MANZ – QUALITÄT SEIT 1849

11 | 2023 | 905–1008 | ecolex

ecolex

FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT

Schwerpunkt

Flexible Kapitalgesellschaft (1. Teil)

> Verhältnis zur GmbH
> Finanzierungsrunden
> Unternehmenswertanteile

Asset Freeze: Eigentumsprüfung

Kartellaufdeckung 2.0

Verteidigungskosten und Finanzstrafverfahren

Energiegemeinschaften und Einlagenrückgewähr

EU-US Data Privacy Framework

Gewalt im Internet

ECOLEX.MANZ.AT

ISSN 1022-9418

MANZ

Cybersicherheitsrecht 2.0: Mangelhafte Compliance kommt teuer

Die NIS-2-RL und ihr Pflichtenprogramm für Unternehmen

BEITRAG. Mit der am 16. 1. 2023 in Kraft getretenen NIS-2-RL schärft der Unionsgesetzgeber im Cybersicherheitsrecht nach. Ein erheblich ausgeweiteter Anwendungsbereich, neue unternehmerische Pflichten – vor allem das Gebot zur Gewährleistung der Cybersicherheit der Lieferkette – und drastische Sanktionen tragen künftig dafür Sorge, dass Netz- und Informationssysteme in der EU ausreichend geschützt werden. Der Beitrag analysiert die Pflichten, die Unternehmen ab Oktober 2024 erfüllen müssen, und legt dar, weshalb der Cybersicherheits-Compliance ab sofort höherer Stellenwert zukommen sollte. ecolex 2023/622

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. NIS-2-RL: Cybersicherheitsrecht 2.0

Mit der am 16. 1. 2023 in Kraft getretenen[1] NIS-2-RL[2] aktualisiert der Unionsgesetzgeber das unionale Cybersicherheitsrecht. Ein initialer Vorstoß[3] zur Gewährleistung eines *„hohe[n] gemeinsame[n] Cybersicherheitsniveau[s]"* in der EU erfolgte bereits durch die NIS-1-RL,[4] die seit rund fünf Jahren kritische Infrastrukturbetreiber in den MS dazu verpflichtet, Maßnahmen der Cybersicherheit zu treffen.

Die NIS-1-RL wies allerdings (und weist nach wie vor) einige Schwachstellen auf (in der Diktion des Unionsgesetzgebers: *„inhärente Mängel"*),[5] wobei diese insb dem Umstand geschuldet waren, dass nach der RL wesentliche Fragestellungen – wie die Festlegung des konkreten Anwendungsbereichs[6] oder die Strafhöhe[7] – in die Prärogative der MS fielen.[8] Das Umsetzungsniveau in den MS divergiert(e) deswegen erheblich, weshalb sich der Unionsgesetzgeber nach einer Evaluation der NIS-1-RL auch dazu genötigt sah, das EU-Cybersicherheitsrecht durch die NIS-2-RL weiterzuentwickeln.[9]

Die NIS-2-RL ist von den MS bis zum 17. 10. 2024[10] umzusetzen. Der vorliegende Beitrag bietet einen Überblick der aus der NIS-2-RL folgenden Anforderungen, denen österr Unternehmen (voraussichtlich) ab dem 18. 10. 2024 unterliegen werden.[11]

B. Erweiterter Anwendungsbereich

Dafür, dass der NIS-2-RL im Vergleich zum Cybersicherheitsrecht der NIS-1-RL gesteigerte Bedeutung in der unternehmerischen Praxis zukommen wird, ist zunächst der erweiterte Anwendungsbereich der RL verantwortlich.[12] Unterfielen bislang bloß Betreiber kritischer Infrastruktur und Anbieter bestimmter digitaler Dienste dem Cybersicherheits-Regime der EU,[13] erhöht die NIS-2-RL zum einen die Zahl kritischer (Infrastruktur)Sektoren von sieben auf elf, wie künftig als „Novum" zum anderen auch bestimmte Unternehmen (bzw Einrichtungen) in Branchen mit gesteigerter Kritikalität unter NIS-2 fallen. Vor allem durch die Einbeziehung eines wesentlichen Teils der produzierenden Industrie (chemische Stoffe,[14] Lebensmittel,[15] elektrotechnische Industrie[16] etc) betrifft das unionale Cybersicherheitsrecht künftig nicht nur wenige ausgewählte Betreiber kritischer Infrastruktur, sondern weite Bereiche der Wirtschaft.[17]

---

1) Siehe Art 45 NIS-2-RL.
2) RL 2022/2555/EU, ABl L 2022/333, 80.
3) So auch *Kristoferitsch/Lachmayer*, Die NIS-Richtlinie und ihre österreichische Umsetzung im NIS-Gesetz, ecolex 2020, 74 (77).
4) RL 2016/1148/EU, ABl L 2016/194, 1.
5) ErwGr 2 NIS-2-RL.
6) Siehe Art 5 NIS-1-RL.
7) Siehe Art 21 NIS-1-RL.
8) Vgl auch ErwGr 4 NIS-2-RL.
9) Vgl ErwGr 4 f NIS-2-RL; s auch das Commission Staff Working Document SWD(2020) 344 final.
10) Art 41 Abs 1 NIS-2-RL.
11) Vgl idZ jedoch den Umstand, dass der österr Gesetzgeber bereits die NIS-1-RL verspätet umsetzte. Die NIS-1-RL sah die Anwendung der innerstaatl Umsetzungsvorschriften ab dem 10. 5. 2018 vor (Art 25 Abs 1 NIS-1-RL). Das österr NISG, das die RL umsetzt, trat aber erst mit 29. 12. 2018 in Kraft (§ 31 NISG). Siehe dazu *Anderl/Müller/Pichler*, Das österreichische Netz- und Informationssystemsicherheitsgesetz, in *Paulus* (Hrsg), Regulierungsrecht. Jahrbuch 2019, 183 (185).
12) So auch *Staffler*, Morgendämmerung der EU-Cybersicherheit-Compliance, JSt 2023, 328 (330).
13) Vgl *Kristoferitsch/Lachmayer*, ecolex 2020, 74 ff; *Staffler*, JSt 2023, 328; vgl idZ zu den Zielen der NIS-1-RL *Kipker*, Cybersecurity[2] (2023) 959.
14) Nr 3 Anhang II NIS-2-RL.
15) Nr 4 Anhang II NIS-2-RL.
16) Nr 5 Anhang II NIS-2-RL.
17) *Kipker*, Chefsache Cybersicherheit: NIS-2 ist da, EuZW 2023, 249 (249).

Die NIS-2-RL legt ihren grundsätzlichen Anwendungsbereich in Art 2 Abs 1 fest. Die RL kommt demnach für *„öffentliche oder private Einrichtungen"* zur Anwendung, sofern diese kumulativ folgende Voraussetzungen erfüllen:

- Es handelt sich um Einrichtungen der in den Anhängen I[18] oder II[19] zur NIS-2-RL genannten Art.
- Im Falle von Unternehmen handelt es sich zumindest um „mittlere Unternehmen"[20] iSd Kommissions-Empfehlung 2003/361/EG (KMU-Empfehlung).[21]
- Die Einrichtungen erbringen ihre Dienste in der EU oder üben ihre Tätigkeit dort aus.[22]

Die NIS-2-RL beseitigt durch den Verweis auf die KMU-Empfehlung insb die in der NIS-1-RL enthaltene Befugnis der MS, die für die Einbeziehung in das NIS-Regime maßgeblichen Unternehmens-Schwellenwerte selbst festzulegen,[23] und vereinheitlicht den Anwendungsbereich des unionalen Cybersicherheitsrechts. Für grenzüberschreitend tätige Unternehmen besteht künftig unabhängig vom jeweiligen MS somit weitestgehend Klarheit darüber, ob sie in den Anwendungsbereich des NIS-2-Regimes fallen.[24]

Fehlt es an einer der Voraussetzungen, untersteht die betreffende Einrichtung der NIS-2-RL grds nicht; die Ausnahmen der NIS-2-RL ergeben sich im Umkehrschluss aus den Anwendungskriterien des Art 2 Abs 1. Dies gilt ausnahmsweise nicht für das Größenkriterium iSd KMU-Empfehlung, das durch die spezifische Kritikalität einer Einrichtung ersetzt werden kann.[25] Für betroffene Unternehmen bringen diese größenunabhängigen Anwendungsbereichsfestlegungen Unsicherheiten mit sich. Abzuwarten bleibt, ob hier Leitlinien der Kommission[26] oder entsprechende Regelungen in den Umsetzungsgesetzen Abhilfe schaffen werden.

C. Pflichten für Unternehmen

1. Risikomanagementmaßnahmen

Die Qualifikation als Einrichtung iSd Art 2 NIS-2-RL,[27] somit die Eröffnung des Anwendungsbereichs der NIS-2-RL, zeitigt für Unternehmen erhebliche Auswirkungen. So geht die Kommission in ihrem *Impact Assessment* zur NIS-2-RL davon aus, dass Unternehmen, die bislang dem NIS-Regime noch nicht unterlagen, ihr Cybersicherheitsbudget um rund 22% erhöhen müssen; sofern bereits die Vorgaben der NIS-1-RL erfüllt wurden, ist zumindest nur mit einer notwendigen Erhöhung von rund 12% zu rechnen.[28]

Für betroffene Unternehmen führt die NIS-2-RL damit zu erheblichen finanziellen Mehrbelastungen. Die Investition in die Cybersicherheits-Compliance, dh die Erfüllung der nachstehend behandelten Pflichten, ist dabei aber angezeigt. Im Falle von Verstößen drohen empfindliche Strafen, wie auch eine persönliche Verantwortlichkeit der „Leitungsorgane", die im äußersten Fall sogar Tätigkeitsverbote umfassen kann.[29]

Jene *„Risikomanagementmaßnahmen im Bereich der Cybersicherheit"*, zu denen die NIS-2-RL Unternehmen verpflichtet, finden sich in Art 21 leg cit. Gemäß dieser Bestimmung müssen Einrichtungen *„geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen"* ergreifen, *„um die Risiken für die Sicherheit der Netz- und Informationssysteme […] zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten"*. Die konkrete Intensität der zu setzenden Maßnahmen bestimmt sich gem Art 21 Abs 1 UAbs 2 NIS-2-RL anhand der Kriterien „Stand der Technik", „einschlägige Normen" (wie ISO 27.001), „Kosten der Umsetzung" und „Risiko des betreffenden Unternehmens", somit im Rahmen einer Verhältnismäßigkeitsprüfung („Risk-based Approach").

Art 21 Abs 1 NIS-2-RL gleicht weitestgehend den entsprechenden Bestimmungen der NIS-1-RL.[30] Das für Unternehmen maßgebliche Pflichtenprogramm des unionalen Cybersicherheitsrechts bleibt deswegen in seinen Grundsätzen ident. Im Detail zeigen sich dann aber doch wesentliche Neuerungen, von denen zwei besonders hervorzuheben sind:

Zum einen wandelt sich der Netzwerkschutz, zu dem Unternehmen verpflichtet sind, durch die NIS-2-RL von „spezifisch" zu „umfassend". Die NIS-1-RL sieht gegenwärtig vor, dass Einrichtungen Netz- und Informationssysteme nur insoweit schützen müssen, als diese bei der Erbringung von kritischen Diensten zum Einsatz kommen.[31] In der NIS-2-RL findet sich eine derartige Einschränkung der Sicherheitspflichten nun nicht mehr. Gem Art 21 Abs 1 NIS-2-RL haben Einrichtungen bzw Unternehmen, die in den Anwendungsbereich der RL fallen, sämtliche im Rahmen ihres Betriebes zum Einsatz kommenden Netz- und Informationssysteme gegen Cyberangriffe abzusichern.

Zum anderen sind Unternehmen gem Art 21 Abs 2 lit d NIS-2-RL künftig verpflichtet, die *„Sicherheit der Lieferkette"* zu gewährleisten. Wie dem *in concreto* nachzukommen ist, ergibt sich aus Art 21 Abs 2 lit d und Abs 3 iVm Art 22 sowie den ErwGr 85, 90 bzw 91 NIS-2-RL. Zusammengefasst erfordert die Verpflichtung zur Gewährleistung der Sicherheit der Lieferkette nach dem Konzept der NIS-2-RL von Unternehmen, dass diese ihre Lieferanten hinsichtlich ihres Cybersicherheitsrisikos einschätzen und bewerten.[32] Daraus folgt, dass nur von solchen Lieferanten Leistungen bezogen bzw nur mit solchen Lieferanten Verträge abgeschlossen werden dürfen, bei denen

---

[18] Anhang I nennt *„Sektoren mit hoher Kritikalität"* (Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Diensten [Business-to-Business], öffentliche Verwaltung, Weltraum) und baut damit auf der aus der NIS-1-RL bekannten Liste von *„Betreiber[n] wesentlicher Dienste"* (Anhang II zur NIS-1-RL) auf, erweitert diese aber partiell.

[19] Anhang II führt als *„sonstige kritische Sektoren"* sensible Branchen an (etwa Abfallbewirtschaftung, Produktion, Herstellung und Handel mit chemischen Stoffen, Produktion, Verarbeitung und Vertrieb von Lebensmitteln), die künftig ebenfalls dem NIS-Cybersicherheitsrecht unterliegen; dies stellt eine wesentliche Neuerung im Vergleich zur NIS-1-RL dar.

[20] Siehe auch ErwGr 7 NIS-2-RL.

[21] „Mittlere Unternehmen" zeichnen sich gem Art 2 Abs 1 und 2 des Anhangs der KMU-Empfehlung dadurch aus, dass sie entweder 50 oder mehr Mitarbeiter beschäftigen oder einen Jahresumsatz bzw eine Jahresbilanz von mehr als 10 Mio Euro aufweisen.

[22] Vgl ErwGr 116 NIS-2-RL.

[23] Siehe *Rath/Ekardt/Schiela*, Cybersicherheit in der Energiewende und das EU-Recht, MMR 2023, 83 (86); vgl ErwGr 4, 7 NIS-2-RL.

[24] So auch ErwGr 7 NIS-2-RL.

[25] Siehe Art 2 Abs 2–4 NIS-2-RL.

[26] Siehe ErwGr 20 NIS-2-RL.

[27] Art 3 NIS-2-RL untergliedert die der RL unterfallenden Einrichtungen weiter in die Kategorien der „wesentlichen" sowie „wichtigen" Einrichtung. Diese Unterscheidung entfaltet allerdings hauptsächlich für die behördlichen Aufsichts- und Durchsetzungsmaßnahmen (Art 32f NIS-2-RL) Relevanz. Das Pflichtenprogramm ist für beide Kategorien von Einrichtungen hingegen grds dasselbe (s auch *Rath/Ekardt/Schiela*, MMR 2023, 87).

[28] Siehe das Commission Staff Working Document SWD(2020) 344 final.

[29] Siehe dazu sogleich unter D.

[30] Art 14 Abs 1 und Art 16 Abs 1 NIS-1-RL.

[31] Siehe ErwGr 22 NIS-1-RL; zum NISG s *Mayer* in *Anderl et al* (Hrsg), NISG (2019) § 17 Rz 2ff.

[32] Vgl ErwGr 85 NIS-2-RL.

im Zeitpunkt des Vertragsabschlusses von der cybersicherheitsrechtlichen Unbedenklichkeit auszugehen ist. Zudem müssen Unternehmen ihre Lieferanten vertraglich zur Einhaltung von Cybersicherheitsstandards verpflichten.[33] Regelmäßig wird dies auf die Aufnahme von Pflichten zur Zertifizierung in die Verträge hinauslaufen.

2. Berichtspflichten

Während das Gebot zur Setzung von Risikomanagementmaßnahmen Cybergefahrenlagen vorbeugen will, bezwecken die Berichtspflichten des Art 23 NIS-2-RL, dass Unternehmen der Behörde[34] bei deren Realisation alle erforderlichen Informationen zur Verfügung stellen. Tritt ein *„erheblicher Sicherheitsvorfall"* ein,[35] sind Einrichtungen gem Art 23 Abs 1 NIS-2-RL deswegen verpflichtet, darüber zu berichten. Eine derartige Vorgabe fand sich zwar bereits in Art 14 Abs 3 bzw Art 16 Abs 3 NIS-1-RL, die Bestimmungen sahen aber davon ab, konkrete Details des Meldungsprozesses festzulegen. Mit Art 23 NIS-2-RL wird die Meldepflicht nunmehr insoweit fortentwickelt, als sie künftig zur Einhaltung eines minutiösen Ablaufprogramms verpflichtet.

Die „Erheblichkeit" eines Sicherheitsvorfalls, die die Pflicht zur Meldung begründet, haben Unternehmen auf Basis einer *„Anfangsbewertung"* zunächst selbst einzuschätzen.[36] Ist sich das Unternehmen bzw die betreffende Einrichtung unsicher, ob ein Sicherheitsvorfall die Schwelle der Erheblichkeit überschreitet, sollte die Meldung im Zweifel eher erfolgen als unterbleiben. Für den Fall, dass die Behörde den zweifelbehafteten Sicherheitsvorfall *ex post* doch als erheblich qualifizieren sollte, führt die in der eigeninitiativen, freiwilligen Meldung zum Ausdruck kommende Kooperationsbereitschaft des Unternehmens zu dessen haftungs- und sanktionsrechtlichen Privilegierung[37].[38]

Wurde ein Sicherheitsvorfall als „erheblich" erkannt, müssen Unternehmen gem Art 23 Abs 4 lit a NIS-2-RL als ersten Schritt im Meldungsprozess die *„Frühwarnung"* an die Behörde erstatten; diese ist „unverzüglich", spätestens binnen 24 Stunden zu übermitteln. Die Hauptlast des initialen Informationsflusses trägt nach dem Konzept der NIS-2-RL dann die gem Art 23 Abs 4 lit b leg cit „unverzüglich", jedenfalls aber innerhalb von 72 Stunden[39] zu tätigende *„Meldung über den Sicherheitsvorfall"*. Deren Zweck liegt gem Art 23 Abs 4 lit b iVm ErwGr 102 NIS-2-RL darin, *„die im Rahmen der Frühwarnung übermittelten Informationen zu aktualisieren und eine erste Bewertung des erheblichen Sicherheitsvorfalls […] vorzunehmen"*. Während im Rahmen der Frühwarnung lediglich eine rudimentäre Erstinformation der Behörde anhand von Verdachtsmomenten erfolgt,[40] müssen Unternehmen mit der Meldung über den Sicherheitsvorfall bereits belastbare Daten vorlegen.

Mit der Erstattung der Meldung über den Sicherheitsvorfall gem Art 23 Abs 4 lit b NIS-2-RL haben Unternehmen ihre Informationsverpflichtung gegenüber der Behörde bis zum Zeitpunkt, zu dem sie den das Meldeprogramm beschließenden Abschlussbericht gem Art 23 Abs 4 lit d NIS-2-RL erstatten müssen, grds erfüllt. Anderes gilt nur insofern, als die Behörde gem Art 23 Abs 4 lit c NIS-2-RL um *„einen Zwischenbericht über relevante Statusaktualisierungen"* ersucht.

Dauert der erhebliche Sicherheitsvorfall im Zeitpunkt der Vorlage des Abschlussberichts *(„spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls")* noch an, müssen Unternehmen an dessen Stelle einen Fortschrittsbericht an die Behörde übermitteln (Art 23 Abs 4 lit e NIS-2-RL). Sofern der erhebliche Sicherheitsvorfall Auswirkungen auf die Erbringung des Dienstes des Unternehmens haben könnte, sind gem Art 23 Abs 1 NIS-2-RL auch die Diensteempfänger (Kunden) zu informieren.[41]

D. Sanktionen

1. Geldbußen/Geldstrafen für juristische Personen

Neben dem erweiterten Anwendungsbereich wird die Wirksamkeit des unionalen Cybersicherheitsrechts im Regime der NIS-2-RL vor allem durch den im Vergleich zur bestehenden Rechtslage erheblich hinaufgesetzten Strafrahmen für die Verhängung von Geldstrafen besorgt. Gemeinsam mit der Anordnung des Art 34 Abs 1 NIS-2-RL, wonach die MS sicherstellen sollen, *„dass die Geldbußen […] unter Berücksichtigung der Umstände des Einzelfalls wirksam, verhältnismäßig und abschreckend sind"*, bauen Art 34 Abs 4 und 5 NIS-2-RL eine erhebliche finanzielle Drohkulisse auf, die Unternehmen zur Cybersicherheits-Compliance motivieren soll.

Zwar verlangt(e) auch Art 21 NIS-1-RL, dass die von den MS erlassenen Sanktionsvorschriften für Verstöße gegen das Cybersicherheitsregime *„wirksam[e], angemessen[e] und abschreckend[e]"* Strafen vorsehen müssen. Konkrete Strafhöhen fanden sich in der NIS-1-RL aber nicht. Der österr Gesetzgeber nutze den daraus resultierenden Umsetzungsspielraum, um, etwas vorsichtig ausgedrückt, in unionsrechtlich fraglicher Weise einer Überspannung der finanziellen Belastung der Normadressaten vorzubeugen. Gem § 26 Abs 1 letzter Satz NISG drohen bei Verletzung der NIS-Cybersicherheitspflichten derzeit lediglich *„Geldstrafe[n] bis zu 50.000 Euro, im Wiederholungsfall bis zu 100.000 Euro"*.

Es waren derartige Umsetzungsmängel, die den Unionsgesetzgeber zur Neufassung des unionalen Cybersicherheitsrechts durch die NIS-2-RL bewogen[42] und ihn auch dazu veranlassten, in der RL konkrete Strafrahmen festzusetzen. Künftig werden für Verstöße gegen die NIS-2-Pflichten gem Art 34 Abs 4 und 5 der RL deswegen nicht Geldstrafen bis zu € 50.000,– bzw € 100.000,–, sondern bis zu 10 Mio bzw 7 Mio Euro oder 2% bzw 1,4% des weltweiten Konzernumsatzes fällig.[43]

Die im Vergleich zur NIS-1-RL und dem NISG deutlich erhöhten Strafen erklären sich aber nicht nur mit der intendierten Verschärfung zur Gewährleistung entsprechender Compliance, sondern ebenfalls damit, dass der Unionsgesetzgeber in der NIS-2-RL das Strafsystem nunmehr vollends auf das Unter-

---

33) Siehe ErwGr 85 NIS-2-RL.

34) Die NIS-2-RL spricht zwar vom Bericht an das *„CSIRT oder gegebenenfalls [die] zuständige[…] Behörde"*. Aufgrund der „Staatsnähe" des Computer Security Incident Response Team (CSIRT) (s Art 10 NIS-2-RL) wird idZ allerdings vereinfachend nur der Begriff der „Behörde" verwendet.

35) Siehe für eine Begriffsdefinition Art 6 Nr 6 iVm Art 23 Abs 3 NIS-2-RL.

36) ErwGr 101 NIS-2-RL.

37) Siehe Art 23 Abs 1, Art 34 Abs 3 iVm Art 32 Abs 7 NIS-2-RL.

38) Vgl idZ insb auch die Auswirkungen des *nemo tenetur*-Prinzips auf die Möglichkeit der Verhängung von Strafen, wenn die Behörde nur aufgrund einer Meldung eines Unternehmens Kenntnis von Rechtsverstößen erlangt. Zuletzt wurde dies im Kontext der DSGVO debattiert. Dazu etwa *Piska,* Die Datenschutzbehörde im Niemandsland zwischen Inquisitor und Entscheidungsorgan – Selbstbezichtigungsverbot im Fokus, ecolex 2023, 614.

39) Siehe aber auch Art 23 Abs 4 letzter UAbs NIS-2-RL.

40) Vgl ErwGr 102 NIS-2-RL.

41) Siehe idZ auch Art 23 Abs 2 NIS-2-RL, der eine Pflicht zur Information der Diensteempfänger auch über Cyberbedrohungen vorsieht.

42) Vgl ErwGr 4f NIS-2-RL.

43) Abhängig davon, ob es sich beim Strafadressaten um eine „wesentliche" oder „wichtige" Einrichtung (Art 3 NIS-2-RL) handelt.

nehmen als Normadressaten fokussiert. Der Wandel zwischen NIS-1 und NIS-2 wird deutlich, kontrastiert man die Sanktionsbestimmung des Art 21 NIS-1-RL mit jener des Art 34 NIS-2-RL. Während erstere bloß davon spricht, dass die MS *„Vorschriften über Sanktionen für Verstöße gegen die nach dieser Richtlinie erlassenen nationalen Bestimmungen“* erlassen, ohne einen Strafadressaten zu nennen, lautet die Marginalrubrik des Art 34 NIS-2-RL nunmehr *„Allgemeine Bedingungen für die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen“*. Im Konzept der NIS-2-RL treffen Geldbußen folglich nur die Unternehmen selbst, ein Umstand, der entsprechend hohe Strafrahmen erforderlich macht. Es ist daher insb davon auszugehen, dass es für die Verhängung von Geldstrafen iSd NIS-2-RL künftig nicht mehr erforderlich sein wird, dass der Verstoß gegen Cybersicherheitspflichten einer bestimmten natürlichen Person im Unternehmen angelastet wird.[44)]

2. Verantwortlichkeit, Haftung und Tätigkeitsverbote für natürliche Personen

Das Sanktionsregime der NIS-2-RL nimmt aber nicht nur die Unternehmen selbst, sondern auch deren wesentliche Entscheidungsträger ins Visier. So haben *„Leitungsorgane“* gem Art 20 Abs 1 NIS-2-RL die von ihren Einrichtungen *„ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit [zu] billigen [und] ihre Umsetzung [zu] überwachen“*. An diese generelle Verantwortlichkeit knüpft die NIS-2-RL entsprechende Sanktionen: Gem Art 20 Abs 1 NIS-2-RL stellen die MS sicher, dass die Leitungsorgane für Verstöße durch ihre Einrichtungen verantwortlich gemacht werden können.[45)] Der Begriff des „Leitungsorgans“ ist dabei funktionell zu verstehen. Die Verantwortlichkeit für die Einhaltung der NIS-2-Pflichten liegt somit stets bei jenen Personen, die im Unternehmen die maßgeblichen Entscheidungen – im Rahmen der konkreten gesellschaftsrechtlichen Ausgestaltung – tatsächlich treffen.[46)]

Die Art der „Verantwortlichkeit“, die gem Art 20 Abs 1 NIS-2-RL auf den Leitungsorganen lastet, gibt die RL hingegen nicht vor. Ihre Ausgestaltung obliegt damit den MS. Als bemerkenswert erweist sich idZ der derzeitige deutsche Gesetzesentwurf zu einem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, der die „Verantwortlichkeit“ als Haftung der Geschäftsleitung für den entstandenen Schaden ausgestaltet. Die Erläuterungen führen dazu aus, dass der *„Schadensbegriff […] sowohl Regressansprüche als auch Bußgeldforderungen umfasst“*.[47)] In Anbetracht der Millionen- und Milliardenstrafen, die die NIS-2-RL vorsieht,[48)] kommt ein vollständiger Durchgriff auf die leitenden natürlichen Personen freilich keinesfalls infrage, womit offen bleibt, nach welchen Kriterien sich der konkrete Anteil der Bußgeldforderung bemisst, für den die Geschäftsleitung einzustehen hat.

