

Cybersicherheit und Künstliche Intelligenz

Aktuelle Herausforderungen und Chancen für die
Versicherungswirtschaft zur sicheren Kundenbetreuung



Q: "Lassen Sie es mich so formulieren: Ich richte im Pyjama am Laptop noch vor meiner ersten Tasse Earl Grey mehr Schaden an, als Sie in einem Jahr Außeneinsatz."

Who am I?

„The normal one.“

BJ 1987 – verheiratet – 1 Tochter

Gesells.-GF Audeca GmbH, Lemgo

Gesells.-GF S.M.I. Lemgo UG (haftungsb.), Lemgo

Ganz viel IT (seit 2006)

- Ausbildung Fachinformatiker
- Studium Angewandte Informatik (B.Sc.)
- Studium Wirtschaftsinformatik (M.Sc.)
- IT-Abteilungsleiter LK Nienburg/Weser
- Speziell: Cybersecurity, Datenschutz und Digital-Beratung



Kontakt Daten

Philipp Meyer

Mail: philipp.meyer@audeca.de

Tel.: 05261 943238-1

www.audeca.de

Audeca GmbH

IT-Service	Datenschutz	Digitalisierung
Server- und Netzwerktechnik Arbeitsplätze Software Schulung Support	Ext. Datenschutzbeauftragter (TÜV) Ext. Datenschutzauditor (TÜV) Beratung Cybersecurity Schulung	Individual-Software-Entwicklung Beratung Digitalisierung Projekt- und Prozessmanagement Schulung

*Aktuell: Betreuung von rund 80 Kunden im KMU-Segment im Raum OWL. Etwa 750 Arbeitsplätze und 80 Server.
Davon 15 Unternehmen mit etwa 200 Personen im Datenschutz-/Security-Segment.*



Einstieg & Relevanz

Begriffsdefinition: KI & Datenschutz & Cybersicherheit

- KI = „Künstliche Intelligenz ist die Eigenschaft eines IT-Systems, »menschenähnliche«, intelligente Verhaltensweisen zu zeigen.“ (BITKOM)
- Datenschutz = Schutz vor Datenmissbrauch von *personenbezogenen* Daten
- Cybersicherheit = Schutz vor Fremdzugriff auf Daten

Warum ist die Versicherungsbranche besonders betroffen?

- Verarbeitung besonders sensibler Daten
- Hohes Automatisierungspotenzial (Schadenprüfung, Risikobewertung)
- Vertrauensabhängigkeit der Kundinnen und Kunden

Technischer Überblick zu KI

Arten von KI im Versicherungswesen:

- Klassifikation (z. B. Schadenshöhe)
- Prognosen (z. B. Krankheitsrisiken, Beitragsanpassungen)
- Natural Language Processing (z. B. Chatbots)

„Training“ mit Alt-Daten = potenziell personenbezogen

KI ≠ deterministischer Algorithmus → Risiken bei Rückverfolgbarkeit

Datenschutzrechtlicher Rahmen

DSGVO

Thema	Relevanter Artikel	Bedeutung für Versicherungen
Grundprinzipien	Art. 5	Transparenz, Datenminimierung, Speicherbegrenzung etc.
Rechtsgrundlagen	Art. 6	Vertrag, berechtigtes Interesse, Einwilligung
Gesundheitsdaten etc.	Art. 9	Verarbeitung nur mit ausdrücklicher Einwilligung (oder Ausnahme)
Profiling / automatisierte Entscheidung	Art. 22	Nur mit ausdrücklicher Einwilligung oder gesetzlicher Grundlage
Datenschutz-Folgenabschätzung	Art. 35	Bei hohem Risiko verpflichtend
Privacy by Design	Art. 25	KI-Systeme müssen von Anfang an datenschutzgerecht konzipiert sein

EU AI Act

Offizieller Name: Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz

Verabschiedung: März 2024, in Kraft 2025, vollständige Anwendung ab 2026

Ziel: Risikobasierte Regulierung von KI-Systemen im Binnenmarkt der EU

EU AI Act

Verbotene KI (Art. 5)

- Systeme mit unvertretbarem Risiko (z. B. Social Scoring, manipulative KI)
- Nicht erlaubt in der EU

Hochrisiko-KI (Art. 6 ff.)

- Z. B. KI im Personalwesen, Kreditvergabe, Justiz, kritischer Infrastruktur
- Auch relevant für Versicherungen, z. B. bei Tarifierung, Scoring, Profiling

EU AI Act

Pflichten für Versicherer bei Hochrisiko-KI

- Technische Dokumentation & Auditierbarkeit
- Erklärbarkeit & Transparenz für Betroffene
- Datenmanagement & Governance
- Meldung an Marktaufsicht
- Einbettung von Menschenkontrolle

EU AI Act

- Komplementär zur DSGVO
- Kein Ersatz, sondern Ergänzung – z. B. bei Profiling & automatisierten Entscheidungen
- Klare Verbindung zu Art. 22 DSGVO
- Regelt nicht nur Verarbeitung, sondern auch die Sicherheit, Transparenz und Kontrolle von KI-Systemen
- Marktüberwachung durch nationale Behörden + EU AI Office
- Strafen: Bis zu 35 Mio. € oder 7 % des Jahresumsatzes bei schwerwiegenden Verstößen

Herausforderungen & Risiken bei Einsatz von KI

Risiko/Herausforderung	Problem in der Praxis
Intransparenz („Black Box“)	Versicherte verstehen nicht, wie Beiträge oder Ablehnungen zustande kommen
Diskriminierung/Bias (Vorurteile)	Trainingsdaten reflektieren historische Benachteiligung (z. B. Gesundheitsrisiken bei Geschlechtern)
Automatisierte Entscheidungen	Beitragserhöhungen, Ablehnungen bei Antrag/Schadenbearbeitung
Rechtsgrundlagen fraglich	Einwilligung vs. berechtigtes Interesse – oft unsauber formuliert
DSFA notwendig, aber nicht durchgeführt	KI wird eingeführt, ohne Risikoabschätzung, obwohl sensible Daten betroffen sind

Bewertungen

Datenschutzkonferenz (DSK)

- 2023: „ChatGPT-ähnliche Systeme sind regelmäßig personenbezogen“
- Versicherungen stehen unter besonderer Beobachtung wegen Profiling und Scoring

EADS-Empfehlung: DSFA bei nahezu jeder Form von KI mit Auswirkungen auf Betroffene.

