WIRTSCHAFTSKAMMER ÖSTERREICH

An das
Bundeskanzleramt
Abteilung I/8
Ballhausplatz 2
1010 Wien

per E-Mail: nis@bka.gv.at

per Webformular:
Parlamentarisches Begutachtungsverfahren

Abteilung für Rechtspolitik
Wiedner Hauptstraße 63 | 1045 Wien
T 05 90 900DW | F 05 90 900
E rp@wko.at
W wko.at/oe/news/rechtspolitik

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
2024-0.220.735	Rp 70.5.3.1.2/2024/WP/Zl Dr. Winfried Pöcherstorfer	4002	25.4.2024

Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden [NIS 2024 Novelle] - Stellungnahme

Sehr geehrte Damen und Herren,

die Wirtschaftskammer erlaubt sich, zu dem Entwurf für ein Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz2012 geändert werden [NIS 2024 Novelle] folgende Stellungnahme abzugeben:

I. Allgemeines

Wir begrüßen die mit diesem in Umsetzung der EU-NIS 2-Richtlinie vorgeschlagenen Entwurf verfolgten Zielsetzungen, ebenso wie den Umstand, dass klar erkennbar Bemühungen entfaltet wurden, eine Umsetzung in Österreich nahe am Richtlinientext vorzusehen und damit das Risiko von Gold Plating möglichst hintanzuhalten. Allerdings bestehen in einigen Bereichen Unklarheiten fort, die großteils ihren Ursprung in der Richtlinie selbst haben, und einzelne Vorgaben hätten eine andere Ausrichtung erfahren können. Speziell unter Berücksichtigung des Umstandes, dass die Anzahl der von den Vorgaben für Cybersicherheit betroffenen Unternehmen gegenüber den bisher geltenden Regelungen auf ein Vielfaches anwachsen und die Zahl der zu treffenden Maßnahmen stark anwachsen wird, besteht hier ein Potential für erhebliche Rechtsunsicherheit, dem bestmöglich bereits auf Ebene der Rechtsetzung entgegengewirkt werden sollte. Im Einzelnen geht es dabei vor allem um folgende Bestimmungen:

II. Im Detail

NISG 2024

Zu § 3 Z 11 - Definition Leitungsorgan

In der NIS 2-Richtlinie findet sich keine Definition des Begriffs Leitungsorgan, während der Entwurf eine sehr weite Auslegung wählt und in den Erläuterungen ausführt.

Wir schlagen im Sinne einer Zusammenschau der Begriffsdefinitionen in Art3 Nr 30 (VO) 2022/2554, RL 2014/65/EU, 2013/36, 2009/65/EG, VO (EU) 909/2014 und (EU) 2016/1011 eine Definition dahingehend vor, dass sich ein Leitungsorgan dadurch auszeichnet, dass es Strategie, Ziele und Gesamtpolitik des Unternehmens festlegt, dass ihm die Personen angehören, die die Geschäfte des Unternehmens tatsächlich führen und vor allem, dass ihm die Letztentscheidungsbefugnis zukommt. Diese Voraussetzungen sollten daher angesichts der Strenge der Bestimmungen kumulativ vorliegen.

In diesem Sinne sollte nach Möglichkeit auch im Gesetzestext selbst eine Ausnahme für Prokuristen vorgesehen werden.

Zu § 3 Z 12 - DNS-Diensteanbieter

Die Definition der DNS-Diensteanbieter laut RL sorgt regelmäßig für technische Diskussionen. Wir gehen davon aus, dass hier nicht alle (Klein- und Kleinst-) Unternehmen, die (auch) DNS-Dienste anbieten, als wesentliche Einrichtungen mit allen rechtlichen Konsequenzen (insbesondere Prüfung durch unabhängige Stelle) erfasst werden sollen.

Hier wäre eine exaktere einschränkende Definition dringend notwendig.

Zu § 3 Z 15 - Anbieter digitaler Dienste

Hier gibt es eine Divergenz zu Anlage 2 Z 6. Hier sind neben Online-Marktplatz und Online-Suchmaschine Dienste sozialer Netzwerke genannt, während § 3 Z 15 Cloud-Computing-Dienste nennt.

Wir regen an, dass in den Erläuterungen nicht einfach § 3 Z 1 ECG zitiert wird, der dann wieder entsprechend auf Online-Marktplatz, Online-Suchmaschine und Dienste sozialer Netzwerke eingeschränkt werden muss, sondern, dass der Anwendungsbereich in den Erläuterungen gleich klargestellt wird.

Was unter „Anbieter digitaler Dienste“ fällt, ist unklar bzw gibt es zwei unterschiedliche Definitionen im Umsetzungsentwurf. Einerseits ist in § 3 Z 15 NISG 2024 aufgezählt, Online-Marktplatz, Online-Suchmaschine und Cloud-Computing Dienst. Im Anhang 2 6 ist als letzter Punkt folgendes angeführt: „*Anbieter einer Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können („Dienste sozialer Netzwerke“)*“ ohne eine nähere Definition. Unzureichend definiert sind auch die Begriffe Internetknoten, Rechenzentrumsdienste und Content Delivery Network.

In der Richtlinie ist es wie im Anhang 2 6. formuliert, daher sollte uE § 3 Z 15 diesbezüglich angepasst werden. In den Erläuternden Bemerkungen zu § 3 Z 15 wird § 3 Z 1 ECG zitiert.

Hier sollte klargestellt werden, dass dieser nur zur Anwendung kommt, wenn die Dienste in § 3 Z 15 aufgezählt sind und nicht generell.

Zu § 3 Z 23 - Anbieter verwalteter Dienste (Managed Service Provider)

Es ist unklar, wie sich das Gesetz in Konzernstrukturen verhält, die unterschiedliche Unternehmensfunktionen auf unterschiedliche Einrichtungen aufteilen (zB Holding-Struktur mit Corporate Services und operativen Gesellschaften).

So ist der Begriff Managed Service Provider vielfach nur im Zusammenhang mit externen Dienstleistern (Outsourcing) bekannt. Ob damit auch gemeint ist, dass konzerninterne Einrichtungen, die Dienstleistungen für andere konzerninterne Einrichtungen erbringen, erfasst sind, kann der Definition nicht entnommen werden. Dies wird durch die Verwendung des Begriffs „Kunden“ in der Legaldefinition noch weiter verschärft.

Hier sollte daher in die Erläuterungen ein Verweis aufgenommen werden, dass konzerninterne Managed Services Provider und generell IT-Dienstleister nicht in den Anwendungsbereich des Gesetzes fallen.

Zu § 4 - Cybersicherheitsbehörde

Die bisher geltende Behördenstruktur im Bereich Cybersicherheit, die geprägt ist von einer gemeinsamen Kompetenzwahrnehmung durch das Bundeskanzleramt und das Bundesministerium für Inneres – durch ersteres als strategische NIS-Behörde und letzteres als operative NIS-Behörde –, hat sich bewährt und konnte auf das Vertrauen der betroffenen Marktteilnehmer bauen.

Mit dem deutlichen Anwachsen der Befugnisse der künftigen Cybersicherheitsbehörde (siehe auch die Anmerkungen zu § 8 betreffend Aufsichtsmaßnahmen) und der Neuorganisation der Zuständigkeit der Behörde stellt sich nunmehr für betroffene Unternehmen nicht nur die Frage nach der Sicherstellung einer möglichst unabhängigen Aufsichtsausübung, sondern auch jene nach der Verfügbarkeit eines wirksamen, gut zugänglichen Rechtsschutzes.

Hier sollten nach Möglichkeit die bisherigen positiven Erfahrungen die Grundlage für Weiterentwicklungen bilden und bewährte Instrumente fortgeführt werden.

Zu § 7 – Unabhängige Stellen und unabhängige Prüfer

Die Bestimmung des § 7 sieht vor, dass akkreditierte Stellen eingesetzt werden, um die Umsetzung von Risikomanagementmaßnahmen wesentlicher und wichtiger Einrichtungen zu beurteilen.

Hier sollte eine Erweiterung um zusätzliche Zertifizierungseinrichtungen (wie zB Quality Austria) vorgesehen werden.

Zu § 8 - Computer-Notfallteams

Computer-Notfallteams (CSIRTs) dürfen von wesentlichen und wichtigen Einrichtungen deren Netz- und Informationssysteme in Echtzeit oder nahezu in Echtzeit überwachen. Dies stellt eine bedenkliche Bestimmung dar, vor allem weil laut Erläuterungen (S 14 f) die Überwachung und

Analyse von Cyberbedrohungen, Schwachstellen und Cybersicherheitsvorfällen, die Erhebung und Analyse forensischer Daten sowie die Ausgabe von Warnungen oder Alarmmeldungen, wenn Informationen über Cyberbedrohungen, Schwachstellen und Cybersicherheitsvorfälle bekannt werden, diese aufgrund von Informationen durchgeführt werden, auch wenn (nicht verifizierte) Informationen etwa von Dritten (anderen CSIRTs, Herstellern, Sicherheitsforschern, Dienstleistern, Non-Profit-Organisationen etc.) stammen.

Hier sollten gerade mit Blick auf mögliche Folgen für betroffene Unternehmen alle erdenklichen Schritte gesetzt werden, um missbräuchliche Meldungen bzw Informationen in Absicht der Schädigung von Unternehmen bereits im Vorfeld zu unterbinden.

Des Weiteren stellt sich uns zum 2. Hauptstück die Frage, was unter „nicht intrusiven Überprüfungen“ nach § 8 Abs 2 zu verstehen ist. Laut Erläuterungen darf eine solche Überprüfung keine nachteiligen Auswirkungen auf das Funktionieren der Dienste haben.

Es wären hier Klarstellungen, zB ob Vulnerability Scans darunterfallen, sehr hilfreich.

Zu § 8 Abs 6 – Aufwandersatz CSIRTs

Gemäß dieser Bestimmung gebührt dem nationalen CSIRT ein pauschalierter Ersatz für die bei „*ihrer*“ (gemeint ist wohl „seiner“) Aufgabenerfüllung gemäß Abs 1 entstandenen Aufwendungen.

Diese Regelung sollte auf sektorspezifische CSIRTs ausgedehnt werden

Zu § 10 – Aufsicht

Gemäß Abs 1 unterliegen CSIRTs hinsichtlich ihrer Tätigkeit der Aufsicht des Bundesministers für Inneres, der laut Abs 2 allgemeine Weisungen oder Weisungen im Einzelfall erteilen kann. Laut Erläuterungen soll diese Regelung eine Verfassungsbestimmung darstellen, jedoch ist dies im Entwurf nicht erkennbar.

Hier sollte daher der Verweis auf den Umstand, dass es sich um eine Verfassungsbestimmung handelt, entsprechend ergänzt werden.

Zu § 11 - Koordinierte Offenlegung von Schwachstellen

Hinsichtlich § 11 ist nicht klar, ob diese koordinierte Offenlegung ein Service ist, den die CSIRTS anbieten, oder dies auch eine Verpflichtung für wesentliche Einrichtungen umfasst, mit den CSIRTS zu kommunizieren und zB Schwachstellen im Rahmen von Penetrationstests an die CSIRTS bekanntzugeben.

Zu § 14 Abs 2 – Operative Koordinierungsstruktur (OpKoord)

Bei der Erweiterung der Operativen Koordinierungsstruktur (OpKoord), welche sich aus dem Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK) und den Computer-Notfallteams (CSIRTs) zusammensetzt, um sonstige Einrichtungen, die selbst nicht in den Anwendungsbereich der NIS-2-Richtlinie fallen, sollte sichergestellt werden, dass diese auf freiwilliger Basis erfolgt.

Zu § 16 – Management von Cybersicherheitsvorfällen großen Ausmaßes

Gemäß § 16 Abs 1 hat die Cybersicherheitsbehörde allgemein die Aufgaben für das Management von Cybersicherheitsvorfällen großen Ausmaßes wahrzunehmen. Diesbezüglich bedarf es daher einer Konkretisierung, welche Kompetenzen die Cybersicherheitsbehörde dabei hat bzw wie die Kompetenzverteilung mit wesentlichen und wichtigen Einrichtungen geregelt ist.

Zu § 18 Abs 2 iVm Abs 3 – Meldeanalysesystem

Es ist wichtig, dass sich betroffene Personen, die ihr Recht auf Information ausüben möchten, an eine Stelle wenden können und dort gebündelt eine umfassende Antwort erhalten. In diesem Zusammenhang ist der Gesetzestext missverständlich formuliert.

Hier sollte eine Konkretisierung im genannten Sinn erfolgen.

Zu § 21 – Zusammenarbeit mit der Datenschutzbehörde

Entgegen Art 33 DSGVO regelt § 21 Abs 2, dass die Cybersicherheitsbehörde (nicht datenschutzrechtlich Verantwortlicher gem Art 4 Z 7 DSGVO) bei Grund zur Annahme, dass Verstöße von wesentlichen und wichtigen Einrichtungen gegen §§ 32 und 34 NISG 2024, die eine Verletzung des Schutzes personenbezogener Daten zur Folge hat, eine Meldung an die Datenschutzbehörde gem Art 33 DSGVO durchzuführen hat.

