oesterreichs energie.

GENERALSEKRETARIAT

Bundeskanzleramt
I/8 (Technologie- und Datenmanagement,
Cybersicherheit und Krisenrechenzentrum)
Ballhausplatz 2
1010 Wien

Per E-Mail an: nis@bka.gv.at

Kontakt	DW	Unser Zeichen	Ihr Zeichen	Datum
[DI Selhofer Armin	232	ARS/CF – 06/2024	Geschäftszahl: 2024-0.220.735	29.04.2024

NISG 2024 – Stellungnahme von Oesterreichs Energie

Sehr geehrte Damen und Herren,

wir bedanken uns für die Übermittlung des aktuellen Entwurfs des Bundesgesetzes, mit dem das neue Netz- und Informationssystemsicherheitsgesetz (NISG 2024) erlassen, das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden sowie für die Möglichkeit, zu diesem Gesetzesentwurf Stellung zu nehmen.
Die Herausforderungen in der weiter voranschreitenden Digitalisierung benötigt klare Rahmenbedingungen und eine gemeinsame Basis organisatorischer, personeller und finanzieller Natur.
Wir begrüßen, dass mit dem vorliegenden Entwurf aktiv die Widerstandsfähigkeit der kritischen Infrastruktur national weiter gestärkt wird. Österreichs E-Wirtschaft bringt sich aktiv und lösungsorientiert sowohl bei der vorliegenden Begutachtung als auch in der laufenden Diskussion mit ein.

Einige Punkte sind im Interesse der Rechtssicherheit oder der praktischen Durchführbarkeit jedenfalls noch zu überarbeiten:

- Klare Trennung der Aufgaben der unabhängigen Stellen bzw. Prüfer von den Aufgaben der Behörde (§ 7)
- Klare Rahmenbedingungen für Computer-Notfallteams (CSIRTs) (§§ 8ff)
- Optimierung des Aufwandes der Überprüfung in Konzernstrukturen (§ 33) und Berücksichtigung bestehender ISO/IEC 27001 Zertifizierung
- Schärfung der Berichtspflicht und Informationsaustausch (§§ 34ff)
- Klare Rahmenbedingungen für Aufsichtsmaßnahmen (§ 38)
- Verbesserungen der Übergangszeit, insbesondere Planungssicherheit (§ 51)

Österreichs E-Wirtschaft

Brahmsplatz 3 Tel +43 1 501 98-0 info@oesterreichsenergie.at
1040 Wien Fax +43 1 501 98-900 www.oesterreichsenergie.at

DVR 0422100, UID ATU37583307, ZVR 064107101; Raiffeisenlandesbank Niederösterreich-Wien AG, SWIFT/BIC: RLNWATWW, IBAN: AT12 3200 0000 1264 4787

Zu den einzelnen Gesetzesbestimmungen des Entwurfs nehmen wir wie folgt Stellung:

Zu § 3 Begriffsbestimmungen:
Wir regen an, zu folgenden Begriffen eine Definition zu ergänzen
„in Echtzeit oder nahezu Echtzeit“ siehe auch diese Stellungnahme zu § 8 Abs. 1 Z 1
„Beteiligung“ siehe auch diese Stellungnahme zu § 8 Abs. 1 Z 6
„vertrauenswürdige Personen“ siehe auch diese Stellungnahme zu § 9 Abs. 1

Folgende Begriffe finden sich nur im Anhang 1. Da auf diese Begriffe im Gesetz nicht Bezug genommen wird schlagen wir alternativ zur Aufnahme unter § 3 eine Ergänzung in den Erläuterungen vor:
„Online-Marktplatz“,
„Online-Suchmaschine“,
„Cloud-Computing“,
„Internet-Knoten“,
„Rechenzentrumsdienste“,
„Content Delivery Network“ und
„Forschungseinrichtung“

Die Begriffsbestimmungen sind insgesamt verständlich. Zwei gute Ansätze sind jedoch nicht konsequent durchgezogen:

1. Abkürzungen / Akronyme werden nur teilweise bei der ersten Verwendung erklärt (Beispiel „Top Level Domain – TLD“`). Wir schlagen vor, dies durchzuziehen, etwa bei „IKT“ oder „DNS“.
2. Manche sperrigen deutschen Formulierungen werden durch ihre bekannteren, englischen Pendants ergänzt, etwa beim Begriff *23. „Anbieter verwalteter Dienste“ (Managed Service Provider)*. oder *29. „Beinahe-Cybersicherheitsvorfall“ (Near Miss)*. Dies wäre bei weiteren Punkten hilfreich, optimalerweise mit der entsprechenden geläufigen Abkürzung, insbesondere:
   9 „Schwachstelle“ (Vulnerability) […]
   24. „Anbieter verwalteter Sicherheitsdienste“ (Managed Security Service Provider – MSSP), […]
   27. „Cyberbedrohung“ (Cyber Threat), […]
   30. „Cybersicherheitsvorfall“ (Cyber Incident), […]

Zu § 7 Unabhängige Stellen und unabhängige Prüfer
Zu Abs. 5
Die vorgeschlagene Bestimmung in § 7 Abs. 5 beschreibt den unabhängigen Prüfer als eine natürliche Person, die „[…] *zur Beurteilung der Umsetzung von Risikomanagementmaßnahmen […] eingesetzt werden kann“*.
Dies geht über die im Erwägungsgrund 125 der NIS2-RL beschriebene Aufgabe der Fachkräfte (Prüfer) hinaus, da laut dieser die *„[…] Inspektionen und die Überwachung … **objektiv** durchgeführt werden“* sollen. Der in § 7 Abs. 5 NISG 2024 genannte unabhängige Prüfer sollte daher einsprechend eine objektive Dokumentation durchführen. **Die Beurteilung der umgesetzten Risikomanagementmaßnahmen jedoch liegt bei der**

Cybersicherheitsbehörde, wie auch schon mehrfach in Diskussionen zu NIS seitens der Behörde bestätigt wurde.

Wir regen daher an, den Text § 7 Abs. 5 wie folgt zu schärfen:
*„Ein unabhängiger Prüfer ist eine natürliche Person, die von einer unabhängigen Stelle zur ~~Beurteilung~~ **objektiven Dokumentation** der Umsetzung von Risikomanagementmaßnahmen wesentlicher und wichtiger Einrichtungen […] eingesetzt werden kann“.*

Zu Abs. 6 Z 2
Entsprechend ist der Text gleichlautend in Abs. 6 Z 2 zu korrigieren auf:
*„2. Gegenüber der Cybersicherheitsbehörde seine Eignung zur ~~Beurteilung~~ **objektiven Dokumentation** der Umsetzung von Risikomanagementmaßnahmen […]“*

Zu § 8 Zweck und Aufgaben der Computer- Notfallteams
Zu Abs. 1
Die Bestimmungen in § 8 Abs. 1 sind dem Art. 11 Abs. 3 der NIS2-RL entnommen und sind bereits dort etwas holprig formuliert. Daher empfehlen wir Formulierungen zu schärfen oder zumindest Begriffe in den Erläuterungen zu definieren.

