**Rückmeldung
zur Konsultation des Bundeskanzleramts zum**

Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024

Wien, 29. April 2024

Über den Verband der öffentlichen Wirtschaft und Gemeinwirtschaft

Der Verband der öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs – VÖWVG – vertritt die Interessen der öffentlichen Wirtschaft, insbesondere im Bereich der Daseinsvorsorge. Der VÖWVG repräsentiert somit Unternehmen und Einrichtungen, die im Eigentum, mit Beteiligung oder im Auftrag von Gebietskörperschaften Dienstleistungen von allgemeinem Interesse erbringen. Neben der Energie- und Trinkwasserversorgung, der Abfall- und Abwasserentsorgung und dem öffentlichen Verkehr sind auch die wirtschafts- und finanzpolitische Steuerung sowie die Bereiche Wohnen, Gesundheit und Soziales vom Begriff der Daseinsvorsorge umfasst.

Rechtsform: Verein

Sitz: Stadiongasse 6-8, A-1010 Wien

ZVR-Zahl (AT): 338965482

Zuständigkeit: LPD Wien, Abteilung für Vereins- Versammlungs- und Medienrechtsangelegenheiten

EU-Transparenzregisternummer: 16441688074-96

Einleitung

Der Verband der öffentlichen Wirtschaft und Gemeinwirtschaft (nachgehend VÖWG) bedankt sich für die Einbindung in das gegenständliche Begutachtungsverfahren und begrüßt die Bestrebungen, ein hohes Cybersicherheitsniveau von Netz- und Informationssystemen durch die Umsetzung der NIS-2-Richtlinie (EU-Richtlinie 2022/2555) in nationales Recht zu gewährleisten. Zum aktuellen Gesetzesentwurf erlaubt sich der VÖWG nachfolgende Stellungnahme einzubringen:

Allgemeines - Mehraufwand

Der zu erwartende Mehraufwand übersteigt für viele VÖWG-Mitgliedsunternehmen die in den Materialien ausgewiesenen Werte mit hoher Wahrscheinlichkeit signifikant. Allein die detaillierten Anforderungen zur Durchführung des Risikomanagements erfordern bereits einen erheblichen technischen Mehraufwand, da nicht nur bestehende Systeme erweitert, sondern auch neue Umsetzungsprozesse etwa in Form von Audits etabliert werden müssen.

Hinzu kommen erhebliche Kosten – sowohl in der Implementierung neuer Risikomanagementmaßnahmen als auch durch laufende Kosten im Betrieb, die sich aus den mit der Umsetzung einhergehenden organisatorischen Maßnahmen sowie dem damit zusammenhängenden Personalmehrbedarf ergeben. Beispielhaft seien erwähnt: die Notwendigkeit in der Anpassung von Dokumenten und Prozessen sowie die Umsetzung und Nachverfolgung von Risikomanagementmaßnahmen für Besprechungen; Schulungen oder Fortbildungen. Dabei muss ergänzend in Betracht gezogen werden, dass durch die erweiterte Definition der Richtlinie auch eine Erweiterung des Anwendungsbereiches innerhalb des Betriebes **erforderlich** ist. Sämtliche Systeme innerhalb der Unternehmung werden als wesentlich und somit als den geforderten Maßnahmenrahmen unterworfen betrachtet. Ergänzend sind die Aufwände im Management der Lieferketten von erheblicher Bedeutung und müssen miteinbezogen werden.

Ad § 1 – Verfassungsbestimmung

Die stark ausgeprägte Konzentration an Kompetenzen beim Bundesminister für Inneres wird vom VÖWG insbesondere in Zusammenhang mit der fehlenden Normierung von Kontrollmechanismen als rechtspolitisch bedenklich eingestuft.

