

Compliance

Die Zeitschrift für Compliance-Verantwortliche

Oktober 2026

Inhalt



© IMAGO / imagebroker

Aufmacher

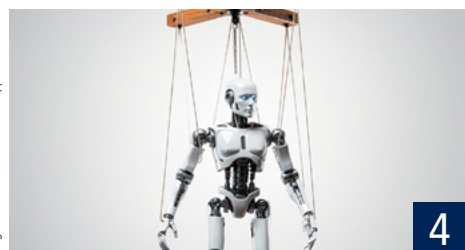
KI- und Datenschutz-Compliance in stürmischen Zeiten

KI und Datenschutz – zwei Gebiete, die zusammen gedacht werden müssen und in vielerlei Hinsicht miteinander verknüpft sind. Compliance-Experten, die sich insbesondere mit diesen Bereichen befassen, machen derzeit stürmische Zeiten durch. Dr. Frank Schemmel richtet vor diesem Hintergrund und mit Blick auf aktuelle politische Entwicklungen drei Appelle an die deutsche Bundesregierung, die Europäische Kommission, Parlament und Ministerrat zu mehr Mut, Sorgfalt und Selbstreflexion.

Recht

News

Praxis



KI-generiert / Christina Kahen-Pappas / Flux 2 Pro



© IMAGO / Imaginetha-Tuchong



© IMAGO / Edgars Sermulis

KI in der Versicherungswirtschaft: Skalierung als Governance-Aufgabe

Künstliche Intelligenz ist in der deutschen Versicherungswirtschaft längst produktiv im Einsatz: im Kundenmanagement bei Chatbots und Vertriebssteuerung, in der Schadenregulierung bei automatisierter Erstprüfung und Betrugserkennung, im Underwriting bei Risikobewertung und Tarifierung. Der Sprung vom Pilotprojekt zur unternehmensweiten Skalierung gelingt jedoch selten.

Bundesregierung bringt Reform des Kartellrechts auf den Weg

Die Bundesregierung hat im September einen Gesetzentwurf zur Reform des Kartellrechts vorgelegt. Kern ist ein innovatives Vergabescreeing, das Kartellabsprachen bei öffentlichen Aufträgen systematisch aufdecken soll.

Deutsche Compliance Konferenz 2027: Compliance zukunftssicher gestalten

EU AI Act: KI wird in Standardsoftware zum Compliance-Risiko

Der EU AI Act wird für deutlich mehr deutsche Unternehmen relevant als bislang angenommen. Diejenigen, die Standardsoftware mit integrierten KI-Funktionen einsetzen – etwa in den Bereichen Biometrie, Leistungsbewertung oder Lernanwendungen –, können unter die Vorschriften für Hochrisiko-KI-Systeme fallen. Verschiebende Fristen verschärfen die Unsicherheit bei der Umsetzung der Compliance-Anforderungen.

Veranstaltungen

Blick hinter die Kulissen der Compliance Audits

Was bei Compliance Checks wirklich zählt
Alle Ihre Fragen von Top-Auditoren beantwortet.

16. Oktober 2026, 11.00 bis 12.00 Uhr | Webinar

Eine Veranstaltung von

Compliance
Berater

und

kertos

Jetzt kostenlos
anmelden!

07.10.2026 | Frankfurt am Main | **Doppel-
lesung „Die Kehrseite“ & „Festschrift für
Bud Spencer“**

13.10.2026 | Online | **Strukturiertes Workflow
Management**

15.10.2026 | Online | **NIS-2-Pflichtschulung für
Geschäftsleitungen**

16.10.2026 | Online | **Blick hinter die Kulissen
der Compliance Audits**

22.10.2026 | Frankfurt am Main | **3. Deutscher
Beschäftigtendatenschutztag**

KI- und Datenschutz-Compliance in stürmischen Zeiten

KI und Datenschutz – zwei Gebiete, die zusammen gedacht werden müssen und in vielerlei Hinsicht miteinander verknüpft sind. Compliance-Experten, die sich insbesondere mit diesen Bereichen befassen, machen derzeit stürmische Zeiten durch. Dr. Frank Schemmel richtet vor diesem Hintergrund und mit Blick auf aktuelle politische Entwicklungen drei Appelle an die deutsche Bundesregierung, die Europäische Kommission, Parlament und Ministerrat zu mehr Mut, Sorgfalt und Selbstreflexion.



Stürmische Zeiten: Compliance-Verantwortliche müssen sich wappnen.

Zentrale Anforderungen der KI-VO und DSGVO sind Transparenzpflichten – zu Recht. Das Telos dahinter: Spezifische Informationen sind die Grundlage von Kontrolle – sei es in der Ausübung von Betroffenenrechten oder Überprüfung durch Behörden. Nach einem aktuellen Beschluss des Koalitionsausschusses soll künftig ein zentrales Element für öffentliche Transparenz und Kontrolle nun aber de facto abgeschafft werden: das Informationsfreiheitsgesetz (IFG). Es ermöglicht allen Menschen, Einblick in staatliche Dokumente zu erhalten und damit das Handeln von Behörden, Parlamenten und Regierungen nachzuvollziehen und damit zu kontrollieren. Die geplante Anpassung würde diesem bewährten Instrument faktisch den Todesstoß versetzen. Das IFG nun derart zu reformieren, dass es seinen eigentlichen Zweck nicht mehr erfüllen kann, ist kurzsichtig, steigert Korruptionsrisiken und zerstört weiter das derzeit sowieso labile Vertrauen in staatliches Handeln. Dies zeigt auch der aktuelle Demokratie-Monitor der Uni Hohenheim: Demnach glaubt gut ein Viertel der Deutschen, dass Politik in ihrem Land von geheimen Mächten gesteuert werde. Eine wehrhafte und lebendige Demokratie muss Transparenz und die daraus folgenden öffentlichen Debatten jedoch aushalten können – mein erster Appell zu mehr Mut und Selbstreflexion seitens der Regierung.

