

13. Hamburger Financial Lines Forum

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

Dr. Oliver Sieg, Partner

Hamburg, 12./13.10.2023

Einleitung

Wachtell, Lipton, Rosen & Katz
Risk Management and the Board of Directors
September 29, 2023

"Public companies and their boards of directors face an increasingly complex array of risks that test the resilience of corporate values, strategies, operations and enterprise risk management frameworks."

"Courts and regulators are increasingly scrutinizing board-level oversight mechanisms, as well as the adequacy of public disclosures and the quality of board responses when crises erupt."

"Pressure from institutional and activist investors, state law enforcement authorities, and federal administrative agencies also continue to mount."

"As business of all profiles become ever more dependent on technology and data management, cybersecurity risks have become increasingly salient. Indeed, failure to adequately identify, control and mitigate cyber risk can be devastating."

Die Netz- und Informationssysteme-Richtlinie belegt exemplarisch die globalen Herausforderungen an das Management und insbesondere Risiko-Management in einer Epoche der „Zeitenwende“

3

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

|||NOERR

Zeitenwende – Globale Herausforderungen für das Management

Risiko-Management

Risiken aufgrund externer Faktoren

- Digitalisierung
- Globalisierung
- ESG
- Inflation und Erhöhung der Leitzinsen
- Corona-Pandemie
- Russischer Angriff auf die Ukraine und Sanktionen
- Zugang zu und Kosten für natürliche Ressourcen
- Lieferengpässe; Transportrouten
- Globaler Wettbewerb Europa – USA – China

Risiken aufgrund unternehmensinterner Faktoren

- Strategische Risiken
- Operative Risiken
- Finanzielle Risiken
- Compliance Risiken

4

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

|||NOERR

Übersicht

I

Netz- und Informationssysteme Richtlinie und Entwurf des Umsetzungsgesetzes (E-BSIG)

II

Ausgangslage Managerhaftung

III

Auswirkungen auf die Rechtspraxis

- Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime
- Rechtsthemen werden zunehmend von Expertenthemen durchdrungen
- Globalisierung der rechtlichen Verantwortlichkeiten

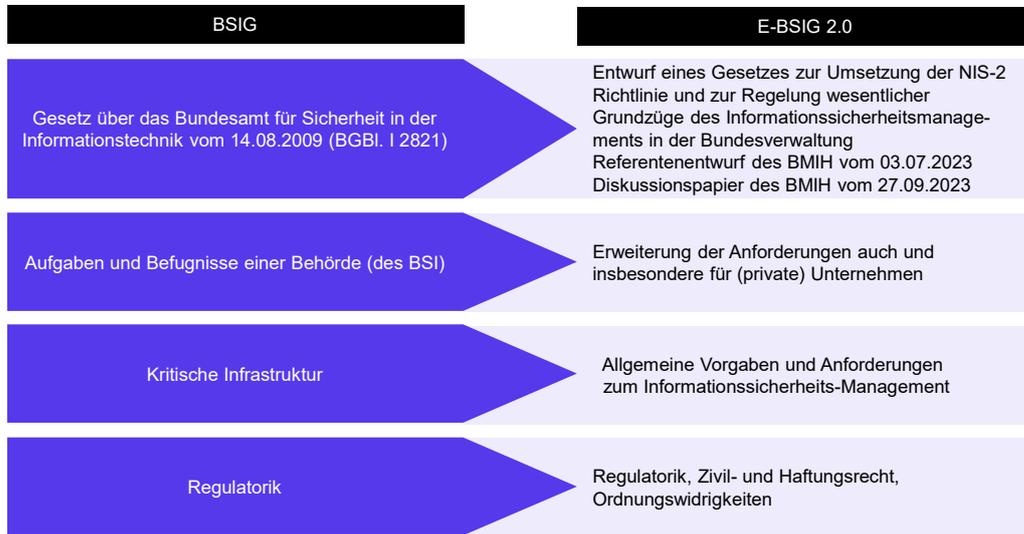
I. Netz- und Informationssysteme Richtlinie