Es ist unklar, mit welchen Mitteln bzw Methoden die Cybersicherheitsbehörde einschätzen kann, ob die Meldepflicht gegeben ist, die ja nur dann besteht, wenn gem Art 33 Abs 1 DSGVO voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht.

Hier wäre eine entsprechende Klarstellung wünschenswert.

Zu § 24 – Zusammenhang – RKE-Regelungen

Alle Unternehmen, die dem künftigen RKE-G (bzw der RKE-RL) betreffend die Resilienz kritischer Einrichtungen unterliegen werden, unterliegen gemäß § 24 Abs 1 Z 1 lit f NISG 2024 auch den Bestimmungen, die sich aus den NISG 2024 ergeben.

Es muss sichergestellt werden, dass es dabei für die betroffenen Unternehmen nicht zu Doppelgleisigkeiten und damit einem überschießenden Mehraufwand kommt.

Zu § 24 Abs 2 – Abgrenzung

Der Gesetzestext ist hier irreführend: Auf den ersten Blick scheint es, dass eine Einrichtung sowohl eine wesentliche als auch wichtige Einrichtung sein könnte. In Zusammenschau mit den Erläuterungen ergibt sich dann, dass die Z 1 eine Auffangklausel darstellen soll. Einrichtungen können nur dann als wichtige Einrichtung qualifiziert werden, wenn sie sowohl ein (mindestens) mittleres Unternehmen (§ 25 Abs 3) betreiben und andererseits dieses einem der Sektoren der Anlagen 1 und 2 zugeordnet werden kann.

Hier besteht demnach Konkretisierungsbedarf.

Zu § 24 Abs 3 - Öffentliche Verwaltung – Gemeinden und Gemeindeverbände

Mit Blick auf die wichtigen Aufgaben von Gemeinden für die Gesellschaft und dass diese dementsprechend beliebte Angriffsziele von Cyberkriminellen sind, ist es nicht verständlich, dass Gemeinden und Gemeindeverbände im Hinblick auf den Sektor öffentliche Verwaltung ausgenommen sind.

An dieser Stelle sei auch darauf hingewiesen, dass es große Unklarheiten gibt, wie die Gemeinden als Sektor bei typischen Aufgaben der Kommunalverwaltung, zB Trinkwasser, Abwasser, Abfallbewirtschaftung behandelt werden. Welche Regelungen gelten, wenn es sich um ausgelagerte Unternehmen zB für den Bereich Trinkwasser im Besitz mehrerer Gemeinden handelt – ist hier bei der Größenberechnung einer ausgelagerten GmbH der Umsatz bzw die Beschäftigtenzahl von den jeweiligen Gemeinden miteinzubeziehen?

Dies sollte jedenfalls klargestellt werden.

Zu § 25 – Ermittlung der Unternehmensgröße

Die Regelung führt gerade in Konzernstrukturen zu erheblichen Abgrenzungsschwierigkeiten.

In den Erläuterungen sollte ausdrücklich festgehalten werden, dass Partnerunternehmen und verbundene Unternehmen ausschließlich bei der Größenerhebung relevant sind, jedoch nicht in den Anwendungsbereich einbezogen werden, sofern sie nicht selbst im konkreten Sektor tätig sind.

Zu § 25 - Zurechnung im Konzern

§ 25 des Entwurfs greift vollständig auf die Kommissionsempfehlung 2003/361/EG samt den darin vorgesehenen Bestimmungen über die Zurechnung von Werten konzernverbundener Unternehmen zurück. Daraus ergibt sich, dass die Pflichten zur Setzung von Risikomanagement-maßnahmen auch dann auf Konzerngesellschaften zur Anwendung kommen sollen, wenn diese lediglich über einzelne Mitarbeiter verfügen, diese unter dem Gesichtspunkt der Netz- und Informationssicherheit keine kritische Infrastruktur betreiben und auch technisch und organisatorisch in keinem Zusammenhang zu den kritischen Lebensmittelunternehmen im Konzern stehen.

Der deutsche Gesetzgeber sah in Orientierung an die „Öffnungsklausel“ des ErwG 16 der NIS 2-RL gewisse Ausnahmen von der Zurechnung vor. Der österreichische Gesetzgeber sollte diese Möglichkeit ebenfalls nutzen, um unverhältnismäßige, für den Wirtschaftsstandort schädliche Härten zu vermeiden und der aus der österreichischen Bundesverfassung folgenden Verpflichtung zur verhältnismäßigen Ausgestaltung des NISG 2024 nachzukommen. Eine vollständige Zusammenrechnung würde den Anwendungsbereich des NISG 2024 entgegen der Zielsetzung der NIS 2-RL ausgestalten, weil diese nicht bezweckt, eine Vielzahl kleiner Unternehmen, deren IT nicht mit kritischen Netz- und Informationssystemen verflochten ist, in den Anwendungsbereich des NIS-2-Cybersicherheitsrechts einzubeziehen.

Wir schlagen daher die Aufnahme eines zusätzlichen Absatzes folgenden Wortlauts in § 25 vor:

„§ 25 Abs 4
Bei der Bestimmung der Anzahl der Mitarbeiter, des Jahresumsatzes und der Jahresbilanzsumme für die Zwecke der Abs. 1 bis 3 sind die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung der Kommission vom 6.5.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, ABl Nr L 124 vom 20.5.2003 S 36, nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der Netz- und Informationssysteme unabhängig von seinen Partner- oder verbundenen Unternehmen ist."

Die obigen Begriffe „rechtliche, wirtschaftliche und tatsächliche Umstände" sollten uE in den Materialien detailliert beschrieben werden, um eine allfällige Rechtsunsicherheit so weit als möglich hintanzuhalten.

Zu § 26 Abs 3 – Größenunabhängige Einstufung

Die Formulierung des Abs 2 ist im Kontext mit dem Abs 3 irreführend. Abs 2 bestimmt, dass eine wichtige Einrichtung als wesentliche Einrichtung mit Bescheid einzustufen ist, sofern die in Abs 3 Z 1-4 genannten Gründe gegeben sind. Der Abs 3 wiederum regelt, dass eine Einstufung einer Einrichtung als wesentliche Einrichtung oder als wichtige Einrichtung zu erfolgen hat, wenn die Ziffern 1-4 erfüllt sind. Sind die Gründe des Abs 3 Z 1-4 gegeben, ist daher nach Abs 2 die Einstufung als wichtige Einrichtung gar nicht mehr möglich, nach Abs 3 jedoch schon.

In diesem Sinne ist auch hier eine Klarstellung vorzunehmen.

Zu § 29 Abs 2 – Registrierung: Bestätigung

Wichtige und wesentliche Einrichtungen gemäß § 29 haben sich innerhalb von drei Monaten nach Inkrafttreten des Gesetzes zu registrieren. Säumnisse ziehen nach § 45 empfindliche Verwaltungsstrafen nach sich.

So ist es zwingend geboten, dass es seitens der Cybersicherheitsbehörde eine Bestätigung der Registrierung und des Registrierungszeitpunkts gibt (und allfällig nachzureichende Angaben im Rahmen eines Nachbesserungsauftrages angefragt werden).

Zu § 29 Abs 2 Z 3 – Register der Einrichtungen

Beim Abstellen auf die einzelnen Sektoren in den Anlagen sollte durchgehend auch auf die entsprechenden NACE-Codes verwiesen werden, da auch diese als Basis für den persönlichen Anwendungsbereich verwendet werden.

Zu § 29 Abs 2 – Registrierung: Frist und Beraten statt Strafen

Der Anwendungsbereich ist dermaßen komplex, dass es selbst für NIS-Expertinnen und Experten oft schwer feststellbar ist, ob Betroffenheit besteht. Es ist auch damit zu rechnen, dass viele Unternehmen in nicht technologieaffinen Branchen sich nicht als kritische Einrichtung sehen und von einem Cybersicherheitsgesetz per se nicht adressiert fühlen und trotz Aufklärungskampagnen nur schwer erreicht werden.

Für die Registrierung sollte daher eine Frist von sechs statt drei Monaten vorgesehen werden.

Das Prinzip „Beraten statt Strafen“ sollte jedenfalls bei Einrichtungen, die nicht ganz offensichtlich in den Anwendungsbereich des Gesetzes fallen, Vorrang genießen.

Zu § 29 Abs 2 – Registrierung: rechtsverbindliche Mitteilung

Die Unternehmen müssen eine Möglichkeit haben, eine rechtsverbindliche Antwort zu erhalten, ob sie in den Anwendungsbereich fallen oder ausgenommen sind.

Schon im Vorfeld zeigt sich, dass große Rechtsunsicherheit bei den Unternehmen bezüglich des komplexen Anwendungsbereichs vorliegt und bei Abgrenzungsfällen auch Experten zu unterschiedlichen Ergebnissen betreffend die Einstufung nach Anlage 1 und 2 bzw den Größenschwellen bei Partner- und verbundenen Unternehmen kommen.

Da die Gesetzgebung weitreichende Rechtsfolgen hat, müssen betroffene Einrichtungen Rechtssicherheit haben, ob sie in den Anwendungsbereich fallen oder ausgenommen sind.
Die Cybersicherheitsbehörde sollte daher registrierenden Einrichtungen, die tatsächlich nicht der Registrierungspflicht unterliegen, dies rechtsverbindlich mitteilen.

Hier bietet sich ein ähnliches Verfahren an, wie es § 6 TKG 2021 vorsieht (siehe insbesondere Abs 3 und 4) und wie es sich in der Praxis bewährt hat. So kann den Rechtsunterworfenen die gebotene Rechtssicherheit gegeben werden. Zugleich erhält die Cybersicherheitsbehörde damit ein valides Register im Sinne § 29 Abs 1 für ihre Aufgaben.

Zu § 29 Abs 3 – Frist für Registrierung

Wenn das Gesetz tatsächlich erst zum letzten fristgerechten Zeitpunkt am 18.10.2024 in Geltung tritt, wäre es angebracht, wenn Unternehmen (die ja dann erst final und rechtssicher die Rechtslage und ggf die finale Betroffenheit kennen) mehr Zeit für die Registrierung und Selbstdeklaration erhalten.

Hier wäre eine Ausdehnung von drei auf zumindest sechs Monate eine angebrachte Erleichterung.

Zu § 29 Abs 4 Z 1 – Pflichten – Register der Einrichtungen

Für die Einmeldung im Register der wesentlichen und wichtigen Einrichtungen ist eine zweiwöchige Frist bei der Änderung vom Namen der Einrichtung, der Anschrift und aktuelle Kontaktdaten, einschließlich der E-Mail-Adressen und Telefonnummern sowie gegebenenfalls ihren benannten Vertreter angegeben.

Die Frist scheint zu eng gegriffen und sollte auf zumindest ein Monat erweitert werden, um den damit verbundenen Aufwänden für Unternehmen Rechnung zu tragen.

Zu § 31 Governance – Haftung von Leitungsorganen

§ 31 Abs 2 sieht vor, dass „Leitungsorgane […] der Einrichtung für den schuldhaft verursachten Schaden“ haften, wenn sie ihre NIS-Pflichten verletzen. § 31 Abs 2 sieht damit eine umfassende Haftung vor, die keinerlei Kriterien für eine etwaige Mäßigung oder Begrenzung beinhaltet.

Dies würde auch bereits leichte Fahrlässigkeit umfassen. Das übersteigt die für das Management zumutbare Haftung. Die Erläuterungen dazu bringen eine zusätzliche Unsicherheit, da nicht klar ist was mit „Einordnung“ gemeint ist: „Die ausdrückliche Anordnung einer solchen Haftung schließt die Einordnung weiterer Bestimmungen, […] nicht aus.“

Zur Erlassung einer solchen Haftungsbestimmung würde die NIS-2-RL indes nicht verpflichten, weil die Haftung der Leitungsorgane bereits gesellschaftsrechtlich ausreichend sichergestellt ist. Aus diesem Grund unterließ es beispielsweise auch der deutsche Gesetzgeber, eine Haftungsbestimmung im deutschen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz zu etablieren, weil sich eine ausreichende Haftung eben bereits aus allgemeinen Grundsätzen ergibt.

Es wird daher angeregt, die Bestimmung des § 31 Abs 2 ersatzlos zu streichen.

Zu § 32 - Risikomanagementmaßnahmen

Einzelne Anforderungen, die bereits durch anerkannte Zertifizierungen erfüllt worden sind (wie zB TISAX im Bereich Automotive oder ISO 27001 uam), sollen auch für nach dem NISG 2024 erforderlichen Nachweise als ausreichend anerkannt werden und nicht mehrfach überprüft werden.

In der noch zu erlassenden Verordnung sollte speziell auch Rücksicht auf die Herausforderungen für kleine und mittlere Unternehmen im Bereich Cybersicherheit genommen werden.

