Ausgabe 5 Oktober 2025

Revisionspraxis

PRev

Journal für Revision, IT-Sicherheit, SAP-Sicherheit und Datenschutz

Kay Odenthal/Ute Seeber/Roger Odenthal
Digital und ohne Regeln – Prüferische IT-Anwendungen im Wandel

Erwin Rödler
KI im Prüfungswesen (Teil 2) – Werkzeuge und Methoden der KI und deren Anwendungsbereiche

Thomas Tiede
Sicherheit und Berechtigungen in der SAP HANA Cloud

Karsten Kinast
Datenverantwortung als Wettbewerbsvorteil – Compliance by Design im Zeitalter von KI, NIS-2, Data Act und Datenschutz

Stephanie Iraschko-Luscher
Dreh- und Angelpunkt moderner Datenschutzpraxis: Die Datenschutzfolgenabschätzung

Felix Sühlmann-Faul
Der gesellschaftliche Wert des Datenschutzes: Solidarität als Grundpfeiler der Demokratie im digitalen Zeitalter

Dominika Juszczyk
DSGVO-Nachweisbarkeit in der Praxis

Rechtsprechung und Aktuelles zum Datenschutz

www.prev.de

ISSN 1862-9032

BOORBERG

Inhalt

Revision 4.0

Digital und ohne Regeln – Prüferische IT-Anwendungen im Wandel 216

KI im Prüfungswesen (Teil 2) – Werkzeuge und Methoden der KI und deren Anwendungsbereiche 221

Sicherheit und Berechtigungen in der SAP HANA Cloud 226

Datenschutz

Datenverantwortung als Wettbewerbsvorteil – Compliance by Design im Zeitalter von KI, NIS-2, Data Act und Datenschutz 234

Dreh- und Angelpunkt moderner Datenschutzpraxis: Die Datenschutzfolgenabschätzung 241

Der gesellschaftliche Wert des Datenschutzes: Solidarität als Grundpfeiler der Demokratie im digitalen Zeitalter 248

DSGVO-Nachweisbarkeit in der Praxis 255

Rechtsprechung und Aktuelles zum Datenschutz 259

Neue Bücher 263

Nachrichten 266

Seminare/Veranstaltungen 269

Impressum/Vorschau 272

Bestellen Sie hier die PRev im Abonnement

Datenschutz

Dr. Michael Foth

Liebe Leserinnen und Leser,

im Beitrag *„Datenverantwortung als Wettbewerbsvorteil – Compliance by Design im Zeitalter von KI, NIS-2, Data Act und Datenschutz“* zeigt Karsten Kinast, wie Unternehmen durch strategisch geplante Datenverantwortung nicht nur ihre regulatorischen Pflichten erfüllen, sondern zugleich echte Wettbewerbsvorteile erzielen können. Der Beitrag verbindet rechtliche Grundlagen mit praxisnahen Umsetzungsperspektiven und betont insbesondere die Bedeutung eines ganzheitlichen GRC-Ansatzes, der Governance, Risiko- und Compliance-Management in einem konsistenten Rahmen zusammenführt. So wird deutlich, wie gesetzliche Vorgaben von der Systemarchitektur bis hin zu Geschäftsprozessen wirksam integriert werden können.

Die Datenschutz-Folgenabschätzung (DSFA) ist weit mehr als ein gesetzliches Pflichtinstrument – sie ist das Herzstück einer modernen, verantwortungsvollen Datenschutzpraxis. Als präventives Verfahren erlaubt sie es, Risiken für die Rechte und Freiheiten natürlicher Personen frühzeitig zu erkennen, geeignete Schutzmaßnahmen zu definieren und dadurch die Einhaltung der DSGVO nachhaltig zu sichern. Gerade im Umgang mit Künstlicher Intelligenz, die in Kommunikation, Analyse oder Prognoseverfahren immer größere Bedeutung gewinnt, wird die DSFA zum unverzichtbaren Werkzeug für Betreiber solcher Systeme. Im vorliegenden Beitrag zeigt Stephanie Iraschko-Luscher, wie die DSFA in der Praxis wirkt, welche besonderen Aspekte bei KI zu beachten sind und warum sie Vertrauen und Compliance gleichermaßen stärkt.

Die Debatte um Datenschutz konzentriert sich meist auf juristische Vorgaben und technische Maßnahmen – doch seine gesellschaftliche Dimension bleibt häufig unbeachtet. In seinem Beitrag „Der gesellschaftliche Wert des Datenschutzes: Solidarität als Grundpfeiler der Demokratie im digitalen Zeitalter“ zeigt Dr. Felix Sühlmann-Faul, dass Datenschutz weit mehr ist als ein individuelles Abwehrrecht: Er ist ein zentrales Element demokratischer Teilhabe. Ausgehend vom politikphilosophischen Konzept des „Schleiers des Nichtwissens“ von John Rawls eröffnet der Beitrag neue Perspektiven auf digitale Solidarität und deren Bedeutung für den gesellschaftlichen Zusammenhalt. Angesichts aktueller Bedrohungen durch Überwachungstechnologien, algorithmische Manipulation und Dark Patterns wird deutlich: Datenschutz ist weit mehr als ein individuelles Abwehrrecht – er ist ein demokratischer Imperativ des 21. Jahrhunderts.

