MANZ – QUALITÄT SEIT 1849

10 | 2023 | 813–904 | ecolex

ecolex

FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT

Schwerpunkt

Die neue ÖNORM B 2110

> Inhaltliche Änderungen

> Versäumnisse

Wärme-*Contracting:* Einschränkungen

Praxis von Joint Ventures

Hausdurchsuchung, Sicherstellung und Ermittlungsverfahren

Verfehlte Entscheidungsform

Schwestergesellschaften im Kartellrecht

Dark Patterns im DSA und DMA

ECOLEX.MANZ.AT

ISSN 1022-9418

MANZ

NIS-2-RL: Wer trägt die Verantwortung im Unternehmen?

Das „Leitungsorgan“ in der NIS-2-RL

BEITRAG. Um dem unionalen Cybersicherheitsrecht endlich zum Durchbruch zu verhelfen, sieht die NIS-2-RL scharfe Sanktionsmechanismen vor – neben Millionen- bzw Milliardengeldbußen für Unternehmen droht künftig auch den „Leitungsorganen“ eine entsprechende Verantwortung. Der Beitrag geht dem Begriffsinhalt des „Leitungsorgans“ auf den Grund und legt dar, weshalb ab (voraussichtlich) Oktober 2024 je nach gesellschaftsrechtlicher Ausgestaltung unterschiedliche Leitungspersonen ein erhebliches Interesse daran haben werden, dass „ihr“ Unternehmen seine Cybersicherheitspflichten erfüllt. ecolex 2023/568

Mag. **Martin Schiefer** ist RA im Vergaberecht mit über 25 Jahren Erfahrung und Gründer und Partner bei Schiefer Rechtsanwälte in Wien.
Dr. **Lukas B. Wieser** ist RAA bei Schiefer Rechtsanwälte in Wien und Lektor an der SFU Wien.

A. Cybersicherheitsrecht: Unionsgesetzgeber schärft nach

Im Vergleich zum Datenschutzrecht der DSGVO spiel(t)en die Cybersicherheitspflichten der NIS-1-RL[1] in der Compliance-Praxis österr Unternehmen und der rechtswissenschaftlichen Debatte bislang lediglich eine untergeordnete Rolle.[2] Dies lag und liegt insb daran, dass das NISG,[3] das die NIS-1-RL für Österreich umsetzt, Verstöße nicht entsprechend sanktioniert(e). Neben den Millionen- und Milliardenstrafen[4] der DSGVO[5] nehmen sich die *„bis zu 50.000“* bzw *„im Wiederholungsfall bis zu 100.000 Euro“,* die § 26 Abs 1 NISG für die Verletzung seiner Cybersicherheitspflichten gegenwärtig vorsieht, vergleichsweise bescheiden aus.[6] Dass der österr Gesetzgeber damit seiner Umsetzungspflicht aus Art 21 NIS-1-RL zur Erlassung *„wirksam[er], angemessen[er] und abschreckend[er]“* Sanktionen nachgekommen ist, kann durchaus bezweifelt werden.

Österreich dürfte aber nicht der einzige Mitgliedstaat sein, dessen Umsetzung der NIS-1-RL zu wünschen übrig ließ. Denn aufgrund des Umstandes, dass das Umsetzungsniveau zwischen den einzelnen Mitgliedstaaten stark divergierte,[7] und dies die Effektivität des unionalen Cybersicherheitsrechts beeinträchtigte, sah sich der Unionsgesetzgeber gezwungen, zur Gewährleistung eines *„hohe[n] gemeinsame[n] Cybersicherheitsniveau[s] in der Union“*[8] dem NIS-Cybersicherheitsrecht ein Update zu verpassen: die NIS-2-RL.[9]

Mit der am 16. 1. 2023 in Kraft getretenen (und bis zum 17. 10. 2024 umzusetzenden)[10] RL schärft der Unionsgesetzgeber im Cybersicherheitsrecht nach. Dass durch die NIS-2-RL Cybersicherheit zur *„Chefsache“* wird,[11] dafür soll neben dem erheblich ausgeweiteten Anwendungsbereich[12] künftig auch das scharfe Sanktionsregime Sorge tragen. Dieses sieht insb eine Verantwortlichkeit der *„Leitungsorgane“* für die Einhaltung der Cybersicherheitspflichten vor (Art 20 Abs 1 NIS-2-RL). *„Compliance-Hammer: ‚NIS-2-Umsetzungsgesetz‘ – ‚Für die Leitungsebene kommt es faustdick.‘“*[13] – so titelt deswegen eine Fachpublikation zum Thema.[14]

Doch „wer“ ist eigentlich „NIS-Leitungsorgan“? Welche Organe bzw Personen werden in österr Unternehmen ab (voraussichtlich) Oktober 2024 die Verantwortung für die Einhaltung der NIS-2-Cybersicherheitspflichten übernehmen müssen? Die NIS-1-RL kannte den Begriff des „Leitungsorgans“ bislang noch nicht; die NIS-2-RL selbst und auch ihre ErwGr schweigen zu dessen Inhalt.

