Land Wien
Amt der Wiener Landesregierung
Magistratsdirektion - Recht

Bundesministerium für Inneres

Rathaus
1010 Wien
Telefon: +43 1 4000 82318
Fax: +43 1 4000 99 82310
post@md-r.wien.gv.at
wien.gv.at

MDR - 1696806-2024-8
Entwurf eines Bundesgesetzes zur Sicherstellung eines hohen Resilienzniveaus von kritischen Einrichtungen (Resilienz kritischer Einrichtungen-Gesetz - RKEG)
Begutachtung;
Stellungnahme

zur Zahl 2024-0.271-366

Wien, 21. Jänner 2025

Zu dem mit Schreiben vom 17. Dezember 2024 übermittelten Entwurf eines Bundesgesetzes wird wie folgt Stellung genommen:

Eingangs ist festzuhalten, dass die gesetzte Frist bis längstens 14. Jänner 2025 in Anbetracht der Feiertage keine eingehende und erschöpfende Auseinandersetzung mit dem Inhalt des Entwurfes ermöglicht und sich das Amt der Wiener Landesregierung daher weitere Stellungnahmen vorbehält.

Vorbemerkung

Die Richtlinien (EU) 2022/2555 (im Folgenden: NIS-2-RL) sowie 2022/2557 (im Folgenden: RKE-RL) stehen in engem Zusammenhang und sollen miteinander verbunden betrachtet werden (vgl. Art. 1 Abs. 2 RKE-RL). Dennoch könnte es zu Konflikten, Überschneidungen und Redundanzen kommen, auf die nachfolgend näher eingegangen wird. Zwar wird im Begutachtungsentwurf des Resilienz kritischer Einrichtungen-Gesetzes (im Folgenden: RKEG) in § 7 Abs. 2 Z 3 und in § 9 Abs. 2 Z 7 auf Gemeinsamkeiten der beiden Richtlinien verwiesen bzw. soll im Rahmen der Strategieausarbeitung für das RKEG (§ 9) der Ablauf einer Koordination zwischen den Behörden ausgearbeitet werden, jedoch findet sich in weiterer Folge im Entwurf kein direkter Zusammenhang zur NIS-2-RL. Diesbezüglich beispielhaft zu erwähnen ist, dass im geforderten Resilienzplan alle Bedrohungen aufgelistet sein könnten und nicht nur jene der RKE-RL.
Die Relevanz einer Verzahnung der Gesetze zur Umsetzung der NIS-2-RL und der RKE-RL wird auch in den Erläuterungen zum RKEG angesprochen. Es wird davon ausgegangen, dass auch bei der Erstellung der Verordnungen und Fact-Sheets sowie bei deren Umsetzung auf diese Herausforderung Rücksicht genommen wird.

Der vorliegende Gesetzesentwurf enthält zahlreiche Rückverweise auf die beiden genannten EU-Richtlinien. Dies erschwert die konkrete Auslegung und Rechtsanwendung, zumal die Komplexität in Hinblick auf das Zusammenwirken des RKEG mit der noch umzusetzenden NIS-2- RL weiter steigen wird. Wünschenswert wäre eine Harmonisierung bzw. zeitliche Zusammenlegung der Begutachtungen der Entwürfe für das RKEG und das Netz- und Informationssystemsicherheitsgesetz 2024 (im Folgenden: NISG 2024).

Beispielhaft wird auf die Diskrepanz hingewiesen, dass laut dem vorliegenden Entwurf des RKEG die Ermittlung kritischer Einrichtungen durch Bescheid des Bundesministers für Inneres erfolgen soll, während sich im Gegensatz dazu gemäß Entwurf des NISG 2024 Einrichtungen zu registrieren haben.

Das RKEG verfolgt den All-Gefahren-Ansatz. Es ist daher davon auszugehen, dass die in der NIS-2-RL umfassten Gefährdungen bzw. Bedrohungen, die gemäß dem Entwurf des NISG 2024[1] ebenfalls auf einem gefahrenübergreifenden Ansatz beruhen, der auf den Schutz von Netz- und Informationssystemen und deren physischer Umwelt vor Cybersicherheitsvorfällen abzielt, im RKEG (bereits vor Entwicklung der Strategie gem. § 9 RKEG) Eingang finden sollten.