Ad § 2 Gegenstand und Ziel des Gesetzes iVm § 3 Begriffsbestimmungen sowie Anlage 1

Zur eindeutigen Klärung der individuellen NIS2-Betroffenheit wäre aus Sicht des VÖWG eine umfangreichere (Legal-)Definition bzw. Abgrenzung zuvor genannter Begriffe notwendig, die sich weder in den Erläuternden Bemerkungen zum NISG 2024 noch in den entsprechenden EU-rechtlichen Dokumenten finden lassen. Aus unserer Sicht ist es wahrscheinlich, dass der Gesetzgeber hier aufgrund einer nicht ausreichend konkretisierten Begriffsbestimmung bzw. -abgrenzung einen weiteren Geltungsbereich des NISG 2024 erwirkt, der eventuell nicht im Sinne der zugehörigen EU-RL ist.

Ad § 3 Begriffsbestimmungen Z. 11 – „Leitungsorgan“

Das NISG 2024 definiert den Begriff der „Leitungsorgane“, die für die Einhaltung der NISG-Bestimmungen verantwortlich sind, äußerst weitgehend. Dieser umfasst etwa auch Aufsichtsratsmitglieder. Die Begriffsweite der „Leitungsorgane“ kann zu gravierenden Konsequenzen für unterschiedliche Gesellschaftsorgane führen, obwohl diese in keinem oder nur in einem entfernten Zusammenhang zur

Cybersicherheit im Unternehmen stehen. Weder im Gesetzestext noch in den Erläuterungen dazu wird Bezug auf die Definition der Leitungsorgane auf Konzern- oder Unternehmensgruppenstrukturen Beachtung genommen. In der Praxis kommt es jedoch häufig vor, dass in derartigen Strukturen beispielsweise sämtliche IT-Kompetenzen im Mutterunternehmen oder einem bestimmten Teilunternehmen für den ganzen Konzern oder die ganze Unternehmensgruppe gebündelt werden und andere Teilunternehmen in solchen Fällen keinerlei bzw. wenig Einfluss auf beispielsweise Risikomanagementmaßnahmen, wie im vorliegenden Gesetzesentwurf gefordert, haben. In derartigen Konstellationen erscheint es auch im Sinne der in der NIS2-Richtlinie eher funktionellen Betrachtung des Begriffes Leitungsorgan nicht zielführend, Leitungsorgane auf Personen oder Organe einzuschränken, die zur Führung der Geschäfte einer Einrichtung oder innerhalb der Einrichtung zur Überwachung der Geschäfte berufen sind. Warum ein derart weitgehendes Begriffsverständnis gewählt wurde, ist nicht ersichtlich, zumal es unionsrechtlich nicht zwingend geboten ist.

Es wird daher angeregt, die Legaldefinition des § 3 Z 11 NISG 2024 wie folgt anzupassen: *„Im Sinne dieses Bundesgesetzes bedeutet ‚Leitungsorgan‘ eine oder mehrere natürliche Personen oder Verwaltungsorgane, die nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte einer Einrichtung und zu deren Vertretung berufen sind“.*

Ad § 4 Abs 1 Z 13 iVm §§ 38, 39 – Cybersicherheitsbehörde

Der Bundesminister für Inneres wird hiermit als zuständige Behörde u.a. für die Ausübung der Aufsichts- und Durchsetzungsmaßnahmen gegenüber wesentlichen und wichtigen Einrichtungen gemäß §§ 38 und 39 definiert.

Anzumerken ist, dass die gegenständlichen Befugnisse des Bundesministers für Inneres vom VÖWG als überschießend eingestuft werden, da u.a. keine ausreichend klaren Vorgaben zum Umfang der zu kontrollierenden Informationen oder der Ad-hoc-Prüfungen bestehen. Dadurch besteht die unweigerliche Gefahr unverhältnismäßiger und somit richtlinienwidriger Eingriffe.

Ad § 10 – Aufsicht

Im vorliegenden Entwurf wird im Rahmen des Aufsichtsrechts des Bundesministers für Inneres über die CSIRTs ein Weisungsrecht eingeräumt. Bisher waren vorgebende und verwaltende Stelle mit dem Bundeskanzleramt und dem Bundesministerium für Inneres voneinander getrennt. Die nunmehrige Zusammenlegung der beiden Funktionen in das Bundesministerium für Inneres stuft der VÖWG als bedenklich ein. Dies vor allem unter dem Blickwinkel der einerseits Unterstützung suchenden Einrichtung und andererseits der behördlichen Funktion gegenüber derselben Einrichtung.

