➢ **Nicht umfasst** sind 1) herkömmliche Softwaresysteme und Programmierungsansätze; 2) Systeme, die ausschließlich auf von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen.

PRAKTIKEN AUßERHALB DES ANWENDUNGSBEREICHS

Systeme zur Verbesserung der mathematischen Optimierung

- Systeme zur Verbesserung der mathematischen Optimierung oder zur Beschleunigung und Annäherung traditioneller, gängiger Optimierungsmethoden wie lineare oder logistische Regressionsmethoden fallen nicht in den Anwendungsbereich. Obwohl solche Modelle ableiten können, gehen sie dennoch nicht über die „grundlegende Datenverarbeitung“ hinaus.
- Diese Systeme können zwar automatische Selbstanpassungen vornehmen, diese Anpassungen zielen aber darauf ab, die Funktionsweise der Systeme zu optimieren, indem ihre Rechenleistung verbessert wird, anstatt zB intelligente Anpassungen ihrer Entscheidungsmodelle zu ermöglichen.

Einfache Datenverarbeitung

- folgt vorab festgelegten, expliziten Anweisungen oder Vorgängen, um Aufgaben auf der Grundlage manueller Eingaben oder Regeln auszuführen, ohne dass in irgendeiner Phase des Systemlebenszyklus Lern-, Schlussfolgerungs- und Modellierungsprozesse ablaufen. Sie arbeiten auf der Grundlage fester, vom Menschen programmierter Regeln, ohne KI-Techniken wie maschinelles Lernen oder logikgestützte Ableitungen einzusetzen, um damit Ausgaben zu erzeugen (zB Datenbankverwaltungssysteme, die zur Sortierung oder Filterung von Daten verwendet werden (zB „alle Kunden, die im letzten Monat ein bestimmtes Produkt erworben haben“), Standard-Tabellenkalkulationsanwendungen.
- Softwaresystem, das statistische Techniken auf Meinungsumfragen oder Umfragedaten anwendet, um deren Validität, Zuverlässigkeit, Korrelation und statistische Signifikanz zu ermitteln

Auf klassische Heuristik gestützte Systeme

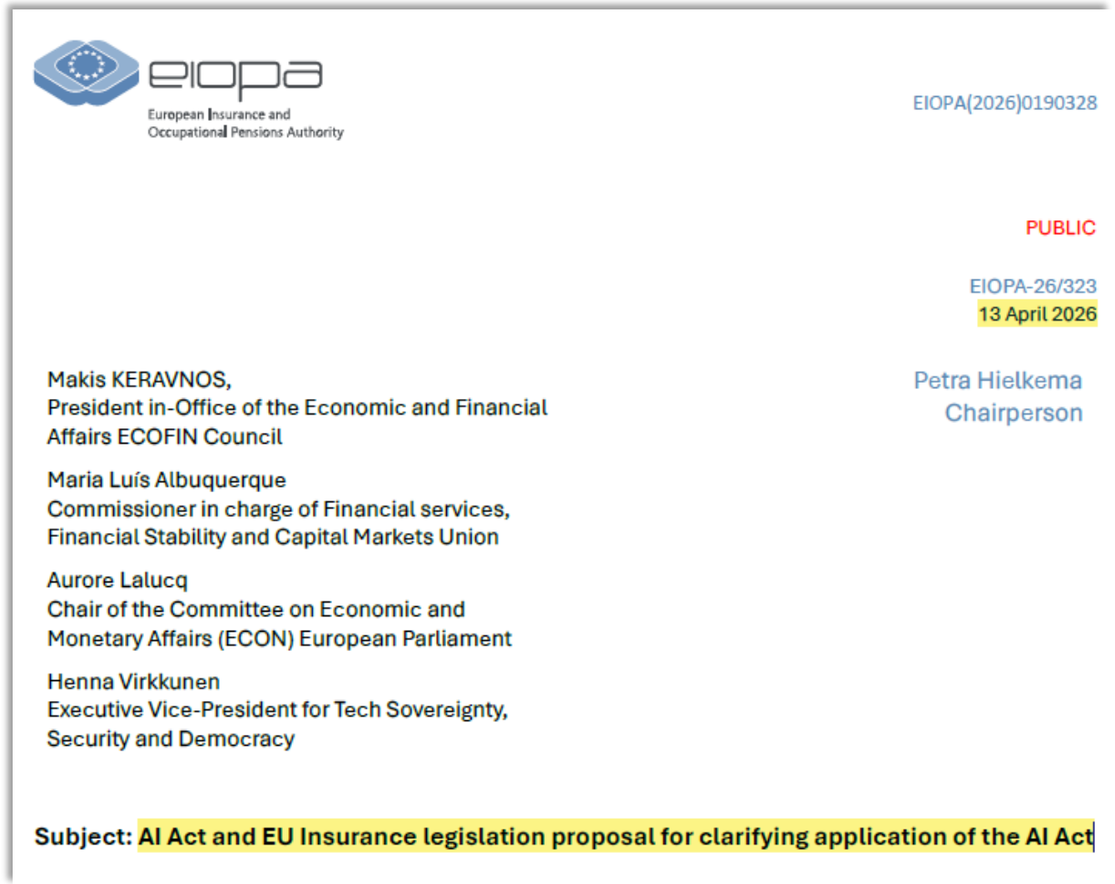
- Problemlösungstechniken, die auf erfahrungsgestützten Methoden beruhen und mit deren Hilfe effizient Näherungslösungen gefunden werden. In der Regel werden heuristische Techniken beim Programmieren eingesetzt, wenn die Suche nach einer genauen Lösung aus Zeit- oder Ressourcenzwängen nicht praktikabel ist. Die klassische Heuristik umfasst üblicherweise regelgestützte Ansätze, Mustererkennung oder Strategien des systematischen Ausprobierens anstelle eines datengesteuerten Lernens. Im Gegensatz zu modernen Systemen des maschinellen Lernens, die ihre Modelle auf der Grundlage von Beziehungen zwischen Eingaben und Ausgaben anpassen, wenden klassische heuristische Systeme vordefinierte Regeln oder Algorithmen an, um Lösungen abzuleiten.

Einfache Vorhersagesysteme

- Alle maschinengestützten Systeme, deren Leistung durch eine grundlegende statistische Lernregel erreicht werden kann, könnten zwar technisch so eingestuft werden, dass sie auf maschinellem Lernen beruhen, sie fallen aber aufgrund ihrer Leistung nicht in den Anwendungsbereich.
- Bei Finanzprognosen (einfaches Benchmarking) können solche maschinengestützten Systeme zur Vorhersage künftiger Aktienkurse verwendet werden, indem eine Mittelwert-Schätzfunktion verwendet wird, um eine Basisvorhersage zu machen (die z. B. stets den historischen Durchschnittspreis vorhersagt).
- Statische Schätzsysteme, wie zB ein System für die Reaktionszeit bei der Kundenbetreuung, das auf einer statischen Schätzung zur Vorhersage der mittleren Zeit zur Lösung des Problems anhand früherer Daten und trivialer Variablen beruht, wie zB Nachfrageprognosen für ein Ladengeschäft.

EK-Leitlinien zur Definition eines Systems der KI, C(2025) 5053)

GENERALISIERTE LINEARE MODELLE (?)



eiopa
European Insurance and Occupational Pensions Authority

EIOPA(2026)0190328

PUBLIC

EIOPA-26/323
13 April 2026

Petra Hielkema
Chairperson

Makis KERAVNOS,
President in-Office of the Economic and Financial Affairs ECOFIN Council

Maria Luís Albuquerque
Commissioner in charge of Financial services, Financial Stability and Capital Markets Union

Aurore Lalucq
Chair of the Committee on Economic and Monetary Affairs (ECON) European Parliament

Henna Virkkunen
Executive Vice-President for Tech Sovereignty, Security and Democracy

Subject: AI Act and EU Insurance legislation proposal for clarifying application of the AI Act

Further clarification on the scope of application of the AI Act would be appropriate. Particularly by expressly excluding generalised linear models (GLMs), for instance linear or logistic regressions, from the scope of the AI Act's definition of an AI system, or at least from the scope of high-risk AI systems, when used for risk assessment and pricing in life and health insurance, given their high degree of explainability and transparency. As suggested by the European Central Bank[5], such a clarification could be reflected in the AI Act, and/or the Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689.

The use of GLMs, including linear and logistic regression, as well as generalised additive models (GAMs), has been widely established in the insurance industry since at least the 1980s, particularly in the context of risk assessment and pricing. While most prominent in non-life insurance, such models are also used in life and health insurance alongside other actuarial techniques.[6]

Both undertakings and insurance supervisors have extensive experience with these models and a sound understanding of the associated risks, including those relating to the protection of consumers.

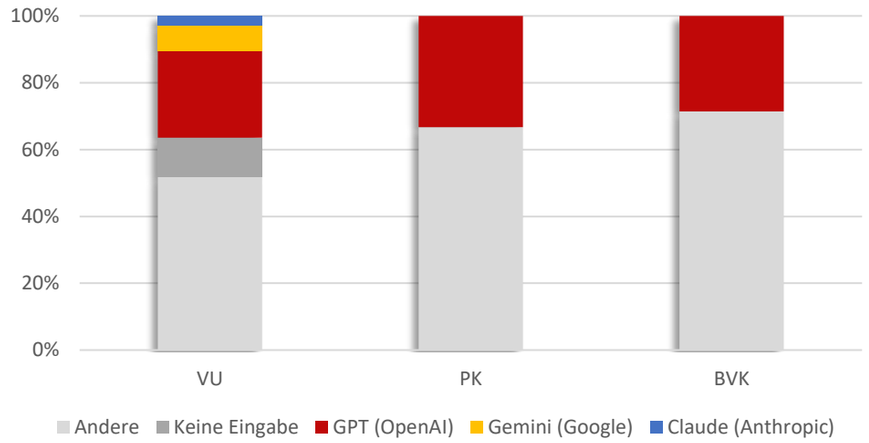
The operation of these models is generally based on a limited and stable set of parameters whose influence on outcomes can be directly interpreted and assessed using well-established statistical methods. As a result, these models are generally transparent and interpretable, and do not in themselves exhibit the 'black-box' characteristics that underpin the AI Act's enhanced governance and risk-mitigation requirements, which are primarily designed to address the challenges posed by complex, non-linear, self-learning systems, for which more specific governance concerns need taking into account.

Q, EIOPA, Letter to EU institutions on AI Act and EU Insurance legislation proposal for clarifying application of the AI Act)

AI-SYSTEME: IN-HOUSE ENTWICKLUNG

→ 6 VU, 1 PK UND 2 BVK FUNGIEREN AUCH ALS **„ANBIETER“** EINES AI-SYSTEMS
INSGESAMT 38 AI-SYSTEME WURDEN VON VU VOLLSTÄNDIG / HAUPTSÄCHLICH **IN-HOUSE ENTWICKELT**

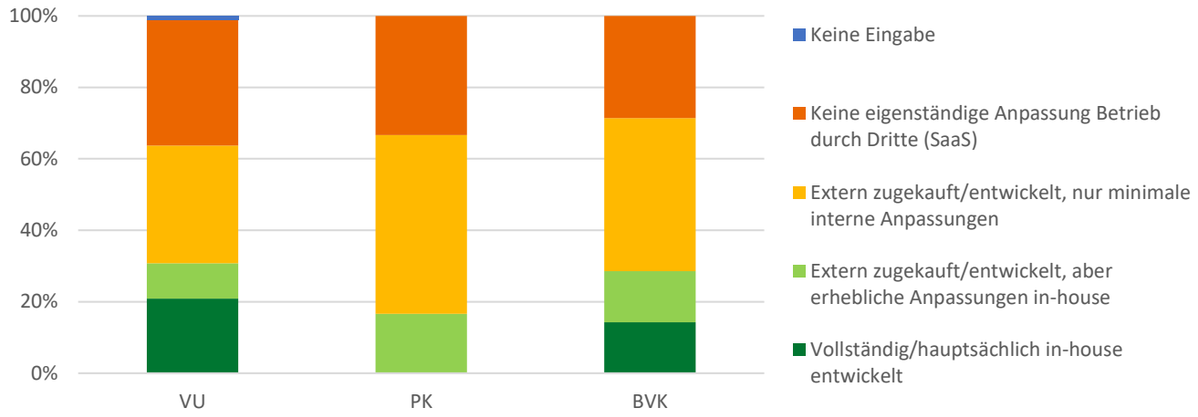
Auf welchem **KI-Modell** basiert das System?



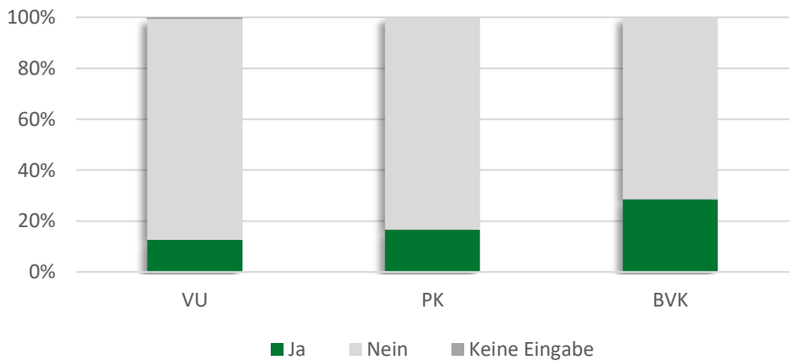
Mathematisches oder statistisches Modell, das die Grundlage für ein KI-System bildet

(47 von 182 Anwendungsfälle basieren bei VU auf GPT / Open AI)

Grad der **internen Systemanpassung**



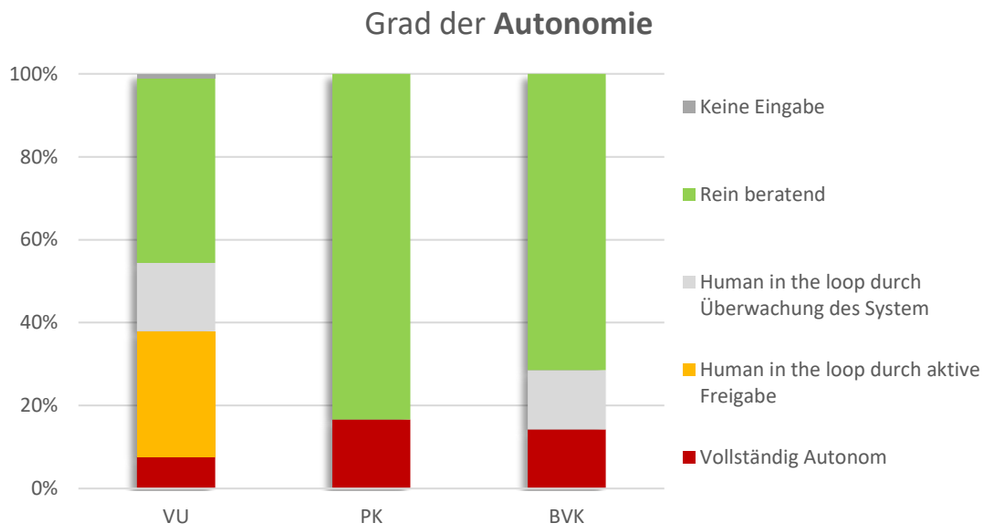
Fungiert das Unternehmen als **Anbieter**?

