DORA, DS-GVO und KI-VO als einheitlicher Compliance-Rahmen für Versicherungs-unternehmen

Ein Leitfaden zur kohärenten Umsetzung digitaler Regulierung in der Versicherungswirtschaft

bitkom

Auf einen Blick

DORA, DS-GVO und KI-VO als einheitlicher Compliance-Rahmen für Versicherungs-unternehmen

Ausgangslage

Die europäische Digitalregulierung stellt Versicherungsunternehmen zunehmend vor die Aufgabe, mehrere Rechtsakte gleichzeitig umzusetzen. DORA, DS-GVO und KI-Verordnung verfolgen unterschiedliche Schutzziele, greifen in der Praxis jedoch häufig auf dieselben Geschäftsprozesse, Datenbestände, IKT-Systeme und Dienstleister zu. Besonders deutlich wird dies bei KI-gestütztem Underwriting, automatisierter Schadenbearbeitung, digitaler Kundenkommunikation, Drittanbietersteuerung und Vorfallmanagement.

Bitkom-Bewertung

Bitkom sieht darin nicht nur eine Compliance-Herausforderung, sondern auch die Chance, Digitalregulierung kohärenter, effizienter und praxisnäher umzusetzen. Voraussetzung dafür ist ein integrierter Ansatz, der regulatorische Anforderungen nicht in Silos behandelt, sondern entlang gemeinsamer Prozess-, Daten-, System- und Risikologiken strukturiert.

Das Wichtigste

Geschäftsprozesse sollten zum gemeinsamen Anknüpfungspunkt digitaler Compliance werden Informationen zu Prozessen, Datenarten, IKT-Systemen, Dienstleistern, Kritikalität und KI-Einsatz sollten strukturiert erhoben und für DORA, DS-GVO und KI-VO regimeübergreifend nutzbar gemacht werden.

Begriffe, Risikokategorien und Meldepflichten müssen besser aufeinander abgestimmt werden. Kritisch wichtige Funktionen, hochriskante KI-Systeme, automatisierte Entscheidungen, Datenschutzvorfälle und IKT-Incidents sollten klarer zueinander ins Verhältnis gesetzt werden.

Proportionalität, menschliche Kontrolle und prüfbare Governance sind entscheidend. Regulierung sollte risikobasiert dort ansetzen, wo tatsächliche Gefahren für Kundinnen und Kunden, Geschäftskontinuität, Datenschutz und Finanzstabilität bestehen.

Inhalt

1 Einführung

Europäische Digitalpolitik und der Digitale Omnibus

Die europäische Digitalregulierung hat sich in den letzten Jahren rasant erweitert. In den verschiedenen Regelungsbereichen – Cybersicherheit (CRA, CSA, NIS2, DORA usw.), Künstliche Intelligenz und Daten (KI-VO, Data Act, DS-GVO, EHDS, DGA usw.), Plattformregulierung (DMA, DSA), Finanzen (MiCA) und digitale Identität (eIDAS, EUDI) – treten Überschneidungen, komplexe Fragestellungen und praktische Schwierigkeiten auf.

Auch wenn jede dieser Initiativen legitime und wichtige Ziele verfolgt, hat ihre kumulative Wirkung zu einem zunehmend dichten und schwer durchschaubaren Rechtsrahmen geführt. Versicherungsprozesse sind nicht regulatorisch trennscharf, sodass beaufsichtigte Unternehmen nur bei Erfüllung mehrerer regulatorischer Regime compliant bleiben.

Der »Digitale Omnibus« der Europäischen Kommission ist zwar ein wichtiger Schritt zur Vereinfachung der europäischen Rechtsvorschriften im Digitalbereich, reicht jedoch noch nicht aus, um die bestehenden Hindernisse abzubauen, die das volle Potenzial der europäischen Digitalwirtschaft weiterhin bremsen.

Kerninhalte des Omnibusses sind insbesondere der europäische Datenrahmen, der Data Act, die DS-GVO, der SEP Incident Reporting sowie deren Harmonisierung, Vereinfachung und konsistente Implementierung. Dennoch bleiben zentrale Punkte weiterhin offen – insbesondere im Hinblick auf Datenklassifikation und Datenzugriff (Data Act und DS-GVO), das Informations-Risikomanagement und das KI-Training (AI-Act und DS-GVO) sowie den sogenannten »Incident Reporting Overload«.

Versicherungsprozesse als gemeinsamer Anknüpfungspunkt

DORA, DS-GVO, KI-VO und angrenzende Rechtsakte wirken in Versicherungsunternehmen nicht isoliert. Sie treffen häufig auf dieselben Geschäftsprozesse, Daten, Systeme, Dienstleister und Verantwortlichkeiten.

Deshalb sollte der Geschäftsprozess der zentrale Anknüpfungspunkt für eine integrierte Digital-Compliance sein. Prozesse wie Underwriting, Schadenbearbeitung, Betrugserkennung, Kundenkommunikation, Risikobewertung und Dienstleistersteuerung können zugleich datenschutzrechtlich relevant, IKT-gestützt, KI-basiert und für die Geschäftskontinuität kritisch sein.

Ein isolierter Blick auf einzelne Rechtsakte führt dagegen schnell zu parallelen Inventaren, was wiederum zu unterschiedlichen Risikobewertungen und unklaren Zuständigkeiten führt. Ein prozessbasierter Ansatz ermöglicht es hingegen, Informationen zu Datenarten, IKT-Systemen, KI-Einsatz, Dienstleistern, Kritikalität, Kontrollen und Verantwortlichkeiten einmalig und strukturiert zu erfassen und regimeübergreifend nutzbar zu machen.

Auf dieser Grundlage lassen sich Anforderungen aus verschiedenen Regelwerken besser miteinander verzahnen: DORA-Anforderungen an IKT-Risikomanagement, Incident Response und Drittanbietersteuerung können mit DS-GVO-Anforderungen an Datenverarbeitung, Rechtsgrundlagen, Betroffenenrechte und Datenschutz-Folgenabschätzungen sowie mit KI-VO-Anforderungen an Transparenz, Risikomanagement und menschliche Aufsicht zusammengeführt werden.

Gerade bei KI-gestütztem Underwriting oder automatisierter Schadenbearbeitung zeigt sich, dass technische Leistungsfähigkeit, Datenschutz, Nichtdiskriminierung, Resilienz und wirksame menschliche Kontrolle gemeinsam betrachtet werden müssen.

Die materiellen Anforderungen der einzelnen Rechtsakte bleiben dabei eigenständig. Ihre praktische Umsetzung kann jedoch auf einer gemeinsamen Informations- und Governance-Grundlage aufbauen.

Der Geschäftsprozess wird somit zur tragenden Basis für eine moderne, effiziente und prüfbare Compliance in der digitalen Versicherungswirtschaft.