Während in den Erläuterungen der Zusatz „Verfassungsbestimmung“ vermerkt ist, fehlt dieser im Gesetzesentwurf. Es wird angemerkt, dass es sich gemäß den §§ 8 ff bei den CSIRTs um Einrichtungen des Bundes handelt, die vom Bundesminister für Inneres zur Aufgabenwahrnehmung ermächtigt werden und diesem daher unterstehen –somit ergibt sich keine Erforderlichkeit einer Verfassungsbestimmung bei der Einräumung des diesbezüglichen Aufsichts- und Weisungsrechts. **Sollte zur Verdeutlichung dieser gesetzlichen Bestimmung die Hebung in den Verfassungsrang legislativ intendiert sein, so ist dies im Gesetz entsprechend zu ergänzen.**

Ad § 11 – Koordinierte Offenlegung von Schwachstellen

Weder im Gesetzestext noch in den Erläuterungen finden sich nähere Beschreibungen zum notwendigen Inhalt, zum Format, zur Struktur sowie zur Art der Übermittlung der anonymen Einmeldung von Schwachstellen durch natürliche oder juristische Personen an den nationalen CSIRT. In Anbetracht dessen, dass anonyme Meldungen dem Ziel der Aufdeckung von Schwachstellen dienen und es das

Vertrauen der einmeldenden Person in diesen Prozess erfordert, ist eine möglichst klare Umschreibung der Anforderungen an die Einmeldung wünschenswert.

Es wird daher angeregt zu präzisieren bzw., in Anlehnung an § 33 Abs 6 NISG 2024, eine Möglichkeit zur Präzisierung durch Verordnung zu schaffen.

Zudem möchte der VÖWG anmerken, dass derzeitige Vigilanzmeldesysteme aus dem Medizinproduktegesetz keinerlei Berücksichtigung in der Bestimmung finden. Dort implementiert sind auch Verantwortungen zur Meldung und Koordination im Wege der Agentur für Gesundheit und Ernährungssicherheit (AGES).

Hier ist bei geplanter Umsetzung mit Unklarheiten in der Zuständigkeit und mit einem doppeltem Melde- und Kommunikationsbedarf zu rechnen. Diesbezüglich ist eine Ausnahme von Medizinprodukten vorzusehen.

Auch ist nicht nachvollziehbar, wie das nationale CSIRT mit den sektorspezifischen CSIRTs und die dortigen Problemstellungen einbezieht, da die übergeordnete Koordination die sektorspezifischen Problemstellungen nicht lösen kann. Hier sollte die sektorspezifischen CSIRTs die Koordination innerhalb der jeweiligen Sektoren übernehmen und in das nationale CSIRT rückmelden.

Ad § 20 – Zusammenarbeit auf nationaler Ebene (vgl. auch §§ 24. 38 und 39)

Im Zusammenwirken mit Medizinprodukten und den dortigen Bestimmungen wird auf die Erforderlichkeit der Miteinbeziehung des Bundesministeriums für Soziales Gesundheit, Pflege und Konsumentenschutz (BMSGPK) sowie der AGES hingewiesen.

Des Weiteren handelt es sich bei der Informationspflicht der Cybersicherheitsbehörde gegenüber der „zuständigen Behörde“ um einen unzulässigen(dynamischen) Verweis, da – wie auch aus den erläuternden Bemerkungen hervorgeht – auf die national noch nicht umgesetzte CER-Richtlinie (EU) 2022/2557 verwiesen wird.

Die Frist hierfür ist zudem auch noch nicht abgelaufen. Die vorliegende Bestimmung ist folglich unbestimmt und lässt die Behörde, welche gemeint ist, sohin die Zuständigkeit nicht determinieren und widerspricht damit insbesondere dem Legalitätsprinzip gem. Art 18 B-VG.

