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