2 DORA als struktureller Ausgangspunkt – Regulatorische Boxen vs. Praxis

Erfahrungen aus der DORA

DORA bleibt hochrelevant, und die Besonderheiten der Versicherungsbranche sollten in der Digitalgesetzgebung nicht unterschätzt werden. Die DORA-Verordnung umfasst eine Vielzahl regulatorischer Anforderungen zu Governance, IKT-Risikomanagement, Incident Response, Testing und Third-Party-Risk. Besonders herausfordernd ist jedoch, dass die strengsten Maßnahmen nicht pauschal für alle Systeme gelten, sondern **primär für die kritisch-wichtigen Funktionen (kwF)**. Diese kwF bilden die **prioritäre Grundlage** für die DORA-Umsetzung: Sie bestimmen, welche Prozesse, IKT-Systeme und Dienstleister unter die höchsten Anforderungen fallen. Der folgende Anforderungskatalog verdeutlicht die thematische Breite der Verordnung und unterstreicht die zentrale Rolle der kwF bei der gezielten Umsetzung.

DORA-Bereich	Artikel	Anzahl Anforderungen	Typische Nachweise/Dokumente
Governance & Organisation	**Art. 5**	33	Policies, Governance-Dokumente
ICT Risk Management Framework	**Art. 6**	31	Framework, Risk Assessments, Reports
ICT Systems, Protocols and Tools	**Art. 7**	13	Protokolle, Standards
Identification	**Art. 8**	10	Inventare, Klassifikationen
Protection and Prevention	**Art. 9**	59	Richtlinien, Kontrollen, Procedures
Recognition	**Art. 10**	6	Detection-Konzept, Monitoring
Response and Recovery	**Art. 11**	13	Incident Response Pläne

DORA-Bereich	Artikel	Anzahl Anforderungen	Typische Nachweise/Dokumente
Backup / Recovery / Restoration	**Art. 12**	9	Backup-, Recovery- und Restoration-Policies
Learning Processes	**Art. 13**	5	Lessons Learned, Trainings
Communication	**Art. 14**	5	Kommunikationsprozesse
ICT Incidents	**Art. 17**	12	Incident-Register, Meldungen
Reporting	**Art. 19 / 23**	3 / 3	Meldungen schwerwiegender Vorfälle
Testing	**Art. 24 / 25**	8 / 3	Testpläne, Testberichte
Third-Party Risk	**Art. 28 / 29 / 30**	15 / 2 / 6	Verträge, Assessments, Exit-Pläne
Information Sharing	**Art. 45**	4	Austauschvereinbarungen

Besonders auffällig sind dabei die hohe Anzahl an Anforderungen im Bereich »Protection and Prevention« (Art. 9: 59 Anforderungen) sowie die zentrale Rolle von Third-Party-Risk (Art. 28-30). Vor dem Hintergrund dieser thematischen und dokumentarischen Breite gewinnen die kritisch wichtigen Funktionen (kwF) als Grundlage für die gezielte Umsetzung an überragender Bedeutung.

Die kritisch-wichtigen Funktionen (kwF)

Ein zentraler Schritt besteht in der Identifikation der kritisch wichtigen Funktionen (kwF) im DORA-Kontext. Versicherungsunternehmen haben diese Funktionen zwar identifiziert, der Reifegrad ihrer Umsetzung entspricht jedoch vielfach noch nicht den aufsichtlichen Erwartungen. Im zweiten Schritt bedarf es einer Identifikation der Drittdienstleister, die die kritisch wichtigen Funktionen unterstützen.

Im Rahmen von DORA sowie der zugehörigen RTS (Regulatory Technical Standards) wird an mehreren Stellen auf »kritische oder wichtige Funktionen« verwiesen.

- Für solche Funktionen gelten erhöhte Anforderungen, insbesondere im Hinblick auf IKT-Dienstleistungen und IKT-Assets, die sie unterstützen.
- Die Klassifikation selbst ist neu und muss daher innerhalb jeder Organisation systematisch durch geeignete Verfahren identifiziert werden.

Wortlaut gemäß Art. 3 Nr. 22 DORA:

- Funktionen, deren Ausfall die finanzielle Leistungsfähigkeit oder die Solidität bzw. Fortführung der Geschäftstätigkeit erheblich beeinträchtigen würde.
- Funktionen, deren Störung oder Nichterfüllung die Einhaltung regulatorischer Anforderungen oder Zulassungsbedingungen wesentlich gefährden würde.

Die korrekte Identifikation kritisch wichtiger Funktionen bildet die Basis für zahlreiche nachgelagerte Verpflichtungen im Rahmen von DORA.

Evaluierung der kwF

Für kritisch oder wichtig eingestufte Funktionen bestehen erhöhte Anforderungen in Bezug auf die digitale operationale Resilienz.

- **Strategische Erwägungen:** Die Unternehmensstrategie ist stärker auf Risiken auszurichten, die kritisch oder wichtige Funktionen betreffen.
- **IKT-Governance:** Änderungen in der Struktur oder den Meldewegen müssen hinsichtlich ihrer Auswirkungen auf diese Funktionen berücksichtigt werden.
- **IKT-Risikomanagementrahmen:** Die digitale Resilienz-Strategie muss IKT-Risiken adressieren, KPIs definieren, die IKT-Referenzarchitektur erklären und den Status der Resilienz (inkl. gemeldeter Incidents) darstellen.
- **IKT-Incidents:** Die Klassifizierung und Behandlung von Vorfällen richten sich nach der Kritikalität der betroffenen Funktionen.
- **IKT-Testing:** Systeme, die kritisch wichtige Funktionen unterstützen, sind mindestens jährlich zu testen.
- **IKT-Dienstleister:** Verträge müssen die erweiterten DORA-Anforderungen berücksichtigen, etwa höhere Informationssicherheitsstandards und Exit-Strategien.
- **Business-Continuity-Management:** BC-Pläne müssen ausdrücklich die Aufrechterhaltung kritisch wichtiger Funktionen sicherstellen.

Durch ein methodisch fundiertes Vorgehen lassen sich Fehlklassifikationen vermeiden und kritisch wichtige Funktionen prüfungssicher herleiten.

Lösungsansatz

Durch ein methodisch fundiertes Vorgehen lassen sich Fehlklassifikationen vermeiden und kritisch wichtige Funktionen nachhaltig sowie prüfungssicher ableiten. Die Herleitung erfolgt idealerweise in mehreren Schritten:

1. Inventarisierung: Erfassung aller wesentlichen Geschäftsprozesse, Systeme und abhängigen IKT-Assets.
2. Analysefall I – Ausfälle: Bewertung der Auswirkungen potenzieller Ausfälle auf Geschäftskontinuität, Finanzergebnisse und Kundenschutz.