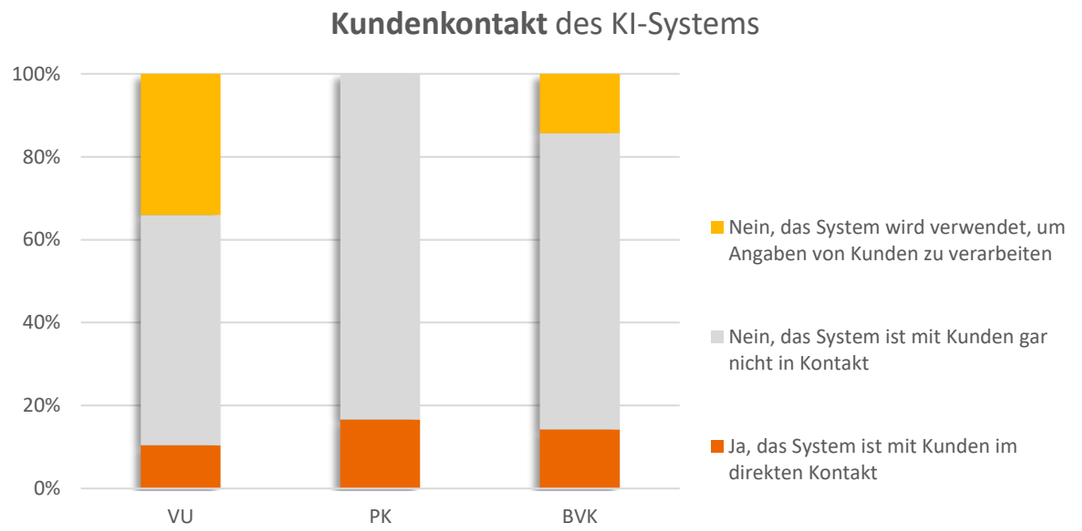


Q, FMA-Erhebung, April 2026: Marktabdeckung von 100% in allen Sektoren (VU/PK/BVK)

AI-SYSTEME: GRAD DER AUTONOMIE

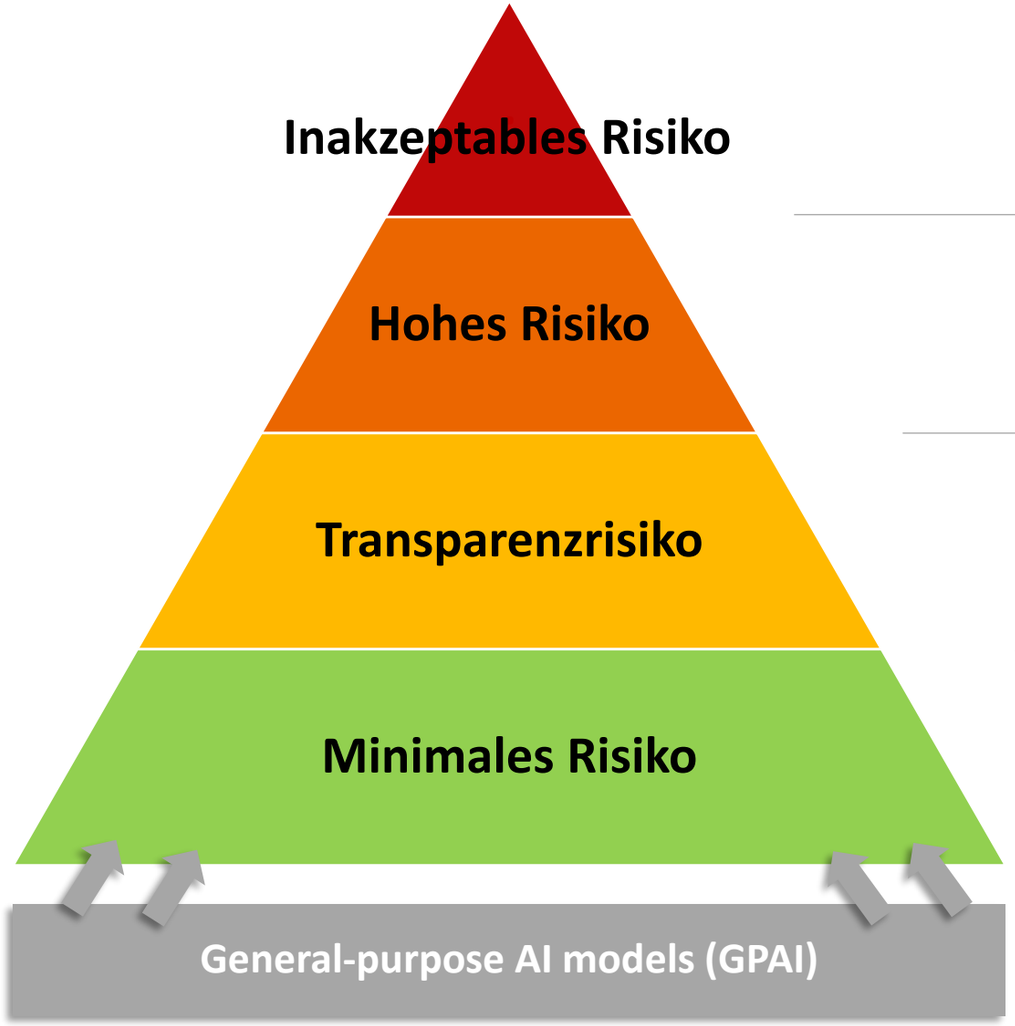
➔ ÜBER ALLE SEKTOREN HINWEG SIND DIE MEISTEN AI-SYSTEME **REIN BERATEND** TÄTIG;
VU SETZEN **HUMAN IN THE LOOP** BEI 55 AI-SYSTEMEN DURCH AKTIVE FREIGABE; BEI 30 DURCH ÜBERWACHUNG + GGF. AUSSTOPPUNG EIN





Q, FMA-Erhebung, April 2026: Marktabdeckung von 100% in allen Sektoren (VU/PK/BVK)

WELCHE ART VON RISIKO STELLT ES DAR?



- **Ausnutzung von Verwundbarkeiten** in Bezug auf Alter, Behinderung, ...
- **Soziales Scoring**
- **Biometrische Kategorisierung** zur Ableitung der Rasse, politischer Meinungen, religiöser Überzeugungen, …

→ **Verbotene KI-Praktiken**

- AI systems intended to be used for risk assessment and pricing in relation to natural persons im Fall der **Lebens-** und **Krankenversicherung** (Annex III, 5 c).

→ **Konformitätsbewertung Gebrauchsanweisung/ Menschliche Aufsicht / Folgenabschätzung in Bezug auf die Grundrechte**

- **Risiken von Identitätsdiebstahl, Manipulation ,** Fehlinformationen oder Täuschung (z. B. Chatbots, Deep Fakes, KI-generierte Inhalte...)

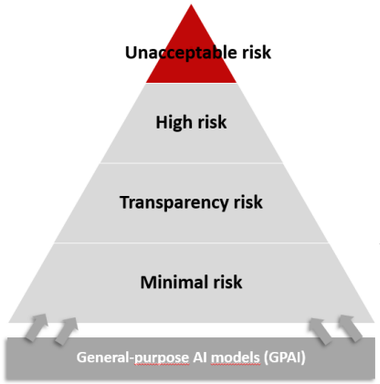
→ **Information von natürlichen Personen, dass sie mit einem KI-System interagieren**

- Die Mehrzahl der KI-Systeme (z.B. Spamfilter) kann im Rahmen der bestehenden Regulierung ohne spezifische rechtliche Verpflichtungen entwickelt und eingesetzt werden. Freiwillig können sich die Anbieter dieser Systeme freiwilligen Verhaltenskodizes anschließen.

→ **KI-Kompetenz der Personen, die mit KI-Systemen befasst sind**

- GPAI models → **Transparenz**
- GPAI models with systemic risks (= GPAI mit “hohen Wirkungsfähigkeiten”) → **Transparenz, Risiko-bewertung und -mitigation**

WELCHE KI-PRAKTIKEN SIND „VERBOTEN“?



Definition verbotener KI-Praktiken (Art 5 Abs 1 iVm ErwGr 31 AIA)	Offene Fragen
▪ **Ausnutzung der Verwundbarkeit** natürlicher Personen oder einer bestimmten Personengruppe aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation mit dem Ziel oder der Wirkung, das Verhalten dieser Person oder einer dieser Gruppe angehörenden Person in einer Weise wesentlich zu verzerren, die dieser Person oder einer anderen Person erheblichen Schaden zufügt oder nach vernünftigem Ermessen wahrscheinlich zufügen wird.	▪ Versicherungsunternehmen verwenden für Underwriting-, Pricing- und Schadenmanagementprozesse häufig Daten aus verschiedenen Quellen. ▪ Fällt die **Verwendung von Daten aus sozialen Medien als zusätzliche Information** zur Aufdeckung von Betrug bei der Schadenbearbeitung oder beim Underwriting und bei der Preisgestaltung unter „verbotene Aktivitäten“? ▪ Das Verbot des Einsatzes von KI-Systemen in Bezug auf die biometrische Kategorisierung könnte die Innovation in bestimmten Versicherungssparten einschränken.
▪ **Social scoring** (= KI-Systeme, die natürliche Personen oder Gruppen von Personen auf der Grundlage mehrerer Datenpunkte bewerten oder klassifizieren, die sich auf ihr Sozialverhalten in verschiedenen Kontexten beziehen oder über bestimmte Zeiträume bekannte, abgeleitete oder vorhergesagte Persönlichkeitsmerkmale aufweisen. Der von solchen KI-Systemen erhaltene Social Score kann zu einer nachteiligen oder ungünstigen Behandlung dieser Person in sozialen Kontexten führen, die nichts mit dem Kontext zu tun haben, in dem die Daten ursprünglich generiert oder erhoben wurden).	
▪ **Biometrische Kategorisierung** zur Ableitung der Rasse, politischer Meinungen, religiöser Überzeugungen, sexueller Orientierung	

?

Die Verbote hinsichtlich der Verwendung bestimmter Daten wurden tw. in den EK-Leitlinien präzisiert.

KI-PRAKTIKEN: ZULÄSSIG / VERBOTEN ?

Fall 1:

- Ein Versicherungsunternehmen A holt bei einer Bank B **Auskünfte über Ausgaben und sonstige Finanzinformationen** ein, die
  - in keinem Zusammenhang mit der Feststellung der Eignung der Bewerber für eine Lebensversicherung stehen und
  - zur Festlegung der Höhe der für eine solche Versicherung zu zahlenden Prämie herangezogen werden.
- Ein **KI-System analysiert diese Informationen** und **empfiehlt** auf dieser Grundlage,
  - einen Vertrag abzulehnen oder
  - für eine bestimmte Einzelperson oder Kundengruppe höhere Lebensversicherungsprämien festzusetzen.

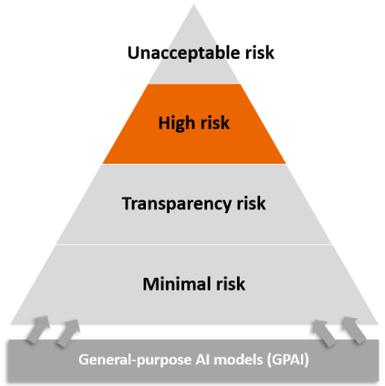
EK-Leitlinien zu verbotenen KI-Praktiken, C(2025) 5052:

Fall 2:

- Ein Versicherungsunternehmen B bietet telematikgestützte Versicherungstarife für das hochriskante Fahrverhalten eines Versicherungsnehmers an und **erhebt** über Telematikgeräte **Informationen, die zeigen, dass ein Fahrer zu schnell fährt oder keine sichere Fahrweise pflegt.**
- Der Versicherer nutzt dann diese Daten dahingehend, dass sie
  - zu einer Erhöhung der Versicherungsprämien für den betreffenden Versicherungsnehmer führen,
  - was mit der durch dieses Fahrverhalten erhöhten Unfallgefahr begründet wird, sofern die Erhöhung der Versicherungsprämie in einem angemessenen Verhältnis zum risikobehafteten Verhalten des Fahrers steht.

Werden sektorspezifische Rechtsvorschriften eingehalten (zB im Bereich der Bonitätsbewertung, der Bekämpfung von Geldwäsche), in denen festgelegt ist, welche Art von Daten für den spezifischen legitimen Zweck der Bewertung als relevant und erforderlich verwendet werden können, und mit denen sichergestellt wird, dass die Behandlung gerechtfertigt ist und in einem angemessenen Verhältnis zum sozialen Verhalten steht, kann somit sichergestellt werden, dass die betreffende KI-Praxis nicht in den Anwendungsbereich des Verbots nach Art. 5 Abs. 1 lit. c fällt.

WELCHE KI-SYSTEME STELLEN EIN „HOHES RISIKO“ DAR?



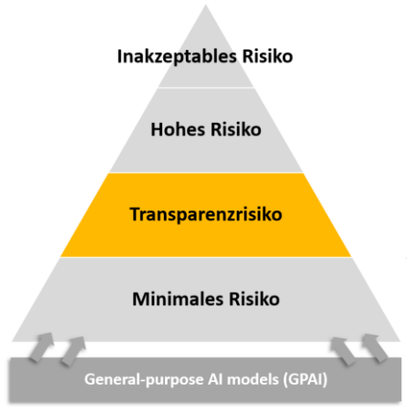
Ein und dasselbe KI-System kann mehreren Zwecken dienen, wobei einige als hochriskant eingestuft werden, andere nicht!
(zB Entwerfen eines E-Mails ⇔ Sammeln von Informationen und Generieren von Input im Underwriting-Prozess)

Definition von Hochrisiko-KI-Systemen (Art 6 iVm Annex III, 5 c und ErwGr 58 AIA)	**Offene Fragen**
▪ AI systems intended to be used for **risk assessment** and **pricing** ▪ in relation to natural persons in the case of **life and health insurance**	▪ Erfasst die Formulierung „Risikobewertung“ auch andere Prozesse als das Underwriting, d.h. das interne Risikomanagement und/oder die Berechnung versicherungstechnischer Rückstellungen? ▪ Gilt die Formulierung „bei Lebens- und Krankenversicherungen“ auch für Renten im Nichtlebensversicherungsgeschäft/Umgang mit Mischprodukten?
Nicht erfasst: 1) AI systems provided for by Union law for the purpose of **detecting fraud** in the offering of financial services 2) AI systems provided for by Union law for prudential purposes to calculate credit institutions’ and insurances undertakings’ **capital requirements** 3) AI systems listed in Annex III which “**do not pose a significant risk**” **EC** to amend the list of high-risk AI systems via **Delegated acts** (Art. 7 (1))	1) Die im ErwGr 58 für beide Sektoren erwähnte Ausnahme bzgl. “fraud detection” ist im Annex III explizit normiert nur für Banken (Annex III.5.b), nicht aber für den Versicherungsbereich (Annex III.5.c). 2) Erfasst diese Ausnahme KI-Systeme, die im internen Risikomanagement und/oder bei der Berechnung versicherungstechnischer Rückstellungen eingesetzt werden? 3) Unter welchen Voraussetzungen ist ein KI-System, das dazu bestimmt ist, eine enge Prozessaufgabe zu erfüllen, davon ausgenommen? (Profiling bleibt immer erfasst!)

?

In den EK-Leitlinien und/oder delegierten Rechtsakten zu klären

WELCHE KI-SYSTEME STELLEN EIN „TRANSPARENZRISIKO“ DAR?



Transparenzpflichten
(Art 50 iVm ErwGr 132ff AIA)

- Die Anbieter stellen sicher, dass **KI-Systeme, die für die direkte Interaktion mit natürlichen Personen bestimmt** sind, so konzipiert und entwickelt werden, dass

  ➢ die betreffenden natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren,

  ➢ es sei denn, dies ist aus Sicht einer angemessen informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich.

Offene Fragen

- **AI Chatbots als Versicherungsvermittler iSd IDD (?)**
- Im Gegensatz zu traditionellen Vertriebskanälen sind öffentlich zugängliche AI-Chatbots (zB Chat-GPT) nicht an vordefinierte Formulare und Fragekataloge gebunden.
- Wenn sie entsprechend aufgefordert werden, können AI-Chatbots in mehreren Interaktionen basierend auf den bereitgestellten persönlichen Daten und den angegebenen finanziellen Verhältnissen

  a) detaillierte Angebote für bestimmte Versicherungsprodukte sowie

  b) ein angemessenes Deckungsniveau empfehlen.
- Diese Interaktion könnte einer persönlichen Beratung ähneln und die Entscheidung beeinflussen, ein bestimmtes Versicherungsprodukt zu kaufen (siehe EIOPA, Q&A 3407).

WELCHE **PFLICHTEN** HABE ICH ALS „BETREIBER“?

Die Pflichten hängen von der Risikokategorie des verwendeten KI-Systems ab:

	Hohes Risiko	Transparenzrisiko	Minimales Risiko
KI-Kompetenz	Art 4	Art 4	Art 4
Offenlegung bezüglich des Einsatzes eines KI-Systems	Art 26 (11)	Art 50 (3), (4)	
Verwendung in Übereinstimmung mit der Gebrauchsanweisung	Art 26 (1), (3), (4)		
Menschliche Aufsicht	Art 26 (2)		
Überwachung des Betriebs des KI-Systems auf der Grundlage der Gebrauchsanweisung	Art 26 (5)		
Meldung von schwerwiegenden Störungen	Art 26 (5), Art 73		
Aufbewahrung der Protokolle, die automatisch vom Hochrisiko-KI-System generiert werden	Art 26 (6)		
Datenschutz-Folgenabschätzung, sofern relevant	Art 26 (9)		
Zusammenarbeit mit den jeweils zuständigen Behörden	Art 26 (12)		
Recht auf Erläuterung der individuellen Entscheidungsfindung	Art 86 (1)		
Unterrichtung der Arbeitnehmervertreter und der betroffenen Arbeitnehmer	Art 26 (7)		
Antrag zur nachträglichen biometrischen Fernidentifizierung	Art 26 (10)		
Folgenabschätzung zu den Grundrechten	Art 27		

Vorschriften zur KI-Kompetenz anwedbar seit **2 Februar 2025** (=> Anbieter und Betreiber von KI-Systemen stellen so gut wie möglich sicher, dass ihr Personal und andere Personen, die in ihrem Namen mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, in ausreichendem Umfang über KI-Kenntnisse verfügen.)

AI-ACT: KI-KOMPETENZ

→ WIE IST DIE KI-KOMPETENZ NACHZUWEISEN (?)

- Inwieweit ist für unterschiedliche KI-Systeme die in Art 4 KI-VO geforderte KI-Kompetenz nachzuweisen?
  - a) Bedarf es für jedes System einen Nachweis, dass speziell auf dieses System geschult wurde, oder
  - b) ist entscheidend welche Art von Künstlicher Intelligenz dem System unterliegt?

