Land Wien
Amt der Wiener Landesregierung
Magistratsdirektion - Recht

Bundeskanzleramt

Rathaus
1082 Wien
Telefon: +43 1 4000 82375
Fax: +43 1 4000 99 82310
post@md-r.wien.gv.at
wien.gv.at

MDR - 515506-2024-8
Entwurf eines Bundesgesetzes, 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,
Begutachtung;
Stellungnahme

zur Zahl 2024-0.220.735

Wien, 30. April 2024

Zu dem mit Schreiben vom 3. April 2024 übermittelten Entwurf eines Bundesgesetzes wird wie folgt Stellung genommen:

Grundsätzliche Anmerkungen:

Die mit der Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) geplanten Sicherheitsmaßnahmen können vom Markt für Medizinprodukte nicht erfüllt werden. Sie nehmen keine Rücksicht auf verfügbare personelle und finanzielle Ressourcen bei den Trägern und am österreichischen Arbeitsmarkt.

Es fehlt die gesetzliche Grundlage für Krankenhausträger-übergreifende Einsparungsmöglichkeiten und Aufwandsminimierungen bei der Überprüfung von Sicherheitsanforderungen in Lieferketten (z.B. die gemeinsame Nutzung von Überprüfungsergebnissen).

Es fehlt zudem bei der Umsetzung der NIS-2-Richtlinie die Möglichkeit zur risikoorientierten Umsetzung geforderter Sicherheitsmaßnahmen auf Grund detaillierter Maßnahmenvorgaben mit maxima-

ler Anforderungsbeschreibung (z. B. die Berücksichtigung aller Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen verursachen).

Die NIS-2-Richtlinie ist eng mit der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (RKE-Richtlinie) gekoppelt und ist ein harmonisiertes Vorgehen hinsichtlich des Zusammenwirkens und der Einflussnahme beider Normvorgaben notwendig. Vor diesem Hintergrund kann der Umstand, dass kein nationales Gesetz oder zumindest ein Entwurf zur Umsetzung der RKE-Richtlinie vorliegt, nicht nachvollzogen werden. Eine entsprechende Begründung ist auch nicht in den Erläuterungen des gegenständlichen Entwurfes enthalten.

Zu Art. 1 (Netz- und Informationssystemsicherheitsgesetz 2024):

Diese Artikelangabe fehlt im Entwurf, dort werden nur die Artikel 2 und 3 genannt.

Zu § 1 (Verfassungsbestimmung):

Zu Abs. 1 und 3:
Diese Bestimmung enthält eine dynamische Kompetenzdeckungsklausel, die es dem Bund nicht nur ermöglicht, die im Entwurf enthaltenen Regelungen im Bereich der Länderkompetenzen zu erlassen und aufzuheben, sondern auch zu ändern. Damit wird das System der bestehenden bundesstaatlichen Kompetenzverteilung unterlaufen. Dies wird vom Land Wien abgelehnt. Es wird darauf hingewiesen, dass von Seiten der Länder eine statische Kompetenzdeckungsklausel gefordert wird (siehe den Beschluss der Landeshauptleutekonferenz vom 3. November 2023).

Als Alternative zu einer statischen Kompetenzdeckungsklausel ist für das Land Wien eine Regelung nach dem Vorbild des Art. 14b Abs. 4 des Bundes-Verfassungsgesetzes (B-VG) denkbar. Es ist aber in diesem Zusammenhang sicherzustellen, dass die Länder in jenen Bereichen des Gesetzes, die wesentliche Auswirkungen auf die Länder haben, Mitwirkungsrechte nach dem Vorbild des Art. 14b Abs. 4 B-VG erhalten. Die in Abs. 3 enthaltene Regelung ist vor diesem Hintergrund zu wenig weitgehend und wird in dieser Form abgelehnt. Es ist daher erforderlich, die Zustimmungsbefugnis der Länder deutlich auszuweiten und die Verpflichtung des Bundes vorzusehen, den Ländern Gelegenheit zu geben, an der Vorbereitung von Gesetzesvorhaben in diesen Angelegenheiten mitzuwirken. Nur dann wäre rechtlich sichergestellt, dass die Länder ausreichend in die Vorbereitung eines Gesetzesvorhabens zur Änderung des NISG 2024 eingebunden werden und solche Gesetze - sofern Länderkompetenzen betroffen sind - nur mit Zustimmung der Länder kundgemacht werden dürfen.

§ 1 Abs. 3 wäre daher wie folgt zu formulieren:

„(3) Änderungen der §§ 17, 24 Abs. 2 Z 2, Abs. 3 und 5, § 44 Abs. 1, § 45 Abs. 5 sowie § 46 dürfen, sofern sie sich jeweils auf Behörden und sonstige Stellen der öffentlichen Verwaltung der Länder, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, beziehen, nur mit Zustimmung der Länder kundgemacht werden. Der Bund hat den Ländern Gelegenheit zu geben, an der Vorbereitung solcher Gesetzesvorhaben mitzuwirken."

Zu Abs. 2:
Die hier vorgesehene Bestimmung stellt den Bundesminister für Inneres über die obersten Organe der Vollziehung des Bundes und der Länder. Bei Art. 19 B-VG handelt es sich jedoch um einen zentralen Systembaustein des B-VG (*Raschauer in Korinek/Holoubek* et al, Band I/2, Art. 19 Abs. 1, Rz. 5). Als solcher ist Art. 19 B-VG ein wesentlicher Bestandteil des demokratischen Grundprinzips (*Raschauer*, aaO, Rz. 6) und steht daher nicht in der uneingeschränkten Disposition des Bundesverfassungsgesetzgebers. Die Bestimmung steht daher - auch wenn sie im Verfassungsrang beschlossen werden soll - mit diesem Grundprinzip in einem Spannungsverhältnis und ist somit verfassungsrechtlich bedenklich und abzulehnen. Keinesfalls kann mit der genannten Regelung ein Weisungsrecht des Bundesministers für Inneres gegenüber den obersten Organen des Bundes und der Länder verbunden sein. Dies wäre zumindest in den Erläuterungen klarzustellen.

Das Argument, eine vergleichbare Regelung bestünde bereits in § 35 Abs. 2 des Datenschutzgesetzes geht insoweit ins Leere, als die Datenschutzbehörde in Angelegenheiten des Datenschutzgesetzes tatsächlich als oberstes Organ der Republik fungiert - sie ist allerdings eine weisungsfreie Behörde, die außerhalb der Datenschutzangelegenheiten über keine Befugnisse oder Funktionen verfügt.

Neben den bestehenden Zuständigkeiten des Bundesministers für Inneres sieht der zu begutachtende Entwurf umfangreiche neue Befugnisse für ihn als Cybersicherheitsbehörde vor:

In § 17 wird der Betrieb von IKT-Lösungen durch den Bundesminister für Inneres geregelt. Die an dieser Stelle ungewöhnlich ausführlichen Erläuterungen führen zahlreiche Maßnahmen an, die mittels dieser Lösungen gesetzt werden können. Diese dienen dazu, „Angriffe, das Vorgehen des jeweiligen Angreifers im Netz des Teilnehmers und seine Kommunikation“ zu überwachen. Damit wird die technische Möglichkeit zur Überwachung des gesamten Datenverkehrs wichtiger und wesentlicher Einrichtungen im Wege der Threat Intelligence eingerichtet.

Vorgesehen ist, gegen Entrichtung eines durch Verordnung des Bundesministers für Inneres festgelegten Pauschalbetrages, auch die freiwillige Teilnahme wesentlicher und wichtiger Einrichtungen, nach den Erläuterungen insbesondere von Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene. Im Hinblick auf den finanziellen Aufwand des Betreibens eigener Lösungen für den öffentlichen Sektor ist davon auszugehen, dass die formal vorgesehene Freiwilligkeit durch finanzielle Zwänge eingeschränkt sein wird.