Apropos Kontrolle: Ende Juni hat der US Supreme Court in der Rechtssache „Trump v Slaughter“

einen wohl folgensweren Paradigmenwechsel vollzogen, der die Unabhängigkeit vieler US-Behörden (im konkreten Fall ging es um die Federal Trade Commission – FTC) tangieren dürfte und damit mithin der Kontrolle durch den Präsidenten unterwirft. Dies dürfte auch mittelbare Auswirkungen auf den Datenschutz haben. Die FTC nimmt die Rolle als eine der Datenschutzbehörden in den USA wahr und wird im EU-US Data Privacy Framework vielfach erwähnt. Und damit ist ein seit mehreren Jahren eigentlich totgeglaubtes Thema plötzlich wieder hochaktuell: der Datentransfer in die USA und „Schrems III“. Besagter Datenschutzaktivist (Max Schrems) hat in diesem Zusammenhang bereits angekündigt, wieder vor den EuGH zu ziehen. Die EU-Kommission täte gut daran, hier zeitnah Klarheit zu schaffen und selbstbestimmt, aber zugleich auch nachhaltig, die richtigen Weichen zu stellen, damit der EuGH nicht auch den dritten Angemessenheitsbeschluss

wieder einkassiert und für Unternehmen wieder massive Rechtsunsicherheit herrscht – mein zweiter Appell zu mehr Selbstreflexion und Sorgfalt seitens der Kommission.

Schließlich hat Ende Juni auch der Rat die Position des Europäischen Parlaments zum Digital Omnibus on AI angenommen. Kernstück ist die Verschiebung des Geltungsbeginns der Pflichten für Hochrisiko-KI-Systeme, zudem gibt es eine Abschwächung der Pflicht zur KI-Kompetenz (Art. 4 KI-VO). Letzteres ist das falsche Signal und schafft keine Erleichterung für Unternehmen, sondern ist lediglich eine Nebelkerze, die sich langfristig rächen wird. Solche Nebelkerzen finden sich auch in den aktuellen Omnibus-Debatten zur Anpassung der DSGVO und dem Abbau von Bürokratie. Anstatt die erkannten Webfehler der DSGVO zu korrigieren und somit tatsächlich Erleichterung für Unternehmen zu schaffen, wird lediglich Ergebniskosmetik betrieben – mein Dritter Appell an die Trilog-Parteien zu mehr Mut, Sorgfalt und Selbstreflexion.



Dr. Frank Schemmel, Compliance Officer (Univ.) ist Head of Privacy bei Media-MarktSaturn in Ingolstadt. Schwerpunkt seiner Arbeit sind Datenschutz, KI-Compliance, Informationssicherheit und die rechtlichen Herausforderungen der Digitalisierung.

Mehr von Dr. Frank Schemmel zu KI und Datenschutz erfahren Sie im [CB 2026, 345](#) und im [Compliance-Podcast RECHTSANWALTER & LEBENKÜNSTNER](#).



4 Wochen
kostenlos
testen!

bo.beck.de/0614310

Compliance

Immer und überall gut beraten

Drei Module für Ihren Erfolg – perfekt zugeschnitten auf Ihre Bedürfnisse. Entdecken Sie unsere Produktfamilie und wählen Sie das passende Modul.

Compliance **PLUS**

Die ideale Grundausstattung für Ihre tägliche Arbeit: Korruption, Datenschutzskandale sowie steigende gesetzliche Anforderungen machen eine systematische Compliance unabdingbar. Beste Unterstützung liefert Ihnen dabei Compliance PLUS: Mit zahlreichen Werken, u.a. **Hauschka/Moosmayer/Lösler, Corporate Compliance; Umnuß, Corporate Compliance Checklisten**, der Zeitschrift **CCZ**, den monatlichen Newsdienst Compliance sowie mit allen relevanten Gesetzestexten und aktueller Rechtsprechung erhalten Sie eine optimale Grundversorgung zu allen wichtigen Compliance-Themen.

€ 84,-/Monat* | Modulvergleich & Preise online: bo.beck.de/061431

Compliance **PREMIUM**

Für komplexe Herausforderungen und ein breiteres Meinungsspektrum: Zusätzlich zu den Inhalten des PLUS-Moduls bietet Ihnen das Modul Compliance PREMIUM weitere wichtige Spezialwerke wie z.B. **Bay/Hastenrath, Compliance-Management-Systeme; Wagner/Ruttloff/Wagner, Das Lieferkettensorgfaltspflichtengesetz in der Unternehmenspraxis**.

€ 170,-/Monat* | Modulvergleich & Preise online: bo.beck.de/124331

Compliance **OPTIMUM**

Schöpfen Sie in Sachen Compliance aus dem Vollen. Das OPTIMUM-Modul enthält alle Inhalte von PLUS und PREMIUM und darüber hinaus noch viele hochkarätige Werke, u.a. **Fleischer/Mankowski, Lieferkettensorgfaltspflichtengesetz, Hilgendorf/Roth-Isigkeit**, Die neue Verordnung der EU zur Künstlichen Intelligenz – Rechtsfragen und Compliance sowie **Thüsing, Hinweisgeberschutzgesetz**.