Nachweisbarkeit ist nicht nur Kern der Rechenschaftspflicht nach der DSGVO, sondern zugleich eine der größten Herausforderungen bei ihrer Umsetzung. Dominika Juszczyk zeigt in ihrem Kurzbeitrag *„DSGVO-Nachweisbarkeit in der Praxis“*, dass Nachweispflichten nicht nur als regulatorische Last verstanden werden sollten. Richtig umgesetzt schaffen sie Effizienz, Transparenz und Risikominimierung. Anhand konkreter Dokumentationspflichten und praxisnaher Tipps verdeutlicht sie, wie Verantwortliche ihre Compliance stärken und gleichzeitig interne Abläufe optimieren können.

Viele neue Erkenntnisse und auch viel Spaß beim Lesen wünscht Ihnen

Ihr
Dr. Michael Foth

Karsten Kinast

Datenverantwortung als Wettbewerbsvorteil – Compliance by Design im Zeitalter von KI, NIS-2, Data Act und Datenschutz

1 Einleitung

In einer zunehmend datengetriebenen Wirtschaft wird der verantwortungsvolle Umgang mit Informationen nicht nur zur rechtlichen Pflicht, sondern zum strategischen Erfolgsfaktor. Im engeren Sinne bezeichnet der Begriff „Compliance" die Einhaltung der für ein Unternehmen und seine Mitarbeiter geltenden rechtlichen Bestimmungen.[1] Unternehmen stehen vor der Herausforderung, gesetzliche Anforderungen wie die Datenschutz-Grundverordnung (DSGVO), den Data Act, Digital Services Act, die NIS-2-Richtlinie sowie Regulierungen im Bereich Künstliche Intelligenz (KI-Verordnung) zu erfüllen – und gleichzeitig wettbewerbsfähig und innovativ zu bleiben.

In den vergangenen Jahren haben sich die traditionellen Disziplinen Corporate Governance, Risikomanagement und Compliance zu einem integrierten GRC-Ansatz (Governance, Risk und Compliance) verbunden. Ziel dieses Gesamtansatzes ist es, Parallelstrukturen aufzubrechen und alle unternehmerischen Abläufe effizient, wirksam und gesetzeskonform zu steuern.[2] „Compliance by Design" beschreibt in diesem Kontext den proaktiven Ansatz, rechtliche und ethische Anforderungen bereits in der Systemarchitektur und den Geschäftsprozessen zu verankern. So verpflichtet Art. 25 Abs. 1 DSGVO („Privacy by Design") Unternehmen zur Datensparsamkeit und zu technischen/organisatorischen Datenschutzmaßnahmen von der Konzeptionsphase an, während Art. 31 DSA („Compliance

1 Ebers, StichwortKommentar Legal Tech, Compliance, Digital Rn. 6, beck-online.
2 Ebers, StichwortKommentar Legal Tech, Compliance, Digital Rn. 28, beck-online.

by design"; „Konformität durch Technikgestaltung") Online-Plattform-Anbieter dazu anhält, ihre Benutzeroberflächen so zu gestalten, dass angeschlossene Händler alle vorvertraglichen Informationspflichten rechtssicher erfüllen können. Durch die GRC-Brille wird dieser Grundsatz zu einem ganzheitlichen Steuerungsinstrument, das Designentscheidungen, Risikobewertungen und Compliance-Kontrollen in einem einheitlichen Rahmen zusammenführt. Insbesondere in komplexen Anwendungsfeldern wie KI-Systemen oder kritischen Infrastrukturen wird damit die Integration von Datenschutz-, Sicherheits- und Transparenzvorgaben erleichtert.

Ziel dieses Beitrags ist es, die juristischen Rahmenbedingungen für Compliance by Design im Spannungsfeld von Datenschutz, Datenzugang, NIS-2 und KI-Regulierung zu beleuchten und aufzuzeigen, wie eine strategisch gedachte Datenverantwortung als Wettbewerbsvorteil genutzt werden kann. Der Beitrag verknüpft rechtliche Grundlagen mit praktischen Umsetzungsperspektiven und richtet sich sowohl an Juristen als auch an Fachleute aus Technik und Unternehmensführung.

2 Rechtlicher Rahmen

Die rechtlichen Anforderungen an datenverarbeitende Systeme und Organisationen haben sich in den vergangenen Jahren deutlich verschärft. Im Zentrum steht Art. 25 DSGVO, der das Prinzip des „Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" (Privacy by Design und by Default) normiert. Unternehmen sind damit verpflichtet, technische und organisatorische Maßnahmen zu implementieren, die den Schutz personenbezogener Daten bereits bei der Entwicklung und Konzeption von Systemen gewährleisten – und nicht erst im Nachhinein.

Ergänzt wird dieses Prinzip durch die NIS-2-Richtlinie (EU 2022/2555), die seit Anfang 2023 in Kraft ist und bis Oktober 2024 in nationales Recht umgesetzt werden musste. Sie verpflichtet insbesondere Betreiber kritischer und wichtiger Einrichtungen zu umfassendem Risikomanagement in Bezug auf Cybersicherheit (vgl. Art. 21 Abs. 2 NIS-2-RL). Dazu gehören unter anderem die Einführung technischer Schutzmaßnahmen, (Art. 21 Abs. 2 lit. d NIS-2-RL), die Schulung von Mitarbeitenden (Art. 21 Abs. 2 lit. g NIS-2-RL) und die Etablierung von Vorfallmanagementprozessen (Art. 21 Abs. 2 lit. e NIS-2-RL). Mit dem einhergehenden kommenden NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, dem Cyber Resilience Act erweitert sich damit die regulatorische Verantwortung über den Datenschutz hinaus auf eine ganzheitliche Sicherheits-Compliance.