B. Wer ist das „Leitungsorgan“?

1. Fehlende Legaldefinition in der NIS-2-RL

Das „Leitungsorgan“ findet in der NIS-2-RL an drei Stellen Erwähnung:[15] in ErwGr 137 sowie in Art 20 Abs 1 und 2. Gem ErwGr 137 NIS-2-RL *„sollten die Leitungsorgane der [von der Richtlinie erfassten] Einrichtungen die Risikomanagementmaßnahmen im Bereich der Cybersicherheit genehmigen und deren Umsetzung überwachen“.* Damit soll *„ein hohes Maß an Verantwortung für die Risikomanagementmaßnahmen und die Berichtspflichten im Bereich der Cybersicherheit“* sichergestellt werden. Gem Art 20 Abs 1 NIS-2-RL gewährleisten die Mitgliedstaaten, *„dass die Leitungsorgane […] die […] ergriffenen Risikomanagementmaßnahmen […] billigen, ihre Umsetzung überwachen und für Verstöße […] durch die betreffenden Einrichtungen verantwortlich gemacht werden können“.* Art 20

---

1) RL 2016/1148/EU, ABl L 2016/194, 1.
2) Siehe dahingehend *Kristoferitsch/Lachmayer,* Die NIS-Richtlinie und ihre österreichische Umsetzung im NIS-Gesetz, ecolex 2020, 74 (75).
3) Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz), BGBl I 2018/111.
4) Dazu etwa *Zeit Online* v 22. 5. 2023, EU-Strafe gegen Meta – Europa regelt, https://www.zeit.de/digital/datenschutz/2023-05/eu-strafe-meta-datenschutz-dsgvo-regulierung (abgefragt 17. 9. 2023).
5) Siehe Art 83 DSGVO.
6) So auch *Kristoferitsch/Lachmayer,* ecolex 2020, 77.
7) ErwGr 4ff NIS-2-RL.
8) So der Langtitel der NIS-2-RL.
9) RL 2022/2555/EU, ABl L 2022/333, 80.
10) Art 41 Abs 1 NIS-2-RL.
11) Vgl *Kipker,* Chefsache Cybersicherheit: NIS-2 ist da, EuZW 2023, 249.
12) Siehe *Wegmann,* Too much of a good thing? Erweiterung und Verschärfung von Cybersicherheitspflichten durch die NIS2-Richtlinie, BB 2023, 835 (838f).
13) *Dittrich,* CB 2023, I.
14) *Dittrich* spricht von *„bislang nie dagewesene[n] Compliance-Vorschriften für die Leitungspersonen“* (CB 2023, I).
15) Die in Anhang I NIS-2-RL genannten *„Flughafenleitungsorgane“* sowie die *„Leitungsorgane von Häfen“* bleiben an dieser Stelle unberücksichtigt, weil die Begriffe eine andere Stoßrichtung aufweisen.

Abs 2 NIS-2-RL enthält eine Verpflichtung für Leitungsorgane, an Cybersicherheits-Schulungen teilzunehmen.

Obwohl der Figur des „Leitungsorgans" im Regime der NIS-2-RL somit zentrale Bedeutung zukommt, sucht man eine Legaldefinition des Begriffs in der RL vergeblich. Schlüsse hinsichtlich des Begriffsinhalts lassen sich aber aus sonstigen Rechtsakten des sekundären Unionsrechts, teleologischen Erwägungen und schließlich über die Umwege der horizontalen Systematik und Teleologie auch aus dem Richtlinientext selbst ziehen.