€ 395,-/Monat* | Modulvergleich & Preise online: bo.beck.de/132331

*Normalpreis für bis zu 3 Nutzer, Vorzugspreis verfügbar, zzgl. MwSt., 6-Monats-Abo

PLUS

PREMIUM

OPTIMUM

Verlag C.H.Beck GmbH & Co. KG, Wilhelmstraße 9, 80801 München | 170273 | Folgen Sie uns auf     Mehr Infos: ch.beck.de/socialmedia
Irrtümer, Preisänderungen und Druckfehler vorbehalten.

beck-online.DIE DATENBANK genügt.

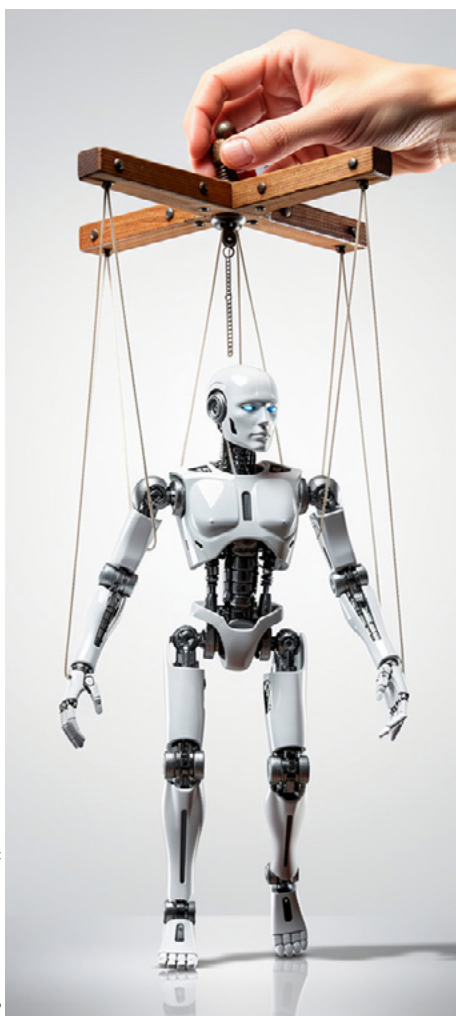
KI in der Versicherungswirtschaft: Skalierung als Governance-Aufgabe

Künstliche Intelligenz (KI) ist in der deutschen Versicherungswirtschaft längst produktiv im Einsatz: im Kundenmanagement bei Chatbots und Vertriebssteuerung, in der Schadenregulierung bei automatisierter Erstprüfung und Betrugserkennung, im Underwriting bei Risikobewertung und Tarifierung. Der Sprung vom Pilotprojekt zur unternehmensweiten Skalierung gelingt jedoch selten.

Zwei Hürden stehen im Weg: gewachsene Legacy-Bestandssysteme, die eine durchgängige Automatisierung technisch erschweren, und ein regulatorisches Umfeld, das an automatisierte Entscheidungen im Serieneinsatz erheblich höhere Anforderungen stellt als im begrenzten Pilotbetrieb. Damit wird KI-Skalierung zur Governance-Aufgabe.

Die **Verordnung (EU) 2024/1689** des sogenannten EU AI Act stuft KI-Systeme zur Risikobewertung und Preisbildung in der Lebens- und Krankenversicherung nach Art. 6 Abs. 2 i. V. m. Anhang III als Hochrisiko-KI-Systeme ein. Die EU (in Erwägungsgrund 58) begründet dies mit möglichen Auswirkungen auf die Existenzgrundlage betroffener Personen, die bis zu finanzieller Ausgrenzung und Diskriminierung führen könne. Für solche Systeme gelten unter anderem ein Risikomanagementsystem (Art. 9), Data-Governance- und Bias-Kontrollpflichten (Art. 10), Dokumentations- und Transparenzpflichten (Art. 11-13) sowie die Pflicht zu wirksamer menschlicher Aufsicht (Art. 14). Versicherer treten meist als Betreiber auf und müssen vor Erstinsetzung eine Folgenabschätzung nach Art. 27 AI Act durchführen; betroffene Personen erhalten zudem ein Recht auf Erläuterung nach Art. 86 AI Act. Für Versicherer als Finanzinstitute gilt eine Erleichterung: Bestehende Governance-Strukturen nach Finanzdienstleistungsrecht werden auf einen Großteil der Qualitätsmanagement- und Dokumentationspflichten angerechnet (Art. 17 Abs. 4, Art. 18 Abs. 3 AI Act).

Unabhängig vom AI Act verlangt § 23 VAG eine wirksame und angemessene Geschäftsorganisation mit transparenten Verantwortungsbereichen und einem wirksamen Risikomanagementsystem. Die BaFin hat dies zuletzt im Rundschreiben 09/2025 (VA) zur Geschäftsorganisation von Versicherungsunternehmen unter Solvabilität II konkretisiert und stellt dort ausdrücklich einen Bezug zum AI Act und zur DORA-Verordnung her. Automatisierte Risikozeichnung, automatisierte Einzelfallentscheidungen bei Schadens- und Leistungsfällen sowie automatisierte Bestandsverwaltung müssen danach angemessen gesteuert und überwacht werden; alle automatisierten Abläufe müssen identifizierbar und nachvollziehbar dokumentiert sein, Eingriffsmöglichkeiten für Verantwortliche müssen bestehen, und die Geschäfts-



KI-gestützte Entscheidungen: Der Mensch muss immer die Fäden in der Hand behalten.

leitung muss in Grundzügen informiert sein. Der Kontrollumfang steigt proportional mit dem Risikoprofil des jeweiligen automatisierten Ablaufs.