Ein weiterer Baustein der europäischen Datenregulierung ist der Data Act, der seit Januar 2024 gilt und ab September 2025 anwendbar wird. Ziel ist es, einen fairen Zugang zu Nutzungsdaten vernetzter Produkte und Dienste zu schaffen. Dateninhaber müssen dafür bereits bei der Systemkonzeption („Access by Design") sicherstellen, dass Daten – personenbezogen oder nicht – strukturiert, sicher und unentgeltlich zugänglich sind (Art. 4 DA). Nutzer erhalten zudem das Recht, diese Daten an Dritte übertragen zu lassen (Art. 5 DA). Um Anbieterwechsel zu erleichtern, sind auch Interoperabilität und Portabilität von Cloud-Diensten verbindlich geregelt.

Künstliche Intelligenz (KI) nimmt einen hohen Stellenwert in der gesellschaftlichen Diskussion ein und erfordert die Beachtung datenschutzrechtlicher Anforderungen bereits bei der Entwicklung von Systemen. Die DSGVO ist aufgrund ihrer Technologieneutralität auch auf KI-Systeme und deren Entwicklung (Trainingsdaten, KI-Training) uneingeschränkt anwendbar. Die KI-Verordnung (KI-VO), die ab dem 1. August 2024 gilt, legt harmonisierte Vorschriften für KI fest. Mit der KI-VO verfolgt die EU einen risikobasierten Regulierungsansatz, der insbesondere Hochrisiko-KI-Systeme strengen Anforderungen unterwirft – etwa im Hinblick auf Datenqualität (Art. 10 KI-VO), Transparenz (Art. 13 KI-VO), Nachvollziehbarkeit (Art. 12 KI-VO) und menschliche Aufsicht (Art. 14 KI-VO) und adressiert damit den Compliance-by-Design-Ansatz.[3]

Die Verbindung dieser Regime – Datenschutz, IT-Sicherheit und KI-VO – führt zu einer komplexen, aber auch strategisch nutzbaren Compliance-Landschaft, in der „Compliance by Design" zum verbindenden Element wird.

3 Compliance by Design in der Praxis

Die Anforderungen der verschiedenen EU-Rechtsakte erfordern eine integrative Umsetzung von „Compliance by Design" in Unternehmen.

3.1 Technisch-organisatorische Maßnahmen

Eine der größten Herausforderungen bei der Umsetzung der europäischen Digitalgesetze besteht darin, dass Produkte und Dienste von Anfang an so konzipiert werden müssen, dass sie den komplexen Anforderungen

3 Wendt/Wendt Das neue KI-Recht/Wendt, 1. Aufl. 2024, §6 Rn. 5.

der unterschiedlichen Rechtsakte gerecht werden. Dies erfordert die Berücksichtigung verschiedenster Aspekte der technischen und organisatorischen Gestaltung.

a) Privacy by Design (DSGVO)

Der Grundsatz „Privacy by Design" ist in Art. 25 Abs. 1 der Datenschutz-Grundverordnung (DSGVO) verankert und fordert, dass datenschutzrechtliche Anforderungen bereits bei der Produktentwicklung durch Technikgestaltung erfüllt werden. Dies bedeutet, dass Unternehmen geeignete technische und organisatorische Maßnahmen (TOMs) implementieren müssen, um den Schutz personenbezogener Daten von Beginn an zu gewährleisten. Die DSGVO ist dabei technologieneutral ausgestaltet, was bedeutet, dass ihre Vorgaben für alle Verarbeitungsarten gelten, unabhängig von der verwendeten Technologie. Dies beinhaltet auch die Berücksichtigung datenschutzrechtlicher Anforderungen bei den Voreinstellungen („Privacy by Default"). In der Praxis umfasst das etwa den Einsatz von Cookie-Bannern, die Nutzern eine granulare Einwilligung ermöglichen, um die eigenen Datenschutzpräferenzen einzustellen und zu verwalten.[4] Ebenso zählt die konsequente Durchführung von Datenschutz-Folgenabschätzungen (DSFA) gemäß Art. 35 DSGVO bei risikoreichen Verarbeitungsvorhaben dazu.

b) Security by Design (NIS-2-RL)

Ähnlich wie der Datenschutz erfordert auch die Cybersicherheit eine «by Design»-Herangehensweise, auch wenn der Begriff «Security by Design» nicht explizit in der Richtlinie verwendet wird. Die NIS-2-Richtlinie zielt darauf ab, die Cybersicherheit in der gesamten EU branchenübergreifend zu stärken. Sie verpflichtet nach ihrem risikobasierten Ansatz in Art. 21 NIS-2-RL Einrichtungen dazu, geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen zu minimieren.[5] Zentrale Elemente sind etwa Zero-Trust-Architekturen, Multi-Faktor-Authentifizierung, Schwachstellenmanagement, Verschlüsselung, SIEM-gestützte Überwachung sowie EDR-Lösungen zur Bedrohungserkennung. Internationale Standards wie ISO/IEC 27001 dienen als Referenz. Ein besonderer Fokus liegt auf der Sicherheit der Lieferkette (Art. 21 Abs. 2 lit. d NIS-2-RL). Auch Zulieferer und Dienstleister sind in das Sicherheitskonzept einzubeziehen. Die Verantwortung liegt ausdrücklich bei der Geschäftsleitung. Die NIS-2-RL bietet mit Art. 21 einen konkreteren (nicht abschließenden) Maßnahmenkatalog als Art. 32 DSGVO und setzt ein höheres Mindestniveau an Schutzmaßnahmen für regulierte Einrichtungen voraus. Beide Regelwerke verfolgen einen risikobasierten Ansatz bei der Umsetzung technischer und organisatorischer Schutzmaßnahmen.