Art. 4 KI-VO verlangt

- **keine Pflicht zur „Zertifizierung“ bzw. zur „Messung“ der KI-Kenntnisse** der Mitarbeitenden
- **keine formale, für jedes einzelne KI-System getrennte Schulung**

- Gefordert werden vielmehr „angemessene Maßnahmen“, die sicherstellen, dass beteiligte Personen über **ausreichende Kompetenz** verfügen. Dies kann erreicht werden durch
  1) **systemübergreifende KI-Trainings** (zB Funktionsweise von ML-Modellen, Risiken, Bias, Datenschutz),
  2) **rollenbezogene Schulungen** (zB für Nutzer von Hochrisiko-KI),
  3) **produktspezifische Anweisungen**.

- **Entscheidend ist der Kontext**, dh:
  - wer die KI-Systeme betreibt oder nutzt (zB Anbieter oder Betreiber),
  - in welchem Umfeld oder Szenario die KI-Systeme eingesetzt werden,
  - welche technischen Kenntnisse, Erfahrungen, Aus-/Weiterbildungen die betreffenden Personen mitbringen,
  - welche Personen oder Personengruppen von der Nutzung der KI-Systeme betroffen sind.

➢ **Je höher das Risiko des KI-Systems, desto spezifischer müssen Schulungsmaßnahmen ausfallen.**

SEKTORALE VORGABEN: KI-GOVERNANCE

➔ DER VERANTWORTUNGSVOLLE EINSATZ VON KI-SYSTEMEN KANN NICHT DURCH EINE EIGENSTÄNDIGE MAßNAHME ERREICHT WERDEN!

Fairness and ethics

- Article 17 of the IDD stipulates that insurance distributors shall always **act honestly, fairly and professionally** in accordance with the best interests of their customers. EIOPA's 2023 Supervisory Statement on Differential Pricing Practices outlines certain pricing practices that are not considered compliant with that rule.

EIOPA-Opinion on AI governance and risk management

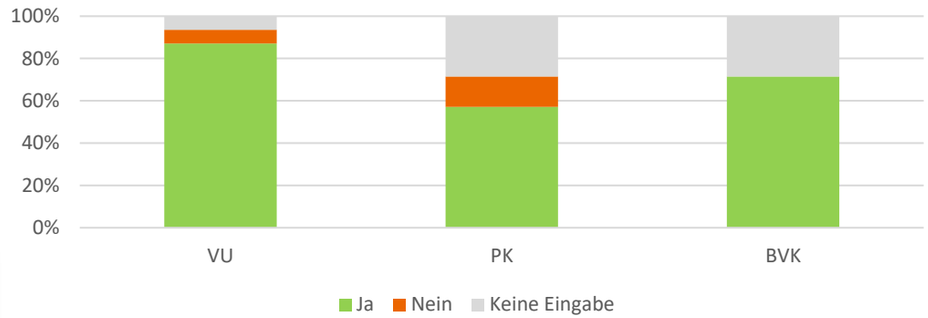
Data governance

- **Data governance policy** for AI systems
- The data used to train and test the AI system should be complete (e.g. sufficient historical information), accurate (e.g. no material errors) and appropriate (e.g. consistent with the purposes for which it is to be used). Any limitations of data in this regard should be duly documented and addressed. In particular, undertakings should make reasonable efforts to remove biases in the data in line with the undertaking's policy.

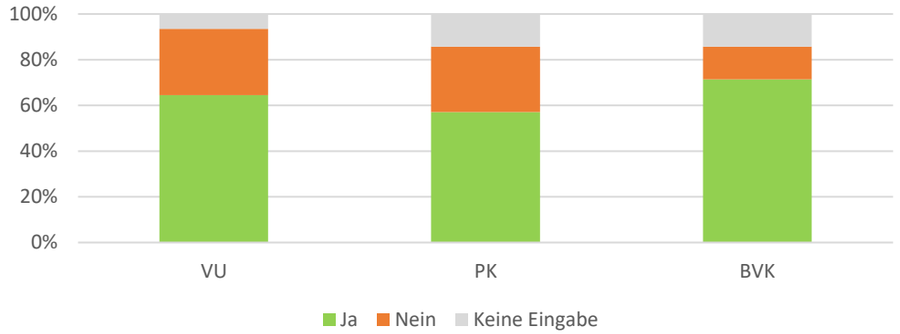
Documentation and record keeping

- appropriate records of the **training and testing data** and the **modelling methodologies** to enable their reproducibility and traceability

Konkrete Regeln / **Policies** für KI-Nutzung?



Register / zentrale Liste aller eingesetzten KI-Anwendungen?



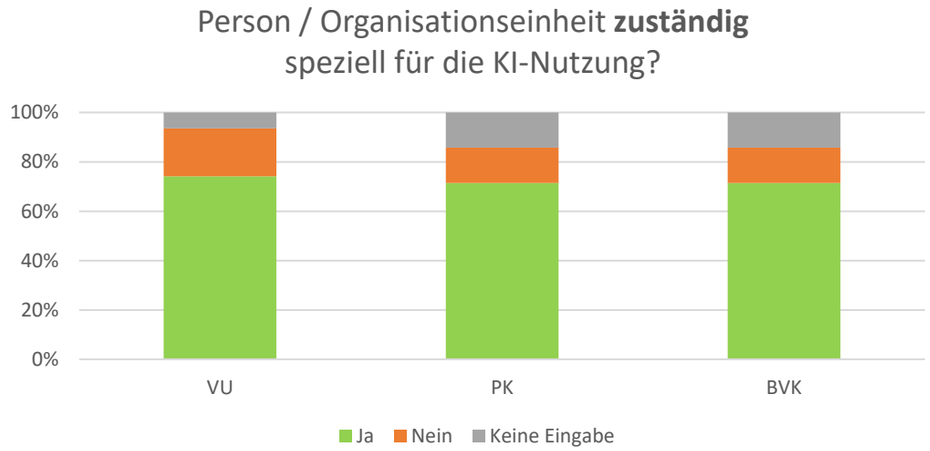
Q, FMA-Erhebung, April 2026: Marktabdeckung von 100% in allen Sektoren (VU/PK/BVK)

SEKTORALE REGELN: KI-GOVERNANCE

➔ DER VERANTWORTUNGSVOLLE EINSATZ VON KI-SYSTEMEN KANN NICHT DURCH EINE EIGENSTÄNDIGE MAßNAHME ERREICHT WERDEN!

Human oversight

- **Vorstand:** overall use of AI systems within the organization + need to have sufficient knowledge of how AI systems are used in their organisation and the potential risks.
- **Compliance-Funktion + Interne Revision:** verify that the use of AI systems within the organisation is compliant with all applicable laws and regulations
- **Aktuarielle Funktion:** controls on AI systems that fall under its responsibilities



Q, FMA-Erhebung, April 2026: Marktabdeckung von 100% in allen Sektoren (VU/PK/BVK)

Transparency and explainability

- Following a risk-based and proportionate approach, undertakings should ensure that the outcomes of AI systems can be meaningfully explained. Different approaches can be used to this extent, such as

  a) using explainable AI algorithms instead of
  b) more opaque (“black box”) ones;
  c) using complex AI systems only for the purpose of challenging and fine-tuning traditional mathematical models;
  d) local and global model-agnostic explanatory tools (LIME or SHAP).

Accuracy, robustness and cybersecurity

- use metrics, including, where appropriate, fairness metrics, to measure the performance (accuracy, recall) adapted to the AI system

EIOPA-Opinion on AI governance and risk management

TO BE CONTINUED…

Anthropics neues KI-Modell Mythos: Zu gefährlich für die Öffentlichkeit

Anthropics neues KI-Modell Mythos soll so effektiv im Finden und Ausnutzen von Sicherheitslücken sein, dass es nur IT-Infrastruktur absichern soll.

08.04.2026, 07:03 Uhr

Von Martin Holland

Anthropic hat mit Mythos ein neues KI-Modell vorgestellt, das so gefährlich sein soll, dass es nicht öffentlich gemacht werden soll. Stattdessen soll Claude Mythos Preview im Rahmen einer Initiative namens Project Glasswing zuerst ausschließlich einer Reihe von Firmen zur Verfügung gestellt werden, die an IT-Sicherheit arbeiten. Die sollen die KI-Technik nutzen, um die „kritischste Software der Welt“ abzusichern. Das KI-Modell habe bereits tausende hochriskante Zero-Day-Lücken identifiziert, begründet Anthropic den Schritt. Solche seien in allen großen Betriebssystemen und jedem Internetbrowser, aber auch in zahlreicher anderer Software entdeckt worden. Vor allem sei Mythos Preview deutlich häufiger in der Lage, einen funktionierenden Exploit zu entwickeln.

Jahrzehntealte Lücken identifiziert

Als Beispiel listet Anthropic etwa eine seit 27 Jahren übersehene Lücke in OpenBSD auf, über die Angreifer ein Gerät aus der Ferne zum Absturz bringen könnten, „indem sie sich nur damit verbinden“. Auch von einer 16 Jahre alten Lücke in FFmpeg ist da die Rede, die bei fünf Millionen automatischen Scans mit speziellen Suchwerkzeugen nicht identifiziert worden sei. Zudem sei das Modell in der Lage gewesen, eine Reihe von bislang unbekannten Lücken im Linux-Kernel zusammenzuführen und daraus eine Attacke zu entwickeln, die es einem Angreifer ermöglichen würde, als normaler User die komplette Kontrolle über einen Rechner zu erlangen. Diese und andere Lücken seien den jeweils Verantwortlichen gemeldet worden. Anthropic hat dazu einen Blogeintrag veröffentlicht.

Anthropics neues KI-Modell Mythos: Zu gefährlich für die Öffentlichkeit | heise online

Microsoft

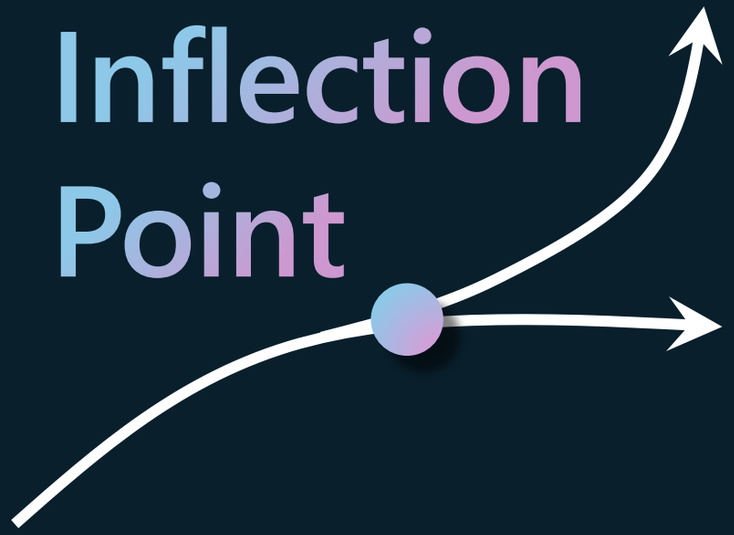
KI-Einsatz am Finanzmarkt: Do`s and Don'ts aus Microsoft-Sicht

FMA-Forum: Next level Tech@Insurance

Bastian Bahnemann
Financial Services Compliance & Business Development Lead, Microsoft Germany

23 April 2026

Inflection Point



a critical juncture or pivotal moment where established norms, practices, or technologies shift dramatically

Technology has created inflection points over time with significant impact on business and growth.

Previous Inflection Points

Personal Computing

New Levels of Productivity

The Internet

New Business Models

Mobile

New Channels, Products and Customer Engagement

Cloud

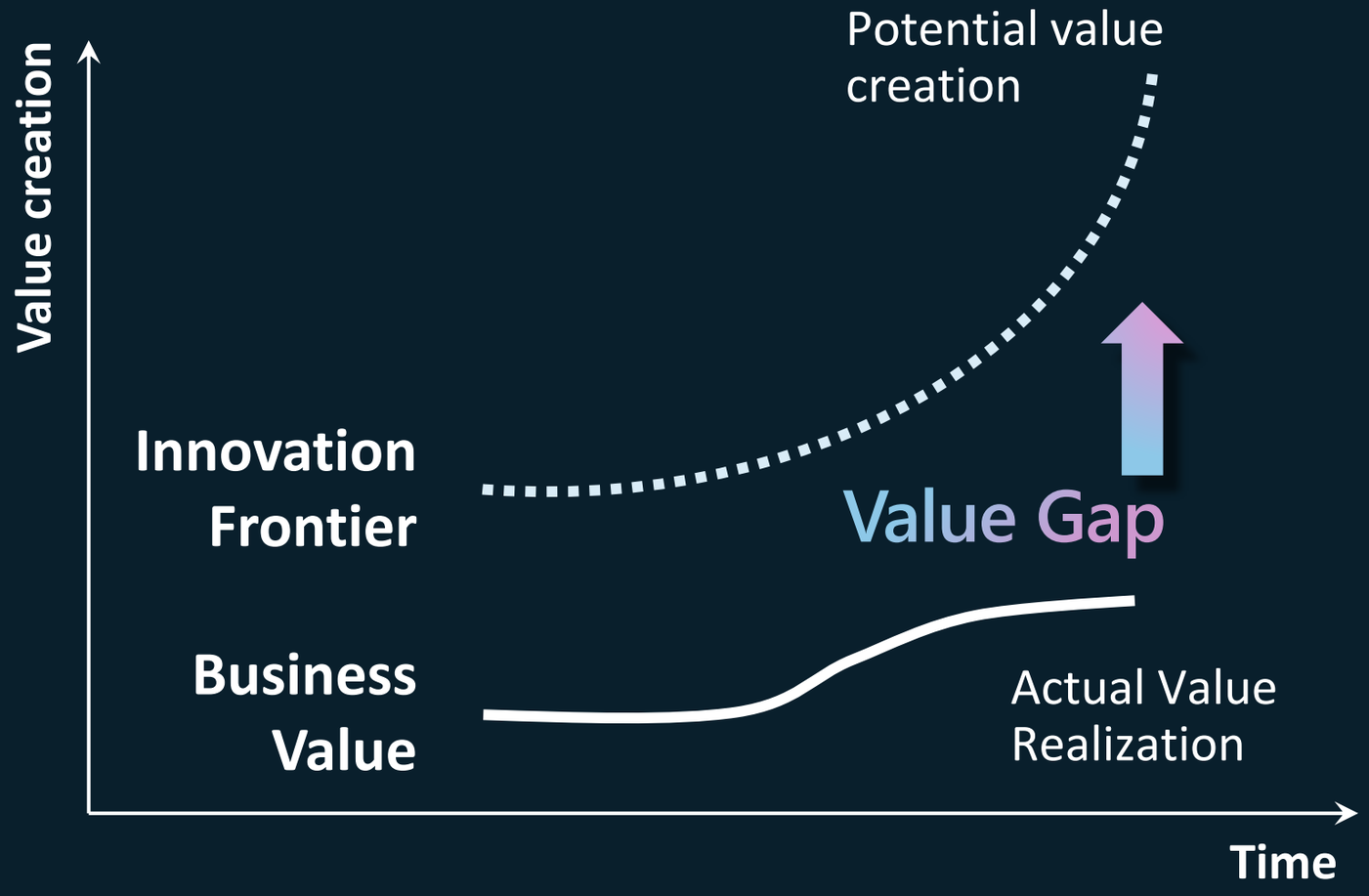
New Agility and Flexibility

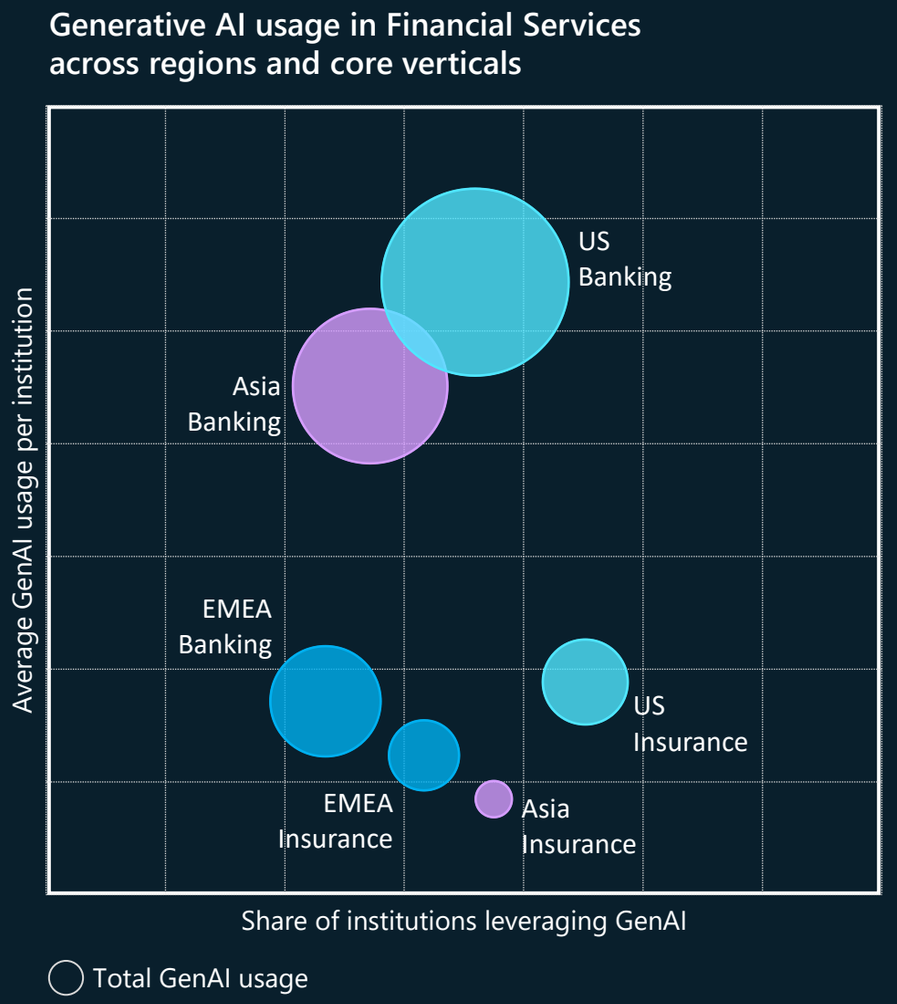
Today

Artificial Intelligence

New and Intelligent Products, Operations and Strategies

An inflection point typically creates a value gap between potential and realized value.