Schon Art. 22 Abs. 1 DSGVO verbietet grundsätzlich ausschließlich automatisierte Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung. Ausnahmen bestehen bei Vertragserfordernis, gesetzlicher Zulassung mit Schutzmaßnahmen oder ausdrücklicher Einwilligung; in den ersten und dritten Fällen ist mindestens ein Recht auf menschliches Eingreifen, Stellungnahme und Anfechtung zu gewährleisten (Art. 22 Abs. 3 DSGVO). Der deutsche Gesetzgeber hat mit § 37 BDSG

eine versicherungsspezifische Öffnungsklausel geschaffen: Das Verbot gilt nicht, wenn dem Begehren der betroffenen Person stattgegeben wird, oder bei Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen mit angemessenen Schutzmaßnahmen. Eine vollautomatisierte Ablehnung bleibt damit datenschutzrechtlich deutlich voraussetzungsvoller als eine automatisierte Stattgabe.

Eine spezifisch auf KI-gestützte Entscheidungen im Underwriting oder in der Schadenregulierung bezogene höchstrichterliche Rechtsprechung fehlt bislang. Der BGH hat sich mit dem automatisierten Abgleich von Schadensanzeigen mit Branchendateien (Uniwagnis-Datei) befasst. Das Bundespatentgericht hat sich mit der Patentfähigkeit eines regelbasierten Prüfsystems für Kfz-Schadengutachten auseinandergesetzt. Beide Urteile beinhalten keine Aussage zu Fairness oder Nachvollziehbarkeit automatisierter Entscheidungen als solcher. International zeigt die Sammelklage Kisting-Leung v. Cigna Corp. in den USA, welches Konfliktpotenzial algorithmische Ablehnungsentscheidungen in der Krankenversicherung bergen, wenn die vorgesehene menschliche Prüfung faktisch entfällt.

Die Skalierungshürde bei KI in der Versicherungswirtschaft liegt nicht allein in der Technik. EU AI Act, Geschäftsorganisation nach VAG und DSGVO verlangen im Zusammenspiel den durchgängigen Nachweis, dass automatisierte Entscheidungen fair, nachvollziehbar und rechtmäßig sind, durch Klassifizierung der KI-Systeme, Verzahnung mit bestehender Governance, wirksamer menschlicher Aufsicht und laufender Bias-Kontrolle. Wer dies von Beginn an mitdenkt, macht aus der Governance-Anforderung einen Skalierungsvorteil.

Udo Pickartz, Counsel, und Regina Radam, Associate, Simmons & Simmons LLP, Düsseldorf

IMPRESSUM

Verlag

Deutscher Fachverlag GmbH, Mainzer Landstraße 251, 60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
UStIdNr. DE 114139662

Geschäftsführung: Peter Esser (Sprecher), Thomas Berner, Markus Gotta

Aufsichtsrat: Andreas Lorch, Catrin Lorch, Dr. Edith Baumann-Lorch, Peter Ruß

Redaktion: Christina Kahlen-Pappas (verantwortlich),

Telefon: 0151 27 24 56 63, E-Mail: christina.kahlen-pappas@dfv.de

Verlagsleitung: RA Torsten Kutschke,

Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de

Anzeigen: Mikhail Tsyganov,

Telefon: 069 7595-2779, E-Mail: Mikhail.Tsyganov@dfv.de

Fachbeirat: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, Berneis Legal & Compliance; Ralf Brandt, divini patch Beteiligungs GmbH; Joern-Ulrich Fink, Regulatory Adherence & Compliance Policy Governance, Deutsche Bank AG; Otto Geiß, Deutsches Netzwerk Wirtschaftsethik; Mirko Haase, Hilti Corporation; Prof. Dr. Katharina Hastenrath, ZHAW Zürcher Hochschule für Angewandte Wissenschaften; Corina Käsler, Senior Advisor, State Street Bank International GmbH; Dr. Karsten Leffrang, General Counsel Germany, Valeo; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Muth-zur-Entwicklung; Stephan Niemann; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, Global Compliance, Miele Group; Hartmut T. Renz, Partner STRATECO GmbH; Dr. Barbara Roth, State Street Bank International; Jörg Siegmund, Getzner Textil AG; Eric S. Soong, Group Head Compliance & Corporate Security, Schaeffler Technologies AG & Co. KG; Dr. Martin Walter, selbstständiger Autor, Berater und Referent für Compliance-Themen

Jahresabonnement: kostenlos

Erscheinungsweise: monatlich (10 Ausgaben pro Jahr)

Layout: Uta Struhalla-Kautz, SK-Grafik, www.sk-grafik.de

Jede Verwertung innerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Keine Haftung für unverlangt eingesandene Manuskripte. Mit der Annahme zur Alleinveröffentlichung erwirbt der Verlag alle Rechte, einschließlich der Befugnis zur Einspeicherung in eine Datenbank.

NIS-2-Pflichtschulung für Geschäftsleitungen

Eine Veranstaltung von

R&W
Fachkonferenzen

15. Oktober 2026, 10.00 bis 12.00 Uhr | Online-Schulung

Jetzt anmelden!

