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

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

30. April 2024

STELLUNGNAHME DER ISPA ZUR ÖFFENTLICHEN KONSULTATION ZUM ENTWURF EINES BUNDESGESETZES MIT DEM EIN NETZ- UND INFORMATIONSSYSTEMSICHERHEITSGESETZ 2024 (NISG 2024) ERLASSEN UND DAS TELEKOMMUNIKATIONSGESETZ 2021 UND DAS GESUNDHEITSELEMATIKGESETZ 2012 GEÄNDERT WERDEN

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, im Rahmen der öffentlichen Konsultation des Entwurfs eines Bundesgesetzes, mit dem ein Netz- und Informationssystemsicherheitsgesetz 2024 (NISG 2024) erlassen und das Telekommunikationsgesetz 2021 und das Gesundheitselematikgesetz 2012 geändert werden, wie folgt Stellung zu nehmen:

Die ISPA begrüßt die Absicht mit diesem Bundesgesetz ein hohes Cybersicherheitsniveau von Netz- und Informationssystemen zu gewährleisten. Dabei sollte allerdings stets darauf Bedacht genommen werden, die daraus resultierenden Pflichten auf das absolut erforderliche Maß zu beschränken und die Anbieter in einem ohnehin stark regulierten Sektor nicht noch mehr als unbedingt notwendig zu belasten.

Konkret hat die ISPA folgende Rückmeldungen:

Zu § 3 NISG 2024: Begriffsbestimmungen

Einige Begriffsbestimmungen aus Art 6 der NIS-2-RL[1] wurden nicht in das NISG 2024 übertragen. Insbesondere fehlt die Definition eines Domainnamensystems (Art 6 Z 19 NIS-2-RL). Lediglich ein DNS-Anbieter wird in § 3 Z 12 NISG 2024 definiert. Aus der Definition eines DNS-Anbieters geht jedoch

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

nicht hervor, was „DNS“ bedeutet und in weiterer Folge auch nicht wie ein Domainnamensystem legaldefiniert wird. Daher sollte die Definition des Domainnamensystem („DNS“) von der NIS-2-RL in das NISG 2024 übertragen werden.

Weiters hat die ISPA eine Verstreuung der Legaldefinitionen auf die Begriffsbestimmungen, auf andere Stellen bzw. die Anlagen des NISG 2024 festgestellt. Beispielhaft genannt werden können § 24 Abs 3 - Abs 5, § 35 Abs 1 NISG 2024 und die in den Anlagen und 1 und 2 enthaltenen Definitionen. Es wird daher vorgeschlagen, die Definitionen in den Begriffsbestimmungen zu konzentrieren, um die Anwenderfreundlichkeit des Gesetzes zu verbessern.

In den Erläuternden Bemerkungen (EB) wird zur Definition des Leitungsorganes § 3 Z 11 NISG 2024 ausgeführt:

> *„Folglich etabliert die Position eines „Chief Information Security Officer (CISO)“ für sich genommen noch kein Leitungsorgan. Es ist jedoch denkbar, dass jene Person, die die Rolle des CISO in einem Unternehmen einnimmt, auch nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte oder zur Überwachung der Geschäftsführung berufen ist“*

Im Hinblick auf die ausgeführte erläuternde Bemerkung bleibt nach Ansicht der ISPA unklar, ob die Berufung einer Person (beispielsweise eines CISOs) zur Führung der Geschäfte bzw. zur Überwachung der Geschäftsführung ein zusätzliches Leitungsorgan etabliert oder ein solches ersetzt. Weiters unklar bleibt, ob bzw. wie sich Beschränkungen im Innenverhältnis auf die Definition eines Leitungsorganes auswirken. In den EB wird lediglich ausgeführt, dass nicht auf die Vertretung im Außenverhältnis abgestellt werden soll. Eine Konkretisierung in den EB wäre daher wünschenswert.

Abschließend wird angeregt, die in den EB enthaltene Definitionen zur Niederlassung bzw. Hauptniederlassung (vgl EB zu § 28) in die Begriffsbestimmungen des NISG 2024 aufzunehmen.