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union



Network and Information Security Directive 2.0

I. Entwurf des Umsetzungsgesetzes zur NIS-2-Richtlinie (E-BSIG)



7

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

INOERR

I. Entwurf des Umsetzungsgesetzes zur NIS-2-Richtlinie (E-BSIG)



8

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

INOERR

I. Entwurf des Umsetzungsgesetzes zur NIS-2-Richtlinie (E-BSIG)

Einrichtungskategorien	
Kritische Anlagen	§§ 2 Abs. 1 Nr. 19; § 28 Abs. 1 Nr. 4 E-BSIG
Besonders wichtige Einrichtungen	§ 28 Abs. 1 E-BSIG
Wichtige Einrichtungen	§ 28 Abs. 2 E-BSIG

I. Entwurf des Umsetzungsgesetzes zur NIS-2-Richtlinie (E-BSIG)

Anforderungskatalog für Risikomanagement (§ 30 Abs. 2 E-BSIG)

Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

Bewältigung von Sicherheitsvorfällen

Aufrechterhaltung des Betriebs (Back-Up-Management und Wiederherstellung) nach einem Notfall sowie Krisenmanagement

Cyber-Sicherheit in der Lieferkette

Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen

I. Entwurf des Umsetzungsgesetzes zur NIS-2-Richtlinie (E-BSIG)

Anforderungskatalog für Risikomanagement (§ 30 Abs. 2 E-BSIG)

Konzepte und Verfahren zur Bewertung und Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit

Konzepte und Verfahren für den Einsatz von Kryptographie und Verschlüsselung

Sicherheit des Personals, Konzepte für die Zugriffs-Kontrolle und Management von Anlagen

Verwendung von Lösungen zur Multifaktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggf. Notfallkommunikationssysteme innerhalb der Einrichtung

I. Entwurf des Umsetzungsgesetzes zur NIS-2-Richtlinie (E-BSIG) Haftung von Geschäftsleitern

Art. 20 NIS-2-Richtlinie - Governance

(1) Die Mitgliedstaaten stellen sicher, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung von Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden können.

Die Anwendung dieses Absatzes lässt die nationalen Rechtsvorschriften in Bezug auf die für die öffentlichen Einrichtungen geltenden Haftungsregelungen sowie die Haftung von öffentlichen Bediensteten und gewählten oder ernannten Amtsträgern unberührt.

(2) [...]

I. Entwurf des Umsetzungsgesetzes zur NIS-2-Richtlinie (E-BSIG) Haftung von Geschäftsleitern

Art. 20 NIS-2-Richtlinie
§ 38 BSIG-E

Abs. 1

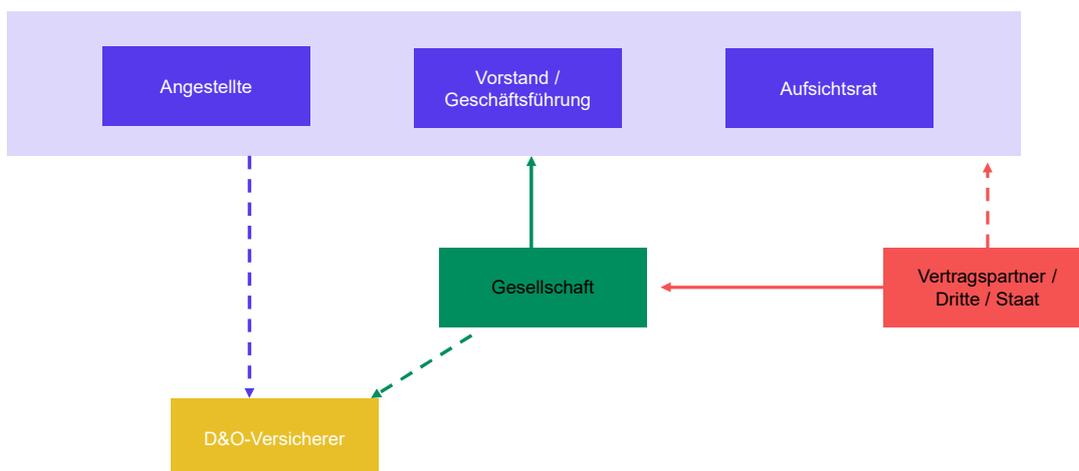
Pflicht der Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen

- Billigung der von diesen Einrichtungen nach dem Gesetz zu ergreifenden Maßnahmen des Cyber-Risikomanagements
- Überwachung der Umsetzung

