Bundeskonferenz der Freien Berufe Österreichs

Karlsgasse 9, 1040 Wien
Tel.: 01 533 22 86
E-Mail: office@freie-berufe.at
Web: www.freie-berufe.at
ZVR: 40043635

Bundeskanzleramt
BKA – I/8 (Technologie- und Datenmanagement,
Cybersicherheit und Krisenrechenzentrum)
Ballhausplatz 2
1010 Wien
Per E-Mail: nis@bka.gv.at

Wien, am 30.4.2024

Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024; Telekommunikationsgesetz, Gesundheitstelematikgesetz, Änderung

Sehr geehrte Damen und Herren!

Die Bundeskonferenz der Freien Berufe Österreichs bedankt sich für die Zusendung und Möglichkeit der Begutachtung und übermittelt dazu folgende

STELLUNGNAHME

Der vorliegende Entwurf betrifft in direkter Anwendung bzw. nachgeordneten Einheiten die österreichische Wirtschaft und Verwaltung und somit auch die Interessen der Freien Berufe und deren Selbstverwaltungskörper und es wird um Überarbeitung hinsichtlich folgender Bereiche ersucht:

Nicht weisungsgebundene Selbstverwaltungskörper:
Als Bundeskonferenz der Freien Berufe gehen wir davon aus, dass unsere Freiberufskammern (Bund/Land) als nicht weisungsgebundene Selbstverwaltungskörper auch nicht von den Pflichten des Gesetzes erfasst werden. Hier wäre eine gesetzliche Klarstellung – ähnlich wie § 24 Abs 3 oder 6 – mit der Ergänzung: „sowie Selbstverwaltungskörper wie die Kammern der Freien Berufe Österreichs“ wünschenswert.

Unabhängigkeit der Behörde sowie eingeschränkte Einsichts- bzw. Kontrollrechte
Die neue Cybersicherheitsbehörde wird mit umfassenden Einsichts-, Eingriffs- und Kontrollrechten ausgestattet und muss als weisungsfreie Behörde aufgestellt werden. Hier ist klar zu definieren, dass alle Handlungen und Befugnisse nur innerhalb rechtsstaatlicher Gesetze bzw. Rahmen sowie im Zuge eines genau definierten Prüfplanes erfolgen dürfen. Die Einschau auf die Netz- und Informationssysteme hat hierbei nur in Form eines gemeinsamen „Audits“ mit der Einrichtung und nicht direkt bzw. eigenständig zu erfolgen. Jegliche Zugriffe auf Systeme und Daten, die im Besonderen nur den zuständigen (Strafverfolgungs-)Behörden mit genehmigten (richterlichen) Durchsuchungsbeschluss zustehen, dürfen nicht gestattet werden.

Als Freie Berufe unterliegen wir besonderen Verschwiegenheitspflichten und haben diese mit allen zur Verfügung stehenden Mitteln schon von Berufs wegen zu beschützen und zu wahren. Geschäfts- und Betriebsgeheimnisse (unternehmerische Aufzeichnungen sowie persönliche bzw. gesundheitsrelevante Kunden-Daten müssen bei behördlichen Einsichtnahmen ausgenommen werden.

Nicht noch mehr Bürokratieaufwand

Da der gegenwärtige Bürokratieaufwand bereits immens und geradezu toxisch für den Wirtschaftsstandort Österreich ist, darf mit dem vorliegenden Gesetzesvorhaben den Berufsständen bzw. der Wirtschaft insgesamt keine weitere Bürde aufgelastet werden. Der bürokratische Aufwand ist so niedrig als möglich zu halten. Demgemäß soll die Cybersicherheitsbehörde nicht zu einem Bürokratie-Moloch werden, sondern es sollte durch Übernahme von Aufgaben sowie Streichung überflüssiger bzw. paralleler Maßnahmen das gegenwärtige System in Anbetracht der DSGVO, DSG, usw. insgesamt verschlankt werden. Keinesfalls soll noch mehr an „Gold Plating" durch vermehrte Bürokratisierung erfolgen – derartige weitere bürokratische Belastungen kann sich der Wirtschaftsstandort Österreich schlichtweg nicht mehr leisten.

Wien, am 30.4.2024

Bundeskonferenz der Freien Berufe

BUKO-Präsident Dr. Daniel Alge
Präsident der Patentanwaltskammer

ÖSTERREICHISCHE APOTHEKERKAMMER

1090 Wien, Spitalgasse 31
T +43 1 404 14-100
F +43 1 408 84 40
E recht@apothekerkammer.at

LEG/NOV/2024/001
L/RK

Ansprechpartner:
Mag. Paul Lambauer / DW 141

An das
Bundeskanzleramt
Abteilung I/8
Ballhausplatz 2
1010 Wien

E-Mail: nis@bka.gv.at

Wien, 30. April 2024

Stellungnahme zum Netz- und Informationssystemsicherheitsgesetz 2024 - NISG 2024
GZ: 2024-0-220-735

Sehr geehrte Damen und Herren!

Die Österreichische Apothekerkammer nimmt zum Ministerialentwurf betreffend Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden, wie folgt Stellung:

Zur Einstufung als wesentliche oder wichtige Einrichtung (§ 24)

Gemäß § 24 Abs. 1 lit. d iVm Abs. 3 Z 1 und Abs. 4 gelten als wesentliche Einrichtungen iSd Gesetzes Einrichtungen im Sektor der öffentlichen Verwaltung, die **zum Zweck eingerichtet wurden, im öffentlichen Interesse liegende Aufgaben nicht gewerblicher Art zu erfüllen**, und die zudem zur Besorgung von Angelegenheiten der Bundesverwaltung berufen sind und entweder als Bundesbehörden eingerichtet wurden oder Rechtspersönlichkeit besitzen.

Gemäß § 1 Abs. 1 Apothekerkammergesetz 2001 ist die „Österreichische Apothekerkammer“ zur Vertretung der Apothekerschaft, der selbständigen und der angestellten Apotheker eingerichtet. Der Zweck ihrer Einrichtung besteht somit eindeutig in der Interessenvertretung und Selbstverwaltung des Berufsstandes der Apotheker:innen und **nicht in der Erfüllung im öffentlichen Interesse liegender Aufgaben**. Sie ist daher **schon dem klaren Gesetzeswortlaut nach nicht als wesentliche oder wichtige Einrichtung iSd § 24 einzustufen**.

Erst im Zuge der Verwaltungsreform wurde der Österreichischen Apothekerkammer die Zuständigkeit zur Erlassung von Bescheiden im übertragenen Wirkungsbereich übertragen. Dies stellt jedoch, wie bereits ausgeführt, eine zusätzliche Aufgabe und nicht den Zweck der Institution als solcher dar. Auch in ihren Auswirkungen bleibt die Tätigkeit der Österreichischen Apothekerkammer als Behörde der mittelbaren Bundesverwaltung weit hinter der jener Behörden zurück, die dem Anwendungsbereich des Gesetzes unterliegen:

So ist die Österreichische Apothekerkammer im übertragenen Wirkungsbereich gemäß § 2a Apothekerkammergesetz 2001 zwar zur Anerkennung von ausländischen Ausbildungsnachweisen zur Ausübung des Apothekerberufes befugt. Allerdings beschränkt sich ihre diesbezügliche Zuständigkeit auf einen **minimalen praktischen Anwendungsbereich**, nämlich im Durchschnitt 30 Anerkennungen ausländischer Berufsqualifikationen pro Jahr. Universitäten führen im Vergleich dazu ein Vielfaches an Nostrifizierungsverfahren durch, sind aber - aus gutem Grund - vom Anwendungsbereich des Gesetzes ausgenommen.

Ebenso wie die Hochschulen sind auch Gemeinden und Gemeindeverbände im aktuellen Entwurf vom Anwendungsbereich des Gesetzes ausgenommen. Die Österreichische Apothekerkammer erlässt zwar im übertragenen Wirkungsbereich Bescheide, diese entfalten aber Auswirkungen von begrenzter Relevanz, wie ein Vergleich deutlich erkennen lässt: So kommt die Zuständigkeit zur Erteilung von Konzessionen für **neu zu gründende** öffentliche Apotheken den Bezirksverwaltungsbehörden zu – die vom Anwendungsbereich des gegenständlichen Gesetzes ausgenommen sind. Nur wenn es um die Übertragung von Konzessionen, die Genehmigung von Gesellschafts- oder Pachtverträgen oder die Verlegung **bereits bestehender öffentlicher Apotheken** geht, ist die Österreichische Apothekerkammer zur Bescheiderlassung zuständig. Es versteht sich daher von selbst, dass die Auswirkungen der von der Österreichischen Apothekerkammer erlassenen Bescheide in ihrer Bedeutung für das öffentliche Gesundheitssystem weit hinter den von den Bezirksverwaltungsbehörden erlassenen Bescheiden zurückbleiben. Da die Bescheide der Österreichischen Apothekerkammer ausschließlich bereits existierende lokale Einrichtungen betreffen, wirken sie sich zudem nur auf lokaler Ebene aus.

Darüber hinaus sollen gemäß Art. 2 Abs. 2 lit. f. sublit. ii der Richtlinie (EU) 2022/2555 solche Einrichtungen der öffentlichen Verwaltung vom Anwendungsbereich der Richtlinie erfasst werden, „**die nach einer risikobasierten Bewertung Dienste erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnten.“**

Wollte man das Gesetz so interpretieren, dass die Österreichische Apothekerkammer seinem Anwendungsbereich unterläge, wäre dies in Hinblick auf den Regelungszweck und vor dem Hintergrund, dass Gemeinden und Gemeindeverbände sowie Einrichtungen des Universitäts-, Hochschul- und Schulwesens gänzlich vom Anwendungsbereich ausgenommen sind, **weder verhältnismäßig noch sachgerecht**.

Um derartige Fehlinterpretationen auszuschließen und Rechtssicherheit im Sinne einer verfassungskonformen Auslegung des Gesetzes zu schaffen, ersucht die Österreichische Apothekerkammer um eine unmissverständliche Klarstellung in § 24, wonach Selbstverwaltungskörper wie die Kammern der freien Berufe vom Anwendungsbereich ausgenommen sind.

Mit freundlichen Grüßen

HR Mag. iur. Rainer Prinz
(Kammeramtsdirektor)

ÖSTERREICHISCHE
ÄRZTEKAMMER
Körperschaft öffentlichen Rechts – Mitglied der World Medical Association

Bundeskanzleramt
Sektion I – Präsidium
Abteilung I/8 – Technologie- und Daten Management, Cybersicherheit und Krisenrechenzentrum
Herrengasse 23
1010 Wien

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

Ihr Zeichen	Ihre Nachricht vom	Unser Zeichen	Datum
2024-0.220.735	03.04.2024	Mag.AM	29.04.2024

Betrifft: Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden; Begutachtung

Sehr geehrte Damen und Herren,

die Österreichische Ärztekammer dankt für die Möglichkeit, sich im Rahmen der Begutachtung des gegenwärtigen Ministerialentwurfs betreffend das Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden, äußern zu können und erstattet hiermit die folgende Stellungnahme:

Eingangs wird festgehalten, dass die im Entwurf für das Netz- und Informationssystemsicherheitsgesetz 2024 vorgesehene Etablierung eines hohen Cybersicherheitsniveaus grundsätzlich befürwortet wird, allerdings sehen wir in einigen Bereichen noch Änderungsbedarf bzw das Erfordernis von Klarstellungen durch den Gesetzgeber:

- Klarstellung des Anwendungsbereichs hinsichtlich Träger der sonstigen Selbstverwaltung mit ausschließlich eigenem Wirkungsbereich (Ärztekammern in den Bundesländern)

Der Anwendungsbereich des gegenständlichen Ministerialentwurfs zum NISG 2024 umfasst gemäß § 2 Z 10 NISG 2024 wesentliche und wichtige Einrichtungen in dem Sektor der öffentlichen Verwaltung. Zu den wesentlichen Einrichtungen zählen gemäß § 24 Abs 1 lit d NISG

2024 Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene, die den kumulativen Voraussetzungen des § 24 Abs 3 NISG 2024 entsprechen sowie gemäß § 24 Abs 4 NISG 2024 zur Besorgung von Angelegenheiten der Bundesverwaltung berufen sind und entweder als Bundesbehörde eingerichtet wurden, oder Rechtspersönlichkeit besitzen. Zu den wichtigen Einrichtungen zählen gemäß § 24 Abs 2 Z 2 iVm § 24 Abs 5 NISG 2024 Einrichtungen im Sektor der öffentlichen Verwaltung auf Landesebene, die den kumulativen Voraussetzungen des § 24 Abs 3 NISG 2024 entsprechen und zur Besorgung von Angelegenheiten der Landesverwaltung berufen sind und Rechtspersönlichkeit besitzen. Unter öffentlicher Verwaltung im Sinne des NISG 2024 ist demnach nur die Bundes- und die Landesverwaltung zu verstehen.

Die Österreichische Ärztekammer geht daher von keiner Anwendung der Bestimmungen des NISG 2024 auf sonstige Selbstverwaltungskörper mit ausschließlich eigenem Wirkungsbereich, insbesondere daher auf die Ärztekammern der Bundesländer aus, weil es sich bei der Tätigkeit im eigenen Wirkungsbereich von Selbstverwaltungskörpern nicht um Bundes- oder Landesverwaltung handelt.

Entsprechend Art 120b B-VG ist nur der übertragene Wirkungsbereich von sonstigen Selbstverwaltungskörpern der staatlichen Verwaltung zuzurechnen, weswegen jedenfalls sonstige Selbstverwaltungskörper, welche ausschließlich über einen eigenen Wirkungsbereich verfügen, nicht zur Besorgung von Angelegenheiten der Bundesverwaltung im Sinne des § 24 NISG 2024 oder zur Besorgung der Landesverwaltung im Sinne des § 24 NISG 2024 berufen sein können. Die Österreichische Ärztekammer ersucht daher, dies im Gesetzestext des NISG 2024 (analog zu den Gemeinden) klarzustellen.

- <u>Gleichheitsrechtlich gebotene Ausnahme sämtlicher Träger der sonstigen Selbstverwaltung (Österreichische Ärztekammer)</u>

Gemäß Art 2 Abs 5 NIS-2-Richtline besteht für die Mitgliedstaaten die Möglichkeit, Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene sowie Bildungseinrichtungen, insbesondere wenn sie kritische Forschungstätigkeiten durchführen, in den Anwendungsbereich der nationalen Umsetzungsrechtsakte aufzunehmen.

Im gegenständlichen Ministerialentwurf wurde von dieser Öffnungsklausel nicht Gebrauch gemacht. Völlig richtig geht der Ministerialentwurf in diesem Zusammenhang davon aus, dass von der in Art 2 Abs 5 NIS-2-Richtlinie enthaltenen Öffnungsklausel in weitestmöglichem Ausmaß Gebrauch zu machen ist. Dadurch sind – wie in den Materialien ausgeführt – neben Gemeinden insbesondere auch Schulen und Universitäten bzw. Hochschulen nicht als wesentliche und wichtige Einrichtungen im Sinne des NISG 2024 anzusehen; sie sind von dessen Anwendungsbereich ausgenommen (vgl Seite 26 der EB).

Nicht nachvollziehbar ist jedoch, weswegen im Entwurf zum NISG 2024 von der Öffnungsklausel für Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene nicht auch dahingehend Gebrauch gemacht wurde, dass auch sämtliche Träger der sonstigen Selbstverwaltung ausgenommen wurden. Ein Vergleich der bundesverfassungsrechtlichen Bestimmungen zu den Gemeinden (territoriale Selbstverwaltung) einerseits und den sonstigen Selbstverwaltungskörpern andererseits zeigt die Ähnlichkeit zwischen den Trägern der territorialen und der sonstigen Selbstverwaltung. Gemäß Art 118 Abs 1 B-VG kommt der Gemeinde ein eigener sowie ein vom Bund und Land übertragener Wirkungsbereich zu, ebenso wie der Österreichischen Ärztekammer, als sonstiger Selbstverwaltungskörper.

Angesichts der vergleichbaren Ausgestaltung ist davon auszugehen, dass sonstige Selbstverwaltungskörper ebenso wie territoriale Selbstverwaltungskörper vom Begriff der „lokalen Ebene" der NIS-2-Richtlinie erfasst sind. Dieser ist unionsautonom zu bestimmen. Ob

eine Einrichtung der Verwaltung der „lokalen Ebene" zuzurechnen ist, richtet sich nicht nach der österreichischen Rechtsordnung, sondern nach den Zwecken der NIS-2-Richtlinie bzw. deren Systematik. Maßgebliches Abgrenzungskriterium für Einrichtungen auf „lokaler Ebene" ist die Besorgung der eigenen Angelegenheiten durch die Mitglieder der Einrichtung, ein Gesichtspunkt, der auf Gemeinden als Träger der territorialen Selbstverwaltung ebenso zutrifft, wie auf die Träger der sonstigen Selbstverwaltung.

Vor diesem Hintergrund einer bestehenden Öffnungsklausel in der NIS-2-Richtlinie sowie einer mit den Gemeinden vergleichbaren Situation ist die Österreichische Ärztekammer aus gleichheitsrechtlichen Gesichtspunkten ebenfalls vom Anwendungsbereich des NISG 2024 auszunehmen. Die Österreichische Ärztekammer ersucht um eine diesbezügliche Klarstellung im Entwurf.

- Vorzusehende Ausnahme für Gruppenpraxen

In Zusammenhang mit der Ermittlung des Anwendungsbereichs des NISG 2024 soll der Begriff des Gesundheitsdienstleisters im Sinne des Art 3 lit g der Richtlinie 2011/24/EU (Patientenmobilitäts-RL) ausgelegt werden. Demnach ist ein Gesundheitsdienstleister jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaates rechtmäßig Gesundheitsdienstleistungen erbringt. In den Erläuternden Bemerkungen zum gegenständlichen Ministerialentwurf wird in Zusammenhang dieser Begriffsdefinition zudem auf Anlage 1 der Gesundheitstelematikverordnung 2013 (GTelV 2013) verwiesen.

Nach Auslegung der eben angeführten Bestimmungen wären freiberuflich Ärzt*innen somit grundsätzlich vom Anwendungsbereich des vorliegenden Ministerialentwurfes mitumfasst, jedoch mit der Einschränkung des Kriteriums der Unternehmensgröße gemäß § 25 NISG 2024. In den Materialien zwar nicht explizit angeführt, aber entsprechend der Auslegung der Begriffsbestimmung des „Gesundheitsdienstleisters" gemäß Art 3 lit g der Patientenmobilitäts-RL iVm der Auflistung in Teil 2 der GTelV 2013 könnten grundsätzlich ärztliche Gruppenpraxen im Sinne des § 52a ff ÄrzteG 1998 bei Vorliegen der Determinanten des § 25 Abs. 3 NISG 2024 („*zumindest 50 Mitarbeiter beschäftigt, oder wenn sie einen Jahresumsatz von über zehn Millionen Euro erzielt und sich die Jahresbilanzsumme auf über zehn Millionen Euro beläuft*") als sog. wichtige Einrichtungen in den Anwendungsbereich fallen.

Durch die sich aus dem NISG 2024 ergebenden Anforderungen und zu ergreifenden Aufwände für diese betroffenen ärztlichen Einrichtungen, welche allem voran auch die wirtschaftliche Leistungsfähigkeit, aber auch personelle Ressourcen strapazieren, könnten sich auch belastenden Auswirkungen auf die Gesundheitsversorgung ergeben. Diese Belastungen und Risiken sollten im Interesse der öffentlichen Gesundheit hintangehalten werden. In einigen Geschäftsbereichen ist davon auszugehen, dass die zu erwartenden hohen, mit der Implementierung der verpflichtenden Maßnahmen verbundenen sowie fortlaufende Kosten, auf Kunden übergewälzt werden. Im ärztlichen Bereich, wie insbesondere bei vertragsärztlichen Gruppenpraxen, welche gesamtvertraglich in das öffentliche Gesundheitssystem eingebunden sind, ist eine diesbezügliche Kostensteuerung hingegen nicht möglich, was eine Ungleichbehandlung gegenüber anderen vom Anwendungsbereich des NISG 2024 erfassten wichtigen Einrichtungen erkennen lässt.

Auch darf an dieser Stelle auf die Materialien zum gegenständlichen Ministerialentwurf Bezug genommen werden, wonach Sozialversicherungsträger gänzlich und daher auch vermutlich bzgl ihrer eigenen Gesundheitseinrichtungen explizit vom Begriff der „Gesundheitsdienstleister" im Sinne der Patientenmobilitäts-RL und damit vom Anwendungsbereich des NISG 2024 ausgenommen sind. Schon alleine aufgrund des Größenschlusses und der aus einem

Cybersicherheitsvorfall potentiell resultierenden Folgen ergibt sich eine Unverhältnismäßigkeit in der rechtlichen Beurteilung von Sozialversicherungsträgern und den potentiellen betroffenen ärztlichen Gruppenpraxen.

Die Österreichische Ärztekammer sieht hier einen dringenden Handlungsbedarf und ersucht den Gesetzgeber – nach dem Vorbild der Sozialversicherungsträger – ebenso eine explizite Ausnahme für ärztliche Gruppenpraxen vom Anwendungsbereich des NISG 2024 im Gesetzestext vorzusehen bzw anderweitig um Berücksichtigung in den Materialien.

- Bedenken hinsichtlich der Bestimmungen der §§ 38, 39, 42 und 43 NISG 2024

Die vom österreichischen Gesetzgeber vorgesehenen weitreichenden Befugnisse in den §§ 38 und 39 NISG 2024, zu deren Erlassung die NIS-2-Richtlinie nicht verpflichtet, werden ebenso kritisch gesehen. Auch hinsichtlich der Vereinbarkeit der in §§ 42 sowie 43 NISG 2024 getroffenen Regelungen zur Datenverarbeitung und Datenübermittlung mit den besonderen berufsrechtlichen Verschwiegenheitspflichten bestehen von Seiten der Österreichischen Ärztekammer Bedenken.

Die Österreichische Ärztekammer ersucht um Berücksichtigung der hier ausgeführten Einwände im weiteren Gesetzgebungsprozess.

Mit freundlichen Grüßen

OMR Dr. Johannes Steinhart
Präsident

ÖSTERREICHISCHE ÄRZTEKAMMER

Bundeskammer der
Ziviltechniker:innen | Arch+Ing

A-1040 Wien, Karlsgasse 9
T +43.1.505 58 07
F +43.1.505 32 11
office@arching.at, www.arching.at

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

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

Wien, am 30. April 2024

Stellungnahme zum 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

GZ: 2024-0.220.735

Sehr geehrte Damen und Herren!

Die Bundeskammer der Ziviltechniker:innen bedankt sich für die Übermittlung des oben genannten Entwurfs und erlaubt sich dazu folgende Stellungnahme abzugeben:

Vorausschicken möchten wir, dass sich weder die Bundeskammer noch die Länderkammern der Ziviltechniker:innen als berufliche Selbstverwaltungskörper vom Anwendungsbereich des vorliegenden Entwurfs betroffen sehen, weil sie weder unter die wesentlichen Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene iSd § 24 Abs. 1 Z 1 lit d iVm Abs. 4 noch unter die wichtigen Einrichtungen im Sektor er öffentlichen Verwaltung auf Landesebene iSd § 24 Abs. 2 Z 2 iVm Abs. 5 fallen. Insbesondere da die Bundeskammer bzw. die Länderkammern im Rahmen der sonstigen Selbstverwaltung iSd Art. 120a bis c B-VG tätig und in der Besorgung ihrer Aufgaben auch nicht weisungsgebunden sind.

Um Unklarheiten zu vermeiden, regt die Bundeskammer aus den oben genannten Gründen eine ausdrückliche Klarstellung – so wie sie in § 24 Abs. 3 für Gemeinden oder in § 24 Abs. 6 für Universitäten usw. vorgesehen ist – dahingehend an, dass Selbstverwaltungskörper, wie die Kammern der Ziviltechniker:innen sowie insgesamt die Kammern der freien Berufe, nicht als wesentliche oder wichtige Einrichtungen der öffentlichen Verwaltung gelten. Zumindest sollte aber jedenfalls eine entsprechende Klarstellung in den Erläuterungen zum Entwurf erfolgen.

ZT
Ziviltechniker:innen sind staatlich befugte und beeidete
Architekt:innen und Zivilingenieur:innen

Zu § 3 Z 1:

Der Ordnung halber wird darauf hingewiesen, dass es den Begriff „Netzsystem", wie es wohl aus der Definition „Netz- und Informationssystem" herauszulesen ist, im Bereich der Informationstechnologie nicht gibt. Ein Netzsystem ist unserer Ansicht nach dem Bereich der Elektrotechnik zuzuordnen.

Zu § 3 Z 26:

In Art. 6 Z 9 Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) wird der Begriff „Risiko" als ein „Potenzial für Verluste oder Störungen, die durch Sicherheitsvorfall verursacht werden" definiert. § 3 Z 26 des Gesetzesentwurfes spricht dagegen von einem Cybersicherheitsvorfall. Die Definitionen zu Sicherheitsvorfall (Art. 6 Z 6 Richtlinie (EU) 2022/2555) und Cybersicherheitsvorfall (§ 3 Z 30) sind jedoch gleichlautend. Ein Cybersicherheitsvorfall könnte eine Begrenzung auf kriminelle Attacken aus dem Internet suggerieren. Im Sinne des Betriebs wichtiger und wesentlicher Einrichtungen greift dies uE zu kurz.

Aus Sicht der Bundeskammer inkludieren Risiken auch im Kontext der NIS-2-Richtlinie alle Ursachen und Ereignisse, die die Zuverlässigkeit (Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität) eines ordnungsgemäßen Betriebs der Netz- und Informationssysteme negativ beeinflussen können. Darunter fallen auch potenziell fehlerhafte Betriebssoftware, Hardware und Steuergeräte, Störungen in der physischen Infrastruktur, Tätermodelle (Innentäter, Außentäter) usw.

Mit Verweis auf das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) sollte unter dem Begriff „Risiko" auch der „All-Gefahren-Ansatz" mitberücksichtigt werden. Ein All-Gefahren-Ansatz ist ein umfassender und integrierter Rahmen für die Vorbereitung auf Notfälle, der bei der Planung von Reaktions- und Eindämmungsmaßnahmen für "alle Gefahren", die auftreten können, angewendet wird. Sollten nur Vorfälle aus Cybergefahren vom Gesetz erfasst werden, sollte dieser Umstand präzisiert werden. Wenn dies nicht erfolgt, öffnet es Tür und Tor für individuelle Auslegungen bei Prüfer:innen.

Zu § 3 Z 33:

In der Begriffsbestimmung des § 3 Z 33 wird die Abkürzung „CSIRT" mit Computer-Notfallteam übersetzt. Nachdem „CSIRT" für „Computer Security Incident Response Team" steht, wird angeregt, als deutsche Übersetzung „Computersicherheits-Ereignis- und Reaktionsteam" oder „Computersicherheits-Reaktionsteam" zu übernehmen.

Zu § 7:

Mit § 7 wird das im NISG bestehende Institut der qualifizierten Stellen (vgl. § 18 NISG) im Wesentlichen in das neue NISG 2024 überführt. Gemäß § 3 der Verordnung über qualifizierte Stellen – QuaSteV, BGBl. II Nr. 226/2019, hatten qualifizierte Stellen bislang „befähigte sicherheitsüberprüfte Prüfer" einzusetzen. Die Anforderungen an diese Prüfer:innen waren in § 4 QuaSteV geregelt. Die Erfüllung dieser Anforderungen waren durch die qualifizierte Stelle gegenüber dem Bundesminister für Inneres bei der Antragstellung nachzuweisen.

Vergleichbar mit dem bisherigen Prüfsystem regelt Abs. 1, dass der Nachweis, dass eine wesentliche oder wichtige Einrichtung die gebotenen Risikomanagementmaßnahmen getroffen hat (§ 33 Abs. 2 und 3) durch eine unabhängige Stelle zu prüfen ist, die sich hierfür zumindest eines unabhängigen Prüfers zu bedienen hat. Unabhängige Stellen haben ihre Eignung gegenüber der Cybersicherheitsbehörde bei der Antragstellung nach Abs. 2 nachzuweisen. In einer

Verordnung des Bundesministers für Inneres sollen die Anforderungen, die eine unabhängige Stelle zur Zulassung erfüllen muss, festgelegt werden (Abs. 13 Z 1).

Unabhängige Prüfer:innen sind natürliche Personen, die von einer unabhängigen Stelle zur Beurteilung der Umsetzung von Risikomanagementmaßnahmen wesentlicher und wichtiger Einrichtungen gemäß § 33 Abs. 2 und 3 eingesetzt werden können (Abs. 5). Als Voraussetzungen dafür sind nach Z 1 eine vor nicht länger als drei Jahren durchgeführte Sicherheitsüberprüfung sowie nach Z 2 die positive Absolvierung einer Fachprüfung gemäß Abs. 8 nachzuweisen.

Zu einer solchen Fachprüfung ist gemäß Abs. 7 zuzulassen, wer über ein österreichisches Reifeprüfungszeugnis, Diplomprüfungszeugnis oder Berufsreifeprüfungszeugnis verfügt (Z 1) und eine facheinschlägige Berufserfahrung von mindestens drei Jahren im Ausmaß von zumindest zwanzig Wochenstunden im Bereich der Cybersicherheit nachweisen kann (Z 2). Im Rahmen der Fachprüfung hat der Prüfungskandidat ausreichende theoretische Fachkenntnisse über die Risikomanagementmaßnahmen gemäß § 32 und ausreichende praktische Fähigkeiten zur Beurteilung der Umsetzung von Risikomanagementmaßnahmen gemäß § 32 in organisatorischer oder technischer Hinsicht nachzuweisen (Abs. 8). Der Bundesminister für Inneres hat mit Verordnung nähere Regelungen zum Verfahren und zu den Inhalten dieser Überprüfung festzulegen (Abs. 13 Z 2).

In diesem Zusammenhang wird seitens der Bundeskammer nochmals ausdrücklich darauf hingewiesen, dass unabhängige, staatlich befugte und beeidete Ziviltechniker:innen im Bereich Informationstechnologie auf dem von ihrer Befugnis umfassten Fachgebiet zur Erbringung von planenden, prüfenden, überwachenden, beratenden, koordinierenden usw. Leistungen, insbesondere zur Vornahme von Messungen und zur Erstellung von Gutachten berechtigt und mit öffentlichem Glauben versehene Personen sind (§ 3 ZTG). Öffentliche Urkunden, welche von Ziviltechniker:innen errichtet werden, begründen vollen Beweis dessen, was darin von der Behörde amtlich verfügt oder erklärt wird (§ 292 ZPO).

Der Verleihung der Ziviltechniker:innenbefugnis hat eine Hochschulausbildung (§ 5 ZTG), eine mindestens dreijährige praktische Betätigung (§ 6 ZTG) sowie die Ablegung der Ziviltechnikerprüfung (§ 7 ZTG) voranzugehen. Zudem sind Ziviltechniker:innen auf dem Fachgebiet ihrer Befugnis zur laufenden Berufsfortbildung verpflichtet, die mittels Fortbildungsverordnungen seitens der Bundeskammer sichergestellt wird (§ 12 Abs. 8 ZTG). Ziviltechniker:innen (-Gesellschaften), die auf dem Fachgebiet der Informationstechnologie tätig sind, verfügen daher grundsätzlich über die in § 7 vorgeschriebene Befähigung zur Zulassung als unabhängige Stellen bzw. unabhängige Prüfer:innen und wären somit schon kraft ihrer Funktion nach entsprechendem Antrag durch die Cybersicherheitsbehörde zuzulassen.

Jedenfalls ist aber sicherzustellen, dass die durch Verordnung des Bundesministers für Inneres festzulegenden Kriterien so ausgestaltet werden, dass Ziviltechniker:innen (-Gesellschaften) insgesamt keine Schlechterstellung zu den bislang geltenden Qualitätsanforderungen erfahren. Insbesondere im Hinblick auf § 51 Abs. 5, wonach Bescheide, die gemäß § 18 Abs. 1 NISG idF 2018 erlassen wurden, mit Inkrafttreten dieses Bundesgesetzes gegenstandslos werden, sofern die qualifizierte Stelle nicht einen Antrag gemäß § 7 Abs. 2 binnen sechs Monaten ab Inkrafttreten der zu erlassenden Verordnung stellt.

Gemäß Abs. 4 hat die Cybersicherheitsbehörde die Zulassung der unabhängigen Stelle bei Nichteinhaltung der Anforderungen zu widerrufen, außer es ist ein Fall von höherer

Gewalt, der außerhalb der Einflusssphäre der unabhängigen Stelle liegt, eingetreten. Nach rechtskräftigem Widerruf kann erst nach Ablauf eines Jahres ein neuerlicher Antrag auf Zulassung gestellt werden. Wenn diese „Sperrfrist" in den Erläuterungen dadurch erklärt wird, dass damit Missbrauch hintangehalten werden soll, ist aus unserer Sicht die „Sperrfrist" dezidiert auf begründete Missbrauchsfälle im Gesetzeswortlaut oder in den Erläuterungen zu beschränken. So würde es für die unabhängige Stelle nämlich einen unverhältnismäßigen Eingriff in ihre Geschäftstätigkeit bedeuten, wenn ihre Zulassung deshalb widerrufen wird, weil sie etwa (unverschuldet) durch Kündigung/längere Krankheit einer Mitarbeiterin oder eines Mitarbeiters die Mindestanzahl an unabhängigen Prüfer:innen unterschreitet. In diesen Fällen kann wohl kein Missbrauch erkannt werden. Vielmehr soll es der unabhängigen Stelle hier möglich sein, innerhalb einer angemessenen Frist eine/n neue/n Prüfer:in zu nennen, bevor es zu einem Widerruf der Zulassung kommt. Ebenso denkbar wäre eine Ruhendstellung der Zulassung, solange die Mindestanforderungen nicht erfüllt werden. Dies insbesondere auch im Hinblick darauf, dass dem Bescheid zum Widerruf der Zulassung keine aufschiebende Wirkung zukommt. Da dies nachteilige Auswirkungen auf wichtige Abläufe in der Prüfung von Einrichtungen haben kann, sollte die aufschiebende Wirkung beibehalten werden. So können auch allfällige Schäden, die durch einen Bescheid, der später aufgehoben oder abgeändert wird, minimiert werden.

Die in § 7 Abs. 3 vorgesehenen umfangreichen Aufsichtsmaßnahmen der Cybersicherheitsbehörde gemäß § 38 Abs. 1 sollen aus den unten dargelegten Gründen nicht zur Kontrolle der unabhängigen Stellen zur Anwendung gelangen. Stattdessen wird angeregt, die notwendigen Kontrollmaßnahmen auf ein unbedingt erforderliches Ausmaß zu reduzieren, die von einer unabhängigen Institution überprüft werden sollen.

Zu § 38:

Der Umfang der in § 38 definierten Aufsichtsmaßnahmen der Behörde ist, angesichts der potenziellen Eingriffsmöglichkeiten in sensible Unternehmensbereiche, zu unklar. Vor dem Hintergrund, dass die Behörde diese Maßnahme laut Abs. 1 in Wahrnehmung ihrer Aufsichtsaufgaben zur Einhaltung der Verpflichtungen nach dem NISG 2024 auch jederzeit („Ad-hoc-Prüfung" siehe § 38 Abs. 1 Z 5) ergreifen kann, fehlt es an einer klaren Präzisierung. So soll etwa klargestellt werden, dass sämtliche Kontrollmaßnahmen ausschließlich unter Mitwirkung der Einrichtung stattzufinden haben. Ebenso fehlt eine gesetzlich verankerte Interessenabwägung in Bezug auf die Erforderlichkeit, Verhältnismäßigkeit und mögliche alternative Maßnahmen. Daraus hat sich zu ergeben, dass eine behördliche Einschau bzw. ein Zugriff auf die Netz- und Informationssysteme nur innerhalb gesetzlicher Schranken, also insbesondere nur in Bezug auf konkrete sicherheits- bzw. prüfungsrelevante Teile und nur in einem unbedingt erforderlichen Ausmaß unter möglichster Schonung der Rechte der betroffenen Einrichtung und Dritter, gewährt werden muss.

Aus rechtsstaatlicher Sicht ist hier eine dringende Anpassung vorzunehmen, weil andernfalls im Anwendungsbereich dieses Gesetzes ein überschießender, umfassender Zugriff auf Systeme möglich wäre, der sonst nur den zuständigen (Strafverfolgungs-)Behörden mit richterlichem Beschluss vorbehalten ist. Ergänzend ist darauf hinzuweisen, dass ein direkter Zugriff auf die IT-Systeme in der Richtlinie nicht vorgesehen ist.

Zudem ist aus unserer Sicht eine dem Gesetzeszweck entsprechende Einschränkung der Aufsichts- und Kontrollrechte der gegenständlichen Behörde vorzunehmen. Der Bundesminister für Inneres als vorgesehene Cybersicherheitsbehörde unterliegt einer

politischen Verantwortung und ist nicht unabhängig, wie dies etwa bei der Datenschutzbehörde der Fall ist. Eine Ausgestaltung der Cybersicherheitsbehörde könnte derart erfolgen, dass diese als neue (unabhängige) Behörde eingerichtet wird oder die Befugnisse einer unabhängigen Behörde übertragen werden.

Zu § 39:
Unabhängige, staatlich befugte und beeidete Ziviltechniker:innen im Fachbereich der Informationstechnologie eignen sich besonders für die Rolle der „Überwachungsbeauftragten" in § 39 Abs. 3 Z 2. Also zur Überwachung der Anforderungen gemäß §§ 32 und 34, um die Umsetzung der mit Bescheid der Cybersicherheitsbehörde angeordneten Maßnahmen sicherzustellen. Die vorgesehenen Rechte des Überwachungsbeauftragten iSd § 3 Abs. 1 Z 37 sollten in dem Zusammenhang dagegen auf Auditrechte beschränkt werden, die nur gemeinsam mit dem/der Ziviltechniker:in und der Einrichtung ausgeübt werden können.

Abschließend wird darauf hingewiesen, dass Ziviltechniker:innen des einschlägigen Fachbereichs als unabhängige Fachexpertinnen und Fachexperten im Bereich der Informationstechnologie sowohl für Peer-Reviews als Sachverständige für Cybersicherheit (§ 23) als auch für die im Gesetzesentwurf vorgesehenen Stellen und Gremien (siehe § 3 Z 32 bis 36) beratend zur Verfügung stehen.

Die Bundeskammer bietet zudem gerne an, wie in der Vergangenheit bereits des Öfteren praktiziert, in weiterführenden Gesprächen zur erlassenden Verordnung hinsichtlich Qualitätssicherung von unabhängigen Stellen bzw. unabhängigen Prüfer:innen entsprechende fachliche Expertise einzubringen.

Mit bestem Dank für die Berücksichtigung der Stellungnahme und
freundlichen Grüßen

Daniel Fügenschuh

Architekt Dipl.-Ing. Daniel Fügenschuh
Präsident

KAMMER DER STEUERBERATER:INNEN UND WIRTSCHAFTSPRÜFER:INNEN

BUNDESKANZLERAMT
Sektion I – Präsidium
BKA – I/8 (Technologie- und Daten Management, Cybersicherheit und Krisenrechenzentrum)
z.H. Herrn Mag. Arno Spiegel
Herrengasse 23
1010 Wien
NIS@bka.gv.at
recht@bka.gv.at

Sachbearbeiter	G. Benesch
Telefon	+43 | 1 | 811 73-0
E-Mail	benesch@ksw.or.at
Datum	30.04.2024

Stellungnahmen zum 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 Gesundheitstelematikgesetz2012 geändert werden
(Geschäftszahl: 2024-0.220.735)

Sehr geehrter Herr Mag. Spiegel,

die Kammer der Steuerberater:innen und Wirtschaftsprüfer:innen dankt für die Einladung zur Abgabe einer Stellungnahme zum im Betreff erwähnten Entwurf.

Stellungnahme

Das Ziel des Vorhabens – Erhöhung der Cybersicherheit zur Abwehr krimineller Aktivitäten wie Spionage und Sabotage – ist von allgemeingesellschaftlicher Bedeutung und wird dem Grunde nach seitens der KSW unterstützt.

Dabei ist, insb. in Hinblick auf den Regelungszweck der umzusetzenden Richtlinie und die zu wahrende Verhältnismäßigkeit in der nationalen Umsetzung, auch darauf zu achten, daß keine überbordenden Regelungen geschaffen werden und Behörden nur jene Befugnisse erhalten, die sie unbedingt benötigen. Bei den einer Behörde zugestandenen Befugnissen ist auch auf eine allenfalls mittelbare Beeinträchtigung von Rechten Bedacht zu nehmen, insbesondere dann, wenn Rechte von Parteienvertreter:innen und deren Mandant:innen betroffen sein können. Ebenso sollten die Auswirkungen auf bürokratische Anforderungen und der daraus entstehenden Aufwand für die Betroffenen bedacht werden und sichergestellt werden, daß diese in einer entsprechenden Verhältnismäßigkeit zum Ziel der Regelungen stehen.

Zu § 24:

Die KSW geht davon aus, dass sie als Selbstverwaltungskörper von den Pflichten des Gesetzes nicht erfasst ist, da sie weder unter die wesentlichen Einrichtungen iSd § 24 Abs 1 Z 1 lit d iVm Abs 4 noch unter die wichtigen Einrichtungen iSd § 24 Abs 2 Z 2 iVm Abs 5 fällt. Zwar sind von der KSW auch Aufgaben im übertragenen Wirkungsbereich zu vollziehen, in welchen der Präsident der Kammer an Weisungen des BMAW gebunden ist. Diese Aufgaben des übertragenen Wirkungsbereiches vollzieht die KSW dennoch im Rahmen der Selbstverwaltung als Selbstverwaltungskörper und damit in gleicher Weise wie die ausdrücklich in Abs. 3 ausgenommenen Gemeinden (vgl. dazu insb. Art 118 Abs 1 B-VG). Das in Art 2 Abs 5 der RL 2022/2555 („NIS-2 RL“) für „Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene“ enthaltene Mitgliedstaatenwahlrecht ist daher uE auf andere Selbstverwaltungskörper anzuwenden, wenn diesen Aufgaben der öffentlichen Verwaltung übertragen wurden, die andernfalls durch ebensolche Einrichtungen auf lokaler Ebene vollzogen würden.

In Hinblick auf den Regelungszweck der Richtlinie und des Vorhabens, nämlich die Schaffung eines hohen Cybersicherheitsniveaus insb. in Schlüsselsektoren, ist deutlich, daß eine Erfassung Einrichtungen wie der KSW über das Regelungsziel hinausgehen würde. Aufgabe der KSW wie auch anderer Kammern der freien Berufe ist die Administration eines Berufes, dem der Gesetzgeber durch Schaffung eines eigenen Berufsgesetzes mit eigener gesetzlicher Vertretung und Selbstverwaltung eine besondere Stellung verliehen hat. Demnach unterliegt diese Administration auch keiner unmittelbaren Einflußnahme durch die staatliche Verwaltung und ist die Kammer nicht in die staatliche Verwaltung integriert (und nicht in die IT der staatlichen Verwaltung eingeschlossen).

Daher regen wir an, dass – ähnlich wie bei der Klarstellung zu Gemeinden, in § 24 Abs 3 sowie zu Universitäten etc in Abs 6 – dies im Gesetzestext durch Ergänzung des Abs 6 klargestellt wird: „*sowie Selbstverwaltungskörper wie die Kammern der freien Berufe*.“

Diese Stellungnahme wird von der Kammer der Steuerberater:innen und Wirtschaftsprüfer:innen dem Präsidium des Nationalrats über nachstehende Internetseite zur Verfügung gestellt.
https://www.parlament.gv.at/PERK/BET/VPBEST/#AbgabeStellungnahme

Wir ersuchen höflich, unsere in dieser Stellungnahme angeführten Vorschläge bzw. Anregungen zu berücksichtigen und verbleiben

mit freundlichen Grüßen

Mag. Herbert Houf
(Präsident)

Mag. Gregor Benesch
(Kammerdirektor Stellvertreter)

Elektronisch gefertigt

ÖSTERREICHISCHE
NOTARIATSKAMMER

An das
Bundeskanzleramt
Ballhausplatz 2
1010 Wien

Wien, am 30.04.2024
GZ: 211/24

Geschäftszahl: 2024-0.220.735

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;

Begutachtungsverfahren

Sehr geehrte Damen und Herren!

Mit Schreiben vom 03. April 2024, bei der Österreichischen Notariatskammer am selben Tag eingelangt, hat das Bundeskanzleramt den 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, übermittelt und ersucht, dazu bis 01. Mai 2024 eine Stellungnahme abzugeben.

Die Österreichische Notariatskammer bedankt sich für die Möglichkeit, sich zum vorliegenden Entwurf äußern zu können, und erlaubt sich, nachstehende

Stellungnahme

abzugeben:

1. **Zur Frage der Anwendbarkeit der Bestimmungen auf die Kammern der Freien Berufe**

Die Tatbestandsmerkmale der Legaldefinition des § 24 Abs 3 NISG 2024 idF des Begutachtungsentwurfs werden weder von der Österreichischen Notariatskammer noch von den Notariatskammern auf Länderkammerebene erfüllt, da sie ausschließlich Aufgaben im eigenen Wirkungsbereich besorgen und als Selbstverwaltungskörper nicht weisungsgebunden sind (vgl. § 24 Abs 3 Z 2 NISG 2024 idF Begutachtungsentwurf).
Desweiteren sind die Notariatskammern nicht ermächtigt, Bescheide zu erlassen, die die Rechte Einzelner im grenzüberschreitenden Personen-, Waren, Dienstleistungs- oder Kapitalverkehr berühren (vgl. § 24 Abs 3 Z 3 NISG 2024 idF Begutachtungsentwurf).

Österreichische Notariatskammer
Landesgerichtsstraße 20 | 1010 Wien | T +43 1 402 450 90 | F +43 402 450 91 00 | kammer@notar.or.at | ihr-notariat.at
Der Informationspflicht laut Datenschutz-Grundverordnung wird mit folgender Datenschutzerklärung (ihr-notariat.at/oenk-dse) entsprochen.
Bei Bedarf ist auch eine postalische Übermittlung möglich.

Die Bestimmungen des NISG 2024 idF des Begutachtungsentwurfs sind daher auf die Notariatskammern nicht anwendbar.

Nichtsdestotrotz wäre eine Klarstellung der Nichtanwendbarkeit auf die Kammern der Freien Berufe wünschenswert. Dies könnte durch Ergänzung des ersten Satzes in § 24 Abs 6 wie folgt umgesetzt werden, sodass dieser lauter wie folgt: *„Einrichtungen im Sektor der öffentlichen Verwaltung, deren Tätigkeiten überwiegend in den Bereichen nationale Sicherheit, öffentliche Sicherheit, militärische Landesverteidigung oder Strafverfolgung ausgeübt werden sowie Einrichtungen des Universitäts-, Hochschul- und Schulwesens, Einrichtungen der Gerichtsbarkeit, Einrichtungen der Gesetzgebung, einschließlich der Parlamentsdirektion sowie die Österreichische Nationalbank sowie Selbstverwaltungskörper wie die Kammern der freien Berufe auf Bundes- und Landesebene gelten nicht als wesentliche oder wichtige Einrichtungen".* Alternativ könnte eine Klarstellung in den Erläuternden Bemerkungen erfolgen.

2. Zur Frage der Anwendbarkeit der Bestimmungen auf Unternehmen

Erwägungsgrund 35 der NIS-2-Richtlinie stellt klar, dass der Begriff des Rechenzentrumsdienstes nicht interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von der betreffenden Einrichtung für eigene Zwecke betrieben werden, umfassen soll. Interne Rechenzentren wären somit von der Anwendbarkeit der NIS-2-Richtlinie ausgenommen.

Im vorliegenden Gesetzesentwurf wurde diese Einschränkung jedoch nicht berücksichtigt. Dies führt zu dem Ergebnis, dass das NISG 2024 idF des Begutachtungsentwurfes auch auf Konzern-IT-Dienstleister, deren Leistungen nicht am offenen Markt angeboten werden, sondern nur für interne Unternehmen und geschlossene Nutzerkreise erbracht werden, anzuwenden wäre.

Die Österreichische Notariatskammer regt an, den Gesetzestext so anzupassen, dass sich die Aussage des Erwägungsgrundes 35 im Gesetzestext widerspiegelt. Dies wäre durch eine Ausnahme der internen Rechenzentren bzw. Rechenzentren mit geschlossenen Nutzerkreisen von der Anwendbarkeit des NISG 2024 bzw. zumindest eine Klarstellung in den Erläuternden Bemerkungen zum NISG 2024 zu erreichen.

Erwägungsgrund 16 der NIS-2-Richtlinie eröffnet zudem dem Österreichischen Gesetzgeber die Möglichkeit, bei der Anwendung von Artikel 6 Abs 2 des Anhangs der Empfehlung 2003/361/EG den Grad der Unabhängigkeit einer Einrichtung gegenüber ihren Partnerunternehmen und verbundenen Unternehmen zu berücksichtigen. Diese Möglichkeit wurde in dem vorliegenden Gesetzesentwurf nicht genutzt.

Dies führt zu dem unverhältnismäßigen Ergebnis, dass Kleinst- oder Kleinunternehmer, die eine zu andere Konzerngesellschaft abgetrennte IT-Infrastruktur haben oder sonst faktisch unabhängig in Bezug auf ihre Systeme agieren, unter die Anwendbarkeit des NISG 2024 fallen könnten, wenn sie in einem Konzernverbund eingebettet sind oder entsprechende Partnerunternehmen haben.

Es wird daher angeregt von der in Erwägungsgrund 16 angeführten Möglichkeit, Gebrauch zu machen und diese Ausnahme richtlinienkonform in das Gesetz aufzunehmen.

3. <u>Zu den Bestimmungen betreffend Einsichts- und Kontrollrechte</u>

Der Umfang der in § 38 NISG 2024 idF des Begutachtungsentwurfs definierten Einsichts- bzw. Kontrollrechte der Cybersicherheitsbehörde ist aus Sicht der Österreichischen Notariatskammer nicht ausreichend klar definiert. Dies ist als kritisch anzusehen, da die Ausübung der Einsichts- bzw. Kontrollrechte zu einer potentiellen Gefahr der Verletzung der notariellen Verschwiegenheit gem. § 37 NO bzw. anderer beruflicher Verschwiegenheitspflichten führen könnte. Sollte eine Kontrolle z.B. bei einem IT-Dienstleister eines Notars/einer Notarin, der in den Anwendungsbereich des NISG 2024 fällt, durchgeführt werden, muss jedenfalls gewährleistet sein, dass die notarielle Verschwiegenheit nicht verletzt wird.

Aus Sicht der Österreichischen Notariatskammer wäre der Gesetzestext daher insoweit anzupassen, als dass der Umfang der Einsichts- bzw. Kontrollrechte klar definiert wird und sichergestellt ist, dass Daten, der notariellen Verschwiegenheit oder anderer beruflicher Verschwiegenheitspflichten unterliegen, von den Einsichts- und Kontrollrechten nicht berührt werden.

Mit vorzüglicher Hochachtung

Dr. Michael Umfahrer
(Präsident)

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

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

Zl. 13/1 24/42

2024-0.220.735
BG, 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

Referentinnen: **Mag. Katharina Bisset, MSc, Rechtsanwältin in Mannersdorf**
Mag. Julia Luksan, LL.M., Rechtsanwältin in Wien

Sehr geehrte Damen und Herren!

Der Österreichische Rechtsanwaltskammertag (ÖRAK) dankt für die Übersendung des Entwurfes und erstattet dazu folgende

Stellungnahme:

1. Allgemeines

Der vorgeschlagene Entwurf zur Neufassung des NISG idgF betrifft – in direkter Anwendung oder in der Lieferkette – weite Teile der österreichischen Wirtschaft und Verwaltung. In dieser Stellungnahme wird auf Punkte eingegangen, in denen das Gesetz die Interessen des ÖRAK und des Rechtsanwaltsstandes betrifft, aber auch solche, die im allgemeinen Interesse der Rechtssicherheit zu überarbeiten wären.

2. Zu § 24 Abs 3

Der ÖRAK geht davon aus, dass weder er selbst noch die Rechtsanwaltskammern von den Pflichten des Gesetzes erfasst sind, da sie weder unter die wesentlichen Einrichtungen iSd § 24 Abs 1 Z 1 lit d iVm Abs 4 noch unter die wichtigen Einrichtungen iSd § 24 Abs 2 Z 2 iVm Abs 5 fallen. Insb unterliegen sie gemäß § 24 Abs 3 Z 2 auch nicht der Aufsicht des

Bundes oder eines Landes und sind als Selbstverwaltungskörper nicht weisungsgebunden sowie ausschließlich im eigenen Wirkungsbereich tätig.
Es wäre jedoch wünschenswert, dass – ähnlich wie bei der Klarstellung zu Gemeinden, in § 24 Abs 3 sowie zu Universitäten etc in Abs 6 – dies im Gesetzestext klargestellt wird. Dies durch Ergänzung des Abs 6: *„sowie Selbstverwaltungskörper wie die Kammern der freien Berufe"*, alternativ als Klarstellung in den Erläuterungen zum Gesetz.

3. Zu § 25

Hier wurde der vom europäischen Gesetzgeber eingeräumten Möglichkeit (vgl Erwägungsgrund 16), für die Beurteilung der Unternehmensgröße im Konzern eine Sonderregelung einzuführen, bedauerlicherweise nicht gefolgt, wie dies beispielsweise im deutschen Gesetzesentwurf der Fall ist.

Der deutsche Entwurf sieht in § 28 folgende Regelung vor: *„Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG sind 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."*

Gerade für kleine und mittelständische Unternehmen in Österreich, die als Tochtergesellschaften nur aufgrund des Konzernverbundes („verbundene Unternehmen") in den Anwendungsbereich des Gesetzes fallen würden, kann das eine unverhältnismäßige Belastung sein, wenn sie eine von anderen Konzerngesellschaften gesonderte IT-Infrastruktur haben, oder sonst faktisch unabhängig in Bezug auf ihre Systeme agieren. Eine richtlinienkonforme Ausnahme von der Hinzurechnung der relevanten Unternehmenskennzahlen bei verbundenen Unternehmen oder Partnerunternehmen sollte daher in das Gesetz aufgenommen werden.

4. Zu § 32 Abs 2 Z 3

Es ist bekannt, dass die NIS2 auch in der Lieferkette weitere Unternehmen treffen kann, die nicht direkt vom Anwendungsbereich betroffen sind. Hier werden in § 15 Abs 4 Z 1 Konzepte für die Cybersicherheit in der Lieferkette im IKT-Bereich als Teil der ÖSCS angegeben. Diese Konzepte werden eine wichtige Leitlinie darstellen, wie Einrichtungen, die unter dieses Gesetz fallen, die Sicherheit ihrer Lieferkette gewährleisten. In Bezug auf die Lieferkette ist jedenfalls klarzustellen, dass sich eine (allfällige) Überbindung der Pflichten nur auf einzelne (Teil-)Systeme beziehen kann. Darüber hinaus sollte, wie in den Erläuterungen zu diesem Punkt erwähnt, im Gesetz klargestellt werden, dass eine Bewertung der jeweiligen Unternehmen in der Lieferkette durch die Einrichtung möglich sein soll.

Weiters sollte klargestellt werden, dass ein direkter Zugriff der Behörden auf Unternehmen in der Lieferkette nicht möglich sein soll.

In Bezug auf die Anwaltschaft ist hier klarzustellen, dass Rechtsanwältinnen und Rechtsanwälte sowie Rechtsanwaltskanzleien, die Einrichtungen anwaltlich beraten und vertreten, nicht von der Lieferkette umfasst sind, vor allem da allfällige Daten bereits aufgrund des Anwaltsgeheimnisses des § 9 Abs 2 RAO und die prozessualen Maßnahmen (§ 321 Abs 1 Z 3 und 4 ZPO, § 157 Abs 1 Z 2 und Abs 2 StPO sowie aufgrund des Umgehungsschutzes des § 157 Abs 3 StPO zu schützen sind. Eine entsprechende Klarstellung sollte jedenfalls zumindest in die Erläuterungen aufgenommen werden.

5. Zu § 34

In der Praxis können Sachverhalte entstehen, die eine Meldung gem § 34 und gleichzeitig eine Meldung an die zuständige Datenschutzbehörde gemäß Art 33 DSGVO bzw § 55 DSG sowie in Zukunft eine Meldepflicht gem Art 11 des geplanten Cyber Resilience Act (COM(2022) 454 final) auslösen können.

Es sieht zwar § 21 NISG eine Zusammenarbeit mit der Datenschutzbehörde vor, die auch eine Weiterleitung von Meldungen beinhaltet, es ist jedoch wünschenswert, dass in Hinblick auf die kurzen Fristen aller Meldungen eine zentrale Meldestelle eingerichtet wird, die an die entsprechenden Behörden weiterleitet, sodass mit einer Meldung alle Meldepflichten erfüllt sind.

Allenfalls sollte auch klargestellt werden, ob eine Information an die DSB gem § 21 Abs 2 die Einrichtung von einer Meldung gem Art 33 DSGVO befreit.

6. Zu § 38
6.1. Allgemeines

Der Umfang der in § 38 definierten Einsichts- bzw Kontrollrechte der Behörde ist unklar, was angesichts der potenziellen Eingriffsmöglichkeiten in sensible Unternehmensbereiche jedenfalls problematisch ist. Das in den Erläuterungen erklärte Ziel, eine behördliche Aufsicht ohne *unverhältnismäßige Eingriffe* zu ermöglichen, sollte sich daher im Gesetzestext widerspiegeln.

So ist insb in § 38 Abs 1 Z 1 unklar, welche Vorgänge von einer behördlichen Einschau „in die diesbezüglichen Netz- und Informationssysteme" und einer solchen „mittels Fernzugriff" erfasst sein sollen. Diesbezüglich fehlt es an einer Präzisierung, sodass eine – jedenfalls erforderliche und zu begrüßende – Vorabverständigung allein nicht ausreichend ist. Es ist nämlich zu beachten, dass die Behörde diese Maßnahme laut Abs 1 in Wahrnehmung ihrer Aufsichtsaufgaben zur Einhaltung der Verpflichtungen nach dem NISG 2024 in einem breiten Umfang und jederzeit ergreifen kann. Weiters ist ein direkter Zugriff auf die IT-Systeme in der Richtlinie nicht vorgesehen; daher sollten die entsprechenden Inhalte aus dem Entwurf entfernt werden.

Eine Interessenabwägung in Bezug auf die Erforderlichkeit, Verhältnismäßigkeit und mögliche alternative Maßnahmen ist vorzunehmen, die ebenfalls nicht im Gesetzesentwurf verankert wurde. Daraus muss sich ergeben, dass eine behördliche Einschau bzw ein Zugriff auf die Netz- und Informationssysteme einer wesentlichen Einrichtung nur innerhalb gesetzlicher Schranken, also insbesondere nur in Bezug auf konkret sicherheits- bzw prüfungsrelevante Teile und nur in einem unbedingt erforderlichen Ausmaß, gewährt werden muss (vgl dazu etwa § 39 Abs 3 Z 2 letzter Satz). Die in Frage kommenden Prüfungsbereiche sollten außerdem im (mit der Vorabverständigung zu übermittelnden) Prüfplan bekannt gegeben werden. Schließlich wird auch angeregt, die Z 1 dahingehend zu ändern, dass sämtliche Kontrollmaßnahmen ausschließlich unter Mitwirkung der Einrichtung stattzufinden haben. Folglich sollten anstatt eines Zugriffs die behördlichen Rechte als „Audit" ausgestaltet werden, welches gemeinsam mit der Einrichtung durchgeführt wird, und nur die entsprechend relevanten Inhalte betrifft.

In diesem Zusammenhang darf nochmals auf den deutschen Gesetzesentwurf verwiesen werden: § 64 Abs 5 der deutschen Parallelregelung definiert das Verfahren in einem

solchen Fall näher wie folgt: *„[…] Die besonders wichtige Einrichtung hat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. […]"*.

In Bezug auf § 38 Abs 1 Z 3 und 4 ist anzumerken, dass die Richtlinie in Art 32 Abs 3 vorsieht, dass die Behörde jedenfalls auch den Zweck der Anfrage und die erbetenen Informationen bei der Ausübung ihrer Befugnisse anzugeben hat.

Vor dem Hintergrund der obigen Ausführungen zu Z 1 sollte insb die Z 5 angepasst werden. Nach diesem Wortlaut wäre die Behörde generell befugt, bei wesentlichen Einrichtungen „Ad-hoc-Prüfungen" durchzuführen, wobei dies **auch** Prüfungen umfassen soll, die aufgrund eines erheblichen Cybersicherheitsvorfalls oder Gesetzesverstoßes durch diese Einrichtung gerechtfertigt sind oder der Überprüfung einer übermittelten Selbstdeklaration dienen.

Diese Formulierung ist aus verschiedener Sicht problematisch: Zunächst ist mangels Definition unklar, was konkret unter einer „Ad-hoc-Prüfung" zu verstehen ist. Des Weiteren wäre eine solche nicht nur in abschließend gesetzlich geregelten Fällen möglich, sondern könnte – wie auch den Erläuterungen zu entnehmen ist – bei wesentlichen Einrichtungen grundsätzlich jederzeit vorgenommen werden. Wenn eine derartige Prüfung die Maßnahmen nach Z 1 bis 4 umfassen sollte, wäre gesetzlich oder in den Erläuterungen klarzustellen, dass diese Mindestanforderungen an das damit verbundene – verhältnismäßige – Vorgehen einzuhalten sind (vgl auch Art 32 Abs 1 der Richtlinie).

Es ist zu beachten, dass diese Maßnahmen auch gegenüber unabhängigen Stellen (vgl § 7 Abs 3) und im Ausmaß der Z 1 bis 4 auch gegenüber wichtigen Einrichtungen im Fall des Abs 2 ergriffen werden können, weshalb eine sorgfältige Abwägung der Verhältnismäßigkeit möglicher Eingriffe, insbesondere auch im Hinblick auf die Datenverarbeitung nach §§ 42, 43 unbedingt erforderlich ist.

Aus rechtsstaatlicher Sicht ist hier eine dringende Anpassung vorzunehmen, da anderenfalls im Anwendungsbereich dieses Gesetzes ein überschießender, umfassender Zugriff auf Systeme möglich wäre, der sonst den zuständigen (Strafverfolgungs-)Behörden mit gerichtlichem Durchsuchungsbeschluss (siehe auch Anmerkungen zu § 42 und 43) vorbehalten ist.

6.2. Einfluss auf das Anwaltsgeheimnis

Die vorgesehenen Kontrollrechte der Behörde sind von zentraler Bedeutung für die Anwaltschaft, da hier ua weitreichend in die Rechte der Mandantinnen und Mandanten eingegriffen werden kann.

Zur formellen Durchführung wird angemerkt, dass auch § 38 Abs 1 Z 2 und Z 5 nur nach vorheriger Verständigung der betroffenen Einrichtung durchgeführt werden sollen.

Wird diese Kontrolle bei Einrichtungen (zB Cloud Provider) durchgeführt, die auch Daten von Rechtsanwältinnen und Rechtsanwälten beinhalten, muss gewährleistet werden, dass die Meldepflicht des § 40 RL-BA eingehalten werden kann.

Darüber hinaus müssen allfällige Kontrollen derart durchgeführt werden, dass das Anwaltsgeheimnis als Pfeiler des Rechtsstaats und Kern des *fair trial*-Grundsatzes des Art 6 EMRK, und konkret der § 9 Abs 2 RAO und die prozessualen Maßnahmen des § 321 Abs 1 Z 3 und 4 ZPO, § 157 Abs 1 Z 2 und Abs 2 StPO sowie der Umgehungsschutz des § 157 Abs 3 StPO nicht verletzt werden.

Es ist ebenso sicherzustellen, dass diese Pflichten auch auf die unabhängigen Stellen, die allfällige Prüfungen begleiten können, überbunden werden.

6.3. Unabhängigkeit der Behörde

Mit Blick auf Art 58 Abs 1 lit b, e, f DSGVO, in der den nationalen Datenschutzbehörden ebenfalls umfangreiche Kontroll- und Einsichtsrechte gewährt werden, ist im Vergleich zum NISG 2024 auszuführen, dass der Zweck der unabhängigen Datenschutzbehörde die Wahrung der datenschutzrechtlichen Bestimmungen ist. Darüber hinaus gibt es in der DSGVO bzw dem DSG keine Möglichkeit der Datenschutzbehörde, Daten an Dritte weiterzugeben, wie es in § 43 (siehe auch Anmerkungen unten) der Fall ist.

Der Bundesminister für Inneres als Cybersicherheitsbehörde (vgl § 4) ist politisch verantwortlich, und nicht unabhängig, wie dies bei der Datenschutzbehörde der Fall ist. Es ist daher eine dem Gesetzeszweck entsprechende Einschränkung der Aufsichts- und Kontrollrechte der gegenständlichen Behörde vorzunehmen. Dies kann dadurch ausgeführt werden, dass die Cybersicherheitsbehörde als neue (unabhängige) Behörde eingerichtet wird, oder die Befugnisse einer unabhängigen Behörde übertragen werden.

7. Zu § 39

Die Rechte des Überwachungsbeauftragten (§ 39 Abs 3 Z 2) sollten ebenso (wie zu § 38 unter Punkt 6.1 ausgeführt) auf Auditrechte beschränkt werden, die gemeinsam und in Zusammenschau mit der Einrichtung ausgeübt werden.

Die Cybersicherheitsbehörde ist weiters befugt, mit Verfahrensanordnung unter Setzung einer angemessenen Frist Maßnahmen anzuordnen, die solche zur Beendigung von Zuwiderhandlungen gegen gesetzliche Verpflichtungen umfassen. Die nachweisliche Umsetzung der Maßnahmen kann auch mit Bescheid aufgetragen werden. Im Fall der Nichtbefolgung ist die Behörde befugt, Durchsetzungsmaßnahmen gem § 39 Abs 4 vorzunehmen. Rechtsmittel gegen diese Entscheidungen der Cybersicherheitsbehörde haben gem § 41, abweichend von § 13 VwGVG, keine aufschiebende Wirkung. Da dies nachteilige Auswirkungen auf wichtige Abläufe und Systeme der Einrichtungen haben kann, sollte die aufschiebende Wirkung beibehalten werden. Dies insb, um allfällige Schäden, die durch einen Bescheid, der später aufgehoben oder abgeändert wird, zu minimieren.

Der unter 6. beschriebene Anpassungsbedarf verdeutlicht sich angesichts dieser möglichen Durchsetzungsmaßnahmen. Es ist für Einrichtungen essentiell, Rechtssicherheit zu haben und Maßnahmen nachvollziehen zu können, um ihre Rechte auch effektiv wahrnehmen zu können.

8. Zu § 42

Die NIS2-Richtlinie bietet für die vorgeschlagenen §§ 42 und 43 keine derart umfassende Grundlage. So sieht die Richtlinie zwar eine Zusammenarbeit der CSIRTs (Art 10) und eine

Internationale Zusammenarbeit (Art 17) vor, jedoch nur im Einklang mit dem Datenschutzrecht der Union und nicht in der Breite, wie es der vorliegende Entwurf des NISG vorsieht. Zwar ist es aus datenschutzrechtlicher Sicht geboten, dass der nationale Gesetzgeber Rechtsgrundlagen für die Verarbeitung personenbezogener Daten schafft, hier ist jedoch sehr kritisch zu hinterfragen, ob eine Verarbeitung in diesem Umfang erforderlich ist.

Insb in Hinblick auf Informationen, die Geschäfts- oder Betriebsgeheimnisse enthalten (zB unternehmerische Aufzeichnungen) ist ein Erfordernis aus einem Cybersicherheits-Aspekt nicht einleuchtend. Darüber hinaus werden die Kategorien personenbezogener Daten nur demonstrativ aufgezählt („insbesondere"), was zur Folge hat, dass auch kategorisierte (Kunden-)Daten der Einrichtungen (gem Art 9 DSGVO), sowie – wie bereits erwähnt – Daten, die vom Anwaltsgeheimnis umfasst sind, von der Verarbeitung betroffen werden können. Die Erläuterungen geben zwar an, dass die Datenkategorien abschließend und die Datenarten demonstrativ aufgezählt wurden, dies spiegelt weder der Gesetzestext wider, noch unterscheidet die DSGVO zwischen „Datenkategorien" und „Datenarten"; es ist daher unklar, welche Aufzählung deklarativ und welche taxativ ist.

Im Sinne der Pflicht zur Datenminimierung (Art 5 Abs 1 lit c DSGVO) muss eine Einschränkung auf technische Daten und solche personenbezogenen Daten, die unbedingt erforderlich sind, um beispielsweise einen Cybersicherheitsvorfall aufzuklären, normiert werden. Grundsätzlich sollte davon ausgegangen werden und dies auch im Gesetz festgehalten, dass die Pflichten der Cybersicherheitsbehörde auch ohne Verarbeitung personenbezogener Daten (ggf mit Ausnahme von IP-Adressen) durchgeführt werden können.

9. Zu § 43

Aufbauend auf den – wie bereits ausgeführt – zu umfassenden Rechten, personenbezogene Daten zu verarbeiten, normiert § 43 das Recht, diese Daten an Dritte weiterzugeben – auch dies ohne entsprechende Grundlage in der NIS2-RL.