Cybersicherheit ist Chefsache. Von der Regulierung der NIS-2-Richtlinie und der Umsetzung im BSIG sind in Deutschland über 29.000 Unternehmen betroffen, viele erstmals. Neben klassischen Betreibern kritischer Infrastrukturen erfasst das Gesetz nun auch mittelständische Unternehmen etwa aus Maschinenbau, Lebensmittelproduktion, Chemie, Post- und Kurierdienstleistung oder Abfallentsorgung – bereits ab 50 Beschäftigten oder einem Jahresumsatz und einer Jahresbilanzsumme von je 10 Mio. Euro. Für die Leitungsorgane der regulierten Unternehmen gilt § 38 Abs. 3 BSIG: diese verpflichtet die Geschäftsleitung zu regelmäßiger Schulung.

DAS ERWARTET SIE:

In dieser Live-Schulung vermitteln wir, was das Gesetz von der Leitungsebene rechtlich verlangt. Der Fokus liegt auf den Rechtspflichten der Leitungsorgane – Risikoerkennung, Steuerungs- und Überwachungsverantwortung, Mindestmaßnahmen, Melde-, Registrierungs- und Dokumentationspflichten, Managemententscheidungen im Krisenfall sowie persönliche Haftung und Bußgelder.

Keine Schulung zum Absitzen: Live-Austausch mit den Referentinnen, Rückfragen ausdrücklich erwünscht, Vermittlung von Inhalten statt Referieren von Paragraphen.

Zielgruppe: Geschäftsführung, Vorstand und Leitungsorgane besonders wichtiger und wichtiger Einrichtungen aller Branchen – insbesondere auch Unternehmen, die erstmals unter die Cybersicherheitsregulierung fallen.

DIE THEMEN IM ÜBERBLICK:

- Überblick zur NIS-2-Richtlinie und zum Umsetzungsgesetz
- Betroffenheitsprüfung
- Pflichten der Geschäftsleitung: Risikomanagement (Steuerung und Überwachung), Melde-, Registrierungs- und Dokumentationspflichten
- Managemententscheidungen im Cyber-Krisenfall
- Persönliche Haftung
- Bußgelder

Teilnahmegebühren (zzgl. MwSt.):

369,- EUR Abonent:innen eines Titels
der Fachmedien Recht und Wirtschaft
399,- EUR Normalpreis



**Teilnahmezertifikat zur Dokumentation der
Einhaltung Ihrer Schulungspflicht**

FREUEN SIE SICH AUF:



Larissa Normann
Partnerin
GÖHMANN Rechtsanwälte



Bettina Zerelles
Partnerin
GÖHMANN Rechtsanwälte

Ihre Ansprechpartnerin: Frau Maria Belz

Projektmanagerin
Tel.: +49 69 7595-1157
E-Mail: Maria.Belz@dfv.de

Deutscher Fachverlag GmbH
Mainzer Landstr. 251
60326 Frankfurt am Main



Mit Unterstützung von **GÖHMANN**
RECHTSANWÄLTE · NOTARE

Medienpartner

**Compliance
Berater**

**DATENSCHUTZ-
BERÄTER**

**Kommunikation
& Recht**



JETZT ANMELDEN UNTER
www.ruw.de/NIS2-Pflicht
oder QR-Code scannen

// WIR FEIERN **80 JAHRE** /

R&W
Fachkonferenzen

Eine Medienmarke der

dfv Mediengruppe

Bundesregierung bringt Reform des Kartellrechts auf den Weg

Die Bundesregierung hat im September einen Gesetzentwurf zur Reform des Kartellrechts vorgelegt. Kern ist ein innovatives Vergabescreening, das Kartellabsprachen bei öffentlichen Aufträgen systematisch aufdecken soll. Gleichzeitig werden die Umsatzschwellen für die Anmeldepflicht von Unternehmensfusionen deutlich angehoben.



Unternehmen auf Einkaufstour: Umsatzschwellen für die Anmeldepflicht von Unternehmenszusammenschlüssen sollen steigen.

Mit dem „Entwurf eines Zwölften Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen und anderer Gesetze“ ist geplant, Kartellrechtsverfahren schneller, effizienter und digitaler zu machen und das Bundeskartellamt zu entlasten, heißt es in einer Meldung des Bundestags von Anfang September.

Der Entwurf setze Vorgaben aus dem Koalitionsvertrag von CDU, CSU und SPD um. Auslöser für die Anpassungen sei die Absicht, die Fusionskontrolle an aktuelle wirtschaftliche Entwicklungen wie die Digitalisierung anzupassen, die Missbrauchsaufsicht im Energiebereich zu verlängern und die Bekämpfung von Submissionsabsprachen bei öffentlichen Vergaben zu verbessern.

Zu den wichtigsten Punkten gehören die Einführung eines Vergabescreenings durch das Bundeskartellamt. Das Bundeskartellamt soll die Befugnis erhalten, Angebotspreise und weitere Daten aus öffentlichen Vergabeverfahren systematisch und verdachtsunabhängig auszuwerten, um Kartellabsprachen besser aufdecken und verfolgen zu können. Dafür werde eine neue Datenübermittlungspflicht für Auftraggeber geschaffen und eine Speicherdauer der Daten von fünf Jahren festgelegt.

Außerdem sind die Reform der Fusionskontrolle und eine Anhebung der Umsatzschwellen vorgesehen. Die Umsatzschwellen für die Anmeldepflicht von Unternehmenszusammenschlüssen werden deutlich erhöht, weltweit auf 750 Mio. EUR, im Inland auf 75 Mio. EUR. Die Transaktionswertschwelle wird rechtssicher ausgestaltet und auf Fälle mit voraussichtlicher künftiger Inlandstätigkeit ausgeweitet, um insbesondere strategische Übernahmen innovativer Unternehmen – sogenannte „killer acquisitions“ – besser erfassen zu können. *chk*

Deutsche Compliance Konferenz 2027: Compliance zukunftssicher gestalten

Die Deutsche Compliance Konferenz 2027 am 27. und 28. April 2027 in Frankfurt am Main vereint aktuelle Informationen und die Möglichkeit für intensiven Austausch in der Compliance-Community. In fünf zentralen Themenblöcken zeigen hochkarätige Referentinnen und Referenten wie Compliance-Verantwortliche ihr Unternehmen resilient aufstellen können – ohne dabei teure Parallelstrukturen aufzubauen.