3. Analysefall II – Pflichtverletzungen: Untersuchung, in welchen Fällen die Nichterfüllung regulatorischer oder vertraglicher Pflichten zu erheblichen Risiken führt.
4. Ermittlung kritisch und wichtiger Funktionen: Klassifikation auf Basis der identifizierten Auswirkungen und regulatorischen Kriterien gemäß Art. 3 Nr. 22 DORA.
5. Anwendung im DORA-Kontext: Ableitung der entsprechenden Governance-, Reporting- und Kontinuitätsanforderungen für alle identifizierten kritisch wichtigen Funktionen.

Praxis-Learnings

DORA-Audits

Die ersten Erfahrungen aus DORA-Audits zeigen, dass theoretisch etablierte Governance-Strukturen in der Praxis oft nicht ausreichend dokumentiert sind und gelebte Prozesse nur schwer nachweisbar sind. Gleichzeitig fehlt es häufig an einer strategischen Integration von ICT-Themen in das Vorstand-Reporting sowie an klaren Entscheidungsprozessen auf höchster Ebene. Auch die sogenannte Legal Entity View wird in der Praxis unterschätzt: Ein Outsourcing an Schwester- oder Muttergesellschaften mag operativ effizient sein, erfordert jedoch weiterhin eine strikte Kontrolle, Übersicht und Entscheidungsbefugnisse auf der Ebene der einzelnen juristischen Einheit. Zudem ist eine enge Kollaboration zwischen Resilience-Teams und IT-Abteilungen essenziell, damit Strategien, Verantwortlichkeiten und Risikoeinschätzungen nahtlos Hand-in-Hand gehen. Schließlich muss das Management von ICT-Providern zentralisiert werden, wobei die 2nd Line of Defence (Information Security, Resilience, Risk) klar definiert und deren Rollen präzise abgestimmt werden.

DORA-Audits vs. IT-Audits

Die Parallelen zwischen DORA-spezifischen und traditionellen IT-Audit-Anforderungen verdeutlichen die Notwendigkeit eines integrierten Ansatzes:

	Anforderungen aus dem DORA-Audit		Anforderungen aus dem klassischen IT-Audit
6.8.5	Berichte über IKT-Vorfälle und Präventionsmaßnahmen	U3.1	Übersicht über wichtige Ereignisse im IT-Bereich
6.7.1	Ergebnisse und Berichte von IKT-Prüfungen	U3.2	Externe und interne IT-bezogene Prüfungsberichte
8.1.1	Bestandsaufnahme aller IKT-gestützten Geschäftsfunktionen, Rollen und Zuständigkeiten	U1.7	Bestandsliste der IT-Anwendungen

	Anforderungen aus dem DORA-Audit		Anforderungen aus dem klassischen IT-Audit
17.1.1	Verfahren zur Bearbeitung von IKT-bezogenen Vorfällen	4.1 CO-2.1	Beschreibung des Prozesses zum Vorfall- und Problemmanagement
9.4.3.6	Leitfaden für die Beschaffung, Entwicklung und Wartung von IKT-Systemen	3.1 PD -1.1	Leitlinien für die Beschaffung und Entwicklung neuer Software

Diese Gegenüberstellung zeigt, dass viele DORA-Anforderungen bereits in klassischen IT-Audits verankert sind. Der Fokus liegt dabei jedoch stärker auf Resilienz, Kritikalität und ganzheitlichen Geschäftsprozessen. Die Erkenntnisse aus den Audits fließen direkt in die kontinuierliche Verbesserung ein.

Nach Abschluss der Umsetzungsprojekte beginnt die Phase der kontinuierlichen Verbesserung, in der der Reifegrad der regulatorischen Compliance fortlaufend erhöht wird. Dazu gehören insbesondere die Meldung im Informationsregister, die Besetzung zentraler Schlüsselfunktionen, die Verabschiedung von Leit- und Richtlinien sowie die Anpassung des Meldewesens. Im Anschluss folgt die operative Konsolidierung durch gezielten Kapazitätsaufbau, die Einführung von KPIs und KRIs, die Steuerung und Überwachung von Dienstleistern sowie die Etablierung toolgestützter, automatisierter Prozesse. Ergänzend werden Bedrohungsszenarien regelmäßig getestet, Transparenz über End-to-End-Prozesse hergestellt und die Risiko-Awareness im gesamten Unternehmen geschärft.

3 Die Überschneidungen der DORA und der DS-GVO

DORA ist ein branchenspezifisches Instrument zur Erhöhung der IT-Sicherheit im Finanzsektor. Mit ihrem informationssicherheitsrechtlichen Schwerpunkt tangieren die DORA-Regelungen zwangsläufig auch die Bestimmungen der DS-GVO. Dies zeigt sich insbesondere im fünften Kapitel zum Management des IKT-Drittanbieter-Risikos (Art. 28-30), in dem explizit geeignete Maßnahmen zum Schutz personenbezogener Daten gefordert werden.

Die Zielsetzungen beider Rechtsakte unterscheiden sich jedoch grundlegend: Während die DS-GVO primär den Schutz personenbezogener Daten und damit die Rechte der betroffenen Personen in den Mittelpunkt stellt, zielt DORA auf die Geschäftsfortführung von Finanzunternehmen und die Stabilität des gesamten Finanzsektors ab.

Der Verordnungsgeber hat das Verhältnis beider Rechtsakte zueinander bewusst offengelassen – trotz unterschiedlicher Zielrichtungen gibt es jedoch Überschneidungsfelder.

Vor diesem Hintergrund stellt sich die zentrale Frage: Wie lassen sich die Anforderungen beider Verordnungen kohärent umsetzen, ohne doppelte Strukturen zu schaffen oder die jeweiligen Schutzgüter zu vernachlässigen?

Die zentralen Begriffe der DORA (IKT-Dienstleistungen, kritisch wichtige Funktionen) wurden im vorherigen Kapitel ausführlich erläutert. Für das Verständnis der Überschneidungen sind nun die maßgeblichen DS-GVO-Begriffe zu definieren:

- **Personenbezogene Daten**: Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (»betroffene Person«) beziehen
- **Verarbeitung**: Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreitung oder Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichten
- **Verantwortlicher**: Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
- **Auftragsverarbeiter**: Natürliche oder juristische Person, Behörde, Einrichtung oder Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (ausschließlich auf dokumentierte Weisung des Verantwortlichen)

Diese Definitionen bilden die Grundlage für die Analyse konkreter Überschneidungsfelder zwischen beiden Verordnungen.

Praktische Schnittstellen

Die Überschneidungen ergeben sich im Drittanbieter-Risikomanagements, wo Finanzunternehmen bzw. deren IKT-Dienstleister regelmäßig personenbezogene Daten verarbeiten. DORA verweist hier an mehreren Stellen explizit auf Datenschutzanforderungen.

