



CLYDE&CO

Europäische Digitalregulierung und ihre Auswirkungen auf Haftung und Versicherungsschutz

27. MCC Kongress, IT-Optionen für Versicherungen

Pavel Rahlov, Rechtsanwalt, Clyde & Co

Agenda

-  Regulatorische Rahmenbedingungen im Überblick
-  Haftungsrechtliche Implikationen
-  Versicherungsrechtliche Implikationen



Die Regulatorik im Überblick

BSIG, DORA, AI-Act, CRA

Das neue BSIG

Überblick



NIS-2-Umsetzungsgesetz

- Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung des Informationssicherheitsmanagements in der Bundesverwaltung mit Wirkung **zum 06.12.2025 in Kraft getreten**
- Gesetz führt insb. zu einer umfassenden Novellierung des BSI-Gesetzes



Anwendungsbereich

- Deutschland: rund **29.500 Unternehmen** (vgl. [BSI - NIS-2](#))
- Bisher: Kritische Infrastruktur, digitale Dienste, Unternehmen im besonderen öffentlichen Interesse
- Jetzt: „**Besonders wichtige Einrichtungen**“ und „**Wichtige Einrichtungen**“



Was ändert sich im BSI-Gesetz?

- Ausweitung des Anwendungsbereichs (§ 28 BSIG)
- Registrierungs- und Meldepflichten
- Ausweitung Eingriffsmöglichkeiten BSI (Auskünfte, Untersuchungen, Weisungen/Anordnungen)
- Bußgelder (§ 65 BSIG)



Kernstück des neuen BSIG

- Pflicht zur Implementierung und Dokumentation von **Risikomanagementmaßnahmen** (§ 30 BSIG)

Das neue BSIG

Überblick

(2) ¹Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. ²Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. **Aufrechterhaltung des Betriebs**, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
10. **Verwendung von Lösungen zur Multi-Faktor-Authentifizierung** oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

„**wichtige Einrichtungen**“

Der Digital Operational Resilience Act (DORA)

Überblick



Gegenstand des Gesetzes

- EU-Verordnung zur digitalen Resilienz im Finanzsektor
- DORA und NIS-2 verfolgen dasselbe Ziel:
Aufstellen von Mindeststandards für die Cyber-Resilienz



Kernthemen des DORA

- Pflicht zur Einrichtung eines umfassenden **IT-Risikomanagements**
- **Governance- und Überwachungspflichten** der Geschäftsleitung
- **Dokumentations- und Nachweispflichten**



Anwendungsbereich

- **Unmittelbar** erfasst sind **Finanzunternehmen** (insb. Kreditinstitute, Versicherungsunternehmen)
- **Mittelbar** können auch **IT-Dienstleister** als Lieferanten der regulierten Unternehmen betroffen sein

Der AI-Act

Überblick



Gegenstand des Gesetzes

- Erste umfassende KI-Regulierung weltweit
- Regelt technische und organisatorische Maßnahmen für verschiedene Arten von KI-Systemen nach risikobasiertem Ansatz



Anwendungsbereich

- Marktteilnehmer der KI-Wertschöpfungskette, also **Anbieter, Einführer, Händler** und **Betreiber**.



Kernthemen des AI-Act

- Hohe Anforderungen für **Hochrisiko-KI-Systeme**, gefolgt von KI-Systemen für **allgemeine Verwendungszwecke**.
- **Transparenzpflichten** für KI-Systeme mit geringem Risiko.
- Durchsetzung mittels **Untersuchungs- und Anordnungsmaßnahmen** durch Behörden.
- Sanktionen durch **Geldbußen**

Der Cyber Resilience Act (CRA)

Überblick



Gegenstand des Gesetzes

- EU-Verordnung für Produkte mit digitalen Elementen
- Ziel ist die Verbesserung der Cybersicherheit von Produkten mit digitalen Elementen
- Definition verbindlicher Cybersicherheitsanforderungen über den gesamten Produktionszyklus



Anwendungsbereich

- „Produkte mit digitalen Elementen“
- Betrifft insb. Softwarehersteller, SaaS-Anbieter und Hardwarelieferanten



Kernthemen des CRA

- **Security by Design** und **Security by Default** als regulatorischer Standard
- Sichere Entwicklung von Produkten
- Vulnerability Management
- Sicherheitsupdates über den Produktlebenszyklus
- Technische Dokumentation und Konformitätsnachweise

The background features a dark, textured surface with a network of glowing blue nodes connected by thin lines, suggesting a digital or molecular structure. A solid teal square is positioned in the upper right quadrant.

Haftungsrechtliche Auswirkungen

Mögliche Haftungsszenarien

BSIG/DORA

- Primäres Haftungsrisiko: **Bußgelder**
- Gem. § 65 BSIG (insb. wegen **fehlender/unzureichender Umsetzung der Maßnahmen nach § 30**): bis zu **1,4 %** (wichtige Einrichtungen) bzw. **2 %** (besonders wichtige Einrichtungen) des Gesamtumsatzes
- Geschäftsleiterhaftung nach dem Gesellschaftsrecht (§ 38 Abs. 1, 2 BSIG)

CRA

- Mögliche Ansprüche gg. Hersteller wg. **Sicherheitslücken** in Software, fehlerhaftem **Vulnerability-Management**, verspäteter Bereitstellung von **Patches**, unsicherer **Standardeinstellungen**
- Erweiterung des Sorgfaltsmaßstabs und potenzielle Steigerung der Inanspruchnahmen

AI-Act

- Mögliche Ansprüche gg. Gesellschaft wg. **fehlerhaften** KI-Empfehlungen, **diskriminierenden** Entscheidungen, **Halluzinationen**, fehlerhaften automatisierten Prozessen, **mangelhafter menschlicher Aufsicht**
- Schwierige Kausalitäts- und verantwortungsfragen

Keine eigenständige Haftungsregelungen – Regelungen können aber zur Konkretisierung von einzuhaltenden Pflichten herangezogen werden

The background features a dark, textured surface with a network of glowing blue nodes and connecting lines, suggesting a digital or molecular structure. A solid teal square is positioned in the upper right quadrant.