Die NIS-2-Richtlinie und auch § 32 Abs. 2 gehen von einem gefahrenübergreifenden Risikomanagement aus. Es sind daher einerseits bei der Setzung von Risikomanagementmaßnahmen und andererseits bei allfälligen Kontrollen dieser Maßnahmen gemäß § 38 Abs. 1 lit. 1 Bereiche der betroffenen Einrichtungen zu erfassen, die weit über die IT-Sicherheit hinausgehen. So wären wohl auch Personalmanagement und Finanzmanagement betroffen.

Die Aufsichtsmaßnahmen in § 38 sehen vor, dass der Bundesminister für Inneres als Cybersicherheitsbehörde befugt ist, wichtige oder wesentliche Einrichtungen durch Kontrollen der Umsetzung von Risikomanagementmaßnahmen mittels Einschau vor Ort, Fernzugriff oder Begleitung von unabhängigen Stellen zu überprüfen. Vorgesehen sind weiters Sicherheitsscans auf Basis objektiver Kriterien, die Anforderung von Informationen zur Bewertung der umgesetzten Risikomanagementmaßnahmen und Cybersicherheitskonzepte, die Anforderung des Zugangs zu für die Aufgabenerfüllung

erforderlichen Daten, Dokumenten und Informationen sowie die Durchführung von Ad-hoc-Prüfungen von wesentlichen Einrichtungen, etwa nach einem Cybersicherheitsvorfall, einem Verstoß gegen das NISG 2024, aber auch schlicht zur Überprüfung einer übermittelten Selbstdeklaration gemäß § 33 Abs. 1.

Es ist auf die Gefahr hinzuweisen, dass wichtige und wesentliche Einrichtungen sowohl im Bereich der Verwaltung als auch im Bereich der Privatwirtschaft - das sind nach aktuellen Schätzungen 4.000 bis 5.000 Unternehmen - durch diese Aufsichtsmaßnahmen zu gläsernen Einrichtungen für den Bundesminister für Inneres werden könnten.

§ 38 sieht keinen unmittelbaren Rechtsschutz vor, eine mangelnde Mitwirkung ist allerdings gemäß § 45 mit umfangreichen Strafen belegt. Die Frage nach dem Rechtsschutz in Zusammenhang mit den Maßnahmen des § 38 bleibt auch in den Erläuterungen unbeantwortet. Der Bundesminister für Inneres ist als Cybersicherheitsbehörde gemäß § 39 Abs. 4 lit. 2 darüber hinaus befugt, Leitungsorganen, also etwa Vorständen und Geschäftsführern sowie Aufsichtsräten von Unternehmen, die vom Bundesminister für Inneres als Cybersicherheitsbehörde mit Bescheid vorgeschriebene Auflagen nicht erfüllen, ihre Tätigkeit zu untersagen. Des Weiteren ist gemäß § 41 eine aufschiebende Wirkung von Beschwerden gegen derlei Bescheide grundsätzlich nicht vorgesehen und kann vom Bundesverwaltungsgericht nur dann zugesprochen werden, 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“.

In einer Zusammenschau all dieser Befugnisse ergibt sich im Hinblick auf die grundsätzlichen rechtsstaatlichen Anforderungen an ein System der Checks and Balances eine sehr hohe Befugniskonzentration beim Bundesminister für Inneres, auch gegenüber der Privatwirtschaft.

Zu § 2 (Gegenstand und Ziel des Gesetzes):

Zu Z 9:
Der Sektor Verwaltung von IKT-Diensten (Business-to-Business) ist in Anbetracht der Definitionen in § 3 Abs. 1 Z 7 (IKT-Dienst) und Anlage 1 Z 9 (Verwaltung von IKT-Diensten (Business-to-Business)) zu unbestimmt. Es wäre daher eine Konkretisierung vorzunehmen, um Rechtssicherheit bei der Bestimmung der von diesem Sektor Erfassten zu haben.

Zu § 3 (Begriffsbestimmungen):

Der Begriff „Dienst“ selbst wird nicht explizit definiert. Eine Definition sollte jedenfalls erfolgen, da derzeit eine sehr weite Auslegung möglich ist und eine Beschränkung auf wesentliche Dienste erforderlich wäre.

Zu Z 2 (Sicherheit von Netz- und Informationssystemen):
Zu dieser Legaldefinition ist anzumerken, dass es weitere Fähigkeiten neben der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit gibt, welche in gewissen Sektoren wie zum Beispiel der Industrie und dem Gesundheitssektor einen höheren Stellenwert haben bzw. höhere Anforderungen

stellen. Derartige Fähigkeiten sind etwa das Safety Kriterium bzw. die Patientensicherheit (patient safety).

Zu Z 11 (Leitungsorgan):
Der Begriff der Leitungsorgane, die für die Einhaltung der NISG 2024- Bestimmungen verantwortlich sind, wird äußerst weitgehend definiert. Er umfasst etwa auch Aufsichtsratsmitglieder. Diese Weite des Begriffs kann zu gravierenden Konsequenzen für unterschiedliche Gesellschaftsorgane führen, obwohl diese in keinem oder nur in einem entfernten Zusammenhang zur Cybersicherheit im Unternehmen stehen. Warum ein derart weitgehendes Begriffsverständnis gewählt wurde, ist nicht ersichtlich, zumal es unionsrechtlich nicht zwingend geboten ist. Der Gesetzesentwurf zum deutschen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz sieht deswegen einen engeren Zugang vor, der nur Organe umfasst, die sowohl zur Geschäftsführung als auch zur Vertretung befugt sind. Die deutsche Bestimmung definiert Organe der „Geschäftsleitung" als „natürliche Personen, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen sind".

Es wird daher angeregt, die Legaldefinition wie folgt anzupassen:
„ ‚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;".

Zu Z 12 (DNS-Diensteanbieter):
Von der Formulierung wäre jeder DNS-Server-Betreiber betroffen, dessen DNS-Server seine Dienste im Internet anbietet. Es würden etwa auch Einzelunternehmen darunterfallen, welche in Verbindung mit § 24 Abs. 1 Z 1 lit c. dann als wesentliche Einrichtung zu qualifizieren wären. Eine diesbezügliche Klarstellung wäre wünschenswert.

Zu Z 27 (Cyberbedrohung):
Bei der notwendigen Definition des Begriffs „Bedrohung" wäre Bezug auf eine realistische Eintrittswahrscheinlichkeit zu nehmen.

Zu Z 29 (Beinahe-Cybersicherheitsvorfall):
Die gewählte Begriffsdefinition erlaubt keine ausreichende Abgrenzung zwischen einem „Beinahe-Cybersicherheitsvorfall" und einem „Cybersicherheitsvorfall" (Z 30).

Zu Z 30 (Cybersicherheitsvorfall):
Es wäre eine Klarstellung erforderlich, ob es sich hiebei um eine ungeplante Beeinträchtigung des erbrachten Dienstes handelt, da auch ein geplantes Wartungsfenster eine Beeinträchtigung darstellt.

Zu § 4 (Cybersicherheitsbehörde):

Es sollte vorgesehen werden, dass von der Cybersicherheitsbehörde nur solches Personal in die jeweiligen nationalen und internationalen Gremien entsendet wird, das über sektorspezifisches Grundlagenwissen verfügt, um die Auswirkungen von Unterstützungen, Empfehlungen und Entscheidungen auf die betroffenen Sektoren abschätzen zu können.

Zudem sollte vorab - im Zuge von Entscheidungsprozessen - eine verpflichtende Abstimmung mit den fachlich zuständigen Ministerien erfolgen, um Auswirkungen auf ebendiese abschätzen zu können.

Problematisch erscheint, dass auf Grund der bislang fehlenden Umsetzung der RKE-Richtlinie insbesondere die Zuständigkeiten und Kompetenzen bei der Verschränkung von Notfällen und Katastrophenfällen von RKE-Richtlinie und NIS-2-Richtlinie unklar sind.

