Digitalisierung und Corporate Governance: Was Unternehmensorgane jetzt wissen müssen

Die digitale Transformation ist längst keine reine IT-Angelegenheit mehr – sie ist Chefsache. Ein sich rapide verdichtendes EU-Regulierungspaket aus KI-Verordnung, digitalem Resilienzrecht und verschärften Haftungsregeln stellt Vorstände, Geschäftsführer und Aufsichtsräte vor neue, handfeste Pflichten. Wer jetzt nicht handelt, riskiert nicht nur empfindliche Bußgelder, sondern auch persönliche Haftung. Dieser Beitrag gibt einen strukturierten Überblick über die drei zentralen Entwicklungsfelder.

1. KI-Governance als neue Leitungsaufgabe: Die EU-KI-Verordnung (AI Act)

Mit der Verordnung (EU) 2024/1689 – dem sogenannten **AI Act** – hat die Europäische Union weltweit als erste Rechtsordnung ein umfassendes Regelwerk für Künstliche Intelligenz geschaffen [1]. Die Verordnung ist am **1. August 2024** in Kraft getreten und entfaltet ihre Wirkung gestaffelt:

- **Seit dem 2. Februar 2025** gelten das Verbot bestimmter KI-Praktiken (z. B. manipulative oder diskriminierende KI-Systeme) sowie die Pflicht zur **KI-Kompetenz (*AI Literacy*)** aller mit KI befassten Mitarbeiterinnen und Mitarbeiter [1] [2].
- **Ab dem 2. August 2025** sind die Governance-Vorschriften und Pflichten für Anbieter sogenannter Allzweck-KI-Modelle (*General-Purpose AI, GPAI*) verbindlich [2].
- **Ab dem 2. August 2026** gelten die umfassenden Anforderungen für Hochrisiko-KI-Systeme [1].

Für Unternehmen bedeutet der AI Act vor allem eines: **Transparenz, Governance und Kompetenzaufbau werden zu regulatorischen Pflichtaufgaben** [3]. Hochrisiko-KI-Systeme – etwa bei der Personalauswahl, der Kreditvergabe oder im Risikomanagement – unterliegen strengen Anforderungen an Datenqualität, Nachvollziehbarkeit und menschliche Aufsicht [2]. Die Bußgelder sind erheblich: Bei Verstößen gegen verbotene KI-Praktiken drohen Geldbußen von bis zu **35 Millionen Euro oder 7 % des weltweiten Jahresumsatzes** – je nachdem, welcher Betrag höher ist [1] [4].

In Deutschland fungiert die **BaFin** als KI-Aufsichtsbehörde im Finanzsektor, flankiert durch die **Bundesnetzagentur** als zentrale Marktüberwachungsbehörde und das **BSI** für

technische Standards [3]. Auf EU-Ebene koordiniert das neu etablierte **AI Office** der Kommission die Umsetzung [4].

Ein Blick in die Praxis zeigt: Während des Geschäftsjahres 2025 hatten erst rund **40 % der europäischen Großunternehmen** eine formale KI-Richtlinie oder zumindest eine dokumentierte Aufsicht über KI-Risiken eingeführt – die Mehrheit ist hier noch im Rückstand [5]. Für Unternehmen, die KI bereits heute einsetzen, besteht dringender Handlungsbedarf.

2. Digitale Resilienz: DORA, NIS2 und Cyber Resilience Act

Parallel zum AI Act hat die EU in den vergangenen Monaten ein dichtes Netz an Vorschriften zur **digitalen Betriebssicherheit und Cybersicherheit** geknüpft, das unmittelbar Governance-Relevanz hat.

DORA – Digital Operational Resilience Act

Der **Digital Operational Resilience Act (DORA, Verordnung EU 2022/2554)** ist seit dem **17. Januar 2025 verbindlich anzuwenden** und richtet sich an Finanzunternehmen: Banken, Versicherungen, Zahlungsdienstleister und viele weitere regulierte Institute [3]. DORA harmonisiert erstmals europaweit die Anforderungen an die **digitale Betriebssicherheit** und schafft einen einheitlichen Rechtsrahmen für den Finanzsektor [3].

Die zentralen Pflichten umfassen:
- **Robustes IKT-Risikomanagement** für eigene und extern eingekaufte IT-Systeme (Cloud-Dienste, Software-Dienstleister)
- **Meldepflichten** für schwerwiegende IT-Sicherheitsvorfälle gegenüber der BaFin
- **Regelmäßige Resilienztests**, darunter sogenannte *Threat-led Penetration Tests (TLPT)*
- **Anpassung aller Verträge** mit IKT-Drittdienstleistern gemäß den DORA-Vorgaben [3]

Wichtig für Compliance-Verantwortliche: DORA ist kein einmaliges Umsetzungsprojekt, sondern ein **dauerhafter Ordnungsrahmen**. Im Verhältnis zur allgemeinen NIS2-Richtlinie gilt für DORA-pflichtige Finanzunternehmen das Spezialitätsprinzip – DORA-Regeln gehen den NIS2-Vorschriften vor [6]. Darüber hinaus hat die BaFin im Dezember 2025 eine Orientierungshilfe zur Behandlung von **IKT-Risiken beim KI-Einsatz** unter DORA veröffentlicht [6].