Zu Z 1
Sowohl die englische als auch die deutsche Version der NIS-2-Richtlinie ist hier nicht ganz eindeutig. Das *„concerned“* des englischen Richtlinientextes ist etwas unglücklich mit *„betreffende“* übersetzt. Im Kontext ist vielmehr jene Einrichtung gemeint, welche von den Bedrohungen, Schwachstellen und Vorfällen betroffen ist. Daher schlagen wir folgende Änderung vor:
„[…] die Unterstützung **betroffener** wesentlicher und wichtiger Einrichtungen […]“

Zu Z 1 und Z 2:
Die Ziffern enden jeweils mit dem Vermerk *„[…] in Echtzeit oder nahezu in Echtzeit;*“. Dies sollte durch *„**unverzüglich:***“ ersetzt werden. Alternativ sollte in § 3 oder in den Erläuterungen eine entsprechende Definition für *„Echtzeit“* aufgenommen werden.

Zu Z 6
Der aktuelle Entwurf enthält *„die Beteiligung am CSIRTs-Netzwerk […]“*, womit keine wirtschaftliche Beteiligung gemeint sein kann. Vielmehr geht es, wie in der englischen Version geschrieben, um die Teilnahme und damit das Mitwirken.

Daher schlagen wir die Formulierung zu ändern auf:
*„die **Teilnahme** am CSIRs-Netzwerk […]“*

Zu Abs. 6
Gemäß § 8 Abs. 6 ist vorgesehen, dass dem nationalen CSIRT *„[…] ein pauschalierter Ersatz für die bei Erfüllung ihrer (sic!) Aufgaben gemäß Abs. 1 entstandenen Aufwendungen“* gebührt.
Im Energiesektor (Elektrizität, Gas und Öl) wurde das Austrian Energy CERT (AEC) als sektorales CSIRT ergänzend im nationalen CSIRT aufgebaut. Im Rahmen von NIS1 wurde

das AEC bereits als sektorales CSIRT ermächtigt. Die Kosten für den Betrieb des AEC wurden und werden weiterhin direkt von den Teilnehmern der ARGE E-CERT getragen.

Laut Abs. 3 ist das nationale CSIRT damit beauftragt, die *„[…] Aufgaben des jeweiligen sektorspezifischen CSIRTs […] wahrzunehmen“*.
Der damit einhergehende Mehraufwand soll in Anlehnung an Abs. 6 mitberücksichtigt werden, insbesondere wenn sektorspezifische CSIRTs in das nationale CSIRT integriert sind. Es ist im Interesse aller den Aufbau und Betrieb von sektoralen CSIRTs zu unterstützen. Gleichzeitig erlangt das nationale CSIRT durch zusätzliches sektorspezifisches Know-how, intensivere Einbindung und verstärkte Wahrnehmung einen erheblichen Qualitätsgewinn zum Nutzen aller.

Wir schlagen daher vor, dass der damit einhergehende Mehraufwand (Abs. 1 und Abs. 3) von den Behörden mitberücksichtigt und aufgenommen wird. **Daher sollte Regelung auf sektorspezifische CSIRTs ausgedehnt werden, da auch diese die gesetzlich vorgesehenen Aufgaben gemäß § 8 Abs. 1 zu erfüllen haben** und damit im Vergleich zum Status Quo ein erheblicher Mehraufwand im nationalen CSIRT erzeugt wird.

Demzufolge schlagen wir inklusiver kleiner grammatikalischer Korrektur vor, den Abs. 6 anzupassen:
*„Dem nationalen CSIRT gebührt vom Bund ein pauschalierter Ersatz für die bei Erfüllung ~~ihrer~~ **seiner** Aufgaben gemäß Abs. 1 **sowie Abs. 3 in diesem Sinne** entstandenen Aufwendungen.“*

Zu § 9 Anforderungen und Eignung von CSIRTs:
Zu Abs. 1
Die CSIRTs müssen über ausreichend geeignetes Personal verfügen. Laut vorliegendem Entwurf darf die Ermächtigung nur *„vertrauenswürdigen Personen“* verliehen werden. Es fehlt eine nähere **Definition** im NISG 2024, was unter dem Begriff *„vertrauenswürdige Person“* zu verstehen ist. Siehe entsprechenden Kommentar in dieser Stellungnahme zu § 3 weiter oben.

Zu Z 1
Die vorgeschlagene Bestimmung in § 9 Abs. 1 Z 1 stellt an die Kommunikationskanäle zu CSIRTs die Anforderung, damit diese *„[…] jederzeit erreichbar bleiben […]“*. Dies würde bedeuten, dass unabhängige Infrastrukturen bestehen, die autark betrieben werden können. Aus unserer Sicht scheint dies nicht realistisch. Wir regen daher an, die Abhängigkeit von funktionierenden Grundinfrastrukturen (Stromversorgung, Telekommunikationsinfrastruktur) zu berücksichtigen und folgende Ergänzung vorzunehmen:
*„1. ihre Kommunikationskanäle weisen einen hohen Grad an Sicherheit, Belastbarkeit und Verfügbarkeit auf, indem punktuellen Ausfällen vorgebeugt und mehrere Kanäle bereitgestellt werden, damit sie**, in Abhängigkeit der funktionierenden Grundinfrastruktur (Stromversorgung, Telekommunikationsinfrastruktur),** jederzeit erreichbar bleiben […]“*

Zu § 10 Aufsicht
Zu Abs. 2
Gemäß der vorgeschlagenen Bestimmung in § 10 Abs. 2 kann der Bundesminister für Inneres gegenüber *„[…] den CSIRTs allgemeine Weisungen oder Weisungen im Einzelfall“* erteilen. Laut § 10 Abs. 1 gilt dieses Weisungsrecht auch gegenüber sektorspezifischen CSIRTs, was in dieser allgemeinen Formulierung sehr kritisch gesehen wird. Um die Unabhängigkeit der CSIRTs weiterhin zu wahren und die Vertrauensstellung sowie den entsprechenden Mehrwert aufrechtzuerhalten, muss das **Weisungsrecht gegenüber sektorspezifischen CSIRTs klarer formuliert und auf die in § 8 Abs. 1 genannten Aufgaben beschränkt werden.**

Daher schlagen wir vor, den Abs. 2 wie folgt zu ergänzen:
„(2) Der Bundesminister für Inneres kann in Ausübung seines Aufsichtsrechts, insbesondere zur Wahrung sicherheitspolitischer Interessen, den CSIRTs allgemeine Weisungen oder Weisungen im Einzelfall erteilen. ***Bei sektorspezifischen CSIRTs ist die Erteilung von Weisungen auf die in § 8 Abs. 1 aufgelisteten Aufgaben eingeschränkt****.“*

Zu § 11 Koordinierte Offenlegung von Schwachstellen
Die Koordinierung der Offenlegung von Schwachstellen durch das nationale CSIRT wird ausdrücklich begrüßt, um Friktionen zwischen Anwendern/Betreibern, Lieferanten/Anbietern und Sicherheitsexperten/-forschern zu vermeiden oder zumindest zu reduzieren.