Zu Abs. 1 Z 13:
Die gegenständlichen Befugnisse des Bundesministers für Inneres sind überschießend, da keine klaren Vorgaben zum Umfang der zu kontrollierenden Informationen oder der Ad-hoc-Prüfungen bestehen. Dies birgt die Gefahr unverhältnismäßiger und daher richtlinienwidriger Eingriffe in sich.

Zu § 6 (Nationales Koordinierungszentrum für Cybersicherheit):

In Abs. 1 Z 8 hätte die Einbeziehung von Interessens- bzw. Sektorenvertretern sowie die Bereitstellung von Ergebnissen an ebendiese „verpflichtend" anstatt „gegebenenfalls" zu erfolgen.

Zu § 7 (Unabhängige Stellen und unabhängige Prüfer):

Zu Abs. 8:
Bei Fachprüfungen wären sowohl Betriebserfahrung sowie Sektorenspezifika zu berücksichtigen und gegebenenfalls die Erläuterungen entsprechend zu ergänzen.

Zu § 8 (Zweck und Aufgaben der Computer-Notfallteams - CSIRTs):

Zu Abs. 1:
Zu Z 1:
Was die "Überwachung [...] von [...] Schwachstellen [...] auf nationaler Ebene" umfasst ist unklar. Anzunehmen ist wohl eine „Überwachung" von Schwachstellen durch Penetration Tests oder permanentes Scannen. In diesem Zusammenhang ist weiters unklar, wie tief bzw. in welchem Umfang die CSIRTs die Netze der Einrichtungen scannen bzw. Penetration Testings durchführen dürfen.

Es sollten die Befugnisse der CSIRTs genauer definiert werden, insbesondere auch, wann und in welcher Form die Überwachung erfolgen soll (etwa durch an die Einrichtungen gerichtete Anfragen oder, ob eine Überwachung durch die Implementierung eines Scansystems im System der Einrichtungen erfolgen soll).

Eine Implementierung eines Scansystems im System der Einrichtungen wird vom Land Wien abgelehnt.

Zu Z 3:
In Z 1 und Z 3 haben die CSIRTs „gegebenenfalls" die Einrichtungen zu unterstützen. Es lässt sich aus diesen Bestimmungen nicht ableiten, wodurch die Unterstützungsleistungen veranlasst sind (durch ein Ersuchen einer Einrichtung oder aus eigenem Antrieb?).

Weiters ist hier nicht klar, ob die Einrichtung die Unterstützung annehmen muss oder ob diese Leistungen auch abgelehnt werden können. Auch stellt sich die Frage, ob in Fällen, in denen eine Einrichtung um Unterstützung ersucht, das CSIRT zur Leistung dieser Unterstützung verpflichtet ist. Insbesondere im Hinblick auf § 8 Abs. 1 Z 5, wonach Unterstützung an die ersuchenden Einrichtungen zu leisten ist, scheinen die Unterstützungsleistungen gemäß Z 1 und Z 3 nicht auf Ersuchen der Einrichtungen zu erfolgen.

Es wäre daher eine Klarstellung und allenfalls eine Anpassung der Formulierungen vorzunehmen.

Zu Abs. 2:
Es wäre notwendig, dass die betroffene Einrichtung über Ergebnisse informiert wird und bei Scans zusätzlich eine Vorabinformation ergeht.

Da je nach Ereignis auch eine Überprüfung weiterer (dritter) Einrichtungen denkbar ist, wird darüber hinaus angeregt, die Wortfolge „wesentlichen oder wichtigen" im dritten Satz zu streichen.

Zu § 10 (Aufsicht):

Das uneingeschränkte Weisungsrecht des Bundesministers für Inneres mit sofortiger Umsetzungsnotwendigkeit für nationale und sektorspezifische CSIRTs gefährdet massiv das Vertrauen in den vertraulichen Umgang mit Informationen meldender und hilfesuchender Einrichtungen. Angemerkt wird zudem, dass der in den Erläuterungen enthaltene Klammerausdruck (Verfassungsbestimmung) im Entwurf keine Entsprechung findet und kann die Erforderlichkeit, das Aufsichtsrecht in den Verfassungsrang zu heben, auch nicht nachvollzogen werden.

Zu § 11 (Koordinierte Offenlegung von Schwachstellen):

Aus semantischen Gründen wird vorgeschlagen, den in § 11 Abs. 1 Z 1 verwendeten Begriff der "betreffenden" Einrichtungen durch den in den Erläuterungen bereits zu findenden Begriff der „betroffenen**"** Einrichtungen zu ersetzen. Dies trifft im Übrigen auf mehrere Stellen des Entwurfs zu.

Das im Medizinprodukterecht etablierte Sicherheitssystem (Vigilanzmeldesystem) samt darin definierter Verantwortungen zur Meldung und Koordination wird im Gesetzesentwurf nicht berücksichtigt. Das führt zu unklaren nationalen Zuständigkeiten in der Bearbeitung gemeldeter Schwachstellen sowie zu doppeltem Melde- und Kommunikationsaufwand für Einrichtungen und auf nationaler Ebene zu doppeltem Koordinationsaufwand für die Koordinierung von Schwachstellen. § 11 sollte bestimmte Ausnahmen für regulierte Produkte, u. a. Medizinprodukte, vorsehen.

Die Koordination der Offenlegung von Schwachstellen wird beim nationalen CSIRT verankert. Sektorspezifische CSIRTs mit sektorspezifischem Know How und Lieferantenkontakten werden nicht direkt eingebunden.

Die Bestimmung wäre dahingehend anzupassen, dass sektorspezifische CSIRTs direkt eingebunden werden müssen und für sektorspezifische Schwachstellen (z. B. in Medizinprodukten) den Koordinationslead übernehmen.

Weiters ist unklar, ob für Betreiber eine Verpflichtung besteht, Schwachstellen zu melden und an wen diese Schwachstellen zu melden sind (z. B. in Bezug auf die Meldung von Beinahe-Vorfällen bzw. auf den definierten Meldeweg (§ 37) über die definierten Sektoren CSIRTS).

Zu § 17 (Betrieb von IKT-Lösungen):

Zu Abs. 2:
Die gewonnenen Erkenntnisse und Ergebnisse wären den betroffenen Einrichtungen ebenfalls zur Verfügung zu stellen.

Zu Abs. 3:
Aus dem Gesetzestext geht nicht klar hervor, wo die Überwachungskomponente positioniert sein soll (extern versus internes Netzwerk).

Die gewonnenen Erkenntnisse und Ergebnisse wären den betroffenen Einrichtungen ebenfalls zur Verfügung zu stellen.

Die Einrichtungen sollten zudem selbst den Datenumfang festlegen dürfen bzw. sollte die Möglichkeit zur Einschränkung der verarbeiteten Daten für die Einrichtung gegeben sein.

Bei der Übermittlung der Daten durch Überwachungskomponenten wird nicht auf die Datenübermittlung im Gesundheitsbereich eingegangen, so bezüglich besonderer Kategorien personenbezogener Daten („sensible Daten"), worunter gemäß Art. 9 Abs. 1 DSGVO sowohl Gesundheitsdaten als auch genetische Daten zählen.