Abs. 2

- Ausdrücklicher zivilrechtlicher Haftungstatbestand (im Diskussionspapier entfallen)
- Klarstellung: Schadensersatz umfasst Regressforderungen und Bußgelder (im Diskussionspapier entfallen)
- Unwirksamkeit eines Verzehs der Einrichtung auf Ersatzansprüche aufgrund einer Verletzung der Pflichten nach Abs. 1
- Unwirksamkeit eines Vergleichs der Einrichtung über diese Ansprüche
- Ausnahme: Insolvenz-Szenarien

II. Ausgangslage Managerhaftung



II. Ausgangslage Managerhaftung



Vorstand
Geschäftsführer

§ 93 AktG
§ 43 GmbHG
§ 34 GenG

Aufsichtsrat

§ 116 AktG
§ 52 GmbHG
§ 41 GenG

15

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

|||NOERR

II. Ausgangslage Managerhaftung

Deutsches Recht

Zivilrecht / Gesellschaftsrecht

Innenhaftung

Gesamtschuld

Ausländisches Recht

Strafrecht
Aufsichtsrecht
Arbeitsrecht

Außenhaftung

Innenregress

16

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

|||NOERR

II. Ausgangslage Managerhaftung



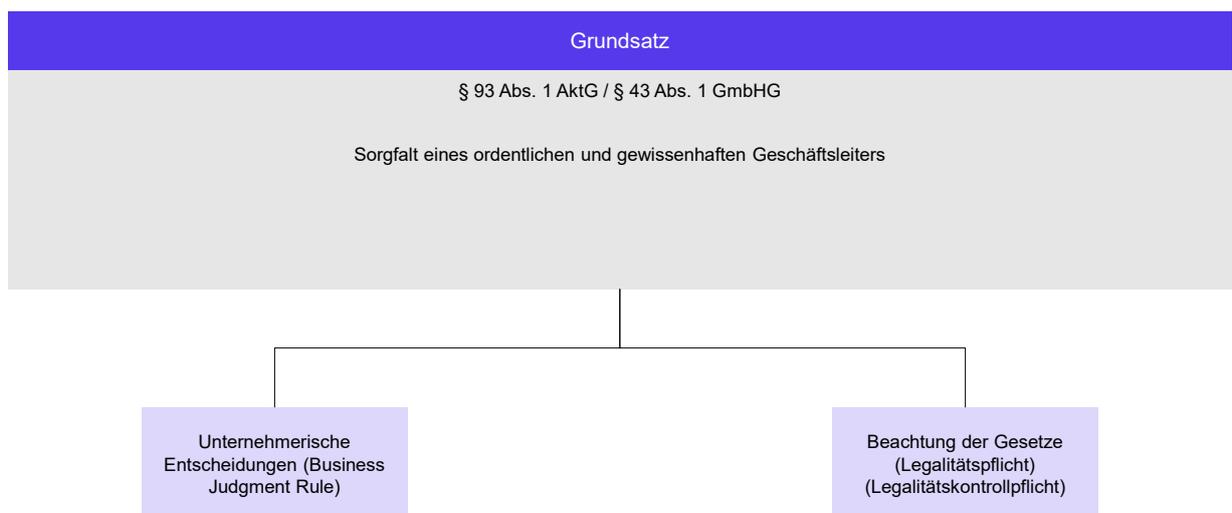
17

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

INOERR

II. Ausgangslage Managerhaftung



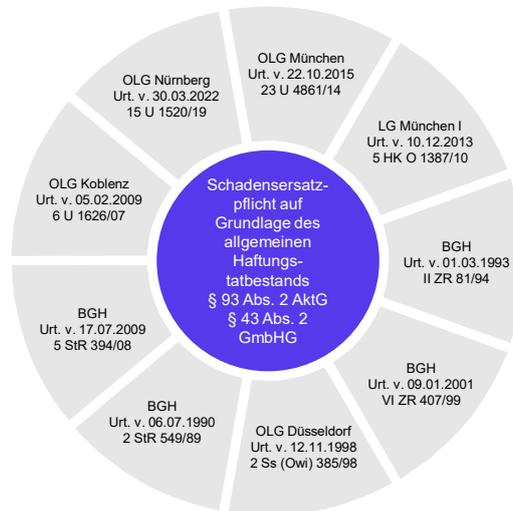
18

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

INOERR

II. Ausgangslage Managerhaftung Organisation und Überwachung



19

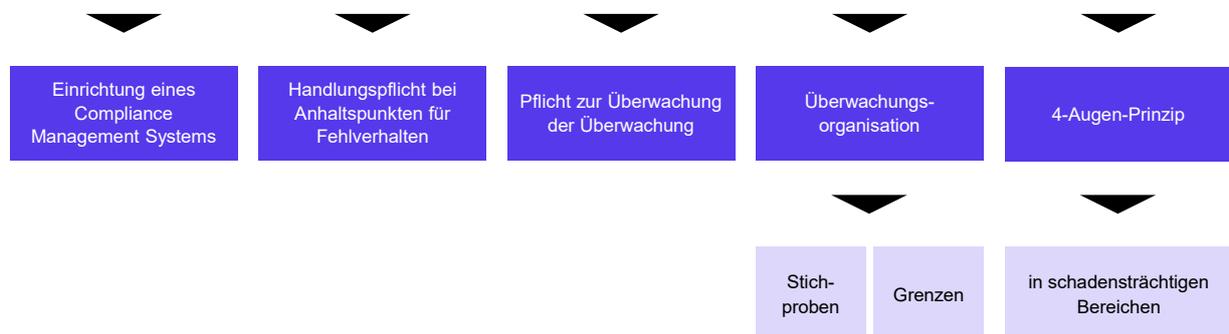
Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

INOERR

II. Ausgangslage Managerhaftung Insbesondere: Compliance- und Unternehmensorganisationspflichten eines Geschäftsleiters