Deckungsrechtliche Auswirkungen

BSIG

Auswirkungen auf die Cyberversicherung – Produkt-Gestaltung

- **Fällt Unternehmen in den Anwendungsbereich? Ist es registriert? Welche Dokumentation liegt vor?**
 - Was ist, wenn Unternehmen selbst nicht erkannt hat, dass es unter die das BSIG fällt? Organisationsverschulden?
 - Wichtig: Die Kosten der Prüfung der Anwendbarkeit des BSIG sind nicht versichert
- **Anpassung der Incident-Response-Dienstleistungen?**
 - Abgestuftes Meldeverfahren bei erheblichen Sicherheitsvorfällen (vom Versicherungsschutz umfasst? Panel-Dienstleister vorbereitet?)
 - Besonders wichtigen Einrichtungen: Unverzüglich, spätestens binnen **24 Stunden**, vgl. § 32 BSIG
- **Bedeutung des Deckungsbausteins für „Regulatorische Verfahren“ (Verwaltungs-RS)**
- **Bedarf an Bußgelddeckungen steigt weiter**
 - Versicherbarkeit von Bußgeldern ist weiterhin umstritten
- **Anpassung vorvertraglicher Risikofragen / technischer Obliegenheiten**



BSIG

Auswirkungen auf die Cyberversicherung - Schadensregulierung

- **Bewertung vorvertraglicher Risikoangaben des Versicherungsnehmers**
 - Ein (Cyber-)Versicherer darf berechtigterweise erwarten, dass VN die Risikofragen des Versicherers **auf Basis gesicherter Kenntnis** und unter **Berücksichtigung anerkannter technischer Standards** beantwortet (OLG Schleswig Beschl. v. 9.1.2025 – 16 U 63/24, [NJW-RR 2025, 416 - beck-online](#))
- **Ausschluss für wissentliche Pflichtverletzungen, vgl. z.B.: A1-17.9 AVB Cyber 2024 („durch wissentliches Abweichen von Gesetz“)**
 - Pflichten aus §§ 38, 30 BSIG als „technische Kardinalpflichten“?
- **Relevanz für Obliegenheiten zur Einhaltung gesetzlicher Sicherheitsvorschriften**
 - Beispiel: A1-16.2 a) AVB Cyber 2024: „Darüber hinaus hat der Versicherungsnehmer alle **gesetzlichen**, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften einzuhalten“
 - BGH: Klausel ist ausreichend transparent und wirksam (vgl. BGH, Urt. v. 25.09.2024 – IV ZR 350/22)
- **Einhaltung des gesetzlich vorausgesetzten Sicherheitsstandards als Mindeststandard für die Erfüllung sonstiger vertraglicher Obliegenheiten?**
 - Z. B.: Stand-der-Technik-Klauseln oder Generalklauseln, zur Einhaltung „angemessener Sicherheitsmaßnahmen“

BSIG

Auswirkungen auf die D&O-Versicherung – Verschiebung des Sorgfaltsmaßstabs

- **Höheres Organhaftungsrisiko**
 - Das BSIG stellt die Geschäftsleitung (noch stärker) in die Verantwortung
 - § 38 Abs. 1 BSIG: Pflicht zur Umsetzung und Überwachung der Risikomanagementmaßnahmen nach § 30 BSIG
 - § 38 Abs. 2 BSIG: Haftung nach dem Gesellschaftsrecht und nach BSIG. Demnach grds. höheres Regresspotenzial
 - § 38 Abs. 3 BSIG: Schulungspflicht
- **Pflichtenmaßstab**
 - Bislang oft streitig, was ein „angemessenes Sicherheitsniveau“ ist - Das BSIG konkretisiert die einzuhaltenden Pflichten

Die Verletzung regulatorischer Cybersicherheitspflichten kann künftig somit wesentlich einfacher eine Organpflichtverletzung begründen.

Mögliche Szenarien unter einer D&O-Police

Inanspruchnahme der Geschäftsführung nach einem Cybervorfall z. B. wegen

- fehlender oder unzureichender Cyber-Governance oder
- unterlassener Umsetzung bzw. Überwachung von Risikomanagementmaßnahmen

Q&A



Ihr Referent

Pavel Rahlov, Rechtsanwalt | Associate, Clyde & Co



Pavel Rahlov

Rechtsanwalt | Associate

Düsseldorf

E: Pavel.Rahlov@clydeco.com

T: +49 211 8822 8867

Über Clyde & Co

500

Partner

2.400

Anwältinnen und Anwälte

5.500

Mitarbeitende

3.200

Beraterinnen und Berater

70+

Büros weltweit*

*einschließlich assoziierter Büros



5.500 Mitarbeitende an 72 Standorten in 30 Ländern
rd. 980 Mio. Euro Umsatz / Best-Friends-Kanzleien in weiteren 81 Ländern



CLYDE&CO

Vielen Dank für Ihre Aufmerksamkeit!

Clyde & Co LLP accepts no responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this summary. No part of this summary may be used, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, reading or otherwise without the prior permission of Clyde & Co LLP.
© Clyde & Co LLP 2025
V2.25

Clyde & Co LLP

www.clydeco.com