Zu § 20 (Zusammenarbeit auf nationaler Ebene):

In den Erläuterungen wird die noch umzusetzende RKE-Richtlinie hinsichtlich der Identifizierung kritischer Einrichtungen bzw. der Zusammenarbeit der jeweiligen Behörden erwähnt. Aus Sicht der betroffenen Unternehmen (kritische Infrastruktur) ist die fehlende Umsetzung der RKE-Richtlinie ein wesentlicher Aspekt, da die Europäische Union die Kohärenz in der Umsetzung beider Richtlinien vorsieht. Hier ist Art. 12 Abs. 1 der RKE-Richtlinie hervorzuheben, der eine Risikobewertung durch kritische Einrichtungen beschreibt, welche Auswirkungen auf die Umsetzung der Risikomanagementmaßnahmen gemäß § 32 hat. Da die nationale Umsetzung ausständig ist, stellt die fehlende Kohärenz somit speziell für die betroffenen Unternehmen ein untragbares Risiko dar. Dies liegt insbesondere auch in der größenunabhängigen Einstufung gemäß § 26 und dem dort erläuterten „Systemrisiko" begründet.

Zu § 21 (Zusammenarbeit mit der Datenschutzbehörde):

Zu Abs. 2:
Die Wahrscheinlichkeit einer direkten Meldung der Cybersicherheitsbehörde an die Datenschutzbehörde wird aufgrund der Verknüpfung von §§ 32 und 34 als niedrig eingestuft. Gegebenenfalls kommt die Cybersicherheitsbehörde der Meldung der betroffenen Einrichtung zuvor. Die Bestimmung wäre dahingehend anzupassen, dass grundsätzlich der betroffenen Einrichtung auf Grund der ihr vorliegenden Informationen und der einschätzbaren Auswirkungen die Entscheidung überlassen

ist, ob eine Meldung gemäß der Datenschutz-Grundverordnung (DSGVO) bzw. des NISG 2024 an die zuständigen Behörden erfolgt. In diesem Zusammenhang sollte auch eine Unterrichtung des Verantwortlichen im Sinne des Art. 4 Z 7 DSGVO vorgesehen werden.

Zu § 24 (Wesentliche und wichtige Einrichtungen):

Zu Abs. 1:
In Z 1 lit f wäre in der Wortfolge "Richtlinie (EU) 2022/2557)" das letzte Klammerzeichen zu streichen.

Zu Abs. 3:
Hier werden die Einrichtungen im Sektor der öffentlichen Verwaltung unter anderem als Einrichtungen definiert, die ermächtigt sind, im Rahmen ihrer gesetzlich übertragenen Aufgaben Bescheide zu erlassen. Die Beschränkung auf die Hoheitsverwaltung kann dem Abs. 5 in dieser Form aber nicht entnommen werden. Der Anwendungsbereich des Abs. 5 wäre daher - in Klarstellung des Verhältnisses zu Abs. 3 - auf den hoheitlichen Tätigkeitsbereich der genannten Stellen einzuschränken.

Zu Abs. 5:
Es ist darauf hinzuweisen, dass in den Sektor der öffentlichen Verwaltung nur Einrichtungen des Bundes und der Länder fallen. Die Gemeinden und ihre Einrichtungen sind ausdrücklich ausgenommen. Diese Vorgabe - also die Ausnahme der Gemeinden vom Wirkungsbereich der Bestimmung - gilt für alle Gemeinden und demnach auch für Wien. Auf Grund der Doppelstellung von Wien als Gemeinde und Land (vgl. Art. 108 B-VG) üben in Wien die Gemeindeorgane auch die Funktion von Landesorganen aus. Demzufolge wird der Magistrat in Teilbereichen auch als Amt der Wiener Landesregierung und somit als Landesorgan tätig. Legt man nun den oben angeführten Anwendungsbereich der Bestimmung auf Wien um, so bedeutet dies, dass jene Bereiche bzw. Dienststellen des Magistrats, die nur der Gemeindeebene zuzurechnen sind, weil sie nicht als Amt der Landesregierung tätig werden, vom Anwendungsbereich der Bestimmung nicht erfasst sind. Das Land Wien versteht daher diese Regelungen so, dass jene Bereiche bzw. Dienststellen, die nur der Gemeindeebene zuzurechnen sind, nicht in den Sektor der öffentlichen Verwaltung fallen. Eine diesbezügliche Klarstellung sollte entweder im Gesetz oder in den Erläuterungen erfolgen.

Zu Abs. 6:
Gerade im Hinblick auf die Regelungsdichte für die vom Anwendungsbereich des NISG 2024 umfassten Sektoren überrascht die vollständige Ausnahme für die Bereiche der nationalen und öffentlichen Sicherheit.

Unklar ist, wie mit jenen Bereichen der bundesstaatlichen Verwaltung in Angelegenheiten der nationalen und öffentlichen Sicherheit umzugehen ist, deren Dienste Grundlage für die vom Anwendungsbereich umfasste Landesverwaltung sind, wie etwa das Zentrale Melderegister, die zentrale Wählerevidenz, das zentrale Personenstandsregister und das Staatsbürgerschaftsregister. Dies ist aber gerade im Hinblick auf § 32 Abs. 2 Z 3 und die Verantwortung der Länder für die Berücksichtigung der Sicherheit kritischer Lieferketten bei der Setzung von Risikomanagementmaßnahmen von wesentlicher Bedeutung.

Zu § 25 (Ermittlung der Unternehmensgröße):

Der Gesetzesentwurf 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. Dies führt dazu, dass das NISG 2024 samt seinen Pflichten zur Setzung von Risikomanagementmaßnahmen etwa auch auf sämtliche Tochtergesellschaften zur Anwendung käme, selbst wenn diese nur über einzelne Mitarbeiter verfügen, sie unter dem Gesichtspunkt der Netz- und Informationssicherheit keine kritische Infrastruktur betreiben und auch technisch und organisatorisch in keinem Zusammenhang zur Muttergesellschaft stehen (Beispiel: Windpark der WIEN ENERGIE GmbH in der Steiermark).

Im Gesetzesentwurf zum deutschen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz sind gewisse Ausnahmen von der Zurechnung vorgesehen, dies im Sinne einer nach dem Erwägungsgrund 16 der NIS-2-Richtlinie ausgestalteten Öffnungsklausel . Diese Ausnahmeregelung sollte zur Vermeidung von unverhältnismäßigen Ergebnissen übernommen werden.

Man sollte die von Erwägungsgrund 16 der NIS-2-Richtlinie 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 etwa als Abs. 4 aufzunehmen. Diese könnte in Anlehnung an den Gesetzesentwurf zum deutschen 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."

Zu § 29 (Register der Einrichtungen):

Zum vorgesehenen Prozedere bei der Registrierung der wesentlichen und wichtigen Einrichtungen wird bemerkt, dass gerade im Vergleich zur bisher geltenden Rechtslage das Abgehen von einer bescheidmäßigen Feststellung der Betroffenheit von Einrichtungen kritisch betrachtet wird. Die vorliegende Regelung verlangt von den betroffenen Einrichtungen, ihre Betroffenheit binnen drei Monaten ab Inkrafttreten des Gesetzes umfassend selbst festzustellen und eine entsprechende Registrierung vorzunehmen.

Dies ist insbesondere im Hinblick auf die Strafbarkeit der nicht fristgerechten Registrierung gemäß § 45 Abs. 1 Z 1, wobei Wissentlichkeit für die Strafbarkeit nicht Voraussetzung ist, und auf die emp-

findliche Erhöhung der Strafen eine große Herausforderung für die infrage kommenden Einrichtungen.

Angesichts der Komplexität der Kriterien, die bei der Beurteilung der Betroffenheit einer Einrichtung zu prüfen sind, scheint die Vorwerfbarkeit eines trotz redlicher Bemühungen unrichtigen Prüfergebnisses fraglich. Es wird daher bereits aus Gründen der Rechtssicherheit angeregt, eine Art optionales Feststellungsverfahren zur Betroffenheit zu schaffen.