Weiters fordert das RKEG ein umfassendes Risikomanagementsystem, das auf Basis von nationalen Risikoanalysen für die jeweiligen Sektoren erstellt werden muss. Im Entwurf des NISG 2024 wird wiederum in § 35 Abs. 2 Z 2 (Erheblicher Cybersicherheitsvorfall) auf die möglichen Auswirkungen von Cybersicherheitsvorfällen auf die Umwelt, die öffentliche Ordnung und Sicherheit, die öffentliche Gesundheit oder die Gesundheit der Bevölkerung oder eines großen Personenkreises abgestellt. Auch wird im RKEG betreffend die Strategie für die Resilienz kritischer Einrichtungen (§ 9) darauf abgezielt, Abhängigkeiten zu anderen Sektoren darzustellen bzw. zu berücksichtigen, und auch dies bereits aus Sicht der dortigen Behörde. Hier fehlt (ebenfalls) der Konnex zum NISG 2024.

Zu § 1 (Kompetenzdeckungsklausel)

Die Formulierung dieser Bestimmung enthält in Abs. 1 neben der Erlassung und Aufhebung weiterhin den Begriff der „Änderung" und ist daher als dynamische Kompetenzdeckungsklausel anzusehen. Damit wird das System der bestehenden bundesstaatlichen Kompetenzverteilung unterlaufen. Dies wird vom Land Wien abgelehnt. Es wird darauf hingewiesen, dass von Seiten der Länder eine statische Kompetenzdeckungsklausel gefordert wird (siehe den Beschluss der Landeshauptleutekonferenz vom 3. November 2023).

Der Entwurf federt die Dynamik der Klausel dadurch ab, dass in § 1 Abs. 2 eine Reihe von Bestimmungen des Entwurfes angeführt werden, deren Änderung durch Bundesgesetz nur dann kundgemacht werden darf, wenn die Länder der Kundmachung zustimmen. Angeführt sind die §§ 5, 6 Abs. 2 sowie die §§ 12 Abs. 1 Z 2, 20, 22 Abs. 6 und 23 des Entwurfes. Die zuletzt genannte Gruppe von Bestimmungen ist nur erfasst, sofern sich die Änderungen auf Behörden und sonstige Stellen der öffentlichen Verwaltung der Länder beziehen. Diese Vorgangsweise entspricht nicht dem

[1] vgl. § 32 Abs. 2 Z 2 dieses Entwurfs, Stand Juni 2024.

Vorschlag des Amtes der Wiener Landesregierung, eine dem Vorbild des Art. 14b Abs. 4 Bundes-Verfassungsgesetz (B-VG) entsprechende Bestimmung aufzunehmen, da keine entsprechenden Mitwirkungsrechte der Länder vorgesehen sind. Die Bestimmung wäre dahingehend zu ergänzen, dass die Länder ausreichend Gelegenheit erhalten, an der Vorbereitung der betreffenden Gesetzesvorhaben des Bundes mitwirken zu können.

Auch wird § 24 Abs. 2 in der Aufzählung in § 1 Abs. 2 nicht erwähnt. Im Hinblick darauf, dass eine Änderung der gesetzlich vorgesehenen Berichtspflicht Auswirkungen auf Behörden der Länder hat, wäre § 24 Abs. 2 zu ergänzen. Angemerkt wird, dass der Entwurf des NISG 2024, Stand Juni 2024, bei einer Änderung des korrespondierenden Paragrafen, nämlich § 44 Abs. 1, eine Zustimmung der Länder vorsieht.

Darüber hinaus wird angeregt, eine Zustimmung der Länder bei einer Änderung des § 12 für den gesamten Abs. 1 und nicht bloß bezogen auf Abs. 1 Z 2 vorzusehen, zumal auch eine Änderung der weiteren Ziffern des Abs. 1 einen Einfluss auf die Zuständigkeit der Länder haben könnte.

Zu § 2 Abs. 1, § 3 Z 6, § 10 Abs. 1 und Abs. 2 Z 3, § 11 Abs. 1, Abs. 2 Z 2 und Abs. 5, § 14 Abs. 2 sowie § 18 Abs. 3

Der Gesetzesentwurf sieht in den genannten Gesetzesstellen einen Verweis auf den Anhang der RKE-RL vor. Aus Gründen der Rechtsklarheit wird angeregt, dem RKEG einen eigenen, selbstständigen Anhang anzufügen, damit die innerstaatliche Regelung präzise und ein Rückgriff auf die Richtlinie selbst nicht erforderlich ist.

Zu § 2 Abs. 2

§ 2 Abs. 2 besagt, dass Angelegenheiten, die in den Anwendungsbereich der NIS-2-RL fallen, vom RKEG unberührt bleiben. Die Erläuterungen zu § 2 Abs. 2 führen unter anderem Folgendes aus:

„Im Hinblick darauf, dass die NIS-2-RL das Thema Cybersicherheit ausreichend abdeckt, soll ihr Inhalt - unbeschadet der besonderen Regelungen für Einrichtungen, die im Bereich der digitalen Infrastruktur tätig sind (vgl. Art. 8 RKE-RL) - vom Anwendungsbereich der RKE-RL ausgenommen werden und soll die RKE-RL explizit nicht für Angelegenheiten gelten, die unter die NIS-2-RL fallen (Art. 1 Abs. 2 RKE-RL). Aufgrund der engen Beziehung bzw. Überschneidungen zwischen Cybersicherheit und physischer Sicherheit kritischer Einrichtungen sowie angesichts der Bedeutung der Cybersicherheit für die Resilienz kritischer Einrichtungen (vgl. auch Erwägungsgrund zur RKE-RL) sind die Mitgliedstaaten jedoch verpflichtet, für eine koordinierte Umsetzung der NIS-2-RL und der RKE-RL zu sorgen (siehe dazu auch die Erläuterungen im Allgemeinen Teil). Demnach ist in Abs. 2 vorgesehen, dass Angelegenheiten, die unter die Bestimmungen der NIS-2-RL fallen, vom Anwendungsbereich des gegenständlichen Gesetzes ausgenommen werden. So sollen etwa - auch mit Blick auf den der NIS-2-RL ebenfalls zugrunde liegenden „All-Gefahren-Ansatz“ - Maßnahmen zum (physischen) Schutz eines Serverraums, in dem die Informationstechnik einer Einrichtung untergebracht ist, lediglich dem NIS-Regelungsregime unterliegen.“

Gemäß § 11 Abs. 1 RKEG hat der Bundesminister für Inneres Einrichtungen die unter bestimmten Voraussetzungen den im Anhang der RKE-RL gelisteten Sektoren und Teilsektoren zugehören, bescheidmäßig als kritisch einzustufen.

§ 11 Abs. 5 regelt, dass in dem gemäß Abs. 1 erlassenen Bescheid kritische Einrichtungen in den im Anhang der RKE-RL gelisteten Sektoren digitale Infrastruktur, Bankwesen und Finanzmarktinfrastrukturen darüber zu informieren sind, dass die Verpflichtungen gemäß Abs. 6 sowie den §§ 14, 15, 17 und 19 auf sie keine Anwendung finden.

Entgegen der eingangs zitierten Bestimmung des § 2 Abs. 2 wonach Angelegenheiten, die unter die NIS-2-RL fallen, von diesem Gesetz unberührt bleiben, ist in § 11 somit doch vorgesehen, dass Einrichtungen der gelisteten Sektoren und Teilsektoren, unter bestimmten Voraussetzungen mittels Bescheid als kritisch einzustufen sind.

Gemäß § 11 Abs. 5 sollen einzelne gelistete Sektoren, wie etwa die digitale Infrastruktur, welche bescheidmäßig als kritische Einrichtung festgestellt wurden, darauf hingewiesen werden, dass einige Bestimmungen des RKEG auf sie nicht anwendbar sind.

Daraus ist abzuleiten, dass auch Einrichtungen, die unter die NIS-2-RL fallen, im Anwendungsbereich des RKEG liegen, auch wenn einige Bestimmungen dieses Gesetzes - zumindest für die angeführten Sektoren - nicht anwendbar sind.