Compliance steht unter Druck: Regulatorische Anforderungen verschärfen sich, KI verändert die Spielregeln, geopolitische Unsicherheiten wachsen, der Kostendruck steigt. Auf diese Herausforderungen fokussiert sich die DCK 2027 in ihrem zweitägigen Programm mit fünf Themenblöcken: Compliance als Querschnittsfunktion, KI & Datenschutz, Geopolitik & Resilienz, Finance & Geldwäsche sowie Updates – Kartellrecht & Unternehmensstrafrecht.

Zentraler Ausgangspunkt der Tagung: Compliance funktioniert nicht isoliert. Es gilt Silodenken zu überwinden. Der Themenblock „Compliance

als Querschnittsfunktion“ beleuchtet, wie Schnittstellen zu Risk Management, Controlling und interner Revision ressourcenschonend und auf dem Fundament einer widerstandsfähigen Unternehmens- und Compliance-Kultur sinnvoll verbunden werden können.

Der Themenblock „KI & Datenschutz“ geht auf die grundlegenden Veränderungen von Compliance-Anforderungen durch Künstliche Intelligenz ein: KI-Governance und Datenschutz müssen strategisch verankert und regulatorische Anforderungen erfüllt werden. Dabei können bestehende Strukturen intelligent genutzt werden, statt Paral-

lelstrukturen bei der Implementierung von KI zu schaffen.

Sanktionen und nationale Sicherheitsinteressen fragmentieren Märkte und prägen globale Lieferketten – auf diese Herausforderungen blickt der Themenblock „Geopolitik & Resilienz“. Denn geopolitische Risiken müssen frühzeitig erkannt werden, um Compliance-Strategien für resiliente Geschäftsmodelle zu entwickeln.

Lernen von den Profis, diese Möglichkeit bietet der Themenblock „Finance & Geldwäsche“. Banken und Versicherer sind Compliance-Profis aus Notwendigkeit. Ihre bewährten Governance-Strukturen lassen sich auf andere Branchen übertragen – pragmatisch und mit messbarem Nutzen.

Der Themenblock „Updates – Kartellrecht & Unternehmensstrafrecht“ informiert zu aktuellen Entwicklungen. Der Gesetzgeber reformiert das Sanktionsrecht und das Kartellrecht grundlegend: Diese Updates vermitteln die neuen Anforderungen und zeigen, worauf sich Compliance-Verantwortliche konkret einstellen müssen. *chk*

Informationen und Anmeldung:
www.ruw.de/dck

SAVE THE DATE

Heute schon Termin vormerken

Eine Veranstaltung der

**GELDWÄSCHE
& RECHT**

25. Februar 2027 | Frankfurt am Main

4. Praxisseminar Geldwäscheprävention 2027

Das Jahresupdate für Kanzleien und Berufsträger:innen



JETZT ANMELDEN UNTER

www.ruw.de/gwp
oder QR-Code scannen

Jetzt Frühbucherrabatt sichern und sparen!

Veranstaltungsort:

dfv Mediengruppe
Mainzer Landstraße 251
60326 Frankfurt am Main

Teilnahmegebühren (zzgl. MwSt.):

629,- EUR Unternehmensvertreter:innen
829,- EUR Abonent:innen GWuR / CB / RdZ / BB
929,- EUR Normalpreis

Anmeldeschluss: 24. Februar 2027

Eine frühzeitige Anmeldung wird empfohlen.
Anmeldung unter www.ruw.de/gwp



Fortbildungsveranstaltung nach § 15 FAO!

Ihre Ansprechpartnerin:

Frau Lena Wehrmann
Projektmanagerin
Deutscher Fachverlag GmbH
Tel.: +49 69 7595-2784
E-Mail: Lena.Wehrmann@dfv.de



Rabatte – so sparen Sie intelligent:

5 % Frühbucherrabatt
bei Anmeldung bis zum 14. September 2026.

5 % Mehrbucherrabatt
bei Anmeldung von mehr als 2 Teilnehmer:innen einer
Kanzlei / eines Unternehmens ab der 3. Anmeldung
(mit anderen Rabatten kombinierbar).

