Holger Reibold

Compliance-Matrix:

NIS-2, DORA, CRA & EU AI Act integriert umsetzen

Risikomanagement,
Governance
und Audit-Readiness
ohne Doppelarbeit

BRAIN-MEDIA.DE

Holger Reibold

Compliance-Matrix

NIS-2, DORA, CRA & EU AI Act integriert umsetzen

Risikomanagement, Governance und Audit-Readiness ohne Doppelarbeit

BRAIN-MEDIA.DE

ISBN: 978-3-95444-355-0

Cover: Freepik / fabrikasimf

Brain-Media.de

Dr. Holger Reibold – Huber-Müller-Str. 52 – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Vorwort

Regulierungswelle: Warum Integration jetzt zählt

Die Jahre 2025 und 2026 markieren einen Wendepunkt für Unternehmen im europäischen Wirtschaftsraum. Was sich über Jahre hinweg angekündigt hat, trifft nun mit voller Wucht zusammen: eine Verdichtung regulatorischer Anforderungen, wie sie in dieser Form bislang nicht existierte. Mit der gleichzeitigen Umsetzung von NIS-2, DORA, dem Cyber Resilience Act und dem EU AI Act entsteht ein regulatorisches Umfeld, das viele Unternehmen als „Regulierungs-Gewitter" erleben. Die Dynamik, die Tiefe und vor allem die Überschneidungen dieser Vorgaben stellen Organisationen vor eine Herausforderung, die sich nicht mehr mit klassischen Einzelprojekten bewältigen lässt.

Genau hier liegt eines der größten Missverständnisse der aktuellen Compliance-Realität. Viele Unternehmen reagieren reflexartig mit isolierten Initiativen: ein Projekt für Cybersicherheit, ein weiteres für DORA, ein separates für KI-Governance. Diese fragmentierte Herangehensweise führt jedoch unweigerlich zu Redundanzen, ineffizientem Ressourceneinsatz und widersprüchlichen Prozessen. Die Folge: steigende Kosten, sinkende Transparenz und im schlimmsten Fall dennoch regulatorische Lücken. Einzelprojekte scheitern nicht an

mangelndem Engagement – sie scheitern an der fehlenden Integration.

Dieses Buch verfolgt daher einen konsequent anderen Ansatz. Statt Regulierung als Sammlung isolierter Anforderungen zu betrachten, wird sie als zusammenhängendes System verstanden. Der Schlüssel liegt in der Identifikation und Nutzung von Synergien. Viele Anforderungen der verschiedenen Regulierungen greifen auf ähnliche Grundprinzipien zurück: Risikomanagement, Governance-Strukturen, Incident Response, Dokumentation und Kontrolle. Wer diese Gemeinsamkeiten erkennt und gezielt nutzt, kann den Aufwand signifikant reduzieren und gleichzeitig die Qualität der Umsetzung erhöhen.

Der integrierte Ansatz bedeutet konkret: nicht vier Programme parallel aufzubauen, sondern ein gemeinsames Fundament zu schaffen. Ein Risikomanagement-System, das gleichzeitig mehrere regulatorische Anforderungen erfüllt. Ein Incident-Response-Prozess, der unterschiedliche Meldepflichten integriert. Eine Governance-Struktur, die sowohl Cybersicherheit als auch KI-Risiken abdeckt. Dieses Prinzip wird in diesem Buch als „Single Point of Compliance“ beschrieben – ein zentrales Zielbild, das es ermöglicht, Komplexität zu reduzieren und Steuerbarkeit zurückzugewinnen.

Mit der neuen Regulierungslandschaft verändert sich jedoch nicht nur die operative Umsetzung, sondern auch die Rolle der Unternehmensleitung grundlegend. Compliance ist längst kein rein technisches oder juristisches Thema mehr. Sie ist zu einer zentralen Managementaufgabe geworden. Geschäftsleiter stehen zunehmend

persönlich in der Verantwortung, regulatorische Anforderungen nicht nur formal zu erfüllen, sondern deren Wirksamkeit nachweisen zu können. Haftungsrisiken sind real und nehmen zu. Gleichzeitig eröffnet genau diese Entwicklung eine neue Perspektive: Wer Compliance strategisch denkt und integriert umsetzt, kann daraus einen echten Wettbewerbsvorteil entwickeln.

Unternehmen, die ihre Prozesse, Systeme und Strukturen entlang regulatorischer Anforderungen modernisieren, steigern nicht nur ihre Sicherheit und Resilienz. Sie verbessern auch ihre Effizienz, ihre Transparenz und ihre Entscheidungsfähigkeit. Compliance wird damit vom Kostenfaktor zum strategischen Asset. Sie stärkt das Vertrauen von Kunden, Partnern und Investoren und wird zunehmend zu einem Differenzierungsmerkmal im Markt.

Ein entscheidender Faktor wird in diesem Kontext jedoch häufig unterschätzt: der Mensch. Trotz aller technologischen Fortschritte und ausgefeilten Kontrollsysteme zeigt die Praxis immer wieder, dass ein Großteil sicherheitsrelevanter Vorfälle auf menschliches Verhalten zurückzuführen ist. Fehlkonfigurationen, unachtsamer Umgang mit Zugangsdaten, Phishing-Angriffe oder die unkontrollierte Nutzung neuer Technologien wie KI-Tools – all dies sind Beispiele für Risiken, die nicht durch Technik allein beherrscht werden können.