OLG Nürnberg, Urt. v. 30.03.2022, 12 U 1520/19, „Tankkarten“



20

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

INOERR

II. Ausgangslage Managerhaftung Zunehmende Sondertatbestände



§ 91 Abs. 2 AktG

§ 25a KWG

§ 130 OWiG

StaRUG

LkSG

Netz- und Informationssysteme-Richtlinie (NIS-2)

21

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

|||NOERR

III. Auswirkungen auf die Rechtspraxis

- 1 Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime
- 2 Rechtsthemen werden zunehmend von Experten-Themen durchdrungen
- 3 Globalisierung der rechtlichen Verantwortlichkeiten

22

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

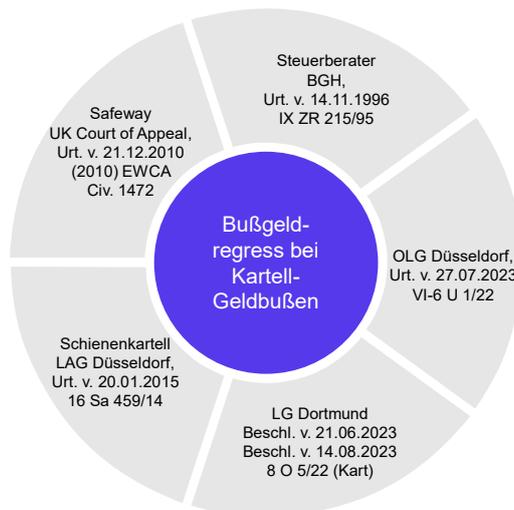
12./13.10.2023

|||NOERR

1. Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime



1. Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime Beispiel: Bußgeldregress



1. Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime Renaissance der deliktischen Außenhaftung?

§ 823 BGB

Abs. 1

„Wer vorsätzlich oder fahrlässig [...] das Eigentum oder ein sonstiges Recht eines anderen verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.“

Abs. 2

„Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt.“

1. Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime

Zunehmende Relevanz des Insolvenzrechts am Beispiel des StaRUG

§ 1 Abs. 1 StaRUG

Fortlaufende Überwachung der Entwicklungen, welche den Fortbestand der juristischen Person gefährden können.