Zu Abs. 2:
Seitens der Behörde muss die Verwendung des gewählten Kommunikationsmediums (Post, E-Mail, Telefon) mit dem Kommunikationszweck verknüpft werden. Der Kommunikationszweck soll die Reaktion der betroffenen Einrichtung bestimmen. E-Mails sind kein Echtzeitkommunikationsmittel, E-Mail Server können technisch ausfallen, der externe Empfang von E-Mails kann im Rahmen der Reaktion auf Sicherheitsvorfälle eingeschränkt werden und etablierte Sicherheitsmechanismen (z. B. Blocklists, Externe Intelligence Informationen, komponentenspezifische Härtungsempfehlungen) können zu einer verzögerten Zustellung von E-Mails führen.

Der Gesetzesentwurf wäre dahingehend anzupassen, dass E-Mails nur für Meldungen mit informativem Charakter und wenn keine unmittelbare Handlungsnotwendigkeit gegeben ist, verwendet werden dürfen.

Zu Abs. 4:
Wesentliche und wichtige Einrichtungen haben 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 strafbewehrt.

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

Zu § 31 (Governance):

Zu Abs. 2:
Hier ist eine Verschuldenshaftung vorgesehen. Diese würde auch bereits leichte Fahrlässigkeit umfassen. Das übersteigt den dem Management zumutbaren Haftungsumfang.

Die Haftung für leichte Fahrlässigkeit sollte daher jedenfalls ausgeschlossen werden. Zur Erlassung einer derart strengen Haftungsbestimmung verpflichtet die NIS-2-Richtlinie nicht, zumal die Haftung der Leitungsorgane bereits gesellschaftsrechtlich ausreichend sichergestellt ist. Aus diesem Grund fehlt beispielsweise im Gesetzesentwurf zum deutschen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz eine Haftungsbestimmung, weil sich eine ausreichende Haftung eben bereits aus allgemeinen Grundsätzen ergibt.

Es wird daher angeregt, Abs. 2 ersatzlos zu streichen.

Zu Abs. 3:
Diese Rechtsvorschrift adressiert Governance-Anforderungen an das Management und an Aufsichtsorgane. Der zweite Satz sollte als eigener Absatz in § 32 verschoben und dahingehend ergänzt werden, dass bei der Ausgestaltung anzubietender Schulungen die jeweiligen Zielgruppen ebendieser Schulungen berücksichtigt werden sollten, sodass angebotene Schulungen möglichst nutzbringend sind (Pflegepersonal, ärztliches Personal, etc. benötigt kein Fachwissen über Managementpraktiken zu Cybersicherheitsrisiken). Zudem ermöglicht eine Verschiebung in § 32 eine risikoorientierte Umsetzung im Zusammenspiel mit den aktuellen Überlegungen zu NIS-2-Cybersicherheitsmaßnahmen, die ein Programm zur Steigerung des Bewusstseins für Cybersicherheit fordern, in dem Schulungen nur ein mögliches Werkzeug darstellen, um das Bewusstsein hinsichtlich Cybersicherheit zu erhöhen.

Es ist noch darauf hinzuweisen, dass es keine klaren Regelungen gibt, welche zwingenden Inhalte solche Schulungen aufweisen müssen (z. B. ob diese extern durchgeführt werden müssen). Unklar ist auch, ob eine Teilnahme an diesen Schulungen genügt oder ob auch Zertifikate erworben bzw. Prüfungen abgelegt werden müssen.

Ohne diese Rahmenbedingungen können keine Schulungen erfolgen und auch keine Strafen für fehlende Schulungen ausgesprochen werden. Es wären Übergangsbestimmungen festzulegen, bis geeignete Schulungsinhalte und Ausbildende zur Verfügung stehen, um diese Schulungen überhaupt absolvieren und folglich eine Nicht-Absolvierung bestrafen zu können.

Zu § 32 (Risikomanagementmaßnahmen im Bereich der Cybersicherheit):

Zu Abs. 2:
Die betroffenen Einrichtungen im Gesundheitssektor verfügen auf Grund der Vielzahl an Netz- und Informationssystemen über unzureichende Ressourcen, um gemäß § 32 Abs. 2 Z 3 lit. a bei den jeweiligen Netz- und Informationssystemen deren spezifische Schwachstellen und die Gesamtqualität zu überprüfen. Bezugnehmend auf § 32 Abs. 2 Z 3a stellt die Beurteilung der Sicherheit der Entwicklungsprozesse in der Lieferkette in Anbetracht der großen Anzahl an Lieferanten in der Lieferkette einen untragbaren Aufwand für alle Betreiber dar. Auf Grund der großen Anzahl der Lieferanten und etwaiger gesetzlicher oder patentrechtlicher Vorrausetzungen ist eine Beurteilung der Sicherheit der Entwicklungsprozesse aus Kundensicht nicht möglich. Es wird in diesem Zusammenhang auf andere Regelungen (Cybersecurity Act, EU-Lieferketten Gesetz) verwiesen, die hier zur Anwendung kommen sollten und eine immense Verringerung der Ressourcen der betroffenen Unternehmen zur Folge hätten.

Zu Abs. 3:
§ 32 Abs. 3 sollte neben Abs. 1 insbesondere auch Abs. 2 Z 3 beinhalten, um eine risikoorientierte Adressierung, unter Wahrung wirtschaftlicher Verhältnismäßigkeit, bei einer Vielzahl an unterschiedlichen Teilnehmern zu ermöglichen. Es sollte ausdrücklich auch auf Abs. 2 Z 3 verwiesen werden, damit zur Sicherheit der Lieferketten explizit auch eine Wirtschaftlichkeitsabwägung erfolgt.

Es wären Übergangsfristen für die Umsetzung von Sicherheitsmaßnahmen vorzusehen, nachdem das Gesetz ohne Übergangsfristen in Kraft tritt (§ 51). Aktuell sind die nicht öffentlich diskutierten Ideen für Sicherheitsanforderungen sehr detailliert ausgestaltet, allerdings nur unvollständig be-

kannt. Eine Umsetzung im Teilsektor Gesundheit ist auf Grund dessen Komplexität und Systems externer Zulieferer und Dienstleister bis zum Inkrafttreten des Gesetzes theoretisch und praktisch nicht vollständig umsetzbar. Für die mangelnde Umsetzung sind dennoch Strafbestimmungen vorgesehen.

Zu Abs. 4:
Es sollte eine Begutachtung der zu erlassenden Verordnung durchgeführt werden, da die Überprüfung der festzulegenden Risikomanagementmaßnahmen auf ihre Praxistauglichkeit für ihren Erfolg wesentlich ist.

Zu § 33 (Nachweis der Wirksamkeit von Risikomanagementmaßnahmen):

Zu Abs. 2:
Die Erbringung von Nachweisen für die Wirksamkeit gestaltet sich auf Grund der Erfahrungen für die betroffenen Einrichtungen hinsichtlich der weitreichenden Interpretation des Begriffs „Netz- und Informationssysteme" im Teilsektor Krankenanstalten (dieser umfasst IT Systeme, Medizintechnik und Haustechnik) sowie auf Grund der Komplexität und Vielzahl an externen Lieferanten und externen Dienstleistern als sehr ressourcenaufwändig. Vor dem Hintergrund von § 51 Abs. 7 wäre eine Ausdehnung des Intervalls von drei Jahren auf fünf Jahre vorzusehen. Dies aus folgenden Gründen:

- Durchlaufzeiten der Prüfungen betragen bis zu neun Monate. Überprüfungen binden eine hohe Anzahl an internen und externen Personalressourcen (u. a. von Lieferanten und Dienstleistern). Die Behörde fordert die Prüfung von qualifizierten Stellen bei Dienstleistern, ohne dass Rechtssicherheit als Basis für die Nutzung von Synergieeffekten durch gemeinsam durchgeführte Überprüfungen besteht. Es gibt hohen internen Abstimmungsbedarf für Feststellungen und umfassende Dokumentationsanforderungen seitens der Behörde. Es müssen Nachweise für die Erfüllung jeder Maßnahmenforderung über den gesamten Scope erbracht werden (gemäß Stichprobe der qualifizierten Stelle).
- Die Umsetzung von Projekten dauert meistens länger (insbesondere bei größeren Trägern), meistens Jahre, bis Änderungen auf alle Kliniken - unter Wahrung der Patientensicherheit - ausgerollt sind.
- Nach der abgeschlossenen Prüfung hat die Behörde anhand des Überprüfungsberichts einen Überblick über die Wirksamkeit der Maßnahmen zur Priorisierung ihrer Prüftätigkeiten. Danach erfolgt seitens der Behörde ein Tracking ausgesprochener Empfehlungen.
- Über die Maßnahmenumsetzung von Empfehlungen muss die betroffene Einrichtung der Behörde laufend Bericht erstatten.
- Sicherheitsmaßnahmen sehen sowieso ein internes Audit, Übungen etc. vor.