Ad § 25 – Ermittlung der Unternehmensgröße

Das NISG 2024 definiert seinen Anwendungsbereich in Bezug auf Unternehmen unter vollständigem Rückgriff auf die Kommissionsempfehlung 2003/361/EG samt den darin enthaltenen Bestimmungen über die Zurechnung von Werten konzernverbundener Unternehmen (§ 25 NISG 2024). Dies führt dazu, dass das NISG 2024 samt seinen Pflichten zur Setzung von Risikomanagementmaßnahmen etwa auch auf bestimmte Tochtergesellschaften von VÖWG-Mitgliedern zur Anwendung käme, selbst 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 zur Muttergesellschaft stehen.

Der österreichische Gesetzgeber sollte die von Erwägungsgrund 16 der NIS-2-RL eröffnete Möglichkeit nutzen und zur Wahrung der aus der österreichischen Bundesverfassung folgenden Verpflichtung zur Verhältnismäßigkeit der Pflichten des NISG 2024, die infolge des Grundsatzes der doppelten Bindung zu berücksichtigen ist, den Anwendungsbereich des Gesetzes entsprechend anpassen, indem er Ausnahmen von der Zurechnung vorsieht.

Es wird daher angeregt, eine entsprechende Bestimmung in das NISG 2024 – etwa als § 25 Abs 4 NISG 2024 – aufzunehmen. Diese könnte in Anlehnung an das deutsche NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz etwa wie folgt lauten:

„Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme für die Zwecke der Absätze 1 bis 3 sind die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse, unabhängig von seinen Partner- oder verbundenen Unternehmen ist.“

Ad § 27 – Ausnahmen von Verpflichtungen für wesentliche oder wichtige Einrichtungen aufgrund sektorspezifischer Rechtsakte der Europäischen Union

Doppelte Zertifizierungen (da z.B. ISO-zertifizierte Unternehmen laut dem aktuellen Gesetzesentwurf nicht automatisch als NIS-zertifiziert gelten) sind für VÖWG-Mitgliedsunternehmen mit einem massiven Mehraufwand verbunden. Um Doppelgleisigkeiten hinsichtlich der Zertifizierungen zu vermeiden, sollten Unternehmen und Einrichtungen, die nach ISO 27001 zertifiziert sind, auch als NIS-zertifiziert gelten.

Der VÖWG regt daher vor daher einen neuen Absatz 3 in § 27 NISG 2024 an: **„(3) Sofern wesentliche oder wichtige Einrichtungen nach ISO 27001 zertifiziert sind, kann der Bundesminister für Inneres diese Zertifizierung und deren Gleichwertigkeit durch Verordnung feststellen.“**

Ad § 29 – Register der Einrichtungen

Gemäß § 29 Abs 4 Z 1 NISG 2024 haben wesentliche und wichtige Einrichtungen gewisse Änderungen der Unternehmensdaten binnen maximal zwei Wochen an die Behörde zu übermitteln. Jegliche Verletzung dieser Verpflichtung, etwa auch geringfügige Überschreitungen der Frist, sind gemäß § 45 Abs 1 Z 2 NISG 2024 strafbewährt.

Es wird angeregt, die zweiwöchige Frist auf vier Wochen auszudehnen, um wesentlichen und wichtigen Einrichtungen mit Hinblick auf allfällige Urlaube oder Krankheiten für die ordnungsgemäß Meldung einen praxisgerechten Spielraum einzuräumen.

Ad § 31 Abs 2 – Haftung von Leitungsorganen

§ 31 Abs 2 NISG 2024 sieht vor, dass „Leitungsorgane [...] der Einrichtung für den schuldhaft verursachten Schaden“ haften, wenn sie ihre NIS-Pflichten verletzen. § 31 Abs 2 NISG 2024 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 NISG 2024 ersatzlos zu streichen.

Ad § 31 Abs 3 – Cybersicherheitsschulungen

Es gibt noch keine klaren Regelungen, welche zwingenden Inhalte solche Schulungen aufweisen müssen und ob solche extern durchgeführt werden müssen oder auch von Expert:innen „in House“ erfolgen können. Es ist nicht definiert, ob eine Teilnahme an diesen Schulungen genügt oder auch Zertifikate erworben und/oder Prüfungen abgelegt werden müssen. Ohne diese Rahmenbedingungen können keine Schulungen erfolgen und auch keine Strafen für fehlende Schulungen ausgesprochen werden. Es sind Übergangsbestimmungen festzulegen bis geeignete Schulungsinhalte und ausbildende Personen zur Verfügung stehen, um diese Schulungen überhaupt absolvieren bzw. eine Nichtabsolvierung bestrafen zu können.