2. Sekundäres Unionsrecht, Teleologie und Richtlinientext

So wird der Begriff des „Leitungsorgans" in anderen Sekundärrechtsakten, wie Art 3 Nr 30 VO (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor, legaldefiniert. Die VO (EU) 2022/2554 stellt nach ErwGr 28 NIS-2-RL einen „sektorspezifischen Rechtsakt" iSd Art 4 NIS-2-RL hinsichtlich Finanzunternehmen dar, in dem *„Risikomanagementmaßnahmen oder Berichtspflichten im Bereich der Cybersicherheit vorgesehen sind",*[16] die in ihrer Wirkung den NIS-2-Pflichten entsprechen.

Zur Begriffsdefinition verweist Art 3 Nr 30 VO (EU) 2022/2554 zunächst als erste von zwei Alternativen auf die Definitionen des Begriffs „Leitungsorgan" in den RL 2014/65/EU, 2013/36/EU und 2009/65/EG sowie in den VO (EU) 909/2014 und (EU) 2016/1011. Allen genannten Sekundärrechtsakten ist dabei gemein, dass sie in ihren Legaldefinitionen ein funktionelles Begriffsverständnis zugrunde legen. Ein „Leitungsorgan" zeichnet sich demnach dadurch aus, dass es Strategie, Ziele und Gesamtpolitik des Unternehmens festlegt,[17] dass ihm die Personen angehören, die die Geschäfte des Unternehmens tatsächlich führen[18] und dass ihm die Letztentscheidungsbefugnis[19] zukommt.

Ein derartiges funktionelles Verständnis setzt dann Art 3 Nr 30 VO (EU) 2022/2554 ebenso selbst als zweite Begriffsalternative fest. „Leitungsorgane" sind demnach auch die *„entsprechenden Personen, die das Unternehmen tatsächlich leiten oder im Einklang mit dem einschlägigen Unionsrecht oder nationalen Recht Schlüsselfunktionen wahrnehmen".*

Ein „Leitungsorgan" zeichnet sich dadurch aus, dass es Strategie, Ziele und Gesamtpolitik des Unternehmens festlegt, dass ihm die Personen angehören, die die Geschäfte des Unternehmens tatsächlich führen und dass ihm die Letztentscheidungsbefugnis zukommt.

Die VO (EU) 2022/2554 geht – als iSd NIS-2-RL sektorspezifischer Cybersicherheits-Rechtsakt – somit unzweifelhaft von einem funktionellen Verständnis des Begriffs des „Leitungsorgans" aus. Aufgrund des Umstandes, dass die NIS-2-RL die VO (EU) 2022/2554 für den Finanzsektor zu ihrem „Pendant" erklärt, muss der betreffenden Legaldefinition der VO (EU) 2022/2554 für die Auslegung des Begriffs des „Leitungsorgans" in der NIS-2-RL entsprechende Bedeutung beigemessen werden. Es ist deswegen mangels gegenteiliger Anhaltspunkte davon auszugehen, dass die NIS-2-RL den Begriff des „Leitungsorgans" ebenso funktionell verwendet.

Ein funktionelles Verständnis des Begriffs des „Leitungsorgans" lässt sich weiters auch aus der Teleologie der NIS-2-RL, dem das Unionsrecht prägenden Auslegungsgrundsatz *effet utile* und nicht zuletzt auch rechtsstaatlichen Prinzipien[20] ableiten. Die NIS-2-RL will ein *„hohes gemeinsames Cybersicherheitsniveau in der Union"*[21] gewährleisten und stellt dies hinsichtlich der erfassten Einrichtungen/Unternehmen nicht zuletzt durch eine entsprechende Verantwortlichkeit der Leitungsorgane sicher. Diese Zweck-Mittel-Relation funktioniert nur insofern, als das Mittel Steuerungswirkung hinsichtlich jener Personen entfaltet, die Einfluss auf die Zweckerreichung nehmen können. Oder anders: Die Sanktionsdrohungen können die Wirkung der Gewährleistung eines hohen Cybersicherheitsniveaus nur dann erreichen, wenn sie jene treffen (und damit motivieren), die innerhalb des jeweiligen Unternehmens über die Setzung von Cybersicherheitsmaßnahmen auch entscheiden können. Es wäre den Zwecken der NIS-2-RL deswegen nicht ausreichend Rechnung getragen, würde man den Begriff des „Leitungsorgans" organisatorisch interpretieren und die Verantwortlichkeit selbst in jenen Fällen pauschal ausschließlich beim Geschäftsführungs- und Vertretungsorgan verorten, in denen dieses etwa mittels Gesellschafterweisung umfassend gesteuert wird.