c) Access by Design (Data Act)

Der Data Act führt „Accessibility by Design" ein, um fairen Datenzugang zu sichern. Nach Art. 3 Abs. 1 DA müssen vernetzte Produkte und Dienste so hergestellt sein, dass ihre Daten – einschließlich Metadaten – standardmäßig für Nutzer einfach, sicher, unentgeltlich, umfassend, strukturiert, gängig und maschinenlesbar zugänglich sind. Diese Pflicht gilt für Produkte und Dienste, die nach dem 12. September 2026 in Verkehr gebracht werden.

Die direkte Zugänglichkeit kann beispielsweise durch einen direkt verbundenen Datenspeicher oder die Übermittlung von einem Server erfolgen, wobei der Zugang über ein Nutzerkonto geregelt werden kann. Der DA verpflichtet Verkäufer, Vermieter oder Leasinggeber von vernetzten Produkten sowie Anbieter verbundener Dienste, den Kunden vor Vertragsabschluss detaillierte Informationen über die generierbaren Daten, deren Format, die Möglichkeit des kontinuierlichen Echtzeit-Zugriffs sowie Speichermöglichkeiten bereitzustellen. Diese Informationspflichten sind zusätzlich zu denen der DSGVO zu beachten und erfordern einen entsprechenden Aufwand.[6] Für Klein- und Kleinstunternehmen sieht der DA gewisse Ausnahmen von den Pflichten zur Datenweitergabe vor. Der Anspruch auf Datenzugang ist für Nutzer einklagbar, und die Bereitstellung muss für den Nutzer unentgeltlich erfolgen.

Das Konzept „Access by Design" (Art. 3 f. DA) kann in der Produktentwicklung in einen Zielkonflikt mit „Privacy by Design" (insb. Art. 5 Abs. 1 lit. c, Art 17 DSGVO) geraten, da ein uneingeschränkter Datenzugang Risiken für die Privatsphäre der Nutzer und den Schutz der Geschäftsgeheimnisse des Dateninhabers birgt.[7] Aus diesen Spannungen entstehen zudem Haftungsrisiken bei Verstößen gegen die zahlreichen Datenweitergabeschranken des Data Acts.[8] Allerdings können und sollten beide Ansätze von Anfang an gemeinsam gedacht werden, um diesen Konflikt zu minimieren. Im Falle eines Widerspruchs genießt das Datenschutzrecht jedoch den Vorrang.[9]

4 Moosmayer/Lösler Corporate Compliance/Zech/Räther, 4. Aufl. 2024, 3. Kap. Rn. 18.
5 Grosmann/Michel, ZD 2025, 250.
6 Staudenmayer, NJW 2024, 1377.
7 Hartl/Vogel, LTZ 2024, 104; Apel/Huber, JuS 2024, 410.
8 Schäfer, GRUR 2025, 715.
9 Erwägungsgrund 7 S. 5 DA, vgl. Baumann/Brunnbauer, ZD 2025, 132.

3.2 Herausforderungen bei KI-Systemen (KI-VO)

„Compliance by Design" wird durch die spezifischen Eigenheiten von KI-Systemen und die neuen regulatorischen Vorgaben der KI-VO auf die Probe gestellt. Für Unternehmen, die KI einsetzen wollen, gilt es einige Herausforderungen zu bewältigen.

Ein zentrales Spannungsfeld ergibt sich zwischen dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und dem datengetriebenen Charakter von KI. Für die Entwicklung leistungsfähiger Modelle sind große, vielfältige und insbesondere qualitativ hochwertige Datensätze erforderlich. Diese Notwendigkeit steht jedoch im Widerspruch zur Pflicht, personenbezogene Daten auf das „erforderliche Maß" zu beschränken. Die Folge: Unternehmen müssen frühzeitig abwägen, welche Datenerhebung tatsächlich notwendig, legitim und vertretbar ist – ein klassischer Compliance by Design-Moment.[10] Weitere Komplexität entsteht beim Umgang mit sensiblen Daten. Die DSGVO untersagt deren Verarbeitung grundsätzlich (Art. 9), während die KI-VO (Art. 10 Abs. 5) sie in Hochrisiko-KI-Systemen zur Diskriminierungserkennung erlaubt. Generative oder nicht-hochriskante KI-Systeme fallen jedoch nicht unter diese Ausnahme – obwohl auch dort Bias-Risiken bestehen. Gleichzeitig fordern die Performance-Anforderungen der KI-VO (Art. 15) eine ausreichende Genauigkeit und Abdeckung diverser Nutzergruppen, was wiederum sensible Merkmale erforderlich machen kann. Dieses Spannungsverhältnis erzeugt Rechtsunsicherheit und erhöht das Haftungsrisiko. Die Wiederverwendung personenbezogener Daten im KI-Training ist ebenfalls rechtlich schwierig, da eine nachträgliche Einwilligung oft nicht praktikabel ist, und die Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) sekundäre Nutzungen begrenzt. Unternehmen müssen hier verstärkt auf Anonymisierung, Pseudonymisierung und synthetische Daten setzen, um konform und innovationsfähig zu bleiben.