Zu § 34 (Berichtspflichten):

Zu Abs. 1:
Hier sollte in Anlehnung an § 37 Abs. 1 folgende Präzisierung (siehe nachfolgende Unterstreichung) vorgenommen werden:
„Wesentliche und wichtige Einrichtungen haben dem für sie zuständigen CSIRT, <u>in Ermangelung eines solchen dem</u> nationalen CSIRT, unverzüglich jeden Cybersicherheitsvorfall (§ 35) zu melden. Das CSIRT leitet die Meldung unverzüglich an die Cybersicherheitsbehörde weiter."

Zu Abs. 2:
Z 4 lit. a sieht „eine ausführliche Beschreibung des Cybersicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen“ vor. Daraus resultiert ein hoher interner Erstellungs- und Abstimmungsaufwand für die Berichterstellung. Das Attribut „ausführliche“ sollte daher gestrichen werden.

Die in Z 5 vorgesehene Frist zur Vorlage des Abschlussberichts ist insoweit unklar, als deren Beginn an die „Behandlung des Cybersicherheitsvorfalls“ anknüpft. Ein Rückgriff auf die in den Erläuterungen benutzte Begrifflichkeit der „Bewältigung des Cybersicherheitsvorfalls“ würde wohl zu einer klareren Rechtslage führen.

Zu Abs. 3:
Hier wird eine Veröffentlichung meldepflichtiger Cybersicherheitsvorfälle ohne Abwägung der Auswirkungen durch die betroffene Einrichtung vorgesehen. Damit ginge eine Desensibilisierung der Bevölkerung einher. Die Bestimmung wäre dahingehend zu adaptieren, dass die betroffene Einrichtung die Notwendigkeit einer öffentlichen Kommunikation von Cybersicherheitsvorfällen auf Grund intern ergriffener Notfallmaßnahmen und deren Auswirkungen auf Patienten selbst abwägt, statt stets zu einer öffentlichen Kommunikation verpflichtet zu sein.

Weiters wäre auch der Begriff „Empfänger der Dienste“ näher zu definieren (Werden darunter ambulante oder stationäre Patienten im Krankenhaus, Patienten im Einzugsgebiet bzw. in der jeweiligen Versorgungsregion verstanden?).

Zu § 35 (Erheblicher Cybersicherheitsvorfall):

Zur besseren Lesbarkeit wäre § 35 vor § 34 zu reihen oder könnte dessen Inhalt in § 34 integriert werden.

Zu Abs. 2:
Die Ergänzung wird begrüßt, da dieser Absatz eine sektorspezifische bzw. unternehmenspezifische Präzisierung von Meldepflichten ermöglicht. Andernfalls müsste der Teilsektor Krankenhaus jeglichen Alarm an das zuständige CSIRT melden, da im Gesundheitsbereich zum Zeitpunkt eines detektierten Alarms immer die Möglichkeit schwerwiegender finanzieller Verluste oder materieller bzw. immaterieller Schäden an natürlichen Personen (Patienten) bestehen kann. In diesem Fall müsste die Behörde eine Applikationsschnittstelle zur automatisierten Weiterleitung einer Vielzahl von Alarmen bereitstellen.

Zu § 36 (Vereinbarungen über den Austausch von Informationen zur Cybersicherheit):

Seitens des Teilsektors Krankenhaus werden stets Bestrebungen zur Förderung des sektorinternen und sektorübergreifenden Informationsaustausches befürwortet. Die Bestimmung ist jedoch bürokratisch mit begrenztem Mehrwert: Mit Lieferanten und Dienstleistern besteht im Rahmen der Serviceerbringung in der Regel ein Informationsaustausch zu den in Abs. 1 genannten Themen. Eine schriftliche Vereinbarung dazu kann z. B. in Allgemeinen Geschäftsbedingungen, Vertragsunterlagen oder sonstigen Vereinbarungen festgehalten sein. Nach dieser Bestimmung wäre jede Vertragsbeendigung und jeder neue Vertragsabschluss an die Behörde zu melden. In Anbetracht des

komplexen und umfangreichen Systems an Lieferanten, Dienstleistern und Kooperationspartnern im Teilsektor Gesundheit ist dieser bürokratische Mehraufwand nicht vertretbar.

Zudem wäre unklar, wie mit bestehenden Vereinbarungen und Vertragsverhältnissen mit Lieferanten und Dienstleistern umgegangen werden soll. Es sollte eine Beschränkung auf die Erstellung von Vorlagen erfolgen, eine Informationsquelle für sektorinterne und sektorübergreifende Abstimmungsmöglichkeiten bereitgestellt werden und eine verbindliche Vertraulichkeit hinsichtlich übersendeter und empfangener Informationen festgeschrieben werden (statt der Vorschrift, eine vorgegebene Vereinbarung zu verwenden) oder der Paragraph ersatzlos gestrichen werden.

Zu § 37 (Freiwillige Meldung relevanter Informationen):

Zu Abs. 3:
Es kann nicht nachvollzogen werden, welchen Mehrwert die Behörde aus einer Meldung hat, aus der die Identität der betroffenen Einrichtung nicht hervorgeht.

Zu § 38 (Aufsichtsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen):

Zu Abs. 1:
Zu Z 1:
In dieser Bestimmung wird die Aufsichtsmaßnahme der Einschau geregelt, wobei diese jeweils nach vorangegangener Verständigung der betroffenen Einrichtung durchgeführt werden darf. In diesem Zusammenhang wäre die Festlegung einer Mindestfrist, welche zwischen Verständigung und Durchführung der Einschaumaßnahme liegt, wünschenswert, da der Begriff “vorangegangen” einen sehr großen Interpretationsspielraum zulässt.
Besser wäre die Normierung einer Frist zur Verständigung von mindestens 14 Tagen, um die Verfügbarkeit interner Ansprechpersonen in der Einrichtung und bei Dienstleistern und Lieferanten sicherstellen zu können; insbesondere auch deshalb, weil Z 1 keine Zeitkritikalität bzw. keine unmittelbare Gefährdung als Kriterium enthält.

Zu Z 2:
Es wird keine Differenzierung zwischen internen und externen Schwachstellenscans vorgesehen. Analog zu den Erläuterungen wäre eine Einschränkung auf externe Schwachstellenscans aus dem Internet vorzunehmen.

Die Bestimmung wäre dahingehend zu überarbeiten, dass Schwachstellenscans der betroffenen Einrichtung jedenfalls 14 Tage vorab angekündigt und vorab mit den betroffenen Einrichtungen abgestimmt werden müssen und in begründbaren Fällen verschoben werden können. Jedenfalls hätte die durchführende Behörde für sämtliche verursachten Personen- und Sachschäden, die potenziell aus der Scandurchführung und weiteren Folgen resultieren können, zu haften.

Es wäre der Rahmen bzw. der Umfang von Sicherheitsscans genauer zu definieren. Es wird in diesem Zusammenhang auf die Anmerkungen zu § 8 Abs. 1 Z 1 hingewiesen.