Ad §§ 32 und 33 – Risikomanagementmaßnahmen im Bereich der Cybersicherheit und Nachweise der Wirksamkeit von Risikomanagementmaßnahmen

Der VÖWG weist nochmals auf den erheblichen Mehraufwand der detaillierten Anforderungen des gegenständlichen Gesetzesentwurfes hin. Die VÖWG-Mitgliedsunternehmen sehen sich mit der Implementierung zahlreicher gegenständlicher Vorgaben - neben des technischen Ausbaus – auch mit der Rekrutierung entsprechend ausgebildeten Personals konfrontiert. Aufgrund des europaweiten Fachkräftemangels erscheint die Umsetzung im vorgesehenen Zeitraum von drei Jahren nur mit enormem finanziellem Aufwand möglich.

Ad § 32 Abs 4 - Abs 4 Risikomanagementmaßnahmen im Bereich der Cybersicherheit

Der VÖWG regt an, den Entwurf der durch das BMI zu erlassenden VO vor deren Inkrafttreten ebenso in Begutachtung zu schicken, da die Überprüfung der festzulegenden Risikomanagementmaßnahmen auf ihre Praxistauglichkeit für ihren Erfolg wesentlich ist.

Ad § 33 – Nachweis der Wirksamkeit von Risikomanagementmaßnahmen

Aus dem Gesetzesentwurf geht nicht klar hervor, ob es sich bei den genannten drei Jahren um eine Mindestfrist handelt, oder ob die Behörde jederzeit neue Aufforderungen schicken und damit ein rollierendes System der Prüfungen auslösen kann. Der VÖWG regt hier dringend die Klarstellung an, dass es sich um eine Mindestfrist handelt, da sonst ein unverhältnismäßiger zeitlicher und monetärer Aufwand zu erwarten ist.

Ad § 34 Abs 1 und Abs 6 – Berichtspflichten

In § 34 (1) sollte wortgleich wie in § 37 (1) folgende Präzisierung vorgenommen werden: *34 (1) Wesentliche und wichtige Einrichtungen haben dem für sie zuständigen CSIRT, in Ermangelung eines solchen an das nationale CSIRT, unverzüglich jeden Cybersicherheitsvorfall (§35) zu melden. Das CSIRT leitet die Meldung unverzüglich an die Cybersicherheitsbehörde weiter.*

Bei § 34 Abs 6 wird nachfolgende Ergänzung angeregt: *„(...) Für die Interessensabwägung der Veröffentlichung ist darauf zu achten, dass nur jene Informationen veröffentlicht werden, die für den Zweck der Auswirkungen auf die Betroffenen erforderlich sind. Es ist auf den Verhältnismäßigkeitsgrundsatz gemäß § 1 Abs 2 DSGVO und auf den Grundsatz der Datenminimierung gem. Art 5 Abs 1 lit c DSGVO Bedacht zu nehmen.“*

Ad § 37 Abs 3 – Freiwillige Meldung relevanter Informationen

Ähnlich zu § 11 Abs 2. finden sich weder im Gesetzestext noch in den Erläuterungen nähere Beschreibungen zur Art der Übermittlung. Auch hier wird daher angeregt, zu präzisieren bzw. eine Möglichkeit zur Präzisierung durch Verordnung zu schaffen.

Ad § 39 – Durchsetzungsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen

Wird Leitungsorganen ein bescheidmäßiges Tätigkeitsverbot erteilt, sieht § 39 Abs 4 Z 2 NISG 2024 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 vorgezeichnet und deswegen unionsrechtlich nicht geboten.

Vor diesem Hintergrund kann es nicht nachvollzogen werden, weswegen der § 39 Abs 4 Z 2 NISG 2024 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 NISG 2024 ersatzlos zu streichen.

Ad § 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.