Die Offenlegung von Schwachstellen wird von uns und anderen Experten als komplex, sehr wichtig, aber gleichzeitig auch als heikles Thema bewertet. Daher sehen wir es als notwendig an, mögliche Missverständnisse entweder in den Erläuterungen oder vermutlich besser **mittels einer Verordnungsermächtigung zu konkretisieren.**

Es müssen die Ziele der Offenlegung explizit genannt und aufgelistet werden. Dazu gehört unter anderem der Schutz des Meldenden und auch allfälliger Betroffener – sowohl Hersteller als auch Anwender. Gleichzeitig soll vermieden werden, dass Infos zu den Schwachstellen ausgenutzt oder – wie es leider schon in Einzelfällen in der EU vorgefallen ist – gewinnbringend weiterverkauft werden.

Außerdem muss das nationale CSIRT über die nötigen personellen und materiellen Ressourcen verfügen, um diese Aufgabe in der nötigen Qualität und in jeweils kurzer Frist wahrnehmen zu können. Ergänzend sei auf die Empfehlung der NIS-Kooperationsgruppe für eine nationale Coordinated Vulerability Disclosure (CVD) Policy hingewiesen.

Die oben angeführten Punkte werden durch den derzeitigen Entwurf nicht ausreichend sichergestellt. Diesbezüglich sehen wir eine Klarstellung für notwendig an. Daher schlagen wir vor, eine Verordnungsermächtigung als § 11 Abs. 5 zu ergänzen:
„(5) Der Bundesminister für Inneres hat in Abstimmung mit dem nationalen CSIRT in einer Verordnung festzulegen, wie sich Sicherheitsforscher beim Fund von Schwachstellen verhalten sollten, wie die Meldung an das CSIRT erfolgen soll und welche Zeitrahmen für die Offenlegung einzuhalten sind.“

Zu § 16 Management von Cybersicherheitsvorfällen großen Ausmaßes
Zu Abs. 1 & 2
Gemäß § 16 Abs. 1 & 2 hat die *„[…] Cybersicherheitsbehörde Aufgaben für das Management von Cybersicherheitsvorfällen großen Ausmaßes wahrzunehmen […]“ sowie zu diesem „Zweck Kapazitäten, Mittel und Verfahren […] zu ermitteln“*.

Diese Passagen sind sehr allgemein gehalten. Zu wünschen wäre, die **Kompetenzen klarer** zu definieren bzw. etwaige Behandlung der wesentlichen bzw. wichtigen Einrichtungen zu erläutern, damit auch die notwendigen **Kapazitäten, Mittel und Verfahren** besser in Relation gesetzt werden können.

Zu § 21 Zusammenarbeit mit der Datenschutzbehörde
Zu Abs. 2
§ 21 Abs. 2 NISG 2024 regelt, dass die Cybersicherheitsbehörde – obwohl nicht datenschutzrechtlich Verantwortlicher gem. Art. 4 Z 7 DSGVO – beim *„[…] Grund zur Annahme, dass ein Verstoß einer wesentlichen und wichtigen Einrichtung gegen die in den §§ 32 und 34 (Anm.: NISG 2024) festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten zur Folge hat“*, eine Meldung an die Datenschutzbehörde gem. Art 33 DSGVO durchzuführen hat.

Einerseits wäre es wünschenswert, dass mit der NIS-Meldung auch die Meldeverpflichtung an die Datenschutzbehörde abgedeckt werden kann. Unklar ist jedoch, mit welchen Mitteln bzw. Methoden die Cybersicherheitsbehörde einschätzen können, ob die Meldepflicht gegeben ist, die ja nur dann besteht, wenn diese gem. Art. 33 Abs. 1 DSGVO voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. **Jedenfalls sind die entsprechenden Datenschutzbeauftragten unverzüglich zu informieren.**

Sinngemäß ist Abs. 2 zu ergänzen:
„(2) […] hat die Cybersicherheitsbehörde unverzüglich, möglichst innerhalb von 72 Stunden, die Datenschutzbehörde zu unterrichten. ***Jedenfalls sind die Datenschutzbeauftragten der betroffenen wichtigen oder wesentlichen Einrichtung unverzüglich über die Meldung an die Datenschutzbehörde zu informieren.*** *[…]“*

Zu § 24 Wesentliche und wichtige Einrichtungen
Zu Abs. 2
In Umsetzung der NIS-2-Richtlinie wird zwischen wesentlichen und wichtigen Einrichtungen unterschieden. Diese Unterscheidung ist im § 24 des vorliegenden Entwurfes aus unserer Sicht nicht eindeutig gewährleistet, da sowohl Abs. 1 (wesentliche Einrichtungen) als auch Abs. 2 (wichtige Einrichtungen) die **Zuordnung** eines **großen** Unternehmens der **Anlage 1** einfordert (beim Vergleich von Abs. 1 Z 3 mit Abs. 2 Z 1).

Daher schlagen wir vor, den § 24 Abs. 2 Z 1 entsprechend der NIS-2-RL Art. 3 Abs. 2 wie folgt zu ergänzen:

*„1. Einrichtungen der in den Anlagen 1 und 2 dieses Gesetzes genannten Art, die ein großes oder mittleres Unternehmen betreiben**, die nicht als wesentliche Einrichtungen im Sinne von Abs. 1 Z 3 gelten,** sowie“*

Zu § 25 Ermittlung der Unternehmensgröße
Zu Abs. 1
Die vorgeschlagene Bestimmung in § 25 Abs. 1 legt fest, dass sich die Einstufung als mittleres oder großes Unternehmen aus der (logischen) UND-Verknüpfung der Anzahl der Mitarbeiter, dem Jahresumsatz und der Jahresbilanzsumme orientiert. Die Absätze 2 und 3 zur Beurteilung eines großen oder mittleren Unternehmens sind durch die ODER-UND-Verknüpfung dieser Kriterien nicht eindeutig. Dies erscheint uns inkonsistent mit der in Abs. 1 festgelegten Einstufung. Wir ersuchen daher um eindeutige **Klarstellung**.

Hinsichtlich der Ermittlung der Unternehmensgröße sieht der Entwurf vor, dass bei der Berechnung der Werte nicht bloß jene des eigenen Unternehmens, sondern auch jene der mit dem Unternehmen verbundenen Unternehmen und (anteilig) jene der Partnerunternehmen hinzugerechnet werden. Hierbei hält sich der Entwurf strikt an die zugrundeliegende Empfehlung der Kommission vom 06.05.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (2003/361/EG) aus wirtschaftlicher Sicht, worauf auch die NIS-2-Richtlinie verweist.