Zu Z 5:
Die Bestimmung sollte dahingehend überarbeitet werden, dass die vorgesehene Ad-hoc-Prüfung ausschließlich in dringlichen Anlassfällen bei unmittelbarer Gefährdung oder Gefahr in Verzug in Abstimmung mit der betroffenen Einrichtung durchgeführt werden kann. In der vorliegenden Textierung wären Ad-hoc-Prüfungen ohne näher definierte Kriterien jederzeit möglich und würden eine Umgehung der Rahmenbedingungen in Z 1 zulassen. In begründeten Einzelfällen sollte es der betroffenen Einrichtung dennoch möglich sein, Prüfungshandlungen zur Wahrung der Patienten- und Betriebssicherheit (z. B. bei laufenden medizinischen Eingriffen) aufzuschieben.

Zu § 39 (Durchsetzungsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen):

Zu Abs. 3:
Zu Z 1:
Zu lit. a:
Diese Bestimmung erlaubt dem Bundesminister für Inneres in der Rolle als Cybersicherheitsbehörde verschiedene Handlungen gegenüber den adressierten Einrichtungen zur Sicherstellung der Einhaltung ihrer Verpflichtungen aus diesem Bundesgesetz. Die Behörde ist befugt, mit Bescheid „die Unterrichtung der potenziell von einer erheblichen Cyberbedrohung betroffenen Personen [...] sowie über mögliche Abwehr- und Abhilfemaßnahmen zu (sic!) anzuordnen“. Auf Ebene der betroffenen Unternehmen erscheint diese Unterrichtung zwar umsetzbar, wenn es sich bei den Betroffenen allerdings um Kunden im Sinne einer großen Zahl von Privatpersonen handelt, erscheint die Umsetzbarkeit fraglich.

Zu lit. b:
Durch die öffentliche Bekanntmachung von Verstößen soll offenbar die Compliance gefördert werden. Allerdings ist anzumerken, dass diese Information per se der Vertraulichkeit unterliegt und ein Sicherheitsrisiko darstellt. Die Verunsicherung der Bevölkerung wäre eine direkte Folge einer solchen Maßnahme. Außerdem würden mögliche Angreifer, sowohl staatliche Akteure als auch kriminelle Elemente, durch publizierte mangelhafte Sicherheitsmaßnahmen erst recht angelockt.

Das Ziel dieser Bestimmung lässt sich aus der NIS-2-Richtlinie nicht direkt ableiten. In diesem Zusammenhang ist auf die vorgesehene Verfassungsbestimmung des § 46 Abs. 2 letzter Satz hinzuweisen. Gemäß dieser darf die Veröffentlichung nur insoweit erfolgen, als diese keine Gefahr für die öffentliche Ordnung oder Sicherheit darstellt. Es wird nicht näher spezifiziert, nach welchen Kriterien die Gefahrenbewertung erfolgt. Im Zweifel ist jede publizierte zuvor nicht öffentliche Information als eine Bedrohung aus Sicht der Informationssicherheit bzw. des Geheimhaltungsschutzes zu werten. Zudem ist nicht klar, ob gegen einen entsprechenden Bescheid der Bezirksverwaltungsbehörde über die Veröffentlichung ein wirksames Rechtsmittel (Unsicherheit über die Zuerkennung der aufschiebenden Wirkung) möglich wäre.

Zu Z 2:
Der Umfang des fachlich notwendigen Wissens und der eingeräumten Kompetenzen des „Überwachungsbeauftragten“ zur Sicherstellung der Umsetzung angeordneter Maßnahmen in der betroffenen Einrichtung ist nicht näher definiert. Der Begriff Sicherstellung sollte gestrichen und gemäß den Erläuterungen durch Beobachtung und fachliche Unterstützung bei der Maßnahmenumsetzung ersetzt werden. Insbesondere sollte dem Überwachungsbeauftragten keine Kompetenz zum Eingriff

in unternehmerische Entscheidungen eingeräumt werden, ohne die entsprechenden Haftungen und Risiken für derartige Eingriffe von den Leitungsorganen auf diesen zu übertragen.

Zu Abs. 4:
Zu Z 2:
Die mediale „Zur-Schau-Stellung" von Leitungsorganen per Bescheid - gemäß § 41 ohne aufschiebende Wirkung - ist überschießend und grenzt an Rufschädigung, insbesondere, da im Fall einer Aufhebung gemäß Abs. 5 keine öffentlichkeitswirksame Kommunikation per Gesetz vorgeschrieben ist.

Dieser „Naming-and-Shaming"-Mechanismus ist in der NIS-2-Richtlinie nicht vorgegeben und deswegen unionsrechtlich nicht geboten.

Vor diesem Hintergrund kann es nicht nachvollzogen werden, weswegen hier ohne ersichtlichen Grund - es besteht kein Informationsinteresse der Öffentlichkeit darüber, dass bestimmten Leitungsorganen ein Tätigkeitsverbot auferlegt wurde - derart schwer in grundrechtlich gewährleistete Rechtspositionen (Art. 8 EMRK, Art. 11. ZP-EMRK, Art. 5 und 6 StGG) betroffener Leitungsorgane eingegriffen wird und warum gerade in diesem grundrechtssensiblen Bereich von der grundsätzlichen Vorgehensweise, Gold-Plating zu vermeiden, abgewichen wird.

Der Satz „Dieser Bescheid ist in einer allgemeinen Weise zu veröffentlichen, die geeignet erscheint, einen möglichst weiten Personenkreis zu erreichen." wäre daher ersatzlos zu streichen.

Zu Abs. 7:
Entscheidungen nach Abs. 4 sollten auch in den Abs. 7 aufgenommen werden.

Zu Z 1:
Die in lit. d normierte willentliche Behinderung von Prüfungen oder Überwachungstätigkeiten darf im Teilsektor Krankenhaus nie zu einer Strafe führen. Eine willentliche Behinderung im Sinne einer begründbaren Notwendigkeit zur Verschiebung von Prüfungs- oder Überwachungstätigkeiten zur Wahrung der Betriebs- und Patientensicherheit muss im Teilsektor Krankenhaus immer straffrei möglich sein.

Zu § 40 (Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung):

Diese Bestimmung wird aus mehreren Gründen als problematisch erachtet. Die Vorschreibung spezieller IKT-Produkte bzw. IKT-Dienste kann zu Schwierigkeiten bei der Implementierung in den Systemen der Einrichtungen führen, da aus der Bestimmung nicht hervorgeht, inwieweit eine Kompatibilität mit bestehenden Systemen gegeben sein muss. Ebenso geht aus dieser Bestimmung nicht hervor, inwieweit vergaberechtliche Vorschriften davon berührt sein könnten.

Diese Bestimmung wäre daher insofern anzupassen, als ein Zusatz aufzunehmen wäre, welcher besagt, dass die besonderen Gegebenheiten der Einrichtungen bei der Verpflichtung zur Verwendung von speziellen IKT-Produkten bzw. IKT-Diensten zu berücksichtigen sind.

Weiters muss die Wirtschaftlichkeit im Verhältnis zum Risiko berücksichtigt werden. Die Verwendung darf nicht zu einer unverhältnismäßigen Erhöhung eines Risikos führen und diese IKT-Lösungen sollten ausschließlich für diesen Verwendungszweck vorgesehen sein.

Zu § 41 (Verfahren vor dem Bundesverwaltungsgericht):

Rechtsmittel gegen Entscheidungen der Behörde gemäß § 39 Abs. 2 und insbesondere § 39 Abs. 4 Z 2 müssen aufgrund der Komplexität sowie der finanziellen und personellen Aufwände für Sicherheitsmaßnahmen gemäß § 32 immer eine aufschiebende Wirkung haben, sonst läge eine Unverhältnismäßigkeit vor, da der Automatismus überschießend ist.

Zu § 44 (Allgemeine Bedingungen für die Verhängung von Geldstrafen):

Die Strafbestimmungen der §§ 44 und 45 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.