Wir erachten Empfehlungen der Behörde hinsichtlich Best Practices wie zB aktuell in Factsheet Nr 9/2022 für sinnvoll.

Der Entwurf einer Verordnung des Innenministers in diesem Bereich sollte jedenfalls öffentlich begutachtet werden.

Zu § 32 - Telekommunikationsbranche

In der Telekommunikationsbranche gibt es eine schon lange etablierte Praxis unter dem Regulierungsregime des TKG (derzeit § 44 TKG 2021), die all diese Maßnahmen beinhaltet und die auch weiterhin der Maßstab für das Risikomanagement der Telekommunikationsbranche sein sollten. An der bisherigen Praxis sollte sich daher auch die Verordnung nach Absatz 4 orientieren. Das bisherige Risikomanagement hat sich als höchst wirksam erwiesen – was nicht verwundert, weil es hier um den Kern der Dienstleistungen der TK-Branche geht.

Daher sollte hier im Sinne einer konsistenten Weiterführung einer Risikomanagementregulierung unbedingt die Verordnung(en) eng mit der Branche und dem Fachverband als gesetzliche Interessenvertretung (im Fall sektorspezifischer Anforderungen) abgestimmt und kooperativ erarbeitet werden im Sinne einer bestmöglichen Effizienz der Maßnahmen im Sinne der NISG 2024-Regulierungsziele.

Es sollte jedenfalls auch erwogen werden, diese Erfordernisse im Rahmen von etablierten Zertifizierungen abzubilden. Naturgemäß können größere Unternehmen mit solch komplexen Materien besser umgehen als KMU, weshalb wir grundsätzlich für alle skizzierten Erfordernisse der Rechtsunterworfenen ein angepasstes NIS Fact Sheet vorschlagen.

Zu § 32 Abs 1 - Risikobetrachtung und Abgrenzung nicht relevanter Dienste

Der Gesetzesentwurf enthält keine explizite Klarstellung, dass – nach erfolgter Risikobetrachtung – jene Systeme und Prozesse im Anwendungsbereich abgegrenzt werden dürfen, die nicht zur Erbringung oder Aufrechterhaltung der Dienste der kritischen Sektoren (im Sinne der Anlagen 1 und 2) erforderlich sind und die die umfassten Dienste nicht beeinflussen können (insbesondere aufgrund vorhandener Netzsegmentierung).

Eine entsprechende Klarstellung (beispielsweise als § 32 Abs 2 Z 4) hätte den positiven Effekt zur Folge, dass die betroffenen Einrichtungen – nach initialer Risikoeinschätzung – möglichst wenig Ressourcen für derart klar abgegrenzte Systeme, welche weder gesellschaftliche noch wirtschaftliche Relevanz haben, aufwenden müssen und damit ein effizienter Schutz der tatsächlichen kritischen Systeme möglich ist. Auch vor dem Hintergrund des bestehenden Fachkräftemangels ist eine derartige Priorisierung sinnvoll.

Zu § 32 Abs 2 Z 3 - Lieferkette

Betreffend die Anforderungen an die Lieferkette ist zu berücksichtigen, dass damit auch eine sehr große Zahl an Klein- und Kleinstunternehmen verpflichtet werden. Es ist von großer Bedeutung für die kleinstrukturierte österreichische Wirtschaft, dass hier angemessene und nicht überbordende Nachweise für die Sicherheit der Lieferkette ausreichen. Insofern ist es wünschenswert, dass Empfehlungen der Behörde – wie derzeit im Factsheet 9/2022 – beibehalten bzw weiterentwickelt werden, wo auf gängige Sicherheitsstandards sowie - auch für KMU praktikable Best Practices – wie zB das KSÖ Cyber Risk Rating verwiesen wird.

Zu § 32 Abs 4 – Risikomanagementmaßnahmen, Verordnungsermächtigung und andere Verordnungen

Kern der Gesetzgebung sind die zu treffenden Risikomanagementmaßnahmen. Die technischen, operativen und organisatorischen Anforderungen werden allerdings erst in einer Verordnung festgelegt. Gleichzeitig sind betroffene Einrichtungen aber mit Inkrafttreten des Gesetzes verpflichtet, die Maßnahmen umgesetzt zu haben.

Es muss den Einrichtungen ein realistischer Zeitraum ab Kenntnis der definitiven Anforderungen (in der Verordnung) gegeben werden, um hier rechtskonform vorgehen zu können. Der Zeitpunkt der Verpflichtung der Umsetzung der Maßnahmen muss daher in einem ausreichend langen Abstand nach Inkrafttreten der Verordnung zur Festlegung der Risikomanagementmaßnahmen liegen, um rechtskonformes Handeln zu ermöglichen.

Keinesfalls dürfen die Unternehmen in die Verlegenheit kommen, Maßnahmen schon umsetzen zu müssen, die dann möglicherweise im Nachhinein gemessen an der später erlassenen Verordnung dieser nicht genügen. Speziell zur Telekombranche sei angemerkt, dass die in § 32 skizzierten Maßnahmen für die Unternehmen nicht neu sind. Cybersicherheit ist dort schon immer ein Kernelement der Geschäftstätigkeit gewesen und wurde maßgebend in der Praxis von diesen Unternehmen weiterentwickelt. Daher die Empfehlung an den Verordnungsgeber, sich hierbei an der bisherigen Praxis zu orientieren, um gleich auf einem hohen Sicherheitsniveau und unter wenig zusätzlichem Aufwand für die Branche weiterzumachen.

Angemerkt sei, dass die Forderung nach ausreichend langer Umsetzungsfristen nach Kenntnis der entsprechenden Verordnungen natürlich auch für andere Verordnungen im Gesetz gilt, die auf die Einrichtungen Auswirkungen haben.

Inhaltlich sei auch angemerkt, dass die NIS 2-RL bereits umfangreiche Vorgaben vorsieht. Es ist darauf zu achten, dass bei der Verordnung zur Festlegung der Risikomanagementmaßnahmen kein Gold Plating erfolgt. Auch wenn Konkretisierungen hier das positive Ziel von Rechtssicherheit verfolgen, darf dies nicht auf Kosten einer Verschärfung der Regelungen erfolgen. Insbesondere ist dabei auch auf die Herausforderungen für kleine und mittlere Unternehmen Bedacht zu nehmen.

Der Bundesminister für Inneres erhält nach § 32 Abs 4 eine sehr starke Ermächtigung zur Verordnung von Risikomanagementmaßnahmen. Zwar sind in den Materialen Verweise auf die Verhältnismäßigkeit (Seite 34 letzter Absatz zu § 32) enthalten. Allerdings wäre eine entsprechende Verankerung im Gesetzestext wünschenswert.

Delegierte Rechtsakte und Durchführungsrechtsakte

Besonders hingewiesen sei außerdem auf Kapitel VIII der NIS 2-Richtlinie und weiters auf Art 21, 23 und insbesondere auf Art 24, wo delegierte Rechtsakte und Durchführungsrechtsakte vorgesehen sind, die in ganz erheblichem Maße Einfluss auf die Verpflichtungen der Einrichtungen haben werden. Auch hier besteht die Gefahr, dass die Unternehmen bereits im Hinblick auf die gesetzlichen Bestimmungen Maßnahmen unter Kosten- und Personalaufwand setzen, die den Maßstäben der kommenden Durchführungsrechtsakte nicht genügen oder überschießend (und damit kostenintensiv) sind.

Zu § 33 Abs 1 – Frist Selbstdeklaration

Unter den Anbietern von Top Level Domain- und Domain Name Server-Diensten werden auch kleine Unternehmen als „wesentliche Einrichtungen“ eingestuft. Die RL lässt hinsichtlich des Anwendungsbereichs zur Unternehmensgröße wenig Spielraum.

Es wäre aber angebracht, wenn zumindest hinsichtlich der Maßnahmennachweise gem § 33 für zB KMU unter (zB bei < 250 Mitarbeitern, oder < 50 Mitarbeitern) längere Fristen gelten.

Grund: Die Umsetzung der technischen Maßnahmen (und damit die Sicherheit) erfolgt als erstes und jedenfalls zeitgerecht, aber die Dokumentation, die sehr viel Zeit in Anspruch nimmt, trifft KMU aufgrund geringerer Personalressourcen unverhältnismäßig stärker und sollte bei den Fristen Berücksichtigung finden (zB von sechs auf neun Monate; selbst zwölf Monate können zu wenig sein, wenn KMU zB überhaupt erst durch die Aufforderung der Behörde Kenntnis von ihrer Betroffenheit erhalten).

Gegenüber der bisherigen Einstufung durch die Behörde mittels Bescheides stellt die Selbstdeklaration für Betroffene in Anbetracht der Komplexität der Materie jedenfalls Herausforderung und Risiko dar.

§ 33 Abs 1 – Nachweis der Wirksamkeit von Risikomanagementmaßnahmen

Hier stellt sich die Frage, in welchem Format die umgesetzten Risikomanagementmaßnahmen gemäß § 32 an die Cybersicherheitsbehörde übermittelt werden müssen.

Der Entwurf spricht von einer Aufforderung durch die Cybersicherheitsbehörde, die einer Selbstdeklaration vorausgeht. Die Rahmenbedingungen für eine solche Aufforderung lässt der Entwurf völlig offen. Insbesondere lässt sich nicht erkennen, wie eine solche Aufforderung ausgestaltet sein muss.

Es sollte klargestellt werden, ob hier die Erlassung eines Bescheides vorgesehen ist oder eine formlose Erledigung. Ferner sollte hier Platz auch für freiwillige Angebote, wie zB Cyber Risk Ratings sein.

Ferner ist unklar, ob es sich bei den genannten drei Jahren um eine Mindestfrist handelt oder die Behörde jederzeit neue Aufforderungen schicken kann und damit ein rollierendes System der Prüfungen ausgelöst wird. Wir empfehlen hier dringend die Klarstellung, dass es sich um eine Mindestfrist handelt, da sonst ein unverhältnismäßiger zeitlicher und monetärer Aufwand zu erwarten ist.

Darüber hinaus sollte sichergestellt werden, dass wesentliche Einrichtungen, die in mehr als einem Sektor gem Anlage 1 tätig sind, nur einmal innerhalb des dreijährigen Prüfungszyklus geprüft werden dürfen. Es sollen also die jeweils relevanten Geschäftsbereiche der wesentlichen Einrichtung als Ganzes geprüft werden und es soll keine sektorspezifische Aufteilung stattfinden. Ansonsten würden im Vergleich zu anderen wesentlichen Einrichtungen, die nur in einem Sektor tätig sind, erheblich Mehrkosten entstehen. Den Kosten soll hinsichtlich Wirtschaftlichkeit und organisatorischer Aufwände ähnlich Rechnung getragen werden, wie es bereits bei den Bestimmungen zur Umsetzung von Risikomanagementmaßnahmen (§ 32 (2) 1 b Entwurf NISG 2024) der Fall ist.

Weiters soll sichergestellt werden, dass alle wesentlichen Einrichtungen eines Konzerns den Nachweis der Wirksamkeit der Risikomanagementmaßnahmen im Rahmen einer gemeinsamen Prüfung erbringen können.

Bei Unternehmen, die bereits nach NIS-1 auditiert wurden, erscheint eine Selbstdeklaration nicht sinnvoll, da diese Unternehmen den Behörden bereits bekannt sind.

Zu § 33 Abs 4 – Kostentragungsregelung - unabhängige Stellen

Die Kosten von Prüfungen durch unabhängige Stellen werden den geprüften Einrichtungen auferlegt. Diese Kostenauferlegung ist erst einmal grundsätzlich unbillig. Es wird hier nämlich keine Leistung erbracht, die originär den Unternehmen nützt oder eine von Ihnen eröffnete Betriebsgefahr adressiert, sondern übergeordneten staatlichen Sicherheitsinteressen dient.

Es ist zu erwarten, dass sich unabhängige Stellen und Prüfer (§ 7) erst nach und nach am Markt etablieren werden, es also sicherlich zum Inkrafttreten des Gesetzes begrenzte Verfügbarkeiten gibt mit entsprechenden Folgen für die Preise dieser Dienstleistungen. Da diese unabhängigen Stellen und die von ihnen eingesetzten unabhängigen Prüfer eine zentrale Funktion im Rahmen des Nachweises der Wirksamkeit von Risikomanagementmaßnahmen gemäß § 33 haben, sollte dies bei verpflichtenden Prüfungen nach § 33 Abs 2 und 3 berücksichtigt werden, um hier die Unternehmen nicht überbordenden Kostenfolgen auszusetzen.

Jedenfalls sollte eine Kostenbegrenzung festgeschrieben werden, sei es durch pauschalierte Sätze oder Zeitvorgaben (zB differenziert nach Unternehmensgröße) für die Prüfungen.