Zu § 29 NISG 2024: Register der Einrichtungen

Durch diese Norm werden offenbar zwei Bestimmungen der NIS-2-RL national umgesetzt. Einerseits Art 3 Abs 3 NIS-2-RL, die Verpflichtung der Mitgliedsstaaten eine Liste der wichtigen und wesentlichen Einrichtungen zu erstellen und andererseits Art 27 NIS-2-RL, die verpflichtende Weitergabe von Angaben, damit die ENISA ein Register erstellen und führen kann. Letztere Bestimmung betrifft jedoch nicht alle wichtigen und wesentlichen Einrichtungen, sondern nur folgende Dienste: DNS-

Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdienste, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter digitaler Dienste.

Es gibt jedoch einen wesentlichen Unterschied zwischen den beiden Bestimmungen. Die in Art 3 Abs 3 NIS-2-RL vorgesehene Umsetzungsfrist beträgt drei und die in Art 27 NIS-2-RL sechs Monate. Daher wird seitens der ISPA angeregt, die Registrierungspflicht für alle nicht in Art 27 Abs 1 NIS-2-RL genannten Dienste auf 6 Monate zu erweitern.

In § 29 Abs 5 NISG 2024 wird der Bundesminister für Inneres zur Erlassung einer Durchführungsverordnung ermächtigt. In diesem Zusammenhang wird angeregt, dass durch die Durchführungsverordnung klargestellt wird, dass bei der Registrierungspflicht Mehrfachmeldungen bei der Angabe von Sektoren bzw. Teilsektoren möglich sind und daher keine mehrfachen Registrierungen nötig sind, nur weil eine Einrichtung in mehreren Sektoren bzw. Teilsektoren tätig ist.

Zu § 32 NISG 2024: Risikomanagementmaßnahmen

Insbesondere vor dem Hintergrund des konsistenten Schwerpunktes des NIS-2-RL, Maßnahmen zu erlassen bzw. Maßnahmen zu ergreifen, die auf einem risikobasierten Ansatz beruhen, sollte im § 32 NISG 2024 eine ausdrückliche Klarstellung erfolgen, dass eine Einrichtung im Rahmen der Risikobewertung, zu dem Schluss kommen kann, dass keine Risikomanagementmaßnahmen erforderlich sind.

Zu § 33 NISG 2024: Nachweis der Wirksamkeit der Risikomanagementmaßnahmen

Um die ordnungsgemäße Übermittlung der Selbstdeklaration zu fördern bzw. zu gewährleisten, wird seitens der ISPA angeregt, den Einrichtungen für die Selbstdeklaration bzw. für die Meldepflicht einer angedachten Prüfung, Leitfäden nach dem Vorbild des „NIS-Factsheets“ zur Verfügung zu stellen.

In § 33 Abs 3 NISG 2024 wird die Möglichkeit normiert, dass die Cybersicherheitsbehörde bei begründeten Hinweisen, insbesondere einer Selbstdeklaration, oder sonstigen begründeten Hinweisen und Informationen, die nahelegen, dass die Einrichtung ihren Pflichten nach § 32 und § 34 NISG 2024 nicht nachkommt, auftragen kann, die Umsetzung der Risikomanagementmaßnahmen gemäß § 32 NISG 2024 mittels einer Prüfung durch eine unabhängige Stelle nachzuweisen.

Unverständlich ist, weshalb ein Verstoß gegen die Berichtspflichten nach § 34 NISG 2024 (bzw. bereits der begründete Verdacht eines Verstoßes von § 34 NISG 2024) eine Prüfung der Risikomanagementmaßnahmen gemäß § 32 NISG 2024 mittels Prüfung durch eine unabhängige Stelle nach sich ziehen soll. Gemeint sein könnte der Verstoß gegen § 34 Abs 3 NISG 2024, welcher die Verpflichtung der Festlegung eines internen Verfahrens vorsieht, welche wiederrum eine Risikomanagementmaßnahme (Umgang mit Cybersicherheitsvorfällen) darstellt. Sollte in § 33 Abs 3 NISG 2024 ein Verstoß gegen § 34 Abs 3 NISG 2024 (und nicht § 34 NISG 2024) gemeint sein, wäre eine Ergänzung um „Abs 3" erforderlich bzw. die Nennung des § 34 (Abs 3) NISG 2024 an dieser Stelle obsolet, da ein solcher Verstoß gegen § 34 Abs 3 NISG 2024 gleichfalls einen Verstoß gegen § 32 NISG 2024 iVm mit den damit zu erlassenden Risikomanagementmaßnahmen darstellt.