2025:

The Year the Frontier Firm Is Born…

2026:

The Year the Frontier Firm Goes Agentic…

When we say Frontier FSI Firm, we mean institutions that are AI native in their operating model - where real time data, agentic AI, and risk calibrated innovation are embedded in every customer journey and control process.

Microsoft

Artificial Intelligence is currently accelerating on its evolutionary journey.

Wave 1

Classical AI, Machine & Deep learning

- Comprehends natural language
- Analyzes (reasons) complex data for reasoning
- Adapts and enhances through feedback

Wave 2

Generative AI

- Able to generate original content
- Enhanced reasoning abilities (PhD level)
- Capable of multimodal functions

Wave 3

Agentic AI

- Pursues goals and adapting to dynamic environments
- Combines generative capabilities with real world interaction
- Multi-agent collaboration

Wave n

Artificial General Intelligence

- Generalized problem solving
- Learns autonomously with limited human intervention
- Operates autonomously & manages uncertainty

Journey to the Frontier Firm

Phase 1

Human with assistant

Every employee has an AI assistant that helps them work better and faster

Phase 2

Human-led agents

Agents join teams as “digital colleagues,” taking on specific tasks at human direction

Phase 3

Human-led, agent-operated

Humans set direction and agents run entire business processes and workflows, checking in as needed

AI Use Case roadmaps should address customer, business processes, innovation & employee dimensions.

Enrich employee experiences

Reinvent customer engagement

Reshape business processes

Bend the curve on innovation

AI Use Cases (selected examples only)

	TOP LINE GROWTH	COST REDUCTION	INNOVATION	ASSET UTILIZATION
ENRICH EMPLOYEE EXPERIENCES	• Personalized learning and coaching • Auto-generated personalized proposals	• Automated routine tasks • AI meeting summarization and task extraction	• AI-based collaboration • Skill-gap prediction	• Intelligent shift scheduling • Workspace & desk utilization optimization
REINVENT CUSTOMER ENGAGEMENT	• RM Augmentation • Long tail SMB coverage	• 24/7 customised customer support • Intelligent Pricing	• Customers build their own product with the help of AI • Intelligent products with situational awareness	• Inventory-aware personalized offers • Smart channel routing to balance load
RESHAPE BUSINESS PROCESSES	• Omni-Channel Optimization • Intelligent Pricing	• Increase productivity (e.g. SOP handling) • Compliance, risk assessment & fraud detection	• Sense & Response capabilities (reading weak signal early)	• Predictive maintenance for uptime • AI-driven capacity & workforce planning
BEND THE CURVE ON INNOVATION	• Time to Market for new products • New business models	• Design for No Operations	• Automated development spaces for experimentation	• Internal marketplace (matching assets to opportunity)

Six ways Agentic AI will change the fabric of business

Near Zero Cost of Software development

Hyper-Personalized Products and Human-Centric Marketing & UX

Real-Time Strategy Adaptation via Agentic Feedback Loops

Collapse of Organizational Silos

Security: Speed & sophistication of attacks and defenses

New Forms of Trust, Compliance & Governance

Microsoft Digital Defense Report 2025 – The threat landscape: Attacks

- **AI-powered attacks**: +200% increase in just 6 months
- **Identity**: Still the #1 Attack Surface
  - 97% of attacks = password spray / brute force. <3% advanced attacks (token theft, AiTM, MFA bypass).
  - Surge in identity infrastructure attacks (Entra, Okta)
- **Ransomware**: Persistent, Evolving Model
  - 82% of incidents involve data exfiltration without encryption
  - SMEs are prime targets
- **Fraud & Social Engineering**
  - AI-phishing CTR = 54% vs 12% (×4.5 increase)
  - ClickFix = primary access vector (47% of incidents)
- **BEC**: High-impact threat
  - 2% of the observed attacks but 21% of successful breaches
- **Cloud & AI**: Expanding Attack Surfaces
  - 58% crypto-mining, 21% credential theft, 15% persistent attack tools
  - Domain impersonation via GANs; AI twinning, prompt injection, A2A exploitation

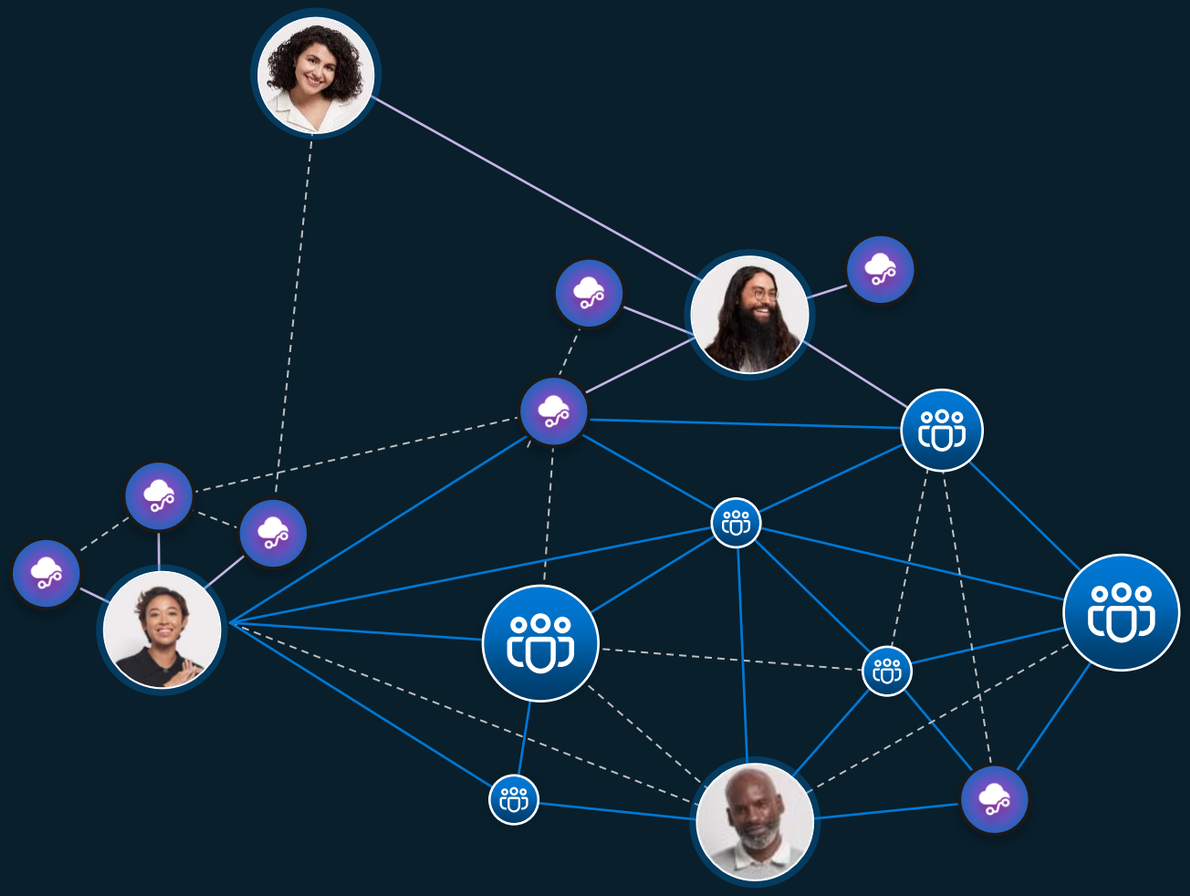
https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

An outside view – JPMC on Mythos/ Glasswing and what CISOs should to now

1. Run the Latest Software Versions
2. Manage Assets and Software Components with Reference Data
3. Build and Operate a Robust Vulnerability Management Program
4. Stress Test Incident Response and Resiliency Plans
5. Know Your Major SaaS and Outsourced Dependencies
6. Optimize Change Management for Speed
7. Aggressively Filter Outbound Traffic from Production Systems
8. Remove Standing Privileges from Employee Entitlements
9. Manage Remote Access and Segment Where Possible
10. Embed Security into the AI Development and Deployment Lifecycle

April 17, 2026: https://www.jpmorganchase.com/about/technology/blog/fortifying-the-enterprise-10-actions-to-take-now-for-ai-ready-cyber-resilience

AI Governance: Agents are joining the workforce



Can you discover and manage them?

Are they behaving appropriately?

Who & what are they sharing sensitive information with?

Are they well governed and audited?

Agents can introduce additional security challenges

Agent sprawl & resource access

82%

of leaders expect to use agents in the next 12–18 months to meet demand for workforce capacity[3]

Data oversharing & leaks

80%

of leaders cited leakage of sensitive data as their main concern[1]

Shadow AI, new AI threats & vulnerabilities

88%

of organizations are concerned about indirect prompt injection attacks[2]

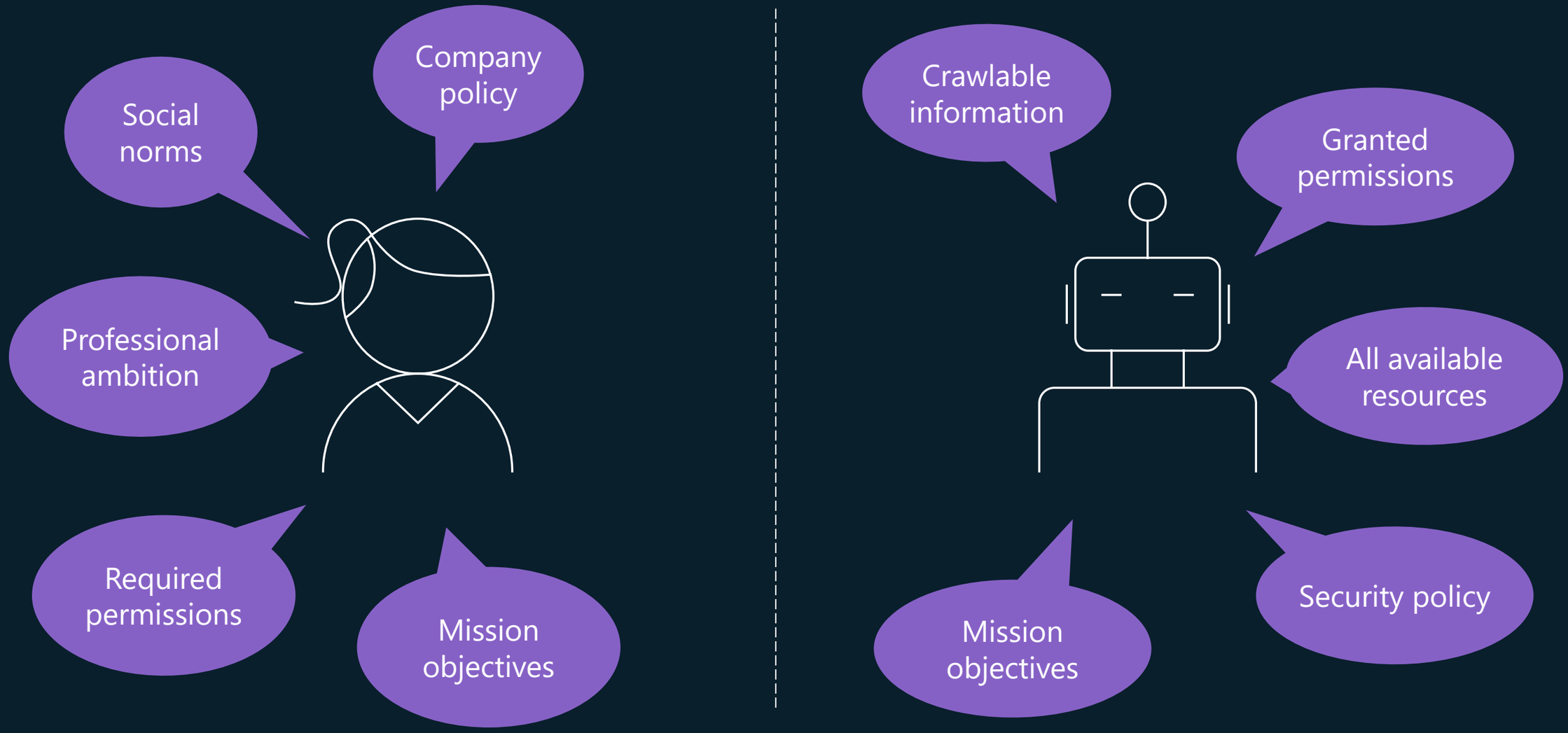
Regulatory compliance

55%

of leaders lack understanding of how AI is and will be regulated and are seeking guidance[1]

1. First Annual Generative AI study: Business Rewards vs. Security Risks, , Q3 2023, ISMG, N=400
2. How to Secure Custom-Built AI Agents, Gartner, 17 March 2025, Dionisio Zumerle, Jeremy D'Hoinne
3. Microsoft Work Trend Index Survey 2025

AI Governance: Humans vs. Agents – Behavioral Differences



Balancing Governance and Innovation

Agent Creator/Maker

- How can I **build a conversational agent** that will answer on my behalf?
- How can I build agents that can **drive efficiency and save efforts and costs** for our enterprise?

CISO

- How can I understand all my **data security risks**?
- How can I **discover** all agents and **protect my data** from external threats?
- How can I ensure agents have the right access to data and **prevent data exfiltration**?
- How can I **stay compliant with regulations**?

CIO

- How can I ensure that solutions people are building **follow guidelines?**
- How can I gain **visibility** to what is getting used?
- How can I get **experts to review agents** before they get shared broadly?
- How can I drive **cost efficiency and ROI?**

AI Governance & Security Roadmap

Where is your organization?

1 No formal governance

- AI experiments proceed without defined guidelines
- Little consideration of ethical, security or regulatory exposure issues yet
- Employees embracing unsanctioned AI tools (Shadow AI)
- No operational visibility (telemetry, monitoring, logging)

2 Basic guidelines

- Initial AI principles or guidelines are drafted to steer projects ethically
- Key risks (privacy, compliance) are identified for each pilot
- Security reviews start for data and models in pilot

3 Emerging governance

- Governance processes are put in place for all new Agentic AI deployments
- A cross-functional team (legal, security, compliance, AI leads) reviews AI projects
- Security and privacy controls are integrated into Agentic AI solutions
- Training on Responsible AI is introduced

4 Integrated governance

- Governance is built into the Agentic AI development lifecycle
- Incident response plans specific to AI systems identified
- Automated monitoring for security posture, not just model performance
- Dedicated bodies (AI ethics committee, risk officers) oversee enterprise AI use

5 Trusted & auditable AI

- The organization has industry-leading AI governance
- Responsible AI is part of the DNA
- AI systems are transparent, auditable, and meet high ethical standards
- Governance as a measurable business enabler (e.g., impact on trust, risk, business outcomes)

Key enablers

- Responsible AI Framework & Principles
- Governance
- AI Security & Risk Mitigation
- Data Privacy and Compliance

Financial services regulatory compliance can be discussed across four core areas – AI requirements too

Contractual compliance

Microsoft Business and Services Agreement (MBSA)

Enterprise Agreement (EA) & Enrollments (EA, EAS, SCE)

Enterprise Services Work Order (ESWO) & Statement of Work (SOW)/ Service Descriptions

Product Terms & Data Protection Addendum

Service Level Agreements (SLAs)

Financial Services Amendments

Microsoft's 'of the cloud' compliance

Service Trust Center (STP)
- Third-party audit reports and attestations
- Penetration test reports
- Whitepapers, compliance mappings
- Sub-contractor information

Enhanced Designated Engineering - Compliance for Microsoft Cloud (EDE CMC – old CPMC)
- Premium support service delivered through a dedicated team of subject matter experts
- Direct expert contact
- Risk and control mapping
- Proactive risk assurance
- Part of Microsoft Unified offering

Information & due-diligence support

Service health, issue & incident communication

Audit engagements
- Group audits (e.g. CCAG & GDV)
- Individual audit engagements

National Security Orders Report

Customers' technical compliance ('in the cloud')

Azure Well Architected Framework

Microsoft Security Adoption Framework (SAF)
- Microsoft Cybersecurity Reference Architectures (MCRA)