Aus unserer Sicht führt dies zu einem **unverhältnismäßig hohen Aufwand für** verbundene Unternehmen. Es werden durch diese Vorgehensweise insbesondere **kleinere, eigenständige Unternehmen in Konzernstrukturen** den Verpflichtungen des NISG 2024 unterworfen, die allein für sich die Schwellenwerte nicht überschreiten würden. Diese Vorgehensweise mag bei Unternehmen nachvollziehbar sein, die systemtechnisch mit dem NISG 2024 unterworfenen verbundenen Unternehmen und Partnerunternehmen verbunden sind, jedoch nicht bei systemtechnisch eigenständigen Unternehmen, welche die Schwellen nicht erreichen würden.

Daher schlagen wir vor, die Referenz auf die Empfehlung der Europäischen Kommission 2003/361/EG **auf Artikel 1 und 2** in Anhang 1 im § 25 Abs. 1 wie folgt zu **beschränken**:
*„[…] Diese Einstufung erfolgt unter Anwendung der Art. 1 **und 2** des Anhangs der Empfehlung der Kommission vom 06.05.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, ABl. Nr. L 124 vom 20.5.2003 S. 36~~, mit Ausnahme des Art. 3 Abs. 4 des Anhangs dieser Empfehlung~~.“*

Zu § 26 Größenunabhängige Einstufung als wesentliche oder wichtige Einrichtung
Zu Abs. 3 Z 2
Es ist entweder unter § 3 oder alternativ in den Erläuterungen eine Definition erforderlich, ab wann eine Störung eine wesentliche Auswirkung auf die öffentliche Ordnung hat, da damit die weiteren Verpflichtungen für Unternehmen bei der NIS-Behörde abhängen.

Zu § 29 Register der Einrichtungen
Zu Abs. 2
Wir empfehlen klarzustellen, dass eine einmalige Registrierung des Konzernes für alle betroffenen Unternehmen eines Konzernverbunds ausreichend ist. Dies erhöht einerseits die Rechts- und Planungssicherheit für Unternehmen als auch die Ressourceneffizienz des Gesamtsystems.

Überdies ist zu erwarten, dass viele Einrichtungen in mehr als einem einzelnen Sektor / Teilsektor aktiv sind und damit auch mehrfache „Art(en) der Einrichtung" zutreffen werden. Dieser Punkt muss daher unbedingt Mehrfachnennungen erlauben.

Wir schlagen daher vor § 29 Abs. 2 Z 3 wie folgt anzupassen
*„3. den**/die** Sektor**(en)**, Teilsektor**(en)** und die Art**(en)** der Einrichtung gemäß Anlage 1 oder 2;"*

Zu § 31 Governance
Zu Abs. 3
Die Maßnahmen zur Bewusstseinsbildung bei den Leitungsorganen werden begrüßt. Derzeit lässt das Gesetz sowohl den Umfang als auch die Mindestvorgaben an den Inhalt, den Umsetzungszeitraum als auch allfällige erneute Durchführung offen.
Es gab im Rahmen der Cyber Security Plattform bereits einen Workshop zu dem Thema. Eventuell lassen sich daraus Eckpunkte für die Vorgaben ableiten.

Zu § 33 Nachweis der Wirksamkeit von Risikomanagementmaßnahmen
Zu Abs. 2 in Verbindung mit Abs. 6
Nach § 33 Abs. 2 des Entwurfes haben wesentliche Einrichtungen innerhalb von drei Jahren nach Aufforderung zur Selbstdeklaration die Umsetzung der Risikomanagementmaßnahmen gegenüber der Cybersicherheitsbehörde mittels Prüfung durch eine unabhängige Stelle in Form eines zu übermittelnden Prüfberichtes je betroffene wesentliche Einrichtung nachzuweisen.

Insbesondere bei **Konzernstrukturen** – wenn dort mehrere wesentliche Einrichtungen existieren – und im Hinblick auf die konzernverbundenen Dienstleistungsunternehmen (z.B. konzerninterne IKT) wäre es wünschenswert, wenn hier die **Prüfungen effizienter gestaltet** werden können.
Es soll 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. Für eine effizientere Abwicklung und Organisation muss hier z.B. eine **Anpassung der Prüfzyklen** ermöglicht werden. Ansonsten würden im Vergleich zu anderen wesentlichen Einrichtungen, die nur in einem Sektor tätig sind, erheblich Mehrkosten entstehen. Den Kosten soll also 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.

Andererseits sollte die Durchführung als **konzentriertes Verfahren** verankert werden. Es ist festzulegen, dass es ausreicht, miteinbezogene Dienstleistungsunternehmen, die für die wesentlichen Einrichtungen gleichartige Dienstleistungen (z.B. IT) erbringen, in **einer Prüfung** (Audit) zu überprüfen, um **Ressourcen zu schonen und den Aufwand zu minimieren**. Es soll sichergestellt werden, dass alle wesentlichen Einrichtungen eines Konzerns den Nachweis der Wirksamkeit der Risikomanagementmaßnahmen im Rahmen einer **gemeinsamen Prüfung** erbringen können. Dies kann entweder direkt im NISG 2024 oder in der Verordnung gemäß Ermächtigung im § 33 Abs. 6 erfolgen.

Bei Prüfungen gemäß NISG haben unabhängige Stelle ein **gültiges Zertifikat nach ISO/IEC 27001 der überprüfenden Einrichtung** im Rahmen mitzuberücksichtigen. Das **Managementsystem gemäß ISO/IEC 27001** – und anderen spezifischen Normen der ISO/IEC 27000er Familie – geben sowohl durch **jährliche externe als auch interne Audits** eine engmaschigere Überprüfung und Überwachung als das NISG vor. Darüber hinaus haben Auditoren*innen und Zertifizierungsstellen nach ISO/IEC 27001 die Pflicht, ihre Kunden zu überwachen. Eine mögliche Pflicht zur Einschau oder Überprüfung, beispielsweise ein außerordentliches Audit nach einem Sicherheitsvorfall, muss durch die Auditoren*innen oder Zertifizierungsstellen für die Einrichtungen gewährleistet werden. Zudem werden Zertifizierungsstellen in einem festgelegten periodischen Zeitraum auch von Akkreditierungsstellen auditiert. Der **Nachweis eines Zertifikats nach ISO/IEC 27001** und stichprobenartige Prüfungen durch die Behörde oder unabhängige Stellen sollten **ausreichend sein, organisatorische Maßnahmen als effektiv anzuerkennen**, solange keine schwerwiegenden 'non-conformities' zum Zeitpunkt der NISG-Prüfung vorliegen und der Anwendungsbereich dem Risko angemessen definiert und angewendet wurde.