Zu § 33 Abs 6 – Verordnung – Nachweis Risikomanagementmaßnahmen

Auch die Verordnung nach § 33 Abs 6 sollte zeitnah mit dem Inkrafttreten des NISG 2024 erlassen werden, die die notwendigen Inhalte, das Format und die Struktur der Nachweise klar und überschaubar bezeichnet. Die Rechtsadressaten dürfen hier nicht im Unklaren darüber sein, welche Anforderungen an sie konkret gestellt werden. Daher bietet sich eine Art Maßnahmenkatalog an, der die genannten Verhältnismäßigkeitsaspekte (siehe vor allem § 32 Abs 3) berücksichtigt, aber dennoch eine gewisse Flexibilität für Erleichterungen im Rahmen weiterer Verhältnismäßigkeitserwägungen im Einzelfall bietet.

Zu § 34 – Berichtspflichten

§ 34 Abs 1 lautet: „Wesentliche und wichtige Einrichtungen haben dem für sie zuständigen CSIRT, andernfalls dem nationalen CSIRT, unverzüglich jeden erheblichen Cybersicherheitsvorfall (§ 35) zu melden. Das CSIRT leitet die Meldung unverzüglich an die Cybersicherheitsbehörde weiter."

In § 34 Abs 1 sollte wortgleich wie in § 37 Abs 1 folgende Präzisierung vorgenommen werden:

> „Wesentliche und wichtige Einrichtungen haben dem für sie zuständigen CSIRT, in Ermangelung eines solchen dem nationalen CSIRT, unverzüglich jeden Cybersicherheitsvorfall (§35) zu melden. …"

Zu § 34 Abs 2 – Mindestinhalte die Frühwarnung und Meldung

Zu § 34 Abs 2 wären Klarstellungen hilfreich, welche Mindestinhalte die Frühwarnung und Meldung haben sollen. Dies könnte man durch entsprechende Umformulierung der Verordnung nach § 35 Abs 3 zur näheren Bestimmung eines erheblichen Cybersicherheitsvorfalls dort unterbringen. Der Fachverband Telekom/Rundfunk in der Bundessparte Information und Consulting spricht sich hier für eine enge Abstimmung mit den jeweiligen Sektoren und dem Fachverband als fachlich zuständiger Interessenvertretungsorganisation aus.

§§ 36 f (3. Abschnitt) – Informationsaustausch

Der 3. Abschnitt des Entwurfs des NISG 2024 regelt den freiwilligen Informationsaustausch zwischen wesentlichen und wichtigen Einrichtungen über relevante Cybersicherheits-informationen. Diese Möglichkeit zum freiwilligen Informationsaustausch zwischen Einrichtungen ist hilfreich und zu begrüßen.

Es wäre darüber hinaus auch wünschenswert, die zuständigen nationalen Behörden gesetzlich dazu zu verpflichten, wesentliche und wichtige Einrichtungen möglichst zeitnah (und entsprechend anonymisiert) über aktuelle, schwerwiegende Bedrohungslagen und Beinahe-Vorfälle in anderen Einrichtungen im Bundesgebiet zu informieren, damit die informierten Einrichtungen ihre Sicherheitsvorkehrungen im Anlassfall gezielt verschärfen können.

§ 38 Abs 1 – Aufsicht – weisungsfreie Behörde

Die in § 38 Abs 1 Z1 NISG 2024 vorgesehene Befugnis der Cybersicherheitsbehörde, "Einschau" in die Netz- und Informationssysteme und Unterlagen der Einrichtungen zu nehmen, erachten wir als problematisch, da diese Behörde in die Zuständigkeit des BMI fällt. Wir geben in diesem

Zusammenhang zu bedenken, dass diese Bestimmung dem Bundesminister für Inneres faktisch den Zugang zu hoch sensiblen - sicherheits- und wettbewerbsrelevanten - Informationen ermöglicht und damit eine nicht unerhebliche Gefahr eines Missbrauchs - insbesondere eines Eingriffs in Geschäfts- und Betriebsgeheimnisse - verbunden ist. Um diese Gefahr angemessen zu entschärfen, wäre aus unserer Sicht die Zuständigkeit einer - dem Vorbild der Datenschutzbehörde folgenden - eigenständigen, weisungsfreien Behörde vorzusehen.

Zu § 38 - Aufsichtsmaßnahmen

Zu den Aufsichtsmaßnahmen nach § 38 ist anzumerken, dass auch nach Abs 1 Z 2 die betreffende Einrichtung in jedem Fall zu informieren und einzubeziehen ist, nicht nur erforderlichenfalls.

Hinsichtlich allfälliger Durchsetzungsmaßnahmen gem § 39 sehen wir den Bedarf zu konkretisieren, was unter einer angemessenen Frist zu verstehen ist. Diese sollte jedenfalls hinreichend lang sein, damit die betroffenen Einrichtungen die Maßnahmen umsetzen können.

Zu § 38 - Aufsichtsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen

Gemäß § 38 Abs 1 Z 4 kann die Cybersicherheitsbehörde den Zugang zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind, anfordern. Bei Einrichtung derartiger Zugänge sollten weiterhin aktuelle organisationseigene Anforderungen eingehalten werden (entsprechende Abwägung, ausreichende Begründung, Verwendung von durch das Unternehmen verwaltete Clients etc).

Zu § 38 - Aufsichtsmaßnahmen (Fernzugriff)

Fernzugriff ist in der NIS 2-RL nicht genannt.

Daher sollte die Durchführung von Aufsichtsmaßnahmen im Wege des Fernzugriffs nur nach ausdrücklicher Zustimmung der betroffenen Einrichtung erfolgen.

Zu § 38 - Datenschutz

Zur Durchführung wird angemerkt, dass auch § 38 Abs 1 Z 2 und Z 5 nur nach vorheriger Verständigung der betroffenen Einrichtung durchgeführt werden sollen. Weiters ist sicherzustellen, dass die ausgewiesenen Pflichten auch auf die unabhängigen Stellen, die allfällige Prüfungen begleiten können, überbunden werden. Mit Blick auf Art 58 Abs 1 lit b, e, f DSGVO, in der den nationalen Datenschutzbehörden ebenfalls umfangreiche Kontroll- und Einsichtsrechte gewährt werden, ist im Vergleich zum NISG ausführen, dass der Zweck der unabhängigen Datenschutzbehörde die Wahrung der datenschutzrechtlichen Bestimmungen ist. Darüber hinaus gibt es in der DSGVO bzw dem DSG keine Möglichkeit der Datenschutzbehörde, Daten an Dritte weiterzugeben, wie es in § 43 NISG (siehe auch Anmerkungen unten) der Fall ist.

Der Bundesminister für Inneres ist als Cybersicherheitsbehörde (§ 4 NISG) keine unabhängige Behörde, wie dies bei der Datenschutzbehörde der Fall ist. Es ist daher eine Einschränkung der Rechte der gegenständlichen Behörde vorzunehmen.

Zu § 39 – Durchsetzungsmaßnahmen – Leitungsaufgaben

Wird Leitungsorganen ein bescheidmäßiges Tätigkeitsverbot erteilt, sieht § 39 Abs 4 Z 2 vor, dass der „Bescheid […] in einer allgemeinen Weise zu veröffentlichen [ist], die geeignet erscheint, einen möglichst weiten Personenkreis zu erreichen“. Dieser „Naming-and-Shaming“-Mechanismus ist in der NIS-2-RL nicht enthalten und deswegen unionsrechtlich nicht geboten.

Es ist nicht nachvollziehbar, weswegen § 39 Abs 4 Z 2 ohne ersichtlichen Grund (es besteht kein Informationsinteresse der Öffentlichkeit, dass bestimmten Leitungsorganen ein Tätigkeitsverbot auferlegt wurde) derart schwer in grundrechtlich gewährleistete Rechtspositionen (Art 8 EMRK, Art 1 1. ZP-EMRK, Art 5 und 6 StGG) betroffener Leitungsorgane eingreift und warum der österreichische Gesetzgeber gerade in diesem grundrechtssensiblen Bereich von seiner grundsätzlichen Vorgehensweise abweicht, „Gold-Plating“ zu vermeiden.

Es wird daher angeregt, den Satz *„Dieser Bescheid ist in einer allgemeinen Weise zu veröffentlichen, die geeignet erscheint, einen möglichst weiten Personenkreis zu erreichen.“* in § 39 Abs 4 Z 2 ersatzlos zu streichen.

Zu § 39 Abs 4 Z 2 – Durchsetzungsmaßnahmen – wesentliche und wichtige Einrichtungen

Die Möglichkeit, Leitungsorganen einer wesentlichen Einrichtung, einschließlich ihrer rechtlichen Vertreter, mit Bescheid vorübergehend zu untersagen, Leitungsaufgaben in dieser wesentlichen Einrichtung wahrzunehmen, ist in dieser Form trotz ihrer Richtlinienkonformität kritisch zu sehen. Denn es bleibt offen, wer die erforderlichen bzw aufgetragenen Maßnahmen setzen soll, wenn eine Einrichtung dadurch praktisch nicht mehr handlungsfähig ist. Auch ist zu befürchten, dass in weiterer Folge Ansprüche – welcher Art auch immer - gegen untätige Leitungsorgane bzw die Einrichtung entstehen könnten.

Folgende Fragestellungen ergeben sich hier:

Müsste man nicht, auch im Sinne der Verhältnismäßigkeit, nur die Leitung für den Bereich der „Cybersicherheit“ untersagen?

Gemäß Absatz 5 muss eine Untersagung bei Wegfall der Versagungsgründe unverzüglich erfolgen. Bei der Versagung stellt das Gesetz „auf einen möglichst weiten Personenkreis“ ab. Die Aufhebung sollte einer in derselben Weise stattfinden wie die Untersagung. Ein Verweis im Gesetz oder den Materialen fehlt dazu.

Wir regen an, entsprechende Aussagen ins Gesetz aufzunehmen. Insbesondere sollte klargestellt werden, wer in einem solchen Falle Maßnahmen setzen soll und ob zB ein Notgeschäftsführer bestellt werden müsste.

Zu § 39 Abs 4 Z 2 Satz 2 – Leitungsorgane (kein „naming and shaming“)

Wird Leitungsorganen mit Bescheid die Tätigkeit im Unternehmen untersagt, ist der betreffende Bescheid gemäß § 39 Abs 4 Z 2 Satz 2 des Entwurfs *„in einer allgemeinen Weise zu veröffentlichen, die geeignet erscheint, einen möglichst weiten Personenkreis zu erreichen“.* Die NIS 2-RL sieht ein derartiges „Bloßstellen“ nicht vor. In Ermangelung einer unionsrechtlichen Verpflichtung ist deswegen völlig unverständlich, warum der § 39 Abs 4 Z 2 Satz 2 NISG 2024

ohne ersichtlichen Grund eine derart eingriffsintensive Maßnahme zulasten der Grundrechte betroffener Leitungsorgane vorsieht (Art 8 EMRK, Art 1 1. ZP-EMRK, Art 5 und 6 StGG).

Es wird daher angeregt, § 39 Abs 4 Z 2 Satz 2 NISG 2024 ersatzlos zu streichen.

Zu § 39 Abs 7 – Bestellung von Überwachungsbeauftragten

Die Bestellung des Überwachungsbeauftragten stellt selbst einen schwerwiegenden Eingriff dar.

Es sollte daher im ersten Satz des Abs 7 ein Teilsatz aufgenommen werden, in dem auch auf das Verhältnis der Schwere des Eingriffs durch die Cybersicherheitsbehörde zu den Verstößen in Relation gesetzt werden.

Zu § 40 - Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung

Die Verpflichtung zur Verwendung spezieller IKT-Produkte, -Dienste und -Prozesse für den Nachweis der in § 32 genannten Anforderungen müssen die Wirtschaftlichkeit im Verhältnis zum Risiko berücksichtigen, dürfen nicht zur unverhältnismäßigen oder ungewollten Erhöhung eines Risikos führen und müssen ausschließlich für diesen Verwendungszweck vorgesehen sein. Für den Fall, dass durch die Cybersicherheitsbehörde Produktentscheidungen getroffen werden, sollte es zumindest eine Auswahl an IKT-Produkten, -Diensten etc geben. Außerdem sollte eingeschränkt werden, wenn zB Risikomanagementmaßnahmen nach wiederholter Aufforderung nicht behoben wurden.

Zudem ist das verwendete, rechtliche Instrument ungeklärt (soll – wenn überhaupt – ein Bescheid ergehen?).

Vor dem Hintergrund der Vorlaufzeiten, allfälligen Implementierungskosten sowie der hohen Strafandrohungen empfehlen wir zur Gewährleistung der Planungs- und Rechtssicherheit zumindest eine Darlegung der Kriterien und des Ablaufs bzw den Zusammenhang mit dem Vollzug dieser Bestimmung sowie deren erwarteten Folgen in den Erläuterungen.