Microsoft Cloud Penetration Testing Rules of Engagement

Microsoft Defender for M365 & Microsoft Sentinel

Azure Security Center

Microsoft Purview & Microsoft Priva for Data Protection

Microsoft Information Protection

Microsoft Teams as Crisis Management Tools

Azure Site Recovery & Microsoft 365 Syntex Backup for Business Continuity

NEW: Agent 365 – The control plane for agents

Other compliance topics

- **Policies and procedures**
- **Risk and control framework**
- **Trainings**
- **Exit strategy & Business Continuity plans (BCM)**
- **Incident & crisis response**
- **Outsourcing governance**
- **Regulatory communication**
- **Approval processes**
- **Risk assessments & risk register**

Responsible AI is about People, Processes and Technology

1. Establish your own principles and embed Responsible AI into your Frontier COE
2. Put principles into practice with your AI Governance; build your Responsible AI Standard and Impact Assessment
3. Establish a Red Team to continuously uncover relevant risks
4. Cycle through ‘Measure and Mitigate’ steps using multiple tools and technologies
5. 24/7 Monitor your GenAI risks and quality while in production

All your agents can be enabled for Agent 365

Agent 365

Agent Registry and Access

Agent Visualization and Security

Agent Interoperability

+

Your Agent

Copilot Studio

Microsoft Foundry

Microsoft Agent Framework

Any AI Stack + Agent 365 SDK

Do`s and Don'ts aus Microsoft-Sicht

Do’s

- Make your agentic AI transformation a top-priority with clear roles and responsibilities (e.g. AI CCoE)
- Match your AI adoption approach with your individual firm’s culture and needs
- Enable experimentation & positive growth mindset

Don’ts

- Underestimate the need for communication, cultural & organizational evolution, as well as training & upskilling
- Wait to build responsible AI & AI agent governance frameworks (and update your existing policies & procedures)
- Wait until you identified the perfect first use- or business case

Microsoft AI Insurance Summit 2026:
The Frontier Insurance Goes Agentic

Fokus:	Agentic AI Use Cases & AI Governance & Security
Datum:	18 & 19 November 2026
Ort:	Köln
Anmeldung:	https://aka.ms/AIInsuranceSummit

Vielen Dank für Ihre Aufmerksamkeit

Bastian Bahnemann

Financial Services Compliance & Business Development Lead, Microsoft Germany

E-mail: bbahnemann@microsoft.com

FMA EVENT | WIEN | 2026

Künstliche Intelligenz im Finanzmarkt

Do's & Don'ts für den verantwortungsvollen KI-Einsatz – die IBM Perspektive

Michael Czachs
General Manager IBM Consulting Österreich
Senior Partner

AGENDA

Künstliche Intelligenz im Finanzmarkt – worüber wir heute sprechen

01	**Status Quo**	KI im europäischen Finanzmarkt – Zahlen, Trends, Realitätscheck
02	**Regulatorischer Rahmen**	EU AI Act, DORA, FMA-Aufsichtsschwerpunkte 2026
03	**Die 6 Do's**	Was Banken & Versicherer jetzt richtig machen müssen
04	**Die 6 Don'ts**	Die häufigsten Fehler – und wie sie vermieden werden
05	**IBM Ansatz**	watsonx, Agentic AI und verantwortungsvolle Skalierung
06	**Call to Action**	Was Vorstände in den nächsten 90 Tagen entscheiden sollten

KI ist kein Technologieprojekt.
KI ist eine Frage der Unternehmensführung.

88 % der Versicherungsvorstände in Europa sagen: KI entscheidet über die Wettbewerbsfähigkeit der nächsten drei Jahre. Gleichzeitig fehlt in vier von zehn Instituten das interne Know-how für eine verantwortungsvolle Skalierung.

Quelle: IBM Institute for Business Value – Insurance in the AI era, 2025

01 STATUS QUO

KI im europäischen Finanzmarkt – der Realitätscheck

40 %

des KI-Budgets fließen in Effizienz

Operative Kostensenkung dominiert – nicht Innovation

77 %

der Versicherer nutzen Agentic AI bis 2027

Schadenregulierung, Underwriting, Betrugserkennung

67 %

nur Traditional AI im Einsatz

GenAI (21 %) und Agentic AI (12 %) am Anfang

44 %

sehen Legacy-IT als KI-Blockierer

Technische Schulden bremsen jeden Skalierungsversuch

DIE ZENTRALE ERKENNTNIS

Der Finanzmarkt investiert massiv in KI – aber fast ausschließlich in Effizienz. Das Ergebnis: Hohe Automatisierung bei gleichzeitig niedrigem Kundenvertrauen und ungelösten Compliance-Risiken. Der Unterschied zwischen Gewinnern und Verlierern entscheidet sich nicht nur in der Technologie, sondern auch in der Governance.

Quelle: IBM IBV Insurance Study 2025 (N=1.500 Executives)

Die regulatorische Uhr tickt – drei Säulen, ein Stichtag

STICHTAG

2. August 2026

EU AI Act – Pflichten für Hochrisiko-KI-Systeme gelten vollständig. Sanktionen bis 35 Mio. € oder 7 % des globalen Umsatzes.

EU AI Act

Pricing, Underwriting und Schadenentscheidungen gelten als Hochrisiko-Systeme. Pflicht zur Grundrechte-Folgenabschätzung, CE-Kennzeichnung, technischer Dokumentation und menschlicher Aufsicht.

DORA

Digital Operational Resilience Act seit Januar 2025 in Kraft. IKT-Risikomanagement, Vorfallsmeldung und strikte Anforderungen an Drittanbieter – auch bei KI-Services und Cloud-Modellen.

FMA 2026

FMA-Aufsichtsschwerpunkt 2026: „Digitalisierung, KI und neue Geschäftsmodelle". Fokus auf faire und diskriminierungsfreie Schadenabwicklung bei KI-basierten Systemen in Versicherungen.

Quellen: EU-VO 2024/1689 (AI Act) · EU-VO 2022/2554 (DORA) · FMA „Fakten, Trends und Strategien 2026" (10.12.2025)

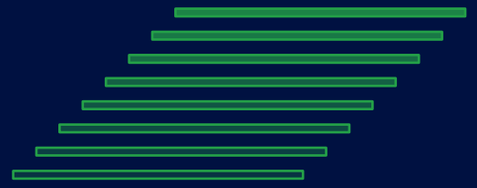
Wo KI-Anwendungen einzuordnen sind

	BEISPIELE AUS DEM FINANZMARKT	PFLICHTEN
VERBOTEN **Unzulässig**	Social Scoring Manipulative KI Emotionserkennung am Arbeitsplatz	*Kein Einsatz zulässig – Strafen bis 35 Mio. € / 7 % des Umsatzes*
HOCHRISIKO **Streng reguliert**	Prämienkalkulation Lebens-/Krankenversicherungs-Risikobewertung Bonitätsprüfung Schadenentscheidungen	*CE-Konformität, FRIA, technische Dokumentation, menschliche Aufsicht, Registrierung*
BEGRENZT **Transparenzpflicht**	Kunden-Chatbots Virtual Assistants Interaktive KI-Systeme mit Endkundenbezug	*Kennzeichnungspflicht („Sie sprechen mit einer KI"), Datenschutzkonformität*
MINIMAL **Freiwillige Standards**	Interne Analysen Textzusammenfassungen Code-Assistenten Dokumenten-Klassifikation	*Keine zusätzlichen gesetzlichen Pflichten – interne Governance empfohlen*

TEIL 3

Die 6 Do's

Was Vorstände im Finanzmarkt jetzt richtig machen müssen.



Unsere Empfehlungen an Vorstände im Finanzmarkt

01

KI & Datenqualität zur Chefsache machen

KI benötigt eine klare Zielrichtung und Strategie. Data Governance, Bias-Analyse und Datenprovenienz sind Pflicht, nicht Kür.

02

KI-Architektur definieren

Klare technische Leitlinien – von der Infrastruktur bis zu den Modellen – sind die Grundlage für eine sichere und wirtschaftlich erfolgreiche KI-Nutzung.

03

KI-Governance und Inventarisierung etablieren

Klare Verantwortlichkeiten, Risikoklassifikation und ethische Leitlinien – vor dem ersten Use Case, nicht danach. Ohne vollständiges Inventar ist Compliance bis 08/2026 unmöglich.

04

Human-in-the-Loop sicherstellen

Bei jeder Hochrisiko-Entscheidung – von Prämienkalkulation bis Schadenablehnung – muss ein Mensch überstimmen können.

05

Transparenz gegenüber Kunden

61 % der Konsumenten wollen explizite Einwilligung beim KI-Einsatz. Offenlegung schafft Vertrauen – und erfüllt die Transparenzpflichten.

06

In Menschen investieren

52 % der Führungskräfte sehen Skills-Lücken. Ohne KI-Fluency der Belegschaft wird jede Technologie-Investition zum Ausfall.

TEIL 4

Die 6 Don'ts

Die teuersten Fehler – und wie Sie sie vermeiden.

Was Finanzdienstleister unbedingt vermeiden müssen

01

Kein KI-Projekt ohne IT-Architektur

71 % kämpfen mit Legacy-Kosten. KI auf maroder Infrastruktur skaliert nie – es entsteht nur neuer technischer Schuldenberg.

02

Keine Kundendaten in Public LLMs

ChatGPT & Co. nicht für sensible Versicherungs- oder Bankdaten nutzen. DSGVO + EU AI Act + DORA – dreifach riskant.

03

Keine Black-Box-KI in Entscheidungen

Nicht erklärbare Modelle in Underwriting, Pricing oder Schaden – bei Verstößen drohen sehr hohe Strafen.

04

Kein Ignorieren schlechter Datenqualität und Risiken

Unvollständige oder verzerrte Daten können zu Bias führen. KI ist kein reines Tech-Thema – Risiken in Regulatorik, Compliance und Business

05

Kein blinder Hype um Agentic AI

77 % planen Agentic AI – ohne Governance wird autonomes Handeln zum Compliance-Albtraum. Erst Kontrolle, dann Autonomie.

06

Keine Versäumnisse bei Dokumentation

Ab 08/2026: Ohne technische Dokumentation, Logging und Risk-Assessment ist kein Hochrisiko-System rechtskonform betreibbar und auditierbar.

Vom Prinzip zur Praxis – der IBM-Ansatz

UNSERE 4 LEITPRINZIPIEN

01 Hybrid

Die hybride KI-Strategie von IBM kombiniert Cloud- und On-Premises-Lösungen um Unternehmen flexible, sichere und skalierbare KI-Anwendungen über verschiedene IT-Umgebungen hinweg zu ermöglichen.

02 Open

Offene Modelle, offene Standards. Keine Vendor-Lock-ins bei Ihrer strategischsten Technologie. Nutzung von Open-Source-Technologien fördert Interoperabilität und vermeidet Abhängigkeiten.

03 Trusted

Governance-by-design. Fokus auf transparente, erklärbare und verantwortungsvolle KI-Systeme.

04 Targeted

Use-Case-orientiert. Entwicklung praxisnaher KI-Anwendungen, die konkrete Geschäftsprobleme lösen und einen definierten ROI liefern.

DER IBM watsonx STACK

Drei Ebenen – ein Ziel: sichere KI im Maßstab.

watsonx.ai

Foundation Models & GenAI – offene, skalierbare Entwicklungsplattform für alle KI-Workloads.

watsonx.data

Hybrid Data Lakehouse – die vertrauenswürdige Datenbasis für jedes produktive KI-Modell.

watsonx.governance

EU AI Act ready – Modell-Audit, Risk Assessment, Factsheets, Agent Monitoring für Hochrisiko-Systeme.

05 DIE IBM PERSPEKTIVE

Warum IBM Ihr Partner in Österreich ist

≈ 100

Jahre

Erfahrung in der Finanzindustrie in Österreich

#1

Marktführer

Leader in Enterprise KI (zB. Gartner Magic Quadrant AI Application Dev., IDC MarketScap)

Client 0

IBM als Innovator

IBM hat selbst viele interne Prozesse mittels KI nachhaltig transformiert

LOKAL VERANKERT, GLOBAL SKALIERT

IBM Consulting Austria – Ihr Partner für KI im regulierten Umfeld

Lokales Beratungsteam

Berater in Wien mit tiefer Technologie- und Sektor-Expertise in Banken, Versicherungen.

KI und Hybrid-Cloud-Expertise

Breite Deployment-Optionen – von On-Premise bis souveräne Cloud.

End-to-End-Ansatz

Strategie, Technologie, Implementierung, Change-Management, Managed Services.

Was Sie in den nächsten 90 Tagen tun sollten

TAG 1 – 30

Status quo – KI Readiness

- KI-Strategie & Business: Überblick zum Status quo der KI-Strategie und -Systeme und Abgleich mit Geschäftszielen und regulatorischen Anforderungen
- Technologie: Einschätzung zu IT-Infrastruktur und vorhandener Systeme in Bezug auf Daten und KI
- Regulatorik: Gap-Analyse gegen regulatorische und Compliance-Anforderungen

TAG 31 – 60

Planen und strukturieren

- Use-Cases & Business Value: Identifikation von KI-Use-Cases und ROI, Priorisierung
- Planung Technologie & Datenbasis: KI-fähige IT-Architektur (z.B. Hybrid-Cloud-Architektur), Integration und Nutzung von Datenquellen, Einsatz von KI-Plattformen
- KI-Governance-Framework und Verantwortlichkeiten definieren
- Schulungsprogramm für Board & Fachbereiche starten

TAG 61 – 90

Umsetzen und skalieren

- Entwicklung und Umsetzung erster Pilotprojekte
- Anpassung und ggf. Erweiterung der IT-Infrastruktur und Datenbasis
- Einführung von KI-Governance-Modellen (Monitoring- und Reporting-Prozesse etablieren, Kontrollsysteme, Transparenz)
- Roll-out Plan für weitere Skalierung

Unser Angebot: IBM AI Readiness Assessment für Ihr Institut – in 4 Wochen zum belastbaren Status vor dem 02. August 2026.

D A N K E

KI verantwortungsvoll einsetzen – gemeinsam.

Michael Czachs
General Manager IBM Consulting Österreich · Senior Partner

Ich freue mich auf Ihre Fragen.

APPENDIX

Quellenverzeichnis

APPENDIX

Quellenverzeichnis

IBM & Studien

- IBM Institute for Business Value – Insurance in the AI era (September 2025)
- IBM IBV – The CEO's guide to generative AI: Business Process Automation (2024)
- IBM IBV – The CEO's guide to generative AI: Customer Service (2024)
- IDC MarketScape: Worldwide AI Governance Platforms 2025 Vendor Assessment
- 2025 Gartner Magic Quadrant for AI Application Development Platforms

Regulatorik EU

- Verordnung (EU) 2024/1689 – Artificial Intelligence Act
- Verordnung (EU) 2022/2554 – Digital Operational Resilience Act (DORA)
- Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO)
- EIOPA Opinion on Artificial Intelligence Governance in Insurance (2025)

FMA Österreich

- FMA – Fakten, Trends und Strategien 2026 (10.12.2025)
- FMA – Aufsichtsschwerpunkte 2026: Digitalisierung, KI und neue Geschäftsmodelle
- FMA – Pressemitteilung Finanzsanktionen ab 01.01.2026

Markt & Branche

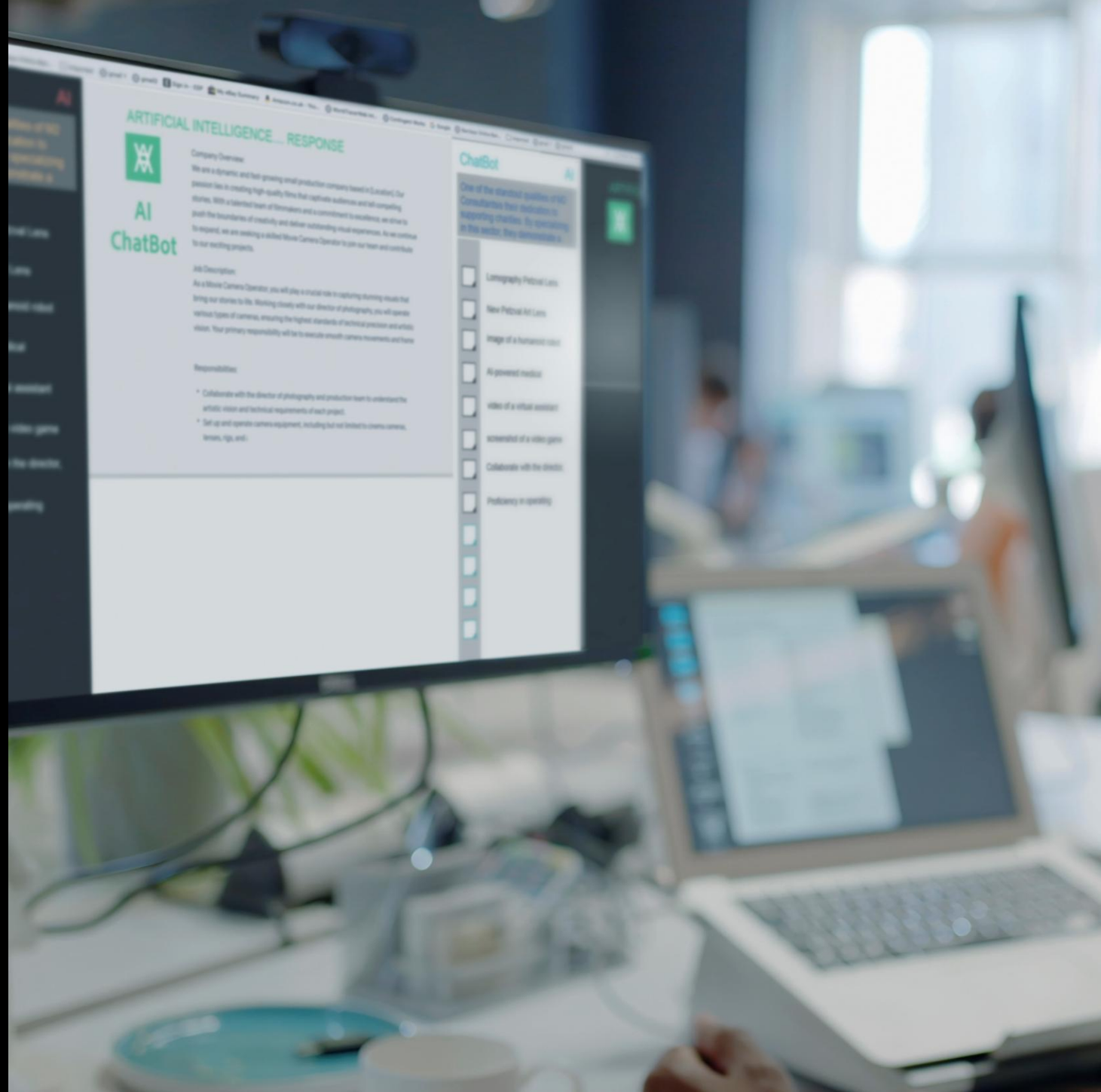
- Swiss Re Sigma 02/2025 – Welt-Versicherungsmarktstudie
- Versicherungsbote – EU AI Act: Was Versicherer wissen müssen (Dezember 2025)
- PwC – Der EU AI Act und die Auswirkungen für Versicherungen