Zu § 45 (Verwaltungsstrafbestimmungen):

Grundsätzlich ist festzuhalten, dass bereits Banalitäten zu Strafen von 7 bis 10 Millionen Euro gemäß § 45 Abs. 2 bis Abs. 3 führen können. Das erscheint als nicht verhältnismäßig, wenn dies beispielsweise auf folgende Verfehlungen zutrifft:

- § 45 Abs. 1 Z 10: Versäumnis der fristgerechten Meldung von Prüfungsplänen an die Behörde
- § 45 Abs. 1 Z 13: Versäumnis der Bekanntgabe von Abschlüssen sowie Rücktritten von Vereinbarungen zum Informationsaustausch gemäß § 36 Abs. 4
- § 45 Abs. 1 Z 7: Versäumnis der fristgerechten Übermittlung der Selbstdeklaration
- § 45 Abs. 1 Z 3: Fehlende Erreichbarkeit über die bekanntgegebenen Kontaktdaten
- § 45 Abs. 1 Z 14, 18,20: Behinderung von Prüfungshandlungen ohne Berücksichtigung einer begründbaren Notwendigkeit (aus Sicht der Patienten- und Betriebssicherheit)
- § 45 Abs. 1 Z 6: Nicht-Nachweisbarkeit der Maßnahmenumsetzung (Eine teilweise Nachweisbarkeit umfasst ebenfalls eine nicht vollständige Nachweisbarkeit und wäre somit der Nicht-Nachweisbarkeit zuzuordnen.)

Zu Abs. 1:
Die hier vorgesehenen Verwaltungsstrafbestimmungen, insb. Z 4, Z 5, Z 10 und Z 12, sollten generell auf ihre Verhältnismäßigkeit hin überprüft und gegebenenfalls nach Abs. 4 verschoben werden.

Zu Abs. 4:
Aus § 44 Abs. 4 ergibt sich augenscheinlich, dass Geldstrafen auch gegen verantwortliche Beauftragte und damit natürliche Personen verhängt werden können. Die einzigen Strafrahmen, die umfassend für Verstöße gegen Pflichten dieses Bundesgesetzes vorgesehen sind, sind die in § 45 Abs. 2 und 3 genannten Beträge von bis zu 7 und 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-Richtlinie nicht geboten, weil diese die Verhängung von Geldbußen nur gegen wesentliche und wichtige Einrichtungen und damit gegen die Unternehmen selbst vorsieht; sie legt damit offensichtlich ein unternehmensbezogenes Konzept der Geldbuße zugrunde. Hier wäre bei den Strafrahmen - wie im Gesetzesentwurf zum deutschen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz- entsprechend zu differenzieren, sodass die Millionen-Strafrahmen gegen natürliche Personen nicht zur Anwendung gelangen.

Es wird daher angeregt, für die Verhängung von Geldstrafen gegen natürliche Personen in den §§ 44 und 45 abweichende Strafrahmen mit deutlich niedrigeren Strafdrohungen vorzusehen oder, da eine Strafbarkeit natürlicher Personen unionsrechtlich ohnedies nicht geboten ist, eine Strafbarkeit nur für juristische Personen vorzusehen.

Zu Abs. 5 (sowie § 46 Abs. 2):
§ 45 Abs. 5 sieht vor, dass die Bestimmung keine Anwendung auf Behörden und sonstige Stellen der öffentlichen Verwaltung, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, findet.

Aus Sicht des Landes Wien werden damit nicht nur Behörden, sondern alle Stellen der öffentlichen Verwaltung, unabhängig davon, ob diese im Rahmen der Hoheitsverwaltung oder der Privatwirtschaftsverwaltung tätig werden, einschließlich ihrer Organe und Organwalter, als auch die Gebietskörperschaften selbst von der Strafbarkeit des § 45 ausgenommen. Diese Auslegung korrespondiert auch mit den Erläuterungen zur genannten Bestimmung.

Aus Gründen der Rechtssicherheit sowie im Hinblick auf eine einheitliche Vollziehung wird jedoch angeregt, dies in § 45 Abs. 5 noch klarer zum Ausdruck zu bringen.

Es wird daher folgender Formulierungsvorschlag erstattet:
„Auf Einrichtungen, Behörden, Organe und sonstige Stellen der öffentlichen Verwaltung, unabhängig davon, ob sie hoheitlich oder im Rahmen der Privatwirtschaftsverwaltung eingerichtet oder tätig sind, sowie gegen ihre Organwalter, findet diese Bestimmung keine Anwendung."

Zu § 51 (Inkrafttretens-, Außerkrafttretens- und Übergangsbestimmungen):

Es sind keine Übergangfristen für die Erfüllung gesetzlicher Vorgaben vorgesehen. Mit Inkrafttreten des Gesetzes müssten sämtliche Leitungsorgane bereits geschult sein (§ 31 Abs. 3) und alle nicht öffentlich bekannt gegebenen, detailliert ausformulierten Sicherheitsmaßnahmen gemäß Anlage 3 umgesetzt sein. Das erscheint weder aus operativer Sicht unter Berücksichtigung der verfügbaren personellen und finanziellen Ressourcen noch unter Einhaltung geltender Gesetze für öffentliche Auftraggeber (Bundesvergabegesetz 2018) möglich. Daher wären Übergangsfristen für die Umsetzung von Pflichten für wesentliche und wichtige Einrichtungen vorzusehen.

Zu Abs. 7:
In Abs. 7 findet sich eine Spezialbestimmung für Betreiber wesentlicher Dienste gemäß § 16 Abs. 1 NISG. Demnach wird für diese die dreijährige Frist des § 33 Abs. 2 erster Satz reduziert, da sie ab dem Zeitpunkt des letzten Nachweises zu berechnen ist, welcher auf jeden Fall vor Inkrafttreten dieses Gesetzes liegt. Die generelle dreijährige Frist verkürzt sich somit für alle Betreiber wesentlicher

Dienste. Je nachdem, wann der letzte Nachweis übermittelt wurde, kommt es zu unterschiedlichen Umsetzungsfristen, was dem Gleichheitsgrundsatz widerspricht.

Konkret durchzuführende Maßnahmen werden sich erst aus einer noch zu erlassenden Verordnung ergeben. Es ist daher noch nicht abschätzbar, welche Unterlagen bis zum Ablauf der Frist vorzulegen sein werden. Aus derzeitiger Sicht ist anzunehmen, dass zukünftig noch mehr Maßnahmen zu ergreifen sind und sich der zu leistende Aufwand noch weiter erhöht als nach dem derzeitigen gesetzlichen Stand. Betreiber wesentlicher Dienste müssen die bestehenden gesetzlichen Bestimmungen bereits erfüllen. Unabhängig davon ist es hier erforderlich, dass auch ihnen ausreichend Zeit zur Umsetzung zur Verfügung steht. Dieser Zeitraum wäre entsprechend eines realistischen Umsetzungszeitraumes für die Betriebe zu wählen.

Insgesamt werden durch diese Spezialbestimmungen Betreiber wesentlicher Dienste sachlich nicht gerechtfertigt benachteiligt. § 51 Abs. 7 sollte daher entfallen.

Für den Landesamtsdirektor:

OMR^{in} Mag.^{a} Eva Tiefenbrunner

Mag.^{a} Birgit Eisler
Obermagistratsrätin

Ergeht an:
1. Präsidium des Nationalrates
2. alle Ämter der Landesregierungen
3. Verbindungsstelle der Bundesländer
4. MA 63
   (zu MA 63 - 51800-2024)
   mit dem Ersuchen um Weiterleitung
   an die einbezogenen Dienststellen
5. MA 53
   zur Veröffentlichung auf der
   Stadt Wien-Website

Stadt Wien

Dieses Dokument wurde amtssigniert.

Information zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.wien.gv.at/amtssignatur