Eine nachhaltige Compliance-Strategie muss daher über Prozesse und Systeme hinausgehen. Sie muss Unternehmenskultur adressieren. Sie muss Bewusstsein schaffen, Verhalten verändern und Verantwortlichkeiten klar definieren. Die „Human Firewall“ ist kein

Schlagwort, sondern ein zentraler Bestandteil moderner Sicherheitsarchitekturen. Ohne sie bleibt jedes noch so ausgefeilte Kontrollsystem unvollständig.

Das Praxisunternehmen als roter Faden

Um diese komplexen Zusammenhänge greifbar zu machen, arbeitet dieses Buch mit einem durchgängigen Praxisbeispiel. Im Zentrum steht das fiktive Unternehmen „MediTech GmbH". Als typischer Vertreter des produzierenden Mittelstands entwickelt und vertreibt MediTech vernetzte Geräte mit IoT-Funktionalitäten und integriert zunehmend KI-basierte Anwendungen in seine Produkte und Prozesse. Damit befindet sich das Unternehmen genau in dem Spannungsfeld, das viele Organisationen aktuell erleben: technologischer Fortschritt auf der einen Seite, steigende regulatorische Anforderungen auf der anderen.

Zu Beginn steht MediTech vor einer Situation, die vielen Lesern vertraut sein dürfte. Einzelne regulatorische Anforderungen werden zwar erkannt, ihre Tragweite jedoch unterschätzt. Verantwortlichkeiten sind unklar, Prozesse fragmentiert, und ein übergreifendes Konzept fehlt. Erst mit zunehmendem Druck durch regulatorische Fristen und konkrete Vorfälle wird deutlich, dass ein grundlegender Perspektivwechsel notwendig ist.

Im Verlauf des Buches wird die Entwicklung von MediTech Schritt für Schritt begleitet. Von der ersten Betroffenheitsanalyse über den

Aufbau einer integrierten Compliance-Struktur bis hin zur Implementierung eines nachhaltigen Betriebsmodells. Die Praxisbeispiele sind bewusst so gestaltet, dass sie typische Herausforderungen, Fehlannahmen und Lösungsansätze widerspiegeln. Sie dienen nicht nur der Veranschaulichung, sondern bieten konkrete Anknüpfungspunkte für die eigene Organisation.

Praxisleitfaden

Dieses Buch versteht sich daher nicht als rein theoretische Abhandlung, sondern als praxisorientierter Leitfaden. Es soll helfen, die Komplexität der aktuellen Regulierungslandschaft zu strukturieren, Zusammenhänge zu erkennen und konkrete Umsetzungswege aufzuzeigen. Ziel ist es, Unternehmen in die Lage zu versetzen, aus dem „Regulierungs-Gewitter" nicht nur unbeschadet hervorzugehen, sondern gestärkt daraus hervorzugehen.

Die zentrale Botschaft ist dabei klar: Die Herausforderung ist groß – aber sie ist beherrschbar. Vorausgesetzt, man verlässt die Denkweise isolierter Einzelmaßnahmen und setzt konsequent auf Integration, Transparenz und Steuerbarkeit. Genau diesen Weg beschreibt die vorliegende Compliance-Matrix.

Ich wünsche Ihnen dabei viel Erfolg.

Herzlichst

Holger Reibold

1 Das Regulierungsquartett

Vier Gesetze, ein System: Compliance neu gedacht

Mit dem Inkrafttreten und der sukzessiven Anwendung von NIS-2, DORA, dem Cyber Resilience Act und dem EU AI Act entsteht erstmals ein regulatorisches Gefüge, das Unternehmen nicht mehr punktuell, sondern systemisch betrifft. Dieses „Regulierungsquartett" adressiert unterschiedliche Perspektiven – von kritischer Infrastruktur über Finanzresilienz bis hin zu Produktsicherheit und Künstlicher Intelligenz – greift jedoch in seinen Anforderungen tief ineinander.

Die zentrale Herausforderung liegt nicht in der isolierten Umsetzung einzelner Vorgaben, sondern in deren gleichzeitiger Wirkung auf Organisation, Prozesse und Technologie. Unternehmen stehen vor der Aufgabe, Sicherheitsmaßnahmen, Governance-Strukturen und Nachweispflichten so zu gestalten, dass sie mehreren Regimen parallel gerecht werden. Genau an dieser Stelle entscheidet sich, ob Compliance zum operativen Risiko oder zum steuerbaren System wird.

Dieses Kapitel schafft die notwendige Grundlage für das Verständnis der folgenden Inhalte. Es ordnet die vier Regulierungen in ihrem jeweiligen Kontext ein, zeigt ihre Schnittmengen auf und macht deutlich, welche Rolle insbesondere das Management in diesem neuen

Umfeld einnimmt. Gleichzeitig wird ein erster Blick auf die zeitlichen Anforderungen geworfen, die den Handlungsdruck maßgeblich bestimmen.