Cyber Resilience Act (CRA)

Der **Cyber Resilience Act** trat im Dezember 2024 in Kraft. Er verpflichtet Hersteller und Anbieter von Produkten mit digitalen Elementen zu Mindestsicherheitsanforderungen und Meldepflichten bei Sicherheitslücken. Die **vollständige Anwendung ist ab Dezember 2027** vorgesehen, Meldepflichten greifen bereits ab September 2027 [3]. Für Unternehmen empfiehlt sich jetzt eine strukturierte Bestandsaufnahme: Welche eingesetzten oder vertriebenen Produkte fallen in den Anwendungsbereich des CRA?

3. Haftungs- und Organpflichten im digitalisierten Unternehmen

Die regulatorische Verdichtung hat eine unmittelbare gesellschaftsrechtliche Dimension: Digitale Compliance ist nicht delegierbar – sie ist **Leitungsverantwortung**.

Sorgfaltspflichten von Vorstand und Geschäftsführung

Nach allgemeinen gesellschaftsrechtlichen Grundsätzen (§ 93 AktG, § 43 GmbHG) haben Geschäftsleiter die Sorgfalt eines ordentlichen und gewissenhaften Kaufmanns anzuwenden. Vor dem Hintergrund des AI Act, DORA und NIS2 bedeutet dies konkret: Die Geschäftsleitung muss sicherstellen, dass das Unternehmen über geeignete **Governance-Strukturen für den KI- und IT-Einsatz** verfügt [7]. Ein integriertes IT- und KI-Governance-Compliance-Managementsystem, das relevante Normen miteinander verzahnt und Verantwortlichkeiten entlang des **Three-Lines-of-Defense-Modells** klar verteilt, ist dabei ein wesentlicher Baustein zur Haftungsminimierung [7].

KI-Governance als Aufgabe des Aufsichtsrats

Der Aufsichtsrat ist gefordert, die KI- und Digitalstrategie des Unternehmens aktiv zu begleiten. Empirische Daten zeigen, dass rund **90 % der europäischen institutionellen Investoren** Schutzmaßnahmen und eine klare Aufsicht über KI-Risiken durch das Board einfordern [5]. Die Mehrheit der befragten Investoren erwartet dabei keine KI-Spezialisten im Aufsichtsrat, wohl aber ein *gesamtheitliches* Governance-Verständnis auf Gremiumsebene [5]. In der Praxis integrieren die meisten Unternehmen die KI-Aufsicht in bestehende Ausschüsse (z. B. Prüfungs- oder Risikoausschuss) oder weisen sie dem Gesamtgremium zu [5].

KI-Governance und Unternehmenshaftung

Besondere Bedeutung kommt dem Zusammenspiel von AI Act und unternehmensinterner Haftungsstruktur zu. KI-Governance wird zunehmend als **Parameter der Angemessenheit**

von Organisationsstrukturen verstanden. Ein fehlendes oder unzureichendes KI-Governance-Framework kann als Indikator für **Organisationsverschulden** gewertet werden und – wo entsprechende nationale Umsetzungsgesetze greifen – auch Konsequenzen für die Unternehmenshaftung haben [8]. Der AI Act fordert zudem für Hochrisiko-KI-Systeme ein **Recht auf Erklärung** individueller KI-gestützter Entscheidungen, was Unternehmen verpflichtet, die Transparenz und Nachvollziehbarkeit ihrer KI-Systeme intern abzusichern [8].

Was bedeutet das für Sie? – Eine Zusammenfassung

Die Schnittstelle von Digitalisierung und Corporate Governance ist zum **zentralen Haftungsfeld** für Unternehmensorgane geworden. Drei Handlungsfelder stehen dabei im Vordergrund:

1. **KI-Bestandsaufnahme und Risikoklassifizierung:** Identifizieren Sie alle im Unternehmen eingesetzten KI-Systeme und ordnen Sie diese den Risikokategorien des AI Act zu. Stellen Sie sicher, dass verbotene KI-Praktiken abgestellt und Mitarbeitende mit ausreichender KI-Kompetenz ausgestattet sind – diese Pflicht gilt bereits seit Februar 2025.

2. **Digitale Resilienz als Daueraufgabe:** Überprüfen Sie alle Verträge mit IT-Dienstleistern auf DORA-Konformität und etablieren Sie ein laufendes IKT-Risikomanagement. Für den Finanzsektor ist dies heute Pflicht; für andere Branchen empfiehlt sich eine frühzeitige Vorbereitung auf den Cyber Resilience Act.

3. **Governance-Strukturen auf der Leitungsebene:** Verankern Sie KI- und Cyber-Governance in der Unternehmensorganisation – sei es durch einen dedizierten KI-Ausschuss, die Zuordnung der Verantwortung in bestehende Gremien oder durch ein integriertes Compliance-Management-System. Die Dokumentation dieser Strukturen ist nicht nur regulatorisch geboten, sondern schützt auch vor persönlicher Haftung.

Haben Sie Fragen zu den dargestellten Regulierungen oder benötigen Sie Unterstützung bei der Umsetzung in Ihrem Unternehmen? Wir beraten Sie gerne.

IHR ANSPRECHPARTNER

Georg Mörchel

IT-, Datenschutz- und Wirtschaftsrecht

Rechtsanwalt

BERGISCHE SEKUNDANZ - Rechtsanwälte Lichtinghagen & Partner mbB
0221 / 9854 - 9999
kanzlei@bergische-sekundanz.de
Bornerhof 5-7, 51643 Gummersbach - Haus Kerberg
www.bergische-sekundanz.de

Online weiterlesen

Aktuelle Fassung dieses Fachbeitrags

www.bergische-sekundanz.de/journal/digitalisierung-und-corporate-governance-was-unternehmensorgane-jetzt-wissen-muessen