Wenn eine unabhängige Stelle gleichzeitig als Zertifizierungsstelle fungiert und die ISO/IEC 27001 Auditoren gleichzeitig auch NISG-Prüfer sind, sollten sogenannte **Kombiaudits bzw. -prüfungen** forciert werden. Durch die Einführung und den Betrieb eines ISO/IEC 27001-zertifizierten Informationssicherheitsmanagementsystems betont das oberste Leitungsorgan ihre Sorgfaltspflicht.

Zu Abs. 5
Gemäß § 33 Abs. 5 soll die Übermittlung eines Prüfplans spätestens ein Monat vor Beginn der Durchführung von Prüfungen erfolgen. Eine zusätzliche Ankündigung von geplanten Prüfungen durch die wesentlichen und wichtigen Einrichtungen an die Cybersicherheitsbehörde wird als **übermäßiger bürokratischer Aufwand** betrachtet, der im Rahmen der verteilten Prüfung auch keinen zusätzlichen Informationsgehalt liefert. Dies erschwert die sinnvolle Planung eines kombinierten Audits, etwa gemeinsam mit ISO 27001. Die Pflicht zur **Vorab-Übermittlung soll unterbleiben** – wir sehen darin **keinen Mehrwert**. Die zeitgerechte Durchführung von Prüfungen ist durch die Nachweisfristen sicherzustellen, jedoch nicht durch die vorhergehenden Ankündigungen.

Daher schlagen wir vor, **diese Bestimmung Abs. 5 gänzlich zu streichen.**

Zu § 34 Berichtspflichten
In einem Konzern können mehrere wesentliche oder wichtige Einrichtungen vorhanden sein, die sich zentraler interner und externer Dienstleister bedienen. Im Kontext der Lieferkette kann es erforderlich sein, dass viele Einrichtungen an das CSIRT berichten müssen. Dies erhöht den Aufwand für das zentrale Sicherheitspersonal, die Rechtsabteilung und viele Leitungsorgane, insbesondere im Krisenmanagement. Letzteres sollte sich mehr mit dem eigentlichen Vorfall auseinandersetzen, als sich mit einem Portal zur Meldung von Sicherheitsvorfällen beschäftigen zu müssen. Sofern rechtlich zulässig und weil Einrichtungen im Konzern weisungsfrei sein müssen, sollte die österreichische Gesetzgebung eine Erleichterung für Unternehmen in Erwägung ziehen.
Darüber hinaus ist zu bedenken, dass Meldesysteme (Webseiten, Telefonie, E-Mail usw.) im Falle eines Vorfalls möglicherweise nicht uneingeschränkt erreichbar sind, daher kann eine derart geforderte Meldung innerhalb des definierten Zeitraums unrealistisch sein.

Zu Abs. 2 Z 1
Nach Art. 23 Abs. 4 lit. a) der NIS-2-Richtlinie müssen die Mitgliedsstaaten sicherstellen, dass die betreffenden Einrichtungen dem CSIRT oder gegebenenfalls der zuständigen Behörde „unverzüglich eine Frühwarnung übermitteln, *„in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige und* ***böswillige*** *Handlungen zurückzuführen ist“*.
Im §34 Abs. 2 Z 1 des vorliegenden Entwurfs wird hier auf *„rechtswidrige und schuldhafte Handlungen“* abgestellt. Aus unserer Sicht geht das deutlich über den Originaltext der NIS-2-Richtlinie hinaus. Außerdem kann gerade in der Anfangszeit eines Vorfalles noch gar nicht abgeschätzt werden, ob ein Verschulden an dem Vorfall vorliegt. Lediglich bei rechtswidrigen und böswilligen, also vorsätzlichen Handlungen (z.B. DDoS-Attacken) kann eine frühzeitige Einschätzung getroffen werden.

Unser Vorschlag ist daher, den NIS-2-RL-Originaltext ***„böswillige“*** oder ***„vorsätzliche“*** zu übernehmen und daher § 34 Abs. 2 Z 1 zu ändern auf:
„[…] dass der Cybersicherheitsvorfall auf rechtswidrige und ~~schuldhafte~~ ***vorsätzliche*** *Handlungen zurückzuführen ist […]“*

Zu Abs. 3
Die in § 34 Abs. 3 vorgeschlagene Bestimmung verlangt bei einem erheblichen Cybersicherheitsvorfall die unverzügliche Unterrichtung der Empfänger des Dienstes bei Einschränkung desselben. Im Sektor Energie, Teilsektor Elektrizität scheint dies nicht sinnvoll oder überhaupt im Anlassfall technisch nicht realistisch. Von dieser Anforderung sollte daher der Sektor Energie, Teilsektor Elektrizität ausgenommen werden bzw. zumindest eingeschränkt werden auf:

Daher schlagen wir folgende Ergänzung vorzunehmen
*„[…] unterrichtet****, soweit möglich,*** *die Einrichtung die Empfänger ihrer Dienste unverzüglich über diesen erheblichen Cybersicherheitsvorfall […]“*
Zu Abs. 4
Das CSIRT übermittelt laut Abs. 4 der meldenden Einrichtung “unverzüglich und nach Möglichkeit” innerhalb von 24 Stunden eine Antwort. Die Erklärung in den Erläuterungen

übersetzen das *„und“* mit *„d.h. spätestens“*. Das „und“ könnte aber auch als „sowie“ verstanden werden, wodurch zwei Antworten zu liefern wären. Eine **Klarstellung der UND-Verknüpfung und der Bedeutung** von *„nach Möglichkeit“* ist hier wünschenswert.

Zu Abs. 6
Art. 23 Abs. 7 der NIS-2-Richtlinie spricht generell über das Informieren der Öffentlichkeit über einen erheblichen Sicherheitsvorfall unter bestimmten Voraussetzungen. Auch die Aufforderung der CSIRT bzw. der Behörde an die betroffene Einrichtung, die Öffentlichkeit von sich aus zu informieren, ist hier vorgesehen.

Gemäß § 34 Abs. 6 des vorliegenden Entwurfes (als direkte Umsetzungsbestimmung des Art. 23 Abs. 7 der NIS-2-Richtlinie) kann die Cybersicherheitsbehörde die Öffentlichkeit über Cybersicherheitsvorfälle unterrichten. Die Definition eines Cybersicherheitsvorfalles gemäß § 3 Z 30 des Entwurfes deckt sich mit der Definition des Sicherheitsvorfalles gemäß Art. 6 Z 6 der NIS-2-Richtlinie. Dementsprechend geht die innerstaatliche Umsetzung weiter als die NIS-2-Richtlinie, da die Öffentlichkeit im Entwurf auch über „nicht erhebliche“ Sicherheitsvorfälle informiert werden kann. Aus unserer Sicht sollte daher in § 34 Abs. 6 auf den Begriff des **erheblichen Cybersicherheitsvorfalles** gemäß § 35 Abs. 1 des Entwurfes zum NISG 2024 abgestellt werden.