Wünschenswert wäre auch eine Konkretisierung und Angabe von Beispielen (in den EB) betreffend die Formulierung „*begründeten Hinweisen, insbesondere einer Selbstdeklaration, oder sonstigen begründeten Hinweisen und Informationen, die nahelegen, dass die Einrichtung ihren Pflichten nach §§ 32 und 34 nicht nachkommt*".

Weiters wird nicht ausdrücklich festgelegt, in welcher Form eine „Aufforderung" seitens der Cybersicherheitsbehörde gemäß § 33 Abs 3 NISG 2024 zu erfolgen hat. Daher wird um Klarstellung im § 33 Abs 3 NISG 2024 (durch Verweis auf § 39 NISG 2024) ersucht, dass diese Aufforderung mittels Verfahrensanordnung bzw. in Bescheidform ergeht, sodass der wirksame Rechtsschutz der betroffenen Einrichtung gewährleistet wird.

In § 33 Abs 6 NISG 2024 wird der Bundesminister für Inneres zur Erlassung einer Durchführungsverordnung für Inhalte, Format, Struktur udgl in Bezug auf die Selbstdeklaration, den Prüfungsbericht und der Mitteilung über eine geplante Prüfung, ermächtigt. Keine Durchführungsverordnungsermächtigung besteht im Zusammenhang mit der näheren Regelung der Kosten der Prüfungen durch die unabhängigen Stellen bzw. Prüfer. Die derzeitige Formulierung des § 33 Abs 2 – Abs 4, worin die verpflichtende Prüfung mittels unabhängiger Stelle bzw. Prüfer vorgesehen wird, lässt offen, wie umfangreich die Prüfung sein wird. Insbesondere werden keine Abstufungen nach der Unternehmensgröße und keine Begrenzung des Prüfungszeitraumes normiert. Daher ist es für die betroffenen Einrichtungen nicht möglich, den im Zusammenhang mit den verpflichtenden Prüfungen anstehenden finanziellen sowie personellen Aufwand einzuschätzen. Im Sinne der Vorhersehbarkeit und Rechtssicherheit dieser Verpflichtung fordert die ISPA, dass die Durchführungsverordnungsermächtigung auf die Regelung der (mittelbaren und unmittelbaren) Kosten

erweitert wird und in weiterer Folge Tageshöchstsätze und die Begrenzung der Audittage (nach dem Vorbild der ISO27001) festgelegt werden, um einerseits die finanziellen, zeitlichen sowie personellen Ressourcen für die Einrichtungen vorhersehbar zu machen.

Weiters wird angeregt, hinsichtlich der in § 33 Abs 4 NISG 2024 genannten Möglichkeit, dass die Cybersicherheitsbehörde amtswegig in hinreichend begründeten Fällen eine anderslautende Entscheidung in Bezug auf die Kostentragung treffen kann, Anwendungsfälle zu konkretisieren bzw. Beispiele zu benennen.

Zu § 34 NISG 2024: Berichtspflichten

Im Zusammenhang mit § 34 Abs 2 NISG 2024 wird angeregt, den notwendigen (Mindest-)Inhalt, der Frühwarnung, der Meldung, des Zwischenberichtes sowie des Abschlussberichtes, zu konkretisieren. Weiters wird eine Ergänzung dahingehend angeregt, wie bei Nicht-Feststellbarkeit des vorgeschriebenen Inhaltes die Berichtspflicht erfüllt werden kann. Beispielsweise könnte man den Gesetzestext dahingehend ergänzen, dass bei Einhaltung der gebotenen Sorgfalt der Inhalt nicht eruiert werden kann, der Berichtspflicht gemäß § 34 NISG 2024 auch dadurch nachgekommen wird, wenn die Einrichtung dem zuständigen CSIRT die verfügbaren Informationen mitgeteilt werden. Abschließend wird angeregt, dass den Einrichtungen für die Meldung von erheblichen Cybersicherheitsvorfällen ein Formular inklusive Anwendungsleitfaden zur Verfügung gestellt werden.

In § 34 Abs 3 NISG 2024 wird normiert, dass soweit ein Cybersicherheitsvorfall auch die Erbringung des jeweiligen Dienstes beeinträchtigt, die Empfänger des Dienstes unverzüglich über diesen sowie über Abhilfemaßnahmen zu informieren sind. In diesem Zusammenhang wird um Klarstellung ersucht, dass eine solche Information an Empfänger auch rechtmäßig ist, wenn die Empfänger der Verarbeitung ihrer Daten nicht eingewilligt haben.