// WIR FEIERN **80 JAHRE** /

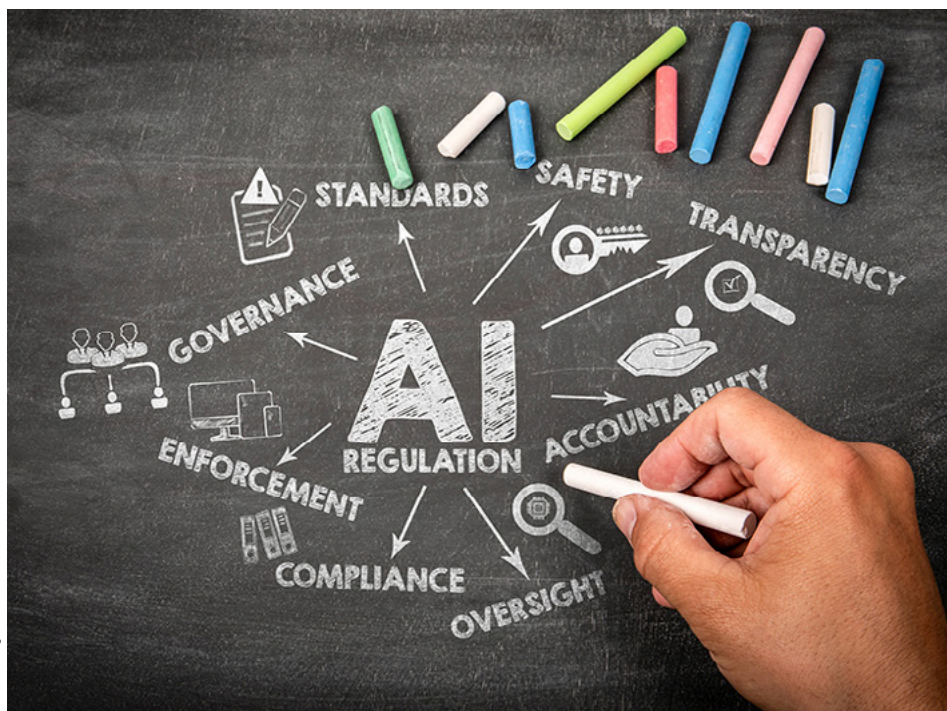
R&W
Fachkonferenzen

Eine Medienmarke der

dfv Mediengruppe

EU AI Act: KI wird in Standardsoftware zum Compliance-Risiko

Der EU AI Act wird für deutlich mehr deutsche Unternehmen relevant, als bislang angenommen. Diejenigen, die Standardsoftware mit integrierten KI-Funktionen einsetzen – etwa in den Bereichen Biometrie, Leistungsbewertung oder Lernanwendungen –, können unter die Vorschriften für Hochrisiko-KI-Systeme fallen. Verschobene Fristen verschärfen die Unsicherheit bei der Umsetzung der Compliance-Anforderungen.



AI Regulation: Compliance-Anforderungen müssen rechtzeitig in Prozesse, Verantwortlichkeiten und Kontrollmechanismen überführt werden.

Der EU AI Act gilt nicht nur für künstliche Intelligenz (KI), die Unternehmen selbst entwickeln, sondern auch für den Einsatz von Unternehmenssoftware, in die KI integriert ist. Auch die Nutzung von KI-Software von Drittanbietern begründet konkrete Dokumentations-, Kontroll- und Nachweispflichten. Das größte Missverständnis rund um den EU AI Act besteht darin, dass er in erster Linie KI-Entwickler und Technologieanbieter betreffe. Tatsächlich gilt das Gesetz für alle Organisationen, die KI-Systeme einsetzen. Das Problem: KI hat sich in Unternehmen längst etabliert, wird jedoch häufig nicht als regulatorisches Risiko wahrgenommen.

In vielen Fällen wird KI nicht als eigenständiges Projekt eingeführt, sondern ergänzt bestehende HR-, Rechts- oder Finanzsysteme um zusätzliche Funktionen. Genau hier besteht Nachholbedarf: Unternehmen müssen sich des tatsächlichen Anwendungsbereichs des EU AI Acts bewusst werden, um die Anforderungen rechtzeitig in Prozesse, Verantwortlichkeiten und Kontrollmechanismen zu überführen.

Die unzureichende Vorbereitung auf den EU AI Act führt schnell zu einem erheblichen Haftungsrisiko. Dabei ist vor allem der Faktor Zeit entscheidend, da in den kommenden zwei Jahren mehrere Fristen greifen. Für Verunsicherung sorgt zudem die EU-Digital-Omnibus-Gesetzgebung, die einige – jedoch keineswegs alle – Fristen der ursprünglichen Verordnung angepasst hat. Viele deutsche Organisationen ordnen die Fristen des AI Acts falsch ein. Sie gehen davon aus, dass sämtliche Verpflichtungen durch den Omnibus verschoben wurden. Das ist jedoch nicht der Fall. Die Trans-

parenzpflichten gelten seit dem 2. August 2026 und wurden nicht verschoben. Der Omnibus hat lediglich die Anforderungen für Hochrisiko-KI-Systeme nach hinten verlegt – und selbst das nicht einheitlich. Für eigenständige Systeme, beispielsweise KI-Tools zur Bewerberauswahl, gilt derzeit voraussichtlich eine Frist bis Dezember 2027. KI, die Bestandteil regulierter Produkte wie Medizinprodukte oder Maschinen ist, muss die entsprechenden Anforderungen hingegen erst bis August 2028 erfüllen.

Bei schwerwiegenden Verstößen drohen Bußgelder von bis zu 35 Mio. EUR oder sieben Prozent des weltweiten Jahresumsatzes. Schwerer als finanzielle Sanktionen dürfte für Unternehmen der Reputationsschaden wiegen. Diskriminierende Entscheidungen bei der Bewerberauswahl oder intransparente KI-gestützte Leistungsbewertungen können als öffentlich bekannt gewordener Compliance-Verstoß schnell erhebliche geschäftliche Risiken nach sich ziehen und die wirtschaftliche Handlungsfähigkeit eines Unternehmens erheblich einschränken. Für Vorstände schafft der AI Act deshalb klare Erwartungen: AI Governance gehört künftig auf die Agenda aller Risiko- und Compliance-Gremien. Dazu gehören regelmäßige Bewertungen des Einsatzes von KI-Systemen, um die erforderlichen Risikobewertungen durchführen zu können, Berichte über Hochrisiko-KI-Systeme, die Überprüfung veröffentlichter KI-generierter Inhalte im Hinblick auf die Transparenzanforderungen sowie eine lückenlose Dokumentation zum Nachweis der Compliance.