Zudem verweist § 34 Abs. 6 in diesem Zusammenhang auf personenbezogene Daten gemäß §§ 42 und 43 des Entwurfes und deren Veröffentlichung im Anlassfall. Bei den unter § 42 Abs. 2 des vorliegenden Entwurfes aufgelisteten personenbezogenen Daten handelt es sich um Kontakt- und Identitätsdaten natürlicher und juristischer Personen. Die genauen Datenarten sind hier auch umfangreich aufgelistet. Die Veröffentlichung der Daten erfolgt zwar nur, wenn dies erforderlich ist und in den dazugehörigen Erläuterungen ist auch angeführt, dass die datenschutzrechtlichen Grundsätze der **Verhältnismäßigkeit und Datenminimierung eingehalten werden müssen**. Trotzdem ist diese innerstaatliche Umsetzung aus unserer Sicht überschießend, da es grundsätzlich nicht erforderlich sein wird, etwa Log-Files und IP-Adressen im Zusammenhang mit einem Sicherheitsvorfall zu veröffentlichen.

Aus unserer Sicht sollte es ausreichend sein, die Öffentlichkeit, so dies als wirklich erforderlich eingestuft wird, nur allgemein über den Sicherheitsvorfall zu informieren und nicht-personenbezogene Daten, wie Firmenname, Firmenadresse, Firmenkontaktdaten ohne Personenbezug zu veröffentlichen.

Alternativ könnte auch eine Bestimmung mitaufgenommen werde, in welcher definiert ist, dass an Unternehmen ähnlicher Branchen, die von einem (erheblichen) Cybersicherheitsvorfall betroffen sein könnten bzw. zur Verhütung von Cybersicherheitsvorfällen, die Behörde weitergehende personenbezogene Daten an diesen engen Kreis in Abstimmung mit dem betroffenen Unternehmen übermitteln darf, verbunden mit einer Pflicht der empfangenden Unternehmen zur Geheimhaltung.

Wir schlagen jedenfalls vor, dass Wording der NIS-2-Richtlinie zu übernehmen und einerseits die Öffentlichkeit nur **allgemein** über einen erheblichen Cybersicherheitsvorfall **zu**

informieren bzw. die hierfür zu veröffentlichenden **Daten auf nicht-personenbezogene bzw. anonymisierte** weiter **einzuschränken**. Jedenfalls auf jene Daten, die es betroffenen Personen ermöglicht, mit der betroffenen Einrichtung Kontakt aufzunehmen.

Es wird daher folgende Änderung vorgeschlagen:
*„(6) Nach Anhörung der von einem **erheblichen** Cybersicherheitsvorfall betroffenen Einrichtungen kann die Cybersicherheitsbehörde **nicht-**personenbezogene Daten **und anonymisierte Informationen** gemäß §§ 42 und 43 nach erfolgter Interessenabwägung bezüglich der Auswirkungen auf die Betroffenen veröffentlichen, um die Öffentlichkeit über **erheblichen** Cybersicherheitsvorfälle zu unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung oder zur Bewältigung von **erheblichen** Cybersicherheitsvorfällen erforderlich ist, oder die Offenlegung des **erheblichen** Cybersicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.“*

Zu § 34 Ergänzung
Bei der freiwilligen Meldung § 37 Abs. 3 gilt, dass sie *„[…] personenbezogene Daten gemäß § 42 Abs. 2 enthalten“* kann. Eine äquivalente Freigabe für die Pflichtmeldung fehlt im § 34 und **sollte ergänzt werden.**

Zu § 35 Erheblicher Cybersicherheitsvorfall:
Zu Abs. 2
Die Bestimmungen in § 35 Abs. 2 Z 1 bis 4 sollen Kriterien zur Beurteilung eines als erheblich einzustufenden Cybersicherheitsvorfalles festlegen. Es ist derzeit schwer konkret abschätzbar, was als erheblicher Cybersicherheitsvorfall anzusehen ist. Eine entsprechende **praxisrelevante Klarstellung in der Verordnung** gemäß Abs. 3 ist anzustreben.

Beispielsweise soll gemäß § 35 Abs. 2 Z 4 als Kriterium zur Beurteilung eines Cybersicherheitsvorfalls das *„geografische Gebiet“*, das von einem Cybersicherheitsvorfall betroffen sein könnte, hinzugezogen werden. Dazu sollen Schwachstellen, die mit dem Grad der Isolierung bestimmter geografischer Gebiete, wie „*insbesondere Berggebiete“* berücksichtigt werden. Wir bitten die Formulierung wie „*insbesondere Berggebiete*“ anhand von Kriterien zu **konkretisieren**.

Zu § 36 Vereinbarungen über den Austausch von Informationen zur Cybersicherheit
Zu Abs. 3
Die in § 36 vorgeschlagene Bestimmung, die Vereinbarungen über den Austausch von Informationen zur Cybersicherheit regelt, ist sehr zu begrüßen. Wir möchten jedoch anregen, dass, angelehnt an die CSIRTs im Sinne von § 8 des vorliegenden Entwurfs, Möglichkeiten für sektorspezifische Vereinbarungen geschaffen werden. Als Motivation für eine engere Kooperation der Einrichtungen sollte die dadurch gegebene Datenschutzfreigabe klarer beschrieben werden, etwa durch einen Verweis auf §42 Abs. 2.

Wir schlagen daher folgende Ergänzung zu Abs. 3 vor:
*„(3) Die Cybersicherheitsbehörde unterstützt die Einrichtungen bei der Ausarbeitung von Vereinbarungen gemäß Abs. 2, insbesondere hinsichtlich der Anwendung der in § 15 Abs. 4 Z 8 genannten Konzepte. **Wenn die verwendeten IKT-Plattformen von einem CSIRT***

betrieben wird, so können auch die in §42 Abs. 2 genannten Daten, wenn das zur Erreichung der in Abs. 1 genannten Ziele nötig ist, übermittelt werden.“

Zu § 38 Aufsichtsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen
Zu Abs. 1
Zu Z 1
Die in § 38 Abs. 1 Z 1 beschriebene Einschau mittels *"Fernzugriff"* geht über die in der NIS-2-RL definierten Aufsichtsmaßnahmen hinaus und kann für Netz- und Informationssysteme von wesentlichen Einrichtungen nur nach schriftlich Anforderung sowie Freigabe und nur ausschließlich unter Mitwirkung der Einrichtung gewährt werden.

Folgende Ergänzung schlagen wir daher vor:
„1. die Durchführung von Kontrollen der Umsetzung der Risikomanagementmaßnahmen gemäß § 32 durch Einschau, insbesondere in die diesbezüglichen Netz- und Informationssysteme und Unterlagen vor Ort, mittels Fernzugriff, ***jedenfalls unter Mitwirkung der Einrichtung und nur nach schriftlicher Freigabe,*** *oder durch Begleitung der Prüfungen von unabhängigen Stellen, jeweils nach vorangegangener Verständigung der betreffenden Einrichtung;“*
Zu Z 2
In § 38 Abs. 1 Z 2 ist die Zusammenarbeit mit der betreffenden Einrichtung verpflichtend notwendig. Außerdem ist zu beachten, dass in Verbindung mit den Strafbestimmungen § 45 Abs. 1 Z 15 die Behörde ein Unternehmen zwingen könnte, beliebige auch intrusive Scans in sensiblen Bereichen vorzunehmen. Dies ist auszuschließen oder alternativ zumindest so weit einzuschränken, dass jegliche unerwünschte Konsequenzen für den Dienst der wesentlichen Einrichtung oder andere negativen Auswirkungen auf die Infrastruktur vermieden werden können.