Specialty Solutions

Versicherung gegen KI-Risiken

FMA-Forum: Next level Tech@Insurance (VU / PK / BVK)

Wien, 23.04.2026



Agenda

I. Aktuelle Schadenlage

II. KI Risiken im Überblick

III. Herausforderungen und neuartige Versicherungslösungen

IV. Versicherbarkeit im Überblick

Top KI-Vorfälle 2025–2026

„Quantum AI"-Betrugsseite in Österreich

- **Deepfake-Video** des Bundespräsidlenten
- **250 €** „Anfangsinvestition"

Online-Betrug mit falscher ORF-Seite

Deloitte-Report-Panne in Australien

- Falsche Quellen im Bericht
- Teilerstattung von 440.000 AUD

KI-Fehler in Regierungsstudie

McDonald's Bewerberdaten-Leck

- **Bis zu 64 Mio.** Datensätze offen
- Unsichere Chatbot-Plattform

Massives Datenschutzproblem

GEMA verklagt OpenAI in München

- Urheberrechtsverletzung durch ChatGPT
- Musiktexte illegal kopiert und genutzt

ChatGPT verletzt deutsches Urheberrecht

ENISA-Berichte mit Fake-Quellen

- Zahlreiche falsche / defekte Quellen
- EU-Cybersicherheits-agentur in Kritik

Revisionsbedarf bei Bedrohungsanalysen

AON

KI Risiken | Überblick

Cyberversicherung

Datenschutz- und Geheimhaltungspflicht-verletzungen durch Nutzung von KI. Prompt Injections und Verwendung von KI als Angriffsmittel.

Intellectual Property

Unrechtmäßige Nutzung von Fotos, Abbildungen, Videos, Texten und Stimme und daraus resultierende Verletzungen von Urheber, Marken- und Patenrechten.

Produkthaftpflicht

Einsatz von KI in der Produktion kann zu Fehlern im Produktionsprozess und mangelhaften Produkten führen. Produktrückrufe können die Folge sein.

Errors & Omissions

KI erteilt einen falschen Rat, „Halluziniert“ und liefert unrichtige Informationen, falsche Ableitungen. KI erteilt schädigende Auskünfte.

Medienrechtsverletzung & Reputationsschaden

KI kann im Bereich des Marketings zu Schäden aufgrund von falschen Werbe-aussagen und Reputationsverletzungen führen.

Vertrauensschaden-versicherung

KI dient als Tatwerkzeug für Social Engineering Fraud, insbesondere durch Nachahmung von Bild und Stimme.

Directors & Officers

Neben den Risiken für Manager durch den Einsatz von KI, rückt auch die Thematik „AI Washing“ immer stärker in den Vordergrund.

Diskriminierung

KI trifft diskriminierende Entscheidung, schließt eine Personengruppe ungerechtfertigt aus, stellt eine Gruppe unrechtmäßig unter Verdacht.

Personen- und Sachschäden

Durch den starken Einsatz von Robotik und IoT kann KI als alleiniger Verursacher von Personen- und Sachschäden fungieren. Dies führt rechtlich zu neuen Herausforderungen.

KI | Herausforderungen für die Versicherbarkeit

Fehlende Standardisierung:

Die starken und dynamischen Entwicklungen im Bereich der künstlichen Intelligenz stellen die Versicherungswirtschaft vor große Herausforderungen. Die Konzipierung von Produkten ist aufgrund der fehlenden Standardisierung kaum möglich.

Unklarheit über den Versicherungsumfang:

Die KI-Revolution erinnert stark an den Beginn der Cyberversicherung. Auch diesmal ist der Versicherungsumfang der bestehenden Produkte in Hinblick auf die neue Risikosituation fraglich. Sogenannte „Silent KI-Deckungen“ finden sich in vielen altbewährten und auch jüngeren Versicherungs-produkten. Wie bereits bei der Cyberversicherung führen diese Deckungen im Schadenfall oftmals zu Deckungsstreitigkeiten und sind aus diesem Grund mit Vorsicht zu behandeln.

Wachsende Risiken durch KI:

Basierend auf den enormen Kapazitäten von KI entsteht eine vollkommen neuartige Risikosituation. Der Versicherungsschutz für diese Risiken muss aus diesem Grund öfter überprüft und angepasst werden.

Komplexe Schadenabwicklung:

Die Schadenabwicklung von KI Schäden stellt alle Beteiligten vor große Herausforderungen, neben den vielen Beteiligten führt oftmals auch die Haftung zu komplexen Rechtsfragen.

Neuartige Versicherungsangebote

- **Munich Re** | KI Performance Versicherungslösung
- **Armilla AI** | Haftpflichtversicherung für KI-Agents
- **AiShelter** | Haftpflichtversicherung für KI-Entwickler
- **Relm Insurance** | Spezielle KI-Versicherungslösungen:
  - **NOVAAI** | Cyber und Tech E&O-Versicherung für Anbieter von KI-Lösungen.
  - **PONTAAI** | Umbrella-Lösung, für Unternehmen die KI-Lösungen nutzen und nicht selbst kreieren; “AI-Wrap”.
  - **RESCAAI** | Eigenschadenversicherung, mit Fokus auf Incident Response für Unternehmen, die eine KI-Lösung von einer Drittpartei beziehen, um ihre Betriebstätigkeit damit auszuüben, beispielsweise Online-Händler oder die diese KI-Lösungen in ihre Produkte einbauen, wie beispielsweise Spielzeug- oder Autohersteller.
- **AXAXL** | Endorsement für KI Risiken innerhalb der Cyberversicherung
  - Data poisoning
  - Usage rights infringement
  - Regulatory violations

KI Risiken | Versicherbarkeit im Überblick*

KI-Risiko	Medien-haftpflicht	Berufs-haftpflicht	Produkt-haftpflicht	Betriebs-haftpflicht	Geistiges Eigentum	Cyber	Vertrauens-schaden	D&O
Haftung für fehlerhafte Produkte und Dienstleistungen	●	●	●	●	●	●	●	●
Urheberrecht, Marken- oder Dienstleistungsmarkenverletzung	●	●	●	●	●	●	●	●
Patentrechtsverletzung	●	●	●	●	●	●	●	●
Diskriminierung/ Voreingenommenheit	●	●	●	●	●	●	●	●
Verleumdung, üble Nachrede, Beleidigung	●	●	●	●	●	●	●	●
Personenschäden	●	●	●	●	●	●	●	●
Sachschäden	●	●	●	●	●	●	●	●
Datenschutz- und Sicherheitsverletzungen	●	●	●	●	●	●	●	●
Verlust finanzieller Vermögenswerte	●	●	●	●	●	●	●	●
Marktmanipulation	●	●	●	●	●	●	●	●
Täuschung	●	●	●	●	●	●	●	●
Robotik	●	●	●	●	●	●	●	●
Produktrückruf	●	●	●	●	●	●	●	●
Betriebsunterbrechung	●	●	●	●	●	●	●	●
Verletzung der Pflichten von Führungskräften	●	●	●	●	●	●	●	●

● Allgemein verfügbar ● Limitiert ● Ausgeschlossen

***Disclaimer:** Der hier dargestellte Überblick über die Versicherbarkeit von KI Risiken stellt keine abschließende Beurteilung dar; Bitte beachten Sie, dass eine abschließende Beurteilung der Versicherbarkeit ausschließlich durch eine Prüfung der zugrundeliegenden Versicherungsbedingungen erfolgen kann.

Ich freue mich auf einen Austausch mit Ihnen!

Mag. Kerstin Keltner
Managing Director Specialty

+43 676 5955424
kerstin.keltner@aon-austria.at

FIDA: State of play and way forward

FMA-Forum:

Next level Tech@Insurance (VU / PK / BVK)

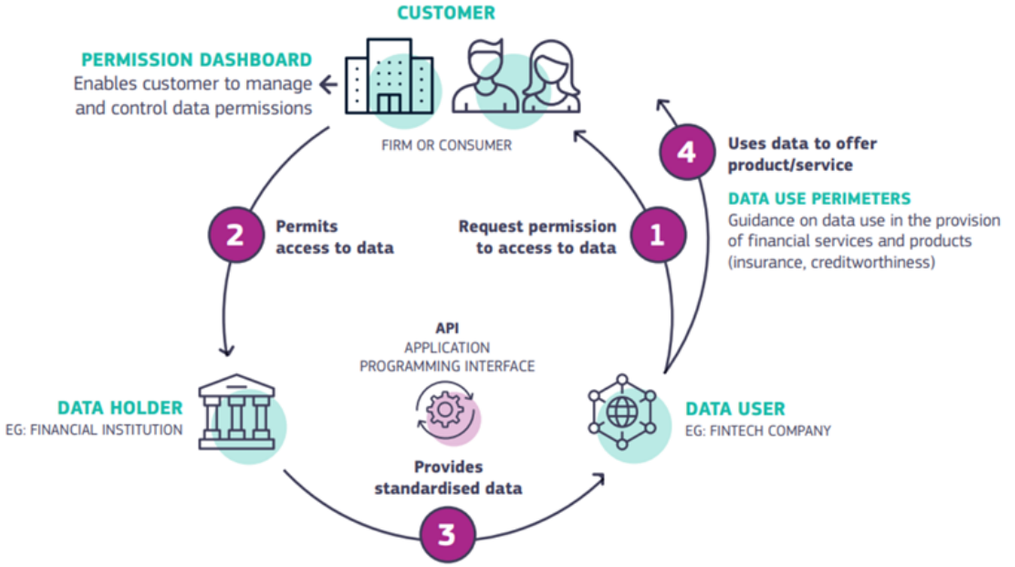
Nadine Wiedermann-Ondrej
Bundesministerium für Finanzen
Wien, 23. April 2026

Financial Data Access Verordnung (FiDA)

- The data holder shall, **upon request from a customer** submitted by electronic means, make the data available to the customer **without undue delay, free of charge, continuously and in real-time**.

- 28. Juni 2023: EK Vorschlag
- 18. April 2024: EP Report
- 4. Dezember 2024: General Approach
- März 2025: Beginn Trilog
- Leaked versions of the Commission's 2025 work programme: proposals to be withdrawn
- Official 2025 Commission work programme: pending proposals

- **Customer control over their data**
  - Oblige data holders to share customer data upon request
  - Introduce permission dashboards
- **Responsible access for data users** where customers want to benefit from innovative products
  - Promote standardisation of customer data
  - Encourage implementation of high-quality interfaces
  - Based on a contractual framework of financial data sharing schemes



Anwendungsbereich

Persönlicher Anwendungsbereich

- Kreditinstitute,
- Wertpapierfirmen,
- Verwalter alternativer Investmentfonds, Verwaltungsgesellschaften von Organismen für gemeinsame Anlagen in Wertpapieren, CASP
- Versicherungs- ~~und~~ ~~Rückversicherungs~~unternehmen,
- Versicherungsvermittler und Versicherungsvermittler in Nebentätigkeit,
- Einrichtungen der betrieblichen Altersversorgung, **soweit sie personal pension products managen**
- Finanzinformationsdienstleister,
- PEPP-Provider

Sachlicher Anwendungsbereich

- Hypothekarkreditverträge, Darlehen und Konten, ausgenommen Zahlungskonten, einschließlich Daten zu Saldo, Konditionen und Transaktionen;
- Ersparnisse, Investitionen in Finanzinstrumente, Versicherungsanlageprodukte, **insurance-based individual pension products**, Kryptowerte, Immobilien; einschließlich Daten, die zur Beurteilung der Eignung und Zweckmäßigkeit gemäß MiFID **und IDD (inkl ESG)**;
- ~~Ruhegehaltsansprüche aus betrieblichen Altersversorgungssystemen;~~ MS-Wahlrecht
- Ruhegehaltsansprüche aus Paneuropäischen Privaten Pensionsprodukten;
- Nichtlebensversicherungsprodukte, ausgenommen Krankenversicherungsprodukte **and data on personal injuries contained in non-life**
- **insurance products**; einschließlich Daten, die zur Ermittlung der Wünsche und Bedürfnisse bzw Beurteilung der Eignung und Zweckmäßigkeit IDD erhoben werden;
- Daten, die zur Beurteilung der Kreditwürdigkeit eines Unternehmens im Rahmen eines Kreditantragsverfahrens

Financial Information Service Provider (FISP)

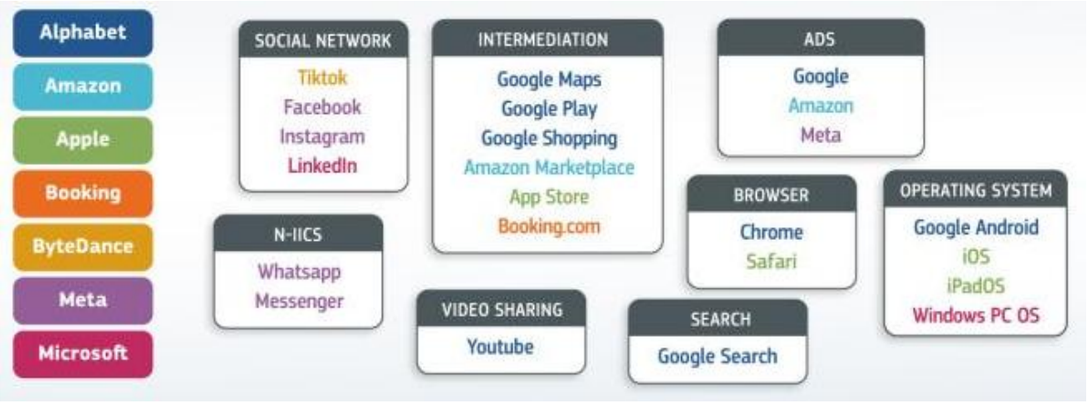
Antrag auf Zulassung als Finanzinformationsdienstleister

- Beschreibung des **Geschäftsmodells**
- **Geschäftsplan** mit einer Budgetplanung für die ersten drei Geschäftsjahre
- Beschreibung der **Regelungen für die Unternehmensführung** und der **internen Kontrollmechanismen**, einschließlich der Verwaltungs-, Risikomanagement- und Rechnungslegungsverfahren
- Beschreibung des **organisatorischen Aufbaus** des Antragstellers sowie eine Beschreibung der **Auslagerungsvereinbarungen**;
- Geschäftsleiter **gut beleumundet** und verfügen sowohl **individuell als auch kollektiv** über ausreichende **Kenntnisse, Fähigkeiten und Erfahrung**;
- Berufshaftpflichtversicherung
- Einhaltung von DORA

➢ Register

Gatekeeper Authorisation

- **specific assessment by the competent authority** of its establishment
- assessment, which sets out the **functioning, services and activities** performed as a data user
- assessment of the **network effects and data driven advantages**
- sufficient safeguards to demonstrate compliance with the **requirements for data users**
- sufficient **IT, governance and organizational safeguards**



gatekeepers based on specific quantitative thresholds: annual EEA turnover exceeding EUR 7.5 billion, market capitalisation exceeding EUR 75 billion, providing Core Platform Services (CPS) to more than 45 million monthly active end users, and serving more than 10 000 active business users on an annual basis

Danke für die Aufmerksamkeit!