Explizite DORA-Verweise auf Datenschutz

Artikel	Inhalt
Art. 28 Abs. 7 lit. c)	Kündigungsrechte bei nachweislichen Schwächen des IKT-Drittdienstleisters im Risikomanagement, **insbesondere bei unzureichender Gewährleistung von Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten** (unabhängig von personenbezogenen Daten)
Art. 29 Abs. 2 Unterabs. 3	Bei Drittland-Dienstleistern für **kritische oder wichtige Funktionen** müssen EU-Datenschutzvorschriften eingehalten und wirksam durchgesetzt werden können
Art. 30 Abs. 2 lit. c)	Verträge müssen Bestimmungen über **Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit** enthalten – explizit inklusive des Schutzes personenbezogener Daten

Herausforderungen bei Drittland-Datentransfers

Die zentrale Herausforderung ergibt sich aus Art. 29 Abs. 2 DORA. Dieser fordert die Einhaltung und Durchsetzbarkeit des EU-Datenschutzrechts bei Drittland-IKT-Dienstleistern für kritische Funktionen. Die DS-GVO gilt direkt im Drittland nicht, weshalb einfache Unterwerfungserklärungen Normenkollisionen riskieren. Die Lösung liegt in Angemessenheitsbeschlüssen der EU-Kommission nach Art. 45 DS-GVO für Länder wie die Schweiz, Großbritannien oder Kanada sowie in Standardvertragsklauseln nach Art. 46 Abs. 2 DS-GVO.

Kontroverse besteht bezüglich Art. 49-Ausnahmen wie Einwilligungen: Während argumentiert wird, diese seien mit dem DORA-Schutzniveau unvereinbar, bleibt die Durchsetzung zulässig, solange das Gesamtschutzniveau von DORA nicht durch Kundeneinwilligungen unterlaufen wird. Entscheidend ist schließlich die präzise Leistungsbeschreibung in Verträgen nach Art. 30 Abs. 2 lit. c) DORA. Sie erforderteine umfassende Sachverhaltsklärung unter Einbindung aller Abteilungenund setzt eine klare Abgrenzung zwischen Auftragsverarbeitung und Verantwortlicher-Status vor AVV-Unterzeichnung voraus.

Parallelen bei Vorfallmeldungen und Risikomanagement

Neben diesen vertraglichen Anforderungen bestehen Parallelen bei Vorfallmeldungen und Risikomanagement. DORA verpflichtet zur Meldung schwerwiegender IKT-Vorfälle innerhalb von 4, 24 und 72 Stunden an Aufsichtsbehörden, während die DS-GVO Datenschutzverletzungen mit Risiko für Rechte natürlicher Personen innerhalb von 72 Stunden an Datenschutzbehörden zu melden vorschreibt. IKT-Risikomanagement nach DORA und Datenschutz-Folgenabschätzungen nach DS-GVO erfordern zudem koordinierte, aber strikt getrennte Dokumentationen – ein schlichtes Kopieren der Dokumente ist nicht ordnungsgemäß.

Fazit: Integrierter Compliance-Ansatz erforderlich

DORA und DS-GVO ergänzen sich im Drittanbieter-Management, erfordern aber präzise Abstimmung. Eine gemeinsame Geschäftsprozess-Erfassung kann als Basis dienen, während DORA- und DS-GVO-spezifische Dokumentationen strikt getrennt bleiben müssen. Die zentrale Herausforderung bei Drittland-Transfers lässt sich durch die Instrumente des DS-GVO-Kapitels V bewältigen, ohne das DORA-Schutzniveau zu unterlaufen. Ein einheitliches Compliance-Framework kann so Doppelstrukturen vermeiden und beide Schutzgüter sowohl die Geschäftsstabilität als auch den Datenschutzgleichwertig wahren.

4 KI-Einsatz in Versicherungsunternehmen

Künstliche Intelligenz eröffnet Versicherungsunternehmen enorme Chancen zur Optimierung von zentralen Geschäftsprozessen wie beispielsweise der Schadenbearbeitung, dem Underwriting oder im Beratungsprozess. Gleichzeitig erhöht sich die regulatorische Aufmerksamkeit für Risiken wie fehlerhafte Entscheidungen, Datenschutzrechtsverletzungen und Diskriminierung. Die KI-Verordnung (KI-VO) legt hier ein risikobasiertes Rahmenwerk fest, das sich direkt mit DS-GVO Art. 22 (automatisierte Entscheidungen) und DORA (IKT-Risikomanagement für kritische Funktionen) verknüpft.

Für Versicherungen sind insbesondere die branchenspezifischen Codes of Conduct nach Art. 13 KI-VO sowie die laufenden Diskussionen um die Digital-Omnibus-Verordnung relevant, die DS-GVO-Anpassungen für KI-Anwendungen anstrebt. Ein integrierter Compliance-Ansatz kann Doppelstrukturen vermeiden und gleichzeitig Wettbewerbsvorteile durch verantwortungsvolle KI-Nutzung schaffen.

Praxisbeispiele aus der Versicherungswirtschaft

Beispiel 1: Automatisierte Schadenbearbeitung – Private Krankenversicherung

Ein typischer KI-Prozess umfasst die vollständige Automatisierung der Rechnungsprüfung: Rechnungen gelangen via App ein und werden mittels OCR (Optical Character Recognition) verarbeitet. GenAI (Large Language Models) extrahiert und strukturiert Rechnungsdaten, erkennt Leistungspositionen und prüft diese automatisch gegen die Gebührenordnung für Ärzte (GOÄ) sowie die vertraglichen Deckungsbedingungen. Die Entscheidung erfolgt automatisiert – Auszahlung, Kürzung oder Weiterleitung zur manuellen Bearbeitung.

Regulatorische Relevanz: Art. 22 DSGVO (automatisierte Entscheidung zu Lasten), Art. 9 DSGVO (Gesundheitsdaten), DORA (kritische Funktion), DSFA-Pflicht.

Beispiel 2: Risikobewertung – Kfz-Haftpflicht

Bei der Neukundengewinnung analysiert KI-Führerscheindaten, Fahrzeuginformationen und Schadenfreiheitsklassen, um ein Risikoprofil zu erstellen. Automatisiert werden Prämien kalkuliert, Risikozuschläge vergeben oder Deckungen ausgeschlossen. Auch hier greift Art. 22 DS-GVO, ergänzt durch KI-VO-Transparenzpflichten und Nichtdiskriminierungsanforderungen.

Regulatorische Relevanz: Art. 22 DS-GVO (Transparenzpflichten), KI-VO(Nichtdiskriminierung).