Hinzu kommen umfangreiche Data-Governance-Pflichten, insbesondere für Hochrisiko-KI. Art. 10 KI-VO verlangt, dass Trainings-, Validierungs- und Testdaten relevant, repräsentativ, fehlerfrei und vollständig sind.[11] Unternehmen müssen daher datenqualitative Maßnahmen schon im Design etablieren – einschließlich systematischer Erhebung, Annotation, Bereinigung und Bias-Prüfung. Auch der sogenannte Memorization-Effekt, bei dem personenbezogene Informationen unbeabsichtigt „im Modell verbleiben", macht frühzeitige technische Schutzmechanismen unerlässlich.[12] Aufgrund der Komplexität und der Wechselwirkungen zwischen der KI-VO und der DSGVO ist eine robuste Data-Compliance-Governance erforderlich, die durch Legal Tech-Anwendungen unterstützt werden kann.[13] Bestehende Datenschutz-Management-Teams müssen sich diesbezüglich weiterentwickeln, um die rechtlichen Herausforderungen zu antizipieren und abzubilden.

10 Schreiber, ZfPC 2025, 46.
11 Schreiber, ZfPC 2025, 46.
12 Sachs/Meder, ZD 2024, 363.

3.3 Compliance als Schnittstelle zwischen Technik, Recht und Unternehmensprozessen

Die Vielzahl und Komplexität der neuen EU-Digitalgesetze schaffen eine umfassende, aber oft auch unklare und sich überschneidende Regulierungslandschaft. Dies erfordert eine kontinuierliche Zusammenarbeit zwischen IT, Recht und operativem Geschäft mit der Compliance Abteilung, um Compliance nicht als nachgelagerte Kontrolle, sondern als integralen Bestandteil der präventiven digitalen Produkt- und Prozessarchitektur zu verankern.[14] Die Umsetzung der Anforderungen kann nicht isoliert in einzelnen Fachabteilungen erfolgen, sondern erfordert eine kohärente und unternehmensweite Integration in alle Phasen des Produkt- und Dienstleistungslebenszyklus.[15]

a) Anpassung operativer Prozesse und Infrastrukturen

Ein zentraler Baustein einer wirksamen Compliance-Architektur betrifft die Anpassung der operativen Unternehmensprozesse und Infrastrukturen an die neuen regulatorischen Anforderungen. Insbesondere der DA und die KI-VO verlangen tiefgreifende technische und organisatorische Veränderungen in der Art und Weise, wie Unternehmen mit Daten umgehen.

So verpflichtet der Art. 3 Abs. 1 DA Unternehmen, Nutzern ihr Datenzugangsrecht sicherzustellen. Dies erfordert nicht nur die technische Fähigkeit, diese Daten in maschinenlesbaren Formaten bereitzustellen, sondern auch die Etablierung belastbarer Prozesse zur Wahrung der Datensicherheit und Datenintegrität. Parallel dazu sind Mechanismen zur kontrollierten Datenweitergabe an Dritte zu implementieren. Dabei ist der Schutz von Geschäftsgeheimnissen sowohl vertraglich als auch technisch abzusichern[16] – etwa durch Zugriffsbeschränkungen, Verschlüsselung und vertragliche Geheimhaltungsklauseln. Ein weiterer Schwerpunkt liegt auf der Gewährleistung von Interoperabilität. Unternehmen müssen offene Schnittstellen und standardisierte Formate schaffen, um Datenportabilität und Anbieterwechsel zu ermöglichen.

13 Hartl/Vogel, LTZ 2024, 104.
14 Bürkle/Hauschka/Schieffer Compliance-Officer/Bürkle/Schieffer, 2. Aufl. 2024, § 1. Rn. 48; Hartl/Vogel, LTZ 2024, 104.
15 Moosmayer/Lösler Corporate Compliance/Klahold/Lochen, 4. Aufl. 2024, § 13. Rn. 70-73.
16 Vogel, DSB 2025, 128, 131.

Bei der Datenverarbeitung im Rahmen von Hochrisiko-KI-Systemen im Sinne der KI-VO ist der Aufbau qualitätsgesicherter Prozesse zur Datenerhebung, -vorverarbeitung und -annotation sowie zur Identifikation und Schließung von Datenlücken erforderlich (vgl. Art. 10). Ein besonderer Fokus sollte hier grundsätzlich auf Maßnahmen zur Vermeidung systemischer Verzerrungen (Bias) liegen.[17] Da die Erfüllung dieser Anforderungen häufig im Spannungsfeld zur Datensparsamkeit der DSGVO steht, sind oft differenzierte verbindliche Risiko- sowie Folgenabschätzungen notwendig.