Im Hinblick auf das in den Materialien zum RKEG mehrfach angesprochene Bestreben, die Regelungen der NIS-2-RL und der RKE-RL in der gesetzlichen Umsetzung zu verzahnen und eng aufeinander abzustimmen, wird vorgeschlagen die Formulierung des § 2 Abs. 2 RKEG nochmals zu überarbeiten und das Zusammenspiel zwischen NIS-2-RL und RKE-RL im Gesetz klarer darzustellen.

Zu § 3 (Begriffsbestimmungen)

Zu Z 3 „Sicherheitsvorfall“: Das RKEG umfasst den Bereich der physischen Sicherheit kritischer Einrichtungen. Der Begriff des Sicherheitsvorfalls in § 3 Z 3 subsumiert darunter allerdings alle Arten von Vorfällen, auch jene, die in den Anwendungsbereich der NIS-2-RL fallen und gemäß § 2 Abs. 2 RKEG daher vom RKEG nicht berührt werden sollen (vgl. dazu auch Erwägungsgrund 9 der RKE-RL). Eine Abgrenzung in der gegenständlichen Begriffsbestimmung zu den Sicherheitsvorfällen gemäß dem Entwurf des NISG 2024 wird angeregt.

Zu Z 5 „kritische Infrastrukturen“: Schutzgut des RKEG ist die kritische Infrastruktur, wobei davon gemäß § 3 Z 5 Folgendes umfasst ist: Objekte, Anlagen, Ausrüstungen, Netze, Systeme oder Teile davon, die für die Erbringung eines wesentlichen Dienstes erforderlich sind. In den Erläuterungen ist in diesem Zusammenhang ausgeführt, dass auch technische Gefahren in Betracht zu ziehen sind. Dazu zählen laut den Erläuterungen fehlerhafte Software, manipulierte Hardware, Datenmissbrauch etc.[2].

[2] vgl. S. 22 der Erläuterungen zum Entwurf des RKEG.

Die Sicherheitsanforderungen in Bezug auf Netze und Hardware (das sind Netz- und Informationssysteme[3] iSd Art. 6 Z 1 NIS-2-RL) werden bereits umfassend durch die NIS-2-RL reguliert. Art. 1 Abs. 2 der RKE-RL sieht in diesem Zusammenhang Folgendes vor:

„[…] Unbeschadet des Artikels 8 der vorliegenden Richtlinie gilt diese Richtlinie nicht für Angelegenheiten, die unter die Richtlinie (EU) 2022/2555 fallen. Angesichts der Beziehung zwischen physischer Sicherheit und Cybersicherheit kritischer Einrichtungen gewährleisten die Mitgliedstaaten eine koordinierte Umsetzung der vorliegenden Richtlinie und der Richtlinie (EU) 2022/2555."

Diese Vorgabe wurde zwar in § 2 RKEG vorgesehen, aber - wie erwähnt - weder im Gesetz noch in den Erläuterungen weiter entsprechend umgesetzt.

Der Umstand, dass das RKEG nicht für Netz- und Informationssysteme gilt, ist weder aus dem RKEG selbst, noch aus den Erläuterungen abzuleiten. Die Erläuterungen sehen - wie zuvor ausgeführt – sogar Gegenteiliges vor (Arg: Software, manipulierte Hardware und Datenmissbrauch).

Vor diesem Hintergrund wird eine an den deutschen Referentenentwurf zur Umsetzung der RKE-RL angelehnte Abänderung des Gesetzesentwurfs wie folgt angeregt:

„5. „kritische Infrastrukturen": Objekte, Anlagen, Ausrüstungen~~, Netze, Systeme~~ oder Teile eines Objekts, einer Anlage, einer Ausrüstung, ~~eines Netzes oder eines Systems,~~ die für die Erbringung eines wesentlichen Dienstes erforderlich sind;"

Der Umstand, dass die Sicherheit von Netz- und Informationssystemen nicht vom RKEG erfasst ist, sollte zumindest in den Erläuterungen entsprechend festgehalten werden.

Diese Klarstellung wird für erforderlich erachtet, da diesfalls in der (RKE-)Risikoanalyse (§ 3 Z 8 RKEG) keine Risiken (§ 3 Z 7 RKEG) i. Z. m. Netz- und Informationssystemen zu berücksichtigen sind, da diese durch das NIS-2-Risikomanagement abgebildet werden. Sollte eine kritische Einrichtung (§ 3 Z 1 RKEG) ein Audit (§ 3 Z 13 RKEG) durchzuführen haben (vgl. § 20 Abs. 1 letzter Satz RKEG), würde sich diese Einschränkung auch unmittelbar auf den Auditumfang auswirken.

Angemerkt wird weiters, dass in den Erläuterungen explizit darauf hingewiesen wird, dass für Z 5 eine andere Definition als im Sicherheitspolizeigesetz (SPG) gewählt wird. Alternativ zur oben vorgeschlagenen Formulierung könnte daher eine Angleichung der beiden Definitionen überlegt werden.

Zu Z 6 „wesentlicher Dienst": Der Bundesminister für Inneres kann per Verordnung weitere Dienste festlegen, die z. B. den Bereich der öffentlichen Gesundheit berühren. Es wird angeregt zu verankern, dass diese Festlegungen gemeinsam mit Vertreter*innen, wie z. B. Bundesministerien, der jeweils betroffenen Sektoren zu erfolgen haben.

[3] Darunter ist Hardware zu verstehen.

Zu § 4 Abs. 2 (Verfassungsbestimmung; Einrichtung des Bundesministers für Inneres als oberstes Organ)

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

Darüber hinaus wird die hohe Befugniskonzentration kritisch betrachtet. Der in den Erläuterungen enthaltene Verweis auf § 35 Abs. 2 Datenschutzgesetz als Begründung für eine Konzentration der Aufgaben des Bundesministers für Inneres als zuständige Behörde nach dem RKEG geht insofern ins Leere, als die Datenschutzbehörde zwar bezogen auf die Angelegenheiten des Datenschutzes als oberstes Organ der Republik fungiert, über diese Aufgaben hinausgehend jedoch anders als der Bundesminister für Inneres über keine Befugnisse und Funktionen verfügt.

Zu § 7

Zu Abs. 1 Z 2: Die angeführten Cyber-bezogenen Risiken, Bedrohungen und Vorfälle sind in der NIS-2-RL geregelt, wie auch die zugehörigen Meldeverpflichtungen.

Im Zusammenwirken mit § 7 Abs. 2 Z 3 ist die Formulierung des Abs. 1 Z 2 verwirrend, zumal dort die Übermittlung der Daten an jene Behörde angeführt wird, die für die Umsetzung des Art. 8 Abs. 1 der NIS-2-RL zuständig ist und dies eine doppelte Meldeverpflichtung implementiert.

Zu Abs. 5 und 6: Die unterschiedlichen Fristen führen dazu, dass eine durchgängige Nachvollziehbarkeit der Verarbeitung von Daten nach Wegfall eines gültigen Bescheides nicht mehr für den gesamten Zeitraum der Datenvorratshaltung nach Wegfall eines gültigen Bescheids gegeben ist. Es wird eine Vereinheitlichung der Fristen auf drei Jahre angeregt.

Zu § 8

Die in § 8 vorgesehene Form der Veröffentlichung von Sicherheitsvorfällen unter Angabe der in Abs. 1 genannten Inhalte ist als äußerst kritisch anzusehen, da mit der Veröffentlichung (abgesehen von möglichen schweren Reputationsschäden und der Beeinträchtigung schutzwürdiger Geheimhaltungsinteressen eines betroffenen Unternehmens) weitere Risiken i. S. d. § 3 Z 7 RKEG einhergehen oder schlimmere entstehen können, wie dies etwa durch eine erhöhte Aufmerksamkeit von

Bedrohungsakteur*innen oder Nachahmungseffekten der Fall sein kann. Es sollte daher vorgesehen werden, dass die Veröffentlichung soweit als möglich ohne Nennung des betroffenen Unternehmens erfolgt bzw. gesetzlich nähere Rahmenbedingungen zur Kommunikation von Sicherheitsvorfällen definiert werden, die den schutzwürdigen Geheimhaltungsinteressen der kritischen Einrichtungen Rechnung tragen.

Angeregt wird folgende Anpassung des Wortlautes von § 8 Abs. 1 vorzunehmen:

„(1) Nach Anhörung der von einem Sicherheitsvorfall betroffenen kritischen Einrichtung kann der Bundesminister für Inneres personenbezogene Kontakt- und Identitätsdaten sowie sonstige erforderliche Informationen, die mit einer Meldung zu einem Sicherheitsvorfall in Zusammenhang stehen, nach Abwägung der Auswirkungen auf die ~~Betroffenen~~ ***kritische Einrichtung*** *veröffentlichen, um die Öffentlichkeit über Sicherheitsvorfälle zu unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung oder zur Bewältigung von Sicherheitsvorfällen* ***unbedingt*** *erforderlich ist ~~oder die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt~~. Die Veröffentlichung darf nur insoweit erfolgen, als diese keine Gefahr* ***für die kritische Einrichtung selbst oder*** *für die öffentliche Ordnung oder Sicherheit oder für die nationale Sicherheit darstellt. Die Veröffentlichung hat unter größtmöglicher Berücksichtigung schutzwürdiger Geheimhaltungsinteressen der kritischen Einrichtung zu erfolgen.“*

Hinsichtlich der vorgesehenen Bekanntgabe personenbezogener Daten wird weiters angemerkt, dass hier wohl in aller Regel ein Datenschutzinteresse der bzw. des Betroffenen gegeben ist. Die Bekanntgabe eines entsprechenden („anonymen“) Abteilungspostfachs (z. B. Email-Adresse) sollte in der Regel genügen.

Zu § 9

Zu Abs. 1: Die vorgesehene anlassbezogene bzw. längstens alle vier Jahre stattfindende Anpassung steht im Spannungsfeld zu den Fristen zur Umsetzung der NIS-2-RL, die diesbezüglich einen Zeitraum von fünf Jahren vorsieht. Es wird angeregt, die nationalen Bestimmungen über die Anpassung zu vereinheitlichen.

Die vorgesehene „Gelegenheit zur Äußerung“ für die jeweils betroffenen Bundesministerien, Länder und Interessenvertretungen erscheint unzureichend, da damit die sektorspezifischen Gegebenheiten nur unzureichend einfließen können. Es sollte vielmehr eine Verpflichtung zur Einbindung und Abstimmung vorgesehen werden.

Zu Abs. 3: Inwiefern die starke Einbindung des Nationalrates - wie in den Erläuterungen angeführt - durch die bloße Übermittlung innerhalb von drei Monaten ab Beschlussfassung durch die Bundesregierung gegeben ist, kann nicht nachvollzogen werden, da keine Anhörung i. S. einer Begutachtung bzw. Einbindung als anzuhörende Partei bzw. keine Erörterung im Nationalen Sicherheitsrat vorgesehen ist.

Zu § 10

Es ist erforderlich, dass die Länder - so wie bei der der Erstellung der Strategie für die Resilienz kritischer Einrichtungen (§ 9) - auch bei der Auswahl der einzelnen Risiken und der Erstellung der Risikoanalyse durch den Bundesminister für Inneres verbindlich einbezogen werden. Die Einbeziehung der Länder ist geboten, damit regionale und lokale Risiken ausreichend berücksichtigt werden. Eine Berücksichtigung dieser Risken ausschließlich in den Risikoanalysen der kritischen Einrichtungen ist nicht ausreichend, da gemäß §§ 14 und 15 die Risikoanalysen und die Resilienzpläne der kritischen Einrichtungen auf Grundlage der Risikoanalyse des Bundesministers für Inneres zu erfolgen haben.

Zu Abs. 2 Z 1: Der durch das hier zitierte Unionsverfahren gewährleistete Schutz gilt vor allem den Menschen, aber auch der Umwelt und dem Eigentum, einschließlich Kulturgütern, bei allen Arten von Naturkatastrophen und vom Menschen verursachten Katastrophen innerhalb oder außerhalb der Union, einschließlich der Folgen von Terroranschlägen, technischen, radiologischen und Umweltkatastrophen, Meeresverschmutzung oder akuten Krisen im Gesundheitsbereich. Im Falle der Folgen von Terroranschlägen oder radiologischen Katastrophen kann das Unionsverfahren lediglich Vorsorge- und Bewältigungsmaßnahmen abdecken.