FiDA-Readiness

Weichenstellungen und ToDo‘s 2026

Johannes Neumeyer
Accenture – FiDA Insurance DACH Lead

accenture

FiDA-Daten werden die Branche entlang der gesamten Customer Journey beeinflussen

Relevanz von FiDA für Versicherer und den Vertrieb

AUSZUG

1 Kundenansprache	2 Kundenberatung	3 Produktangebot und Abschluss	4 Service-leistungen	5 Schadens-/Leistungsfall	6 Kündigung
Individualisierte Kundenansprache, basierend auf versicherten/ unversicherten Risiken (inkl. Fremdverträge)	**360° Blick auf Kundenbedarfe** zur Sicherstellung ganzheitlicher Beratung	**Individualisierte Produkte**, basierend auf bestehenden Absicherungs-lücken	Kundenportale im Sinne eines **Financial Homes**	**Effiziente Schaden-ermittlung und Kommunikation**, zwischen Ver-sicherern	**Entkopplung Produkt und Berater-beziehung -** Einbindung neuer Versicherungsdaten in Beratungskonzept (AO/ DV)
Zielgerichtete Kundenansprache auf **Basis von Präferenzen** (Zielmarkt)	**Einbindung aller Sparprodukte** (inkl. Immobilien) in Rentenplanung	**Optimierung der Abschluss-strecken** durch digitale Verfüg-barkeit von Risikodaten	**Anbieterüber-greifende E2E-Service-prozesse** in eigenen/dritten Portalen	**Portfolio-management, inkl. Wiederanlage** (IBIP/ Anlageprodukte/ Rentenberatung)	**Churn-Management** durch ganzheitliche Indikatoranalysen

TAKE AWAY | FiDA-Use Cases entsprechen den bestehenden Zielbildern der meisten Kunden-/ Vertriebsstrategien .

Intensiverer Wettbewerb durch steigende Transparenz, Angriff insbesondere durch Nicht-Versicherungen

Erwartete Marktauswirkungen für Versicherer

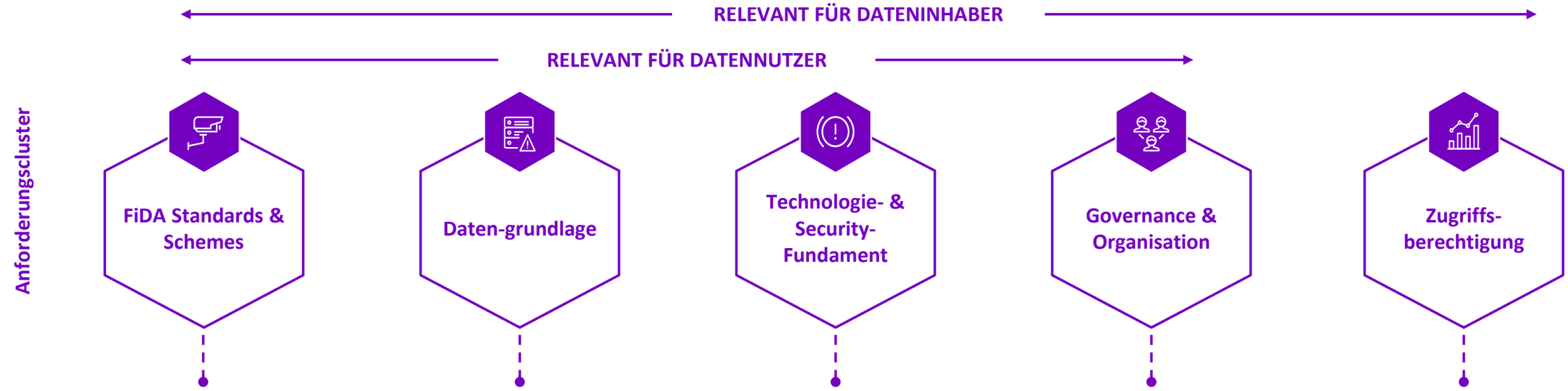
	Erste Einschätzung zum Marktimpact	Strategische Implikationen
Wettbewerb mit anderen VU	• Starker **Preis- und Konditionenwettbewerb** in commoditisierten Sparten (Kfz, Haft, Hausrat etc.) • Zunahme **gezieltes Umdecken** und **Cross-Selling** • Wettbewerbsfokussierung führender Versicherer auf/in einzelne(n) LoBs	• Wettbewerb intensiviert sich in den Dimensionen **Preis-Leistung,** Differenzierung über operativer Exzellenz, Pricing-Fähigkeit und Customer Experience/Kundenbindung • Top-Performer **skalieren über Plattformen**; Nachzügler sind Margendruck ausgesetzt
„Neue“ Wettbewerber	• **Banken** durch gute Kundeninteraktion (Frequenz, Vertrauen, Relevanz) mit Vorteilen • **FinTech (Neobroker, Dig. Makler, Vergleicher)** mit hoher digitaler Kompetenz (Kundenansprache, UX) mit Vorteilen • **BigTechs** treten punktuell/indirekt über (Tech)Ökosysteme, und White-Label-Modelle in Erscheinung	• Gefahr weniger durch „Big Tech“ und „Full-Stack-Versicherer“, sondern durch **fokussierte Wertschöpfungsangriffe** (z. B. Vertrieb, Pricing, Schaden) • Re-Fokussierung der Marktbearbeitung; Prüfung der zu bearbeitenden Kundenschnittstellen
Kunden	• Höhere **Markttransparenz** und „Mündigkeit“ durch Vergleicher und GenAI, **sinkender Aufwand für Wechsel** • **Steigende Kundenerwartungen** an Einfachheit, Schnelligkeit und Individualisierung • **Gewerbekunden professionalisieren Einkauf** und Ausschreibungen	• Machtverschiebung zugunsten der Kunden erzwingt besseres **datengetriebenes Pricing**, **aktives Bestandsmanagement**, **personalisierte Angebote** statt Standardansätze • **Kundenbindung** und Storno Prävention werden zum kritischen Werttreiber
Wertschöpfungs-logik	• Zunehmende **Abhängigkeit von Dritten**, insb. Technologie-Anbietern, an der **Kundenschnittstelle** • Veränderung **Skills** (Marketing, Data Science, IT-Architektur)	• **Strategischer Aufbau FiDA-bezogener Kompetenzen**: Technologie, Prozesse, Talente, Governance

Drei Analyse-Cluster zum Status quo helfen bei der Auswahl einer individuell sinnvollen FiDA-Positionierung

Strategische Grundpositionen von FiDA

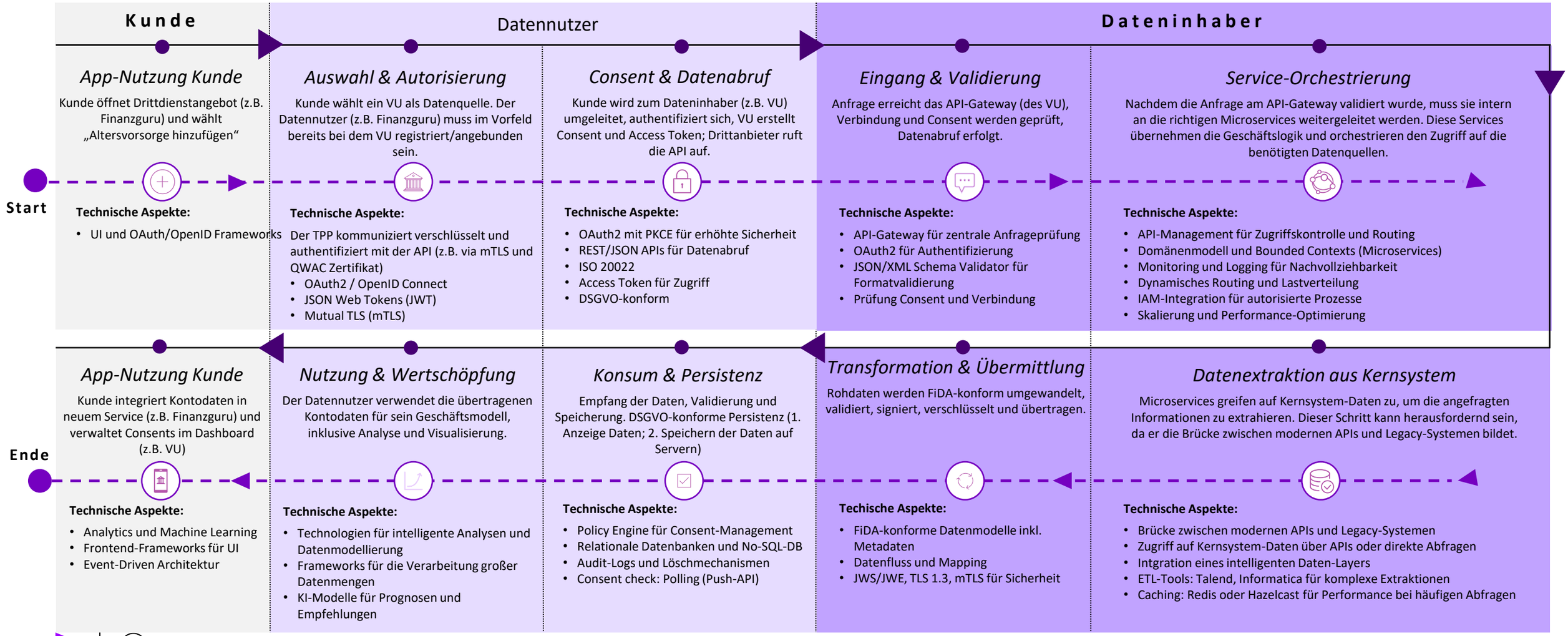
Zur Analyse des FiDA-Impacts und Vorbereitung der Umsetzung können fünf Anforderungscluster herangezogen werden

Technische Handlungsfelder



Für die „minimale“ Ausprägung eines Datenabrufs lassen sich bereits heute technische Anforderungen ableiten

Beispiel: Technische Anforderungen einen E2E-Datenabrufs



Fachliche Annahmen und klare Zielbilder sind die Basis der FiDA-Vorbereitung – müssen aber kontinuierlich überprüft werden

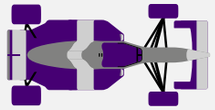
Unser bewährtes Framework für Vorstudien und Implementierungsmaßnahmen

Das Qualifying läuft bereits…

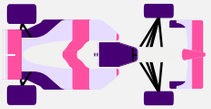
Das Rennen startet 2026…

FiDA-Vorbereitung

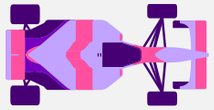
Schritt 1:
Dezidierte FiDA-Strategie formulieren und positives Leitbild schaffen



Schritt 2:
FiDA-Ziel-Architektur entlang fachl./reg. Anforderungen definieren

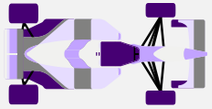


Schritt 3:
GAP-Analyse durchführen und Roadmap ableiten

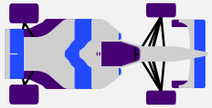


FiDA-Umsetzung

Schritt 4:
Projektsteuerungs- und -governance-Struktur implementieren



Schritt 5:
Use Cases und Go2Market fokussieren



Projekterfahrung

Die fachlichen Grundlagen sind entscheidend, um die informationstechnischen Konsequenzen zu identifizieren. Sie bestimmen den konkreten Scope des individuellen FiDA-Readiness Assessments.

Aufgrund der bestehenden Unsicherheiten zur FiDA-Umsetzung ist eine **hypothesen-getriebene Analyse notwendig**. Strategien sollten mehrere Szenarien abbilden und die beabsichtigte **FiDA-Rolle** berücksichtigen.

Es ist davon auszugehen, dass sich legislative und marktbezogene Einflussfaktoren (kontinuierlich) verändern. **Vorstudien müssen die aktuelle Dynamik, Entwicklungskorridore und das unternehmerische Engagement beim Scheme-Building konzeptionell integrieren.**

Diskussion

accenture

Wir freuen uns auf Diskussionen zur FiDA-Readiness

Ihre Ansprechpartner

Johannes Neumeyer

Insurance Strategy

johannes.neumeyer@accenture.com

Dr. Timo Biskop

Insurance Strategy

timo.biskop@accenture.com

TC 445

European CEN Standards for the Customer Data Access and Portability in the Insurance Sector

Dr. Manuel Reimer

FIDA-Datenzugriff – Welchen Standard nutzen ?

TC 445

- Es gibt keinen europäischen oder globalen Standard für den Datenzugriff im Versicherungssektor.
- In einigen Ländern oder Märkten gibt es bereits Standards, die speziell für digitale Prozesse zwischen Versicherern und Vermittlern entwickelt wurden und nun für den FIDA-Datenzugriff genutzt werden können, in AT: OMDS.
- Viele europäische Länder verfügen jedoch noch nicht über entsprechende Standards.
- Parallele Standardisierung in diesen Ländern, - macht das Sinn ?
- Und EU-weite Use Cases ?
- Digitaler europäischer Binnenmarkt im Versicherungssektor ?

EU Kommission fordert europäische FIDA Standards

TC 445

- EU Kommission möchte den Datenzugang im Finanzsektor erleichtern.
- Sie fordert daher Standards für GDPR Artikel 20 und FIDA Regulation.
- Aufgrund der Datenvielfalt zunächst im Versicherungssektor:
  - Aktion 12 im **2024 Annual Union Work Programme for European Standardisation**: “Customer data in the insurance sector”
    https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202401364
- Aktuell nun auch in allen anderen Finanzsektoren:
  - Aktion 28 im **2026 Annual Union Work Programme for European Standardisation**: “Customer data in the financial sector”
    https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202601695
- Anforderungen der EU an die europäischen Standardisierungsorganisationen.

CEN – European Standardisation Organisation

TC 445

Austria

Belgium

Bulgaria

Croatia

Cyprus

Czech Republic

Denmark

Estonia

Finland

France

Germany

Greece

Hungary

Iceland

Ireland

Italy

Latvia

Lithuania

Luxembourg

Malta

Netherlands

Norway

Poland

Portugal

Republic of North Macedonia

Romania

Serbia

Slovakia

Slovenia

Spain

Sweden

Switzerland

Turkey

United Kingdom

Standardisation in CEN

TC 445

200 000
Experts

497
Technical Committees

1 903
Working Groups

23 901
Standards

614
Technical Specifications

636
Technical Reports

CEN/TC 445
Digital Information Interchange in the Insurance Industry

TC 445

- Gründung 2016
- Vorsitz Dr. Manuel Reimer
- Sekretariat DIN (deutsche Normungsorganisation)
- Experten Versichererverbände, Vermittlerverbände, markt-spezifische Standardisierungsorganisationen des Versicherungssektors
- Liaisons BIPAR – European Association of Insurance Intermediaries
  Insurance Europe – European Association of Insurers
- Website https://tc445.info

European Standards for the Customer Data Access and Portability in the Insurance Sector

TC 445

Aktive Teilnehmer

- Belgien
- Deutschland
- Finnland
- Frankreich
- Lettland
- Litauen
- Norwegen
- Österreich
- Schweden
- BIPAR
- Insurance Europe

Kommentierende Teilnehmer

- Großbritannien
- Irland
- Niederlande
- Zypern

13 Länder

2 Liaison-Organisationen

50 Experten

Scope

TC 445

European standards for data access and portability in the insurance sector

- **B2C:**
  Zugriff vom Kunden (natürliche oder juristische Person) auf die beim Dateninhaber gespeicherten Kundendaten – EU FIDA Regulation Artikel 4
- **B2B:**
  Zugriff vom Datennutzer mit Kundenberechtigung auf die beim Dateninhaber gespeicherten Kundendaten – EU FIDA Regulation Artikel 5
- Daten von Versicherungsprodukten im Umfang von EU FIDA Artikel 2 (1)
- Kundendaten im Umfang von EU FIDA Artikel 3 (3)