Ad § 41 – Verfahren vor dem Bundesverwaltungsgericht

§ 41 NISG 2024 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 NISG 2024 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 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, abweichend von § 13 des Verwaltungsgerichtsverfahrensgesetzes (VwGVG), BGBl. I Nr. 33/2013, keine aufschiebende Wirkung. Das Bundesverwaltungsgericht kann die aufschiebende Wirkung im betreffenden Verfahren auf Antrag zuerkennen, wenn nach Abwägung aller berührten Interessen mit dem Vollzug*

des Bescheides oder mit der Ausübung der mit dem Bescheid eingeräumten Berechtigung für den Beschwerdeführer ein schwerer und nicht wiedergutzumachender Schaden verbunden wäre.“

Ad § 42 Abs 2 – Datenverarbeitung

Hierbei wird nachfolgende Ergänzung angeregt: *„(...) Die Verarbeitung dieser personenbezogenen Daten hat auf den Verhältnismäßigkeitsgrundsatz gemäß § 1 Abs 2 DSG und den Grundsatz der Datenminimierung gem. Art 5 DSGVO zu erfolgen.“*

Ad § 43 – Datenübermittlung

Hierbei wird nachfolgende Ergänzung angeregt: *„(...) soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist.“*

Ad §§ 44 und 45 – Allgemeine Bedingungen für die Verhängung von Geldstrafen & Verwaltungsstrafbedingungen

Die Strafbestimmungen der §§ 44 und 45 NISG 2024 sind unbestimmt und damit verfassungsrechtlich problematisch. Es erscheint nicht ausgeschlossen, dass es die Bestimmungen ermöglichen, auch gegen natürliche Personen Geldstrafen in voller Höhe des Strafrahmens zu verhängen.

Einige Strafbestimmungen gemäß §45 sind unserer Ansicht nach in ihrer derzeitigen Einstufung nicht verhältnismäßig und sollten daher von Abs 1 in Abs 4 verschoben werden. Dies gilt insbesondere für §45 Z 4 und Z 5 (siehe oben zu § 31), Z 10 und Z 12 NISG 2024.

Aufgrund des § 44 Abs 4 NISG 2024 ist augenfällig, dass Geldstrafen nach dem NISG 2024 auch gegen verantwortliche Beauftragte und damit natürliche Personen verhängt werden können. 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 daher angeregt, für die Verhängung von Geldstrafen gegen natürliche Personen in den §§ 44 und 45 NISG 2024 abweichende Strafrahmen mit deutlich niedrigeren Strafdrohungen vorzusehen oder, da eine Strafbarkeit natürlicher Personen unionsrechtlich nicht geboten ist, eine Strafbarkeit nur für juristische Personen vorzusehen.

Ad § 46 – Anzeigepflicht des Bundesministers für Inneres

Zunächst wird festgehalten, dass weder im Entwurf noch in den Erläuterungen erwähnt wird, ob es sich bei § 46 um eine Verwaltungsstrafbestimmung oder eine behördliche Anordnung handelt. In Gesamtbetrachtung spricht mehr gegen das Vorliegen einer Verwaltungsstrafbestimmung, zumal die eindeutige Bezeichnung als solche fehlt und das Bestimmtheitsgebot aufgrund des Fehlens konkreter Fristen und Sanktionen nicht erfüllt ist.

In Abs 1 wird eine Anzeigepflicht des Bundesministers für Inneres an die Bezirksverwaltungsbehörden im Falle der Nichteinhaltung der aus diesem Gesetzesentwurf ergebenden Verpflichtungen normiert. Nachdem sich aus der NIS-2-RL (EU) 2022/2555 diesbezüglich keine Verpflichtung ableiten lässt, ist die in Rede stehende Anzeigepflicht zu streichen oder zumindest ein restriktiver und klardefinierter Ermessensspielraum für den Bundesminister für Inneres vorzugeben.

Zudem ist eine Ergänzung erforderlich, welche den Überprüfungen zur Feststellung der Nichteinhaltung vorgelagert sind. Ein Verweis auf die diesbezüglichen Paragraphen dieses Entwurfes wird angeregt.