Daher schlagen wir die Streichung des Wortes „erforderlichenfalls“ und Ergänzung um eine Abstimmung mit der betroffenen Einrichtung vor:
„2. die Durchführung von Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, ~~erforderlichenfalls~~ in ***Abstimmung und*** *Zusammenarbeit mit der betreffenden Einrichtung;“*

Zu Z 4
In § 38 Abs. 1 Z 4 wird erwähnt, dass der Cybersicherheitsbehörde auf Anforderung ein Zugang zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind, bereitzustellen ist. Diese Anforderung soll mittels **Bescheides** kommuniziert werden. Für das Einrichten derartiger Zugänge würden weiterhin aktuelle Anforderungen der Einrichtung einzuhalten sein (entsprechende Abwägung, ausreichende Begründung, Verwendung von durch Einrichtung verwalteten Clients etc.).

Diese Änderung bzw. alternativ die Einschau vor Ort ist zu ergänzen:
„4. die Anforderung des Zugangs ***mittels Bescheides oder alternativ Einschau vor Ort*** *zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind;“*

Zu Z 5
In § 38 Abs. 1 Z 5 wird die Möglichkeit einer Ad-hoc-Prüfung ohne Vorankündigung angeführt. Diese Prüfungen sollten ebenfalls mittels **Bescheides** kommuniziert werden. Es wäre zudem ratsam entsprechende Kriterien und Fristen festzulegen.

Daher schlagen wir folgende Ergänzung vor:
*„5. die Ad-hoc-Prüfung einer wesentlichen Einrichtung **mittels Bescheides**, einschließlich solcher, die aufgrund eines erheblichen Cybersicherheitsvorfalls oder Verstoßes gegen dieses Bundesgesetz durch diese Einrichtung gerechtfertigt ist oder der Überprüfung einer übermittelten Selbstdeklaration gemäß § 33 Abs. 1 dienen."*

Zu § 40 Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung
Die Bedingungen zur verpflichteten Verwendung bestimmter IKT-Produkte, -Dienste oder -Prozesse kann insbesondere in Nischenbereichen oder im operativen Umfeld wesentlicher Einrichtungen zu deutlichen Einschränkungen mit weitreichenden Folgen führen. Unter anderem besteht die Gefahr den Markt zu stark einzuschränken bis hin zur Monopolisierung mit negativen wirtschaftlichen, operativen und sicherheitstechnischen Folgen sowie Konsequenzen im Bereich Innovation und Forschung. Daher sollte zumindest ausreichende Anzahl zur Auswahl gestellt werden. Eine solche Verpflichtung kann nur mittels Bescheids angeordnet werden. Alternativ könnte statt der Verpflichtung eine Empfehlung ausgesprochen werden.

Folgende Ergänzung schlagen wir daher vor:
*„Die Cybersicherheitsbehörde kann **mittels Bescheid** wesentliche und wichtige Einrichtungen dazu verpflichten, **für** spezielle **Zwecke** IKT-Produkte, -Dienste und -Prozesse **aus einer geeigneten Auswahl** zu verwenden, die von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft werden und die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß Art. 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind, um die Erfüllung bestimmter in § 32 genannter Anforderungen nachzuweisen."*

Zu § 44 Allgemeine Bedingungen für die Verhängung von Geldstrafen
Im Rahmen des NISG 2024 orientiert sich der Strafrahmen an dem der Datenschutzgrundverordnung (DSGVO). Die Verhängung von Sanktionen obliegt den Bezirksverwaltungsbehörden, die üblicherweise moderate Beträge als Verwaltungsstrafen festsetzt. Es ist daher zu hinterfragen, ob der Strafrahmen der Kompetenz der Bezirksverwaltungsbehörden entspricht.

Zu § 51 Inkrafttretens-, Außerkrafttretens- und Übergangsbestimmungent

Zu Abs. 6
Im Interesse von Betreiber wesentlicher Dienste nach dem aktuell gültigen NISG, die auch als wesentliche Einrichtungen nach dem vorliegenden Entwurf des NISG 2024 gelten, deren Überprüfungsfälligkeit (bei Beibehaltung des § 51 Abs 7 in der aktuell vorgeschlagenen Fassung innerhalb eines Jahres) ab In-Kraft-Treten des NISG 2024 eintritt, sollten qualifizierte Stellen gemäß § 18 Abs. 1 des derzeit geltenden NISG ohne die derzeit

vorgesehene Antragstellung berechtigt werden, Prüfungen innerhalb des oben genannten Zeitraumes durchzuführen. Dies ist im Interesse der **Planungssicherheit** und zur **frühzeitigen Beauftragung** eines Prüfungsdienstleisters geboten. Es wird daher vorgeschlagen, die Rechtsfolgen ex lege ohne Antrag der qualifizierten Stelle eintreten zu lassen und diesen Stellen ggf. ein Opt-Out aus der ex lege eingetretenen Eigenschaft einer *„unabhängigen Stelle“* nach NISG 2024 zu ermöglichen. Durch diese Änderung tritt zudem eine Reduktion des Verwaltungsaufwandes zur Entlastung der betroffenen Behörde und qualifizierten/unabhängigen Stellen ein.

Zu § 51 Abs. 7
Für Betreiber wesentlicher Dienste nach dem aktuell gültigen NISG, die auch als wesentliche Einrichtungen nach dem vorliegenden Entwurf des NISG 2024 gelten, beginnt die dreijährige Frist für den erstmaligen Nachweis der Anforderungen des § 32 nicht ab der Aufforderung zur Selbstdeklaration durch die Cybersicherheitsbehörde, sondern ab dem Zeitpunkt des letzten Nachweises gemäß § 17 Abs. 3 des derzeit geltenden NISG. Nach den Erläuterungen zu dieser Bestimmung soll dieses Vorgehen den betroffenen Einrichtungen erlauben, die bereits etablierten Prüfprozesse weiterzuführen und sollen die wirtschaftlichen Auswirkungen reduziert werden. Diese Bestimmung soll daher den Betreiber wesentlicher Dienste, die auch als wesentliche Einrichtungen nach dem NISG 2024 eingestuft werden, aus den genannten Gründen entgegenkommen.