In § 34 Abs 6 NISG 2024 wird Art 23 Abs 7 der NIS-2-RL umgesetzt:

Art 23 Abs 7 NIS-2-RL lautet:

> *„Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder einen laufenden erheblichen Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das CSIRT eines Mitgliedstaats oder gegebenenfalls seine zuständige Behörde sowie*

gegebenenfalls die CSIRTs oder die zuständigen Behörden anderer betreffender Mitgliedstaaten nach Konsultation der betreffenden Einrichtung die Öffentlichkeit über den erheblichen Sicherheitsvorfall informieren oder die Einrichtung auffordern, dies zu tun.“

§ 34 Abs 6 NISG 2024 lautet:

„Nach Anhörung der von einem Cybersicherheitsvorfall betroffenen Einrichtungen kann die Cybersicherheitsbehörde ***personenbezogene Daten*** *gemäß §§ 42 und 43 nach erfolgter Interessenabwägung bezüglich der Auswirkungen auf die Betroffenen veröffentlichen, um die Öffentlichkeit über Cybersicherheitsvorfälle zu unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung oder zur Bewältigung von Cybersicherheitsvorfällen erforderlich ist, oder die Offenlegung des Cybersicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.“*

Die Veröffentlichung von personenbezogenen Daten zur Information der Öffentlichkeit über einen Sicherheitsvorfall ist in der NIS-2-RL nicht vorgesehen. Die ISPA hegt daher Bedenken hinsichtlich der Notwendigkeit der Veröffentlichung von personenbezogenen Daten und falls dies bejaht wird, ob ausreichende Maßnahmen zum Schutz der personenbezogen Daten getroffen worden sind.

Die erwähnte Gesetzesstelle knüpft die Veröffentlichung weder an besondere Anforderungen oder weitere Bedingungen, um eine Veröffentlichung von personenbezogenen Daten einerseits als notwendig einstufen, andererseits als rechtmäßig qualifizieren zu können. Wenngleich in den EB erwähnt ist, dass bei der vorzunehmenden Interessensabwägung auf den Verhältnismäßigkeitsgrundsatz gemäß § 1 Abs 2 DSG und auf den Grundsatz der Datenminimierung gemäß Art 5 Abs 1 Buchstabe c DSGVO[2] Bedacht zu nehmen ist, scheint diese Erwähnung in den EB nicht ausreichend zu sein, um einen entsprechenden Datenschutz nach DSGVO und DSG zu gewährleisten.

Betreffend die Rechtmäßigkeit der Verarbeitung ist idF Art 6 lit c DSGVO maßgeblich. Die Verarbeitung von personenbezogenen Daten ist demnach rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung, die der Verantwortliche unterliegt, erforderlich ist. Betreffend die Anforderungen an eine Rechtsgrundlage wird im ErwG 41 der DSGVO näher ausgeführt, dass eine Rechtsgrundlage, die zur

[2] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Verarbeitung von personenbezogenen Daten verpflichtet (oder ermächtigt) klar und präzise sein und ihre Anwendung für die Rechtsunterworfenen vorhersehbar sein sollte. § 34 Abs 6 NISG 2024 entspricht weder den Anforderungen an die Vorhersehbarkeit der Rechtsgrundlage nach ErwG 41 DSGVO noch lässt sich den EB entnehmen, dass eine allgemeine Datenschutz-Folgeabschätzung gem. 35 Abs 10 DSGVO betreffend die Erlassung einer derartigen Gesetzesgrundlage zur Veröffentlichung von personenbezogenen Daten erfolgt ist.

Nach Ansicht der ISPA ist die geschaffene Rechtsgrundlage gemäß § 34 Abs 6 NIISG 2024, wonach die Veröffentlichung von personenbezogenen Daten ermöglicht wird, daher überschießend.

Zu § 35 NISG 2024: Erheblicher Sicherheitsvorfall

In § 35 Abs 3 NISG 2024 wird der Bundesminister für Inneres zur Erlassung einer Durchführungsverordnung für die Festlegung weiterer Kriterien und näherer Regelungen für das Vorliegen eines erheblichen Cybersicherheitsvorfalles, ermächtigt. Im Sinne der Vorhersehbarkeit und Rechtssicherheit, sollte diese Durchführungsverordnung ehestbald erlassen und sollten die in der Durchführungsverordnung enthaltenen Inhalte klar und eindeutig determiniert werden (nach dem Vorbild des § 3 Abs 2 TK-NSiV 2020[3]).

Zu § 38 NISG 2024: Aufsichtsmaßnahmen

Im Zusammenhang mit den der Cybersicherheitsbehörde zugewiesenen Aufsichtsmaßnahmen wird angeregt, dass die Form der zu ergreifenden Maßnahmen ausdrücklich im § 38 NISG 2024 festgelegt wird, um die Rechtssicherheit sowie den Rechtsschutz der Einrichtungen zu gewährleisten. Es wird daher angeregt an dieser Stelle auf § 39 Abs 1 und Abs 2 NISG 2024 zu verweisen.

Unter welchen konkreten Voraussetzungen bzw in welchem Umfang die Aufsichtsmaßnahmen gemäß § 38 NISG 2024 seitens der Cybersicherheitsbehörde erfolgen können, wird nicht normiert. Lediglich in den EB zum § 38 NISG 2024 wird ausgeführt, dass die Cybersicherheitsbehörde durch diese Norm, Befugnisse erhält, um die Aufsicht der Einhaltung der sich aus dem NISG 2024 ergebenden Verpflichtungen möglichst effektiv und ohne unverhältnismäßige Eingriffe zu tätigen. Ein Verweis auf die Verhältnismäßigkeit der Maßnahmen findet sich im Gesetz nicht.

[3] Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste im Zusammenhang mit Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen – Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020)

Aufgrund des dem der Cybersicherheitsbehörde eingeräumten (beträchtlichen) Ermessenspielraumes ist das Vorsehen expliziter Bedingungen, die Festlegung des Umfanges, die Durchführung einer verpflichtenden Interessensabwägung vor einer geplanten Aufsichtsmaßnahme sowie ein expliziter Bezug auf die Verhältnismäßigkeit der Aufsichtsmaßnahmen in § 38 NISG 2024 nach Ansicht der ISPA unerlässlich. Vergleichsweise ist hinsichtlich der in § 39 NISG 2024 der Cybersicherheitsbehörde eingeräumten Durchsetzungsmaßnahmen zumindest die gebührende Berücksichtigung der Umstände im Einzelfall in § 39 Abs 7 NISG 2024 vorgesehen.

Beispielsweise ist die in § 38 Abs 1 Z 1 NISG 2024 normierte Aufsichtsmaßnahme, wonach die Cybersicherheitsbehörde befugt ist, vor Ort in Netz- und Informationssicherheitssysteme und Unterlagen sowie mittels Fernzugriff unter Mitwirkung der betroffenen Einrichtung oder durch Begleitung der Prüfungen von unabhängigen Stellen, jeweils nach vorangegangener Verständigung der Einrichtung Einschau zu nehmen, hinsichtlich ihres Umfanges unklar. Die Verständigung der Einrichtung ist nach Ansicht der ISPA jedenfalls unzureichend, um die mit dieser Aufsichtsmaßnahme einhergehenden Verpflichtung der Eingriff als verhältnismäßig zu qualifizieren.

Bezüglich der in § 38 Abs 1 Z 2 NISG 2024 normierten Aufsichtsmaßnahme, wonach die Cybersicherheitsbehörde befugt ist, bei einer Einrichtung Sicherheitsscans durchzuführen, fordert die ISPA die Klarstellung, dass eingerichtete Sicherheitsmaßnahmen (wie beispielsweise Firewalls) keine Be- oder Verhinderung der Durchführung der Kontrolle im Sinne des § 45 Abs 1 Z 14 NISG 2024 darstellen.

Weiters bleibt unklar, unter welchen Voraussetzungen (in den EB erfolgt lediglich eine Aufzählung von Beispielen) eine Ad-Hoc-Prüfung gemäß § 38 Abs 1 Z 5 NISG 2024, wer diese durchzuführen und wer die Kosten für eine solche zu tragen hat. Daher wird seitens der ISPA, Klarstellung gefordert, unter welchen Voraussetzungen, in welchem Umfang und ob AD-Hoc-Prüfungen durch eine unabhängige Stelle oder die Cybersicherheitsbehörde durchgeführt werden sollen. Weiters sollen die Kosten von Ad-Hoc-Prüfungen nach Ansicht der ISPA aus dem Bundesbudget beglichen werden.

Zu § 39 NISG 2024: Durchsetzungsmaßnahmen

Betreffend Allgemeine Aspekte der Aufsicht und Durchsetzung ist in Art 31 Abs 1 NIS-2-RL Folgendes festgelegt:

„Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden die Einhaltung der Verpflichtungen aus dieser Richtlinie wirksam beaufsichtigen und die erforderlichen Maßnahmen treffen."

Grundsätzlich ist die Cybersicherheitsbehörde nach § 39 Abs 1 und Abs 2 NISG 2024 befugt, bei Verstößen gegen das NISG 2024 den Einrichtungen mit Verfahrensanordnung bzw. mit Bescheid eine Maßnahme aufzutragen. Das Nichtbefolgen eines Bescheides gemäß § 39 Abs 2 NISG 2024 stellt eine Verwaltungsstrafe gemäß § 45 Abs 1 Z 19 NISG 2024 dar und kann daher mit den in § 45 Abs 2 und 3 NISG 2024 vorgesehenen Geldstrafen geahndet werden.

Die in § 39 Abs 3 und Abs 4 NISG 2024 der Cybersicherheitsbehörde zugewiesenen Durchsetzungsmöglichkeiten werden als zusätzliche Möglichkeiten („*Zudem ist die Cybersicherheitsbehörde befugt*…") der Durchsetzung nach § 39 Abs 1 und Abs 2 NISG 2024 normiert.

Unter welchen konkreten Voraussetzungen die Durchsetzungsmaßnahmen gemäß § 39 Abs 3 und Abs 4 NISG 2024 seitens der Cybersicherheitsbehörde erfolgen können, wird nicht normiert. Lediglich die gebührende Berücksichtigung der Umstände im Einzelfall wird in § 39 Abs 7 NISG 2024 vorgesehen und eröffnet der Cybersicherheitsbehörde daher einen beträchtlichen Ermessenspielraum. Vor diesem Hintergrund hegt die ISPA Bedenken hinsichtlich der in § 39 Abs 3 und Abs 4 NISG 2024 normierten Durchsetzungsmaßnahmen. Beispielsweise enthält die in § 39 Abs 3 Z 2 NISG 2024 normierte Durchsetzungsmaßnahme, die Befugnis der Cybersicherheitsbehörde einen betrauten Überwachungsbeauftragen zur Überwachung der Einrichtung zu benennen, jedoch werden keine konkreten Anwendungsfälle bzw. Bedingungen für diese zusätzliche Befugnis normiert.

Gemäß § 39 Abs 4 Z 1 NISG 2024 ist die Cybersicherheitsbehörde weiters befugt, die zuständige Behörde zu ersuchen, die Zertifizierung oder Genehmigung für einen Teil oder alle der Einrichtung erbrachten einschlägigen Dienste oder Tätigkeiten auszusetzen oder die nationale Behörde für die Cybersicherheitszertifizierung zu ersuchen, die Zertifizierung oder Genehmigung auszusetzen. Weiters ist die Cybersicherheitsbehörde gemäß § 39 Abs 4 Z 2 NISG 2024 befugt, Leitungsorganen (einschließlich ihrer rechtlichen Vertreter) einer wesentlichen Einrichtung zu untersagen Leitungsaufgaben wahrzunehmen. Auch betreffend diese beiden Bestimmungen fehlen im Entwurf des Gesetzestextes konkrete Anwendungsfälle, in welchen diese Maßnahmen möglich sein soll.

Daher wird seitens der ISPA gefordert, die in § 39 Abs 3 und Abs 4 NISG 2024 genannten Durchsetzungsmaßnahmen an explizite Voraussetzungen zu knüpfen und somit diese auf das

unbedingt erforderliche Maß zu beschränken, um für die betroffenen Einrichtungen Rechtssicherheit und Vorhersehbarkeit der möglichen Durchsetzungsmaßnahmen zu gewährleisten.

Zu § 40 NISG 2024: Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung

Die Cybersicherheitsbehörde wird in § 40 NISG 2024 ermächtigt, wesentliche und wichtige Einrichtungen zur Verwendung von speziellen IKT-Produkten, -Diensten und -Prozessen (die eine Cybersicherheitszertifizierung, gemäß Art. 49 der Verordnung (EU) 2019/881 angenommen und zertifiziert sind) verpflichten zu können, um die Erfüllung bestimmter in § 32 NISG 2024 genannter Anforderungen nachweisen zu können.

§ 40 NISG 2024 setzt Art 24 der NIS-2-RL um. Art 24 NIS-2-RL sieht jedoch nicht die verpflichtende, sondern lediglich die mögliche nationale Umsetzung vor („die Mitgliedstaaten können …"). Weiters wird die Kommission laut Art 24 Abs 2 NIS-2-RL - für den Fall, dass ein unzureichendes Niveau der Cybersicherheit festgestellt wurde - ermächtigt, delegierte Rechtsakte iZm mit der Verpflichtung wesentlicher und wichtiger Einrichtungen bestimmte zertifizierte IKT-Produkte, -Dienste und -Prozesse zu nutzen, zu erlassen. Ein Umkehrschluss daraus ergibt, dass solche Maßnahmen nur erlassen werden sollen, wenn ein angemessenes Cybersicherheitsniveau nicht anders erreicht werden kann. Des Weiteren ist, um den tatsächlichen Bedarf einer solchen Verpflichtung zu gewährleisten, vorgesehen, dass ein delegierter Rechtsakt der Europäischen Kommission nur unter den strengen Anforderungen des Art 38 NIS-2-RL zu erlassen ist. Vor diesem Hintergrund ist nicht ersichtlich, woraus sich die Notwendigkeit der nationalen Umsetzung ergibt. Auch die EB enthalten über die Notwendigkeit einer solchen nationalen Regelung keine näheren Ausführungen.

Da eine solche verpflichtende Verwendung im Sinne des § 40 NISG 2024 im Bedarfsfall durch die Europäische Kommission erfolgen könnte, ist die nationale Umsetzung nach Ansicht der ISPA überschießend und fordert die ISPA daher die ersatzlose Streichung dieser Bestimmung. Sollte der nationale Gesetzgeber zum Schluss kommen, dass eine ersatzlose Streichung nicht möglich ist, wird gefordert, eine Ausnahme hinsichtlich der von wichtigen bzw. wesentlichen Einrichtungen entwickelten IKT-Produkten, -Diensten und -Prozessen in § 40 NISG 2024 vorzusehen. Andernfalls würde sich die Bestimmung des § 40 NISG 2024 innovationshemmend auf österreichische Unternehmen, die selbst die genannten IKT-Produkte, -Dienste und -Prozesse entwickeln, auswirken.

Zu § 45 NISG 2024

Insbesondere vor dem Hintergrund, dass das NISG 2024 im Gegensatz zum bisherigen NISG viel mehr Unternehmen und weiters einen sehr hohen Anteil von KMUs (und hier auch sehr viele kleine Unternehmen) umfasst, wird seitens der ISPA angeregt den Grundsatz „Beraten statt Strafen“ iSd. § 33a VStG[4] verstärkt anzuwenden. Insbesondere sollen umsetzungswillige Einrichtungen bei der ordnungsgemäßen Umsetzung der NISG 2024 unterstützt und beraten werden, um ein aktuelles rechtswidriges Verhalten abzustellen und künftige Verwaltungsübertretungen zu vermeiden.

Zu § 51 Abs 7 NISG 2024: Inkrafttretens-, Außerkrafttretens- und Übergangsbestimmungen

In den Inkrafttretens-, Außerkrafttretens- und Übergangsbestimmungen wird normiert, dass für Betreiber wesentlicher Dienste gemäß § 16 Abs. 1 NISG in der Fassung BGBl. I Nr. 111/2018, die auch als wesentliche Einrichtungen gemäß § 24 Abs. 1 gelten, die dreijährige Frist des § 33 Abs. 2 erster Satz für den erstmaligen Nachweis der Anforderungen des § 32 nicht ab der Aufforderung zur Selbstdeklaration, sondern ab dem Zeitpunkt des letzten Nachweises gemäß § 17 Abs. 3 NISG in der Fassung BGBl. I Nr. 111/2018, beginnt. Der Nachweis nach § § 17 Abs. 3 NISG in der Fassung BGBl. I Nr. 111/2018 betrifft im Gegensatz zum Nachweis nach § 33 NISG 2024 einzelne Dienste und nicht die gesamte Einrichtung. Nach Ansicht der ISPA führt diese Bestimmung zu einer sachlich nicht gerechtfertigten Benachteiligung, weshalb die dreijährige Frist einheitlich ab Aufforderung zur Selbstdeklaration beginnen und dieser Absatz ersatzlos gestrichen werden sollte.

Zur Änderung des § 44 TKG 2021:

Die Regulierungsbehörde wird ermächtigt, mit Verordnung nähere Bestimmungen über technische und organisatorische Sicherheitsmaßnahmen festzulegen, sofern die Maßnahmen nach dem NISG 2024 nicht ausreichen, um die Aufrechterhaltung der Sicherheit der Netze und Dienste zu gewährleisten. Aufgrund des absehbaren Inkrafttretens des NISG 2024 ist aus Sicht der ISPA unklar, in welchem Verhältnis die Berichtspflichten iZm mit erheblichen Sicherheitsvorfällen nach dem NISG 2024 mit den derzeit bestehenden Berichtspflichten nach der Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020)[5] stehen. Sollten beide Regelungen nebeneinander bestehen bleiben, hätte dies zur Folge, dass die Einrichtungen mehrfache Meldeverpflichtungen treffen. Daher fordert die ISPA das Außerkrafttreten der TK-NSiV 2020.

[4] Verwaltungsstrafgesetz 1991 – VStG; BGBl. Nr. 52/1991 (WV) idF BGBl. I Nr. 194/1999 (DFB).
[5] vgl Fn 3.

Der Regulierungsbehörde wird weiters im Entwurf zu § 44 Abs 3 Z 2 TKG 2021 auch die Aufgabe übertragen, an der Erstellung eines Mustersicherheitskonzeptes für Betreiber gemäß 4 Z 25 TKG 2021 und Anbieter gemäß § 4 Z 36 TKG 2021 *mitzuwirken.* Aus dieser Formulierung ist nicht ersichtlich, wer das Mustersicherheitskonzept zu erstellen *hat*. Nach Ansicht der ISPA ist daher die Klarstellung erforderlich, dass ein solches Mustersicherheitskonzept zu erstellen ist und nicht nur an diesem mitgewirkt werden soll. Abschließend sollte an dieser Stelle des Gesetzes die Erstellung des Mustersicherheitskonzeptes an eine bestimmte Frist geknüpft werden, welche idealerweise vor dem Zeitpunkt der verpflichtenden Umsetzung der zu erlassenden Risikomanagementmaßnahmen liegt.

Einrichtung eines Single Point of Contact

Ein Single Point of Contact ist derzeit bei CERT.at eingerichtet. Aufgrund der positiven Erfahrungen mit der Zuweisung wäre es begrüßenswert, diesen Dienst auch nach Inkrafttreten des NISG 2024 bei CERT.at zu belassen. In diesem Zusammenhang wird ergänzend angeregt, zusätzlich einen Single Point of Contact speziell für die Telekommunikationsbranche einzurichten.

Sonstige Punkte

Um eine angemessene Vorbereitungszeit auf die zukünftigen Verpflichtungen der Einrichtungen sicherzustellen, regt die ISPA das ehestbaldige Erlassen der Durchführungsverordnungen an. Insbesondere im Zusammenhang mit der Umsetzung der in Anlage 3 zu regelnden Risikomanagementmaßnahmen benötigen die Einrichtungen einen angemessenen Zeitrahmen, um die Vielzahl an Risikomanagementmaßnahmen mit gebotener Sorgfalt umzusetzen.

Abschließend wird angeregt, Bestimmungen über Pflichten, die nach NISG 2024 Einrichtungen mit Konzernstrukturen treffen, dahingehend zu konkretisieren, ob Pflichten (beispielsweise §§ 29, 32, 33, 34 NISG 2024) unter bestimmten Voraussetzungen vom Mutter- bzw. Tochterunternehmen konsumiert werden können.

Wir möchten uns noch einmal für die Gelegenheit zur Stellungnahme bedanken. Für weitere Informationen oder Fragen können Sie uns gerne kontaktieren.

Mit freundlichen Grüßen,

ISPA Internet Service Providers Austria

Stefan Ebenberger
Generalsekretär

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.