Unternehmen sollten die regulatorischen Anforderungen proaktiv angehen und frühzeitig kontinuierliche Prozesse etablieren. Sie sollten zunächst erfassen, welche KI-Systeme sie einsetzen, zu welchen Zwecken diese genutzt werden und welche Ergebnisse sie erzeugen. Daraus sollte ein vollständiges KI-Inventar entstehen, das nicht nur selbst entwickelte Anwendungen, sondern auch KI-Funktionen in eingekaufter Software umfasst. Anschließend können die einzelnen Systeme entsprechend ihrer Risikokategorie gemäß EU AI Act eingeordnet werden, um einen Überblick über die jeweiligen Fristen und Verpflichtungen zu erhalten. Voraussetzung dafür sind klar definierte Verantwortlichkeiten. Unternehmen sollten frühzeitig festlegen, wer für die AI Governance verantwortlich ist, und geeignete Systeme schaffen, über die Mitarbeitende potenzielle Probleme unkompliziert melden können. Zwar hat die EU ein zentrales Meldeportal speziell für Verstöße gegen den EU AI Act eingerichtet. Unternehmen, die bereits heute eigene Hinweisgebersysteme etablieren, ermöglichen ihren Mitarbeitenden jedoch eine geschützte interne Meldung und können potenzielle Probleme frühzeitig intern erkennen und beheben. Ebenso sollten Unternehmen eine kontinuierliche Dokumentation und Überwachung ihrer KI-Systeme etablieren.

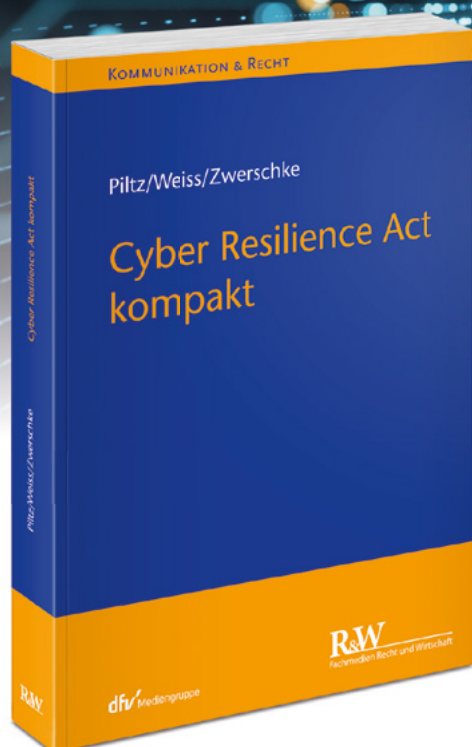
Erena Langley



Erena Langley, Director of Regulatory Solutions, NAVEX.

Neuerscheinung

Der neue Rechtsrahmen für digitale Produkte



Der Cyber Resilience Act verändert die Anforderungen an digitale Produkte in der EU grundlegend. Das Rechtshandbuch gibt einen kompakten, praxisnahen Überblick über die seit dem 10. Dezember 2024 geltenden und ab dem 11. Dezember 2027 vollständig anwendbaren Cybersicherheitsvorgaben sowie deren rechtssichere Umsetzung. Praxisbeispiele und Checklisten ergänzen die Darstellung.

Die Themenschwerpunkte im Überblick:

- Ziele der Verordnung und ihr Verhältnis zu anderen europäischen Regelwerken
- Anwendungsbereich und Begriff des Produkts mit digitalen Elementen
- Pflichten von Herstellern, Einführern und Händlern von Produkten mit digitalen Elementen
- Zuständige Behörden und deren Maßnahmen zur Marktüberwachung sowie Sanktionen

Die Autoren

Dr. **Carlo Piltz** ist Rechtsanwalt und Partner der Kanzlei Piltz Legal sowie zertifizierter Datenschutzbeauftragter (TÜV®) und CIPP/E. Er berät nationale und internationale Mandanten im Datenschutz-, IT-Sicherheits- und IT-Recht und begleitet sie bei komplexen Fallgestaltungen und Vertragsverhandlungen. Darüber hinaus ist er als externer Datenschutzbeauftragter tätig.

Alexander Weiss ist Rechtsanwalt bei Piltz Legal. Seine Schwerpunkte liegen im Datenschutzrecht, IT-Recht und der europäischen Digitalregulierung. Er berät nationale und internationale Unternehmen und veröffentlicht regelmäßig Fachbeiträge und Vorträge zu Themen wie KI-Verordnung, Cyber Resilience Act und Data Act.

Johannes Zwerschke, LL.M. ist Syndikusrechtsanwalt bei dem digitalen Speditions- und Logistikunternehmen sennder. Er berät insbesondere im Datenschutz-, IT- und IT-Sicherheitsrecht und veröffentlicht regelmäßig Fachbeiträge. Zudem ist er Fachanwalt für Informations-technologierecht sowie u. a. CIPP/E- und ISO/IEC-27001/27002- und BSI-IT-Grundschutz-zertifiziert.

Piltz/Weiss/Zwerschke

Cyber Resilience Act kompakt

1. Auflage 2026 | K&R-Schriftenreihe
ca. 200 Seiten | Broschur
ISBN: 978-3-8005-1979-8
€ 69,00

Weitere Informationen

shop.ruw.de



Keine Buch-Neuerscheinung mehr verpassen? Abonnieren Sie doch gerne unseren Newsletter: shop.ruw.de/newsletter