Artikel 22 DS-GVO: Automatisierte Entscheidungen in Versicherungen

Artikel 22 DS-GVO regelt automatisierte Entscheidungen im Einzelfall, die rechtliche Wirkungen oder die betroffene Person ähnlich erheblich beeinträchtigen. Für Versicherungen gilt: Vollständig automatisierte Prozesse oder das Zusammenwirken automatisierter Schritte, die im Ergebnis eine Entscheidung erzeugen (z. B. Schadenablehnung), fallen darunter.

Rechtmäßigkeit:

- Entscheidungen zu Gunsten (Auszahlungen) immer zulässig
- Entscheidungen zu Lasten (Ablehnungen, Kürzungen) nur gegenüber Versicherungsnehmern erlaubt, nicht gegenüber versicherten Dritten
- Muss erforderlich für Vertragserfüllung sein
- Bei Einwilligung keine Einschränkungen
- Gesundheitsdaten (Art. 9) erfordern zwingend Einwilligung

Transparenzpflichten: Information über automatisierte Entscheidungen inklusive Logik (»ob« und »wie«) sowie Betroffenenrechte (»was jetzt«). Praktisch umgesetzt über erweiterte Datenschutzhinweise in Ablehnungsschreiben.

Prozessuale Anforderungen: »Human in the loop« – auf Verlangen menschliche Überprüfung prozessual verankern; vollständige Dokumentation der Entscheidungsgründe für Audits.

Schritte zum verantwortungsvollen KI-Einsatz in Versicherungen

Schritt 1: Keine verbotenen KI-Anwendungen

Vor dem Einsatz ist eine Prüfung nach Anhang I der KI-VO erforderlich. Verboten sind etwa Echtzeit-Biometrie zur Schadenprüfung oder soziale Scoring-Systeme zur Prämienberechnung, die diskriminierende Effekte erzeugen könnten.

Schritt 2: Transparenz und Kommunikation

Offene Bekanntgabe des KI-Einsatzes in Datenschutzerklärungen und Ablehnungsschreiben ist verpflichtend. Die Erklärbarkeit der Entscheidungslogik muss technisch und organisatorisch gewährleistet sein, damit Versicherte die wesentlichen Entscheidungsgründe nachvollziehen können.

Schritt 3: Verantwortlichkeit und Genauigkeit

Kontinuierliche Überwachung der KI-Systeme im produktiven Betrieb erkennt Abweichungen vom beabsichtigten Verhalten frühzeitig. Automatisierte Alerting-Systeme und regelmäßige Validierungen stellen die Modellgenauigkeit sicher.

Schritt 4: Sicherheit und Resilienz

Die DORA-Anforderungen an kritische Funktionen (jährliches Penetrationstesting, Incident Response innerhalb 4, 24 und 72 Stunden) müssen erfüllt werden. Redundanzkonzepte minimieren Ausfälle bei KI-gestützter Schadenbearbeitung.

Schritt 5: Nichtdiskriminierung

Bias-Audits prüfen Trainingsdaten und Modell-Outputs regelmäßig. Faire Modellarchitekturen verhindern nachteilige Behandlung bestimmter Kundengruppen (z. B. nach Wohnort oder Beruf).

Schritt 6: Datenschutz

Datenminimierung schränkt die verarbeiteten Schadensmerkmale auf relevante Merkmale ein. Pseudonymisierung und DSFA bei hohem Risiko sind zwingend; Art. 22 DS-GVO-Konformität muss dokumentiert werden.

Schritt 7: Menschliche Kontrolle

Risikobasierte Stichprobenkontrolle (z. B. 10 Prozent hochrisikoreicher Fälle) und klare Eskalationskriterien gewährleisten »Human in the loop«. Automatisierte Audit-Trails ermöglichen Nachverfolgbarkeit.

Verantwortungsvoller KI-Einsatz als Wettbewerbsvorteil

KI in der Versicherungswirtschaft erfordert die gleichzeitige Einhaltung von KI-VO, DS-GVO Art. 22, DORA und den branchenspezifischen Codes of Conduct. Ein einheitliches Compliance-Framework mit zentraler Geschäftsprozesserfassung, risikobasierter Dokumentation und »human in the loop« schafft Rechtssicherheit und Effizienz. Verantwortungsvoller KI-Einsatz positioniert Versicherer als innovative, Compliance-starke Marktteilnehmer.

5 Abgrenzung der Regulierungen mit besonderem Blick auf den CRA

Die europäische Digitalregulierung umfasst inzwischen mehrere miteinander verbundene Regelungsbereiche. Neben DORA, der DS-GVO und der KI-VO ist auch die Cybersicherheit digitaler Produkte durch den Cyber Resilience Act (CRA) geregelt. Für ein einheitliches Verständnis ist zunächst zu unterscheiden, welcher Rechtsakt welche Schutzrichtung verfolgt und an welchem Punkt er in der digitalen Wertschöpfungskette ansetzt.

Während DORA die digitale operationale Resilienz von Finanzunternehmen regelt, schützt die DS-GVO personenbezogene Daten, die KI-VO den Einsatz von KI-Systemen und der CRA die Cybersicherheit von Produkten mit digitalen Elementen. Gerade für Versicherungsunternehmen ist diese Abgrenzung wichtig, weil sie als Nutzer, Betreiber und Auftraggeber digitaler Systeme von mehreren dieser Regelungen zugleich betroffen sein können

Beispiele

- **DORA:** Ausfall des Policy-Admin-Systems (PAS) führt zu Zahlungsunfähigkeit → kritische Funktion (Art. 3 Nr. 22)
- **DS-GVO**: Automatisierte Schadenablehnung bei Krankenversicherung → Art. 22 + Gesundheitsdaten (Art. 9)
- **KI-VO:** GenAI strukturiert Rechnungsdaten für Deckungsprüfung → Transparenzpflichten + menschliche Kontrolle
- **CRA:** Cloud-Plattform für Schadenbearbeitung ohne CE-Kennzeichnung → Lieferanten müssen Konformität nachweisen.

CRA - Regelungsgegenstand: Produkte mit digitalen Elementen

Der Cyber Resilience Act (CRA) regelt Produkte mit digitalen Elementen gemäß Art. 3 Nr. 1 CRA: *Ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden*. Der Anwendungsbereich umfasst Hardware (IoT-Geräte, Computer, Wearables) und Software (Betriebssysteme, Apps, Open-Source-Komponenten), sofern sie schnittstellenbasierte Konnektivität beinhalten – kabelgebunden oder kabellos.

Kernkriterium: Bestimmungsgemäße oder vernünftigerweise vorhersehbare logische/physische Datenverbindung mit Geräten/Netzen (Art. 3 Nr. 10 CRA). Beispiele

sind vernetzte Smart-Home-Geräte, Wearables oder cloudbasierte Steuerungssysteme.
Ausgenommen: Reine Offline-Software, analoge Telefondienste.

Besonderheit FOSS: Freie und quelloffene Software unterliegt CRA nur bei kommerziellem Vertrieb – Innovationen bleiben geschützt.

Relevanz für Versicherungsunternehmen: CRA gilt NICHT direkt für Versicherer, sondern deren IKT-Lieferanten:

Betroffene Produkte in Versicherungen:

- Policy-Admin-Systeme (PAS):
  - z. B. Systeme zur Vertragsverwaltung, Policierung, Bestandsführung, Beitragsberechnung und Vertragsänderung
- Schadenbearbeitungssoftware
  - z. B. Tools zur Schadenmeldung, Schadenprüfung, Dokumentenverarbeitung, automatisierten Regulierung oder Betrugserkennung
- Cloud-Plattformen (IaaS/PaaS/SaaS)
  - z. B. Hosting- und Infrastrukturplattformen, cloudbasierte CRM-, Datenanalyse-, Collaboration- oder Workflow-Lösungen
- KI-gestützte Risikomodelle
  - z. B. Modelle für Underwriting, Tarifierung, Risikoselektion, Betrugserkennung, Storno-Prognosen oder Schadenprognosen
- Dokumenten- und Datenverarbeitungssysteme
  - z. B. OCR-Lösungen, Input-Management-Systeme, elektronische Akten, Datenextraktions- und Klassifikationstools
- Zahlungs- und Inkassosysteme
  - z. B. Systeme zur Beitragszahlung, Auszahlung von Versicherungsleistungen, Mahnverfahren oder Zahlungsabwicklung
- Telematik-, IoT- und Wearable-Anwendungen
  - z. B. Kfz-Telematik, Smart-Home-Sensorik, Gesundheits- oder Fitnessdaten-Anwendungen, soweit sie in Versicherungsprodukte eingebunden sind
- Schnittstellen- und API-Management-Systeme
  - z. B. Anbindungen an Vergleichsportale, Maklerpools, Partnerplattformen, Open-Finance-Ökosysteme oder externe Datenanbieter
- Cybersecurity- und Monitoring-Lösungen
  - z. B. Systeme für Security Monitoring, SIEM, Schwachstellenmanagement, Identity & Access Management oder Incident Response.

Kernanforderungen:

- Security-by-Design: Cybersicherheit ab Entwicklung

- Schwachstellenmanagement: Kontinuierliche Updates
- CE-Kennzeichnung: Für EU-Marktzugang
- Risikoklassen: Kritisch/Wichtig/Sonstige

DORA und CRA-Schnittstellen

DORA (Finanzinstitut)	CRA (IKT-Provider)
kwF-Identifikation (Art. 3)	Kritische Produkte (Class I/II)
IKT-Drittanbieter-Risiko (Art. 28-30)	Konformitätsbewertung/CE-Marke
Incident-Meldung (4/24/72h)	Schwachstellen-Meldepflicht
Jährliches Testing	Sicherheitsupdates

Die DORA Art. 30 verlangt bereits heute, dass Verträge mit IKT-Drittdienstleistern die Konformität mit aufsichtsrechtlichen Standards nachweisen. Mit dem Cyber Resilience Act (CRA) wird diese Pflicht konkretisiert: Lieferanten müssen CRA-Konformität ihrer Produkte nachweisen – inklusive CE-Kennzeichnung, technischer Dokumentation und Schwachstellenmanagement. Versicherungsunternehmen stehen vor der Herausforderung, diese neuen Anforderungen proaktiv in bestehende DORA-Prozesse zu integrieren.

Praktische Umsetzungsschritte:

1. Lieferanten-Audit erweitern: CE-Kennzeichnung + CRA-Dokumentation verlangen
2. Vertragsklauseln: Nachweis von Schwachstellenmanagement + Update-Strategie
3. Risikobewertung: CRA-Status in DORA-IKT-Register aufnehmen
4. Incident-Koordination: Abstimmung DORA/CRA-Meldepflichten

6 Digital-Omnibus-Verordnung: Aktueller Stand und Ausblick

Die Digital-Omnibus-Verordnung strebt wesentliche Anpassungen der DS-GVO an den technologischen Fortschritt an, um Rechtssicherheit für KI-Anwendungen zu schaffen. Sie adressiert drei zentrale Bereiche, deren Umsetzung jedoch politisch umstritten bleibt:

1. Automatisierte Entscheidungsfindung (Art. 22 DS-GVO):
Der Vorschlag klärt, dass automatisierte Entscheidungen zulässig sind, wenn sie »für den Abschluss oder die Erfüllung eines Vertrags mit der betroffenen Person erforderlich« sind – unabhängig davon, ob die Entscheidung theoretisch auch manuell getroffen werden könnte. Diese Klarstellung würde Versicherungsunternehmen erhebliche Rechtssicherheit bieten, da viele Schadenbearbeitungs- und Deckungsprüfungsprozesse genau diese Kriterien erfüllen. Der Positionierungsentwurf des Rates lehnt diese Liberalisierung jedoch ab und lässt die derzeitige Rechtsunsicherheit bestehen.

2. Künstliche Intelligenz und Rechtsgrundlagen:
Ein neuer **Art. 88c D-SGVO** soll kodifizieren, dass **berechtigtes Interesse** (Art. 6 Abs. 1 lit. f DS-GVO) als Rechtsgrundlage für die Entwicklung und den Betrieb von KI-Systemen zulässig ist. Die allgemeinen Anforderungen an die Interessensabwägung und DS-GVO-Grundsätze würden weiterhin gelten, ergänzt um ein uneingeschränktes Widerspruchsrecht und »enhanced transparency«. Kritisch wird gesehen, dass unklar bleibt, ob dies eine eindeutige Rechtsgrundlage schafft oder nur die Aussicht auf ein berechtigtes Interesse regelt. Die pauschale Einschränkung »where appropriate« führt zu weiterer Rechtsunsicherheit.

Zusätzlich soll **Art. 9 DS-GVO** erweitert werden, um besondere Kategorien personenbezogener Daten (z. B. Gesundheitsdaten für Risikomodelle) für KI-Entwicklung nutzbar zu machen – unter strengen Auflagen für Schutzmaßnahmen wie Pseudonymisierung und DSFA. Insgesamt könnten diese Regelungen die KI-Entwicklung in Europa deutlich vereinfachen und stärken, wobei eine Klarstellung in den genannten Punkten wünschenswert wäre.

3. Personenbezug von Daten (Art. 4 Nr. 1 DS-GVO):
Die weitreichendste Änderung betrifft ein **relatives Verständnis von personenbezogenen Daten**: »Informationen, die sich auf eine natürliche Person beziehen, sind nicht allein deshalb für jede andere Person oder Stelle personenbezogene Daten, nur weil eine andere Stelle diese natürliche Person identifizieren kann.« Dies würde pseudonymisierte Daten aus dem DS-GVO-Anwendungsbereich nehmen, wenn für den konkreten Verantwortlichen kein Identifizierungsrisiko besteht.