- Ergreifen geeigneter Gegenmaßnahmen
- Berichterstattung gegenüber Überwachungsorganen
- Einbeziehung anderer zuständiger Geschäftsleiter

§ 1 Abs. 3 StaRUG

- Pflichten aus anderen Gesetzen bleiben unberührt

§ 43 StaRUG

- Pflichten und Haftung der Organe bei Restrukturierung

§ 57 StaRUG

- Haftung der Organe während Stabilisierungsverfahrens

1. Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime

Wer ist verantwortlich? – Geschäftsleiterpflichten

Krisenunabhängige Pflicht zur Risikovorsorge

Pflicht zur Krisenfrüherkennung seit dem 01.01.2021 ausdrücklich geregelt in:

§ 1 Unternehmensstabilisierungs- und Restrukturierungsgesetz (StaRUG)

- (1) Die Mitglieder des zur Geschäftsführung berufenen Organs einer juristischen Person (Geschäftsleiter) wachen fortlaufend über Entwicklungen, welche den Fortbestand der juristischen Person gefährden können.
Erkennen sie solche Entwicklungen, ergreifen sie geeignete Gegenmaßnahmen und erstatten den zur Überwachung der Geschäftsleitung berufenen Organen (Überwachungsorganen) unverzüglich Bericht.
Berühren die zu ergreifenden Maßnahmen die Zuständigkeiten anderer Organe, wirken die Geschäftsleiter unverzüglich auf deren Befassung hin.
- (2) Bei Gesellschaften ohne Rechtspersönlichkeit im Sinne von § 15a Absatz 1 Satz 3 und Absatz 2 der Insolvenzordnung gilt Absatz 1 entsprechend für die Geschäftsleiter der zur Geschäftsführung berufenen Gesellschafter.
- (3) Weitergehende Pflichten, die sich aus anderen Gesetzen ergeben, bleiben unberührt.

1. Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime

Wer ist verantwortlich? – Geschäftsleiterpflichten

Krisenunabhängige Pflicht zur Risikovorsorge

Pflicht zur Krisenfrüherkennung seit dem 01.01.2021 ausdrücklich geregelt in:

§ 43 Pflichten und Haftung der Organe

- (1) Handelt es sich bei dem Schuldner um eine juristische Person oder um eine Gesellschaft ohne Rechtspersönlichkeit im Sinne des § 15a Absatz 1 Satz 3, Absatz 2 der Insolvenzordnung, wirken dessen Geschäftsleiter darauf hin, dass der Schuldner die Restrukturierungssache mit der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters betreibt und die Interessen der Gesamtheit der Gläubiger wahrt. Für die Verletzung dieser Pflicht haften sie dem Schuldner in Höhe des den Gläubigern entstandenen Schadens, es sei denn sie haben die Pflichtverletzung nicht zu vertreten.
- (2) Ein Verzicht des Schuldners auf Ansprüche nach Absatz 1 Satz 2 oder ein Vergleich über diese Ansprüche ist unwirksam, soweit der Ersatz zur Befriedigung der Gläubiger erforderlich ist. Dies gilt nicht, wenn sich der Ersatzpflichtige zur Abwendung eines Insolvenzverfahrens über sein Vermögen mit seinen Gläubigern vergleicht, wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird oder wenn für den Ersatzberechtigten ein Insolvenzverwalter handelt.
- (3) Ansprüche nach Absatz 1 Satz 2 verjähren in fünf Jahren. Ist der Schuldner zum Zeitpunkt der Pflichtverletzung eine börsennotierte Gesellschaft, verjähren die Ansprüche in zehn Jahren.

1. Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime Wer ist verantwortlich? – Geschäftsleiterpflichten