Zu § 40 - Schemata für die Cybersicherheitszertifizierung

§ 40 ist insofern problematisch als hier delegierte Rechtsakte vorgesehen sind, um die NIS-2-Richtlinie mit Ausführungen zu ergänzen, welche Kategorien wesentlicher und wichtiger Einrichtungen verpflichtet sind, bestimmte zertifizierte IKT-Produkte, -Dienste und -Prozesse zu nutzen oder ein bestimmtes Zertifikat für die Cybersicherheitszertifizierung zu erlangen (Art 24 Abs 2 NIS 2-RL). Auf die Problematik delegierter Rechtsakte wurde oben schon hingewiesen.

Hinsichtlich des Verweises auf den Cybersecurity Act (Verordnung EU 2019/881) darin, der eine Festlegung europäischer Schemata für die Cybersicherheitszertifizierung ermöglicht, mit dem Ziel, für IKT-Produkte und -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten, sehen wir es als kritisch an, wenn im Ergebnis Unternehmen zur Verwendung bestimmter Produkte verpflichtet werden können.

Zu § 40 – Verwendung spezieller IKT-Produkte

Eine solche Forderung bedeutet für Unternehmen ggf erhebliche Beschaffungs- und Integrationskosten. Da noch nicht absehbar ist, welche IKT-Produkte in welchem Ausmaß hier gemeint sind, ist eine solche Verpflichtung aus Unternehmenssicht nicht vertretbar.

Daher sollte die Forderung zu einer Empfehlung umformuliert werden und von einer verpflichtenden Verwendung abgesehen werden.

Zu § 41 – Aufschiebende Wirkung von Beschwerden

Gemäß § 41 NISG 2024 soll Beschwerden gegen gewisse Bescheide der Behörde ex lege keine aufschiebende Wirkung zukommen. Im Hinblick auf die Bescheide gemäß § 39 Abs 2, 3 und 4 Z 2 NISG 2024 (Durchsetzungsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen) ist dieser Automatismus überschießend und unverhältnismäßig. Hier sollte die aufschiebende Wirkung der Beschwerde der Regelfall sein, sodass diese bereits ex lege und nicht nur ausnahmsweise über behördliche Zuerkennung eintritt.

Es wird daher angeregt, die Bestimmung des § 41 NISG 2024 wie folgt zu ändern:

> Rechtsmittel gegen Entscheidungen der Cybersicherheitsbehörde gemäß § 7 Abs. 4 und 10 sowie § 10 Abs 7 haben aufschiebende Wirkung. § 13 Abs 2 des Verwaltungsgerichtsverfahrensgesetzes (VwGVG), BGBl I Nr 33/2013 ist sinngemäß anzuwenden.

Zu § 41 – Verfahren vor dem Bundesverwaltungsgericht

§ 41 schließt die aufschiebende Wirkung von Beschwerden gegen gewisse Bescheide der Behörde aus; im Einzelfall kann die aufschiebende Wirkung zuerkannt werden.

Zumindest im Hinblick auf die gemäß § 39 Abs 2, 3 und 4 Z 2 erlassenen Bescheide, das sind Durchsetzungsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen, erscheint dieser Automatismus überschießend und unverhältnismäßig. Hier sollte das Regel-Ausnahme-Verhältnis umgekehrt werden, sodass die aufschiebende Wirkung bereits ex lege und nicht nur ausnahmsweise über behördliche Zuerkennung eintritt.

Es wird daher angeregt, die Bezugnahme auf „§ 39 Abs 2, 3 und 4 Z 2“ in § 41 zu streichen.

Zu § 42 – Datenverarbeitung

Die NIS2-Richtlinie bietet keine Grundlage für eine derart umfangreiche Verarbeitung. Zwar wird eine Zusammenarbeit der CSIRTs (Art 10) und eine internationale Zusammenarbeit (Art 17) vorgesehen, jedoch nur im Einklang mit dem Datenschutzrecht der Union. Es ist dementsprechend kritisch zu hinterfragen, ob eine Verarbeitung in diesem Umfang erforderlich ist.

Insbesondere in Hinblick auf Informationen, die Geschäfts- oder Betriebsgeheimnisse enthalten, ist ein Erfordernis aus einem Cybersicherheits-Aspekt nicht einleuchtend. Weiters wäre aufgrund der missverständlichen Formulierung auch denkbar, dass Daten der Einrichtungen gem Art 9 DSGVO betroffen sein können, demnach besonders schützenswerte personenbezogene Daten. Im Sinne der Pflicht zur Datenminimierung gem Art 5 Abs 1 lit c DSGVO muss eine Einschränkung auf

technische Daten und solche personenbezogenen Daten, die unbedingt erforderlich sind (bspw um einen konkreten Cybersicherheitsvorfall aufzuklären) vorgenommen werden.

Zu § 42 Abs 2 - Aufzeichnungen

Es ist klarzustellen, was unter unternehmerischen Aufzeichnungen zu verstehen ist und wofür diese benötigt werden.

Zu § 43 - Datenübermittlung

Die Weiterleitung von personenbezogenen Daten an einen derart weitgehenden Empfängerkreis ist uE unverhältnismäßig. Eine Übermittlung personenbezogener Daten (inkl Geschäfts- oder Betriebsgeheimnissen, besonders geschützter personenbezogener Daten oÄ) an Behörden im Ausland (Abs 1 Z 6, Abs 2) ist uE abzulehnen. Eine Weiterleitung an andere Einrichtungen (Abs 3), die beispielsweise Konkurrenzunternehmen sind, sowie zwischen CSIRTs (Abs 4) sollte ausschließlich ohne Personenbezug, Identifizierbarkeit und Geschäfts- oder Betriebsgeheimnissen der betroffenen Einrichtung durchgeführt werden.

Zu § 44 - Verhängung von Geldstrafen (Bezirksverwaltungsbehörden)

Die Zuständigkeit der Bezirksverwaltungsbehörde sollte aus unserer Sicht angesichts der Komplexität der Regelungen und des hohen Strafrahmens überdacht werden. Wir regen – auch im Sinne einer bundesweit einheitlichen Strafpraxis an – die Zuständigkeit einer bundesweit einheitlichen fachlich spezialisierten Behörde zu übertragen.

Als unklar stufen wir die Frage ein, ob vor der Verhängung einer Verwaltungsstrafe durch die Bezirksverwaltungsbehörde gem § 44 NISG 2024 der Maßnahmenkatalog durch die Cybersicherheitsbehörde laut den Vorschriften des § 39 NISG 2024 ausgeschöpft werden muss, oder ob diese beiden Vorgänge parallel stattfinden können. In den Erläuterungen zu § 39 NISG 2024 heißt es, dass die Cybersicherheitsbehörde entsprechend den in den Abs 1 bis 4 vorgesehenen Maßnahmen vorzugehen hat. Des Weiteren wird in den Erläuterungen angemerkt, dass die bisherige Vorgehensweise nach dem NISG (Verstoß - Verfahrensanordnung - Bescheid und in weiterer Folge Sachverhaltsdarstellungen an die Bezirksverwaltungsbehörde) weitergeführt wird. Daran anschließend wird auch in § 44 Abs 1 NISG 2024 festgehalten, dass der Bundesminister für Inneres der Bezirksverwaltungsbehörde eine Verwaltungsübertretung anzuzeigen hat. Diese beiden Argumente sprechen dafür, dass erst nach Ausschöpfung der Maßnahmen durch die Cybersicherheitsbehörde Anzeige bei der Bezirksverwaltungsbehörde erstattet und anschließend eine Strafe verhängt werden kann.

Eine Klarstellung des Textes in diese Richtung wäre zu begrüßen.

Zu §§ 44, 45 – Geldstrafen und Verwaltungsstrafbestimmungen (natürliche Personen)

Die Strafbestimmungen der §§ 44 und 45 sind teilweise unbestimmt und damit insoweit verfassungsrechtlich problematisch. Es erscheint nicht ausgeschlossen, dass es die Bestimmungen ermöglichen, auch gegen natürliche Personen Geldstrafen in voller Höhe des Strafrahmens zu verhängen.

Nach dem Wortlaut des § 44 Abs 4 können Geldstrafen auch gegen verantwortliche Beauftragte und damit natürliche Personen verhängt werden. Die einzigen Strafrahmen, die das NISG 2024

umfassend für Verstöße gegen seine Pflichten vorsieht, sind die in § 45 Abs 2 und 3 NISG 2024 genannten Beträge von bis zu 7 bzw 10 Millionen Euro, weswegen diese Strafrahmen auch für die Verhängung von Strafen gegen natürliche Personen heranzuziehen wären.

Ein derartiges Vorgehen ist nach der NIS-2-RL nicht geboten, weil die RL die Verhängung ihrer Geldbußen nur gegen wesentliche und wichtige Einrichtungen und damit die Unternehmen selbst vorsieht; die NIS-2-RL legt augenfällig ein unternehmensbezogenes Konzept der Geldbuße zugrunde. Hier wäre bei den Strafrahmen – wie im deutschen Umsetzungsgesetz – entsprechend zu differenzieren, sodass die Millionenstrafrahmen gegen natürliche Personen nicht zur Anwendung gelangen.

Es wird angeregt, für die Verhängung von Geldstrafen ausschließlich gegen juristische Personen vorzusehen.

Zu § 45 Abs 1 Z 1 - Geldstrafen bei Verletzung der Registrierungsbestimmungen

Vor dem Hintergrund der Unklarheiten zum Anwendungsbereich und der kurzfristigen Umsetzung durch den Gesetzgeber erscheint der hohe Strafrahmen für die Verletzung von Registrierungs-bestimmungen unverhältnismäßig und wird von der NIS-2-Richtlinie auch nicht in diesem Ausmaß verlangt. Um „Gold Plating“ zu vermeiden, empfehlen wir einen eigenen – wesentlich geringeren – Strafrahmen einzuführen.

Zu § 45 - Verwaltungsstrafbestimmungen – Beraten statt Strafen

Entsprechend der NIS 2-RL können wesentliche Einrichtungen mit Strafen bis zu EUR 10 Mio oder 2% des Konzernjahresumsatzes und wichtige Einrichtungen mit Strafen bis zu EUR 7 Mio oder 1,4% des Konzernjahresumsatzes belegt werden.

Eine unabhängige Kontrollinstanz sowie eine Schlichtungsstelle wären hier unter Umständen erforderlich. Andernfalls bleibt nur der Weg zum Verwaltungsgerichtshof, der wohl gerade bei kleineren Beschwerden eine große Hürde darstellen würde.

Des Weiteren werden unangemessen hohe Verwaltungsstrafen für Verstöße bei nicht fristgerechter Registrierung (§45 Abs 1 Z 1), im Falle, dass Änderungen nicht bekannt gegeben werden (Z2) oder wenn eine Einrichtung nicht erreichbar ist (Z3), bei den weiteren Aufzählungen in §45 NISG, die nicht von §32 und §34 NISG umfasst sind (die die Umsetzung von Art 21 und 23 der NIS2-Richtlinie darstellen) vorgesehen.

Derart hohe Strafen sind nach der Richtlinie nur bei Verstößen gegen die Verpflichtung der Risikomanagementmaßnahmen und Berichtspflichten vorgesehen. Die konkrete nationale Umsetzung ist daher überschießend und derartige Strafhöhen sind bei dazu im Vergleich kleineren Verstößen (wie das Bekanntgeben von Änderungen der Kontaktdaten) nicht nachvollziehbar.

Es wird daher dahingehend um Differenzierung und Anpassung ersucht.

Abzustellen ist dabei nach dem Gesetzeswortlaut jeweils auf den weltweiten Umsatz des Unternehmens, dem die wesentliche oder wichtige Einrichtung angehört. Dies erscheint vor allem in jenen - praktisch weit überwiegenden - Fällen undeutlich, in denen sich bereits aus der Definition der wesentlichen/wichtigen Einrichtung ergibt, dass es sich dabei um ein

Unternehmen handelt sowie, wenn ein Unternehmen einer übergeordneten Unternehmensgruppe angehört.

Um nicht den ungewollten Anschein einer Konzernhaftung zu schaffen, ersuchen wir um Klarstellung, dass nur der Umsatz der betroffenen Einrichtung für §45 NISG 2024 herangezogen wird.

Ferner sollte am Vorbild des § 11 DSG – zumindest für KMU – ein gesetzlicher Vorrang für „Beraten statt Strafen“ bei erstmaligen Verstößen verankert werden, da es sich für tausende Unternehmen um gänzlich neue Rechtsvorschriften mit hoher Strafdrohung handelt und die strengen Verpflichtungen zu Cybersicherheit auch Kleinstunternehmen oder technologisch tendenziell wenig affine Branchen betreffen (zB industriell fertigende Bäckerei ab 50 Beschäftigten).

Weiters ist es unangemessen, alle Pflichten des Entwurfs der maximalen Sanktionsdrohung zu unterwerfen. So sollte beispielsweise das bloße Unterlassen der Registrierung (Z 1) oder wenn Kontaktdaten nicht zur Verfügung stehen (Z 3) nicht mit der maximalen Sanktionsdrohung behaftet sein.