Das derart erzielte funktionelle Auslegungsergebnis des Begriffs des „Leitungsorgans" lässt sich schließlich wieder auf den Text der NIS-2-RL zurückführen. Gem Art 32 Abs 5 lit b NIS-2-RL sind als Ultima Ratio Tätigkeitsverbote über *„natürliche[…] Personen, die auf Geschäftsführungs- bzw Vorstandsebene oder Ebene des rechtlichen Vertreters für Leitungsaufgaben in dieser wesentlichen Einrichtung zuständig sind",* zu verhängen. Der Begriff des „Leitungsorgans" muss damit einen Inhalt aufweisen, der sich von der *„Geschäftsführungs- bzw Vorstandsebene oder Ebene des rechtlichen Vertreters"* unterscheidet und über diese hinausgeht, weil der Unionsgesetzgeber die Tätigkeitsverbote sonst einfach für alle „Leitungsorgane" hätte vorsehen können („über natürliche Personen, die als Leitungsorgane […]"). Der Methodenkanon gebietet es, im Zweifel von der unterschiedlichen Bedeutung verschiedener Begrifflichkeiten auszugehen.

Zudem korreliert mit der Anordnung der Verantwortlichkeit der Leitungsorgane in Art 20 Abs 1 NIS-2-RL eine Verpflichtung der Mitgliedstaaten gem Art 32 Abs 6 bzw Art 33 Abs 5 iVm Art 32 Abs 6 NIS-2-RL, sicherzustellen, dass jede *„natürliche Person, die für eine […] Einrichtung verantwortlich ist"* oder *„auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als Vertreterin der wesentlichen Einrichtung handelt, befugt ist zu gewährleisten, dass die Einrichtung diese Richtlinie erfüllt".* Die Mitgliedstaaten müssen dabei vorsehen, *„dass diese natürlichen Personen für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung dieser Richtlinie haftbar gemacht werden können".* Damit wird wiederum deutlich, dass sich der Begriff des Leitungsorgans, das eben gem Art 20 Abs 1 NIS-2-RL *„für eine […] Einrichtung verantwortlich"* ist, nicht bloß auf die Geschäftsführungs- bzw Vorstandsebene im Sinne des österr Gesellschaftsrechts bezie-

---

16) Siehe ErwGr 25 NIS-2-RL.
17) Art 4 Abs 1 Nr 36 RL 2014/65/EU; Art 3 Abs 1 Nr 7 RL 2013/36/EU; Art 2 Abs 1 Nr 45 VO (EU) 909/2014; Art 3 Abs 1 Nr 20 VO (EU) 2016/1011.
18) Art 4 Abs 1 Nr 36 RL 2014/65/EU; Art 3 Abs 1 Nr 7 RL 2013/36/EU; Art 2 Abs 1 Nr 45 VO (EU) 909/2014; Art 3 Abs 1 Nr 20 VO (EU) 2016/1011.
19) Art 2 Abs 1 lit s RL 2009/65/EG.
20) Im Rechtsstaat ist man grundsätzlich nur für eigenes Verhalten verantwortlich.
21) Vgl nur die Langbezeichnung der NIS-2-RL.

hen kann. Denn diesfalls bedürfte es der zusätzlichen Anordnung *„oder auf der Grundlage ihrer Vertretungsbefugnis […]“* nicht.

Letztlich liegt der NIS-2-RL jedoch ohnedies ein umfassendes Konzept der „Verantwortung“ bzw „Haftung“ der Entscheidungsträger im Unternehmen für die Verletzung von Cybersicherheitspflichten zugrunde. Deshalb würde selbst dann, wenn man entgegen der hier vertretenen Auffassung den Begriff des Leitungsorgans in organisatorischer Weise auf die Geschäftsführungs- und Vorstandsebene beschränkt und nur deren „Verantwortlichkeit“ annimmt, über den Umweg des Art 32 Abs 6 bzw Art 33 Abs 5 iVm Art 32 Abs 6 NIS-2-RL und der darin festgelegten Haftung in jedem Fall eine gewisse Art der „Verantwortlichkeit“ aller Entscheidungsträger hergestellt.