Ein neuer **Art. 41a DS-GVO** ermächtigt die EU-Kommission, Kriterien und Methoden festzulegen, wann pseudonymisierte Daten für bestimmte Akteure nicht mehr personenbezogen gelten. **Vorteile**: Massive Reduktion von Compliance-Aufwänden bei Daten, die de facto kein Risiko für natürliche Personen bergen (z. B. aggregierte

Schadensdaten). **Risiken**: Gefahr, dass schutzbedürftige pseudonyme Daten aus der DS-GVO fallen; unklare Grenzziehung erfordert mehr Schärfe.

Aktueller Stand: Laut neuesten Berichten lehnt der Rat diese grundlegenden Änderungen ab, was die bestehende regulatorische Unsicherheit für KI-Anwendungen in der Versicherungswirtschaft verlängert. Für Versicherer bleibt ein **pragmatischer, risikobasierter Compliance-Ansatz** essenziell, bis politische Klarheit geschaffen ist

Die Digital-Omnibus-Verordnung soll DS-GVO-Anpassungen für KI-Anwendungen schaffen, steht jedoch unter politischem Druck. Zur automatisierten Entscheidungsfindung sollte klargestellt werden, dass Vertragserfüllung auch bei theoretisch manueller Möglichkeit zulässig ist – der Rat lehnt dies aktuell ab.

Aktueller Stand: Der Positionierungsentwurf des Rates lehnt diese grundlegenden Änderungen ab, was die bestehende regulatorische Unsicherheit für KI-Anwendungen in der Versicherungswirtschaft verlängert. Für Versicherer bleibt ein pragmatischer, risikobasierter Compliance-Ansatz essenziell, bis politische Klarheit geschaffen ist.

Regulatorische Überschneidungen als Compliance-Chance

Die gemeinsame Basis aller digitalen Regulierungen bildet der Geschäftsprozess selbst. DORA verlangt gemäß Art. 28 ein IKT-Informationsregister, das Funktion, Kritikalität und Gründe für die Einstufung (etwa »B_06_01 – Hochkritisch – Ausfall führt zu Liquiditätsengpässen«) sowie die Differenzierung zwischen ICT-Providern und Betreibern erfasst.

Die DS-GVO fordert nach Art. 30 ein Verzeichnis Verarbeitungstätigkeiten, das personenbezogene Daten, Verarbeitungszwecke und notwendige Auftragsverarbeitungsverträge (AVV) dokumentiert.

Die KI-VO ergänzt dies durch ein KI-Register mit detaillierten Risikoeinschätzungen und Zweckdefinitionen für KI-Systeme.

Ein einheitliches Risikomanagement kann hierbei mehrere Dimensionen gleichzeitig abdecken – von Operationellem Risiko über Compliance-Risiken bis hin zu AML-Risiken und Datenschutzrisiken. Auch Rollen- und Rechtemanagement, etwa die Zuweisung von Edit-Rechten in Geschäftsprozess 123 mit der Frage nach notwendiger DSFA-Unterstützung, lässt sich zentral erfassen. Gleiches gilt für das Dienstleister-Management, das AVV-Pflichten mit DORA-Provider-Registrierung und KI-VO Anforderungen verknüpft.

Diese Überschneidungen bieten eine einzigartige Chance für ein integriertes Compliance-Framework, das parallele Silo-Lösungen vermeidet und stattdessen die vorhandenen Dokumentationsinfrastrukturen nutzt. Die detaillierte Gegenüberstellung zeigt, dass ein solcher einheitlicher Ansatz für DORA, DS-GVO und KI-VO nicht nur möglich, sondern zwingend erforderlich.

7 Forderungen für einen einheitlichen Compliance-Rahmen

Die europäische Digitalregulierung stellt Versicherer und InsurTechs zunehmend vor die Herausforderung, mehrere Regelungsregime gleichzeitig umzusetzen. Mit DORA, der DS-GVO und der KI-Verordnung treffen Anforderungen an digitale operationale Resilienz, Datenschutz, Datenverarbeitung, automatisierte Entscheidungen und KI-Governance in der Praxis häufig auf dieselben Geschäftsprozesse, Systeme und Datenbestände. Dadurch entstehen Überschneidungen, parallele Dokumentationspflichten, unterschiedliche Begrifflichkeiten und Unsicherheiten bei der praktischen Umsetzung.

Gerade im Versicherungsumfeld wird deutlich, dass digitale Geschäftsmodelle nicht entlang regulatorischer Silos funktionieren. Prozesse wie Underwriting, Schadenbearbeitung, Betrugserkennung, Kundenkommunikation oder Risikobewertung können zugleich IKT-relevant, datenschutzrechtlich sensibel und KI-gestützt sein. Für Unternehmen ist daher entscheidend, dass regulatorische Anforderungen nicht isoliert nebeneinanderstehen, sondern kohärent miteinander verzahnt werden.

Vor diesem Hintergrund braucht es eine praxisnahe Logik, die gemeinsame Anknüpfungspunkte schafft, Auslegungsunsicherheiten reduziert und integrierte Compliance-Ansätze ermöglicht. Ziel sollte sein, Informationen zu Geschäftsprozessen, Datenarten, IKT-Systemen, Kritikalität, KI-Einsatz und Verantwortlichkeiten strukturiert zu erfassen und regimeübergreifend nutzbar zu machen – ohne die jeweiligen materiellen Anforderungen von CRA, DORA, DS-GVO und KI-VO abzuschwächen.

Mit PRISMA schlagen wir hierfür einen kohärenten Forderungsrahmen vor. PRISMA steht für Prozessbasis, abgestimmte Begriffe, koordinierte Meldungen, risikobasierte Skalierung, wirksame menschliche Kontrolle und prüfbare Assurance – als gemeinsame Logik zur Verzahnung von CRA, DORA, DS-GVO und KI-VO. Der Ansatz soll dazu beitragen, Regulierung wirksamer, verständlicher und umsetzbarer zu machen und zugleich Innovation, Rechtssicherheit und verantwortungsvolle digitale Anwendungen in der Versicherungswirtschaft zu stärken. P-R-I-S-M-A: PRISMA steht für Prozessbasis, abgestimmte Begriffe, koordinierte Meldungen, risikobasierte Skalierung, wirksame menschliche Kontrolle und prüfbare Assurance – als kohärente Logik zur Verzahnung von CRA, DORA, DS-GVO und KI-VO.

1. Gemeinsame Geschäftsprozesslogik als sinnvoller Anknüpfungspunkt

Wir sprechen uns dafür aus, die Umsetzung von CRA, DORA, DS-GVO und KI-Verordnung stärker an einer gemeinsamen Geschäftsprozess- und Systemlogik auszurichten.