Die Weiterleitung der personenbezogenen (!) Daten – und eben nicht nur technische Informationen – an einen derart weiten Empfängerkreis kann nach Auffassung des ÖRAK keinesfalls gutgeheißen werden. Nicht nur im Hinblick auf den Schutz des bereits mehrfach erwähnten Anwaltsgeheimnisses müssen insb auch bei Übermittlung der Daten an Sicherheitsbehörden (Abs 1 Z 4), Staatsanwaltschaften und Gerichte (Abs 1 Z 5) die entsprechenden prozessualen Rahmenbedingungen eingehalten werden. Andernfalls könnten in der Praxis beispielsweise Strafverfolgungsbehörden über die Cybersicherheitsbehörde ohne Weiteres Zugriff auf Daten bekommen, die sie im ordentlichen Verfahren nicht oder nur mit gerichtlicher Bewilligung erhalten können.

Eine Übermittlung personenbezogener Daten (inkl Geschäfts- oder Betriebsgeheimnissen, kategorisierter Kundendaten, etc) an Behörden im Ausland (Abs 1 Z 6, Abs 2) ist jedenfalls abzulehnen. Eine Weiterleitung an andere Einrichtungen (Abs 3), die beispielsweise Konkurrenzunternehmen sind, sowie zwischen CSIRTs (Abs 4) sollte ausschließlich ohne Personenbezug, Identifizierbarkeit und Geschäfts- oder Betriebsgeheimnissen der betroffenen Einrichtung durchgeführt werden.

Zusammenfassend sollte eine Weiterleitung von Daten ausschließlich auf 1. Technische Daten, 2. Daten ohne Personenbezug, und 3. Daten ohne Geschäfts- oder Betriebsgeheimnisse, eingeschränkt werden.

Nach Auffassung des ÖRAK muss die Umsetzung der NIS2-RL einerseits sicherstellen, dass gesetzlich normierte Rechte, wie der Schutz des Anwaltsgeheimnisses, und der Datenschutz (Einschränkung der Verarbeitung und keine Weitergabe der Daten) gewahrt werden, und andererseits der Anwendungsbereich – insb bei Selbstverwaltungskörpern, Konzernunternehmen und in der Lieferkette – für betroffene österreichische Einrichtungen klargestellt werden.

Wien, am 30. April 2024

Der Österreichische Rechtsanwaltskammertag

Dr. Armenak Utudjian
Präsident

Österreichische Tierärztekammer

An das
Bundeskanzleramt
Abteilung 1/8
Ballhausplatz 2
1010 Wien

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

Bearbeiter/-in: KAD Mag. Nicole Hafner-Kragl
Mag. Elisabeth Kaufmann
oe@tieraerztekammer.at
Wien, 30.04.2024

Stellungnahme zum Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024
GZ 2024-0.220.735

Sehr geehrte Damen und Herren!

Die Österreichische Tierärztekammer erstattet zum Ministerialentwurf betreffend Bundesgesetz, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden, folgende

S t e l l u n g n a h m e.

Zu § 24 – Wesentliche und wichtige Einrichtungen

Der Geltungsbereich des Gesetzes erstreckt sich auf Einrichtung, die als wesentlich bzw. wichtig eingeordnet werden. Aus den Erläuterungen geht hervor, dass diese Einstufung von zwei Faktoren abhängig ist, nämlich
*- ob eine Einrichtung zumindest einem der **Sektoren** des § 2, die in den Anlagen 1 und 2 dieses Bundesgesetzes näher spezifiziert werden, zuzuordnen ist und*
*- ob sie ein **mittleres oder großes Unternehmen** ist (sofern die Einstufung als wichtige oder wesentliche Einrichtung nicht bereits größenunabhängig erfolgt).*

Die Österreichische Tierärztekammer ist als Standesvertretung aller österreichischen Tierärztinnen und Tierärzte dazu berufen, die wirtschaftlichen und sozialen Interessen aller Tierärztinnen und Tierärzte zu vertreten. Neben dem eigenen Wirkungsbereich erstreckt sich das Aufgabengebiet der Kammer auch auf einen übertragenen Wirkungsbereich, der im Wesentlichen die Führung der Tierärzteliste beinhaltet.

Die Österreichische Tierärztekammer geht davon aus, dass Sie nicht Adressat dieses Gesetzes ist, da sie weder unter die wesentlichen Einrichtungen iSd § 24 Abs 1 noch unter die Definition wichtiger Einrichtungen iSd § 24 Abs 2 fällt. Darüber hinaus stellt die Österreichische Tierärztekammer auch keine Einrichtung im Sektor der öffentlichen Verwaltung darf, die unter vollständiger Aufsicht des Bundes/Landes steht. Dieser übertragene Wirkungsbereich ist aus unserer Sicht nicht ausreichend dafür, dass die Österreichische Tierärztekammer als „Einrichtung der Öffentlichen Verwaltung auf Bundesebene“ anzusehen ist, zumal der Zweck der Einrichtung in der Interessensvertretung liegt und nicht in der Erfüllung im öffentlichen Interesse liegender Aufgaben.

Auch in Art 2 Abs. 2 lit f. sublit. ii der Richtlinie (EU) 2022/255 welcher den Anwendungsbereich der Richtlinie normiert, wird auf Einrichtungen der öffentlichen Verwaltung abgestellt, „die nach einer risikobasierten Bewertung Dienste erbringt, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnten“.

Um Rechtsunsicherheiten zu vermeiden, ersuchen wir um eine Klarstellung, wonach die Kammern der freien Berufe explizit im Gesetzestext vom Anwendungsbereich ausgenommen werden, wie etwa Gemeinden, Gemeindeverbände sowie Einrichtungen des Universitäts-, Hochschul- und Schulwesens.

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

Der konkrete Umfang der in § 38 Abs. 1 angeführten Aufsichtsmaßnahmen der Cybersicherheitsbehörde ist aus unserer Sicht nicht ausreichend präzisiert. Es geht aus dem Entwurf nicht hervor, welche Vorgänge von der behördlichen Einschau erfasst sein sollen. Weiters erachten wir einen direkten Zugriff auf IT-Systeme gemäß der Richtlinie als nicht erforderlich und überschießend. Aus unserer Sicht darf hier ohne einen richterlichen Beschluss nicht auf ein System des Unternehmens zugegriffen werden.

Die Österreichische Tierärztekammer ersucht höflich um Berücksichtigung der vorgenannten Einwände.

Mit freundlichen Grüßen

Mag. Kurt Frühwirth e.h.
Präsident der Österreichischen Tierärztekammer

ÖSTERREICHISCHE
ZAHNÄRZTE
KAMMER

Körperschaft öffentlichen Rechts
Mitglied der Fédération Dentaire Internationale

An das
Bundeskanzleramt
Sektion I - Präsidium
Abteilung I/8 - Technologie- und Daten Management, Cybersicherheit und Krisenrechenzentrum

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

Via Website an Parlamentsdirektion

Wien, 30. 4. 2024
KAD HR Dr. Kr/Mag. Ro.-

Betreff: 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

Sehr geehrte Damen und Herren!

Zum im Betreff genannten Begutachtungsentwurf gibt die Österreichische Zahnärztekammer binnen offener Frist folgende Stellungnahme ab:

Die geplante rechtzeitige innerstaatliche Umsetzung der NIS-2-Richtlinie ist zwar grundsätzlich zu begrüßen, es ergeben sich jedoch aufgrund der weiten und teilweise unbestimmten Formulierungen einige Unklarheiten, insbesondere wer überhaupt vom NISG 2024 betroffen ist.

Der Entwurf normiert in § 24 Abs. 3 Z 3, dass Einrichtungen, die ermächtigt sind, im Rahmen ihrer gesetzlich übertragenen Aufgaben Bescheide zu erlassen, die Rechte Einzelner im grenzüberschreitenden Personen-, Waren-, Dienstleistungs- oder Kapitalverkehr berühren, Einrichtungen im Sektor der öffentlichen Verwaltung sind. Ausgenommen sind ausdrücklich Gemeinden und Gemeindeverbände, sowie die in Abs. 6 genannten Einrichtungen (so gelten etwa Universitäten „nicht als wesentliche oder wichtige Einrichtungen“).

Die Österreichische Zahnärztekammer regt daher aus gleichheitsrechtlichen Gründen dringend an, von der in der NIS-2-Richtlinie enthaltenen Öffnungsklausel Gebrauch zu machen und auch die Selbstverwaltungskörper wie die Kammern der freien Berufe, zu denen auch die Österreichische Zahnärztekammer zählt, in die Ausnahmebestimmung des Abs. 6 **ausdrücklich aufzunehmen**. Alternativ sollte eine Klarstellung in den Erläuterungen zum Gesetz erfolgen.

Im Falle, dass die Selbstverwaltungskörper nicht vom Anwendungsbereich dieses Gesetzes ausgenommen werden, möchten wir hinsichtlich der Bestimmungen der §§ 38, 39 und 42, 43 allgemein folgende Bedenken äußern:

Die Zuständigkeiten der Cybersicherheitsbehörde im vorliegenden Entwurf sind äußerst umfassend ausgestaltet. Derart weitreichende Befugnisse einer nicht unabhängigen Behörde stehen im offenkundigen Widerspruch zu den Grundsätzen eines Rechtsstaats. Insbesondere ist unklar, welche Vorgänge von einer behördlichen Einschau gemäß § 38 Abs. 1 Z 1 erfasst sein sollen und wie bzw. in welchem Umfang ein sogenannter „Fernzugriff“ erfolgen kann. Weiters ist mangels Definition unklar, was konkret unter einer „Ad-hoc-Prüfung“ in Z 5 zu verstehen ist.

Auch die Ausgestaltung der Datenschutzbestimmungen des § 42 und der Ermächtigungen zur Datenübermittlung des § 43 ist aus Sicht der Österreichischen Zahnärztekammer überschießend.

Im Übrigen schließt sich die Österreichische Zahnärztekammer der Stellungnahme der Bundeskonferenz der Freien Berufe Österreichs (BUKO) vollinhaltlich an.

Die Österreichische Zahnärztekammer ersucht, die aufgeworfenen Punkte zu berücksichtigen und verbleibt

mit vorzüglicher Hochachtung

Dr. B. Vetter-Scheidl
Präsidentin

1010 Wien | Kohlmarkt 11/6 | T + 43 - (0) 5 05 11 - 0 | F + 43 - (0) 5 05 11 - 1167
office@zahnaerztekammer.at | www.zahnaerztekammer.at