C. Fazit und Ausblick

Vorbehaltlich der noch ausstehenden Umsetzung durch den österr Gesetzgeber lässt sich daher festhalten, dass die Verantwortlichkeit für die Einhaltung der NIS-2-Cybersicherheitspflichten künftig je nach der konkreten gesellschaftsrechtlichen Aufgabenverteilung unterschiedliche Organe treffen kann. Wenn man daher fragt, wer das verantwortliche „Leitungsorgan“ iSd NIS-2-RL ist, so lautet die Antwort: Es kommt darauf an … wer eben die maßgeblichen Entscheidungen in der Gesellschaft trifft und das Unternehmen tatsächlich leitet.[22)]

Das können anstelle der oder neben den Geschäftsführungs- und Vertretungsorganen bei entsprechender Einflussmöglichkeit etwa der Aufsichtsrat oder die GmbH-Generalversammlung sein, bspw wenn die AG-Satzung Ersterem gewisse einschlägige Mitwirkungsrechte einräumt[23)] oder einzelne Personen in der GmbH-Generalversammlung mittels des gesellschaftsrechtlichen Weisungsrechts gegenüber der Geschäftsführung die Gesellschaft *de facto* – und damit „tatsächlich“ – leiten. Angesichts der diesbezüglichen Unsicherheit, die das funktionelle Verständnis des Begriffs des „Leitungsorgans“ nach sich zieht, sollten künftig alle Leitungspersonen im Unternehmen gleichermaßen ein maßgebliches Interesse daran haben, dass ihre wesentliche oder wichtige Einrichtung die NIS-Cybersicherheitspflichten erfüllt. Sei es, weil sie als *„Leitungsorgane“* gem Art 20 Abs 1 NIS-2-RL die Verantwortung tragen. Oder aber, weil sie als *„natürliche Person“* gem Art 32 Abs 6 NIS-2-RL für Verstöße ihrer Einrichtung gegen Cybersicherheitspflichten haften.

Abschließend bleibt noch rechtsvergleichend hervorzuheben, dass der derzeitige deutsche Gesetzesentwurf zu einem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz die RL wohl unzureichend umsetzt. Denn darin wird die Verantwortlichkeit für die Cybersicherheit nur den „Geschäftsleitern“ und damit jenen natürlichen Personen auferlegt, *„die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer Einrichtung berufen sind“*.[24)] Diese Einschränkung auf Organe, die kumulativ sowohl die Geschäfte führen als auch die Gesellschaft vertreten, wird dem funktionellen Begriff des „Leitungsorgans“ der NIS-2-RL, der darauf abstellt, wer im Unternehmen die maßgeblichen Entscheidungen tatsächlich trifft, nicht gerecht.

Schlussstrich

Mit der am 16. 1. 2023 in Kraft getretenen NIS-2-RL schärft der Unionsgesetzgeber im Cybersicherheitsrecht nach. Dass durch die RL Cybersicherheit zur *„Chefsache“* wird, dafür soll künftig auch das drakonische NIS-2-Sanktionsregime Sorge tragen. Dieses sieht insb eine Verantwortlichkeit der „Leitungsorgane“ für die Einhaltung der Cybersicherheitspflichten vor, wobei die NIS-2-RL ein funktionelles Begriffsverständnis zugrunde legt. „Leitungsorgane“ sind demnach jene Gesellschaftsorgane, die die maßgeblichen Entscheidungen in der Gesellschaft treffen und das Unternehmen tatsächlich leiten. Abhängig von der konkreten gesellschaftsrechtlichen Aufgabenverteilung kann die Verantwortlichkeit für die Einhaltung der unionalen Cybersicherheitspflichten damit künftig auf unterschiedlichen Schultern lasten und anstelle der oder neben den Geschäftsführungs- und Vertretungsorganen bei entsprechender Einflussmöglichkeit etwa auch den Aufsichtsrat oder die GmbH-Generalversammlung treffen.

[22)] Vgl idZ auch die Bestimmung des § 78 Abs 2 BVergG 2018, die in Umsetzung des Art 57 Abs 1 RL 2014/24/EU hinsichtlich der Verwirklichung von vergaberechtlichen Ausschlussgründen typisierend darauf abstellt, wem im betreffenden Unternehmen entsprechende Einflussmöglichkeiten zukommen (siehe ErläutRV 69 BlgNR 26. GP 100).

[23)] Vgl § 95 Abs 5 AktG; *Eckert/Schopper* in *Artmann/Karollus* (Hrsg), AktG II[6] (Stand 1. 10. 2018, rdb.at) § 95 AktG Rz 65 f.

[24)] Siehe § 2 Z 11 iVm § 38 des Art 1 (BSI-Gesetz) des Entwurfs zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz.