Die NIS-2-RL und ihre Anforderungen an Unternehmen

1.1. Inhaltsverzeichnis

1. Executive Summary

- Mit der am 16.1.2023 in Kraft getretenen NIS-2-RL schärft der Unionsgesetzgeber im unionalen Cybersicherheitsrecht nach. Dabei beseitigt er insbesondere die „inhärenten Mängel" der NIS-1-RL.

- Für die größere Durchschlagskraft des NIS-Cybersicherheitsrechts sorgen im Vergleich zur NIS-1-RL vor allem der erheblich ausgeweitete Anwendungsbereich der NIS-2-RL sowie das scharfe Sanktionsregime.

- Während sich der Anwendungsbereich der NIS-1-RL noch auf Unternehmen in kritischen Sektoren und ausgewählte Anbieter digitaler Dienste beschränkte, erstreckt sich die NIS-2-RL künftig auf weite Teile der Wirtschaft in den Mitgliedstaaten.

- Durch die NIS-2-RL wächst die Liste kritischer Infrastrukturbetreiber von 7 auf 11 Sektoren und es werden künftig auch Unternehmen in Branchen mit erhöhter Sensibilität, wie der Produktion, der Herstellung und des Handels mit chemischen Stoffen, der Produktion, der Verarbeitung und des Vertriebs von Lebensmitteln oder der Telekommunikation in den Anwendungsbereich des NIS-2-Regimes einbezogen.

- Durch das Abstellen auf die Unternehmensschwellenwerte der KMU-Empfehlung der Kommission legt die NIS-2-RL ihren grundsätzlichen Anwendungsbereich im Gegensatz zur NIS-1-RL unionsweit einheitlich fest.

- Für grenzüberschreitend tätige Unternehmen besteht künftig unabhängig vom jeweiligen Mitgliedstaat weitestgehend Klarheit darüber, ob sie in den Anwendungsbereich des NIS-2-Regimes fallen oder nicht.

- Das unternehmerische Pflichtenprogramm ändert sich durch die NIS-2-RL im Vergleich zur NIS-1-RL in seinen Grundsätzen nicht. Weiterhin sind betroffene Unternehmer einerseits zur Setzung von Risikomanagementmaßnahmen zur Verhinderung von Cybersicherheitsvorfällen, andererseits zur Meldung von Vorfällen an die Behörde verpflichtet.

- Als neue Unternehmenspflichten sieht die NIS-2-RL insbesondere ein Gebot zur Gewährleistung der Cybersicherheit der Lieferkette und die Notwendigkeit von Schulungsmaßnahmen für Leitungsorgane und Mitarbeiter vor.

- Durch die NIS-2-RL wandelt sich die Pflicht zum Schutz von Netz- und Informationssystemen von „spezifisch" zu „umfassend". Unternehmen sind künftig verpflichtet, das gesamte Netz- und Informationssystem im Unternehmen zu schützen.

- Der Prozess der Meldung von erheblichen Sicherheitsvorfällen wird von der NIS-2-RL strikt getaktet. Die Unternehmen werden zur Übermittlung von spezifischen Informationen an die Behörde innerhalb konkreter, knapp bemessener Zeitfenster verpflichtet.

- Sofern Sicherheitsvorfälle auch Auswirkungen auf die Empfänger der Dienste eines Unternehmens haben können, sind auch diese zu informieren.

- Das NIS-Sanktionsregime wird durch die NIS-2-RL erheblich verschärft.

- Im Gegensatz zur NIS-1-RL überlässt die NIS-2-RL die Festsetzung des Strafrahmens für Geldbußen nicht mehr den Mitgliedstaaten, sondern sieht diese konkret vor.

- Bei Verstößen gegen die Unternehmenspflichten der NIS-2-RL können Geldbußen in Höhe von 10 sowie 7 Mio Euro bzw 2 sowie 1,4% des weltweiten Konzernumsatzes fällig werden.

- Leitungsorgane bzw Leitungspersonen trifft eine persönliche Verantwortlichkeit bzw Haftung für Verstöße ihrer Einrichtung gegen die NIS-2-RL.

- Als Ultima Ratio sieht die NIS-2-RL Tätigkeitsverbote für Leitungspersonen vor.

- Die NIS-2-RL ist von den Mitgliedstaaten bis 17.10.2024 innerstaatlich umzusetzen. Zum gegenwärtigen Zeitpunkt liegt noch kein Entwurf des österreichischen Gesetzgebers für die Umsetzung der NIS-2-RL vor.

- Es ist davon auszugehen, dass es der österreichische Gesetzgeber bei der Mindestharmonisierung der NIS-2-Pflichten belassen wird. Von einer Übererfüllung („Gold Plating") der unionsrechtlichen Anforderung an die unternehmerische Cybersicherheit ist nicht auszugehen.

- Es ist davon auszugehen, dass die NIS-2-Umsetzungsnovelle das Ende des „State driven Approach" (Ermittlung von einbezogenen Einrichtungen mittels Bescheid) im NISG herbeiführen wird.

- Die NIS-2-RL ist hinsichtlich der Anforderungen, die sie an Unternehmen stellt (aber auch sonst), der DSGVO sehr ähnlich. Unternehmen können deswegen bei der Aufsetzung des NIS-2-Cybersicherheits-Projekts auf ihre Erfahrungen aus der Umsetzung der DSGVO zurückgreifen.

- Betroffene Unternehmen werden die Verpflichtungen aus der NIS-2-RL bei rechtzeitiger Umsetzung durch den österreichischen Gesetzgeber ab dem 18.10.2024 zu erfüllen haben.

- Die Europäische Kommission schätzt, dass je nachdem, ob Unternehmen bereits NIS-1 erfüllen oder nicht, sie ihr Cybersicherheitsbudget um 12 bzw 22 % erhöhen werden müssen.

2. Ausgangssituation sowie Zweck und Struktur des White Paper

CISCO Systems Austria ist ein Unternehmen der Telekommunikationsbranche, das als Mitglied des weltweit agierenden CISCO Systems-Konzerns (Weltmarktführer in den Bereichen IT und Netzwerk) unterschiedliche Hard- und Softwareprodukte für den Netzwerkbetrieb anbietet. Neben Hardwarekomponenten wie Routern, Switches oder industriellen IOT-Lösungen wie Sensoren umfasst das Produktportfolio von CISCO Systems Austria unter anderem auch Software zur Gewährleistung der Netzwerksicherheit und unterschiedliche Cloud-Lösungen.

CISCO Systems Austria hat Schiefer Rechtsanwälte mit dem Verfassen eines White Papers zur NIS-2-RL[1] beauftragt. Die NIS-2-RL ist am 16.1.2023 in Kraft getreten[2] und von den Mitgliedstaaten gemäß Artikel 41 Absatz 1 NIS-2-RL bis zum 17.10.2024 umzusetzen. Bei rechtzeitiger Umsetzung durch den österreichischen Gesetzgeber[3] haben betroffene Unternehmen in Österreich die Pflichten aus der NIS-2-RL damit ab dem 18.10.2024 zu erfüllen.[4]

Mit der NIS-2-RL, die ein hohes gemeinsames Cybersicherheitsniveau von Netz- und Informationssystemen in der Union sicherstellen soll,[5] aktualisiert der Unionsgesetzgeber den bisherigen unionsrechtlichen Stammrechtsakt zur Cybersicherheit, die NIS-1-RL.[6] Zweck des vorliegenden White Papers ist die Darstellung der aus der NIS-2-RL folgenden Anforderungen an Unternehmen, denen diese ab dem 18.10.2024 voraussichtlich unterliegen werden.[7]

Zum Zeitpunkt des Verfassens des vorliegenden White Paper liegt noch kein Entwurf für eine Novelle zum österreichischen NISG[8] vor; sämtliche im White Paper getroffene Feststellungen stehen deswegen unter der Bedingung der rechtmäßigen Umsetzung der NIS-2-RL durch den österreichischen Gesetzgeber. Aus zwei Gründen lassen sich aber dennoch bereits zum jetzigen Zeitpunkt konkrete Aussagen treffen: Zum einen, weil die NIS-2-RL die unternehmensbezogenen Pflichten – nicht zuletzt auch im Vergleich zur NIS-1-RL – überaus detailliert festlegt; regelungstechnisch nähert sich die NIS-2-RL dadurch einer Verordnung an, ein Umstand, der mit einem verminderten mitgliedstaatlichen Spielraum bei der Umsetzung einhergeht.

Zum anderen, weil die NIS-2-RL zwar lediglich Mindeststandards (Stichwort: Mindestharmonisierung) vorsieht,[9] der österreichische Gesetzgeber in jüngerer Zeit jedoch regelmäßig von der Übererfüllung unionsrechtlicher Umsetzungspflichten absah (Stichwort: „Anti-Gold Plating");[10] auch die Umsetzung der NIS-1-RL im NISG war von der gesetzgeberischen Intention getragen, die RL nicht „überzuerfüllen".[11] Es kann deswegen davon ausgegangen werden, dass sich der österreichische Gesetzgeber bei der Novellierung des NISG weitestgehend an den entsprechenden Vorgaben der NIS-2-RL orientieren wird.

Zur besseren Verständlichkeit bietet Punkt 3. zunächst einen Überblick über die unternehmensbezogenen Pflichten im Regelungsregime der NIS-1-RL sowie des NISG in seiner aktuellen Fas-

1 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

2 Siehe Artikel 45 NIS-2-RL.

3 Richtlinien der EU kommt – insbesondere zulasten Privater – keine unmittelbare Wirksamkeit zu. Die in ihnen enthaltenen Rechtsvorschriften sind von den Mitgliedstaaten in innerstaatliches (nationales) Recht umzusetzen; nicht staatliche Adressaten werden erst durch die innerstaatlichen Umsetzungsbestimmungen verpflichtet. Siehe Vcelouch in Jaeger/Stöger, EUV/AEUV Art 288 AEUV Rz 34 ff.

4 Siehe auch Artikel 41 Absatz 1 Satz 3 NIS 2-RL.

5 Vgl nur den Langtitel der NIS-2-RL.

6 RL 2016/1148/EU.

7 Vgl idZ jedoch den Umstand, dass der österreichische Gesetzgeber bereits die NIS-1-RL verspätet umsetzte. Die NIS-1-RL sah die Anwendung der innerstaatlichen Umsetzungsvorschriften ab dem 10.5.2018 vor (Artikel 25 Absatz 1 NIS-1-RL). Das österreichische NISG, das die Richtlinie umsetzt, trat aber erst mit 29.12.2018 in Kraft (§ 31 NISG). Siehe dazu näher Anderl/Müller/Pichler in Paulus 185.

8 Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz), BGBl I 111/2018.

9 Siehe Artikel 5 NIS-2-RL.

10 Siehe nur das Anti-Gold-Plating-Gesetz 2019, BGBl I 46/2019.

11 Vorblatt und WFA RV 369 BlgNR 26. GP 2; siehe auch Anderl et al in Anderl et al, NISG § 2 NISG Rz 4.

sung. Daran anschließend erfolgt in Punkt 4. eine überblicksmäßige Darstellung über die wesentlichen Neuerungen der NIS-2-RL. Punkt 5. widmet sich sodann dem durch die NIS-2-RL künftig stark erweiterten Anwendungsbereich des unionalen Cybersicherheitsrechts. In Punkt 6. werden die wesentlichen unternehmensbezogenen Pflichten der NIS-2-RL und in Punkt 7. das entsprechende Sanktionsregime erörtert. Punkt 8. liefert einen Ausblick auf die innerstaatliche Umsetzung der NIS-2-RL durch die erwartete NISG-Novelle, bevor Punkt 9. auf den Umstand hinweist, dass Unternehmen bei der Umsetzung der NIS-2-Pflichten auf DSGVO-Erfahrungen zurückgreifen können.

3. Bisherige Rechtslage: NIS-1-RL und das NISG

3.1. NIS-1-RL: Erste Schritte in der Cybersicherheit

Wie bereits die Namensgebung nahelegt,[12] handelt es sich bei der NIS-2-RL nicht um den ersten unionalen Rechtsakt, mit dem Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union festgelegt werden. Ein dahingehender initialer Vorstoß[13] erfolgte bereits durch die NIS-1-RL, die seit rund 5 Jahren[14] kritische Infrastrukturbetreiber in den Mitgliedstaaten 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"),[15] wobei diese insbesondere dem Umstand geschuldet sind, dass die Richtlinie wesentliche Fragen – wie die Festlegung des konkreten Anwendungsbereichs[16] oder die Strafhöhe[17] – der Prärogative der Mitgliedstaaten überließ.[18] Dies führte dazu, dass das Umsetzungsniveau in den Mitgliedstaaten erheblich divergierte, weshalb sich der Unionsgesetzgeber nach einer Evaluation der NIS-1-RL auch dazu genötigt sah, das unionale Cybersicherheitsrecht mit der NIS-2-RL weiterzuentwickeln.[19]

Der österreichische Gesetzgeber kam seiner aus der NIS-1-RL resultierenden Umsetzungsverpflichtung (zumindest zum Teil)[20] mit der Erlassung des Netz- und Informationssystemsicherheitsgesetzes (NISG) nach. Eine Befassung mit diesem ist zum gegenwärtigen Zeitpunkt aus zwei Gründen geboten: Zum einen stellt es bis zum Ablauf der Umsetzungsfrist der NIS-2-RL am 17.10.2024[21] das maßgebliche innerstaatliche Cybersicherheits-Regelungsregime dar. Es kann für betroffene Unternehmer deswegen als Ausgangspunkt für die Aufsetzung und den Start ihres Cybersicherheits-Compliance-Projekts dienen; oder anders gewendet: Bevor die NIS-2-Pflichten erfüllt werden, sollten Unternehmen zunächst einmal sicherstellen, dass sie den Anforderungen der NIS-1-RL und damit des NISG entsprechen.

Zum anderen liegt gegenwärtig noch kein Entwurf für eine NIS-2-Umsetzungsnovelle des NISG vor, weshalb sämtliche Aussagen zu den künftig bestehenden unternehmensbezogenen Cybersicherheitspflichten zumindest zum Teil prognosebehaftet sind. Dem NISG kommt in diesem Zusammenhang gewisse Orientierungsfunktion zu, als der österreichische Gesetzgeber bei der Umsetzung der NIS-2-RL wohl nicht grundlos von bestehenden Konzepten – wie etwa der Pflichtenkonkretisierung durch Verordnung[22] – abweichen wird.

3.2. Anwendungsbereich des NISG

3.2.1. Allgemeines

Vom Anwendungsbereich des österreichischen Umsetzungsgesetzes zur NIS-1-RL, dem NISG, werden gemäß § 2 NISG gegenwärtig nur jene Unternehmen erfasst, die entweder als „Betreiber wesentlicher Dienste" oder als „Anbieter digitaler Dienste" zu qualifizieren sind.[23] Bei der Festlegung des Anwendungsbereichs des NISG auf Unter-

12 Siehe zur Fortentwicklung der NIS-1-RL durch die NIS-2-RL bereits unter 2.

13 So auch Kristoferitsch/Lachmayer, ecolex 2020, 77: „Mit der NIS-RL beginnt der Unionsgesetzgeber – abgesehen von Art 32 DSGVO – erstmals gesetzliche Vorgaben für den Bereich der IT-Sicherheit festzulegen".

14 Die NIS-1-RL war zum 10.5.2018 umzusetzen. Artikel 25 Absatz 1 NIS-1-RL.

15 Erwägungsgrund 2 NIS-2-RL.

16 Siehe Artikel 5 NIS-1-RL.

17 Siehe Artikel 21 NIS-1-RL.

18 Vgl auch Erwägungsgrund 4 NIS-1-RL: „In der Richtlinie (EU) 2016/1148 wurde den Mitgliedstaaten auch ein sehr großer Ermessensspielraum bei der Umsetzung der in der Richtlinie festgelegten Verpflichtungen in Bezug auf die Sicherheit und die Meldung von Sicherheitsvorfällen eingeräumt. Diese Verpflichtungen wurden daher auf nationaler Ebene auf sehr unterschiedliche Weise umgesetzt".

19 Vgl Erwägungsgrund 4 f NIS-2-RL.

20 So darf es etwa durchaus bezweifelt werden, dass die in § 26 Absatz 1 NISG festgelegten Geldstrafen in Höhe von „bis zu 50.000 Euro, im Wiederholungsfall bis zu 100.000 Euro" den Anforderungen des Artikel 21 NIS-1-RL an die „wirksam[e], angemessen[e] und abschreckend[e]" Wirkung von Sanktionen gerecht werden.

21 Artikel 41 Absatz 1 NIS-2-RL.

22 Siehe § 4 Absatz 2 Ziffer 3 NISG.

23 Die ebenfalls in § 2 NISG genannten „Einrichtungen der öffentlichen Verwaltung" werden aufgrund des Fokus auf Unternehmen ausgeklammert.

nehmen beschränkte sich der österreichische Gesetzgeber insoweit weitestgehend auf die Mindestharmonisierung,[24]
als er es unterließ, über die Vorgaben des Artikel 1 NIS-1-RL in Verbindung mit Anhängen II und III der NIS-1-RL hinausgehend Unternehmen den Anforderungen des unionalen Cybersicherheitsrechts zu unterwerfen.[25]

3.2.2. Betreiber wesentlicher Dienste

Bei den gemäß § 2 NISG dem Gesetz unterliegenden „Betreibern wesentlicher Dienste" handelt es sich gemäß § 3 Ziffer 10 NISG um Einrichtungen *„mit Niederlassung in Österreich, die einen wesentlichen Dienst erbring[en]"*. Letzterer wird in § 3 Ziffer 9 NISG wiederum als *„Dienst"* definiert, *„der in einem der in § 2 genannten Sektoren"* – das sind die Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und digitale Infrastruktur – erbracht wird; vereinfachend lassen sich die „Betreiber wesentlicher Dienste" auch als „kritische Infrastrukturbetreiber" bezeichnen.[26]

Neben der Leistungserbringung in einem der Sektoren des § 2 NISG ist für einen „wesentlichen Dienst" gemäß § 3 Ziffer 9 NISG weiters erforderlich, dass der Dienst *„eine wesentliche Bedeutung insbesondere für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie hat"* und das seine Verfügbarkeit *„abhängig von Netz- und Informationssystemen ist"*. Die Aufzählung der genannten Tätigkeiten, für deren Aufrechterhaltung der „wesentliche Dienst" „wesentliche" Bedeutung entfaltet, ist dabei demonstrativ (*argumentum*: *„insbesondere"*), wie nicht zuletzt auch ein Blick in die NIS-1-RL verdeutlicht: Gemäß Artikel 5 Absatz 2 littera a NIS-1-RL handelte es sich bei „wesentlichen Diensten" um Dienste, die *„für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich"* sind. Auch die Aufrechterhaltung von anderen kritischen gesellschaftlichen oder wirtschaftlichen Tätigkeiten, als jene in § 3 Ziffer 9 NISG aufgezählten, kann damit die Qualifikation als „wesentlicher Dienst" begründen.

In Zusammenschau der §§ 2, 3 Ziffer 9 sowie 3 Ziffer 10 NISG fallen Unternehmen als „Betreiber wesentlicher Dienste" damit immer dann in den Anwendungsbereich des NISG, wenn sie (kumulativ)

- in Österreich niedergelassen sind,
- sie ihre Tätigkeit in einem der Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und digitale Infrastruktur ausüben,
- der von ihnen erbrachte Dienst wesentliche Bedeutung für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten entfaltet, und
- die Verfügbarkeit des Dienstes von Netz- und Informationssystemen abhängig ist.

Der Anwendungsbereich der unternehmensbezogenen Sicherheitspflichten erstreckt sich für „Betreiber wesentlicher Dienste" allerdings nur soweit, wie ihre Netz- und Informationssysteme in die Bereitstellung des wesentlichen Dienstes eingebunden sind.[27] Das NISG (in Umsetzung der NIS-1-RL) geht gegenwärtig somit von einem spezifischen Netzwerkschutz aus, der all jene Teile der Gesamtheit an Netz- und Informationssystemen der Betreiber wesentlicher Dienste ausklammert, die mit der Erbringung des wesentlichen Dienstes nichts zu tun haben (dies ändert sich mit der NIS-2-RL).[28] Erwägungsgrund 22 NIS-1-RL führt das anschauliche Beispiel eines Flughafenbetreibers an, der neben wesentlichen Diensten wie dem *„Start- und Landebahn-Management"* auch nicht-wesentliche Dienste wie die *„Bereitstellung von Einkaufsbereichen"* erbringt. Nur die in das *„Start- und Landebahn-Management"*

24 Vgl in diesem Zusammenhang Anderl et al in Anderl et al, NISG § 2 NISG Rz 2, die davon sprechen, dass das NISG einen eingeschränkten, und keinen gesamtgesellschaftlichen Ansatz verfolge. Der Gesetzgeber hätte „weitere Bereiche hinzufügen können" (Rz 4).

25 Der österreichische Gesetzgeber ging allerdings insoweit über die Mindestharmonisierung der NIS-1-RL hinaus, als er gemäß § 2 NISG auch „Einrichtungen der öffentlichen Verwaltung" in den Anwendungsbereich des NISG einbezog.

26 Vgl Kristoferitsch/Lachmayer, ecolex 2020, 74 ff.

27 Siehe § 17 Absatz 1 NISG; weiters Artikel 14 Absatz 1 in Verbindung mit Erwägungsgrund 22 NIS-1-RL; Kristoferitsch/Lachmayer, ecolex 2020, 76.

28 Durch die NIS-2-RL wandelt sich das Schutzkonzept für Netz- und Informationssysteme grundlegend. Künftig haben wesentliche und wichtige Einrichtungen sämtliche Netz- und Informationssysteme, und damit nicht nur jene, die in die kritische Diensteerbringung eingebunden sind, zu schützen. Siehe dazu unter 6.2.

eingebundenen Netz- und Informationssysteme fallen unter das Schutzkonzept der NIS-1-RL und des NISG, nicht hingegen die zur *„Bereitstellung von Einkaufsbereichen"* dienenden Netzwerke.

Angesichts der erheblichen Zahl an unbestimmten Rechtsbegriffen, mit denen der Anwendungsbereich des NISG operiert (*„eine wesentliche Bedeutung insbesondere für die Aufrechterhaltung […]"*),[29] war und ist es für betroffene Unternehmen entlastend, dass das System des NISG gegenwärtig eine bescheidmäßige Ermittlung der österreichischen Betreiber wesentlicher Dienste durch den Bundeskanzler vorsieht („State driven Approach").[30] „Betreiber wesentlicher Dienste" wird man dadurch, dass einen der Bundeskanzler mit Bescheid dazu erklärt, wobei dessen Rechtskraft für die Betreibereigenschaft konstitutive Wirkung entfaltet.[31]

3.2.3. Anbieter digitaler Dienste

Zusätzlich zu den *„Betreibern wesentlicher Dienste"* bringt § 2 NISG das Gesetz auch auf *„Anbieter[…] digitaler Dienste"* zur Anwendung. Bei diesen handelt es sich gemäß § 3 Ziffer 13 NISG um juristische Personen oder eingetragene Personengesellschaften, *„die einen digitalen Dienst in Österreich anbiete[n]"*. „Anbieter digitaler Dienste" unterliegen dem NISG aber nur, sofern sie zusätzlich als zumindest „mittleres Unternehmen" im Sinne der KMU-Empfehlung der Kommission gelten[32] und entweder ihre Hauptniederlassung in Österreich haben oder einen Vertreter im Sinne des § 3 Ziffer 14 NISG namhaft gemacht haben.[33]

Den Begriff des „digitalen Dienstes" definiert § 3 Ziffer 12 NISG als *„einen Dienst im Sinne des § 3 Z 1 E-Commerce-Gesetz (ECG)"*, bei dem es sich um *„einen Online-Marktplatz, eine Online-Suchmaschine oder einen Cloud-Computing-Dienst handelt"*. Um unter das NISG zu fallen, müssen die betreffenden Unternehmen folglich entweder eine Online-Marktplatz, eine Online-Suchmaschine oder einen Cloud-Computing-Dienst betreiben, wobei aufgrund des Verweises auf das ECG zusätzlich erforderlich ist, dass der Dienst entgeltlich erbracht wird (die Entgeltlichkeit ist auch bei Umwegrentabilität – etwa Werbeeinnahmen – gegeben).[34]

Auch für Anbieter digitaler Dienste gilt, dass sich der Anwendungsbereich der unternehmensbezogenen Sicherheitspflichten auf sie nur soweit erstreckt, wie ihre Netz- und Informationssysteme in die Bereitstellung des betreffenden digitalen Dienstes eingebunden sind; es kann diesbezüglich auf die hinsichtlich der Betreiber wesentlicher Dienste getätigten Ausführungen verwiesen werden.[35] Anders als hinsichtlich der Betreiber wesentlicher Dienste ist eine bescheidmäßige Ermittlung der Anbieter digitaler Dienste („State driven Approach") aber nicht vorgesehen.

3.3. Die unternehmerischen Pflichten gemäß §§ 16 ff NISG

Wesentlichste Rechtsfolge der Qualifikation eines Unternehmens als „Betreiber wesentlicher Dienste" oder „Anbieter digitaler Dienste" ist, dass sie damit dem Cybersicherheits-Pflichtenprogramm des NISG entsprechen müssen. Die Pflichten, die Unternehmen als Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste gemäß den Bestimmungen der §§ 16 ff NISG treffen, lassen sich in die zwei Gruppen „IT-Sicherheitsmaßnahmen" und „Meldepflichten" teilen.[36] Für Betreiber wesentlicher Dienste enthält § 17 NISG die Regelungen bezüglich *„Sicherheitsvorkehrungen"* und § 19 NISG die entsprechende Meldepflicht bei Sicherheitsvorfällen. Spiegelbildliche Vorgaben für Anbieter digitaler Dienste finden sich in § 21 NISG.

Auf gesetzlicher Ebene (§§ 17 Absatz 1 und 21 Absatz 1 NISG) werden die unternehmensbezogenen Pflichten zur Setzung von *„Sicherheitsvorkehrungen"* abstrakt dahingehend umschrieben,

29 § 3 Ziffer 9 NISG.
30 Siehe § 16 Absatz 1 NISG; Anderl/Müller/Pichler in Paulus 186 f.
31 Häusler in Anderl et al, NISG § 16 NISG Rz 12.
32 Siehe zu den Kriterien der KMU-Empfehlung, bei deren Erfüllung ein „mittleres Unternehmen" vorliegt, unter 5.2.3.
33 Fraglich ist, ob dieses zusätzliche Erfordernis (Hauptniederlassung oder benannter Vertreter) für die Qualifikation als „Anbieter digitaler Dienste" im NISG der NIS-1-RL entspricht.
34 Siehe Anderl et al in Anderl et al, NISG § 3 NISG Rz 33 ff.
35 Siehe dazu bereits unter 3.2.2.
36 Siehe Kristoferitsch/Lachmayer, ecolex 2020, 76.

dass *„geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen"* sind. Diese müssen den Stand der Technik berücksichtigen *„und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen […] sein"*.[37] Gemäß § 4 Absatz 2 Ziffer 3 NISG ist der *„Bundeskanzler […] im Einvernehmen mit dem Bundesminister für Inneres"* ermächtigt, mit Verordnung die Sicherheitsvorkehrungen im Sinne des § 17 Absatz 1 NISG detaillierter auszugestalten.

Auf Basis der genannte Verordnungsermächtigung ist die NISV[38] ergangen, in deren § 11 in Verbindung mit Anlage I leg cit die Sicherheitsanforderungen des § 17 Absatz 1 NISG für Betreiber wesentlicher Dienste näher konkretisiert werden. Für Anbieter digitaler Dienste enthält die NISV hingegen keine Vorgaben, weil die NIS-1-RL diesen Bereich vollharmonisiert.[39] Eine entsprechende Verordnungsermächtigung im NISG fehlt deswegen; § 21 Absatz 1 NISG nennt lediglich unterschiedliche Gesichtspunkte, die bei der Festsetzung von Sicherheitsmaßnahmen zu berücksichtigen sind (*„Sicherheit der Systeme und Anlagen"*, *„Bewältigung von Sicherheitsvorfällen"*, *„Betriebskontinuitätsmanagement"*, *„Überwachung"*, *„Überprüfung und Erprobung"*, *„Einhaltung der internationalen Normen"*). Entsprechende Konkretisierungen für Anbieter digitaler Dienste finden sich („Vollharmonisierung") in der Durchführungsverordnung 2018/15/EU.

Trotz dieser gesetzlichen Differenzierung und des Umstandes, dass die in § 11 NISV aufgelisteten Sicherheitsmaßnahmen für Anbieter digitaler Dienste keine Relevanz entfalten,[40] wird in der Literatur zutreffend darauf hingewiesen, dass sich die von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste konkret zu setzenden Sicherheitsmaßnahmen im Ergebnis allerdings nicht wesentlich unterscheiden dürften. Denn die in § 11 NISV angeführten Sicherheitsmaßnahmen orientieren sich weitgehend an internationalen Standards – wie ISO/IEC 27001 –, auf die ebenso § 21 Absatz 1 littera e NISG verweist (*„Einhaltung der internationalen Normen"*) und auf die auch Anbieter digitaler Dienste regelmäßig zurückgreifen. Zudem enthält die Durchführungsverordnung 2018/15/EU weitestgehend Sicherheitsmaßnahmen, die die Sicherheitsvorgaben der NISV widerspiegeln.[41]

Während Anbieter digitaler Dienste die Erfüllung der NIS-Cybersicherheitspflichten gemäß § 21 Absatz 4 NISG nur auf Verlangen des Bundesministers für Inneres (BMI) nachweisen müssen, normiert § 17 Absatz 3 NISG für Betreiber wesentlicher Dienste eine Verpflichtung zum periodischen Nachweis. Letztere haben *„mindestens alle drei Jahre nach Zustellung des Bescheides gemäß § 16 Abs. 4 Z 1 [– mit dem sie als Betreiber wesentlicher Dienste ermittelt werden –] die Erfüllung der Anforderungen […] gegenüber dem Bundesminister für Inneres nachzuweisen"*.

Bereits der Gesetzestext des § 17 Absatz 3 NISG hebt dabei die Bedeutung hervor, die Zertifizierungen nach internationalen Normen – etwa ISO/IEC 27001 – in diesem Zusammenhang zukommt. Zum Nachweis der Erfüllung ihrer Verpflichtungen übermitteln Betreiber wesentlicher Dienste eine *„Aufstellung der vorhandenen Sicherheitsvorkehrungen durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen"*. Die Umsetzung des NIS-Cybersicherheits-Compliance-Projekts besteht damit in aller Regel darin, sich entsprechend dem Stand der Technik zertifizieren zu lassen, wobei die Literatur ausdrücklich betont, dass eine *„lediglich interne Überprüfung im Unternehmen samt Nachweis – bspw durch die interne Revision – […] nicht ausreichend [ist], auch wenn das zu überprüfende Unternehmen selbst als qualifizierte Stelle anerkannt wurde"*.[42]

Sollte trotz aller (oder aufgrund des Fehlens von) Sicherheitsvorkehrungen dennoch ein *„Sicherheitsvorfall"* eintreten, sind sowohl Betreiber wesentlicher Dienste (§ 19 NISG) als auch Anbieter digitaler Dienste (§ 21 Absatz 2 NISG) verpflichtet, eine behördliche Meldung zu erstatten. Zur Ab-

37 § 17 Absatz 1 NISG und im Wesentlichen gleichlautend § 21 Absatz 1 NISG.

38 Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung), BGBl II 215/2019.

39 Siehe Heußler in Anderl et al, NISG § 21 NISG Rz 1 ff.

40 Heußler in Anderl et al, NISG § 21 NISG Rz 4.

41 Heußler in Anderl et al, NISG § 21 NISG Rz 4.

42 Mayer in Anderl et al, NISG § 17 NISG Rz 17 ff.

wicklung des Meldeprozederes wurde die staatliche Plattform <https://nis.cert.at/> eingerichtet, die es sowohl Betreibern wesentlicher Dienste als auch Anbietern digitaler Dienste unbürokratisch ermöglicht, eine entsprechende Meldung – wie gesetzlich gefordert – „unverzüglich" zu erstatten.[43]

3.4. Verwaltungsstrafen (§ 26 NISG)

Trotz des Umstandes, dass das NISG damit *„den von der NIS[-1]-RL umfassten Unternehmen zahlreiche und durchaus aufwendige Pflichten auferlegt"*,[44] fristet(e) das unionale Cybersicherheitsrecht bislang, etwa im Vergleich zum Datenschutzrecht der DSGVO, ein stiefmütterliches Dasein. Dies dürfte vor allem dem Sanktionsregime des NISG geschuldet sein. Bei Verstößen gegen das NISG drohen gemäß § 26 leg cit gegenwärtig lediglich Geldstrafen bis zu 50.000 Euro; im Wiederholungsfall kann die Behörde Geldstrafen bis zu 100.000 Euro verhängen.

In Anbetracht dessen, dass das NISG seinen Anwendungsbereich derzeit im Ergebnis nur auf große oder sehr große Unternehmen erstreckt,[45] dass § 26 Absatz 6 NISG ein Absehen von der Bestrafung des natürlichen Verantwortlichen bei Bestrafung der juristischen Person ermöglicht (Opportunitätsprinzip),[46] sowie der nach der herrschenden Rechtsprechung und Lehre bestehenden Zulässigkeit der Übernahme von gegen natürliche Personen verhängte Geldstrafen durch die Gesellschaft,[47] waren die Compliance-Anreize für die dem NISG unterworfenen Unternehmen denkbar schwach ausgeprägt. Bezeichnenderweise existiert auch – soweit ersichtlich – kein einziges verwaltungsgerichtliches Judikat zum NISG, ein Umstand, der dafürspricht, dass das NISG in der verwaltungsstrafrechtlichen Praxis der Behörden bislang nicht oder kaum vollzogen wurde. Abschließend bleibt zu bemerken, dass es sich bei den niedrigen Strafen des NISG[48] um einen jener Mängel in der Umsetzung der NIS-RL gehandelt haben dürfte,[49] die den Unionsgesetzgeber letztlich zur Revision des unionalen Cybersicherheitsrechts durch die NIS-2-RL bewogen.

3.5. Zwischenresümee

Zusammenfassend entfaltet das NISG derzeit nur für jene Unternehmen, die entweder bestimmte kritische Infrastrukturdienstleistungen (Betreiber wesentlicher Dienste)[50] oder ausgewählte digitale Dienste („Anbieter digitaler Dienste") erbringen, Relevanz. Diese werden zum einen auf die Setzung von Sicherheitsmaßnahmen verpflichtet, um die Integrität jener Netz- und Informationssysteme zu gewährleisten, die sie zur Erbringung ihrer Dienste nutzen. Zum anderen haben Betreiber wesentlicher Dienste und Anbieter digitaler Dienste „Sicherheitsvorfälle" „unverzüglich" behördlich zu melden.

Den eingeschränkten Ansatz des gegenwärtig in Geltung stehenden Cybersicherheitsrechts, nur Unternehmen in einigen wenigen, ausgewählten Sektoren in den Fokus zu nehmen, gibt der Unionsgesetzgeber mit der NIS-2-RL nunmehr weitestgehend auf. Künftig wird sich das NIS-2-Cybersicherheitsrecht über erhebliche Teile der Wirtschaft legen und sich damit immer mehr in Richtung eines allgemeinen Cybersicherheitsrechts wandeln.[51]

43 Siehe §§ 19 Absatz 1 und 21 Absatz 2 NISG.

44 Kristoferitsch/Lachmayer, ecolex 2020, 75.

45 Vgl in diesem Zusammenhang bereits unter 3.2.

46 Siehe Müller in Anderl et al, NISG § 26 NISG Rz 13.

47 OGH 3 Ob 96/55; Graf in Kletečka/Schauer, ABGB-ON1.05 § 879 ABGB Rz 205.

48 Die geringe Strafhöhe des NISG wird auch in der Literatur zutreffend hervorgehoben. Siehe etwa Kristoferitsch/Lachmayer, ecolex 2020, 77, die von einer „bemerkenswerten Abkehr von den hohen Strafrahmen der DSGVO" sprechen.

49 Vgl Erwägungsgründe 2 ff NIS-2-RL.

50 Der Anwendungsbereich der NIS-1-RL ist auf einzelne Sektoren kritischer Infrastruktur beschränkt; etwa sind die Sektoren „Lebensmittel" und „Abwasserversorgung" vom Anwendungsbereich der RL ausgenommen. Siehe Anderl/Müller/Pichler in Paulus 184 f.

51 Siehe zum erweiterten Anwendungsbereich der NIS-2-RL im Detail unter 5.

4. Überblick NIS-2-RL – Was ist neu?

Bevor im Detail auf die unternehmensbezogenen Regelungen der NIS-2-RL eingegangen wird, sollen die wesentlichen Neuerungen der Richtlinie kurz überblicksartig dargestellt sein. Ein Vergleich mit der NIS-1-RL macht umgehend deutlich, dass der Unionsgesetzgeber mit der NIS-2-RL einen Paradigmenwechsel im Cybersicherheitsrecht der Union einläutet.[52]

Dieser Umstand zeigt sich zunächst anhand des erheblich ausgeweiteten Anwendungsbereichs:[53] Beschränkte der Unionsgesetzgeber den Anwendungsbereich der NIS-1-RL noch auf Unternehmen in kritischen Sektoren und ausgewählte Anbieter digitaler Dienste, erstreckt sich die NIS-2-RL künftig auf weite Teile der Wirtschaft in den Mitgliedstaaten.[54] In diesem Umstand kommt eine wesentliche Änderung der Zielsetzung des unionalen Cybersicherheitsrechts zum Ausdruck. Cybersicherheit soll künftig nicht nur in ausgewählten Sektoren kritischer Infrastruktur die Aufrechterhaltung des Betriebs sichern, sondern im Sinne eines umfassenden Ansatzes ein allgemein hohes Niveau an Cybersicherheit in der Union gewährleisten.

Während sich beim Anwendungsbereich der NIS-Bestimmungen vieles ändert, bleibt das für Unternehmen maßgebliche Pflichtenprogramm in seinen Grundsätzen gleich: Auch in der NIS-2-RL stehen Risikomanagementmaßnahmen und die Meldung von Sicherheitsvorfällen im Zentrum der unternehmerischen Pflichten.[55] Die Feinheiten liegen allerdings im Detail. Zum einen schärft der Unionsgesetzgeber an unterschiedlichen Stellen nach, etwa, indem er konkrete und knapp bemessene Fristen für den Ablauf des Meldungsprozesses vorsieht. Zum anderen werden mit dem Gebot zur Gewährleistung der Cybersicherheit der Lieferkette und der Notwendigkeit von Schulungsmaßnahmen für Leitungsorgane und Mitarbeiter teils auch neue Unternehmenspflichten geschaffen.

Bemerkenswert ist in dieser Hinsicht, dass die NIS-2-RL von einbezogenen Einrichtungen bzw Unternehmen künftig verlangt, ihre Netz- und Informationssysteme nicht bloß spezifisch, sondern umfassend zu schützen.[56] Im Regime der NIS-1-RL war dies nicht der Fall: Betreiber wesentlicher Dienste und Anbieter digitaler Dienste mussten Sicherheitsmaßnahmen nur hinsichtlich jener Teile ihrer Netzwerke setzen, die sie zur Erbringung ihrer wesentlichen und digitalen Dienste nutzten.

Die augenfälligste Änderung aber, die die NIS-2-RL mit sich bringt, liegt im maßgeblich verschärften Sanktionsregime.[57] Während die NIS-1-RL die Festsetzung des Strafrahmens noch den Mitgliedstaaten überließ, weswegen der österreichische Gesetzgeber im NISG einen Strafrahmen von 50.000 Euro vorsehen konnte, setzt die NIS-2-RL nunmehr selbst auf Millionen- bzw Milliardenstrafen (10 sowie 7 Mio Euro bzw 2 sowie 1,4% des weltweiten Konzernumsatzes). Zu den drakonischen Geldbußen tritt künftig zudem eine Verantwortlichkeit bzw Haftung von Leitungsorganen sowie Leitungspersonen, die im äußersten Fall in Tätigkeitsverboten münden kann. Gemeinsam mit dem ausgeweiteten Anwendungsbereich wird das verschärfte Sanktionsregime dafür Sorge tragen, dass Cybersicherheit im unternehmerischen Alltag ab sofort eine weit größere Rolle spielen wird, als bisher.

52 Vgl Kipker, EuZW 2023, 249.
53 Siehe dazu im Detail unter 5.
54 Vgl Erwägungsgrund 6 NIS-2-RL; siehe weiters Kipker, EuZW 2023, 249; Wegmann, BB 2023, 835.
55 Siehe dazu im Detail unter 6.
56 Siehe dazu im Detail unter 6.2.
57 Siehe dazu im Detail unter 7.

5. Der erweiterte Anwendungsbereich der NIS-2-RL

5.1. Cybersicherheit: Vom Nischenthema zur „Chefsache"[58]

Dafür, dass der NIS-2-RL bzw den einschlägigen Umsetzungsbestimmungen im Vergleich zum Cybersicherheitsrecht der NIS-1-RL gesteigerte Bedeutung für die Unternehmenspraxis zukommen wird, zeichnet neben dem deutlich verschärften Strafregime[59] vor allem der erweiterte Anwendungsbereich der Richtlinie verantwortlich. Unterfielen nach der NIS-1-RL bloß Betreiber kritischer Infrastruktur und Anbieter bestimmter digitaler Dienste dem Cybersicherheits-Regime der EU,[60] erweitert die NIS-2-RL zum einen die Zahl kritischer Sektoren von 7 auf 11, wie künftig als Novum zum anderen auch bestimmte Unternehmen (bzw Einrichtungen) in Branchen mit erhöhter Kritikalität unter NIS-2 fallen.[61]

Des Weiteren beseitig die NIS-2-RL auch die Befugnis der Mitgliedstaaten, die zur Bestimmung des Anwendungsbereichs maßgeblichen Schwellenwerte für die Unternehmensgröße selbst festzulegen.[62] Diese Kompetenz der Mitgliedstaaten war mit ein Grund für das mitgliedstaatliche Umsetzungsdefizit der NIS-1-RL gewesen.

Im Ergebnis führt die Erweiterung des Anwendungsbereichs der NIS-2-RL dazu, dass Cybersicherheit zur *„Chefsache"* wird. Denn dem NIS-Cybersicherheitsregime unterliegen künftig nicht mehr bloß ein kleiner Kreis von kritischen Infrastrukturbetreibern, sondern weite Teile der Wertschöpfungskette in der Union. Für eine erhebliche Zahl von Unternehmen rückt Cybersicherheits-Compliance aufgrund der NIS-2-RL nunmehr in den Fokus.

5.2. Erfasste Einrichtungen

5.2.1. Kumulative Voraussetzungen

Die NIS-2-RL legt ihren grundsätzlichen Anwendungsbereich in Artikel 2 Absatz 1 leg cit fest.[63] Gemäß der Bestimmung kommt die Richtlinie für *„öffentliche oder private Einrichtungen"* zur Anwendung, sofern diese kumulativ die folgenden Voraussetzungen erfüllen:

a) Es handelt sich um öffentliche oder private Einrichtungen der in den Anhängen I oder II zur NIS-2-RL genannten Art.
b) Im Falle von Unternehmen handelt es sich zumindest um „mittlere Unternehmen" im Sinne der Kommissions-Empfehlung 2003/361/EG (iwF: KMU-Empfehlung).
c) Die öffentliche oder private Einrichtung erbringt ihre Dienste in der Union oder übt ihre Tätigkeit dort aus.

Fehlt es an einer (oder mehreren) der Voraussetzungen, unterfällt die betreffende Einrichtung der NIS-2-RL grundsätzlich nicht. Dies gilt ausnahmsweise nicht für das Größenkriterium im Sinne der KMU-Empfehlung, das durch die spezifische Kritikalität der Einrichtung (Artikel 2 Absätze 2-4 NIS-2-RL) ersetzt werden kann.[64]

Die in Artikel 3 NIS-2-RL getroffene Unterscheidung zwischen „wesentlichen" und „wichtigen" Einrichtungen hat – anders als dem ersten Anschein nach – hinsichtlich des Anwendungsbereichs der unternehmensbezogenen Pflichten der NIS-2-RL keine besondere Relevanz.[65] Der Unterschied zwischen „wesentlichen" und „wichtigen" Einrichtungen besteht vor allem darin, dass erstere im Vergleich zu letzteren einer wesentlich strengeren behördlichen Aufsicht unterworfen werden. Für „wesentliche" Einrichtungen sieht Artikel 32 NIS-2-RL eine laufende behördliche Überwachung vor;

58 Kipker, EuZW 2023, 249.
59 Dazu näher unter 7.
60 Dazu bereits unter 3; weiters etwa Kristoferitsch/Lachmayer, ecolex 2020, 74 ff.
61 Siehe dazu im Detail sogleich unter 5.2.2.
62 Siehe Rath/Ekardt/Schiela, MMR 2023, 86.
63 Zu den Bereichsfestlegungen der Anwendung in Artikel 2 Absätze 2-4 NIS-2-RL siehe sogleich unter 5.4.
64 Siehe dazu sogleich unter 5.4.
65 Wesentliche und wichtige Einrichtungen unterliegen grundsätzlich denselben Verpflichtungen. Siehe Artikel 20 ff NIS-2-RL.

„wichtige" Einrichtung unterliegen hingegen bloß einer nachträglichen (*ex post*-) Kontrolle *(„nachträgliche[…] Aufsichtsmaßnahmen")*.[66]

5.2.2. Einrichtungen im Sinne der Anhänge I und II der NIS-2-RL

Um den Anwendungsbereich der NIS-2-RL für eine Einrichtung zu begründen, bedarf es zunächst ihrer Qualifikation als Einrichtung im Sinne der Anhänge I oder II zur NIS-2-RL. Anhang I zählt dabei unterschiedliche *„Sektoren mit hoher Kritikalität"* auf und baut damit im Wesentlichen auf der aus der NIS-1-RL bekannten Liste von *„Betreiber[n] wesentlicher Dienste" (Anhang II zur NIS-1-RL) auf – mit teilweisen Ergänzungen* durch die NIS-2-RL. Im Ergebnis können folgende Sektoren (mitsamt Teilsektoren) den Anwendungsbereich des NIS-2-Cybersicherheitsrechts begründen, wobei Anhang I die spezifischen in die Richtlinie fallenden Arten der Einrichtung innerhalb der einzelnen Sektoren konkretisierend anführt:

- Energie (Nummer 1 Anhang I zur NIS-2-RL)
  - Elektrizität
  - Fernwärme und –kälte
  - Erdöl
  - Erdgas
  - Wasserstoff
- Verkehr (Nummer 2 Anhang I zur NIS-2-RL)
  - Luftverkehr
  - Schienenverkehr
  - Schifffahrt
  - Straßenverkehr
- Bankwesen (Nummer 3 Anhang I zur NIS-2-RL)
- Finanzmarktinfrastrukturen (Nummer 4 Anhang I zur NIS-2-RL)
- Gesundheitswesen (Nummer 5 Anhang I zur NIS-2-RL)
- Trinkwasser (Nummer 6 Anhang I zur NIS-2-RL)
- Abwasser (Nummer 7 Anhang I zur NIS-2-RL)
- Digitale Infrastruktur (Nummer 8 Anhang I zur NIS-2-RL)
- Verwaltung von IKT-Diensten (Business-to-Business) (Nummer 9 Anhang I zur NIS-2-RL)
- Öffentliche Verwaltung (Nummer 10 Anhang I zur NIS-2-RL)
- Weltraum (Nummer 11 Anhang I zur NIS-2-RL)

In Anhang II zur NIS-2-RL findet sich im Anschluss eine Liste der *„sonstige[n] kritische[n] Sektoren"*, die eine wesentliche Neuerung im Vergleich zur NIS-1-RL darstellt. Wiederum werden Sektoren, Teilsektoren sowie die spezifische Art der Einrichtung angeführt, die den Anwendungsbereich des Cybersicherheitsrechts begründen:

- Post- und Kurierdienste (Nummer 1 Anhang II zur NIS-2-RL)
- Abfallbewirtschaftung (Nummer 2 Anhang II zur NIS-2-RL)
- Produktion, Herstellung und Handel mit chemischen Stoffen (Nummer 3 Anhang II zur NIS-2-RL)
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln (Nummer 4 Anhang II zur NIS-2-RL)
- Verarbeitendes Gewerbe/Herstellung von Waren (Nummer 5 Anhang II zur NIS-2-RL)
  - Herstellung von Medizinprodukten und In-vitro-Diagnostika
  - Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
  - Herstellung von elektrischen Ausrüstungen
  - Maschinenbau
  - Herstellung von Kraftwagen und Kraftwagenteilen
  - sonstiger Fahrzeugbau
- Anbieter digitaler Dienste (Nummer 6 Anhang II zur NIS-2-RL)
- Forschung (Nummer 7 Anhang II zur NIS-2-RL)

Insgesamt erweist sich der Kreis der einbezogenen Sektoren und Branchen damit im Vergleich zur NIS-1-RL deutlich erweitert. Vor allem durch die Einbeziehung eines erheblichen Teils der produzierenden Industrie (chemische Stoffe,[67] Lebensmittel,[68] elektrotechnische Industrie,[69] etc), aber etwa auch des Telekommunikationssektors,[70] betrifft das unionale Cybersicherheitsrecht künftig nicht nur wenige, ausgewählte Betreiber kritischer Infrastruktur, sondern weite Teile der Wirtschaft in den Mitgliedstaaten.[71]

66 Artikel 33 NIS-2-RL.
67 Nummer 3 Anhang II NIS-2-RL.
68 Nummer 4 Anhang II NIS-2-RL.
69 Nummer 5 Anhang II NIS-2-RL.
70 Siehe Nummer 8 Anhang I NIS-2-RL.
71 Kipker, EuZW 2023, 249.

5.2.3. Überschreitung Schwellenwerte KMU-Empfehlung

Die Qualifikation als Einrichtung im Sinne der Anhänge I oder II der NIS-2-RL alleine genügt für die Begründung des Anwendungsbereichs der Richtlinie allerdings nicht. Im Falle von Unternehmen ist gemäß Artikel 2 Absatz 1 NIS-2-RL zusätzlich erforderlich, dass es sich dabei zumindest um „mittlere Unternehmen" im Sinne der KMU-Empfehlung der Europäischen Kommission handelt. Im Umkehrschluss bedeutet dies, dass all jene Unternehmen, die im Sinne der Empfehlung als Klein- und Kleinstunternehmen zu qualifizieren sind, grundsätzlich[72] nicht in den Anwendungsbereich der NIS-2-RL fallen. „Mittlere Unternehmen" zeichnen sich gemäß Artikel 2 Absatz 1 und 2 der KMU-Empfehlung durch eine der folgenden Eigenschaften aus:

- ➔ Das Unternehmen beschäftigt zumindest 50 Mitarbeiter.
- ➔ Der Jahresumsatz bzw die Jahresbilanz des Unternehmens übersteigt 10 Mio Euro.

Bezüglich der in Nummer 10 Anhang I NIS-2-RL genannten „Einrichtungen der öffentlichen Verwaltung" spielen die Unternehmens-Schwellenwerte der KMU-Empfehlung der Kommission für die Eröffnung des Anwendungsbereichs der NIS-2-RL naheliegenderweise keine Rolle; sie werden deswegen gemäß Artikel 2 Absatz 2 littera f NIS-2-RL *„[u]nabhängig von der Größe der Einrichtung […]"* in den Anwendungsbereich der Richtlinie einbezogen. Anderes gilt entgegen dem ersten Anschein für die in Anhang II Nummer 7 NIS-2-RL erwähnten *„Forschungseinrichtungen"*. Bei diesen handelt es sich gemäß der Legaldefinition des Artikel 6 Nummer 41 NIS-2-RL nur um jene Forschungseinrichtungen, *„deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen"*. *„Bildungseinrichtungen"* – und damit insbesondere die öffentlichen Universitäten – werden explizit ausgeschlossen. *„Forschungseinrichtungen"* im Sinne der NIS-2-RL erfüllen damit die Definition des „Unternehmens" der KMU-Empfehlung (Einheiten, die eine wirtschaftliche Tätigkeit ausüben)[73] und können folglich an ihren Schwellenwerten gemessen werden.

5.2.4. Unionsbezug der Tätigkeit

Als letzte Voraussetzung erfordert die Anwendbarkeit der NIS-2-RL auf betreffende Einrichtungen, dass diese *„ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben"*. Während das Kriterium des Unionsbezuges der Tätigkeit bei Bestehen einer Niederlassung in der Union unproblematisch ist – in diesem Fall werden zumindest die *„Tätigkeiten dort aus[ge]üb[t]"* – bedarf das Tatbestandsmerkmal der „Erbringung der Dienste in der Union" näherer Erläuterung.

Diese liefert die NIS-2-RL in ihrem Erwägungsgrund 116. Demnach hängt die Frage, ob eine Einrichtung Dienste in der Union anbietet, von einer entsprechenden Absicht der Einrichtung ab. Erwägungsgrund 116 NIS-2-RL betont dabei, dass die *„bloße Zugänglichkeit der Website einer Einrichtung oder eines Vermittlers von der Union aus oder einer E-Mail-Adresse oder anderer Kontaktdaten […] zur Feststellung einer solchen Absicht ebenso wenig als ausreichend betrachtet werden wie die Verwendung einer Sprache, die in dem Drittland, in dem die Einrichtung niedergelassen ist, allgemein gebräuchlich ist"*. Eine entsprechende Absicht kann aber das Vorliegen von unterschiedlichen Faktoren, *„wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Dienste in dieser Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern in der Union"*, indizieren.

Zusammenfassend lässt sich festhalten, dass der Anwendungsbereich der NIS-2-RL mangels Unionsbezugs stets dann nicht eröffnet sein wird, wenn der einzige Bezug zur Union darin besteht, dass der Internetauftritt des Unternehmens aus den Mitgliedstaaten aufgerufen werden kann. Bei englischsprachigen Websites wird im Detail zu prüfen sein, ob eine entsprechende Ausrichtung auf Kunden bzw Nutzer in der Union vorliegt, oder nicht.[74]

72 Siehe in diesem Zusammenhang aber die größenunabhängige Einbeziehung von Einrichtungen aufgrund ihrer spezifischen Kritikalität gemäß Artikel 2 Absätze 2-4 NIS-2-RL. Dazu unter 5.4.

73 Siehe Artikel 1 des Anhangs der KMU-Empfehlung sowie Erwägungsgrund 3 KMU-Empfehlung.

74 Vgl idZ zum räumlichen Anwendungsbereich der DSGVO, Leissler/Wolfbauer in Knyrim, DatKomm Art 3 DSGVO

5.3. Ausgenommene Einrichtungen

Jene *„öffentliche[n] oder private[n] Einrichtungen"*, die von der NIS-2-RL ausgenommen sind, ergeben sich nach dem bisher Ausgeführten im Umkehrschluss aus Artikel 2 Absatz 1 NIS-2-RL. Sofern Einrichtungen entweder keiner der in Anhang I oder II zur NIS-2-RL angeführten Tätigkeit nachgehen,[75] sie als Klein- oder Kleinstunternehmen die Schwellenwerte der Kommissionsempfehlung 2003/361/EG (KMU-Empfehlung) nicht überschreiten[76] oder sie ihre Dienste nicht in der Union erbringen oder ihre Tätigkeiten dort nicht ausüben,[77] findet die NIS-2-RL auf sie keine Anwendung.

Aufgrund der erheblichen Ausweitung des Anwendungsbereichs der NIS-2-RL, die sich mit aller Deutlichkeit an der Einbeziehung von in *„Produktion, Verarbeitung und Vertrieb von Lebensmitteln"*[78] tätigen Einrichtungen oder den Einrichtungen des *„[v]erarbeitende[n] Gewerbe[s]/Herstellung von Waren"*[79] zeigt – womit die NIS-2-RL künftig weite Teile der Wirtschaft in den Mitgliedstaaten umfasst[80] –, wird eine Ausnahme vom Pflichtenregime der Richtlinie in Zukunft vor allem über die Klein- und Kleinstunternehmerausnahme zu bewerkstelligen sein. Angesichts der beträchtlichen Kosten, die für Unternehmen mit der Implementierung von Cybersicherheits-Compliancemaßnahmen im Sinne der NIS-2-RL einhergehen und angesichts des Umstandes, dass ein Ausfall von Klein- und Kleinstunternehmen in systemischer Hinsicht weitestgehend vernachlässigbar ist,[81] entbindet die Richtlinie Klein- und Kleinstunternehmen von ihren Cybersicherheitspflichten. Von der NIS-2-RL sind Unternehmen als Klein- und Kleinstunternehmen im Sinne der KMU-Empfehlung immer dann ausgenommen, wenn sie kumulativ

a) weniger als 50 Mitarbeiter beschäftigen
b) und ihr Jahresumsatz bzw ihre Jahresbilanz 10 Mio Euro nicht übersteigt.

Sofern Klein- und Kleinstunternehmen aber – dazu sogleich – dennoch in den Anwendungsbereich der NIS-2-RL fallen, sollen die daraus resultierenden Belastungen nach dem Willen des Unionsgesetzgebers zumindest abgefedert werden. Gemäß Erwägungsgrund 20 NIS-2-RL soll die Kommission *„dafür sorgen, dass Kleinstunternehmen und Kleinunternehmen, die in den Anwendungsbereich dieser Richtlinie fallen, eine angemessene Anleitung erhalten"*. Erwägungsgrund 56 verlangt von den Mitgliedstaaten, *„mittels ihrer nationalen Cybersicherheitsstrategien kleine und mittlere Unternehmen dabei [zu] unterstützen, die Herausforderungen in ihren Lieferketten zu bewältigen"*. *Die Mitgliedstaaten sollen weiters „über eine Kontaktstelle für kleine und mittlere Unternehmen auf nationaler oder regionaler Ebene verfügen, die kleinen und mittleren Unternehmen entweder Leitlinien und Unterstützung bietet oder sie an die geeigneten Stellen für Leitlinien und Unterstützung in Fragen im Zusammenhang mit der Cybersicherheit weiterleitet". Zur Entlastung sollen „Kleinstunternehmen und kleinen Unternehmen, die nicht über diese Fähigkeiten verfügen, Dienste wie die Konfiguration von Websites und die Aktivierung der Protokollierung" durch Einrichtungen der Mitgliedstaaten angeboten werden.*

5.4. Gegenausnahme – Einbeziehung ohne Rücksicht auf Größe der Einrichtung

Von der Ausnahme für Klein- und Kleinstunternehmen besteht sodann aber wiederum eine gewichtige Gegenausnahme: Sofern Klein- und Kleinstunternehmen aufgrund der Sensibilität der ausgeübten Tätigkeit eben doch ein systemisches Risiko darstellen, bringt die NIS-2-RL ihr Pflichtenprogramm unabhängig von der Größe der betreffenden Einrichtung zur Anwendung; die maßgeblichen Bestimmungen finden sich in Artikel 2 Absätze 2-4 NIS-2-RL.

Gemäß Artikel 2 Absatz 2 NIS-2-RL gilt die Richtlinie zunächst *„[u]nabhängig von der Größe der*

75 Dazu bereits oben unter 5.2.2.
76 Dazu bereits oben unter 5.2.3.
77 Dazu bereits oben unter 5.2.4.
78 Nummer 4 Anhang II zur NIS-2-RL.
79 Nummer 5 Anhang II zur NIS-2-RL.
80 Siehe nur Kipker, EuZW 2023, 249.
81 Diese Ratio der Ausnahme von Klein- und Kleinstunternehmen zeigt sich daran, dass gemäß Artikel 2 Absatz 2 NIS-2-RL bestimmte, besonders kritische Unternehmen unabhängig von der Größe einbezogen werden.

Einrichtungen […] auch für Einrichtungen der in den Anhang I oder II genannten Art, wenn"

c) *„die Dienste erbracht werden von:*
   iv) Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten;
   v) Vertrauensdiensteanbietern;
   vi) Namenregistern der Domäne oberster Stufe und Domänennamensystem-Diensteanbietern;

a) *es sich bei der Einrichtung in einem Mitgliedstaat um den einzigen Anbieter eines Dienstes handelt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist;*

b) *sich eine Störung des von der Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;*

c) *eine Störung des von der Einrichtung erbrachten Dienstes zu einem wesentlichen Systemrisiko führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;*

d) *die Einrichtung aufgrund der besonderen Bedeutung, die sie auf nationaler oder regionaler Ebene für den betreffenden Sektor oder die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren in dem Mitgliedstaat hat, kritisch ist.* "[82]

Sind Einrichtungen damit für das Funktionieren gesellschaftlicher oder wirtschaftlicher Prozesse essenziell (*argumentum*: *„einzige[r] Anbieter eines Dienstes*", *„für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich*"), unterliegen sie selbst dann dem NIS-2-Regime, wenn es sich um Klein- oder Kleinstunternehmen handelt. Für die betroffenen Einrichtungen ist die Anordnung des Artikel 2 Absatz 2 NIS-2-RL naheliegenderweise mit erheblichen Unsicherheiten belastet. Während die grundsätzliche Koppelung des NIS-2-Anwendungsbereichs an die Größenschwellen der KMU Empfehlung[83] für Unternehmen in den Sektoren der Anhänge I und II NIS-2-RL die Sicherheit einfach und eigenständig ermittelbarer Kriterien bietet,[84] lässt sich der Anwendungsbereich gemäß Artikel 2 Absatz 2 NIS-2-RL von Klein- und Kleinstunternehmen kaum selbst einschätzen. Abhilfe könnten Leitlinien der Kommission schaffen, die gemäß Erwägungsgrund 20 NIS-2-RL dem Zweck dienen sollen, die *„Anwendung der für Kleinstunternehmen und kleine Unternehmen geltenden Kriterien bereit[zu]stellen, um zu bewerten, ob sie in den Anwendungsbereich dieser Richtlinie fallen*".

Fraglich ist, ob aus Artikel 3 Absatz 1 littera e NIS-2-RL eine Vorgabe an die Mitgliedstaaten folgt, den Anwendungsbereich des NIS-2-Cybersicherheitsrechts in den Fällen des Artikel 2 Absatz 2 littera b-e NIS-2-RL im Sinne eines „State driven Approach"[85] mittels Hoheitsakts vorzunehmen. Dies aufgrund der etwas kryptischen Formulierung, wonach als „wichtige Einrichtungen" im Sinne der Richtlinie jene *„sonstige[n] Einrichtungen der in Anhang I oder II aufgeführten Art [gelten], die von einem Mitgliedstaat gemäß Artikel 2 Absatz 2 Buchstaben b bis e als wesentliche Einrichtungen eingestuft werden*" (*argumentum*: „Einstufen"). Eine derartige Einstufung sieht Artikel 2 Absatz 2 NIS-2-RL allerdings gar nicht vor; dieser bringt die Richtlinie vielmehr *ex lege* zur Anwendung (*argumentum*: *„Unabhängig von der Größe der Einrichtungen gilt*"). Klarheit hinsichtlich der Frage, wie dieser Normenkonflikt aufzulösen ist, wird wohl erst der EuGH bringen.

Die NIS-2-RL gilt zudem gemäß Artikel 2 Absatz 3 leg cit auch dann unabhängig von der Größe der Einrichtung, wenn es sich bei dem betreffenden Unternehmen um eine „kritische Einrichtung" im Sinne der CER-RL[86] handelt. Gemäß Artikel 2 Absatz 4 NIS-2-RL sind *„Einrichtungen, die Domänennamenregistrierungsdienste erbringen*", unabhängig von ihrer Größe in den Anwendungsbereich des unionalen Cybersicherheitsrechts einbezogen

82 Artikel 2 Absatz 2 littera f NIS-2-RL (Einrichtungen der öffentlichen Verwaltung) kann im gegebenen Zusammenhang aufgrund des Fokus auf Unternehmen außer Acht bleiben.

83 Siehe dazu bereits unter 5.2.3.

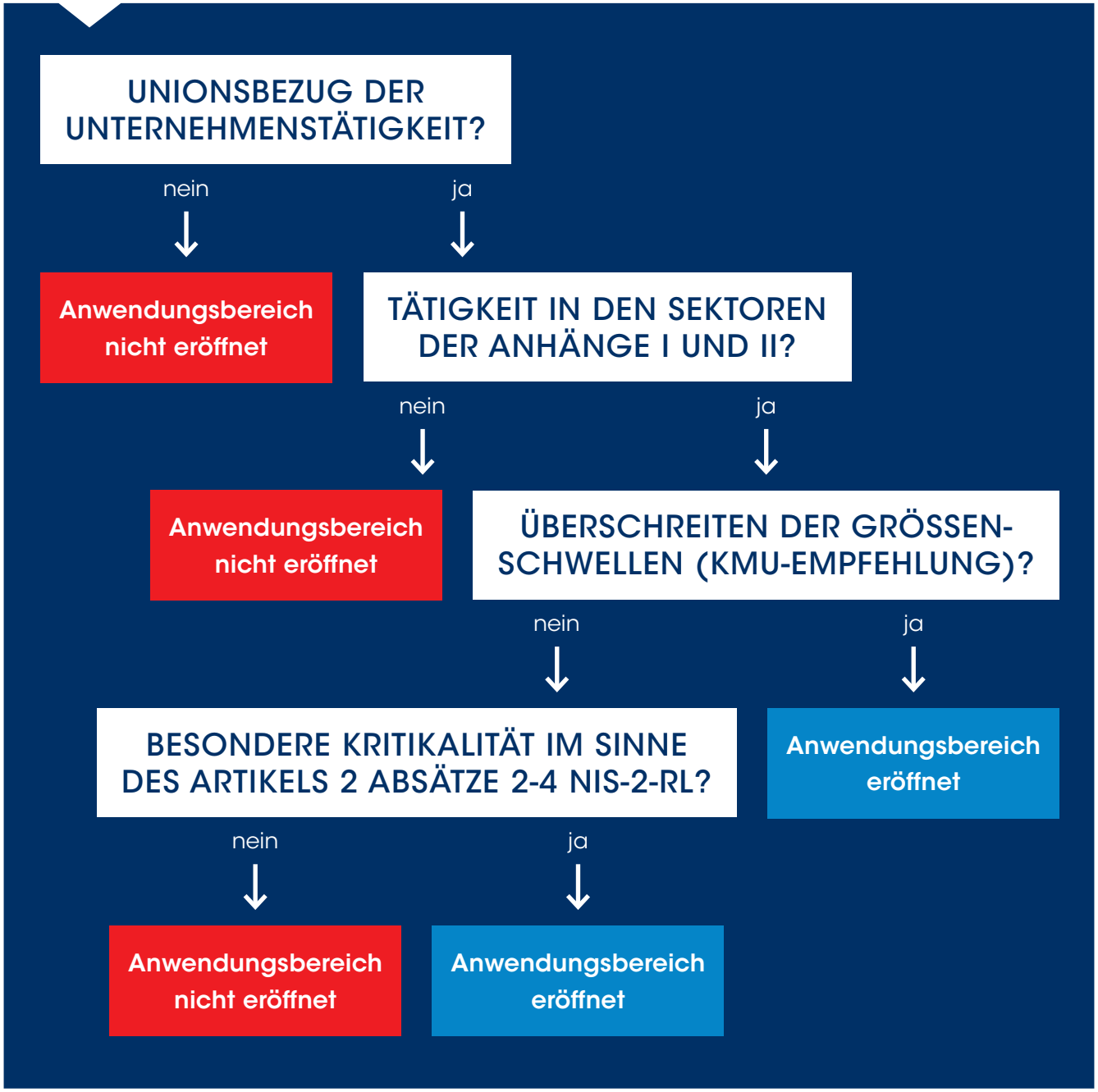
84 So auch Erwägungsgrund 7 NIS-2-RL.

85 Siehe dazu insbesondere unter 8.3.

86 RL 2022/2557/EU.

5.5. Prüfschema Anwendungsbereich

Vereinfachend lassen sich die Schritte zur Prüfung des Anwendungsbereiches der NIS-2-RL folgendermaßen grafisch veranschaulichen:



Beispiel 1

Ein kommunaler Tierkörperverwerter mit 30 Mitarbeitern und einem Jahresumsatz von 4 Mio Euro ist der einzige Tierkörperverwerter einer österreichischen Kleinstadt und der umliegenden Region. Da das Unternehmen seine Dienste im Sektor *„Abfallbewirtschaftung"* gemäß Nummer 2 Anhang II NIS-2-RL erbringt, würde es in den Anwendungsbereich der NIS-2-RL fallen. Allerdings unterschreitet das Unternehmen die Schwellenwerte der KMU-Empfehlung der Kommission (weniger als 50 Mitarbeiter und Jahresumsatz von weniger als 10 Mio Euro), weshalb es vom NIS-2-Regime grundsätzlich ausgenommen ist.
Das Unternehmen könnte aber wegen Artikel 2 Absatz 2 littera c NIS-2-RL dennoch in den Anwendungsbereich der NIS-2-RL fallen. Denn gemäß dieser Bestimmung gilt die Richtlinie *„[u]nabhängig von der Größe der Einrichtungen […] auch für Einrichtungen der in den Anhang I oder II genannten Art"*, wenn *„sich eine Störung des von der Einrichtung erbrachten Dienstes wesentlich auf […] die öffentliche Gesundheit auswirken könnte"*. Sofern ein Ausfall des kommunalen Tierkörperverwerters etwa dazu führt, dass Kadaver nicht mehr rechtzeitig abgeholt werden und deswegen gesundheitliche Risiken (Seuchengefahr) drohen, fällt der kommunale Tierkörperverwerter trotz Unterschreitens der Größenschwellen der KMU-Empfehlung in den Anwendungsbereich der NIS-2-RL.

Beispiel 2

Ein britischer Vertrauensdiensteanbieter betreibt eine englischsprachige Website. Das Unternehmen erbringt seine Dienste ausschließlich in Großbritannien und ist in keinem einzigen Mitgliedstaat der Union als Vertrauensdiensteanbieter zertifiziert.
Das Unternehmen fällt nicht in den Anwendungsbereich der NIS-2-RL, weil es seine Dienste nicht in der Union erbringt und dort auch keine Tätigkeit ausübt (siehe Artikel 2 Absatz 1 NIS-2-RL). Der Umstand, dass der Vertrauensdiensteanbieter über eine Website in englischer Sprache verfügt, die vom Unionsgebiet aus abgerufen werden kann, ist irrelevant.

5.6. Zwischenresümee

Der Anwendungsbereich der NIS-2-RL zeigt sich gegenüber der NIS-1-RL deutlich ausgeweitet und wartet mit einem etwas diffizilen Ausnahme-Gegenausnahme-Modell auf. Die Liste kritischer Infrastrukturbetreiber wächst von 7 auf 11 Sektoren und es werden künftig auch Unternehmen in Branchen mit erhöhter Sensibilität wie der *„Produktion, [der] Herstellung und [des] Handel[s] mit chemischen Stoffen"* oder der *„Produktion, [der] Verarbeitung und [des] Vertrieb[s] von Lebensmitteln"* in den Anwendungsbereich des NIS-2-Regimes einbezogen.

Für betroffene Unternehmen bringen vor allem die zum Teil größenunabhängigen Anwendungsbereichsfestlegungen erhebliche Unsicherheiten mit sich. Abzuwarten bleibt, ob hier Kommissionsleitlinien oder gar entsprechende Regelungen in den Umsetzungsgesetzen Abhilfe schaffen werden.

Positiv erweist sich in diesem Zusammenhang aber, dass der Anwendungsbereich des Cybersicherheitsrechts der Union durch Verweis auf die Schwellenwerte der KMU-Empfehlung in der NIS-2-RL endlich unionsweit einheitlich festgelegt ist. Für grenzüberschreitend tätige Unternehmen besteht damit künftig unabhängig vom jeweiligen Mitgliedstaat weitestgehend Klarheit darüber, ob sie in den Anwendungsbereich des NIS-2-Regimes fallen oder eben nicht.[87]

87 So auch Erwägungsgrund 7 NIS-2-RL.

6. Die unternehmensbezogenen Pflichten der NIS 2-RL

6.1. Allgemeines

Die Qualifikation eines Unternehmens als „wesentliche" oder „wichtige" Einrichtung,[88] somit die Eröffnung des Anwendungsbereichs der NIS-2-RL, zeitigt für dieses erhebliche Auswirkungen. So geht die Europäische 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 werden müssen; sofern bereits die Vorgaben der NIS-1-RL erfüllt wurden, ist zumindest nur mit einer notwendigen Erhöhung von rund 12 % zu rechnen.[89]

Für ein Unternehmen, das in den Anwendungsbereich der NIS-2-RL fällt, bedeutet dieser Umstand damit eine erhebliche finanzielle Mehrbelastung. Die Investition in die Cybersicherheits-Compliance – und damit die Erfüllung der im folgenden Abschnitt behandelten NIS-2-Pflichten – ist dabei aber durchaus sinnvoll. Im Falle von Verstößen drohen empfindliche Strafen,[90] wie auch eine persönliche Verantwortlichkeit der „Leitungsorgane",[91] die im äußersten Fall sogar Tätigkeitsverbote[92] umfassen kann.

Anders als es die in Artikel 3 NIS-2-RL enthaltene Differenzierung zwischen „wesentlichen Einrichtungen" und „wichtigen Einrichtungen" nahelegen würde, resultiert die Unterscheidung grundsätzlich nicht in Unterschieden hinsichtlich des Pflichtenprogramms. Die Verpflichtung zur Setzung von *„Risi*komanagementmaßnahmen im Bereich der Cybersicherheit" gemäß Artikel 21 NIS-2-RL wie auch die „Berichtspflichten" gemäß Artikel 23 NIS-2-RL treffen wesentliche und wichtige Einrichtungen gleichermaßen.[93]

Das bedeutet allerdings nicht, dass die Cybersicherheits-Compliance im Sinne der NIS-2-RL in sämtlichen erfassten Einrichtungen die gleichen Maßnahmen umfassen wird. Die – nicht zuletzt auch grundrechtlich gebotene[94] – Feinsteuerung erfolgt in der NIS-2-RL allerdings nicht über pauschal differenzierte Pflichtenbereiche, sondern wird auf andere Weise, über die Verhältnismäßigkeitsklausel des Artikel 21 Absatz 1 NIS-2-RL, besorgt. Sämtliche „wesentliche und wichtige Einrichtungen" mögen folglich zwar unabhängig von Größe und Art der Tätigkeit denselben Pflichten unterliegen, die Intensität des Pflichtenprogrammes unterscheidet sich aber unter Umständen erheblich.

6.2. Vom spezifischen zum umfassenden Netzwerkschutz

Eine wesentliche Neuerung der NIS-2-RL im Vergleich zur NIS-1-RL ist, dass sich der Netzwerkschutz, zu dem wesentliche und wichtige Einrichtungen verpflichtet werden, von einem spezifischen zu einem umfassenden Netzwerkschutz wandelt:

Die NIS-1-RL sieht gegenwärtig vor, dass von ihrem Anwendungsbereich erfasste Einrichtungen Netz- und Informationssysteme nur insoweit schützen müssen, als diese bei der Erbringung von kritischen Diensten zum Einsatz kommen. Dies ergibt sich aus Artikel 14 und 16 in Verbindung mit Erwägungsgrund 22 NIS-1-RL. *„Betreiber wesentlicher Dienste sollten den spezifischen Si-*

88 Im Folgenden werden die Begriffe der „wesentlichen und wichtigen Einrichtung" sowie des „Unternehmens" synonym verwendet. Unternehmen fallen nur insofern in den Anwendungsbereich der NIS-2-RL, als man sie als „wesentliche" oder „wichtige" Einrichtung qualifiziert (siehe zum Anwendungsbereich der NIS-2-RL oben unter 5.). Aus der Brille des NIS-2-Cybersicherheitsrechts sind Unternehmen folglich nur sichtbar, sofern sie zugleich „wesentliche" oder „wichtige" Einrichtung sind, weswegen sich die Begriffe für die Zwecke der gegenständlichen Ausführungen als austauschbar erweisen.

89 Siehe das Commission Staff Working Document SWD(2020) 344 final: *„For the companies that would fall under the scope of the NIS framework, it is estimated that they would need an increase of maximum 22% of their current ICT security spending for the first years following the introduction of the new NIS framework (this would be 12% for companies already under the scope of the current NIS Directive)"*.

90 Siehe zu den Geldbußen der NIS-2-RL unter 7.2.

91 Siehe zum Begriff des „Leitungsorgans" der NIS-2-RL unter 7.3.

92 Siehe dazu unter 7.4.

93 Die Differenzierung zeitigt ihre wesentlichen Folgen in Bezug auf die behördliche Kontrolle: Während „wesentliche Einrichtungen" gemäß Artikel 32 NIS-2-RL einer laufenden behördlichen Aufsicht unterliegen, beschränkt sich die Tätigkeit der Behörde hinsichtlich „wichtiger Einrichtungen" gemäß Artikel 33 NIS-2-RL auf die Setzung *„nachträgliche[r] Aufsichtsmaßnahmen"*.

94 Siehe nur Artikel 16 GRC.

cherheitsanforderungen nur in Bezug auf die als wesentlich geltenden Dienste unterworfen sein. "[95]

In Beachtung dieser Vorgabe der NIS-1-RL schränkte der österreichische Gesetzgeber die Verpflichtung zur Setzung von Cybersicherheitsmaßnahmen deswegen auch entsprechend ein. Gemäß § 17 NISG haben Betreiber wesentlicher Dienste derzeit nur in Hinblick auf jene Netz- und Informationssysteme *„geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen"* zu treffen, *„die sie für die Bereitstellung des wesentlichen Dienstes nutzen"*. Die dem NISG unterliegenden Einrichtungen *„müssen daher nur in Bezug auf die […] als wesentlich bestimmten Dienste, inkl der dazugehörigen Prozesse, von denen der wesentliche Dienst abhängig ist bzw die diesen unterstützen, die spezifischen Sicherheitsanforderungen erbringen"*.[96]

Die NIS-2-RL sieht eine Einschränkung der Sicherheitspflichten auf jene Netz- und Informationssysteme, die bei der Ausübung kritischer Tätigkeiten zum Einsatz kommen, nun nicht mehr vor. Gemäß Artikel 21 Absatz 1 NIS-2-RL haben wesentliche und wichtige Einrichtungen künftig geeignete Maßnahmen zu ergreifen, *„um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen"*, zu beherrschen.

Im Ergebnis läuft Artikel 21 Absatz 1 NIS-2-RL damit darauf hinaus, dass ein Unternehmen bzw eine Einrichtung, die in den Anwendungsbereich der Richtlinie fällt, sämtliche im Rahmen ihres Betriebes zum Einsatz kommende Netz- und Informationssysteme gegen Cyberangriffe absichern wird müssen. Diese Wende vom spezifischen zum umfassenden Netzwerkschutz erklärt sich letztlich mit der Erkenntnis des Unionsgesetzgebers, dass Cyberangriffe regelmäßig über Schwachstellen in der IT oder insbesondere in der OT erfolgen[97] und einer gewandelten Funktion des Cybersicherheitsrechts der Union. Stand die NIS-1-RL noch – ähnlich der CER-RL – eher im Zeichen der Gewährleistung der Funktion kritischer Infrastruktur, so hat sich der Unionsgesetzgeber seiner Digitalstrategie[98] entsprechend und der aktuellen Bedrohungslage Rechnung tragend mit der NIS-2-RL der umfassenden Cybersicherheit zugewandt. Da es für die Verwirklichung der Gefahr von Cyberangriffen letztlich unerheblich ist, über welche Schwachstelle der Einbruch ins System erfolgt, verlangt die NIS-2-RL künftig von einem erheblichen Teil der Unternehmen im Binnenmarkt,[99] ihre Netz- und Informationssysteme umfassend zu schützen.

6.3. Risikomanagementmaßnahmen

6.3.1 „Risk-based-Approach" (Verhältnismäßigkeit)

Wie erwähnt, unterliegen wesentliche und wichtige Einrichtungen den in Artikel 21 NIS-2-RL festgelegten *„Risikomanagementmaßnahmen im Bereich der Cybersicherheit"* unabhängig von ihrer Tätigkeit und Größe. Grundsätzlich sieht die NIS-2-RL damit ein einheitliches Pflichtenprogramm vor.

Es liegt auf der Hand, dass ein derartiges One-Size-Fits-All-Modell den unterschiedlichen Realitäten in den Unternehmen nicht ausreichend Rechnung tragen würde. Aus diesem Grund differenziert die NIS-2-RL dann doch die Verpflichtungen, die sie Unternehmen auferlegt – über die individuelle Verhältnismäßigkeitsklausel des Artikel 21 Absatz 1 NIS-2-RL.

Gemäß Artikel 21 Absatz 1 NIS-2-RL müssen wesentliche und wichtige Einrichtungen *„geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, 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 Pflichtenintensität bestimmt sich dabei gemäß Artikel 21 Absatz 1 Unterabsatz 2 NIS-2-RL anhand folgender Gesichtspunkte:

95 Erwägungsgrund 22 NIS-1-RL.
96 *Mayer* in Anderl et al, NISG § 17 NISG Rz 2 ff.
97 Vgl Erwägungsgrund 58 NIS-2-RL.
98 Vgl die Mitteilung der Kommission COM(2021) 118 final, Digitaler Kompass 2030: der europäische Weg in die digitale Dekade.
99 Siehe zum ausgeweiteten Anwendungsbereich der NIS-2-RL bereits unter 5.

- Was ist der Stand der Technik?
- Bestehen einschlägige sicherheitstechnische europäische und internationale Normen?
- Wie viel kostet die Umsetzung?
- Wie hoch ist das Risiko?
  - Ausmaß der Risikoexposition der Einrichtung
  - Größe der Einrichtung
  - Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen

Die Beurteilung des Umfanges der zu setzenden Risikomanagementmaßnahmen hat damit im Rahmen einer Verhältnismäßigkeitsprüfung zu erfolgen. Es ist eine ausgewogene Balance zwischen erzielbarem Sicherheitsniveau und dem der betreffenden Einrichtung zumutbaren Aufwand zu erzielen. Diesen Umstand spiegelt auch Erwägungsgrund 81 NIS-2-RL wider, wenn es dort heißt, dass *„die Risikomanagementmaßnahmen im Bereich der Cybersicherheit in einem angemessenen Verhältnis zu den Risiken stehen [müssen], denen das betreffende Netz- und Informationssystem ausgesetzt ist"*, um zu verhindern, dass *„unverhältnismäßige finanzielle und administrative Belastung[en]* für wesentliche und wichtige Einrichtungen" entstehen.

Mit anderen Worten: Je höher das Risiko eines Cyberangriffs und je bedeutender die betreffende Einrichtung für gesellschaftliche und wirtschaftliche Prozesse, desto umfangreicher werden die zu setzenden Maßnahmen sein; je höher das Gesamtrisiko, desto weniger kann die Realisation von Cybergefährdungslagen hingenommen werden. Umgekehrt dürfen die Anforderungen an Unternehmen, die gerade noch als „mittlere Unternehmen" im Sinne der KMU-Empfehlung[100] gelten und keine besondere Relevanz für das Funktionieren gesellschaftlicher und wirtschaftlicher Prozesse entfalten, nicht überzogen werden. Es macht eben einen Unterschied, ob der Energieversorger einer Großstadt wegen eines Cyberangriffs ausfällt, oder ein mittelständischer Lebensmittelhändler.

Die NIS-2-RL bedient sich für die Festlegung der konkret zu treffenden Risikomanagementmaßnahmen folglich eines „Risk-based-Approach"[101] und damit eines Regelungskonzepts, das Unternehmen bereits aus der DSGVO bekannt sein dürfte.[102] Auch die technischen und organisatorischen Maßnahmen (TOM), die Verantwortliche gemäß Artikel 32 DSGVO treffen müssen, richten sich nach den Realitäten des jeweiligen Datenverarbeiters sowie dem technisch Machbaren (Stand der Technik).[103] Jene Erfahrungen, die Unternehmen im Zusammenhang mit der DSGVO gewonnen haben, können als Grundlage für ihre Projekte der Cybersicherheits-Compliance herangezogen werden.

Beispiel

Ein österreichischer Obst- und Gemüsegroßhandel beschäftigt 800 Mitarbeiter und erzielt einen Jahresumsatz von 43 Mio Euro. Als Einrichtung im Sektor „Produktion, Verarbeitung und Vertrieb von Lebensmitteln" mit 50 oder mehr Mitarbeitern und einem Jahresumsatz von mehr als 10 Mio Euro fällt das Unternehmen gemäß Artikel 2 NIS-2-RL in Verbindung mit Nummer 4 Anhang II zur NIS-2-RL in Verbindung mit Artikel 3 Nummer 2 VO 178/2002/EU als „wichtige Einrichtung" in den Anwendungsbereich der Richtlinie.
Bei der Feststellung, welche „Risikomanagementmaßnahmen im Bereich der Cybersicherheit" gemäß Artikel 21 NIS-2-RL der Obst- und Gemüsegroßhandel konkret setzen muss, ist zum einen zu berücksichtigen, dass das Unternehmen – etwa verglichen mit einem Energieversorger, einem Trinkwasserversorger oder einer Fluglinie – ein geringes Cybersicherheitsrisiko aufweist. Zum anderen würde eine Betriebsschließung infolge eines Cyberangriffs weit geringere gesellschaftliche und wirtschaftliche Auswirkungen entfalten (eventuell kurzfristige Lieferschwierigkeiten bei Obst und Gemüse),

100 Siehe dazu bereits unter 5.2.3.

101 Siehe in diesem Zusammenhang zur NIS-1-RL bereits *Anderl/Müller/Pichler* in Paulus 189 f.

102 Siehe zum Umstand, dass aus DSGVO-Umsetzungsprojekten gewonnene Erfahrungen für die Implementierung der NIS-2-Cybersicherheitspflichten fruchtbar gemacht werden können, unter 9.

103 Dazu etwa *Bergauer* in Jahnel, DSGVO Art 32 DSGVO Rz 4 ff.

als ein Ausfall der genannten Energie- oder Trinkwasserversorger oder einer Fluglinie.
Im Ergebnis hat der Obst- und Gemüsegroßhandel damit zwar gewisse Risikomanagementmaßnahmen zu treffen. Die daraus folgende Gesamtbelastung für das Unternehmen muss allerdings im Hinblick auf das zu adressierende Cybersicherheits-Risiko verhältnismäßig sein.

6.3.2. Verweis auf den „Stand der Technik" und internationale Normen (Zertifizierung)

Im Kern führt die Festlegung des NIS-2-Pflichtenprogramms über den unbestimmten Rechtbegriff *„technische, operative und organisatorische Maßnahmen"* sowie die Verhältnismäßigkeitsklausel des Artikel 21 Absatz 1 NIS-2-RL zum einen zu einer Delegation der Maßnahmenbestimmung an IT-Experten. Zum anderen folgt daraus, dass sich die konkret zu treffenden Maßnahmen stetig ändern können (und auch werden), etwa durch das Hervorkommen neuer Cyberangriffs-Methoden oder Entwicklungen in der IT-Sicherheit.

Die Frage, welche konkreten Risikomanagementmaßnahmen wesentliche und wichtige Einrichtungen zu setzen haben, ist damit nur „formell" rechtlicher Provenienz. Materiell wird sie ganz regelmäßig von Industriestandards beantwortet.

Die NIS-2-RL trägt diesem Umstand dadurch Rechnung, dass sie den *„Stand[…] der Technik"* und die *„einschlägigen europäischen und internationalen Normen"* in Artikel 21 Absatz 1 Unterabsatz 2 NIS-2-RL als erste jener Abwägungskriterien anführt, die bei der Verhältnismäßigkeitsprüfung zu berücksichtigen sind. Bei den genannten *„einschlägigen europäischen und internationalen Normen"* für Cybersicherheit handelt es sich etwa um die Normen *„der Reihe ISO/IEC 27000"*, die Erwägungsgrund 79 NIS-2-RL auch explizit erwähnt.

Die Bedeutung von Industrienormen für die Feststellung, welche Risikomanagementmaßnahmen konkret zu treffen sind, kommt ebenso in Artikel 25 Absatz 1 NIS-2-RL zum Ausdruck. Dieser sieht vor, dass die Mitgliedstaaten *„ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer und internationaler Normen und technischer Spezifikationen für die Sicherheit von Netz- und Informationssystemen"* fördern, *„[u]m die einheitliche Anwendung des Artikels 21 Absätze 1 und 2"* über die Risikomanagementmaßnahmen zu gewährleisten.

Im Ergebnis werden wesentliche und wichtige Einrichtungen die Erfüllung der ihnen gemäß Artikel 21 NIS-2-RL obliegenden Pflichten zur Setzung von Risikomanagementmaßnahmen somit in aller Regel durch entsprechende Zertifizierungen nachweisen. Diese Funktion erfüllen Zertifizierungen bereits gegenwärtig; gemäß § 17 Absatz 3 NISG haben Betreiber wesentlicher Dienste die Erfüllung der NISG-Sicherheitspflichten alle drei Jahre nachzuweisen und übermitteln zu diesem Zweck *„eine Aufstellung der vorhandenen Sicherheitsvorkehrungen durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen"* an die Behörde. Die in diesem Zusammenhang *„oft getroffene[…] Vermutung"*, dass dazu eine Zertifizierung nach ISO/IEC 27001 *„per se"* ausreicht, bezweifelt die Literatur allerdings bereits für den Anwendungsbereich des NISG,[104] weshalb für die NIS-2-RL umso mehr infrage gestellt werden muss, ob wesentliche und wichtige Einrichtungen mit dieser Norm alleine das Auslangen finden.

6.3.3. Das „Pflichtprogramm" des Artikel 21 Absatz 2 NIS-2-RL

Da eine vollständige Delegation der Bestimmung der zu setzenden Risikomanagementmaßnahmen an IT-Experten durch Stand-der-Technik-Klauseln oder den Verweis auf internationale Normen und Standards rechtsstaatlich unzulässig wäre, legt die NIS-2-RL einige Risikomanagementmaßnahmen dann doch selbst fest. Auch wenn die von einer bestimmten Einrichtung konkret zu setzenden Maßnahmen im Rahmen der Abwägung gemäß Artikel 21 Absatz 1 NIS-2-RL zu ermitteln sind, müssen sich darunter gemäß Artikel 21 Absatz 2 NIS-2-RL zumindest folgende Maßnahmen finden:

➔ *„Konzepte in Bezug auf die Risikoanalyse und*

104 Mayer in Anderl et al, NISG § 17 NISG Rz 9.

Sicherheit für Informationssysteme" (Artikel 21 Absatz 2 littera a NIS-2-RL);
- ➔ *„Bewältigung von Sicherheitsvorfällen*" (Artikel 21 Absatz 2 littera b NIS-2-RL);
- ➔ *„Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement*" (Artikel 21 Absatz 2 littera c NIS-2-RL);
- ➔ *„Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern*" (Artikel 21 Absatz 2 littera d NIS-2-RL);
- ➔ *„Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen*" (Artikel 21 Absatz 2 littera e NIS-2-RL);
- ➔ *„Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit*" (Artikel 21 Absatz 2 littera f NIS-2-RL);
- ➔ *„grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit*" (Artikel 21 Absatz 2 littera g NIS-2-RL);
- ➔ *„Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung*" (Artikel 21 Absatz 2 littera h NIS-2-RL);
- ➔ *„Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen*" (Artikel 21 Absatz 2 littera i NIS-2-RL);
- ➔ *„Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung*" (Artikel 21 Absatz 2 littera j NIS-2-RL).

Alle gesetzten Risikomanagementmaßnahmen sollen nach der Intention des Unionsgesetzgebers auf einem *„gefahrenübergreifenden Ansatz*" beruhen, weil *„Gefahren für die Sicherheit von Netz- und Informationssystemen unterschiedliche Ursachen haben können*". Der sämtlichen Risikomanagementmaßnahmen zugrunde liegende gefahrenübergreifende Ansatz zielt darauf ab, *„Netz- und Informationssysteme und ihr physisches Umfeld vor Ereignissen wie Diebstahl, Feuer, Überschwemmungen und Telekommunikations- oder Stromausfällen oder vor unbefugtem physischen Zugang zu Informationen und Datenverarbeitungsanlagen […] und vor der Schädigung dieser Informationen und Anlagen […] zu schützen*".

Die Cybersicherheits-Risikomanagementmaßnahmen müssen deswegen stets auch die *„physische Sicherheit und die Sicherheit des Umfelds von Netz- und Informationssystemen berücksichtig[en][…], indem Maßnahmen zum Schutz dieser Systeme vor Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen*" gesetzt werden.[105]
Erwägungsgrund 79 NIS-2-RL betont ausdrücklich die Bedeutung, die Zertifizierungen gemäß internationalen Normen in diesem Zusammenhang zukommt (die betreffenden Maßnahmen sollen *„im Einklang mit europäischen und internationalen Normen, wie denen der Reihe ISO/IEC 27000*", gesetzt werden).

Der Kommission kommt gemäß Artikel 21 Absatz 5 NIS-2-RL die Kompetenz zu, mittels Durchführungsrechtsakten die *„technischen und methodischen Anforderungen*" an die in Artikel 21 Absatz 2 NIS-2-RL angeführten Maßnahmen festzulegen; *„in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter*" ist sie dazu sogar verpflichtet. Durch die Anordnung des Artikel 21 Absatz 5 Unterabsatz 3 NIS-2-RL, dass sich die Kommission bei der Ausarbeitung der *„genannten Durchführungsrechtsakte […] so weit wie möglich an europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen*" orientiert, wird der diesbezügliche Prozess zu einer zirkulären Determinierung führen.

Denn die Frage, welche europäischen und internationalen Normen einschlägig sind, bestimmt sich insbesondere anhand des Maßnahmenkataloges des Artikel 21 Absatz 2 NIS-2-RL. Jene Durchführungsrechtsakte, die den Maßnahmenkatalog näher ausgestalten, sollen aber umgekehrt wieder die einschlägigen Normen berück-

105 Erwägungsgrund 79 NIS-2-RL.

sichtigen. Aufgrund dieses Umstandes ist für den Zeitraum unmittelbar nach Geltungsbeginn des NIS-2-Regimes damit zu rechnen, dass sich ein abschließender Bestand an relevanten Normen und *Best-Practice*-Modellen erst schrittweise herauskristallisieren wird.

6.3.3.1. Es empfiehlt sich jetzt schon an konkrete Lösungen zu denken wie man als wesentliche oder wichtige Einrichtung diese Maßnahmen umsetzen zu gedenkt. CISCO Systems Austria kann bei der Umsetzung der zuvor genannten Maßnahmen Unterstützung leisten und bietet folgende Lösungen zu den jeweiligen Maßnahmen an:[106]

- *„Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme"*
  - Risikoanalyse, Risiko Priorisierung mit risikobasierten Vulnerability Management
  - Sicherheitsstrategie-, Risiko- und Compliance-Services
  - Beratungsworkshop für CISO
  - Software-Lebenszyklusentwicklung mit Security & Trust Office Abteilung
  - Netzwerksicherheit Referenz Architekturen
  - Schulungsmaßnahmen
  - Identitäts- und Zugriffsmanagement

- *„Bewältigung von Sicherheitsvorfällen"*
  - Vorbereitung auf eine Krise und Unterstützung während einer Krise
  - Threat modelling workshops
  - Managed Detection and Response Services
  - Security Operations Center, Software und Services

- *„Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement"*
  - Vorbereitung auf eine Krise und Unterstützung während einer Krise
  - Wiederherstellung der Infrastruktur nach einem Notfall

- *„Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern"*
  - Software-Inventarliste erstellen
  - Partnerschaft mit Ihrer Security & Trust Office Abteilung

- *„Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen"*
  - Bereitstellung von Dokumenten zu Sicherheit, Vertrauen, Datenschutz und Privatsphäre, einschließlich ISO-, SOC-Zertifizierungen und Compliance-Dokumente.
  - Schwachstellenforschung, Malware Erkennungs- und Präventionssysteme

- *„Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit"*
  - Risikoanalyse, Risiko Priorisierung mit risikobasierten Vulnerability Management
  - Sicherheitsstrategie-, Risiko- und Compliance-Services

- *„grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit"*
  - Vorbereitung auf eine Krise und Unterstützung während einer Krise
  - Threat modelling workshops
  - Schulungsmaßnahmen u.a. Security Awareness

- *„Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung"*
  - Verschlüsselung auf allen Ebenen des ISO/OSI Referenzmodells
  - Verschlüsselung in Lösungen zur gesicherten Sprach-, Video- und Textkommunikation

- *„Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen"*
  - Lösungen zu Video- Aufzeichnungen (CCTV) und deren Analyse
  - Lösungen zur Unterstützung des AAA-Frameworks (Authentifizierung, Autorisierung und Accounting)
  - Lösungen zu gesicherten Remote Zugriff auf OT-Equipment

106 Für eine detaillierte Aufschlüsselung wird auf das „NIS-2 Richtlinie Anforderungen erfüllen mit Cisco"-Security White Paper verwiesen, das als Appendix zu diesem White Paper verfasst wurde.

- ➔ *„Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung"*
  - ➔ Multifaktor Lösungen für Authentifizierung nach dem Zero Trust Prinzip
  - ➔ Lösungen zur Zusammenarbeit für eine gesicherte Sprach- Video- und Textkommunikation

6.3.4. Sicherheit der Lieferkette (Artikel 21 Absatz 2 littera d NIS-2-RL)

Eine der in Artikel 21 Absatz 2 NIS-2-RL angeführten Risikomanagementmaßnahmen ist im gegebenen Zusammenhang aufgrund ihrer Neuartigkeit und der Herausforderungen, vor die sie Unternehmen stellt, besonders hervorzuheben. Gemäß Artikel 21 Absatz 2 littera d NIS-2-RL sind wesentliche und wichtige Einrichtungen künftig verpflichtet, die *„Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern"* zu gewährleisten.

Wie wesentliche und wichtige Einrichtungen dieser Verpflichtung *in concreto* nachkommen können, ergibt sich in Zusammenschau der Artikel 21 Absatz 2 littera d und Absatz 3 NIS-2-RL in Verbindung mit Artikel 22 NIS-2-RL sowie den Erwägungsgründen 59, 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 zweierlei:

Einerseits müssen wesentliche und wichtige Einrichtungen ihre Lieferanten hinsichtlich ihres Cybersicherheitsrisikos einschätzen und bewerten.[107] Daraus folgt die Verpflichtung, nur von solchen Lieferanten Leistungen zu beziehen bzw nur mit solchen Lieferanten Verträge abzuschließen, bei denen im Zeitpunkt des Vertragsabschlusses von ihrer cybersicherheitsrechtlichen Unbedenklichkeit ausgegangen werden darf. Sollte sich während laufender Vertragsbeziehung ein Cybersicherheitsrisiko bezüglich des Lieferanten offenbaren, sind wesentliche und wichtige Einrichtungen verpflichtet, entsprechende Maßnahmen zu ergreifen (etwa Kündigung des Vertrages).

Andererseits müssen wesentliche und wichtige Einrichtungen ihre Lieferanten vertraglich auf die Einhaltung von Cybersicherheitsstandards verpflichten.[108] Oftmals wird dies darauf hinauslaufen, dass Vertragspflichten hinsichtlich einschlägiger Zertifizierungen der Lieferanten in die Verträge aufgenommen werden.

Eine gewisse Hilfestellung bei der Bewertung und Berücksichtigung der Cybersicherheitsrisiken ihrer Lieferanten erhalten wesentliche und wichtige Einrichtungen durch das Instrument der *„Koordinierte[n] Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf Ebene der Union"* gemäß Artikel 22 NIS-2-RL. In deren Rahmen führt *„[d]ie Kooperationsgruppe*[109] *[…] in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren durch[…]"*. Die Ergebnisse der koordinierten Risikobewertungen sind von wesentlichen und wichtigen Einrichtungen gemäß Artikel 21 Absatz 3 NIS-2-RL bei der Risikobewertung in Bezug auf die Sicherheit kritischer Lieferketten zu berücksichtigen.

6.3.5. Schulungsmaßnahmen für Leitungsorgane und Mitarbeiter (Artikel 20 Absatz 2 NIS-2-RL)

Eine weitere Neuerung im Vergleich zur NIS-1-RL findet sich in Artikel 20 Absatz 2 NIS-2-RL. Gemäß dieser Bestimmung sind wesentliche und wichtige Einrichtungen künftig verpflichtet, ihre Leitungsorgane[110] und Mitarbeiter entsprechend schulen zu lassen. *„[D]ie Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen*

107 Vgl Erwägungsgrund 85 NIS-2-RL: „Die wesentlichen und wichtigen Einrichtungen sollten daher die Gesamtqualität und Widerstandsfähigkeit der Produkte und Diensten, die darin enthaltenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter, einschließlich ihrer sicheren Entwicklungsprozesse, bewerten und berücksichtigen".

108 Siehe Erwägungsgrund 85 NIS-2-RL.

109 Bei der „Kooperationsgruppe" handelt es sich um ein gemäß Artikel 14 Absatz 1 NIS-2-RL eingesetztes Organ, dass „sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen[setzt]".

110 Zur Auslegung des Begriffs des „Leitungsorgans" siehe unter 7.3.

[müssen] an Schulungen teilnehmen", wie auch wesentliche und wichtige Einrichtungen aufgefordert sind, „*allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten*". Dies, „*um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben*".

Vorgaben zur Art der Schulungsmaßnahmen oder deren Ausmaß enthält die NIS-2-RL aber nicht. In diesem Zusammenhang besteht damit ein entsprechender mitgliedstaatlicher Umsetzungsspielraum, die konkreten Rahmenbedingungen der Schulungsverpflichtung für Mitglieder der Leitungsorgane und Mitarbeiter festzulegen. Umsetzungsmaßnahmen müssen aber jedenfalls den Verhältnismäßigkeitsgrundsatz beachten,[111] weshalb gesetzliche Schulungspflichten unzulässig wären, die überbordende zeitliche oder inhaltliche Anforderungen aufstellen. Umgekehrt wäre die Verankerung eines zu geringen zeitlichen oder inhaltlichen Ausmaßes der Schulungsverpflichten im NISG unionsrechtswidrig, als die von den mitgliedstaatlichen Gesetzgebern zu erlassenden Umsetzungsbestimmungen gewährleisten müssen, dass „*ausreichende Kenntnisse und Fähigkeiten*" erworben werden.

6.3.6. Europäische Schemata für die Cybersicherheitszertifizierung (Artikel 24 NIS-2-RL)

In Artikel 24 Absätzen 1 und 2 NIS-2-RL findet sich schließlich eine Ermächtigung der Mitgliedstaaten (Absatz 1) sowie der Kommission (Absatz 2), „*wesentliche und wichtige Einrichtungen dazu [zu] verpflichten, spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden*", „*die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung[…] zertifiziert sind*". Die Verpflichtung, bestimmte im Sinne des Artikel 24 NIS-2-RL zertifizierte Produkte zu nutzen, besteht damit nur insoweit, als entweder die Mitgliedstaaten oder die Kommission von ihrer jeweiligen Kompetenz Gebrauch gemacht haben.

6.4. Meldepflichten (Artikel 23 NIS-2-RL)

6.4.1. Gesetzlich festgelegtes Notfallprogramm

Während das Gebot zur Setzung von Risikomanagementmaßnahmen Cybergefahrenlagen vorbeugen will, bezwecken die Meldepflichten des Artikel 23 NIS-RL, dass Unternehmen der Behörde bei deren Realisation alle erforderlichen Informationen zur Verfügung stellen. Gemäß Artikel 23 Absatz 1 NIS-2-RL sind wesentliche und wichtige Einrichtungen deswegen verpflichtet, „*unverzüglich über jeden Sicherheitsvorfall [zu] unterrichten, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste […] (erheblicher Sicherheitsvorfall)*" hat. Eine derartige Vorgabe fand sich zwar bereits in Artikel 14 Absatz 3 NIS-1-RL. Mit Artikel 23 NIS-2-RL wird die Meldepflicht aber insoweit fortentwickelt, als Unternehmen künftig zur Einhaltung eines minutiösen Ablaufprogramms verpflichtet sind.

Während Artikel 14 Absatz 3 NIS-1-RL davon absah, die konkreten Details des Meldungsprozesses festzulegen, weshalb auch die Umsetzungsbestimmung des § 19 NISG in zeitlicher Hinsicht lediglich die Vorgabe einer – auslegungsbedürftigen–„unverzüglichen" Meldung (Was bedeutet „unverzüglich?") enthält,[112] lässt Artikel 23 NIS-2-RL für derartige Interpretationsspielräume keinen Platz. In Artikel 23 Absatz 4 NIS-2-RL finden wesentliche und wichtige Einrichtungen als gesetzlich festgelegtes Notfallprogramm zum einen konkrete Fristen und zum anderen jene Schritte (in der Diktion der Richtlinie: „*mehrstufiger Ansatz für die Meldung erheblicher Sicherheitsvorfälle*"),[113] die sie setzen müssen, um ihrer Verpflichtung zur Meldung erheblicher Sicherheitsvorfälle an die Behörde[114] zu entsprechen.

6.4.2. Erheblicher Sicherheitsvorfall (Artikel 23 Absatz 3 NIS-2-RL)

Der Begriff des „Sicherheitsvorfalls", der im Zentrum der Meldepflichten der NIS-2-RL steht, wird in Artikel 6 Nummer 6 NIS-2-RL legaldefiniert. Bei einem Sicherheitsvorfall handelt es sich demnach um „*ein Ereignis, das die Verfügbarkeit, Authentizi-*

111 Vgl nur Artikel 21 Absatz 1 NIS-2-RL, wobei sich dieser Umstand ebenso aus allgemeinen Rechtsgrundsätzen sowie dem unionalen Primärrecht (insbesondere der GRC) ergibt.

112 Siehe zum daraus folgenden Zeitpunkt der Meldung gemäß § 19 NISG, Anderl/Mayer in Anderl et al, NISG § 19 NISG Rz 22 ff.

113 Erwägungsgrund 101 NIS-2-RL.

114 Artikel 23 NIS-2-RL spricht zwar stets von der Meldung an das „CSIRT oder gegebenenfalls [die] zuständige[…] Behörde", aufgrund der staatlichen Qualität des CSIRT wird im Folgenden aber für beide der Überbegriff der „Behörde" verwendet.

tät, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt".

Die Erheblichkeit eines Sicherheitsvorfalls, die die Pflicht zu dessen Meldung gemäß Artikel 23 Absatz 1 NIS-2-RL auslöst, wird in Artikel 23 Absatz 3 NIS-2-RL anhand zweier alternativer Kriterien definiert. Erheblich ist ein Sicherheitsvorfall demnach, wenn er entweder

- *„schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann"* (Artikel 23 Absatz 3 littera a NIS-2-RL), oder
- *„er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann"* (Artikel 23 Absatz 3 littera b NIS-2-RL).

Die negativen Auswirkungen, die die Erheblichkeit eines Sicherheitsvorfalles begründen, können damit sowohl die Einrichtung selbst als auch Dritte (*„andere natürliche oder juristische Personen"*) betreffen. Die Einrichtung hat die Erheblichkeit auf Basis einer *„Anfangsbewertung"* selbst einzuschätzen.[115] Erwägungsgrund 101 NIS-2-RL präzisiert die Gesichtspunkte, die bei der Anfangsbewertung zu berücksichtigen sind:

- Welche Netz- und Informationssysteme sind betroffen und welche Bedeutung haben diese für die Erbringung der Dienste der Einrichtung?
- Wie schwer ist die Cyberbedrohung und welche technischen Merkmale weist sie auf?
- Welche Schwachstellen wurden bzw werden ausgenutzt?
- Welche Erfahrungen hat die Einrichtung mit ähnlichen Vorfällen gemacht?
- Wie groß ist das Ausmaß, in dem das Funktionieren des Dienstes beeinträchtigt wird?
- Wie lange ist die geschätzte Dauer des Sicherheitsvorfalls?
- Wie groß ist die Zahl der betroffenen Nutzer von beeinträchtigten Diensten?

Ist sich das Unternehmen bzw die betreffende Einrichtung im Rahmen der Anfangsbewertung unsicher, ob ein Sicherheitsvorfall die Schwelle der Erheblichkeit überschreitet oder nicht, sollte die Meldung im Zweifel eher erfolgen als unterbleiben. Denn 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.

Zum einen legt Artikel 23 Absatz 1 NIS-2-RL fest, dass *„[m]it der bloßen Meldung […] keine höhere Haftung der meldenden Einrichtung begründet"* wird, wodurch sich die schadensmindernde Wirkung freiwilliger Meldungen bezüglich etwaiger Haftungen jedenfalls als vorteilhaft erweist. Zum anderen wirkt ein proaktives und kooperatives Verhalten des betreffenden Unternehmens bei einer etwaigen Strafbemessung auch strafmildernd. Denn unter den in Artikel 32 Absatz 7 NIS-2-RL genannten Elementen, die gemäß Artikel 34 Absatz 3 NIS-2-RL *„[b]ei der Entscheidung über die Verhängung einer Geldbuße und deren Höhe […] in jedem Einzelfall […] gebührend zu berücksichtigen"* sind, finden sich unterschiedliche Anknüpfungspunkte, die im Falle einer unterlassenen Meldung zur Straferhöhung bzw bei erfolgter Meldung zur Strafmilderung führen können.

So hat etwa gemäß Artikel 32 Absatz 7 littera a NIS-2-RL *„eine unterlassene Meldung oder Behebung von erheblichen Sicherheitsvorfällen"* stets zur Folge, dass der Verstoß gegen die Vorschriften der NIS-2-RL als „schwer" zu qualifizieren ist. Gemäß Artikel 32 Absatz 7 littera f NIS-2-RL entfalten die *„von der Einrichtung ergriffene Maßnahmen zur Verhinderung oder Minderung des materiellen oder immateriellen Schadens"* bei der Strafbemessung ebenso Relevanz, wie gemäß Artikel 32 Absatz 7 littera h NIS-2-RL der *„Umfang der Zusammenarbeit der verantwortlichen natürlichen oder juristischen Personen mit den zuständigen Behörden"* bei der Festsetzung der Strafhöhe Berücksichtigung finden muss. Ein proaktives, freiwilliges und kooperatives Verhalten von wesentlichen und wichtigen Einrichtungen wird sich damit regelmäßig förderlich auf ein

115 Erwägungsgrund 101 NIS-2-RL.

etwaiges Verwaltungsstrafverfahren auswirken.

Zudem sei an dieser Stelle noch bemerkt, dass die Zulässigkeit der Verhängung von Strafen für den Fall, dass die Behörde lediglich aufgrund einer Meldung gemäß Artikel 23 NIS-2-RL Informationen über Verstöße gegen die Vorschriften der RL erlangt, ohnedies mehr als fraglich ist. Das in Artikel 6 Absatz 2 EMRK[116] sowie Artikel 90 B-VG[117] verankerte *nemo tenetur*-Prinzip (Verbot der Selbstbezichtigung)[118] verbietet es, natürliche und juristische Personen ausschließlich auf der Grundlange von Beweisen zu bestrafen, die diese in Erfüllung einer rechtlichen Verpflichtung selbst (an die Behörde) geliefert haben.[119]

Aus all diesen Gründen können freiwillige Meldungen selbst für den Fall, dass sich *ex post* die Unerheblichkeit des Sicherheitsvorfalles herausstellen sollte, die Position der meldenden Einrichtung kaum verschlechtern. Sofern sich der Sicherheitsvorfall aber nachträglich als „erheblich" herausstellen sollte, würde das Unterlassen der Meldung gemäß Artikel 32 Absatz 7 littera a NIS-2-RL stets einen schweren – und damit entsprechen strafverschärfenden – Verstoß gegen die Richtlinie darstellen. Bei Unklarheit über die Erheblichkeit eines Sicherheitsvorfalles sollten wesentliche und wichtige Einrichtungen die Meldung gemäß Artikel 23 NIS-2-RL deshalb vornehmen.

6.4.3. Ablauf des Meldungsprozesses

6.4.3.1. Frühwarnung (Artikel 23 Absatz 4 littera a NIS-2-RL)

Als ersten Schritt, den wesentliche und wichtige Einrichtungen nach Erkennen eines erheblichen Sicherheitsvorfalles zu setzen haben, sieht Artikel 23 Absatz 4 littera a NIS-2-RL die Erstmeldung (in der Diktion der NIS-2-RL *„Frühwarnung"*) an das Computer-Notfallteam (CSIRT = Computer Security Incident Response Team)[120] oder gegebenenfalls der zuständigen Behörde (in weiterer Folge beide gemeinsam: „Behörde") vor. Folgende Informationen sind in der Frühwarnung von wesentlichen und wichtigen Einrichtungen zu übermitteln:

- Ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist.
- Ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall grenzüberschreitende Auswirkungen haben könnte.

Wie aus Erwägungsgrund 102 NIS-2-RL ersichtlich, dürfen die Anforderungen an den Informationsgehalt der Frühwarnung aber nicht überspannt werden. *„Die Frühwarnung sollte lediglich die Informationen enthalten, die erforderlich sind, um das CSIRT oder gegebenenfalls die zuständige Behörde über den Sicherheitsvorfall zu unterrichten und es der betreffenden Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen."*[121]

Fraglich ist, zu welchem Zeitpunkt die Frühwarnung erstattet werden muss. Aus dem Umstand, dass Artikel 23 Absatz 4 littera a NIS-2-RL davon spricht, dass die Frühwarnung *„unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls"* vorzunehmen ist, folgt, dass es sich bei der Frist von 24 Stunden um eine Maximalfrist handelt. Unternehmen haben damit keinesfalls länger als 24 Stunden Zeit, die Frühwarnung abzugeben. Sie dürfen sich aber auch nicht in jedem Fall 24 Stunden Zeit lassen, weil eben die Information *„unverzüglich"* zu übermitteln ist.

Eine gewisse Orientierungshilfe für die Bestimmung des Zeitpunktes der Vornahme der Frühwarnung bietet wiederum Erwägungsgrund 102 NIS-2-RL: Demnach sollen die Mitgliedstaaten bei der Umsetzung der Richtlinie in innerstaatliches Recht dafür Sorge tragen, *„dass die Verpflichtung, diese Frühwarnung oder die anschließende Meldung eines Sicherheitsvorfalls zu übermitteln, nicht dazu führt, dass die meldende Einrichtung die Ressourcen von Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfäl-*

116 Europäische Menschenrechtskonvention.

117 Bundes-Verfassungsgesetz, BGBl 1/1930 (WV).

118 Dazu etwa Muzak, B-VG6 Art 6 MRK Rz 33.

119 Die Auswirkungen des nemo tenetur-Prinzips auf die Möglichkeit der Verhängung von Strafen, wenn die Behörde nur aufgrund einer Meldung eines Unternehmens Kenntnis von Verstößen erlangt, wurde zuletzt insbesondere im Kontext der DSGVO diskutiert. Siehe dazu etwa Piska, ecolex 2023, 614.

120 Siehe Artikel 10 NIS-2-RL.

121 Erwägungsgrund 102 NIS-2-RL.

len — was vorrangig behandelt werden sollte — umlenken müssen". Dies, „*um zu verhindern, dass die Verpflichtung zur Meldung von Sicherheitsvorfällen entweder dazu führt, dass Ressourcen für die Bewältigung erheblicher Sicherheitsvorfälle umgelenkt oder die diesbezüglichen Maßnahmen der Einrichtungen auf andere Weise beeinträchtigt werden*".

Vereinfachend lässt sich daher der konkrete Zeitpunkt innerhalb der 24-Stunden-Frist, zu dem die Frühwarnung abgesendet werden muss, als „so früh wie möglich, so spät als nötig" zusammenfassen. Solange alle internen Ressourcen in die Abwehr des Cyberangriffes oder die sonstige Eindämmung des erheblichen Sicherheitsvorfalles fließen müssen, um diesen zu bewältigen, will die NIS-2-RL wesentliche und wichtige Einrichtungen daran nicht hindern. Sobald sich allerdings – wobei insbesondere die geringen Anforderungen an den Informationsgehalt der Frühwarnung zu berücksichtigen sind (Erwägungsgrund 102 NIS-2-RL) – das Personal soweit freigespielt hat, dass es ohne spürbare Beeinträchtigung der Maßnahmen zur Eindämmung des Sicherheitsvorfalles möglich ist, muss die Frühwarnung erstattet werden. Sind die 24 Stunden nach Kenntnisnahme vom erheblichen Sicherheitsvorfall allerdings verstrichen, hat die wesentliche oder wichtige Einrichtung ihre Pflicht zur Erstattung einer Frühwarnung aber jedenfalls verletzt.

In diesem Zusammenhang ist noch zu betonen, dass die Notwendigkeit, alle personellen Ressourcen zur Bewältigung des Sicherheitsvorfalles einzusetzen, von der wesentlichen und wichtigen Einrichtung wohl dann nicht rechtfertigend geltend gemacht werden kann, wenn diese zu wenig Personal beschäftigt. Artikel 21 Absatz 1 NIS-2-RL verpflichtet wesentliche und wichtige Einrichtungen zur Setzung auch von „*organisatorische[n]*" Risikomanagementmaßnahmen im Bereich der Cybersicherheit, worunter nicht zuletzt auch die Sicherstellung eines dem Risiko der betreffenden Einrichtung angemessenen Personalstandes zählt. Beschäftigt ein Unternehmen damit, bezogen auf sein spezifisches Cybersicherheits-Risiko, zu wenig IT-Fachkräfte, wird es folglich auch bei schuldlosem Eintritt eines erheblichen Sicherheitsvorfalles im Zusammenhang mit den vorzunehmenden Meldungen regelmäßig gegen seine Pflichten aus der NIS-2-RL verstoßen. Denn entweder die verspätete Meldung offenbart den unzureichenden Mitarbeiterstand, oder die Vornahme der Meldung führt zur unzureichenden Setzung von Abwehrmaßnahmen. Daraus folgt die Notwendigkeit, interne Vorgaben für den Ablauf des Meldungsprozesses anhand von wahrscheinlichen Szenarien zu entwickeln.

6.4.3.2. Meldung über den Sicherheitsvorfall (Artikel 23 Absatz 4 littera b NIS-2-RL)

Bereits aus dem Begriff der „*Frühwarnung*", mit dem die NIS-2-RL den ersten Informationsakt gegenüber der Behörde bezeichnet,[122] wird ersichtlich, dass diese nur vorbereitenden Charakter hat. Die Hauptlast der initialen[123] Informationsübermittlung an die Behörde ruht nach dem Konzept der NIS-2-RL auf der gemäß Artikel 23 Absatz 4 littera b leg cit innerhalb von 72 Stunden zu übermittelnden „*Meldung über den Sicherheitsvorfall*".

Der Zweck der „*Meldung über den Sicherheitsvorfall*" liegt gemäß Artikel 23 Absatz 4 littera b in Verbindung mit Erwägungsgrund 102 NIS-2-RL darin, „*die im Rahmen der Frühwarnung übermittelten Informationen zu aktualisieren und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seiner Schwere und seiner Auswirkungen, sowie etwaiger Kompromittierungsindikatoren (indicators of compromise — IoC), sofern verfügbar, vorzunehmen*". Während im Rahmen der Frühwarnung lediglich eine rudimentäre Erstinformation der Behörde anhand von Verdachtsmomenten erfolgt, haben wesentliche oder wichtige Einrichtungen mit der Meldung über den Sicherheitsvorfall bereits eine Beurteilung des erheblichen Sicherheitsvorfalles vorzunehmen.

Wie hinsichtlich der Frühwarnung, verlangt die NIS-2-RL ebenso für die Meldung über den Sicherheitsvorfall die „unverzügliche" Übermittlung, wobei Artikel 23 Absatz 4 littera b NIS-2-RL als Maximalfrist „*72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls*" vorsieht. Damit gilt wie für die Frühwarnung wiederum, das die Meldung über den Sicherheitsvorfall „so früh wie möglich, so spät als nötig" zu erfolgen hat.[124]

122 Siehe dazu soeben unter 6.4.3.1.
123 Siehe zum Abschlussbericht gemäß Artikel 23 Absatz 4 littera d NIS-2-RL unter 6.4.3.4.
124 Siehe zur Auslegung des Begriffs „unverzüglich" bereits unter 6.4.3.1.

Anderes gilt gemäß Artikel 23 Absatz 4 letzter Unterabsatz NIS-2-RL für *„Vertrauensdiensteanbieter"*. Sie haben *„in Bezug auf erhebliche Sicherheitsvorfälle, die sich auf die Erbringung [ihrer] Vertrauensdienste auswirken"*, die Meldung über den Sicherheitsvorfall *„unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls"*, zu übermitteln. Vertrauensdiensteanbieter unterliegen damit im Hinblick auf den ihnen für die Übermittlung der Meldung über den Sicherheitsvorfall zur Verfügung stehenden Zeitraum im Vergleich zu sonstigen wesentlichen oder wichtigen Einrichtungen deutlich verschärften Anforderungen. Sie müssen der Behörde die Beurteilung des erheblichen Sicherheitsvorfalles innerhalb jenes Zeitfensters zukommen lassen, das sonstigen wesentlichen oder wichtigen Einrichtungen für die rudimentäre Erstinformation (Frühwarnung) zur Verfügung steht. Fraglich bleibt dabei, ob sich damit die Frühwarnung für Vertrauensdiensteanbieter erübrigt, oder ob sie diese trotz der Pflicht zur Erstattung der Meldung über den Sicherheitsvorfall innerhalb von 24 Stunden dennoch übermitteln müssen. Im Ergebnis wird wohl davon auszugehen sein, dass die Pflicht zur Frühwarnung auch für Vertrauensdiensteanbieter gilt, sofern die Übermittlung der betreffenden Informationen an die Behörde vor der Meldung über den Sicherheitsvorfall zu dessen Eindämmung beitragen kann.[125]

6.4.3.3.Zwischenbericht auf behördliches Ersuchen (Artikel 23 Absatz 4 littera c NIS-2-RL)

Mit der Erstattung der Meldung über den Sicherheitsvorfall gemäß Artikel 23 Absatz 4 littera b NIS-2-RL haben wesentliche und wichtige Einrichtungen ihre Informationsverpflichtung gegenüber der Behörde bis zum Zeitpunkt, zu dem sie den Abschlussbericht gemäß Artikel 23 Absatz 4 littera f NIS-2-RL erstatten müssen,[126] grundsätzlich erfüllt. Anderes gilt nur insofern, als die Behörde die wesentliche oder wichtige Einrichtung gemäß Artikel 23 Absatz 4 littera c NIS-2-RL um *„einen Zwischenbericht über relevante Statusaktualisierungen"* ersucht.

Die Behörde wird bei der Entscheidung, ob sie einen derartigen Zwischenbericht anfordert und welche Frist sie für dessen Erstattung einräumt, wiederum auf die personellen Ressourcen des Unternehmens Rücksicht nehmen müssen. Im Sinne von Erwägungsgrund 102 NIS-2-RL ist davon auszugehen, dass das Ersuchen um einen Zwischenbericht nicht dazu führen darf, *„dass die meldende Einrichtung die Ressourcen von Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen […] umlenken" muss.*

6.4.3.4.Abschlussbericht (Artikel 23 Absatz 4 littera d NIS-2-RL)

Den Meldeprozess beschließt – *nomen est omen* – der gemäß Artikel 23 Absatz 4 littera d NIS-2-RL zu übermittelnde *„Abschlussbericht"*. In diesem haben wesentliche und wichtige Einrichtungen die folgenden Informationen an die Behörde zu übermitteln:

- *„eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen"*,
- *„Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat"*,
- *„Angaben zu den getroffenen und laufenden Abhilfemaßnahmen"*, sowie
- *„gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls"*.[127]

Dauert der erhebliche Sicherheitsvorfall im Zeitpunkt der Vorlage des Abschlussberichts (*„spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls"*) noch an, müssen wesentliche und wichtige Einrichtungen stattdessen einen Fortschrittsbericht an die Behörde übermitteln. Der Abschlussbericht ist diesfalls gemäß Artikel 23 Absatz 4 littera e NIS-2-RL *„innerhalb eines Monats nach Behandlung des Sicherheitsvorfalls"* vorzulegen.

Fraglich ist, zu welchem Zeitpunkt der Abschlussbericht konkret übermittelt werden muss. Artikel 23 Absatz 4 littera d NIS-2-RL setzt zwar auch für diesen eine Maximalfrist (*„spätestens einen Monat nach Übermittlung der Meldung des*

125 Vgl in diesem Zusammenhang Artikel 23 Absatz 5 NIS-2-RL, wonach „[d]as CSIRT oder die zuständige Behörde […] der meldenden Einrichtung unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach Eingang der Frühwarnung gemäß Absatz 4 Buchstabe a eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operativer Beratung für die Durchführung möglicher Abhilfemaßnahmen", übermittelt.

126 Siehe zum Abschlussbericht gemäß Artikel 23 Absatz 4 littera d NIS-2-RL sogleich unter 6.4.3.4.

127 Artikel 23 Absatz 4 littera d NIS-2-RL.

Sicherheitsvorfalls") fest.[128] Anders als hinsichtlich der „*Frühwarnung*" und der „*Meldung über den Sicherheitsvorfall*" verzichtet die Richtlinie allerdings darauf, die Erstattung „unverzüglich" zu fordern.

Aufgrund des Umstandes, dass die betreffenden Anordnungen in engstem textuellen Zusammenhang (Artikel 23 Absatz 4 littera a-d NIS-2-RL) getroffen werden, ist davon auszugehen, dass die NIS-2-RL durch das Fehlen der Verpflichtung zur „unverzüglichen" Übermittlung des Abschlussberichts für betroffene Unternehmen einen großzügigeren zeitlichen Rahmen schafft, als hinsichtlich der „*Frühwarnung*" und der „*Meldung über den Sicherheitsvorfall*". Während ein Unternehmen seine Verpflichtungen zur Übermittlung der „*Frühwarnung*" und der „*Meldung über den Sicherheitsvorfall*" verletzt, sofern es diese nicht – innerhalb der Maximalfrist – übermittelt, sobald es seine personellen Ressourcen zulassen, dürften wesentliche und wichtige Einrichtungen der Verpflichtung zur Übermittlung des Abschlussberichts stets dann entsprechen, wenn sie diese nur bis zum Ende der Monatsfrist des Artikel 23 Absatz 4 littera d NIS-2-RL absenden.

6.4.3.5. Unverzügliche Meldung bzw Information an Diensteempfänger (Artikel 23 Absatz 1 u 2 NIS-2-RL)

Sofern der erhebliche Sicherheitsvorfall auch Auswirkungen auf die Erbringung des jeweiligen Dienstes der wesentlichen oder wichtigen Einrichtung haben könnte, sind auch die „*Empfänger [der] Dienste*" des Unternehmens („Diensteempfänger") zu informieren. Gemäß Artikel 23 Absatz 1 NIS-2-RL unterrichten wesentliche und wichtige Einrichtungen die Empfänger ihrer Dienste gegebenenfalls „unverzüglich" über einen erheblichen Sicherheitsvorfall, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnte.

Anders als für die Übermittlung der behördlichen Meldungen (Frühwarnung,[129] Meldung über den Sicherheitsvorfall[130] und Abschlussbericht)[131] sieht die NIS-2-RL davon ab, eine Maximalfrist für die Meldung an die Diensteempfänger vorzusehen, sondern verlangt nur deren „Unverzüglichkeit". Hinsichtlich des Begriffsverständnisses der „Unverzüglichkeit" kann auf die unter 6.4.3.1. getätigten Ausführungen verwiesen werden, wobei zusammenfassend wiederum gilt, dass die Diensteempfänger „so früh wie möglich, so spät als nötig" informiert werden müssen.

Als wesentlich bemerkenswerter als die – gewissermaßen auf der Hand liegende – Verpflichtung zur Information der Diensteempfänger nach Eintritt eines erheblichen Sicherheitsvorfalls erweist sich aber die Verpflichtung gemäß Artikel 23 Absatz 2 NIS-2-RL: Demnach haben wesentliche und wichtige Einrichtungen die Empfänger ihrer Dienste auch hinsichtlich erheblicher Cyberbedrohungen „unverzüglich" zu informieren, sofern diese potenziell davon betroffen sind.

Den Begriff der „Cyberbedrohung" definiert die NIS-2-RL nicht selbst, sondern verweist dazu in Artikel 6 Nummer 10 NIS-2-RL auf die Begriffsdefinition in „*Artikel 2 Nummer 8 der Verordnung (EU) 2019/881*". Bei einer „Cyberbedrohung" handelt es sich demnach um „*einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte*".[132]

Die Informationen, die im Zusammenhang mit einer derartigen Mitteilung über eine erhebliche Cyberbedrohung an die Diensteempfänger übermittelt werden müssen, ergeben sich aus Artikel 23 Absatz 2 in Verbindung mit Erwägungsgrund 102 NIS-2-RL; sie „*sollte kostenlos sein, und die Informationen sollten in leicht verständlicher Sprache abgefasst werden*". Den Diensteempfängern sind „*alle Maßnahmen oder Abhilfemaßnahmen mit[zu]teilen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können*". Über die Cyberbedrohung selbst ist hingegen nur dann jedenfalls zu informieren, wenn „*die erhebliche Cyberbedrohung wahrscheinlich eintreten wird*". ErwGr 103 NIS-2-RL stellt zudem ausdrücklich klar, dass „*[d]ie Verpflichtung zur*

128 Siehe in diesem Zusammenhang bereits zu den Maximalfristen für die Erstattung der Frühwarnung (6.4.3.1.) und für die Erstattung der Meldung über den Sicherheitsvorfall (6.4.3.2.).

129 Dazu unter 6.4.3.1.

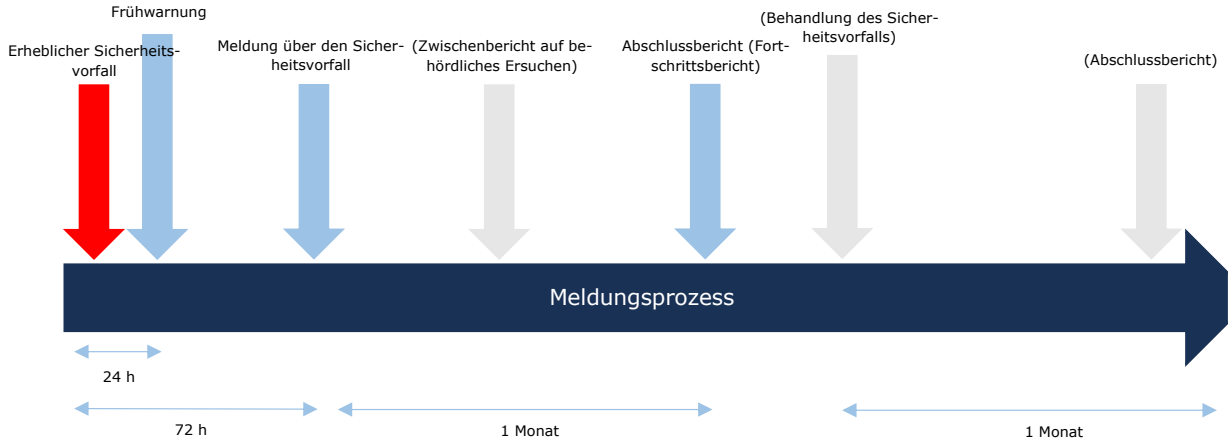
130 Dazu unter 6.4.3.2

131 Dazu unter 6.4.3.4.

132 Artikel 2 Nummer 8 Verordnung 2019/881/EU (Rechtsakt zur Cybersicherheit).

Information der Empfänger über solche erheblichen Bedrohungen " zwar *„nach besten Kräften erfüllt werden* " sollte, die betreffende Einrichtung *„jedoch nicht von der Pflicht befrei[t], auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede derartige Bedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen* ".

niveau des Dienstes wiederherzustellen".



6.5. Zwischenresümee

Zusammengefasst baut die NIS-2-RL mit ihren unternehmensbezogenen Pflichten auf bereits Bekanntem auf. Wie in der NIS-1-RL bilden wiederum Verpflichtungen zur Setzung von Risikomanagementmaßnahmen einerseits und Meldepflichten andererseits den Kern des Cybersicherheits-Pflichtenprogramms für Unternehmen.

Im Detail zeigen sich die Anforderungen an Unternehmen aber dann doch verändert: Um den *„inhärente[n] Mängel[n]* "[133] der NIS-1-RL abzuhelfen, erweitert der Unionsgesetzgeber nicht nur den Anwendungsbereich des unionalen Cybersicherheitsrechts, sondern er schärft auch an vielen Stellen nach. So müssen wesentliche und wichtige Einrichtungen künftig ihre gesamte IT und OT und nicht nur jene Teile ihrer Netz- und Informationssysteme schützen, die bei der Erbringung von kritischen Diensten zum Einsatz kommen. Schulungspflichten für Leitungsorgane und Mitarbeiter etabliert die NIS-2-RL ebenso neu, wie Gebote zur Gewährleistung einer sicheren Lieferkette.

Besonders strikt wird in der NIS-2-RL schließlich der Prozess der Meldung von erheblichen Sicherheitsvorfällen getaktet. Knapp bemessene Zeitfenster und detaillierte Anforderungen an den Inhalt von Meldungen an die Behörde sollen künftig dafür Sorge tragen, dass Unternehmen im Fall des Falles alle notwendigen Informationen zur Bewältigung des Cybersicherheitsvorfalls zur Verfügung stellen.

Aufgrund dieser Verschärfung der Cybersicherheitspflichten wird die NIS-2-RL für betroffene Unternehmen einen erheblichen finanziellen Aufwand nach sich ziehen. Die Europäische Kommission schätzt, dass je nachdem, ob Unternehmen bereits NIS-1 erfüllen oder nicht, Erhöhungen des Cybersicherheitsbudgets zwischen 12 bis 22 % anstehen. Unternehmen sollten die diesbezüglich aufgewendeten Mittel allerdings nicht als bloße Kosten, sondern vielmehr als Investition betrachten. Denn nicht nur, dass NIS-2-Compliance kostspielige Cyberkrisen verhindert. Sie schützt auch vor den Millionen- bzw Milliardengeldbußen, die gemäß Artikel 34 NIS-2-RL als Damoklesschwert über wesentlichen und wichtigen Einrichtungen schweben.

133 Erwägungsgrund 2 NIS-2-RL.

7. Das Sanktionsregime der NIS 2-RL

7.1. Allgemeines

Um sicherzustellen, dass wesentliche und wichtige Einrichtungen ihren Cybersicherheitspflichten auch nachkommen,[134] setzt das unionale Cybersicherheitsrecht mit der NIS-2-RL künftig auf ein Bündel an scharfen und schärfsten Sanktionsmaßnahmen. Am augenfälligsten erweisen sich dabei zum einen die prohibitiven Strafrahmen der gemäß Artikel 34 NIS-2-RL gegen wesentliche und wichtige Einrichtungen zu verhängenden Geldbußen (in der österreichischen verwaltungsstrafrechtlichen Diktion: Verwaltungsstrafen/Geldstrafen). Bis zu 10 bzw 7 Mio Euro oder 2 % bzw 1,4 % des weltweiten Konzernumsatzes beträgt die maximale Höhe jener finanziellen Sanktionen, die – voraussichtlich – ab 18.10.2024 im Raum stehen.

Zum anderen verortet die NIS-2-RL die Verantwortung für die Einhaltung ihrer unternehmensbezogenen Cybersicherheitspflichten nunmehr ausdrücklich bei den Leitungspersonen wesentlicher und wichtiger Einrichtungen. Diesen drohen nicht nur eine persönliche Haftung, sondern im äußersten Fall auch vorübergehende Tätigkeitsverbote.

7.2. Zuständigkeiten

Grundsätzlich sind gemäß Artikel 26 NIS-2-RL die Mitgliedsstaaten zuständig, in denen die Einrichtungen niedergelassen sind. Eine Ausnahme besteht jedoch für den Sektor Digitale Infrastruktur, sowie für Einrichtungen der öffentlichen Verwaltung.

Anbieter öffentlicher elektronischer Kommunikationsnetze sowie Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste unterliegen der Zuständigkeit des Mitgliedstaats, in dem sie ihre Dienste erbringen.

Für Einrichtungen die Dienste in mehreren Mitgliedstaaten erbringen oder über Niederlassungen in mehreren Mitgliedstaaten verfügen, gibt es eine getrennte und parallele Zuständigkeit der betreffenden Mitgliedstaaten. Es wird Fälle geben wo nationale Behörden grenzübergreifend miteinander zusammenarbeiten werden. Einrichtungen brauchen jedoch keine Angst davor zu haben, dass auf einen Verstoß gegen die Bestimmungen der NIS-2-RL Durchsetzungsmaßnahmen und Sanktionen aus mehreren Mitgliedstaaten folgen werden. Es gilt der Grundsatz „ne bis in idem"; also das Verbot der Doppelbestrafung.[135]

Für DNS-Dienstanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Anbieter von Online-Suchmaschinen oder Anbieter von Plattformen für Dienste sozialer Netzwerke gilt die Zuständigkeit des Mitgliedstaats, in dem sie ihre Hauptniederlassung im Sinne des Artikel 26 Absatz 2 NIS-2-RL haben. Als Hauptniederlassung gilt dabei

➔ *„die Niederlassung in demjenigen Mitgliedstaat, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement vorwiegend getroffen werden".*

Kann ein solcher Mitgliedstaat nicht bestimmt werden oder werden diese Entscheidungen nicht in der Union getroffen, so gilt als Hauptniederlassung

➔ *„der Mitgliedstaat, in dem die Cybersicherheitsmaßnahmen durchgeführt werden".*

Kann wiederum ein solcher Mitgliedstaat nicht bestimmt werden, so gilt als Hauptniederlassung

➔ *„der Mitgliedstaat, in dem die betreffende Einrichtung die Niederlassung mit der höchsten Beschäftigtenzahl in der Union hat".*

134 Siehe zu den unternehmensbezogenen Cybersicherheitspflichten soeben unter 6.

135 Vgl Erwägungsgrund 113 f NIS-2-RL.

Beispiel

Ein österreichischer Anbieter von Cloud-Computing-Diensten hat ein Tochterunternehmen in Deutschland. Diese Tochter ist operativ zwar unabhängig, für die angebotenen Produkte ist jedoch weiterhin das Mutterunternehmen zuständig. Nun ereignet sich bei der deutschen Tochter ein Cybersicherheitsvorfall, weil der angebotene Cloud-Computing-Dienst nicht den Anforderungen der NIS-2-RL entsprechend gesichert war. Zuständig für diesen Vorfall ist die österreichisches Behörde.

Das ist auch insofern von Bedeutung, als dass die kommenden innerstaatlichen Umsetzungen doch voneinander abweichen könnten, auch hinsichtlich des Strafrahmens.[136]

7.3. Geldbußen (Artikel 34 NIS-2-RL)

7.3.1. Strafrahmen

Eine wesentliche Änderung, die die NIS-2-RL im Vergleich zur bestehenden Rechtslage (NIS-RL und NISG) mit sich bringt und die ihre Relevanz für die Unternehmenspraxis maßgeblich erhöhen wird, ist der in Artikel 34 Absätze 4 und 5 leg cit verankerte, im Vergleich zur NIS-1-RL deutlich angehobene Strafrahmen. Gemeinsam mit der Anordnung des Artikel 34 Absatz 1 NIS-2-RL, wonach die Mitgliedstaaten sicherstellen sollen, *„dass die Geldbußen […] unter Berücksichtigung der Umstände des Einzelfalls wirksam, verhältnismäßig und abschreckend sind"*, bauen Artikel 34 Absätze 4 und 5 NIS-2-RL eine erhebliche finanzielle Drohkulisse auf, die wesentliche und wichtige Einrichtungen zur Cybersicherheits-Compliance motivieren soll.

Zwar verlangt(e) auch Artikel 21 NIS-1-RL, dass die von den Mitgliedstaaten 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 österreichische Gesetzgeber nutzt den daraus resultierenden Umsetzungsspielraum, um – nicht zuletzt im Vergleich zum Sanktionssystem der DSGVO, das zum Zeitpunkt der Erlassung des NISG bereits in Kraft stand – , etwas vorsichtig ausgedrückt, einer Überspannung der finanziellen Belastung der Normadressaten vorzubeugen.[137] Gemäß § 26 Absatz 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"*; dass § 26 Absatz 1 letzter Satz NISG den Anforderungen des Artikel 21 NIS-1-RL (*„wirksam, angemessen und abschreckend"*) gerecht wird, darf bezweifelt werden.

Es waren derartige Umsetzungsmängel, die den Unionsgesetzgeber zur Neufassung des unionalen Cybersicherheitsrechts durch die NIS-2-RL bewogen.[138] Künftig werden für Verstöße gegen die NIS-Cybersicherheitspflichten nicht Strafen in Höhe von bis zu 50.000,– oder bis zu 100.000,– Euro, sondern gemäß Artikel 34 Absätze 4 und 5 NIS-2-RL Geldbußen *„mit einem Höchstbetrag von mindestens 10 000 000EUR"*[139] bzw *„mit einem Höchstbetrag von mindestens 7 000 000EUR"*[140] fällig.

Der Strafrahmen hängt dabei davon ab, ob die Sanktion eine wesentliche oder eine wichtige Einrichtung treffen soll. Gegen wesentliche Einrichtungen dürfen Strafen bis zu 10.000.000,– Euro oder bis zu *„einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens"*, verhängt werden, je nachdem, welcher Betrag höher ist (Artikel 34 Absatz 4 NIS-2-RL). Über wichtige Einrichtungen kann die Behörde Geldbußen *„mit einem Höchstbetrag von mindestens 7 000 000EUR oder mit einem Höchst-*

136 Siehe zum Strafrahmen sogleich unter 7.3.1.

137 Vgl in diesem Zusammenhang *Kristoferitsch/Lachmayer*, ecolex 2020, 77; abschwächend *B. Müller* in Anderl et al, NISG § 26 NISG Rz 1.

138 Vgl Erwägungsgrund 4 f NIS-2-RL.

139 Artikel 34 Absatz 4 NIS-2-RL.

140 Artikel 34 Absatz 5 NIS-2-RL.

betrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens " verhängen, wiederum je nachdem, welcher Betrag höher ist (Artikel 34 Absatz 5 NIS-2-RL).

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 Unternehmen als Normadressaten fokussiert. Er bedient sich damit eines Konzepts, das etwa auch aus der DSGVO bekannt ist. Der Wandel zwischen NIS-1 und NIS-2 wird deutlich, kontrastiert man die Sanktionsbestimmung des Artikel 21 NIS-1-RL mit jener des Artikel 34 NIS-2-RL. Während erstere bloß davon spricht, dass die Mitgliedstaaten *„Vorschriften über Sanktionen für Verstöße gegen die nach dieser Richtlinie erlassenen nationalen Bestimmungen* " erlassen, ohne einen Strafadressaten zu nennen, lautet die Marginalrubrik des Artikel 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 in der Hauptsache Unternehmen, ein Umstand, der entsprechend hohe Strafrahmen erforderlich macht.

Es ist daher insbesondere davon auszugehen, dass es für die Verhängung von Geldstrafen gemäß der NIS-2-RL künftig nicht mehr erforderlich sein wird, dass der Verstoß gegen Cybersicherheitspflichten einer bestimmten natürlichen Person im Unternehmen angelastet wird.[141] Persönliches Verschulden eines konkreten Entscheidungsträgers dürfte sich damit – sofern der österreichische Gesetzgeber die NIS-2-RL ordnungsgemäß umsetzt – für die Verhängung einer Geldstrafe gegen ein Unternehmen erübrigen.[142]

Trotz der prohibitiven Strafhöhen haben Behörden bei der Verhängung von Geldstrafen auf der Grundlage von Artikel 34 NIS-2-RL aber selbstverständlich den Grundsatz der Verhältnismäßigkeit zu beachten; Entsprechendes ordnet Artikel 34 Absatz 1 NIS-2-RL auch explizit an,[143] würde sich aber ebenso aus allgemeinen Grundsätzen ergeben. Der Verhältnismäßigkeitsgrundsatz strukturiert die diesbezügliche behördliche Entscheidungsfindung in zweierlei Hinsicht: Einerseits muss sich bereits die Verhängung der Geldbuße an sich als verhältnismäßig erweisen; dies kann insbesondere bei bloß geringfügigen, leicht fahrlässigen Verstößen zweifelhaft sein. Andererseits hat die Behörde die konkrete Strafhöhe unter Berücksichtigung von Gesichtspunkten wie der finanziellen Verhältnisse der wesentlichen und wichtigen Einrichtung festzulegen;[144] Geldbußen, die aufgrund ihrer Höhe für die betreffende wesentliche oder wichtige Einrichtung ruinös wirken, wären unverhältnismäßig und damit unzulässig.

7.3.2. Strafbemessung

Innerhalb des Strafrahmens der Artikel 34 Absätze 4 und 5 NIS-2-RL hat die Behörde die konkret zu verhängende Strafe anhand der Kriterien des Artikel 32 Absatz 7 NIS-2-RL zu bemessen.[145] Artikel 32 Absatz 7 NIS-2-RL enthält dabei unterschiedliche Gesichtspunkte, die als Strafzumessungsgründe auf Basis der Handlungen der betreffenden wesentlichen oder wichtigen Einrichtung zu einer Erhöhung oder Absenkung der Strafe führen können. Die Behörde hat bei der Strafzumessung – im Rahmen des Grundsatzes der Verhältnismäßigkeit[146] – Folgendes gebührend zu berücksichtigen:

- *„die Schwere des Verstoßes und die Wichtigkeit der Bestimmungen, gegen die verstoßen wurde, wobei u. a. Folgendes immer als schwerer Verstoß anzusehen ist:* "[147]
  - *„wiederholte Verstöße* ",
  - *„eine unterlassene Meldung oder Behebung von erheblichen Sicherheitsvorfällen* ",
  - *„eine Nichtbehebung von Mängeln nach verbindlicher Anweisung der zuständigen Behörden* ",

141 Vgl nur die Schlussanträge des Generalanwalts Campos Sánchez-Bordona in der Rs C-807/21 (*Deutsche Wohnen SE*).

142 Das NISG setzt gegenwärtig für die Verhängung von Geldstrafen persönliches Verschulden noch voraus. Siehe *B. Müller* in Anderl et al, NISG § 26 NISG Rz 5.

143 Siehe auch Erwägungsgrund 127 NIS-2-RL.

144 Siehe zur Strafbemessung sogleich unter 7.2.2.

145 Artikel 34 Absatz 3 NIS-2-RL.

146 Siehe dazu bereits 7.2.1.

147 Artikel 32 Absatz 7 littera a NIS-2-RL.

- *„die Behinderung von Prüfungen oder Überwachungstätigkeiten, die nach der Feststellung eines Verstoßes von der zuständigen Behörde angeordnet wurden, sowie"*
- „Übermittlung falscher oder grob verfälschender Informationen in Bezug auf Risikomanagementmaßnahmen im Bereich der Cybersicherheit oder Berichtspflichten gemäß den Artikeln 21 und 23."

- *„die Dauer des Verstoßes";*[148]
- *„einschlägige frühere Verstöße der betreffenden Einrichtung";*[149]
- *„der verursachte materielle oder immaterielle Schaden, darunter finanzieller oder wirtschaftlicher Verlust, Auswirkungen auf andere Dienste und die Zahl der betroffenen Nutzer";*[150]
- *„etwaiger Vorsatz oder etwaige Fahrlässigkeit des Urhebers des Verstoßes";*[151]
- *„von der Einrichtung ergriffene Maßnahmen zur Verhinderung oder Minderung des materiellen oder immateriellen Schadens";*[152]
- *„Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren";*[153]
- *Umfang der Zusammenarbeit der verantwortlichen natürlichen oder juristischen Personen mit den zuständigen Behörden.*[154]

Sofern die betreffende Geldstrafe gegen eine Person verhängt werden soll, *„bei der es sich nicht um ein Unternehmen handelt", folgen aus Erwägungsgrund 130 NIS-2-RL weitere Vorgaben für die Festsetzung der Strafhöhe. Die zuständige Behörde hat „bei der geeigneten Bemessung der Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung" zu tragen.*

Anhand der Strafzumessungsgründe des Artikel 32 Absatz 7 NIS-2-RL wird umgehend deutlich, dass Unternehmen, sofern sie ihr Cybersicherheits-Compliance-Projekt ernsthaft und sorgfältig vorantreiben, von hohen Geldstrafen weitestgehend verschont bleiben werden. Dies gilt selbst dann, wenn trotz allem ein erheblicher Sicherheitsvorfall eintreten sollte. Hat das Unternehmen die dem Stand der Technik entsprechenden Risikomanagementmaßnahmen gemäß Artikel 21 NIS-2-RL ergriffen und bemüht es sich im Fall des Falles um ernsthafte Schadensbegrenzung und Zusammenarbeit mit der Behörde, scheiden prohibitive Geldstrafen aus. Insbesondere der Verweis auf *„genehmigte[…] Verhaltensregeln oder genehmigte[…] Zertifizierungsverfahren"* lässt erkennen, dass Unternehmen, die sich entsprechend zertifizieren lassen und anhand der entsprechenden Standards vorgehen, kaum etwas zu befürchten haben.

7.4. Verantwortlichkeit der Leitungsorgane (Artikel 20 Absatz 1 NIS-2-RL)

Die besondere Brisanz, die die NIS-2-RL für die unternehmerische Praxis entfalten wird, folgt zu wesentlichen Teilen aber auch daraus, dass sie die Verantwortlichkeit für die Einhaltung der oben dargelegten unternehmerischen Pflicht zur Setzung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit bei den zuständigen Entscheidungsträgern verortet.[155] Denn die Verantwortlichkeit für die Einhaltung der Verpflichtungen zur Ergreifung von Risikomanagementmaßnahmen liegt gemäß Artikel 20 Absatz 1 NIS-2-RL bei den *„Leitungsorgane[n] wesentlicher und wichtiger Einrichtungen"*. Sie haben gemäß Artikel 20 Absatz 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 auch entsprechende Sanktionen: Gemäß Artikel 20 Absatz 1 NIS-2-RL stellen die Mitgliedstaaten sicher, dass die Leitungsorgane für Verstöße durch ihre Einrichtungen verantwortlich gemacht werden können. Fraglich bleibt dabei, was unter dem Begriff des „Leitungsorgans" zu verstehen ist.

148 Artikel 32 Absatz 7 littera b NIS-2-RL.
149 Artikel 32 Absatz 7 littera c NIS-2-RL.
150 Artikel 32 Absatz 7 littera d NIS-2-RL.
151 Artikel 32 Absatz 7 littera e NIS-2-RL.
152 Artikel 32 Absatz 7 littera f NIS-2-RL.
153 Artikel 32 Absatz 7 littera g NIS-2-RL.
154 Artikel 32 Absatz 7 littera h NIS-2-RL.
155 Siehe zu dieser bereits unter 6.3.

Der Begriff des „Leitungsorgans" findet in der NIS-2-RL an drei Stellen Erwähnung:[156] in Erwägungsgrund 137 sowie in Artikel 20 Absätze 1 und 2 NIS-2-RL. Gemäß Erwägungsgrund 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 *„auf Ebene der wesentlichen und wichtigen Einrichtungen ein hohes Maß an Verantwortung für die Risikomanagementmaßnahmen und die Berichtspflichten im Bereich der Cybersicherheit"* gewährleistet werden. Gemäß Artikel 20 Absatz 1 NIS-2-RL stellen die Mitgliedstaaten eben sicher, *„dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen […] ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und für Verstöße […] durch die betreffenden Einrichtungen verantwortlich gemacht werden können"*. Artikel 20 Absatz 2 NIS-2-RL enthält eine Verpflichtung für Leitungsorgane, an Cybersicherheits-Schulungen teilzunehmen.

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

So wird der Begriff des „Leitungsorgans" in anderen Sekundärrechtsakten, wie Artikel 3 Nummer 30 Verordnung 2022/2554/EU über die digitale operationale Resilienz im Finanzsektor, legaldefiniert. Die Verordnung 2022/2554/EU stellt nach Erwägungsgrund 28 NIS-2-RL einen sektorspezifischen Rechtsakt der Union im Sinne des Artikel 4 NIS-2-RL hinsichtlich Finanzunternehmen dar, *„in denen Risikomanagementmaßnahmen oder Berichtspflichten im Bereich der Cybersicherheit vorgesehen sind"*, die in ihrer Wirkung den NIS-2-Pflichten entsprechen.

Artikel 3 Nummer 30 VO 2022/2554/EU über die digitale operationale Resilienz im Finanzsektor verweist in seiner Definition des „Leitungsorgans" seinerseits zunächst als erste Alternative auf die Begriffsdefinitionen in den RL 2014/65/EU, RL 2013/36/EU und RL 2009/65/EG sowie in den VO 909/2014/EU und VO 2016/1011/EU. Allen genannten Sekundärrechtsakten ist dabei gemeinsam, dass sie ein funktionelles Begriffsverständnis zugrunde legen. Ein „Leitungsorgan" zeichnet sich dadurch aus, dass es Strategie, Ziele und Gesamtpolitik des Unternehmens festlegt,[157] dass ihm die Personen angehören, die die Geschäfte des Unternehmens tatsächlich führen[158] und dass ihm die Letztentscheidungsbefugnis[159] zukommt.

Artikel 3 Nummer 30 Verordnung 2022/2554/EU setzt aber auch selbst als zweite Begriffsalternative des „Leitungsorgans" ein derartiges funktionelles Verständnis 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"*.

Als im Sinne der NIS-2-RL sektorspezfischer Cybersicherheits-Rechtsakt geht die Verordnung 2022/2554/EU damit unzweifelhaft von einem funktionellen Verständnis des Begriffs des „Leitungsorgans" aus. Aufgrund des Umstandes, dass die NIS-2-RL die Verordnung 2022/2554/EU für den Finanzsektor zu ihrem „Pendant" erklärt, muss der entsprechenden Legaldefinition der Verordnung 2022/2554/EU für die Auslegung des Begriffs des Leitungsorgans in der NIS-2-RL erhöhte Bedeutung beigemessen werden. Es ist deswegen davon auszugehen, dass auch die NIS-2-RL den Begriff des „Leitungsorgans" funktionell verwendet.

Ein derartiges, systematisch angezeigtes funktionelles Verständnis des Begriffs des „Leitungsorgans" lässt sich weiters auch aus der Teleolo-

156 Die im Anhang II NIS-2-RL genannten *„Flughafenleitungsorange" sowie die „Leitungsorgane von Häfen" bleiben an dieser Stelle unberücksichtigt, weil diese Begriffe eine andere Stoßrichtung aufweisen.*

157 Artikel 4 Absatz 1 Nummer 36 RL 2014/65/EU; Artikel 3 Absatz 1 Nummer 7 RL 2013/36/EU; Artikel 2 Absatz 1 Nummer 45 VO 909/2014/EU; Artikel 3 Absatz 1 Nummer 20 VO 2016/1011/EU.

158 Artikel 4 Absatz 1 Nummer 36 RL 2014/65/EU; Artikel 3 Absatz 1 Nummer 7 RL 2013/36/EU; Artikel 2 Absatz 1 Nummer 45 VO 909/2014/EU; Artikel 3 Absatz 1 Nummer 20 2016/1011/EU.

159 Artikel 2 Absatz 1 littera s RL 2009/65/EG.

gie der NIS-2-RL, dem das Unionsrecht prägende Auslegungsgrundsatz *effet utile* und nicht zuletzt auch rechtsstaatlichen Prinzipien ableiten. Die NIS-2-RL will ein *„hohes gemeinsames Cybersicherheitsniveau in der Union"*[160] gewährleisten und stellt dies hinsichtlich der erfassten Einrichtungen 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 gewendet: 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 nicht ausreichend Rechnung getragen, würde man den Begriff des „Leitungsorgans" organisatorisch interpretieren und die Verantwortlichkeit für die Einhaltung der Cybersicherheits-Pflichten auch in jenen Fällen pauschal ausschließlich beim Geschäftsführungsorgan verorten, in denen dieses etwa mittels Gesellschafterweisung umfassend gesteuert wird.

Das derart erzielte Auslegungsergebnis des Begriffs des „Leitungsorgans" lässt sich schließlich wieder auf den Text der NIS-2-RL selbst zurückführen. Gemäß Artikel 32 Absatz 5 littera b NIS-2-RL sind als Ultima Ratio Berufsverbote über *„natürliche[…] Personen, die auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters für Leitungsaufgaben in dieser wesentlichen Einrichtung zuständig sind"*, zu verhängen. Hätte der Unionsgesetzgeber die Berufsverbote für alle „Leitungsorgane" vorsehen wollen, hätte er dies schlicht auch so anordnen können („über natürliche Personen, die als Leitungsorgane …"). Der Begriff des „Leitungsorgans" muss damit einen Inhalt aufweisen, der sich von der *„Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters"* unterscheidet.

Zudem korrelieren mit der Anordnung der Verantwortlichkeit der Leitungsorgane in Artikel 20 Absatz 1 NIS-2-RL eine Verpflichtung der Mitgliedstaaten in Artikel 32 Absatz 6 bzw Artikel 33 Absatz 5 in Verbindung mit Artikel 32 Absatz 6 NIS-2-RL, sicherzustellen, *„dass jede natürliche Person, die für eine wesentliche 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 sicherstellen, *„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 gemäß Artikel 20 Absatz 1 NIS-2-RL *„für eine wesentliche Einrichtung verantwortlich"* ist, nicht bloß auf die Geschäftsführungs- bzw Vorstandsebene im Sinne des österreichischen Gesellschaftsrechts beziehen kann. Denn diesfalls bedürfte es der zusätzlichen Anordnung *„oder auf der Grundlage ihrer Vertretungsbefugnis"* nicht.

Letztlich liegt der NIS-2-RL 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 Artikel 32 Absatz 6 bzw Artikel 33 Absatz 5 in Verbindung mit Artikel 32 Absatz 6 NIS-2-RL und der darin festgelegten Haftung auf alle Fälle eine gewisse Art der „Verantwortlichkeit" der Entscheidungsträger hergestellt.

Vorbehaltlich der noch ausstehenden Umsetzung durch den österreichischen Gesetzgeber lässt sich daher festhalten, dass die Verantwortlichkeit für die Einhaltung der NIS-Cybersicherheitspflichten künftig je nach der konkreten gesellschaftsrechtlichen Aufgabenverteilung unterschiedliche Organe treffen wird können. Wenn man daher fragt, wer das verantwortliche „Leitungsorgan" ist, so muss die Antwort lauten: Es kommt darauf an … wer eben die maßgeblichen Entscheidungen in der Gesellschaft trifft und das Unternehmen tatsächlich leitet.

Das können anstelle der oder neben den Geschäftsführungs- und Vertretungsorganen bei

160 Vgl nur die Langbezeichnung der NIS-2-RL.

entsprechender Einflussmöglichkeit etwa der Aufsichtsrat oder die GmbH-Generalversammlung sein, bspw wenn die AG-Satzung ersterem gewisse einschlägige Mitwirkungsrechte einräumt[161] oder einzelne Personen in der GmbH-Generalversammlung mittels des gesellschaftsrechtlichen Weisungsrechts gegenüber der Geschäftsführung *de facto* – und damit „tatsächlich" – die Gesellschaft 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" gemäß Artikel 20 Absatz 1 NIS-2-RL die Verantwortung tragen. Oder aber, weil sie als *„natürliche Person"* gemäß Artikel 32 Absatz 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 Richtlinie 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"*. 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.

Beispiel

Ein mittelständisches österreichisches Chemieunternehmen mit 70 Mitarbeitern und 9 Mio Euro Umsatz fällt aufgrund Artikel 2 Absatz 1 in Verbindung mit Nummer 3 Anhang II NIS-2-RL in Verbindung mit der KMU-Empfehlung der Kommission in den Anwendungsbereich der NIS-2-RL. Es wird als GmbH betrieben, wobei der Hauptgesellschafter 85 % der Geschäftsanteile hält.
Der Hauptgesellschafter ist zwar nicht selbst Geschäftsführer, aber in erheblichem Ausmaß in sämtliche Agenden der Geschäftsführung durch den Fremdgeschäftsführer involviert.
Der Fremdgeschäftsführer muss regelmäßig im Einverständnis mit dem Hauptgesellschafter vorgehen und de facto alle bedeutenderen Fragen seiner Geschäftsführung von diesem genehmigen lassen.
Aufgrund der Umstände, dass der Hauptgesellschafter des Chemieunternehmens dessen Strategie, Ziele und Gesamtpolitik im Rahmen der Kompetenzen der Generalversammlung festlegt, dass ihm als Hauptgesellschafter mit entsprechendem Weisungsrecht gegenüber der Geschäftsführung die Letztentscheidungsbefugnis in der Unternehmensführung zukommt sowie, dass tatsächlich er die Geschäfte des Unternehmens führt, ist der Hauptgesellschafter als „Leitungsorgan" im Sinne der NIS-2-RL zu qualifizieren. Für die Einhaltung der NIS-2-Cybersicherheitspflichten trägt er die Verantwortung.

161 Vgl § 95 Absatz 5 AktG; *Eckert/Schopper in Artmann/Karollus, AktG II*[6] § 95 AktG Rz 65 f.

7.5.„Tätigkeitsverbote" für natürliche Personen

Besondere Beachtung verdient weiters die in Artikel 32 Absatz 5 littera b NIS-2-RL vorgesehene Möglichkeit der Behörde, *„natürlichen Personen, die auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters für Leitungsaufgaben in dieser wesentlichen Einrichtung zuständig sind, vorübergehend [zu] untersagen, Leitungsaufgaben in dieser Einrichtung wahrzunehmen"*. Diese *„Aufsichts- und Durchsetzungsmaßnahme[…]"* gilt zwar nur für wesentliche Einrichtungen und als Ultima Ratio; in Anbetracht der erheblichen Auswirkungen, die die Maßnahme für den Fall ihrer Verhängung entfaltet, ist sie in ihrer Bedeutung aber nicht geringzuschätzen. Gemäß Erwägungsgrund 133 NIS-2-RL haben die befristeten Tätigkeitsverbote auch explizit den Zweck, entsprechende *„Abschreckungskraft"* zu entfalten.

Voraussetzung für die Erlassung von Tätigkeitsverboten gemäß Artikel 32 Absatz 5 littera b NIS-2-RL ist zunächst, dass die Behörde Durchsetzungsmaßnahmen gemäß Artikel 32 Absatz 4 littera a-d und f NIS-2-RL ergriffen hat, diese sich jedoch als unwirksam erwiesen haben. Bei den genannten Durchsetzungsmaßnahmen handelt es sich um die Herausgabe von Warnungen,[162] die Erlassung verbindlicher Anweisungen,[163] die Anweisung an die betreffende Einrichtung, einen Verstoß gegen NIS-Pflichten einzustellen,[164] die Anweisung an die betreffende Einrichtung, ihre Risikomanagementmaßnahmen mit Artikel 21 NIS-2-RL in Einklang zu bringen bzw ihren Berichtspflichten gemäß Artikel 23 NIS-2-RL nachzukommen,[165] sowie die Anweisung, im Rahmen einer Sicherheitsprüfung formulierte Empfehlungen umzusetzen.[166]

Sodann muss die Behörde gemäß Artikel 32 Absatz 5 Unterabsatz 1 NIS-2-RL nach Erkennen der Unwirksamkeit der ursprünglichen Maßnahme und damit der Untätigkeit der betreffenden Einrichtung eine entsprechende Nachfrist setzen, *„innerhalb derer die wesentliche Einrichtung die erforderlichen Maßnahmen ergreifen muss, um die Mängel zu beheben oder die Anforderungen dieser Behörden zu erfüllen"*. Lediglich im Fall, dass auch diese Nachfristsetzung erfolglos bleibt, darf die Behörde gemäß Artikel 32 Absatz 5 littera b NIS-2-RL zeitlich befristete Tätigkeitsverbote gegen die natürlichen Leitungspersonen verhängen.

Ausweislich Erwägungsgrund 133 NIS-2-RL verkennt die Richtlinie dabei nicht, dass es sich bei den vorübergehenden Tätigkeitsverboten um eine gravierende Sanktion handelt. *„Angesichts ihrer Schwere und ihrer Auswirkungen"* sollten sie deswegen *„lediglich im Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden"*. Hierzu soll auch die Frage zählen, *„ob der Verstoß vorsätzlich oder fahrlässig begangen wurde*; ebenso sind die *„zur Verhinderung oder Minderung des materiellen oder immateriellen erlittenen Schadens ergriffenen Maßnahmen" zu berücksichtigen.* Die vorübergehenden Tätigkeitsverbote sollten deswegen *„nur als letztes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden"*.

Bereits der Umstand, dass sich die zeitlichen Tätigkeitsverbote in der Bestimmung des Artikel 32 NIS-2-RL über die *„Aufsichts- und Durchsetzungsmaßnahmen"* findet, wird auch der Umstand deutlich, dass es sich dabei weniger um Sanktions-, als vielmehr um Zwangsmittel zur Herstellung eines rechtlich gebotenen Zustandes handelt. Gemäß Erwägungsgrund 133 sollen sie deswegen *„nur so lange [verhängt werden], bis die betreffende Einrichtung die erforderlichen Maßnahmen zur Behebung der Mängel ergreif[t]*

162 Artikel 32 Absatz 4 littera a NIS-2-RL: *„Warnungen über Verstöße gegen diese Richtlinie durch die betreffenden Einrichtungen herauszugeben"*.

163 Artikel 32 Absatz 4 littera b NIS-2-RL: *„verbindliche Anweisungen zu erlassen, auch in Bezug auf Maßnahmen, die zur Verhütung oder Behebung eines Sicherheitsvorfalls erforderlich sind, sowie Fristen für die Durchführung dieser Maßnahmen und für die Berichterstattung über ihre Durchführung zu setzen, oder Anordnungen zu erlassen, um diese Einrichtungen aufzufordern, die festgestellten Mängel oder die Verstöße gegen diese Richtlinie zu beheben"*.

164 Artikel 32 Absatz 4 littera c NIS-2-RL: *„die betreffenden Einrichtungen anzuweisen, das gegen diese Richtlinie verstoßende Verhalten einzustellen und von Wiederholungen abzusehen"*.

165 Artikel 32 Absatz 4 littera d NIS-2-RL: *„die betreffenden Einrichtungen anzuweisen, entsprechend bestimmten Vorgaben und innerhalb einer bestimmten Frist sicherzustellen, dass ihre Risikomanagementmaßnahmen im Bereich der Cybersicherheit mit Artikel 21 im Einklang stehen, bzw. die in Artikel 23 festgelegten Berichtspflichten zu erfüllen"*.

166 Artikel 32 Absatz 4 littera f NIS-2-RL: *„die betreffenden Einrichtungen anzuweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen"*.

oder die Anforderungen der zuständigen Behörde, auf die sich solche vorübergehenden Aussetzungen oder Verbote beziehen, erfüll[t]".
Ist die wesentliche Einrichtung ihrer Verpflichtung nachgekommen, derentwegen die ursprüngliche Durchsetzungsmaßnahme erlassen wurde, muss das Tätigkeitsverbot damit aufgehoben werden, womit die betroffenen natürlichen Personen ihre Tätigkeit im Unternehmen wieder aufnehmen dürfen.

Beispiel

Eine gemäß Artikel 32 Absatz 2 littera b NIS-2-RL durchgeführte Sicherheitsprüfung in der Energie-AG, die als wesentliche Einrichtung im Sinne der NIS-2-RL zu qualifizieren ist, hat erhebliche Cybersicherheitsmängel offenbart. Die zuständige Behörde formuliert deswegen Empfehlungen an die Energie-AG, bestimmte Maßnahmen binnen 6 Monaten umzusetzen.
Nach Verstreichen der 6-Monats-Frist stellt die Behörde fest, dass die Energie-AG die Empfehlungen noch immer nicht umgesetzt hat. Die Behörde setzt dem Unternehmen deswegen gemäß Artikel 32 Absatz 5 NIS-2-RL eine Nachfrist von 2 Monaten, um den Empfehlungen doch noch zu entsprechen. Sollte auch diese Frist verstreichen, ist die Behörde gemäß Art 32 Absatz 5 littera b NIS-2-RL befugt, den Vorständen der Energie-AG ein vorübergehendes Tätigkeitsverbot auszusprechen. Dieses hat den Zweck, die Energie-AG dazu zu bewegen, den rechtlich geforderten Zustand herzustellen. Sobald die Cybersicherheitsmängel von der Energie-AG behoben wurden, hat die Behörde das Tätigkeitsverbot deswegen auch aufzuheben, womit die Vorstände wieder Leitungsaufgaben in der Energie-AG wahrnehmen dürfen.

7.6. Sanktionen gemäß Artikel 36 NIS-2-RL

Komplettiert wird das Sanktionsregime der RL schließlich durch die Anordnung des Artikel 36 NIS-2-RL, wonach die Mitgliedstaaten Vorschriften über Sanktionen erlassen sollen, *„die bei Verstößen gegen die gemäß dieser Richtlinie erlassenen nationalen Maßnahmen zu verhängen sind"*. *„Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein"*, wie auch die Mitgliedstaaten *„alle für die Anwendung der Sanktionen erforderlichen Maßnahmen"* treffen sollen. Fraglich bleibt, in welchem Verhältnis die Bestimmung des Artikel 36 NIS-2-RL etwa zur Vorschrift des Artikel 34 Absatz 1 NIS-2-RL über die Verhängung von Geldbußen steht.

Auf den ersten Blick könnte man aufgrund des Wortlautes meinen, die Bestimmungen hätten einen unterschiedlichen Anwendungsbereich. Die Geldbußen des Artikel 34 Absatz 1 NIS-2-RL würden Verstöße gegen die Pflichten der NIS-2-RL sanktionieren (*„Geldbußen, die gemäß dem vorliegenden Artikel gegen wesentliche und wichtige Einrichtungen in Bezug auf Verstöße gegen diese Richtlinie verhängt werden"*), während Artikel 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"*).

Diesbezüglich ist aber problematisch, dass ein Verstoß gegen die Bestimmungen der NIS-2-RL durch nicht-staatliche Einrichtungen[167] gar nicht möglich ist. Richtlinienadressaten sind die Mitgliedstaaten; eine unmittelbare Wirksamkeit von Richtlinienbestimmungen kann nur zulasten des säumigen Mitgliedstaats, nicht jedoch zulasten Privater eintreten.[168] Aufgrund des Artikel 34 Absatz 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 gemäß Artikel 34 NIS-2-RL hauptsächlich gegen nicht-staatliche wesentliche und wichtige Einrichtungen richten. Die Anordnung des Artikel 34 Absatz 1 NIS-2-RL (*„Geldbußen, die gemäß dem vorliegenden*

167 Aufgrund des Umstandes, dass die Mitgliedstaaten die Adressaten der NIS-2-RL sind, können staatliche Einrichtungen (etwa *„Einrichtungen der öffentlichen Verwaltung"* im Sinne der Nummer 10 des Anhang I NIS-2-RL) hingegen schon gegen die Richtlinie selbst verstoßen. Siehe *Vcelouch* in Jaeger/Stöger, EUV/AEUV Art 288 AEUV Rz 34 ff.

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

Artikel gegen wesentliche und wichtige Einrichtungen in Bezug auf Verstöße gegen diese Richtlinie verhängt werden") lässt sich folglich nicht dahingehend deuten, dass sie hauptsächlich Geldbußen gegen staatliche Einrichtungen adressieren wolle.

Zusammenfassend dürfte es sich bei der in Artikel 34 Absatz 1 NIS-2-RL enthaltenen Formulierung *„Geldbußen, die […] in Bezug auf Verstöße gegen diese Richtlinie verhängt werden"*[169] um ein Redaktionsversehen handelt. Es ist davon auszugehen, dass auch die gemäß Artikel 34 NIS-2-RL verhängten Geldbußen Verstöße gegen die nationalen Umsetzungsbestimmungen, und nicht die RL selbst sanktionieren. Welcher Anwendungsbereich damit für die Bestimmung des Artikel 36 NIS-2-RL verbleibt, ist fraglich.

7.7. Zwischenresümee

Die NIS-2-RL stellt auch das Sanktionensystem im Cybersicherheitsrecht der EU auf neue Beine. Nachdem die Umsetzung der NIS-1-RL durch die mitgliedstaatlichen Gesetzgeber dem NIS-Regime nicht die nötige Wirkungskraft verlieh, macht der Unionsgesetzgeber nun ernst.

Im Gegensatz zur NIS-1-RL finden sich in der NIS-2-RL konkrete Strafrahmen, die in ihrer Höhe an die DSGVO erinnern. Zudem werden die Mitgliedstaaten verpflichten, Verantwortlichkeiten bzw Haftungen von Leitungsorganen und Leitungspersonen für Verstöße gegen die NIS-2-Cybersicherheitspflichten vorzusehen. Im äußersten Fall hält die Richtlinie Tätigkeitsverbote bereits.

Angesichts der Schwere der drohenden Sanktionen ist es für wesentliche und wichtige Einrichtungen geboten, ihr NIS-2-Compliance-Projekt bereits zum gegenwärtigen Zeitpunkt in Angriff zu nehmen und sorgfältig voranzutreiben. Millionen- und Milliardenstrafen werden hauptsächlich jenen Unternehmen drohen, die ihre Cybersicherheitspflichten gröblich vernachlässigen.

169 Derartiges ordnet auch die englische Sprachfassung des Artikel 34 Absatz 1 NIS-2-RL an: *„Member States shall ensure that the administrative fines imposed […] in respect of infringements of this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case"*.

8. Ausblick auf die innerstaatliche Umsetzung (NISG-Novelle und Vollzugspraxis)

8.1. Kein „Gold Plating" zu erwarten

Zum gegenwärtigen Zeitpunkt liegt noch kein Entwurf des österreichischen Gesetzgebers für die innerstaatliche Umsetzung der NIS-2-RL vor. Es lassen sich deswegen derzeit kaum konkrete Aussagen dahingehend treffen, wie der österreichische Gesetzgeber die ihm von der NIS-2-RL belassenen Spielräume ausfüllen wird und wie deswegen das Pflichtenprogramm österreichischer wesentlicher und wichtiger Einrichtungen ab (voraussichtlich) 18.10.2024 im Detail aussieht.

Berücksichtigt man allerdings die Gesetzgebungspraxis der letzten Jahre und nicht zuletzt auch das derzeit in Geltung stehende NISG,[170] so darf zumindest davon ausgegangen werden, dass es der österreichische Gesetzgeber bei der in Artikel 5 NIS-2-RL angesprochenen *„Mindestharmonisierung"* belassen wird. Von einer Übererfüllung („Gold Plating") der unionsrechtlichen Anforderung an die unternehmerische Cybersicherheit ist nicht auszugehen.

8.2. Verwaltungsstrafen/Vollzugspraxis

Weiters erscheint es deswegen als geradezu ausgeschlossen, dass der österreichische Gesetzgeber von der durch Artikel 34 Absatz 4 und 5 NIS-2-RL eröffneten Möglichkeit (*argumentum*: *„mit einem Höchstbetrag von mindestens"*) Gebrauch macht, höhere als die dort genannten Strafrahmen vorzusehen. Ebenso wenig ist zu erwarten, dass die ausstehende Novelle auf Basis des Artikel 36 NIS-2-RL scharfe innerstaatliche Sanktionsinstrumente im NISG verankern wird. Die Cybersicherheits-Geldbußen werden sich daher aller Voraussicht nach innerhalb des durch Artikel 34 Absatz 4 und 5 NIS-2-RL gesteckten, ohnedies ausreichend hohen Rahmens von 10 sowie 7 Mio Euro bzw 2 % sowie 1,4 % des weltweiten Konzernumsatzes bewegen.

Sucht man Anhaltspunkte hinsichtlich jenes Strafausmaßes, das von wesentlichen und wichtigen Einrichtungen bei Verstoß gegen die NIS-Cybersicherheitspflichten im Falle ihrer behördlichen Bestrafung konkret zu erwarten ist, könnte sich die bisherige Entscheidungspraxis der Datenschutzbehörde (DSB) als aufschlussreich erweisen. Derzeit liegt die Zahl der Strafbescheide, die die DSB aufgrund von Verstößen gegen die DSGVO verhängt, bei rund 30 pro Jahr (2022: 28 Geldbußen in Höhe von insgesamt *„knapp über EUR 50.000"* sowie 7 Verwarnungen).[171]

Es darf damit davon ausgegangen werden, dass bei ordnungsgemäßer Aufsetzung und Durchführung des NIS-2-Compliance-Projekts im Fall, dass innerhalb einer wesentlichen und wichtigen Einrichtung leicht fahrlässig gegen Cybersicherheitspflichten verstoßen wird, die Behörde keine oder lediglich sehr niedrige Geldstrafen verhängt. Sofern Unternehmen ihre Cybersicherheitspflichten allerdings gravierend vernachlässigen, könnten sie sich durchaus mit drakonischen Strafen – bspw in der Art der knapp 10 Mio Euro Geldbuße gegen die Post AG[172] – konfrontiert sehen.

8.3. Anwendungsbereich: Ende des „State driven Approach"?

Zu erwarten ist, dass die NIS-2-Umsetzungsnovelle das Ende des „State driven Approach" im NISG herbeiführen wird. Derzeit fallen Betreiber wesentlicher Dienste auch bei Erfüllung sämtlicher Kriterien nur dann in den Anwendungsbereich des NISG, wenn sie durch Bescheid des Bundeskanzlers als „Betreiber wesentlicher Dienste" ermittelt werden. Dem Bescheid kommt konstitutive Wirkung zu; erst dessen Rechtskraft führt dazu, dass ein spezifischer Infrastrukturbetreiber zu einem „Betreiber wesentlicher Dienste" im Sinne

170 Vgl nur das Anti-Gold-Plating-Gesetz 2019, BGBl I 46/2019.

171 Siehe den Datenschutzbericht 2022 der DSB, 45 <https://www.dsb.gv.at/dam/jcr:ee7b155a-0a1f-4d00-98e9-902314c7022d/Datenschutzbericht_2022.pdf> (abgerufen am 15.9.2023).

172 Siehe *Der Standard Online v 28.9.2021, Post AG muss für Datenskandal 9,5 Millionen Euro Strafe zahlen <https://www.derstandard.at/story/2000130022725/post-ag-muss-fuer-datenskandal-9-5-millionen-euro-strafe> (abgerufen am 15.9.2023).*

des NISG wird.[173]

Beim „State driven Approach" der Anwendungsbereichsfestlegung des NISG handelt(e) es sich um eine Eigenschöpfung des österreichischen Umsetzungsgesetzgebers; die NIS-1-RL sah Derartiges nicht verpflichtend vor. Vergleichsweise waren und sind Infrastrukturbetreiber in Deutschland auch bislang zur Selbsteinschätzung verpflichtet, ob sie in den Anwendungsbereich des NIS-Cybersicherheitsrechts fallen oder nicht („Provider driven Approach").[174]

Für das NISG der NIS-2-RL ist nunmehr ebenso für Österreich ein Ende des „State driven Approach" zu erwarten. Aufgrund der erheblichen Ausweitung des Anwendungsbereichs und der ungemein größeren Anzahl an Unternehmen, die künftig als wesentliche oder wichtige Einrichtungen dem NIS-2-Cybersicherheitsrecht unterliegen werden, ist es vor dem Hintergrund des betreffenden Verwaltungsaufwands schwer vorstellbar, dass es der Gesetzgeber bei der bescheidmäßigen Ermittlung jener Unternehmen belässt, die unter das NISG fallen.

173 *Heußler in Anderl et al, NISG § 16 NISG Rz 12.*
174 *Heußler in Anderl et al, NISG § 16 NISG Rz 1 f.*

9. NIS-2-Implementierung: DSGVO-Erfahrungen nutzen

Trotz des erheblichen Umsetzungsaufwandes, mit dem die NIS-2-RL wesentliche und wichtige Einrichtungen konfrontiert, bleibt diesen ein Lichtblick: Die NIS-2-RL ist hinsichtlich der Anforderungen, die sie an Unternehmen stellt (aber auch sonst), der DSGVO sehr ähnlich.

So entsprechen die NIS-2-Riskomanagementmaßnahmen konzeptionell den technischen und organisatorischen Maßnahmen (TOMs), zu deren Setzung Verantwortliche gemäß Artikel 32 DSGVO verpflichtet sind. Wie Artikel 33 DSGVO zur Meldung von *Data Breaches* innerhalb bestimmter Frist an die Behörde verpflichtet, sieht Artikel 23 NIS-2-RL künftig einen Prozess der Meldung von erheblichen Sicherheitsvorfällen vor. Gemäß Artikel 34 NIS-2-RL drohen ab 2024 Geldbußen, die klar jenen der DSGVO nachgebildet sind.

Wesentliche und wichtige Einrichtungen können deswegen bei der Aufsetzung des NIS-2-Cybersicherheits-Projekts 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, machen musste: Wer bis zum Tag des Anwendungsbeginnes damit wartet, seinen unternehmensbezogenen Pflichten nachzukommen, bezahlt dies unter Umständen teuer. Wesentliche und wichtige Einrichtungen sollten ihr NIS-2-Compliance-Projekt deswegen bereits jetzt starten, am 18.10.2024 wird es dafür zu spät sein.

10. Literaturverzeichnis

- Anderl et al (Hrsg), NISG (2019)
- Anderl/Müller/Pichler, Das österreichische Netz- und Informationssystemsicherheitsgesetz – Überblick und praktische Auswirkungen, in Paulus (Hrsg), Regulierungsrecht. Jahrbuch 2019 183
- Bergauer in Jahnel (Hrsg), Kommentar zur Datenschutz-Grundverordnung (Stand 1.12.2020, rdb.at) Art 32 DSGVO
- Eckert/Schopper in Artmann/Karollus (Hrsg), AktG II6 (Stand 1.10.2018, rdb.at) § 95 AktG
- Graf in Kletečka/Schauer (Hrsg), ABGB-ON1.05 (Stand 1.8.2019, rdb.at) § 879 ABGB
- Kipker, Chefsache Cybersicherheit: NIS-2 ist da, EuZW 2023, 249
- Kristoferitsch/Lachmayer, Die NIS-Richtlinie und ihre österreichische Umsetzung im NIS-Gesetz, ecolex 2020, 74
- Leissler/Wolfbauer in Knyrim (Hrsg), DatKomm (Stand 1.3.2021, rdb.at) Art 3 DSGVO
- Muzak, B-VG6 (Stand 1.10.2020, rdb.at) Art 6 MRK
- Piska, Die Datenschutzbehörde im Niemandsland zwischen Inquisitor und Entscheidungsorgan – Selbstbezichtigungsverbot im Fokus, ecolex 2023, 614
- Rath/Ekardt/Schiela, Cybersicherheit in der Energiewende und das EU-Recht, MMR 2023, 83
- Vcelouch in Jaeger/Stöger (Hrsg), EUV/AEUV (Stand 1.11.2017, rdb.at) Art 288 AEUV
- Wegmann, Too much of a good thing? Erweiterung und Verschärfung von Cybersicherheitspflichten durch die NIS2-Richtlinie, BB 2023, 835