b) Rechtliche Absicherung und Dokumentation

Auch in rechtlicher Hinsicht sind bestehende Unternehmensprozesse umfassend zu überprüfen und anzupassen. Unternehmen müssen ihre Vertragsstrukturen – insbesondere im B2B-Bereich – an die Vorgaben des DA anpassen.[18] Faire, transparente und nichtdiskriminierende Bedingungen sind künftig verpflichtend (Art. 13 Abs. 1 DA). Die für Herbst 2025 angekündigten unverbindlichen Mustervertragsklauseln der EU-Kommission werden Orientierung bieten,[19] ersetzen aber keine individuelle Prüfung. Auch die neuen Informationspflichten vor Vertragsschluss des Art. 3 DA erfordern klare, adressatengerechte Kommunikation – ähnlich, aber zusätzlich zur DSGVO-Transparenz.[20] Zudem müssen Meldepflichten aus DSGVO und NIS-2-RL koordiniert werden, etwa bei Cyberangriffen mit Datenschutz- und Sicherheitsbezug.[21] Eine zentrale Incident-Response-Struktur ist hier ratsam.[22] Nicht zuletzt steigen die Anforderungen an eine nachvollziehbare Dokumentation. Die DSGVO (Rechenschaftspflicht nach Art. 5 Abs. 2 i. V. m. Art. 24) und NIS-2-RL (Art. 21 Abs. 2 lit. a) verlangen eine systematische Erfassung technischer und organisatorischer Maßnahmen (TOMs). Gerade im KI-Kontext müssen auch iterative Änderungen an Modellen und Systemen lückenlos dokumentiert werden – das erfordert eine enge Abstimmung zwischen Recht, IT und Compliance.

c) Verantwortung und Schulung

Compliance by Design steht und fällt mit den Menschen im Unternehmen. Technische Maßnahmen greifen nur, wenn sie verstanden und richtig angewendet werden. Ebenso ist kein Compliance-Ziel ohne das entsprechende Normen- und Rechtsbewusstsein der Betroffenen erreichbar.[23] Entsprechend fordern NIS-2-RL, KI-VO, DSGVO und DA eine kontinuierliche Qualifizierung der Mitarbeitenden – von der operativen Ebene bis zur Geschäftsleitung.

Die NIS-2-RL betont die Verantwortung der Führungsebene für das Cybersicherheits-Risikomanagement (Art. 20) und verpflichtet zu regelmäßigen Schulungen (Art. 21 Abs. 2 lit. g). Die KI-VO schreibt in Art. 4 Abs. 4 für Anbieter und Betreiber von KI-Systemen eine organisationsweite Schulungspflicht vor, insbesondere zu Themen wie Datenqualität, Transparenz und menschliche Aufsicht. Auch Art. 39 Abs. 1 lit. b DSGVO verlangt, dass Datenschutzbeauftragte die Einhaltung datenschutzrechtlicher Vorschriften etwa zum Umgang mit Betroffenenrechten, Rechtsgrundlagen, Verarbeitungszwecken und Dokumentationspflichten durch entsprechende Schulungsmaßnahmen fördern. Im Hinblick auf die Gewährleistung von Datenzugangsrechten, Weitergabeprozessen und Vertragsfairness des DA bedürfen zuständige Mitarbeitende ein solides Verständnis.[24]

In der Summe zeigt sich, dass der Erlass von Richtlinien und Prozessen allein nicht ausreicht. Es bedarf einer strukturierten, rollen- und normenspezifischen Schulungsarchitektur, die sowohl grundlegende Sensibilisierungen als auch vertiefte Fachschulungen umfasst. Nur so kann sichergestellt werden, dass Mitarbeitende Systeme, Software und KI-Anwendungen verantwortungsvoll nutzen und Risiken frühzeitig erkennen. Unternehmen, die Schulung als integralen Bestandteil ihrer Governance begreifen, stärken nicht nur ihre Sicherheitskultur, sondern schaffen die Grundlage für eine resiliente und zukunftsfähige Digitalisierung.

4 Datenverantwortung als strategischer Vorteil

Die rechtssichere und zweckgebundene Verarbeitung von Daten entwickelt sich – im Spannungsfeld von Datenschutz, Informationssicherheit und technologischer Innovation – zunehmend zu einem strategischen Differenzierungsmerkmal im Wettbewerb.

4.1 Vertrauen und Kundenbindung

Die Einhaltung datenschutzrechtlicher und sicherheitsbezogener Vorgaben wird zunehmend nicht nur als regulatorische Pflicht, sondern als strategischer Vorteil wahrgenommen. Unternehmen, die frühzeitig auf „Compliance by Design“ setzen, stärken das Vertrauen

17 Schäfer, ZD 2025, 12.
18 Apel/Huber, JuS 2024, 410.
19 https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained, letzter Zugriff 11.07.2025.
20 Vogel, DSB 2025, 128, 129.
21 Bitkom Papier: Digitalgesetzgebung der EU: Konfliktzonen und Wege zur Kohärenz, S. 15, Version 1.0, April 2025.
22 Zu den Meldepflichten von NIS-2 und DSGVO vgl. Hessel/Callewaert/Schneider, RDi 2024, 208.
23 Bussmann, CCZ 2016, 50, 55.
24 Vogel, DSB 2025, 128, 131.

ihrer Kunden und Partner[25] – ein immaterieller Wert, der in der digitalen Ökonomie zunehmend geschäftsentscheidend ist. Insbesondere in sensiblen Bereichen wie Gesundheitsdaten, Finanzinformationen oder KI-gestützten Entscheidungsprozessen erwarten Kunden heute nachvollziehbare, sichere und datenschutzkonforme Lösungen. Ein transparenter und verantwortungsvoller Umgang mit Daten wirkt reputationsfördernd[26] und kann zur nachhaltigen Kundenbindung beitragen.

Entgegen der weit verbreiteten Annahme, Compliance sei primär ein Innovationshemmnis, zeigt die Praxis, dass datenschutzkonforme und sicherheitsorientierte Systemarchitektur vielmehr als Innovationsmotor wirken kann. Wer Datenflüsse, Rechtearchitektur und Risikomanagement von Beginn an mitdenkt, entwickelt robustere, resilientere und marktfähigere Produkte. In einer Zeit, in der regulatorische Anforderungen stetig steigen, verschafft diese strategische Integration einen Wettbewerbsvorteil[27] – nicht zuletzt durch verkürzte Entwicklungszyklen, geringere Haftungsrisiken und erleichterte Marktzugänge, insbesondere in regulierten Sektoren.