Am Beispiel der fiktiven MediTech GmbH wird zudem sichtbar, wie schnell Unternehmen von regulatorischer Relevanz betroffen sein können – oft früher und umfassender als zunächst angenommen. Damit bildet dieses Kapitel den Einstieg in eine zentrale Erkenntnis dieses Buches: Wer die Regulatorik frühzeitig integriert denkt, gewinnt Handlungsspielraum – wer zu spät reagiert, verliert ihn.

1.1 NIS-2 – Sicherheit für kritische Sektoren

Mit der NIS-2-Richtlinie erreicht die europäische Cybersicherheitsregulierung eine neue Qualität. Während die ursprüngliche NIS-Richtlinie vor allem auf Betreiber kritischer Infrastrukturen fokussiert war, erweitert NIS-2 den Anwendungsbereich erheblich und verschärft zugleich die Anforderungen an Unternehmen und deren Leitung. Ziel ist es, ein einheitlich hohes Sicherheitsniveau in der gesamten Europäischen Union zu schaffen und gleichzeitig die Resilienz gegenüber zunehmend komplexen Cyberbedrohungen zu stärken.

Eine der zentralen Neuerungen liegt in der deutlichen Ausweitung der betroffenen Unternehmen. Neben klassischen kritischen Infrastrukturen wie Energie, Verkehr oder Gesundheit rücken nun auch weitere Sektoren in den Fokus, darunter Teile der Industrie, digitale Dienste und bestimmte produzierende Unternehmen. Gerade für den

Mittelstand bedeutet dies eine neue Realität: Organisationen, die sich bislang nicht als reguliert wahrgenommen haben, fallen plötzlich in den Anwendungsbereich der Richtlinie. Die Einordnung erfolgt dabei anhand von Sektoren, Unternehmensgröße und Kritikalität der erbrachten Leistungen.

Inhaltlich setzt NIS-2 stark auf ein strukturiertes Risikomanagement. Unternehmen sind verpflichtet, geeignete technische und organisatorische Maßnahmen zu implementieren, um Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu identifizieren, zu bewerten und zu minimieren. Dazu gehören unter anderem Maßnahmen zur Zugriffskontrolle, zur Sicherstellung der Betriebskontinuität, zum Umgang mit Sicherheitsvorfällen sowie zur Absicherung der Lieferkette. Besonders hervorzuheben ist der All-Gefahren-Ansatz: Nicht nur gezielte Cyberangriffe, sondern auch technische Ausfälle, menschliches Fehlverhalten oder externe Abhängigkeiten müssen berücksichtigt werden.

Ein weiterer wesentlicher Bestandteil der NIS-2 ist die Verschärfung der Meldepflichten. Sicherheitsvorfälle müssen innerhalb klar definierter Fristen an die zuständigen Behörden gemeldet werden. Dies erfordert nicht nur funktionierende Incident-Response-Prozesse, sondern auch eine enge Verzahnung zwischen IT, Management und Kommunikation. Unternehmen müssen in der Lage sein, Vorfälle schnell zu erkennen, zu bewerten und strukturiert zu berichten – eine Fähigkeit, die in vielen Organisationen erst aufgebaut werden muss.

Besondere Aufmerksamkeit verdient zudem die Rolle der Geschäftsleitung. NIS-2 verankert die Verantwortung für Cybersicherheit explizit auf Management-Ebene. Geschäftsleiter sind verpflichtet, sich mit den Risiken auseinanderzusetzen, geeignete Maßnahmen zu überwachen und deren Umsetzung sicherzustellen. Versäumnisse können nicht nur zu erheblichen Bußgeldern führen, sondern auch persönliche Haftungsrisiken nach sich ziehen. Damit wird Cybersicherheit endgültig zu einem strategischen Thema.

Am Beispiel der MediTech GmbH zeigt sich die praktische Relevanz dieser Entwicklung deutlich. Als mittelständischer Hersteller vernetzter Produkte fällt das Unternehmen zunächst nicht offensichtlich unter klassische Kritische Infrastrukturen. Durch die Kombination aus digitalisierten Produktionsprozessen, vernetzten Produkten und internationaler Lieferkette wird jedoch schnell klar, dass eine Einstufung als „wichtige Einrichtung" möglich ist. Die Erkenntnis, regulatorisch betroffen zu sein, markiert für MediTech den Ausgangspunkt einer umfassenden Transformation – von punktuellen Sicherheitsmaßnahmen hin zu einem strukturierten, integrierten Risikomanagement.

NIS-2 ist damit weit mehr als eine weitere Compliance-Anforderung. Sie zwingt Unternehmen, Cybersicherheit ganzheitlich zu denken und organisatorisch zu verankern. Wer diese Herausforderung frühzeitig annimmt, schafft nicht nur regulatorische Konformität, sondern legt auch die Grundlage für nachhaltige Resilienz in einer zunehmend digitalisierten Wirtschaft.