Zu § 45 Abs 5 - Ausnahmeregelung

Eine klare Aufnahme von Körperschaften des öffentlichen Rechts sollte in § 45 Abs 5 erfolgen, um den Gleichklang mit § 30 Abs 5 DSG sicherzustellen. Dass dieser bestehen soll, ist auch in den Erläuternden Bemerkungen zu dieser Bestimmung klar ausgeführt.
Ohne diese Aufnahme könnte es zu einem „Auseinanderfallen“ der Bestimmungen kommen und somit zu Schwierigkeiten bei der Auslegung und Anwendung. Das entspräche nicht der Intention des Gesetzesgebers.

Es sollte daher in diesem Sinne die folgende Formulierung gewählt werden:

> Diese Bestimmung findet keine Anwendung auf Behörden, ~~und~~ sonstige Stellen der öffentlichen Verwaltung, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen und Körperschaften öffentlichen Rechts.

Zu § 51 – Inkrafttreten, Außerkrafttreten, Übergangsbestimmungen

Die Bestimmungen über das Inkrafttreten des Gesetzes lassen vermuten, dass die §§ 1 und 46 Abs 2 des NISG 2024 ab 18.10.2024 Geltung entfalten werden. Dieser Termin entspricht den Vorgaben der NIS 2-RL. Keinesfalls sollten die entsprechenden Verpflichtungen für die betroffenen Einrichtungen zu einem früheren Zeitpunkt in Kraft treten (zB am Tag nach Veröffentlichung des Gesetzes im BGBl).

Bereits die zeitgerechte gesetzeskonforme Ausrichtung wird für viele betroffene Einrichtungen zu einer nur sehr schwer überwindbaren Hürde werden. Die Anforderungen aus dem Gesetz sind umfassend und erfordern ausreichend Zeit für die Umsetzung.

Das in § 51 Abs 2 NISG 2024 vorgesehene phasenweise Inkrafttreten erachten wir als sinnvoll und würden eine längere Übergangfrist begrüßen.

Zu § 51 Abs 7 – Ausschluss von Übergangsfristen für Betreiber wesentlicher Dienste (NISG)

Die in § 51 Abs 7 normierte Ausnahme zum § 33 Abs 2 ist gröblich benachteiligend für alle darunterfallenden Unternehmen.

Das NISG 2024 normiert umfassende Änderungen und Erweiterungen sowohl was den Anwendungsbereich betrifft (bisherige Einschränkung auf wesentliche Dienste entfällt), als auch von Pflichten im Vergleich zum geltenden NISG. Daher benötigen alle Unternehmen eine angemessene Vorlaufzeit, um diese umzusetzen und durch eine Prüfung durch eine unabhängige Stelle nachzuweisen. Dies betrifft insbesondere die technischen, operativen und organisatorischen Risikomanagementmaßnahmen in den Bereichen der Anlage 3, wobei der Verordnungsinhalt hier noch gänzlich offen ist.

Durch den in § 51 Abs 7 normierten Ausschluss der Dreijahresfrist müssen einzelne Unternehmen teils binnen weniger Monate nach Inkrafttreten des Gesetzes bereits die Prüfung durch eine unabhängige Stelle nachweisen, während wesentliche Einrichtungen, die nicht Betreiber wesentlicher Dienste iSd NISG sind, dafür drei Jahre nach Aufforderung zur Selbstdeklaration Zeit haben.

Anders als vorgesehen (Erläuterungen: „Diese Abweichung…erlaubt es Prüfprozesse weiterzuführen und reduziert die wirtschaftlichen Auswirkungen des Bundesgesetzes“) hat dies eine enorme wirtschaftliche Mehrbelastung für die bisherigen Betreiber wesentlicher Dienste zur Folge.

Auch vor dem verfassungsrechtlich gebotenen Gleichheitssatz empfehlen wir daher die ersatzlose Streichung des § 51 Abs 7.

Anlage 1 – Sektoren mit hoher Kritikalität

Zu Anlage 1 – Betreiber von Ladepunkten

Nachdem die Definition in Anhang I der NIS 2-RL („*Betreiber von Ladepunkten, die für die Verwaltung und den Betrieb eines Ladepunkts zuständig sind und Endnutzern einen Aufladedienst erbringen, auch im Namen und Auftrag eines Mobilitätsdienstleisters*“) gegenüber der Definition in Anhang I des NISG 2024 abweicht, ist völlig unklar, ob ein Ladepunktbetrieb, den ein Unternehmen nur für die Auflademöglichkeit seiner eigenen Mitarbeiter bzw der eigenen Mitarbeiter und Poolfahrzeuge unterhält, tatsächlich vom Gesetz umfasst sein soll.

Darüber hinaus würde der Verweis auf § 2 Z 3 Bundesgesetz zur Festlegung einheitlicher Standards beim Infrastrukturaufbau für alternative Kraftstoffe, BGBl I Nr 38/2018, dazu führen, dass grundsätzlich jeder Ladepunktbetrieb, auch der von privaten „Wallboxen“ grundsätzlich unter Anhang I fiele, was wohl nicht der Wille des Gesetzgebers sein kann.

Wir regen eine Klarstellung mittels eingeschränkter Definition unmittelbar in Anlage I an und plädieren für eine Ausnahme von firmeninternen Ladelösungen an Betriebsstandorten bzw Anwendbarkeit des NISG 2024 lediglich auf Betreiber von öffentlich zugänglichen Ladepunkten im Sinne des Bundesgesetzes zur Festlegung einheitlicher Standards beim Infrastrukturaufbau für alternative Kraftstoffe, BGBl I Nr 38/2018.

Zu Anlage 1 - Rechenzentrumsdienste

Die Sektorbeschreibung zu „Rechenzentrumsdiensten“ ist nicht für Unternehmen mit komplexen Strukturen definiert. Geht man davon aus, dass ein Konzern eine zentrale IT-Abteilung und ein zentrales Rechenzentrum betreibt, um konzernweite IT-Services anzubieten, wäre das im Sinne der Definition ggf als *„Anbieter von Diensten, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden („Rechenzentrumsdienste“)“* zu sehen.

Derzeit wird davon ausgegangen, dass konzerninterne Rechenzentrumsdienste nicht in den Geltungsbereich der NIS 2-RL fallen. Ungeachtet weiterer Sektoren, unter die das Unternehmen ggf noch fallen würde, wäre ein solche zentrale Dienste zur Verfügung stellendes Unternehmen – je nach Größe – ggf als wesentlich oder wichtig zu deklarieren.

Um diesen offenen Punkt zu klären, ist eine genauere Spezifizierung hinsichtlich komplexer Unternehmensstrukturen notwendig und insbesondere die Ausnahme von konzerninternen Rechenzentrumsdiensten festzulegen.

Zu Anlage 1 Z 5 - Gesundheitswesen

Anwendungsbereich

Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Art 22 der Verordnung (EU) 2022/123 eingestuft werden, fallen in den Anwendungsbereich des NISG 2024. Solch eine Liste der kritischen Medizinprodukte wird allerdings erst nach der Feststellung einer Notlage im Bereich der öffentlichen Gesundheit erstellt. Es ist somit zu bezweifeln, dass über diese Feststellung eine rechtzeitige Prävention bei den Herstellern von „kritischen“ Medizinprodukten möglich ist. Das Setzen von Präventionsmaßnahmen erst nach dem Eintritt einer Notlage ist wohl zu spät. Andererseits muss verhindert werden, dass Medizinprodukte, von denen rund 500.000 unterschiedliche Produkte zugelassen sind, zu umfassend und überschießend in die Bestimmungen aus dem NISG 2024 fallen. Eine anwendbare Liste kritischer Medizinprodukte auf EU-Ebene ist derzeit nicht bekannt.

Hier wäre die Zurverfügungstellung einer indikativen Liste hilfreich.

Ferner sollte in den Erläuterungen klargestellt werden, dass die Bestimmung erst Wirksamkeit entfaltet, sobald eine entsprechende Liste vorhanden ist.

Frage der Betroffenheit bestimmter gewerblicher Berufsgruppen

Die Berufsgruppen der Gesundheitsberufe aus der Bundessparte Gewerbe (im Einzelnen Augenoptiker/Kontaktlinsenoptiker, Hörgeräteakustiker, Orthopädieschuhmacher/Schuhmacher, Orthopädietechniker/Bandagisten, Zahntechniker) stellen unterschiedliche Medizinprodukte, die als kritisch eingestuft werden könnten, her bzw passen diese an. Bei Recherchen wurde lediglich die Liste der EMA für Arzneimittel gefunden.

Die „Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“, welche genannt wird, gibt es unseres Wissens noch nicht.

Zudem ist unklar, wer unter den Begriff „Gesundheitsdienstleiter“ fällt. Es wird auf folgende Definition in der RL 2011/24/EU verwiesen: „Gesundheitsdienstleister“ jede natürliche oder

juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt; eine Definition von „Gesundheitsdienstleistungen“ findet sich in der genannten Richtlinie nicht.

Betriebe der Bundessparte Tourismus und Freizeitwirtschaft

Für die Mitgliedsbetriebe der Bundessparte Tourismus und Freizeitwirtschaft, die im Gesundheitsbereich tätig sind, ist aufgrund der ausdrücklichen Erwähnung des Gesundheitswesens in Anlage 1 Punkt 5 zum NISG 2024 und des darin genannten Begriffs der Gesundheitsdienstleister bei Erreichen der Unternehmensgrößen-Schwellenwerte eine Betroffenheit vom NISG 2024 gegeben. Für Betriebe mit mehr als 50 Mitarbeiterinnen und Mitarbeitern bedeutet dies somit einen zusätzlichen personellen, administrativen und vor allem finanziellen Aufwand, den die Betriebe aus eigenen Mitteln leisten müssen und dies in Zeiten von ohnehin schon hohen Kostensteigerungen in allen Bereichen!

Der Begriff des Gesundheitsdienstleisters ist dabei sehr vage und nur durch einen Verweis auf die Patientenmobilitätsrichtlinie (Art 3 lit g) und die dortige Begriffsbestimmung definiert, nämlich: „Gesundheitsdienstleister“ ist jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt.

Etwas mehr Klarheit bringen diesbezüglich die erläuternden Bestimmungen zum Gesetzesentwurf, die diesbezüglich auf die Aufzählung in der Anlage 1 der Gesundheitstelematik-VO 2013 verweisen. Allerdings hat auch diese Liste vorwiegend demonstrativen Charakter und lässt Anwenderfragen offen.

Daher wäre es hier essenziell, dass sich klar und abschließend dem Gesetz entnehmen lässt, welche Berufsgruppen und Einrichtungen nun tatsächlich als Gesundheitsdienstleister im Sinne des NISG 2024 zu sehen sind und somit entsprechende Vorkehrungsmaßnahmen zu treffen haben.

Positiv ist, dass sich in den Erläuternden Bestimmungen nun etwas klarere Aussagen betreffend den Bereich der Pflege finden. So wären Dienstleistungen der Langzeitpflege und damit einhergehend Einrichtungen der Pflege und Pflegeanstalten nicht vom Anwendungsbereich der NIS-2 RL und somit des NISG 2024 umfasst. Für die Abgrenzung zwischen Pflege in einem Pflegeheim und Pflege in einer Krankenanstalt sei in Folge darauf abzustellen, ob die Betroffenen eine ständige Pflege oder aber bloß fallweise einer ärztlichen Betreuung bedürfen. Überwiegt der Pflegeaspekt, liegt ein Pflegeheim vor, überwiegt der Bedarf an ärztlicher Betreuung, eine Krankenanstalt.

Diese ausdrückliche Ausnahme des Pflegebereiches vom NIS-Anwendungsbereich sowie die Abgrenzung von Pflegeheim und Krankenanstalt ist von großer Relevanz für unsere Mitgliedsbetriebe in diesem Bereich und sollte so jedenfalls Eingang in das Gesetz finden.

Im Lichte des Umstandes, dass die gegenständliche Regelung mit 18.10.2024 in Kraft treten wird und noch einige Verordnungsermächtigungen vorgesehen sind (§ 32) und daher mit weiteren nationalen Verordnungen zu rechnen ist, ergibt sich eine erhebliche Rechtsunsicherheit für betroffene Unternehmen. Letztere wissen weiterhin nicht, welche Maßnahmen zB für das Risikomanagement vorgesehen und umzusetzen sind. Der Aufwand für die Betriebe ist enorm, daher wäre eine rechtzeitige Kenntnis der Pflichten und Maßnahmen wünschenswert.