Informationen zu Geschäftsprozessen, Datenarten, IKT-Systemen, Kritikalität und KI-Einsatz könnten strukturiert einmal erhoben und – unter Wahrung der jeweiligen materiellen Anforderungen – regimeübergreifend genutzt werden.

Dies würde Konsistenz schaffen und integrierte Compliance-Ansätze praktikabler machen.

2. Bessere Abstimmung zentraler Begriffe und Bewertungsmaßstäbe

Wir halten es für sinnvoll, zentrale Begriffe und Risikokategorien der Digitalregulierung stärker aufeinander abzustimmen bzw. eindeutiger zueinander ins Verhältnis zu setzen.

Insbesondere betrifft dies kritisch wichtige Funktionen, hochriskante KI-Systeme, automatisierte Entscheidungen sowie Rollenabgrenzungen.

Klarere Abgrenzungen könnten Auslegungsunsicherheiten reduzieren und die Umsetzung deutlich erleichtern.

3. Koordinierte und praxistaugliche Vorfallmeldungen

Wir sprechen uns für eine stärkere Koordinierung der Vorfallmeldepflichten aus CRA, DORA, DS-GVO und KI-Verordnung aus.

Ein gemeinsamer Kern an Meldeinformationen mit klar abgegrenzten Ergänzungen für die jeweiligen Regime könnte Prozesse verschlanken und zugleich die Qualität der Meldungen erhöhen.

4. Proportionalität konsequent an Kritikalität ausrichten

Wir befürworten eine konsequente Anwendung des Proportionalitätsprinzips, insbesondere durch eine klare Fokussierung auf kritisch wichtige Funktionen.

Einheitlichere aufsichtliche Erwartungen zur Identifikation und Bewertung dieser Funktionen würden dazu beitragen, Regulierung zielgerichtet dort wirken zu lassen, wo tatsächliche Risiken bestehen. Beispielsweise sollte bei Unternehmen, die nur aufgrund einer versicherungsvermittelnden Nebentätigkeit von DORA erfasst werden, die Anwendung vereinfachter Anforderungen ausschließlich anhand des Umsatzes aus der Versicherungsvermittlung beurteilt werden. Der Umsatz aus dem nicht-finanziellen Hauptgeschäft sollte hierfür nicht maßgeblich sein. Dadurch würde DORA stärker an der tatsächlichen Finanzmarktrelevanz ausgerichtet und überflüssiger administrativer Aufwand vermieden.

5. Klarere Leitplanken für automatisierte Entscheidungen

Wir sprechen uns für mehr Klarheit bei der Anwendung von Art. 22 DS-GVO im Versicherungsumfeld aus, insbesondere bei automatisierten Entscheidungen im Rahmen der Vertragserfüllung.

Eine präzisere Einordnung könnte die Verzahnung von DS-GVO und KI-Verordnung erleichtern und den Weg für verantwortungsvolle KI-Anwendungen unter klaren rechtlichen Rahmenbedingungen ermöglichen. Aus unserer Sicht wäre es hilfreich, den Begriff der »ausschließlich automatisierten Entscheidung« weiter zu präzisieren und dabei klarzustellen, wann eine menschliche Beteiligung tatsächlich als wirksam anzusehen ist.

6. Einheitliche Governance-, Nachweis- und Verantwortlichkeitslogik

Wir sprechen uns dafür aus, die Umsetzung von CRA, DORA, DS-GVO und KI-Verordnung durch eine einheitliche Governance- und Assurance-Logik zu flankieren. Regulatorische Anforderungen an Dokumentation, Nachweisführung, Audit-Trails und Verantwortlichkeiten könnten stärker aufeinander abgestimmt werden, um integrierte Compliance-Ansätze dauerhaft prüf- und betreibbar zu machen.

8 Fazit

Die digitale Versicherungswirtschaft steht an einem Punkt, an dem regulatorische Anforderungen nicht mehr isoliert betrachtet werden können. Obwohl DORA, DS-GVO und KI-Verordnung unterschiedliche Ziele verfolgen, treffen sie in der Praxis aber häufig auf dieselben Prozesse, Systeme, Daten und Dienstleister. Versicherungsunternehmen sind daher gezwungen, Compliance nicht mehr länger entlang einzelner Rechtsakte, sondern entlang realer Geschäftsprozesse und Risikozusammenhänge zu organisieren.

Ein integrierter Compliance-Ansatz ist dabei mehr als eine Effizienzmaßnahme. Er schafft die Grundlage für rechtssichere Innovation, belastbare Governance und vertrauenswürdige digitale Geschäftsmodelle. Gerade bei KI-gestütztem Underwriting, automatisierter Schadenbearbeitung, digitaler Kundeninteraktion und Drittanbietersteuerung entscheidet die Fähigkeit zur kohärenten Umsetzung regulatorischer Anforderungen darüber, ob digitale Innovationen skalierbar und verantwortungsvoll eingesetzt werden können.

Der europäische Gesetzgeber und die Aufsichtsbehörden sollten diese Entwicklung aktiv unterstützen, auch um internationale Wettbewerbsfähigkeit anzustreben.

Die zentrale Aufgabe von Versicherern und InsurTechs besteht darin, ihre Prozess-, Daten-, IKT- und KI-Governance stärker miteinander zu verzahnen. Wer regulatorische Anforderungen frühzeitig integriert, schafft nicht nur Compliance-Sicherheit, sondern auch einen Wettbewerbsvorteil: durch schnellere Umsetzung, bessere Steuerbarkeit, höhere Resilienz und größeres Vertrauen bei Kundinnen und Kunden sowie der Aufsicht.

Mit PRISMA schlägt Bitkom eine kohärente Logik für diesen nächsten Schritt vor. Der Ansatz verbindet Prozessbasis, abgestimmte Begriffe, koordinierte Meldungen, risikobasierte Skalierung, wirksame menschliche Kontrolle und prüfbare Assurance zu einem Rahmen, der digitale Regulierung wirksamer, verständlicher und umsetzbarer machen kann.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Elena Kouremenou | Referentin Datenschutz
T +49 30 27576-425 | e.kouremenou@bitkom.org

Lukas Spohr | Referent Digitale Transformation
T +49 30 27576-340 | l.spohr@bitkom.org

Autorinnen und Autoren
Frank Fischer | Hiscox SA; Fabio Herrmann | Deloitte GmbH;
Sofie Kasperek | Deloitte GmbH; Martin Lippert | Deloitte GmbH;
Nils Osterhoff | Markel Insurance SE; Romina Pierce | Sixsentix Deutschland GmbH;
Matthias Rasking | Sixsentix Deutschland GmbH; Pascal Schwarze | Deloitte GmbH

Verantwortliches Bitkom-Gremium
AK Datenschutz
AK Digital Insurance & InsurTech

Copyright
Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.