1.2 DORA – Digitale Resilienz im Finanzsektor

Mit der Digital Operational Resilience Act (DORA) schafft die Europäische Union erstmals einen einheitlichen regulatorischen Rahmen für die digitale Resilienz im Finanzsektor. Ziel ist es, sicherzustellen, dass Finanzunternehmen auch unter widrigen Bedingungen – insbesondere bei Cyberangriffen oder IT-Ausfällen – ihre kritischen Funktionen aufrechterhalten können. Im Gegensatz zu klassischen Sicherheitsansätzen steht bei DORA nicht nur der Schutz, sondern vor allem die Widerstandsfähigkeit und Wiederherstellungsfähigkeit im Mittelpunkt.

DORA adressiert eine Vielzahl von Akteuren innerhalb des Finanzökosystems. Dazu zählen nicht nur Banken, Versicherungen und Wertpapierfirmen, sondern auch Zahlungsdienstleister, Kryptodienstleister sowie – besonders relevant – IKT-Drittanbieter. Gerade diese Erweiterung ist von zentraler Bedeutung, da viele Finanzunternehmen wesentliche Teile ihrer IT-Infrastruktur an externe Dienstleister ausgelagert haben. Damit verschiebt sich der regulatorische Fokus von der isolierten Organisation hin zu einem vernetzten System von Abhängigkeiten.

Kern von DORA ist ein umfassendes IKT-Risikomanagement. Finanzunternehmen sind verpflichtet, robuste Governance-Strukturen zu etablieren, Risiken systematisch zu identifizieren und geeignete Maßnahmen zu implementieren. Dazu gehören unter anderem kontinuierliches Monitoring, klare Verantwortlichkeiten, Notfallpläne sowie

regelmäßige Überprüfungen der Wirksamkeit. Besonders hervorzuheben ist die Verpflichtung zu Resilienztests. Unternehmen müssen ihre Systeme aktiv auf Belastbarkeit prüfen, beispielsweise durch Penetrationstests oder simulationsbasierte Szenarien. Ziel ist es, Schwachstellen nicht erst im Ernstfall zu erkennen.

Ein weiterer zentraler Baustein sind die Meldepflichten. DORA verlangt eine strukturierte und zeitnahe Meldung von IKT-Vorfällen an die zuständigen Aufsichtsbehörden. Im Vergleich zu anderen Regulierungen sind die Fristen teilweise deutlich kürzer, was hohe Anforderungen an die interne Organisation stellt. Unternehmen müssen in der Lage sein, Vorfälle schnell zu klassifizieren, deren Auswirkungen zu bewerten und die notwendigen Informationen bereitzustellen. Dies erfordert eine enge Integration von Incident Response, Kommunikation und regulatorischem Reporting.

Besonders anspruchsvoll ist zudem der Umgang mit IKT-Drittanbietern. DORA verpflichtet Finanzunternehmen, Risiken entlang ihrer Lieferkette aktiv zu steuern. Dazu gehören vertragliche Anforderungen, regelmäßige Prüfungen sowie die Überwachung kritischer Dienstleister. Gleichzeitig unterliegen bestimmte besonders kritische Anbieter künftig selbst einer direkten europäischen Aufsicht. Damit entsteht ein mehrschichtiges Kontrollsystem, das die Stabilität des gesamten Finanzsystems erhöhen soll.

Auch unter DORA spielt die Rolle des Managements eine zentrale Rolle. Die Geschäftsleitung ist verantwortlich für die Festlegung und Überwachung des IKT-Risikomanagements. Sie muss sicherstellen,

dass ausreichende Ressourcen bereitgestellt werden und dass die Organisation in der Lage ist, regulatorische Anforderungen zu erfüllen. Digitale Resilienz wird damit zu einem integralen Bestandteil der Unternehmenssteuerung.

Für die MediTech GmbH ist DORA auf den ersten Blick nicht unmittelbar einschlägig, da das Unternehmen kein klassisches Finanzinstitut ist. Die Relevanz entsteht jedoch indirekt über Kundenbeziehungen und Lieferketten. Als Anbieter vernetzter Produkte und potenzieller IKT-Dienstleistungen kann MediTech als Drittanbieter für regulierte Finanzunternehmen auftreten. In diesem Fall wirken die Anforderungen von DORA mittelbar auf das Unternehmen ein – etwa in Form von vertraglichen Verpflichtungen, Sicherheitsanforderungen oder Auditrechten.

DORA zeigt damit exemplarisch, wie sich Regulierung zunehmend entlang von Wertschöpfungsketten ausbreitet. Unternehmen müssen nicht nur ihre eigene Compliance im Blick haben, sondern auch die Anforderungen ihrer Kunden und Partner verstehen. Digitale Resilienz wird so zu einem gemeinsamen Standard, der über Branchengrenzen hinweg wirkt.

Insgesamt verschiebt DORA den Fokus von reaktiver Sicherheit hin zu proaktiver Widerstandsfähigkeit. Unternehmen, die diesen Ansatz konsequent umsetzen, stärken nicht nur ihre regulatorische Position, sondern auch ihre Fähigkeit, in einem zunehmend volatilen digitalen Umfeld stabil zu operieren.