Aufgrund der erhöhten Anforderungen des NISG 2024 und der Erweiterung des Anwendungsbereiches auf die gesamte Einrichtung gegenüber dem derzeitigen NISG bedarf es jedoch umfassender Umsetzungsmaßnahmen, selbst bei jenen wesentlichen Einrichtungen, die schon derzeit als Betreiber wesentlicher Dienste eingestuft werden.
Es sind Fälle bekannt, in welchen diese Scope-Erweiterung eine Verzehnfachung der hierfür zu betrachteten Assets (Prozesse, Systeme, Personal) bedeutet.
Je nach dem Zeitpunkt des letzten Nachweises gemäß derzeit geltendem NISG könnte daher die Frist für den Nachweis nach dem NISG 2024 in diesen Fällen stark verkürzt sein.
Die **Umsetzungsfrist** wird durch diesen Absatz aber auf weniger als ein Drittel der üblichen Zeit verkürzt wird, wodurch der Umsetzungsaufwand für betroffene Unternehmen überproportional höher ist, als dies in der in § 33 festgelegten Frist der Fall wäre.
Diese Tatsache stellt eine **grobe Benachteiligung** der betroffenen Unternehmen dar, im Vergleich zu jenen Unternehmen, welche neu in den Anwendungsbereich von NISG 2024 fallen werden, was gegen den Grundsatz der Gleichbehandlung verstößt.

Aus unserer Sicht sollte daher auch für Betreiber wesentlicher Dienste, gemäß § 16 Abs. 1 NISG in der Fassung BGBl. I Nr. 111/2018, die **dreijährige Frist nach** Aufforderung zur **Selbstdeklaration** Anwendung finden, auch, um gegenüber anderen wesentlichen Einrichtungen **nicht schlechter gestellt zu sein**.

Alternativ sollte für Betreiber wesentlicher Dienste, die auch als wesentliche Einrichtungen gemäß § 24 Abs. 1 detaillierte Übergangsbestimmungen und die **Möglichkeit zu einer einmaligen Fristverlängerung** geschaffen werden. Die Rechts- und Planungssicherheit wird dadurch deutlich verbessert. Damit eine Prüfung für den gesamten Scope und den dazugehörigen Nachweis nach § 33 möglich wird, sollte es eine **explizite**

Übergangsbestimmung für Scope-Erweiterungen innerhalb von Einrichtungen geben, die bereits bisher als Betreiber wesentlicher Dienste identifiziert wurden.

Wir weisen darauf hin, dass **die im aktuellen Entwurf vorgeschlagene Vorgehensweise einen erhöhten Aufwand** für wesentliche Einrichtungen mit sich bringen kann, insbesondere, wenn in einem Konzern divergierende Prüfungsschemata für Sicherheitsverantwortliche bestehen. In Konzernen, in denen mindestens zwei Betreiber wesentlicher Dienste gemäß § 17 Abs. 3 NISG die Prüfungen durch qualifizierte Stellen bereits absolviert haben, könnten viele neue Sektoren im Konzern zur Selbstdeklaration aufgefordert werden. Dies könnte die Zeitpläne für Prüfungen und Selbstdeklarationen der einzelnen Einrichtungen im Konzern verschieben. Zudem könnten zentrale Dienstleister, Hersteller und Dritte, insbesondere im Kontext der Lieferkette oder ausgelagerter Prozesse, zahlreiche Prüfungen innerhalb einer Periode oder in sehr kurzen Abständen durchführen müssen, was auch Einrichtungen betrifft, die in mehreren Mitgliedstaaten situiert sind.

Ebenfalls kann dieser Passus zu einem großen Problem für die Einrichtungen führen, wenn es zu **Verzögerungen** kommt und das Gesetz nicht wie angestrebt mit 18. Oktober 2024 in Kraft treten wird. Sollte die zugehörige Verordnung auf sich warten lassen, fehlt den Einrichtungen die konkreten Vorgaben und damit der ausreichende Vorbereitungszeitraum. Ein Hauptproblem sehen wir darin, dass wenn eine Veröffentlichung oder Anpassung der Risikomanagementmaßnahmen kurz vor einer Nachweispflicht oder Aufsichtspflicht im Sinne von §§ 33 und 38 des vorliegenden Entwurfes stattfinden wird, dass hier kein Nachweis im Risikomanagement und derzeitige Akzeptanz durch die Leitungsorgane als ausreichend anerkannt wird.

Zu Anlage 3 Risikomanagementmaßnahmen
Die österreichische Gesetzgebung sollte darauf abzielen, Wettbewerbsverzerrungen für österreichische Unternehmen auf europäischer Ebene zu verhindern. Daher sollte auf eine **EU-weit harmonisierte Umsetzung der Ausarbeitungen von der europäischen NIS-Kooperationsgruppe** abgezielt werden.
Uns ist bewusst, dass eine präzisere Spezifizierung der Risikomanagementmaßnahmen eine harmonisierte Umsetzung in den Einrichtungen ermöglichen würde und die Perspektiven der Einrichtung, unabhängigen Stellen, der Cybersicherheitsbehörde und der Verwaltungsstrafbehörden klarer darstellen würde. Dies würde ebenfalls ein kontinuierlich verbessertes und betriebenes Informationssicherheitsmanagementsystem nach internationalen Normen zulassen.
Wir weisen darauf hin, dass ein **zentraler Ansatz eines Risikomanagementsystems**, wie er bereits durch das GmbH-Gesetz vorgeschrieben ist zu begrüßen ist. Dieser zentrale Ansatz ermöglicht es, die Risikomanagementmaßnahmen den Stakeholdern transparent, nachweisbar und mit den gleichen Ergebnissen wiederausführbar darzustellen.

Zu Artikel 3 Änderung Gesundheitstelematikgesetz 2012
Im Zusammenhang mit der Änderung des Gesundheitstelematikgesetzes weisen wir darauf hin, dass die Gesundheitstelematikverordnung in Anlage 2 auf einen Verschlüsselungsalgorithmus (TDEA) verweist, der nicht mehr dem Stand der Technik entspricht. (Siehe: https://csrc.nist.gov/pubs/sp/800/67/r2/final)

Wir danken für die Kenntnisnahme der Anliegen von Österreichs E-Wirtschaft und ersuchen um deren Berücksichtigung.

Mit freundlichen Grüßen

Mag. Dr. Michael Strugl
Präsident

Dr. Barbara Schmidt
Generalsekretärin

Über Oesterreichs Energie
Oesterreichs Energie ist die Interessenvertretung der österreichischen E-Wirtschaft. Im Auftrag seiner rund 140 Mitgliedsunternehmen vertritt der Verband im Sinne einer sicheren, sauberen und leistbaren Energiezukunft die Brancheninteressen gegenüber Politik, Verwaltung und Öffentlichkeit. Als erste Anlaufstelle zum Thema Energie arbeitet Oesterreichs Energie eng mit politischen Institutionen, Behörden sowie anderen Verbänden zusammen und bringt seine Expertise lösungsorientiert und kundenzentriert in laufende Debatten ein.