EU AI Act (2024/2025)

- Klassifiziert KI-Systeme in Risiko-Kategorien
 - **Hohes Risiko:** z. B. Kredit- und Versicherungsbewertung
 - **Pflichten:** Risikomanagement, Transparenz, menschliche Kontrolle

Basics – Basics – Basics!

- ✓ Türen und Fenster verschließen
- ✓ Geräte beim Verlassen sperren
- ✓ Virenschutz- und Firewall-System nutzen
- ✓ Verschlüsselungen nutzen
- ✓ Ausgedrucktes abheften und sicher verstauen (ggf. in verschließbaren Schränken)
- ✓ Mobile Datenträger stets sicher verstauen, keine fremden Datenträger einlesen
- ✓ Unbekannte E-Mails (mit/ohne Anhang) stets kritisch hinterfragen
- ✓ Gespräche soweit möglich vertraulich führen
- ✓ Kennwörter hinreichend komplex wählen
(min. 8 Zeichen: Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen)
- ✓ (Regelmäßiger Kennwortwechsel: 3 – 4 Mal pro Jahr) → **MFA verwenden, wenn angeboten/möglich**
- ✓ IT-Systeme aktuell halten (Updates einspielen, Produktlebenszyklen beachten ...)
- ✓ Datensicherungen anlegen und sicher verwahren (nicht nur Cloud/Online – auch Offline!)

Fallbeispiel 1

Ausgangslage:

Ein privater Krankenversicherer führt ein KI-System ein, das auf Basis von Gesundheitsdaten vergangener Jahre eine neue Risikoeinstufung vornimmt. Viele Versicherte erhalten daraufhin Beitragserhöhungen. Eine Widerspruchsmöglichkeit wird nicht angeboten.

Diskussionsfragen:

- Ist die KI-basierte Beitragsanpassung datenschutzkonform?
- Was sagt Art. 22 DSGVO dazu?
- Welche datenschutzrechtlichen Pflichten hat der Versicherer?

Musterlösung:

- Beitragserhöhung = automatisierte Entscheidung mit wesentlicher Auswirkung → Art. 22 DSGVO greift
- Widerspruchsrecht hätte eingeräumt werden müssen
- DSFA wäre zwingend erforderlich
- Rechtsgrundlage? Keine Einwilligung → problematisch, wenn nicht gesetzlich erlaubt

Fallbeispiel 2

Ausgangslage:

Ein Versicherer nutzt einen KI-gestützten Chatbot, der Schadenmeldungen entgegennimmt. Der Bot fragt unter anderem nach Ort, Datum, Beteiligten, Fotos und persönlichen Eindrücken.

Diskussionsfragen:

- Ist hier eine Einwilligung erforderlich?
- Werden besondere Kategorien personenbezogener Daten verarbeitet?
- Muss eine DSFA durchgeführt werden?

Musterlösung:

- Es werden auch sensible Daten (z. B. Gesundheitsdaten bei Unfall) erfasst → Art. 9 DSGVO
- Einwilligung muss ausdrücklich und spezifisch sein (Checkbox reicht nicht)
- Transparenzpflichten (Art. 13) sind relevant → Erklärung, was mit den Daten passiert
- DSFA notwendig → Schadenfälle betreffen große Personenzahl und sensible Daten

Fallbeispiel 3

Ausgangslage:

Ein Lebensversicherer setzt ein KI-System ein, das Vorhersagen trifft, ob Versicherte ihren Vertrag kündigen könnten. Auf dieser Basis werden gezielt Rabatte oder Anrufe durch den Vertrieb ausgelöst.

Diskussionsfragen:

- Ist das Profiling im Sinne der DSGVO?
- Dürfen solche Daten zu Marketingzwecken genutzt werden?
- Welche Informationspflichten hat der Versicherer?

Musterlösung:

- Profiling liegt vor (Art. 4 Nr. 4 DSGVO), da Verhalten vorhergesagt wird
- Marketingmaßnahmen auf dieser Grundlage brauchen eine saubere Rechtsgrundlage (oft: berechtigtes Interesse, Art. 6 Abs. 1 lit. f DSGVO – aber mit Interessenabwägung!)
- Informationspflichten: Betroffene müssen über Profiling und Zweck informiert werden (Art. 13/14 DSGVO)
- Transparenz entscheidend, sonst droht Bußgeld

Fazit

- ✓ KI bietet enormes Potenzial – auch in der Versicherungswelt
- ✓ DSGVO & AI Act setzen klare Leitplanken
- ✓ Transparenz, DSFA, Rechtsgrundlage & Betroffenenrechte sind Schlüssel
- ✓ Frühzeitige Einbindung von Datenschutzbeauftragten verhindert spätere Rechtsverstöße

**Vielen Dank
für Ihre Aufmerksamkeit!**