1.3 CRA – Sicherheit für digitale Produkte

Mit dem Cyber Resilience Act (CRA) erweitert die Europäische Union den regulatorischen Fokus von organisatorischer Sicherheit hin zur Sicherheit von Produkten selbst. Erstmals wird Cybersicherheit systematisch entlang des gesamten Produktlebenszyklus reguliert – von der Entwicklung über die Bereitstellung bis hin zum Betrieb und zur Wartung. Damit betrifft der CRA insbesondere Hersteller und Anbieter digitaler Produkte, unabhängig davon, ob es sich um Software, Hardware oder vernetzte Systeme handelt.

Im Zentrum des CRA steht das Prinzip „Security by Design" und „Security by Default". Produkte müssen bereits bei ihrer Konzeption so gestaltet sein, dass sie grundlegende Sicherheitsanforderungen erfüllen. Dazu gehören unter anderem sichere Voreinstellungen, Schutz vor unbefugtem Zugriff, Integrität der Software sowie die Fähigkeit, Sicherheitsupdates bereitzustellen. Diese Anforderungen gelten nicht nur für klassische IT-Produkte, sondern zunehmend auch für industrielle Systeme, Maschinen und IoT-Geräte.

Eine wesentliche Neuerung des CRA ist die klare Zuordnung von Verantwortlichkeiten. Hersteller sind verpflichtet, die Sicherheit ihrer Produkte über den gesamten Lebenszyklus hinweg sicherzustellen. Dazu gehört insbesondere die Bereitstellung von Sicherheitsupdates und das Management von Schwachstellen. Gleichzeitig müssen sie Transparenz schaffen, etwa durch Dokumentation, Risikobewertungen und die Bereitstellung einer Software Bill of Materials (SBOM).

Diese ermöglicht es Kunden und Partnern, die eingesetzten Komponenten und deren potenzielle Risiken nachzuvollziehen.

Neben Herstellern können auch Importeure, Händler und Integratoren in die Verantwortung genommen werden. Besonders relevant ist in diesem Zusammenhang das Konzept des „Hidden Manufacturer". Unternehmen, die Produkte unter eigenem Namen vertreiben oder bestehende Lösungen wesentlich verändern, können regulatorisch als Hersteller eingestuft werden – selbst wenn sie die Produkte nicht selbst entwickelt haben. Für viele mittelständische Unternehmen stellt dies eine neue und oft unerwartete Verpflichtung dar.

Ein weiterer zentraler Aspekt des CRA sind Melde- und Informationspflichten. Sicherheitslücken und Vorfälle müssen innerhalb definierter Fristen gemeldet werden. Gleichzeitig sind Hersteller verpflichtet, aktiv über bekannte Schwachstellen und verfügbare Updates zu informieren. Dies erfordert nicht nur technische Fähigkeiten, sondern auch etablierte Prozesse für Vulnerability Management und Kommunikation.

Für die MediTech GmbH hat der CRA eine unmittelbare und weitreichende Bedeutung. Als Hersteller vernetzter Geräte mit integrierter Software fällt das Unternehmen klar in den Anwendungsbereich der Verordnung. Produkte, die bislang primär unter funktionalen Gesichtspunkten entwickelt wurden, müssen nun systematisch unter Sicherheitsaspekten betrachtet werden. Dies betrifft sowohl die Entwicklungsprozesse als auch die Organisation von Support und Wartung.

Besonders herausfordernd ist dabei die Integration von Sicherheitsanforderungen in bestehende Produktentwicklungszyklen. MediTech muss sicherstellen, dass Sicherheitsaspekte bereits in der Designphase berücksichtigt werden und sich durch alle weiteren Phasen ziehen. Gleichzeitig entsteht die Notwendigkeit, Prozesse für das Management von Schwachstellen aufzubauen, inklusive Monitoring, Bewertung und Bereitstellung von Updates.

Der CRA macht damit deutlich, dass Cybersicherheit nicht mehr ausschließlich eine Frage des Betriebs ist, sondern zunehmend im Produkt selbst verankert sein muss. Für Unternehmen bedeutet dies einen Paradigmenwechsel: Sicherheit wird zu einem Qualitätsmerkmal von Produkten und damit zu einem Wettbewerbsfaktor.

Unternehmen, die diese Entwicklung frühzeitig antizipieren, können daraus einen strategischen Vorteil ziehen. Sie schaffen Vertrauen bei Kunden, reduzieren langfristig Risiken und positionieren sich als verlässliche Anbieter in einem zunehmend regulierten Markt. Der CRA ist somit nicht nur eine regulatorische Verpflichtung, sondern auch ein Impuls für nachhaltige Produktqualität und Innovation.

1.4 EU AI Act – Risikobasierte KI-Regulierung

Mit dem EU AI Act etabliert die Europäische Union erstmals einen umfassenden Rechtsrahmen für den Einsatz von Künstlicher Intelligenz. Ziel ist es, Innovation zu ermöglichen und gleichzeitig Risiken für Sicherheit, Grundrechte und Gesellschaft zu begrenzen. Anders

als viele klassische Regulierungen folgt der Act einem klar risikobasierten Ansatz: Nicht jede KI ist gleich – und entsprechend differenziert fallen auch die regulatorischen Anforderungen aus.