Zu § 11

Zu Abs. 5: § 11 Abs. 5 normiert, dass kritische Einrichtungen in den im Anhang der RKE-RL gelisteten Sektoren digitale Infrastruktur, Bankwesen und Finanzmarktinfrastrukturen mit Bescheid zu informieren sind, welche Verpflichtungen nach dem vorliegenden Gesetzesentwurf auf sie keine Anwendung finden. Die in § 18 Abs. 3 des Gesetzesentwurfes vorgenommene Aufzählung dieser Verpflichtungen wurde in § 11 Abs. 5 insofern nicht vollständig übernommen, als die Abs. 7 und 8 des § 11 nicht angeführt sind, diese wären hinzuzufügen. Im Hinblick auf die nachstehende Stellungnahme zu § 18 Abs. 3 wären in § 11 Abs. 5 außerdem die §§ 20 bis 23 zu ergänzen.

Zu Abs. 6: Die Bekanntgabe einer zentralen Kontaktstelle einer kritischen Einrichtung ist nachvollziehbar und steht im Einklang mit dem Gesetzeszweck. Anders zu sehen ist dies hinsichtlich der Daten einer konkreten Ansprechperson. Im Sinne von (dauerhaft oder auch kurzfristig) wechselnden Personenzuständigkeiten erscheint diese Vorgehensweise abträglich, sie wird auch nicht von der RKE-RL (vgl. Art. 9 Abs. 7) verlangt. Es wird angeregt, im Gesetz anstelle der Benennung einer konkreten Ansprechperson Kontaktdaten wie E-Mail-Adressen und (ständig besetzte, zentrale) Telefonnummern sowohl im konkreten Anlassfall als auch für den Kontakt zur Abstimmung vorzusehen. Analog wäre auch die Strafbestimmung (§ 22 Abs. 1 Z 1) entsprechend anzupassen.

Zu Abs. 10: Die Ermittlung der kritischen Einrichtungen durch den Bundesminister für Inneres ist mit keiner Frist versehen, obwohl die RKE-RL eine Frist bis 17. Juli 2026 festlegt (vgl. Art. 6 Abs. 1). Dadurch ergibt sich für die kritischen Einrichtungen kein planbarer Zeitraum, bis wann ein möglicher Bescheid übermittelt wird und die notwendigen Maßnahmen nach §§ 14, 15 und 17 umgesetzt werden müssen. Ebenso erscheint ein Zeitraum von neun Monaten ab Bescheidübermittlung für die Risikoanalyse nach § 14 sowie die Umsetzung aller notwendigen Maßnahmen nach § 15 spätestens nach

zehn Monaten ab Bescheidübermittlung weder realistisch noch umsetzbar. Eine sektorspezifische bzw. einrichtungsbezogene Erweiterung dieser Frist wäre nicht nur wünschenswert, sondern erscheint notwendig.

Zu § 12 Abs. 1

Diese Bestimmung enthält in Abs. 1 Z 2 eine Ausnahme bezüglich der Länder, Gemeinden und Gemeindeverbände. Dazu wird angeregt, jedenfalls in den Erläuterungen klarzustellen, dass diese Begriffe organisatorisch zu verstehen sind und damit alle Organe der Länder und Gemeinden erfasst sind, unabhängig von dem Wirkungsbereich, in dem sie tätig werden.

Zur Verdeutlichung des in den Erläuterungen festgehaltenen Willens des Gesetzgebers[4], Behörden der Länder, der Gemeinden sowie der Gemeindeverbände, vom Anwendungsbereich des RKEG auszunehmen, darf angeregt werden, diese Ausnahme explizit in § 2 Abs. 3 des Entwurfes aufzunehmen.

Zu § 13

Zum Begriff der Resilienzmaßnahmen: Das RKEG verwendet mehrfach den Begriff der Resilienzmaßnahmen (wie etwa in § 13 Z 2, 6 und 7, § 15, § 20 Abs 5, § 22 RKEG). Der Begriff der Resilienzmaßnahme ist - anders als der Begriff der Risikomanagementmaßnahmen des NISG 2024 - inhaltlich nicht ausgestaltet bzw. definiert.

Eine nähere Ausgestaltung des Begriffs sollte dahingehend erfolgen, dass zumindest die abstrakten Zielvorgaben einer Konkretisierung zugeführt werden, wie dies im deutschen Referentenentwurf zur Umsetzung der RKE-RL der Fall ist.