4.2 Kommunikation und PR

Strategisch verankerte Datenverantwortung birgt nicht nur operative Vorteile, sondern auch reputationsbildende.[28] Unternehmen, die Compliance by Design transparent kommunizieren und als Teil ihrer Markenidentität etablieren, senden ein starkes Signal an Kunden, Investoren und die Öffentlichkeit. In Zeiten wachsender Skepsis gegenüber datenverarbeitenden Technologien wird Vertrauen zur Schlüsselressource. Besonders in sensiblen Branchen – etwa Finanzen, Medizintechnik oder Bildung – beeinflusst die Wahrnehmung verantwortungsvoller Datenpraxis Kauf- und Investitionsentscheidungen maßgeblich. In diesen regulierten Branchen korrespondiert eine durchdachte Compliance-Kommunikation eng mit Public Relations, Markenstrategie und Wettbewerbsvorteilen.[29] Wer nicht nur compliant ist, sondern dies auch sichtbar macht, positioniert sich als Vorreiter einer digitalen Unternehmenskultur, die regulatorische Verantwortung als Wertversprechen versteht.[30]

Compliance-Kommunikation ist dabei mehr als Regelvermittlung. Sie stärkt durch gezielte, adressatengerechte Ansprache das Verständnis und die Akzeptanz – intern wie extern.[31] Durch gezielte, zielgruppenspezifische Ansprache (Mitarbeiter, Führungskräfte, Geschäftspartner, Öffentlichkeit) schafft sie Verständnis, Akzeptanz und aktive Unterstützung für Compliance-Maßnahmen.[32] So trägt sie zur Etablierung einer wertebasierten Unternehmenskultur bei und reduziert zugleich Haftungs- und Reputationsrisiken.[33] Als Teil der Marken- und Kommunikationsstrategie wird sie damit zum Differenzierungsmerkmal im Wettbewerb – insbesondere in einem Umfeld, in dem unternehmerische Integrität zunehmend über Marktzugang und Kundenbindung entscheidet.

4.3 Beispiele aus der Praxis

Zahlreiche Unternehmen haben diesen Ansatz bereits erfolgreich umgesetzt: Globale Anbieter wie Microsoft[34] betonen öffentlich ihre Datenschutz- und KI-Selbstverpflichtungen – etwa zur Datenspeicherung in Europa oder zur transparenten Steuerung von KI-Systemen. Für Microsoft hat die Einhaltung europäischer Compliance-Standards strategische Relevanz. Als US-Unternehmen unterliegt es dem Cloud Act, der US-Behörden extraterritorialen Datenzugriff ermöglicht – was insbesondere im Kontext der DSGVO zu einem hohen rechtlichen Risiko führt. Zugleich steht viel auf dem Spiel, da die EU einer der größten Märkte für Microsoft ist, mit zahlreichen Großkunden – darunter die Europäische Kommission.[35] Der Verlust regulatorischen Vertrauens könnte daher zu einem massiven Reputations- und Umsatzrisiko führen. Entsprechend zielgerichtet agiert Microsoft in seiner Kommunikationsstrategie. Mit der im April 2025 veröffentlichten Selbstverpflichtung „European Cloud and AI Sovereignty Commitments" positioniert sich das Unternehmen offensiv als Partner eines digitalen Europas, der europäische Werte respektiert. Bereits im Juni folgte die Präsentation konkreter technischer Maßnahmen („Comprehensive Sovereign Solutions"), darunter regional abschottbare Cloud-Angebote, und dedizierte Schlüsselverwahrung. Diese zeitlich eng getaktete Kommunikationsstrategie verfolgt erkennbar

25 ISO 31700-1, Consumer protection – Privacy by design for consumer goods and services – Part 1: High-level requirements, First edition 2023-01, S. vii.
26 Zu den reputationsschädigenden Folgen von Non-Compliance am Beispiel Wirecard: Moosmayer/Lösler Corporate Compliance/Schorn/Viebranz, 4. Aufl. 2024, § 11. Rn. 14.
27 Differenzierend: Schäfer, GRUR 2025, 715.
28 Vgl.: Trüg, NZWiSt 2022, 106.
29 https://www.compliance-manager.net/artikel/compliance-ist-kommunikation/, letzter Zugriff am 16.06.2025.
30 Bussmann, CCZ 2016, 50.
31 https://www.compliance-manager.net/artikel/compliance-ist-kommunikation/, letzter Zugriff am 16.06.2025.
32 https://www.compliance-manager.net/artikel/compliance-ist-kommunikation/, letzter Zugriff am 16.06.2025.
33 Klaas/Momsen/Wybitul DatenschutzsanktionenR-HdB/Brams, 1. Aufl. 2023, § 6 Rn. 59; Forgó/Helfrich/Schneider Betr. Datenschutz-HdB/Spies/Kraska Teil XIII. Kap. 1 Rn. 33.
34 https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/, letzter Zugriff am 23.06.2025.
35 https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-follows-compliance-european-commissions-use-microsoft-365_en, letzter Zugriff am 09.07.2025.

das Ziel, regulatorische Bedenken proaktiv zu adressieren, Vertrauen aufzubauen und die Marktposition in einem zunehmend souveränitätsbewussten Europa zu festigen. Ob diese Versprechen rechtlich belastbar sind, bleibt jedoch kritisch zu prüfen – insbesondere im Hinblick auf tatsächliche Zugriffsmöglichkeiten durch US-Behörden und die faktische Unabhängigkeit der europäischen Infrastrukturen.