Im Zentrum steht die Einteilung von KI-Systemen in verschiedene Risikoklassen. Während Anwendungen mit minimalem Risiko weitgehend unreguliert bleiben, unterliegen Systeme mit hohem Risiko strengen Anforderungen. Dazu zählen unter anderem KI-Anwendungen in sicherheitskritischen Bereichen, in der Personalentscheidung oder im Zugang zu wesentlichen Dienstleistungen. Für diese Systeme gelten umfassende Pflichten hinsichtlich Risikomanagement, Datenqualität, Transparenz, Nachvollziehbarkeit und menschlicher Aufsicht.

Eine zentrale Herausforderung des EU AI Act liegt in der Rollenverteilung. Die Regulierung unterscheidet insbesondere zwischen Anbietern (Provider) und Betreibern (Deployer) von KI-Systemen. Anbieter sind für die Entwicklung und Konformität der Systeme verantwortlich, während Betreiber für den konkreten Einsatz und die Einhaltung der Nutzungsvorgaben zuständig sind. In der Praxis verschwimmen diese Rollen jedoch häufig, insbesondere in Unternehmen, die KI sowohl entwickeln als auch intern einsetzen. Die klare Zuordnung von Verantwortlichkeiten wird damit zu einer wesentlichen Voraussetzung für Compliance.

Ein weiterer wichtiger Aspekt ist die Verpflichtung zur Dokumentation und Nachweisführung. Unternehmen müssen in der Lage sein, die Funktionsweise ihrer KI-Systeme zu erklären, Risiken zu bewerten

und Entscheidungen nachvollziehbar zu machen. Dies erfordert neue Prozesse, insbesondere im Bereich der Modell-Governance, der Datenverwaltung und der kontinuierlichen Überwachung. Gleichzeitig entstehen Anforderungen an die Schulung von Mitarbeitern, die mit KI-Systemen arbeiten oder deren Ergebnisse nutzen.

Besondere Aufmerksamkeit verdient zudem das Thema Transparenz. Nutzer müssen darüber informiert werden, wenn sie mit KI-Systemen interagieren oder wenn Entscheidungen automatisiert getroffen werden. Dies betrifft nicht nur externe Anwendungen, sondern auch interne Prozesse. Unternehmen sind gefordert, klare Richtlinien für den Umgang mit KI zu definieren und deren Einhaltung sicherzustellen.

Für die MediTech GmbH ergibt sich aus dem EU AI Act eine doppelte Herausforderung. Zum einen integriert das Unternehmen zunehmend KI-Funktionalitäten in seine Produkte, etwa zur Analyse von Sensordaten oder zur Optimierung von Prozessen. In dieser Rolle agiert MediTech als Anbieter und muss sicherstellen, dass die entwickelten Systeme den regulatorischen Anforderungen entsprechen. Zum anderen nutzt das Unternehmen intern KI-Tools, beispielsweise in Marketing, Entwicklung oder Verwaltung. Hier tritt MediTech als Betreiber auf und muss den sicheren und regelkonformen Einsatz gewährleisten.

Besonders kritisch ist in diesem Zusammenhang das Phänomen der sogenannten „Schatten-KI“. Mitarbeitende greifen eigenständig auf externe KI-Dienste zurück, ohne dass eine zentrale Steuerung oder Kontrolle erfolgt. Dies kann zu erheblichen Risiken führen, etwa

durch den unbewussten Abfluss sensibler Daten oder durch die Nutzung nicht validierter Systeme. Der Act macht deutlich, dass solche informellen Nutzungen nicht mehr tolerierbar sind und in strukturierte Governance-Modelle überführt werden müssen.

Der AI Act steht damit exemplarisch für eine neue Generation von Regulierung: technologieoffen, risikobasiert und tief in organisatorische Prozesse eingebettet. Für Unternehmen bedeutet dies, dass KI nicht nur als Innovationsfeld, sondern auch als Compliance-Thema verstanden werden muss. Wer frühzeitig klare Strukturen schafft, Verantwortlichkeiten definiert und Kompetenzen aufbaut, kann die regulatorischen Anforderungen nicht nur erfüllen, sondern gleichzeitig die Potenziale von KI sicher und nachhaltig nutzen.

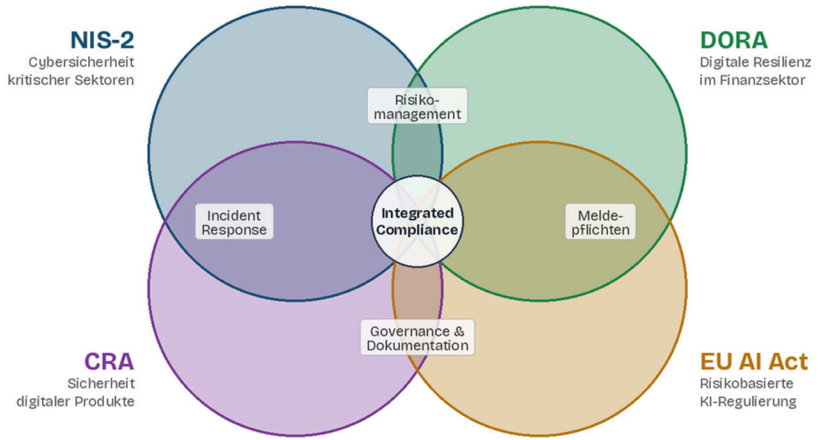


Abbildung 1: Überblick über das Regulierungsquartett und seine inhaltlichen Schnittmengen als Grundlage für integrierte Compliance.