Zu Anlage 1 Z 15 - Konkretisierung - Definition "Anbieter digitaler Dienste“

Unklar und weiterhin offen ist, ob damit tatsächlich sämtliche Anbieter von beispielsweise Software as a Service-Lösungen (welche ebenfalls als Cloud-Computing Lösungen anzusehen sind) als wesentliche Einrichtung einzustufen sind - sofern dies bejaht werden würde, würden

sämtliche Unternehmen, die an sich als unkritisch anzusehen sind oder nur als Nebendienstleistung SaaS-Dienstleistungen (wie Softwarelösungen zusätzlich zu einem vernetzten Produkt) anbieten, als wesentliche Einrichtung gelten und es würden ihnen strengere Sorgfaltspflichten auferleget werden. Fraglich ist, ob dies tatsächlich von der ratio der NIS2-RL gedeckt ist und ob eine solche ausufernde Auslegung bedacht worden ist.

Es wird hier daher um eine entsprechende Konkretisierung und ergänzende Erläuterungen ersucht.

Zu Anlage 1 Punkt 1 lit a) - Energie, Teilsektor Elektrizität

Es handelt sich bei den erfassten Unternehmen um „Marktteilnehmer im Sinne des Art 2 Z 25 Verordnung 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Art 2 Z 18, 20 und 59 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU, ABl L 158 vom 14.6.2019, S 125 anbieten“.

In Bezug auf den Teilsektor Regelenergie sollte – ähnlich wie im Fall des Teilsektors Fernwärme (Anlage I Punkt 1 lit b) – in den Erläuterungen zum NISG 2024 eine Klarstellung dahingehend mitaufgenommen werden, dass Industrieunternehmen, die nicht unmittelbar als Marktteilnehmer auf einem organisierten Elektrizitätsmarkt im Sinne von Artikel 2 Ziffer EU Durchführungsverordnung 1348/2014 auftreten, sondern lediglich aufgrund von Anfragen eines Netzbetreibers an einen Aggregator Strommengen zum Zwecke der Stabilisierung der Netzinfrastruktur beziehen, nicht in den Anwendungsbereich der NISG 2024 fallen.

Eine solche Klarstellung in den Erläuterungen zum NISG 2024 erscheint uns unter folgenden Erwägungen sachgerecht zu sein:

Der überwiegende Teil der österreichischen Industrieunternehmen, die an Regelenergiemärkten teilnehmen, bedient sich der Dienstleistungen eines Aggregators. Dabei beschränkt sich die Tätigkeit/Funktion der Industrieunternehmen auf die physische Abnahme von Strommengen aus dem Stromnetz (Regelenergie) aufgrund einer Anfrage des Netzbetreibers an den Aggregator.

Nachdem Industrieunternehmen in dieser Konstellation weder Dienste zum Zwecke der Bilanzierung, Aggregierung oder Energiespeicherungen erbringen noch als eigenständige Marktteilnehmer auf einem organisierten Elektrizitätsmarkt im Sinne von Art 2 Z EU Durchführungsverordnung 1348/2014 agieren, erscheint es sachgerecht zu sein, diese Industrieunternehmen vom NISG 2024 Anwendungsbereich auszunehmen.

Ähnlich wie im Fall des Teilsektors Fernwärme könnte diese Klarstellungen wohl auch durch einen entsprechenden Hinweis in den Erläuterungen zum NISG 2024 erfolgen.

Zu Anlage 1 Z 7 - Abwasser

Der Sektor Abwasser Anlage 1 Z 7 stellt auf Unternehmen ab, „die kommunales, häusliches oder industrielles Abwasser […] sammeln, entsorgen oder behandeln, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung, oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist“.

Hier stellt sich definitiv die Frage, nach welchen Kriterien festgestellt werden kann, ob die Haupttätigkeit des Unternehmens vorliegt (zB Umsatz der einzelnen Bereiche, Anzahl der Beschäftigten etc).

Wenn man diese Frage nicht beantwortet, so wird immer die Gefahr bestehen, dass sich ein Unternehmen nicht als NIS–unterworfen sieht und sich dadurch verwaltungsrechtlich, aber unter Umständen auch zivilrechtlich mit negativen Folgen (Strafen, Schadenersatzforderungen, versicherungsrechtlichen Problemen) konfrontiert sieht.

Gerade derart unklare Abgrenzungen zeigen die Notwendigkeit eines Feststellungsbescheids zur Schaffung von Rechtssicherheit in Bezug auf den Anwendungsbereich in unklaren Fällen auf.

Wir sprechen uns neben der Festlegung konkreter Kriterien dafür aus, dass ganz generell die Unternehmen auch im Rahmen des NISG die Möglichkeit haben sollen, einen Feststellungsbescheid zu beantragen, um herauszufinden, ob ihr Unternehmen unter das NISG fällt oder nicht.

Anlage 2 – Sonstige kritische Sektoren

Zu Anlage 2 Z 1 – Post- und Kurierdienste

Mit der Einbeziehung von Post- und Kurierdiensten in den Anwendungsbereich des Gesetzes steigt für die österreichische Transportwirtschaft auch der Verwaltungsaufwand erheblich.

Da Post- und Kurierdienste iSd § 3 Z 3 und 4a PMG, in Anlage 2 des Entwurfs als Sektor mit hoher Kritikalität definiert werden und gemäß § 24 des Entwurfs die in Anlage 1 und 2 genannten Einrichtungen, wenn sie ein großes oder mittleres Unternehmen betreiben, als wichtige Einrichtung gelten („Kurierdienste“), fällt für Kurierdienste eine bürokratische Doppelbelastung an, da sie sowohl nach dem PMG als auch nach dem vorliegenden Entwurf zahlreiche Pflichten treffen.

Es sollte hier danach getrachtet werden, bereits bestehende Mechanismen und Zertifizierungen in diesem Bereich tunlichst anzuerkennen, um zusätzliche Belastungen in einem geringst-möglichen Umfang zu halten.

Zu Anlage 2 Z 3 - Produktion, Herstellung und Handel mit chemischen Stoffen

Wir halten den Verweis auf die REACH-Verordnung, bei der es um die Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe geht und den die Richtlinie vorgibt, für äußerst unglücklich und missverständlich. Die Rechtsmaterien passen nicht zueinander, wodurch eine juristisch korrekte Bewertung der Betroffenheit unmöglich ist. Unter REACH gibt es verschiedene Rollen (Importeur, Hersteller, nachgeschalteter Anwender, etc.), die zur Formulierung der RL (Herstellung, Handel) nicht passen. Hier treffen verschiedene Rechtsmaterien aufeinander, die in der Praxis nicht zusammenpassen, was zahlreiche Abgrenzungsprobleme und damit Rechtsunsicherheit verursacht. Klarstellungen wären äußerst wünschenswert.

So sollte zB präzisiert werden, dass durch eine Vermischung von chemischen Produkten kein neues chemisches Produkt entsteht, sondern eine bloße Verwendung im Sinne Art 3 Z 4 REACH-Verordnung vorliegt. Konkret sollte beispielsweise klargestellt werden, dass folgende Tätigkeiten nicht in den Anwendungsbereich fallen: ein Farbenhändler, der zwei Farben mischt oder das Mischen von Zement, Wasser und Sand zu Mörtel auf der Baustelle; ein Energiehändler, der Diesel mit einem Farbstoff versieht, um daraus Heizöl zu machen oder Winterdiesel, bei dem Diesel ein Additiv zugesetzt wird.

Zu den sonstigen kritischen Sektoren zählt laut Anlage 2 auch der Handel mit chemischen Stoffen. Wir gehen nicht davon aus, dass hiervon auch Möbelhäuser betroffen sind, die beispielsweise Möbel-, Leder- oder etwa Bodenpflegemittel/-polituren verkaufen, da eben keine Produktion bzw Herstellen erfolgt, sondern nur der Verkauf.

Eine Klarstellung in den Erläuterungen zu Anlage 2, Punkt 3 (Sektor „Produktion, Herstellung und Handel mit chemischen Stoffen"), wonach der reine Handel mit chemischen Stoffen nicht in den Anwendungsbereich fällt, wird daher gefordert. Daher wird um Aufnahme des klarstellenden Satzes ersucht: *„Reine Händler fallen nicht in den Anwendungsbereich des NISG 2024."*

Ferner sollte in den Erläuterungen auch eine Klarstellung erfolgen, dass Großhändler nicht in den Anwendungsbereich des NISG 2024 fallen, wenn sie nicht gleichzeitig Stoffe iSd Art 3 Z 9 der Verordnung (EG) Nr 1907/2006 herstellen.

Auch im Bereich Produktion stellt sich die Frage, welche Unternehmen gemeint sind, die Erzeugnisse iSd Art 3 Z 3 REACH VO aus Stoffen oder Gemischen produzieren. Letztendlich bestehen die meisten Produkte aus Stoffen oder Gemischen (zB Kugelschreiber, Tisch, Buch, etc.).

- Beispiel Baumarkt, der Farben mischt oder Platten zuschneidet/verleimt; Anwendungsbereich: Tischlerei, Papierindustrie, Stahlproduktion, Futtermittelhersteller, etc.
- Beispiel Baubereich: Mischen von bestimmten Stoffen vor Ort auf der Baustelle zB Beton, Gips, Anstriche, etc.
- Beispiel Gebäudereiniger: Arbeiten mit chemischen Reinigungsmitteln, durch Anmischen/Abfüllen vor Ort – hier sollte nicht von Produktion ausgegangen werden.

Zu Anlage 2 Z 4 – Lebensmittelunternehmen (Lebensmittelhandel)

Gemäß Anlage 2 Z 4 soll das NISG 2024 auf Lebensmittelunternehmen zur Anwendung kommen, die „im Großhandel" oder „in der industriellen Produktion und Verarbeitung" tätig sind. Demnach sollen Lebensmittelgroßhändler entsprechender Unternehmensgröße in den Anwendungsbereich fallen, selbst wenn sie keinerlei Tätigkeit der industriellen Produktion und Verarbeitung verüben. Dies stellt uE ein erhebliches „Gold-Plating" durch den österreichischen Gesetzgeber dar und wird abgelehnt, da es die Konkurrenzfähigkeit österreichischer Lebensmittelunternehmen im Binnenmarkt unnötig gefährdet und den Wirtschaftsstandort schädigt.

Aus dem Text des Anhangs II Z 4 der NIS-2-RL ergibt sich nach Heranziehung sämtlicher Auslegungsmethoden sowie Berücksichtigung der englischen, französischen sowie spanischen Richtlinienversionen unzweifelhaft, dass nur jene Lebensmittelunternehmen in den Anwendungsbereich fallen sollen, welche (kumulativ!) im Großhandel und in der industriellen Produktion und Verarbeitung tätig sind. Hätte der Richtliniengesetzgeber eine alternative Verknüpfung statuieren wollen, wäre anstelle der Wörter „und" oder „sowie" ein „oder" eingefügt worden; wäre intendiert gewesen, lediglich den Einzelhandel aus dem Anwendungsbereich auszunehmen, wäre schlicht eine explizite Ausnahme vorgesehen worden. Der NIS-2-RL zu unterstellen, sie sei zwingend dahingehend auszulegen, dass die dort gebrauchten Worte „sowie" und „und" als alternative Satzteilverknüpfungen zu verstehen sind, erscheint uE dogmatisch nicht tragbar. Die Erstreckung der NIS-2-Pflichten auf reine Großhändler, ist daher überschießend und unverhältnismäßig - nach derzeitigem Entwurfswortlaut würden Agrargroßhändler (zB Obst-, Gemüse- und Eierhändler) in den Anwendungsbereich fallen.

Sollte ein Lebensmittelgroßhändler als kritische Einrichtung iSd RKE-RL eingestuft werden, würde dieser ohnehin gem § 24 Abs 1 Z 1 lit f des gegenständlichen Entwurfs als wesentliche Einrichtung dem NISG 2024 unterliegen.

Änderungsvorschlag:

> „Lebensmittelunternehmen im Sinne des Art. 3 Z 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit, ABl. L 31 vom 1.2.2002 S. 1, die im Großhandel UND in der industriellen Produktion und Verarbeitung tätig sind."

Eine entsprechende Klarstellung sollte in den Erläuterungen aufgenommen werden.

Zu Anlage 2 Z 4 – Produktion, Verarbeitung und Vertrieb von Lebensmitteln

Die sektorale Betroffenheit bzw Nicht-Betroffenheit betreffend die *industrielle* Produktion und Verarbeitung von Lebensmitteln ist im Sinne einer Gesamtbetrachtung des Unternehmens selbst vorzunehmen (Selbsteinschätzung). Eine Dokumentation der Entscheidungskriterien wird empfohlen.

Eine industrielle Produktion ist durch die überwiegende Erfüllung der in § 7 GewO angeführten Kriterien gekennzeichnet.

Zu Anlage 2 Z 5 – Verarbeitendes Gewerbe/Herstellung von Waren

In Anlage 2 werden weitere kritische Sektoren definiert. Enthalten ist hier auch das verarbeitende Gewerbe/Herstellung von Waren. Zieht man die Herstellung von elektronischen Ausrüstungen heran, so sind hier Unternehmen angeführt, die Wirtschaftstätigkeiten in den angeführten NACE-Codes ausüben.