In Abs 2 wird als Verfassungsbestimmung festgehalten, dass die Bezirksverwaltungsbehörde, die gem. Abs 1 angezeigte Nichteinhaltung mit Bescheid festzustellen hat und dabei eine angemessene Frist für die Herstellung des rechtmäßigen Zustandes eingeräumt wird.

Die „Herstellung des rechtmäßigen Zustandes“ muss je nach Art und Umfang der Verfehlung sowie nach Größe und Art der Einrichtung variieren, da diese weitreichenden Maßnahmen und Aufwendungen in der gesamten Einrichtung zur Folge haben können.

Die Angemessenheit der von der Behörde zu setzenden Frist für die Herstellung des rechtmäßigen Zustandes ist ebenfalls von diesen Faktoren abhängig. Da es sich hierbei um eine von der Verwaltungsbehörde festgelegte, behördliche Frist handelt, ist diese grundsätzlich veränderlich und eine Fristerstreckung möglich.

Es fehlen diesbezügliche Ausführungen insbesondere zu Art und Umfang der Verfehlung und Herstellung des rechtskonformen Zustandes (zumindest in den Erläuterungen) und werden daher dringend angeregt.

In Bezug auf die Veröffentlichungspflicht ist dem VÖWG Zweck und Ausgestaltung dieser Bestimmung unklar. Vor allem fehlen konkrete Vorgaben zur Dauer oder Art und Weise der Veröffentlichung, wie etwa, ob eine Veröffentlichung durch ein Medium oder auf andere Weise zu erfolgen hat. Aus Rechtssicherheitsgründen wird ein Verweis auf das bewährte System gemäß dem Mediengesetz angeregt.

Auch fehlt es an einem datenschutzrechtlichen Verweis, der vorsieht, dass bloß jene Informationen über die Nichteinhaltung von Verpflichtungen öffentlich bekannt gemacht werden dürfen, die keine konkreten Rückschlüsse auf die mit der Pflichtverletzung einhergehenden Sicherheitsmängel zulassen.

Weiters ist eine Bestimmung erforderlich, wer die diesbezüglichen Kosten der Veröffentlichung zu tragen hat. Die diesbezüglichen Klarstellungen sind hinsichtlich Überprüfbarkeit, Nachvollziehbarkeit und Transparenz der Bescheide iSd § 46 Abs 2 erforderlich.

Anknüpfend daran wird zum angewandten Prinzip des „naming and shaming“ angemerkt, dass insbesondere im Bereich der öffentlichen Verwaltung dies als zweckwidrig und überschießend anzusehen ist. Auch birgt es die Gefahr vulnerable Stellen potenziellen „Gefährdern“ kenntlich zu machen. Diesbezüglich ist auf eine verhältnismäßige Maßnahmensetzung bzw. Ausgestaltung Bedacht zu nehmen.

Abschließend darf der VÖWG auf die verkürzte parlamentarische Stellungnahmefrist von 4 Wochen hinweisen, die die profunde und vollumfängliche Begutachtung eines derartig wirkungsträchtigen Gesetzes erschwert.

Ad § 51 – Inkrafttretens-, Außerkrafttretens- und Übergangsbestimmungen

Abs 6:

Im Interesse von Betreiber wesentlicher Dienste nach dem noch geltenden NISG, die auch als wesentliche Einrichtungen nach dem NISG 2024 gelten, deren Überprüfungsfrist (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.

Abs 7:

Durch § 51 Abs. 7 im NISG 2024 wird die Umsetzungsfrist für Unternehmen, welche bereits in den Anwendungsbereich des bestehenden NISG fallen im Vergleich zu Unternehmen, welche erst in den neuen Anwendungsbereich von NISG 2024 fallen, deutlich verkürzt. Diese Verkürzung wird aufgrund folgender Gründe als problematisch betrachtet:

Das NISG 2024 stellt eine deutliche und umfangreiche Erweiterung des Anwendungsbereiches innerhalb von wesentlichen und wichtigen Einrichtungen dar, da der Anwendungsbereich vom wesentlichen Dienst auf die gesamte Einrichtung erweitert wird. Gleichzeitig wird die Umsetzungsfrist durch diesen Absatz aber erheblich verkürzt, wodurch der Umsetzungsaufwand für betroffene Unternehmen überproportional höher ist, als dies in der in § 33 NISG 2024 festgelegten Frist der Fall wäre. Diese Tatsache stellt eine grobe Benachteiligung der betroffenen Unternehmen im Vergleich zu jenen Unternehmen dar, welche neu in den Anwendungsbereich von NISG 2024 fallen werden, was gegen den Grundsatz der Gleichbehandlung verstößt.