Krisenunabhängige Pflicht zur Risikovorsorge

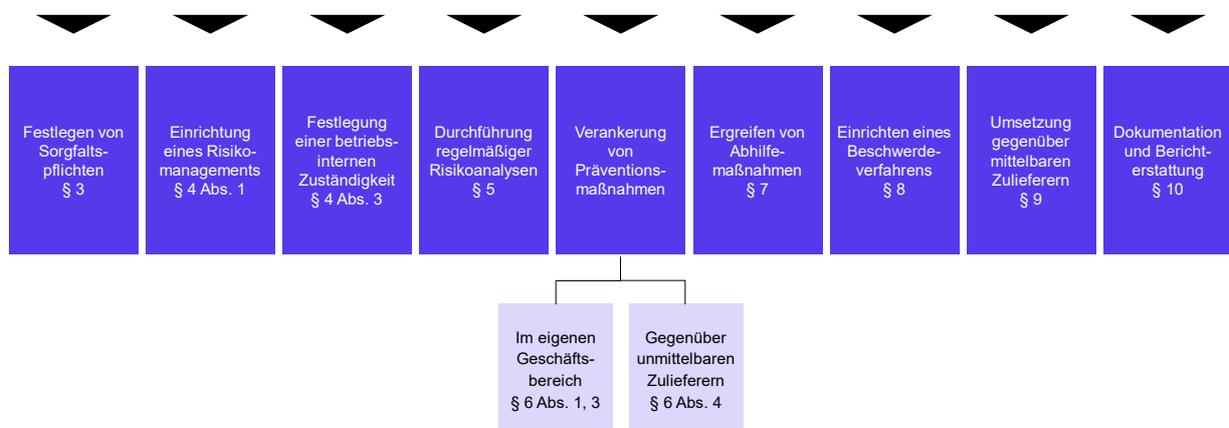
Pflicht zur Krisenfrüherkennung seit dem 01.01.2021 ausdrücklich geregelt in:

§ 57 Haftung der Organe

Handelt es sich bei dem Schuldner um eine juristische Person oder um eine Gesellschaft ohne Rechtspersönlichkeit im Sinne des § 15a Absatz 1 Satz 3, Absatz 2 der Insolvenzordnung und erwirkt er aufgrund vorsätzlich oder fahrlässig unrichtiger Angaben eine Stabilisierungsanordnung, ist der Geschäftsleiter den davon betroffenen Gläubigern zum Ersatz des Schadens verpflichtet, den diese durch die Anordnung erleiden. Dies gilt nicht, wenn ihn kein Verschulden trifft. Die Sätze 1 und 2 gelten auch für den Ersatz des Schadens, der einem Gläubiger aus einer nicht ordnungsgemäßen Auskehrung oder Verwahrung der Erlöse nach § 54 Absatz 2 entsteht. Für Ansprüche nach den Sätzen 1 und 3 gilt § 43 Absatz 3 entsprechend.

1. Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime Beispiel des Lieferkettensorgfaltspflichtengesetzes (LkSG)

Kein eigenständiger Schadensersatztatbestand § 3 Abs. 3



1. Tendenz zur Verknüpfung der Haftungs- und Sanktionsregime Beispiel des Lieferkettensorgfaltspflichtengesetzes (LkSG)



31

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

INOERR

2. Rechtsthemen werden zunehmend von Experten-Themen durchdrungen



32

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

INOERR

3. Globalisierung der rechtlichen Verhältnisse



Industriepolitik und Standortwettbewerb

Innerhalb der EU sowie weltweit

Forum Shopping

→ Beispiel: Kartellrechtliche Follow-On Claims

→ Beispiel: ESG-related disputes

33

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

|||NOERR

NSI-2 und Managerhaftung – Zusammenfassung

Die Richtlinie und der Entwurf des deutschen Umsetzungsgesetzes belegen eine Tendenz des Gesetzgebers zur Verknüpfung von regulatorischen Vorgaben, regulatorischen Eingriffsrechten, Straf- und Bußgeldtatbeständen mit zivilrechtlichen Sanktionen wie insbesondere der Managerhaftung.

Das abstrakte gesetzliche Regelwerk der Managerhaftung bedarf an sich keiner spezialgesetzlichen Klarstellungen mit bereichs- oder branchenspezifischen Organhaftungstatbeständen.

In der Fallbearbeitung werden die rechtlichen Themen noch stärker von Expertenthemen durchdrungen und abhängig.

Wir sehen auch am Beispiel der NIS-2-Richtlinie und dem Entwurf des deutschen Umsetzungsgesetzes Entwicklungen zur Globalisierung der rechtlichen Verantwortlichkeiten, staatliche Industriepolitik und einen Wettbewerb der Rechts- und Wirtschaftssysteme.

34

Umsetzung der Netz- und Informationssysteme-Richtlinie und Managerhaftung

12./13.10.2023

|||NOERR

Ihr Ansprechpartner



Dr. Oliver Sieg

Rechtsanwalt
Partner

+49 211 49986220
oliver.sieg@noerr.com