Hier ist der Umfang der „Herstellung" nicht ausreichend definiert. Sieht man die Definition der Herstellung als "serienmäßige, maschinelle Herstellung von Gütern, Waren", so ergeben sich insb. im Zusammenhang mit komplexen Unternehmensstrukturen Fragestellungen, welche juristischen Personen hier genau betroffen sind.

Betrachtet man in Konzernstrukturen die Herstellung von Waren, so sind hier derzeit nur die tatsächlichen Produktionswerke zu sehen, sofern sie eine eigene juristische Person sind. Unklar bleibt, ob ggf weitere juristische Personen im Konzern oder die Konzernmutter, wenn diese den NACE-Codes entsprechen, auch zu registrieren sind. Des Weiteren ist unklar, ob der Begriff „Herstellung" ggf auch eine Produktentwicklung einschließt.

Daher ist hier eine genaue Definition der Begriffe „Herstellung" und „verarbeitendes Gewerbe" notwendig, insbesondere für komplexe Unternehmensstrukturen.

Offene Fragen der Papierindustrie

Positiv ist anzumerken, dass laut Erläuterungen zur Anlage 1 Unternehmen, die lediglich Fernwärme in ein Fernwärmenetz einspeisen (ohne zugleich Betreiber des Fernwärmenetztes zu sein), vom NIS 2 Anwendungsbereich ausgenommen sind.

Aufgrund der Tatsache, dass mehrere der Papier-Produktionsstandorte am Energiemarkt (Regelenergie) teilnehmen, könnte es aber sein, dass sie über diese Markteilnahme doch in den NIS 2 Anwendungsbereich fallen.

Vielleicht könnte man auch für diesen kritischen Teilsektor – ähnlich wie im Fall der Fernwärme – in den Erläuterungen eine Klarstellung dahingehend aufnehmen, dass der (bloße) Strombezug von Überschusskapazität (ohne dass dabei weitere Dienstleistungen erbracht werden, die üblicherweise ein Bilanzkreisverantwortlicher zu erbringen hat) nicht in den NIS 2 Anwendungsbereich fällt.

Leider konnten wir auch in den Erläuterungen keine Antwort auf unsere Frage finden, ob Papierfabriken, die Papier und/oder Zellstoff produzieren, grundsätzlich in den Anwendungsbereich der NIS 2 Richtlinie fallen. Wir gehen bisher davon aus, dass das nicht der Fall ist. Nach REACH-Experten könnte allerdings über den Sektor „Produktion, Herstellung und Handel mit chemischen Stoffen“ im Anhang II der RL (sonstige kritische Sektoren) bzw. Anlage 2, Punkt 3 eine Betroffenheit bestehen.

Wir ersuchen um Klärung dieser Frage bzw Aufnahme entsprechende Hinweise in die Erläuterungen.

Anlage 3 – Risikomanagementmaßnahmen-Bereiche

In Art 21 (2) der NIS2-Richtlinie waren 10 Risikomanagementmaßnahmen aufgelistet. Diese wurden in Anlage 3 des NISG 2024 präzisiert bzw. erweitert. Unser grundsätzliches Verständnis war, dass sich die Risikomanagementmaßnahmen zu einem großen Teil an der ISO 27001 Version 2013 orientieren. Aktuell ist jedoch bereits die ISO 27001 Version 2022 gültig.

Wir plädieren daher dafür, die mittlerweile 13 Risikomanagementmaßnahmen strukturell möglichst nahe an die neue Version der ISO 27001:2022 anzupassen.

Zu Anlage 3 Punkt 6 bzw 6a

Während die NIS2-Richtlinie in ihren Erwägungsgründen (siehe ErwG 49, 50 und vor allem 89 für wesentliche und wichtige Unternehmen) mehrfach zumindest punktuell auf den Begriff der Cyberhygiene eingeht, wird dieser in den erläuternden Bemerkungen zum NISG 2024 nicht erwähnt und kommt er im NISG 2024 nur in Bezug auf die Bürgerinnen und Bürger sowie auf KMU vor. Da der Begriff Cyberhygiene aber in Hinkunft von wesentlichen und wichtigen Unternehmen umzusetzen ist, sollte er entsprechend eindeutig beschrieben sein.

Wir regen an, für den Begriff der Cyberhygiene eine entsprechende Definition im NISG 2024, idealerweise in § 3 (Begriffsbestimmungen) vorzusehen.

Zu Artikel 2

Änderung § 44 TKG 2021

Artikel 2 mit der Änderung von § 44 TKG 2021 fällt unter dem Aspekt der NIS-Regulierung aus dem Rahmen. Die NIS 2-Richtlinie 2022/2555 sieht in Artikel 34 ausdrücklich die Änderung des EECC (Richtlinie EU 2018/1972, kurz: EECC) dahingehend vor, dass die Artikel 40 und 41 gestrichen werden. Diese beiden Artikel wiederum wurden im TKG 2021 mit § 44 umgesetzt, dem

also nach dem genannten Datum die unionsrechtliche Verankerung fehlen würde, er sohin als nationales Recht ohne europarechtliche Basis im engeren Sinne bestehen würde, was grundsätzlich möglich wäre.

Allerdings sehen wir trotz der Erläuterungen im Entwurf doch deutliche Abgrenzungsfragen zum vom NISG 2024 erfassten Regelungsbereich. Hier muss man sicherlich zuerst dem Richtliniengeber vorhalten, dass er die Ziele des EECC dort in Art 2 Abs 2 lit a nicht angepasst hat, nämlich die Sicherheit von Netzen und Diensten zu gewährleisten. So bleibt dann Platz für die Argumentation, dass aufgrund der darauf gründenden und fortbestehenden Zielbestimmung des TKG 2021 (§ 1 Abs 2 Z 4) die bisherige Regulierungsbehörde mit Verordnung nähere Vorgaben über technische und organisatorische Sicherheitsmaßnahmen festlegen kann. Damit läge eine Regulierung im Kernbereich des NISG 2024 vor, weshalb nach den Erläuterungen eine „ausdrückliche“ Subsidiarität (wiewohl unklar bleibt, was diese von einer nicht ausdrücklichen Subsidiarität unterscheidet) angeordnet werden soll, um eine „Normenkollision“ zu vermeiden.

Wir sehen nicht, dass die in den Bestimmungen des NISG 2024 vorgesehenen Maßnahmen nicht zur Erreichung eines hohen Cybersicherheitsniveaus (und auch dem Ziel von § 1 Abs 2 Z 4 TKG) ausreichen könnten. Sollte es im Einzelfall Nachbesserungsbedarf geben, dann kann dies mit den Vorkehrungen des NISG 2024 bewerkstelligt werden. Wir sehen vielmehr die konkrete Gefahr einer Doppelregulierung derselben Materie, ohne dass dies einen Zusatznutzen im Hinblick auf die Sicherheit von Netzen und Diensten der Telekommunikationsbranche bringen würde. Ein möglicher Mehraufwand im Meldefall, gar eine zweite Meldeverpflichtung über eine separate Meldeschiene, wäre ein weiterer abzulehnender Aspekt.

Im Hinblick auf den vorgeschlagenen § 44 Abs 3 Z 1 TKG 2021 ist anzumerken, dass wir auch weiterhin eine alle paar Jahre durchgeführte Risikoanalyse für den Telekommunikationssektor begrüßen, wiewohl dies künftig eine Aufgabe für ein CSIRT oder Branchen-CSIRT sein könnte, deren Aufgaben mit § 8 Abs 1 skizziert sind und dies ohne weiteres umfassen könnte. Sie könnte mit dem bei der Behörde und bei den dabei mitarbeitenden Unternehmen gewachsenen Know how nahtlos weitergeführt werden.

Gleiches gilt für die „Erstellung eines Mustersicherheitskonzeptes für Betreiber“ nach Z 2, das aufgrund der Bedeutung für die Erreichung eines hohes Cybersicherheitsniveaus ebenfalls in § 8 Abs 1 als Thema im Grunde angelegt ist. Wir empfehlen hier außerdem eine Einbeziehung des Fachverbandes Telekom-Rundfunk, der alle Unternehmen der Branche umfasst und adressiert.

Für die nach Z 3 vorgesehene Mitwirkung in Arbeitsgruppen der ENISA wäre folglich auch eine neue Zuständigkeit gegeben. Die im NISG 2024-E gemäß § 5 Abs 2 Z 2, § 29 Abs 6 und § 34 Abs 5 vorgesehenen Berührungspunkte mit der ENISA sollten um sinnvolle Mitwirkungen in deren Arbeitsgruppen ergänzt werden.

Konsequenterweise wäre bei einem Entfall von § 44 TKG 2021 auch § 34 Abs 8 grundsätzlich zu streichen. Allerdings sehen wir hier einen möglichen Informationsbedarf Richtung Regulierungsbehörde/RTR GmbH hinsichtlich der Aufgabenerfüllung nach § 45 TKG, der mit dem Wegfall von § 44 TKG keine Einschränkung erfährt und wiederum auf die Empfehlung (EU) 2019/534 der europäischen Kommission zurückgeht (dazu auch im nächsten Absatz).

Ungeklärt wäre dann weiters, ob und wie die Regelungen aus der Telekom Netzsicherheits-verordnung (TK-NSiV 2020) fortgeführt und verankert werden könnten und wie künftig die „EU

toolbox for 5G security“ (EU-Instrumentarium für 5G-Sicherheit) oder die einzelnen Aspekte davon im nationalen Recht verankert sein“ würden.

III. Zusammenfassung

Der vorliegende Vorschlag für eine NIS 2024 Novelle wird seiner Zielsetzung nach grundsätzlich begrüßt, ebenso wie der Umstand, dass der österreichische Gesetzgeber großteils geneigt ist, im Wege einer richtliniennahen Umsetzung Gold Plating zu vermeiden.

Allerdings bestehen in der NIS 2-Richtlinie selbst zahlreiche Regelungen, die es für Unternehmen herausfordernd machen, zu erkennen, ob sie den neuen, deutlich umfangreicheren Vorgaben und Verpflichtungen zur Cybersicherheit unterliegen oder nicht und wie betroffene Einrichtungen die einschlägigen Vorgaben gegebenenfalls umsetzen können. Gerade betreffend den Anwendungsbereich bleiben viele Fragen, die sich bereits betreffend die NIS 2-Richtlinie gestellt hatten, offen. Eine möglichst verbindliche Klärung erscheint hier vordringlich und so sollten vor allem in den aufgezeigten Bereichen Nachschärfungen von Definitionen bzw Klarstellungen vorgenommen werden, geht es doch allem voran um Rechtssicherheit für die betroffenen Einrichtungen. Auch die vom noch geltenden NIS-G betroffenen Einrichtungen sind durch den erweiterten Anwendungsbereich des künftigen NIS-Rahmen in Österreich stark gefordert.

Darüber hinaus wird es darum gehen, die zahlreichen neu in die Verpflichtungen zur Cybersicherheit einbezogenen Einrichtungen an die Thematik heranzuführen, um vor allem auch Akzeptanz für das neue Regime zu erreichen. Dazu wird aus unserer Sicht gerade auch bei kleineren Unternehmungen und geringfügigen Übertretungen die konsequente Anwendung des Grundsatzes „Beraten statt Strafen“ zu gehören haben.

Unbestrittenermaßen ist Cybersicherheit ein zentrales Element modernen Wirtschaftens. Umso wichtiger ist es, angesichts stetig wachsender Bedrohungen Informationen über aktuelle Vorfälle zwischen Normunterworfenen und Behörden - in beide Richtungen - zu teilen und damit rasche Reaktionen auf solche Bedrohungsszenarien zu ermöglichen.

Gerade was den Vollzug der Regelungen zur Cybersicherheit betrifft, kann Österreich bereits auf wertvolle Erfahrungen zurückblicken. Auch unter dem neuen, wesentlich weiterreichenden Rechtsrahmen für die Cybersicherheit nach dem NISG 2024 sollte auf bewährten Strukturen (zB Austausch in der Cybersicherheit-Plattform) und Methoden (Standards und Best Practices) aufgebaut werden, um Cybersicherheit in Österreich bestmöglich faktisch sicherzustellen, ohne Unternehmen aber dabei zu überfordern oder ihnen unnötige zusätzliche Belastungen aufzuerlegen.

Wir ersuchen um Berücksichtigung unserer Anmerkungen. Diese Stellungnahme wird auch per Webformular im Rahmen des parlamentarischen Begutachtungsverfahrens übermittelt.

Freundliche Grüße

Dr. Harald Mahrer
Präsident

Karlheinz Kopf
Generalsekretär

Unterzeichner	**Wirtschaftskammer Österreich**
Datum/Zeit-UTC	**2024-04-29T11:16:30+02:00**
Aussteller-Zertifikat	**CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT**
Serien-Nr.	**2033604334**
Hinweis	**Dieses Dokument wurde amtssigniert.**
Prüfinformation	**Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter https://www.signaturpruefung.gv.at/.**