1.5 Management-Fokus: Persönliche Haftung

Mit der neuen Regulierungslandschaft verschiebt sich die Verantwortung für Cybersicherheit und Compliance deutlich in Richtung Unternehmensleitung. Was früher häufig als operatives IT- oder Compliance-Thema betrachtet wurde, ist heute eine explizite Managementaufgabe mit klar definierten Pflichten und persönlichen Konsequenzen. Sowohl NIS2 als auch DORA verankern die Verantwortung der Geschäftsleitung unmittelbar und machen deutlich: Delegation entbindet nicht von Verantwortung.

Geschäftsleiter sind verpflichtet, sich aktiv mit den Risiken auseinanderzusetzen, geeignete Maßnahmen zu initiieren und deren Umsetzung zu überwachen. Dabei geht es nicht nur um die formale Einrichtung von Prozessen, sondern um deren tatsächliche Wirksamkeit. Regulatoren erwarten, dass das Management in der Lage ist, fundierte Entscheidungen zu treffen, Risiken zu verstehen und im Ernstfall angemessen zu reagieren. Diese Erwartungshaltung verändert die Rolle der Führungsebene grundlegend.

Besonders relevant ist dabei die Frage der Nachweisbarkeit. Im Falle von Vorfällen oder Prüfungen müssen Unternehmen belegen können, dass sie ihren Sorgfaltspflichten nachgekommen sind. Dokumentation wird damit zum zentralen Schutzmechanismus. Fehlende oder unzureichende Nachweise können als Organisationsverschulden gewertet werden und im schlimmsten Fall persönliche

Haftungsrisiken nach sich ziehen. Bußgelder, Reputationsschäden und rechtliche Konsequenzen sind dabei reale Szenarien.

Für viele Unternehmen bedeutet dies einen Paradigmenwechsel. Compliance wird nicht mehr als reine Erfüllung externer Anforderungen verstanden, sondern als integraler Bestandteil der Unternehmensführung. Entscheidungen zu Investitionen, Prioritäten und Ressourcen müssen vor dem Hintergrund regulatorischer Anforderungen getroffen werden. Gleichzeitig entsteht die Notwendigkeit, Governance-Strukturen so zu gestalten, dass Verantwortlichkeiten klar definiert und nachvollziehbar sind.

Am Beispiel der MediTech GmbH wird diese Entwicklung besonders deutlich. Die Geschäftsführung erkennt zunächst vor allem die operative Dimension der neuen Anforderungen. Mit zunehmender Auseinandersetzung wird jedoch klar, dass die eigentliche Herausforderung auf Management-Ebene liegt: Wie lassen sich Risiken strukturiert erfassen? Welche Maßnahmen sind angemessen? Und wie kann sichergestellt werden, dass diese Maßnahmen auch tatsächlich umgesetzt und dokumentiert werden?

Die Antwort liegt in der Etablierung eines integrierten Steuerungsmodells. Geschäftsleiter benötigen transparente Informationen, klare KPIs und belastbare Entscheidungsgrundlagen. Nur so können sie ihrer Verantwortung gerecht werden und gleichzeitig die Organisation effektiv steuern. Compliance wird damit zu einem Instrument der Unternehmensführung – nicht nur zur Risikominimierung, sondern auch zur strategischen Weiterentwicklung.

Die zunehmende persönliche Haftung ist somit nicht nur Risiko, sondern auch Chance. Sie zwingt Unternehmen, Strukturen zu professionalisieren, Transparenz zu schaffen und Verantwortung klar zu verankern. Wer diesen Wandel aktiv gestaltet, stärkt nicht nur seine regulatorische Position, sondern auch die langfristige Stabilität und Wettbewerbsfähigkeit des Unternehmens.

1.6 Fristen-Radar 2026–2028

Neben inhaltlichen Anforderungen ist es vor allem die zeitliche Dimension, die den Handlungsdruck für Unternehmen maßgeblich bestimmt. Die verschiedenen europäischen Regulierungen treten nicht gleichzeitig in Kraft, entfalten ihre Wirkung jedoch in kurzen, sich überlappenden Intervallen. Für viele Organisationen entsteht dadurch eine Situation, in der mehrere Umsetzungsprogramme parallel geplant, gesteuert und umgesetzt werden müssen. Genau hier entscheidet sich, ob Compliance strukturiert erfolgt – oder in operative Überlastung führt.