Auch ist im Zusammenhang mit der Weiterführung der etablierten Prüfprozesse nicht klar, wie mit Empfehlungen bzw. Abweichungen aus bisherigen Überprüfungen laut NISG 2018 umzugehen ist.

Dieser Regelung liegt somit eine nicht sachliche Differenzierung zu Grunde. So sind Fallkonstellationen denkbar, wo Einrichtungen, die ihren letzten Nachweis gemäß § 17 Abs. 3 NISG vor längerer Zeit erbracht haben, eine entsprechend kurze Frist hätten, die neuen Maßnahmen aus dem NISG 2024 nachzuweisen. Wenn beispielsweise im Jahr 2022 der letzte Nachweis gemäß § 17 Abs 3 NISG übermittelt wurde, würde somit nur ein Jahr (bis 2025) zur Verfügung stehen, den Prüfbericht samt umgesetzte Maßnahmen aus NISG 2024 vorzulegen. Diesfalls stünde Betreibern wesentlicher Dienste gemäß § 16 Abs 1 NISG keine oder kaum Vorlaufzeit zur Verfügung, ein Umstand, der die verfassungsrechtliche Unverhältnismäßigkeit des § 51 Abs 7 NISG 2024 nach sich zieht.

Es wird daher angeregt, auch für Betreiber wesentlicher Dienste gemäß § 16 Abs 1 NISG in der Fassung BGBl I 111/2018 an den Zeitpunkt der Aufforderung zur Selbstdeklaration anzuknüpfen.

Alternativ sollte für Betreiber wesentlicher Dienste (*Scope alt*), die auch andere bisher unwesentliche Geschäftstätigkeiten erbringen (Multidienstleistungsunternehmen wie insbesondere Stadtwerke und kommunale Mehrspartenunternehmen) und nunmehr auch als wesentliche Einrichtungen gemäß §

24 Abs 1 gelten (*Scope neu*), die Möglichkeit geschaffen werden, den bisher nicht überprüfungspflichtigen Teil der Einrichtung unter Anwendung der dreijährigen Frist nach Aufforderung zur Selbstdeklaration einer Überprüfung zuzuführen. Die Gesetzesbestimmung könnte diesfalls eine Überprüfung des *Scope alt* unter Einhaltung der derzeit im Entwurf verankerten Frist und eine Überprüfung des *Scope neu* und damit der gesamten wesentlichen Einrichtung bis zum Ablauf der – im Falle von getrennten Rechtspersönlichkeiten/Organisationsformen – zur Anwendung gelangenden dreijährigen Frist vorsehen. Dadurch würden integrierte Multidienstleistungsunternehmen, die bereits Betreiber wesentlicher Dienste nach dem derzeit geltenden NISG waren, gegenüber anderen wesentlichen Einrichtungen nicht schlechter gestellt sein.

Angeregt wird zudem, dass für Betreiber wesentlicher Dienste, die auch als wesentliche Einrichtungen gemäß § 24 Abs 1 gelten, detaillierte Übergangsbestimmungen und die Möglichkeit zu einer zumindest einmaligen Fristverlängerung geschaffen werden, um die Rechts- und Planungssicherheit zu erhöhen.

Der VÖWG dankt nochmals für die Möglichkeit einer Stellungnahme und ersucht höflich um Berücksichtigung der hier dargelegten Überlegungen im weiteren Gesetzgebungsprozess.

Inhaltliche Verantwortung

Verena Wehr

Referentin - Digitalpolitik und rechtliche Angelegenheiten

+43-1-4082204-13

verena.wehr@voewg.at