Leitlinien für „Kundendaten“

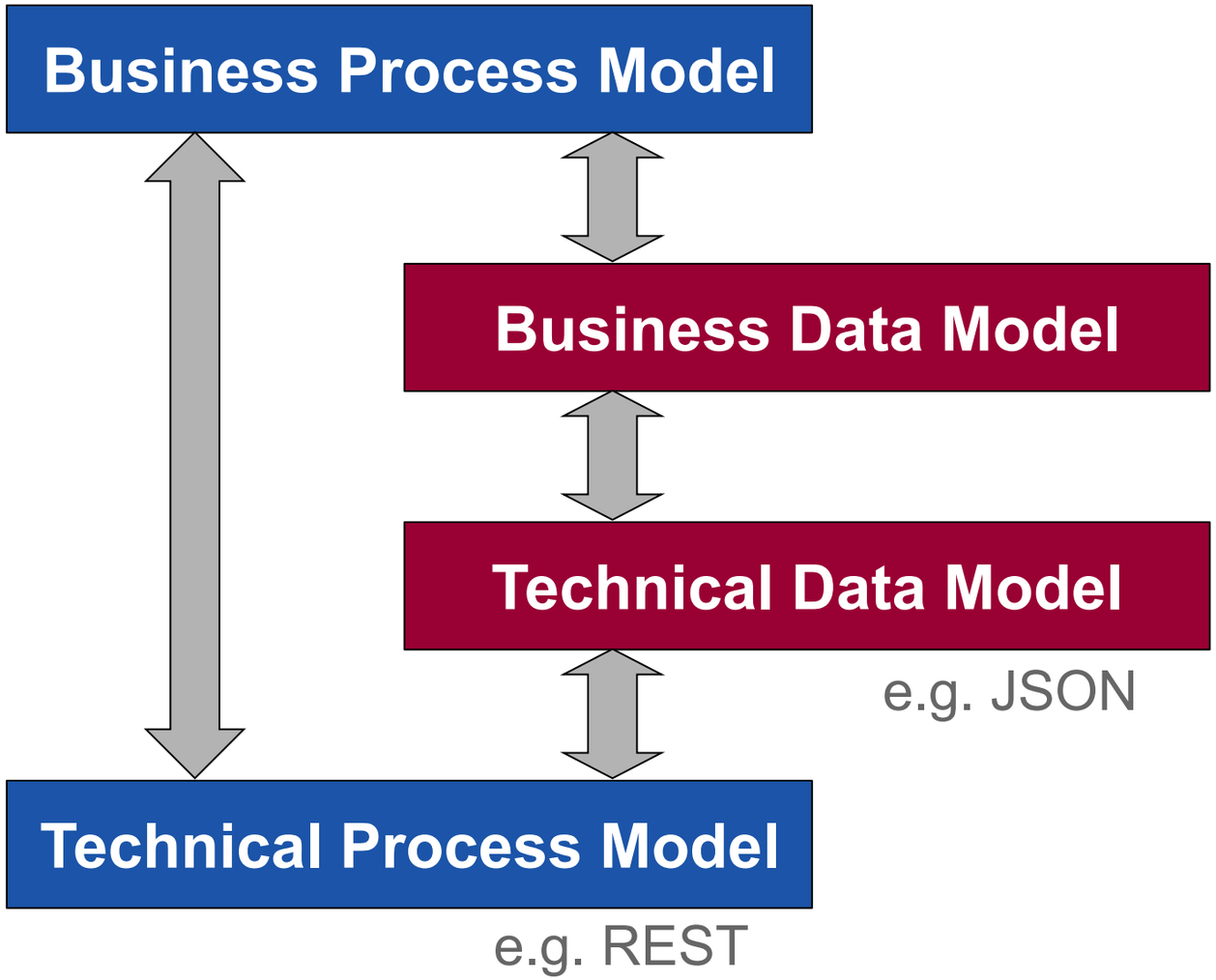
TC 445

European standards for data access and portability in the insurance sector

- Alle Daten sollen im Standard enthalten sein, die der Kunde dem Dateninhaber zur Verfügung stellt, – die vom Dateninhaber gespeicherten sogenannten „Rohdaten“.
- Alle Daten sollen im Standard enthalten sein, die der Dateninhaber dem Kunden zur Verfügung stellt, – die Daten der Versicherungspolice, von Statusberichten zu Policen oder von Schadenfällen.
- Nicht im Standard enthalten sind alle Daten, die dem Kunden nicht übermittelt werden, sogenannte „abgeleitete Daten“ zur Bewertung des Kunden oder des Risikoobjekts und zur Prämienberechnung, sowie Provisionsdaten, Rückversicherungsdaten etc.

Ebenen der Prozess- und Daten-Normierung

TC 445



Business Level
=
Semantics

Technical Level
=
Syntax
=
Implementation

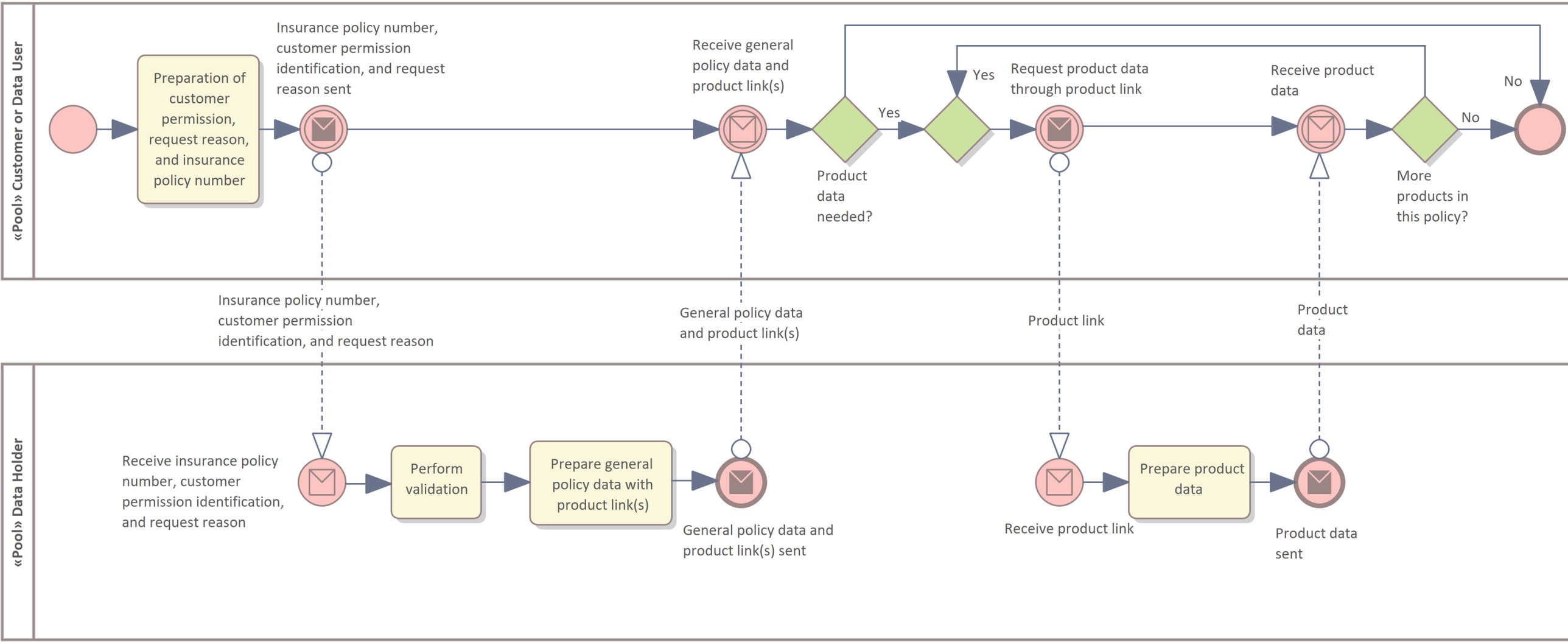
Normen (1)

TC 445

- **European Standard EN 18356-1**:
  - Semantische Definition der Schnittstelle für den Datenzugriff eines Kunden oder Datennutzers auf die beim Dateninhaber gespeicherten Kundendaten
  - Datenmodell für die Kundendaten
  - Semantische Definition jedes einzelnen Datenelements der Kundendaten mit Name und Beschreibung
  - Norm auf der fachlichen Ebene mit einer Syntax-neutralen Spezifikation unabhängig von einer spezifischen Implementierungs-Technologie

EN 18356-1: Semantischer Prozess für Datenzugriff

TC 445



EN 18356-1: Daten für alle FIDA Versicherungssparten

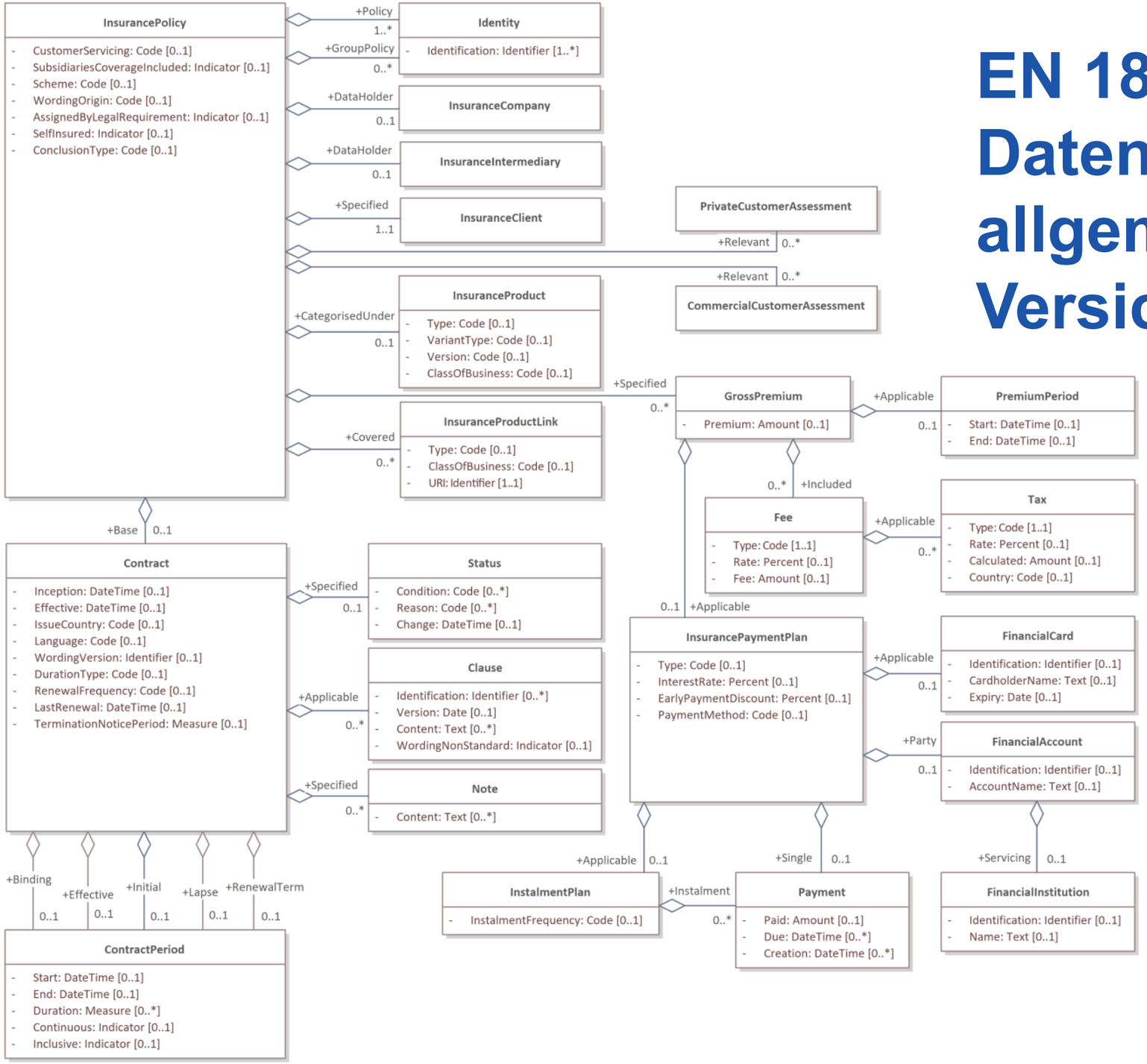
TC 445

European standards for data access and portability in the insurance sector

- Allgemeine Policen- und Kundendaten (214 Datenelemente)
- Risiko- und Bedürfnisanalyse von Kunden gemäß IDD und MiFID II (229)
- Private und gewerbliche Kraftfahrtversicherung (530)
- Private Sachversicherung (614)
- Gewerbliche Sachversicherung (773)
- Private und gewerbliche Haftpflichtversicherung (477)
- Unfallversicherung (284)
- Private und gewerbliche Rechtsschutzversicherung (366)
- Private und gewerbliche Reiseversicherung (339)
- Vermögensschadenversicherung (Warenkredit, Vertrauensschaden, Kaution) (380)
- Versicherungs-basierte Investmentprodukte und private und betriebliche Altersvorsorgeprodukte (418)

EN 18356-1: Datenmodell für allgemeine Daten der Versicherungspolice

TC 445



Normen (2)

TC 445

- **CEN Technical Specification TS 18356-2**:
  - Technische Spezifikation der API (Application Programming Interface) in der Open API Technology, entwickelt von der Open API Initiative, ein Open-Source Projekt der Linux Foundation
  - State-of-the-art Technologie für Cloud-basierte Micro-Service Systeme: REST/JSON
  - TS enthält die Open API Spezifikationen (in YAML Format) als digitale Attachments für eine unmittelbare Implementierung mit Tools für automatische Codegenerierung, Dokumentation und Testfälle
  - Für zukünftige Technologien können weitere TS normiert werden

Digitale Anhänge der Normen

TC 445

- **European Standard EN 18356-1**:
  - Datenmodelle mit Diagrammen
  - Datenmodelle mit detaillierten Beschreibungen für jedes Datenelement in Tabellen
  - Datenmodelle als Viewer im Browser
  - Datenmodelle als XMI-Export zum Import in Tools
- **CEN Technical Specification TS 18356-2**:
  - Open API Spezifikationen als YAML-Dateien
  - Beispiele als Diagramme
  - Beispiele im JSON-Format

Flexible Nutzung des europäischen Standards

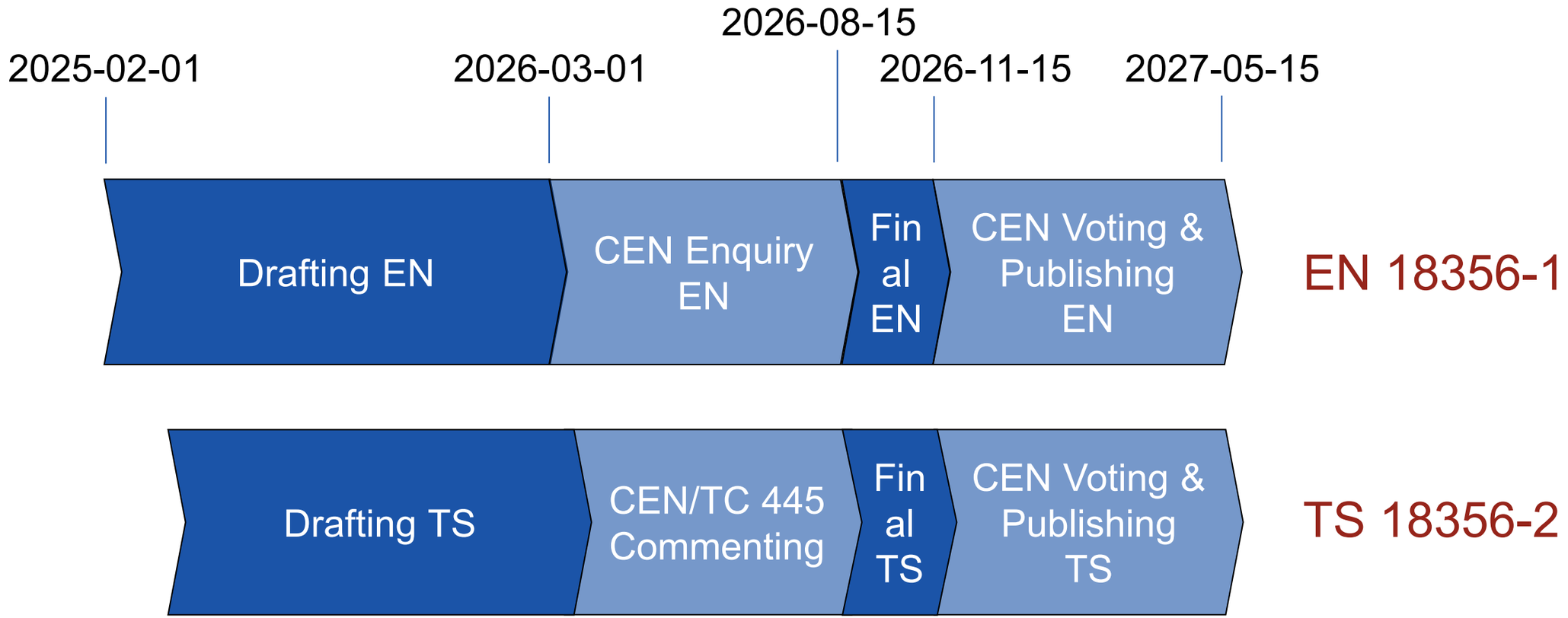
TC 445

- Als Basis für Markt-spezifische FIDA-Schemes
  - Auswahl einer Teilmenge der benötigten Datenelemente
  - Erweiterung um Markt-spezifische Datenelemente
  - Festlegung Markt-spezifischer Wertelisten für codierte Datenelemente
- Als Basis für grenzüberschreitende FIDA-Schemes
- Als Basis für Interoperabilität zwischen existierenden Markt-Standards
  - Mapping vom Markt-Standard zum europäischen Standard
  - Mapping vom europäischen Standard zum Markt-Standard

➢ **Europäische Norm ist ein freiwilliges Angebot und wird in der FIDA-Verordnung nicht verpflichtend angeordnet.**

Status der europäischen Normen für Versicherungen

European standards for data access and portability in the insurance sector



➢ **Normen für weitere Finanzprodukte und Berechtigungsprozesse folgen**

TC 445

More information

Website: tc445.info

Dr. Manuel Reimer

Chair CEN/TC 445

MR-Consulting
Oesterleystr. 36
22587 Hamburg
Germany
Tel: +49-1723604216
Mail: mail@MR-Consulting.eu
Web: MR-Consulting.eu