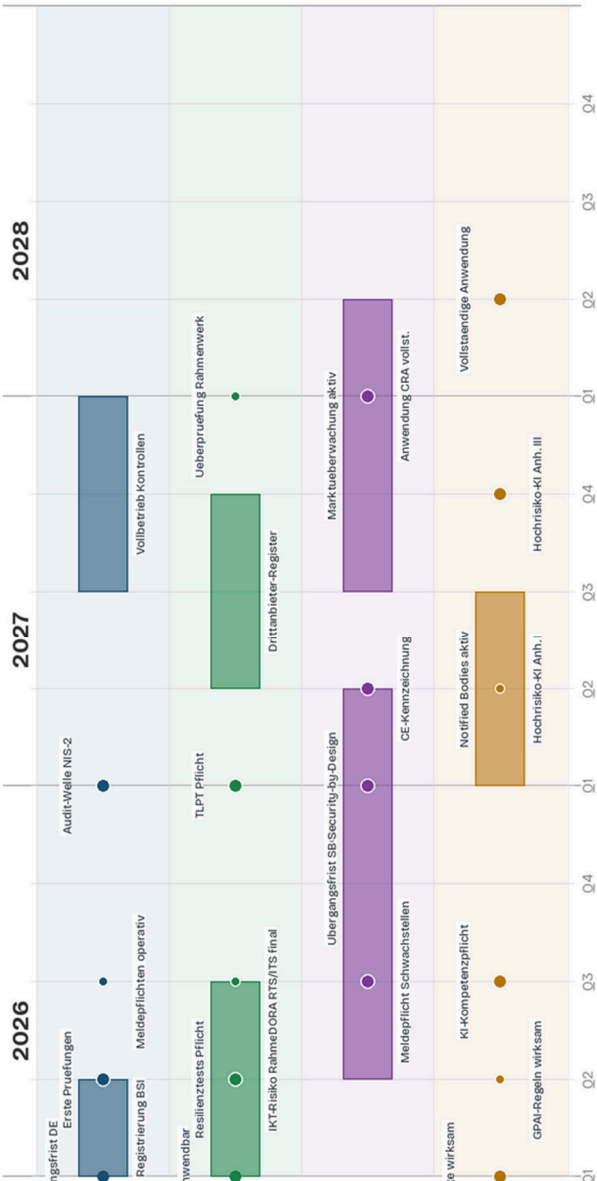
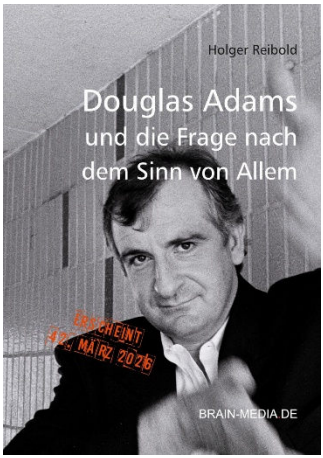


Abbildung 2: Zeitliche Einordnung zentraler regulatorischer Fristen und ihrer Überschneidungen im Zeitraum 2026–2028.

Mehr von Brain-Media.de

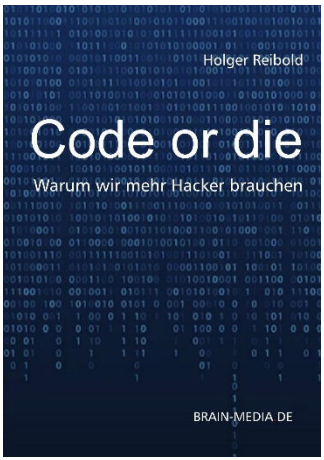


42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.
Umfang: 140 Seiten
Preis: 14,99 EUR
Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.
100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.
Umfang: 120 Seiten
Preis: 14,99 EUR

Lokale KI – Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen

RAG- und LLM-Plattformen mit klarer Architektur, Guardrails, Monitoring und Governance kontrolliert und resilient betreiben.
Umfang: 270 Seiten
Preis: 29,99 EUR

Knowledge as a Service (KaaS)

Compliance als operativer Vorteil

NIS-2, DORA, EU AI Act, CRA – der regulatorische Druck wird zum Geschäftsrisiko. KaaS (Knowledge as a Service) macht Ihr Unternehmen sicher und audit-ready – schnell, strukturiert und ohne externe Beratungsabhängigkeit. Statt fragmentierter Anforderungen und schwer umsetzbarer Vorgaben erhalten Sie ein System, das Compliance in operative Umsetzung überführt:

- klare, priorisierte Anforderungen
- direkt umsetzbare Templates
- auditfähige Dokumentation
- kontinuierlich aktualisierte Inhalte

Von Unsicherheit und Einzelmaßnahmen zu strukturierter, prüfbarer Umsetzung. KaaS reduziert Ihre Risiken, beschleunigt die Umsetzung und schafft Transparenz auf allen Unternehmensebenen.

Vier Varianten – für jeden Bedarf die passende Lösung

KaaS ist in vier Tarifen verfügbar: von Personal für Einzelpersonen und IT-Leiter über Team (empfohlen) für Compliance-Abteilungen und Berater bis zu Business für Mittelstand und IT-Dienstleister – und Enterprise für größere Unternehmen und KRITIS-Betreiber mit unbegrenzter Nutzerzahl. Ihren Fragen beantwortet unsere FAQ. Für Kunden steht eine 20seitige Einleitung zur Nutzung von KaaS bereit.

Individuelle Anforderungen

Kein Unternehmen ist wie das andere – Branche, Größe, Reifegrad und regulatorisches Umfeld unterscheiden sich signifikant. Sie haben individuelle Anforderungen? Wir setzen diese gerne um.