Als Ultima Ratio und drastischste „Sanktion“ sieht Art 32 Abs 5 lit b NIS-2-RL schließlich Tätigkeitsverbote vor. Jenen Personen, *„die auf Geschäftsführungs- bzw Vorstandsebene oder Ebene des rechtlichen Vertreters für Leitungsaufgaben“* zuständig sind, kann die Wahrnehmung ihrer *„Leitungsaufgaben in dieser Einrichtung“* untersagt werden, wenn dies erforderlich ist, um die Umsetzung von behördlichen Maßnahmen gem Art 32 Abs 4 lit a–d, f NIS-2-RL zu erzwingen. Aufgrund ihres exekutiven Charakters handelt es sich bei den Tätigkeitsverboten streng genommen nicht um Sanktionsmaßnahmen, weshalb sie auch aufzuheben sind, sobald das betreffende Unternehmen die Maßnahmen umsetzt.[49)]

3. Sanktionen gem Art 36 NIS-2-RL

Komplettiert wird das Sanktionsregime durch die aufgrund von Art 34 NIS-2-RL etwas sonderbare Anordnung des Art 36 NIS-2-RL, wonach die MS Vorschriften über Sanktionen erlassen sollen, *„die bei Verstößen gegen die gemäß dieser Richtlinie erlassenen nationalen Maßnahmen zu verhängen sind“*. Fraglich ist, in welchem Verhältnis die Bestimmung des Art 36 NIS-2-RL zu Art 34 Abs 1 NIS-2-RL über die Verhängung von Geldbußen steht.

Auf den ersten Blick könnte man meinen, die Bestimmungen hätten unterschiedliche Anwendungsbereiche. Die Geldbußen des Art 34 Abs 1 NIS-2-RL würden Verstöße gegen die Pflichten der NIS-2-RL sanktionieren *(„Geldbußen, die […] in Bezug auf Verstöße gegen diese Richtlinie verhängt werden“),* während Art 36 NIS-2-RL nur die Sanktionen für Verstöße gegen nationale Umsetzungsbestimmungen beträfe *(„Sanktionen, die bei Verstößen gegen die gemäß dieser Richtlinie erlassenen nationalen Maßnahmen zu verhängen sind“).*

Ein Verstoß gegen die Bestimmungen der NIS-2-RL durch nicht-staatl Einrichtungen[50)] ist aber gar nicht möglich. Adressaten der RL sind die MS; eine unmittelbare Wirksamkeit von Richtlinienbestimmungen kann nur zulasten des säumigen MS, nicht jedoch zulasten Privater eintreten.[51)] Aufgrund des Art 34 Abs 7 NIS-2-RL, wonach *„jeder Mitgliedstaat Vorschriften dafür festlegen [kann], ob und in welchem Umfang gegen Einrichtungen der öffentlichen Verwaltung Geldbußen verhängt werden können“,* wird aber klar ersichtlich, dass sich auch die Geldbußen gem Art 34 NIS-2-RL hauptsächlich gegen nicht-staatl Einrichtungen und damit Unternehmen richten. Die Anordnung des Art 34 Abs 1 NIS-2-RL *(„Geldbußen, die […] in Bezug auf Verstöße gegen diese Richtlinie verhängt werden“)* lässt sich deswegen nicht dahingehend deuten, dass sie hauptsächlich Geldbußen gegen staatl Einrichtungen behandle. Bei der in Art 34 Abs 1 NIS-2-RL enthaltenen Formulierung, *„Geldbußen, die […] in Bezug auf Verstöße gegen diese Richtlinie verhängt werden“,*[52)] dürfte es sich folglich um ein Redaktionsversehen handeln. Es ist davon auszugehen, dass auch die iSd Art 34 NIS-2-RL verhängten Geldbußen Verstöße gegen die nationalen Umsetzungsbestimmungen und nicht die RL selbst sanktionieren. Welcher (faktische) Anwendungsbereich für die Bestimmung des Art 36 NIS-2-RL verbleibt, ist unklar.

---

44) Vgl nur die SA des GA *Campos Sánchez-Bordona* in C-807/21 *(Deutsche Wohnen SE).*

45) Siehe idZ auch Art 32 Abs 6 NIS-2-RL.

46) Siehe dazu *Schiefer/L. B. Wieser,* NIS-2-RL: Wer trägt die Verantwortung im Unternehmen? – Das „Leitungsorgan“ in der NIS-2-RL, ecolex 2023, 900.

47) Siehe § 38 Abs 2 des Art 1 (BSI-Gesetz) des Entwurfs zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz.

48) Siehe dazu soeben unter D.1.

49) Siehe Art 32 Abs 5 NIS-2-RL.