Auch die Volkswagen AG geht nach einem Bußgeld im Jahr 2022[36] wegen datenschutzrechtlicher Defizite bei Fahrassistenzsystemen aktiv den Weg von Compliance by Design und sucht proaktiv den Schulterschluss mit den Aufsichtsbehörden. In enger Zusammenarbeit[37] werden seither Assistenz- und Sicherheitssysteme datenschutzkonform gestaltet – mit Fokus auf Datenminimierung, Zweckbindung und frühzeitiger Risikoanalyse. Volkswagen zeigt damit, dass Datenschutz von Beginn an mitgedacht und regulatorische Kooperation als strategisches Gestaltungsinstrument genutzt werden kann. Ein Beispiel aus dem Gesundheitssektor zeigt die OPASCA GmbH[38], die frühzeitig auf die Anforderungen der NIS-2-RL reagierte und sich bereits 2022 nach ISO 27001 zertifizieren ließ. Sie setzt auf eine mehrschichtige Sicherheitsarchitektur mit technischer Absicherung, Systemmonitoring und regelmäßigen Schulungen. Damit integriert das Unternehmen Cybersicherheit und Datenschutz konsequent in seine Produktentwicklung und zeigt, dass Compliance by Design auch im sensiblen Gesundheitssektor strategisch mit passender PR Kommunikation umgesetzt werden kann.

5 Fazit und Ausblick

Compliance by Design ist nicht lediglich ein operativer Mechanismus zur Vermeidung von Regelverstößen und zum Reduzieren von Bußgeldern[39], sondern ein rechtlich-normativer Gestaltungsansatz, der es Unternehmen ermöglicht, regulatorische Anforderungen systematisch, proaktiv und strukturell in Geschäftsprozesse, Produkte und Technologien zu integrieren. Er verkörpert einen Paradigmenwechsel: weg von reaktiver Regelbefolgung, hin zur präventiven, rechtsdogmatisch fundierten Strukturierung unternehmerischer Wertschöpfung. Im Zentrum steht die frühzeitige Antizipation rechtlicher Risiken und Pflichten – insbesondere im Kontext des Datenschutzes (Art. 25 DSGVO), der Datenweitergabe, der Produkthaftung, des Wettbewerbsrechts, der KI-VO sowie sektorspezifischer Aufsichtsnormen (z. B. NIS-2, MaRisk, BAIT, DORA). Compliance wird damit Teil des unternehmerischen Steuerungssystems – und nicht bloß ein nachgelagerter Kontrollprozess. Die rechtlich gebotene Implementierung technischer und organisatorischer Maßnahmen (TOMs), risikoadäquater Governance-Strukturen und rechtskonformer Designentscheidungen wirkt präventiv und haftungsmindernd – zivil-, straf- wie aufsichtsrechtlich.

Aus ökonomischer Sicht transformiert sich Compliance durch diesen systematischen Designansatz in ein strategisches Asset: Unternehmen, die regulatorische Anforderungen nicht nur erfüllen, sondern operationalisieren, können komplexe Produkte schneller auf den Markt bringen, internationale Zulassungsanforderungen effizienter adressieren und Vertrauen bei Stakeholdern – insbesondere Regulierungsbehörden, Investoren und Geschäftspartnern – nachhaltig stärken. Die Einhaltung von Compliance durch Design schafft eine belastbare Legalitäts- und Legitimitätsgrundlage für digitale Geschäftsmodelle. Die flankierende Compliance-Kommunikation – intern wie extern – wirkt dabei reputationsbildend und trägt zur Verankerung einer Compliance-Kultur bei. Sie ist jedoch ein abgeleitetes Instrument, kein Selbstzweck: Die eigentliche Compliance-Leistung liegt in der rechtskonformen, integrierten und belastbaren Gestaltung von Strukturen, Prozessen und Technologien.

36 Pressemitteilung der LFD Niedersachsen vom 26.07.2022; https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/1-1-millionen-euro-bussgeld-gegen-volkswagen-213835.html , letzter Zugriff am 23.06.2025.

37 Pressemitteilung des LfDI Baden-Württemberg vom 22.04.2025, https://www.baden-wuerttemberg.datenschutz.de/vw-datenverarbeitung-austausch/, letzter Zugriff 23.06.2025.

38 https://opasca.com/nis-2-richtlinie-gesundheitssektor-opasca/?lang=de, letzter Zugriff 23.06.2025.

39 Zur Berücksichtigung eines Compliance-Management-Systems bei der Bußgeldbemessung vgl. BGH, Urt. v. 9.5.2017 – 1 StR 265/16, BeckRS 2017, 114578.

Rechtsanwalt **Dr. Kinast** ist Gründer und geschäftsführender Gesellschafter von KINAST Rechtsanwälte. Er ist Externer Datenschutzbeauftragter zahlreicher nationaler und internationaler Großkonzerne, Banken und Versicherungen sowie Organisationen der Kirche und öffentlichen Hand. Weiterhin berät Herr Dr. Kinast als Externer Compliancebeauftragter diverse Unternehmen der verschiedensten Branchen.