50) Da die MS Adressaten der NIS-2-RL sind, können staatl Einrichtungen (etwa *„Einrichtungen der öffentlichen Verwaltung“* iSd Nr 10 des Anhang I NIS-2-RL) hingegen schon gegen die RL selbst verstoßen. Siehe *Vcelouch* in *Jaeger/Stöger* (Hrsg), EUV/AEUV Art 288 AEUV Rz 34 ff, 71 (Stand 1. 11. 2017, rdb.at).

51) Siehe etwa *Vcelouch* in *Jaeger/Stöger,* EUV/AEUV Art 288 AEUV Rz 68 ff.

52) Derartiges ordnet auch die englische Sprachfassung des Art 34 Abs 1 NIS-2-RL an.

E. Fazit und Ausblick

Zum gegenwärtigen Zeitpunkt liegt noch kein Gesetzesentwurf für die innerstaatl Umsetzung der NIS-2-RL vor. Es lassen sich deswegen keine abschließenden Aussagen dahingehend treffen, wie der österr Gesetzgeber die ihm von der NIS-2-RL belassenen Spielräume ausfüllen wird und wie deswegen die Pflichten österr Unternehmen ab (voraussichtlich) 18. 10. 2024 im Detail aussehen werden.

Ungeachtet der damit bestehenden Unsicherheiten sollten betroffene Unternehmen dennoch nicht auf den innerstaatl Gesetzesentwurf zur NISG-Novelle warten. Die einschlägigen Regelungen der NIS-2-RL zeichnen sich durchwegs durch einen hohen Detail- und Konkretisierungsgrad aus, weshalb die zentralen Konturen des unternehmerischen Pflichtenprogramms bereits feststehen. Berücksichtigt man zudem die rezentere Gesetzgebungspraxis[53] und nicht zuletzt auch das derzeit in Geltung stehende NISG, so darf davon ausgegangen werden, dass es bei der in Art 5 NIS-2-RL angesprochenen „Mindestharmonisierung" bleibt; von einer Übererfüllung („Gold Plating") der unionsrechtlichen Anforderung an die unternehmerische Cybersicherheit ist nicht auszugehen.

Betroffenen Unternehmen bleibt schließlich trotz des erheblichen Umsetzungsaufwands, mit dem sie die NIS-2-RL konfrontiert, ein Lichtblick: Die NIS-2-RL ist hinsichtlich der Anforderungen, die sie an Einrichtungen stellt (aber auch sonst), der DSGVO sehr ähnlich. Bei der Aufsetzung des NIS-2-Compliance-Projekts können Unternehmen deswegen auf ihre Erfahrungen aus der Umsetzung der DSGVO zurückgreifen. Dabei sollten sie vor allem eine Erkenntnis berücksichtigen, die so manches Unternehmen im Mai 2018, dem Beginn der Anwendung der DSGVO, erlangen musste: Wer bis zum Tag des Anwendungsbeginns damit wartet, seinen Pflichten nachzukommen, bezahlt dies unter Umständen teuer. Das NIS-2-Compliance-Projekt sollte deswegen bereits jetzt starten; am 18. 10. 2024 wird es dafür zu spät sein.

Schlussstrich

Die am 16. 1. 2023 in Kraft getretene NIS-2-RL aktualisiert das unionale Cybersicherheitsrecht und beseitigt jene inhärenten Mängel der NIS-1-RL, die dem Ziel der Gewährleistung eines „hohen gemeinsamen Cybersicherheitsniveaus" in der EU bislang im Weg standen. Dass Netz- und Informationssysteme in der Union künftig besser geschützt werden, dafür sorgen im System der NIS-2-RL vor allem ein erheblich ausgeweiteter Anwendungsbereich sowie scharfe Sanktionen. Hinsichtlich des unternehmerischen Pflichtenprogramms setzt die NIS-2-RL auf Bekanntes. Wie bereits die NIS-1-RL verpflichtet auch ihre Nachfolgerin Unternehmen zum einen zur Setzung von Risikomanagementmaßnahmen und zum anderen zur Information der Behörde bei Eintritt eines Sicherheitsvorfalls. Im Gegensatz zur NIS-1-RL sanktioniert die NIS-2-RL Verstöße gegen diese Gebote aber drastisch: Zukünftig drohen Geldbußen in Höhe von 10 Mio bzw 7 Mio Euro oder 2% bzw 1,4% des weltweiten Konzernumsatzes, eine persönliche Verantwortlichkeit bzw Haftung der Leitungspersonen sowie im äußersten Fall sogar Tätigkeitsverbote für das Management.

[53] Vgl nur das Anti-Gold-Plating-Gesetz 2019, BGBl I 2019/46.