Ein Ausgangspunkt dafür ist in der Legaldefinition der Resilienz (§ 3 Z 2 RKEG) zu finden, diese umfasst die Fähigkeit einer kritischen Einrichtung, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, einen solchen abzuwehren, darauf zu reagieren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall zu bewältigen oder sich von einem solchen Vorfall zu erholen.

So könnten (etwa in § 15 RKEG) für den

obigen Punkt 1) konkrete Maßnahmen zur Notfallvorsorge wie z. B. Notfallpläne und Szenarienentwicklungen auf der Grundlage der Risikoanalyse i. S. d. § 10 RKEG,

obigen Punkt 2) konkrete Maßnahmen der physischen Sicherheit,

obigen Punkt 3) ein Resilienzplan auf der Grundlage der Risikoanalyse (§ 3 Z 8 RKEG), die wiederum auf den Risiken der Risikoanalyse i. S. d. § 10 RKEG beruht und für den

[4] vgl. S. 20 der Erläuterungen zum Entwurf des RKEG.

obigen Punkt 4) konkrete Maßnahmen zur Aufrechterhaltung des Betriebs, der Notstromversorgung sowie die Ermittlung alternativer Lieferketten vorgesehen werden.

Sektorspezifische Resilienzmaßnahmen: Zusätzlich könnte zur Erhöhung sowohl der Rechtssicherheit als auch der praktischen Umsetzbarkeit eine Konkretisierung der sektorspezifischen Resilienzmaßnahmen in Anlehnung an § 17 Abs. 2 NISG erfolgen. Die entsprechende Regelung im NISG lautet wie folgt:

„Gemeinsam mit ihren Sektorenverbänden können die Betreiber wesentlicher Dienste sektorenspezifische Sicherheitsvorkehrungen zur Gewährleistung der Anforderungen nach Abs. 1 vorschlagen. Der Bundesminister für Inneres stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Abs. 1 zu erfüllen."

Diese Möglichkeit zur sektorspezifischen Festlegung und Konkretisierung ist von maßgeblicher Bedeutung, da sich z. B. der Sektor Energie im Hinblick auf die Objektsicherheit, aber auch auf die Kritikalität ganz entscheidend von anderen Sektoren unterscheidet. Überlegt werden könnte beispielsweise folgende Formulierung, die etwa in einem neu zu schaffenden § 13 Abs. 2 RKEG umgesetzt werden könnte:

„(2) Gemeinsam mit ihren Sektorenverbänden können kritischen Einrichtungen sektorenspezifische Risikoanalysen und Resilienzmaßnahmen unter Berücksichtigung des § 10 zur Gewährleistung der Anforderungen nach §§ 14 und 15 vorschlagen. Dies kann auch die Ausnahmen von Verpflichtungen für kritische Einrichtungen iSd § 18 für den jeweiligen Sektor umfassen. Der Bundesminister für Inneres stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach §§ 14, 15 und 18 zu erfüllen."

Zu den Unterstützungsleistungen: Die gewählte „Kann"-Formulierung lässt viel Spielraum in der tatsächlichen Umsetzung zu. Vor dem Hintergrund, dass die technischen und organisatorischen Anforderungen an die kritischen Einrichtungen über weite Strecken unbestimmt sind, sollte in § 13 RKEG vorgesehen werden, dass zumindest die angeführten Punkte jedenfalls umgesetzt werden müssen bzw. sollte hinsichtlich der Unterstützungsmaßnahmen, die vom Bundesminister für Inneres zu erbringen sind, zwischen verpflichtenden und möglichen Unterstützungsmaßnahmen differenziert werden.

Verpflichtende Vorlagen, Muster und Guidelines sollten etwa für folgende Anforderungen verpflichtend bereitgestellt werden: Risikoanalyse (§ 3 Z 8), Resilienzplan (§ 3 Z 12), Mitarbeit bei der Normung mit Bezug auf die physische Sicherheit. Dies hätte den Vorteil, dass Umfang, Struktur und Format (siehe dazu etwa § 14 Abs. 1 erster Satz RKEG) der zu übermittelnden Unterlagen seitens des Bundesministers für Inneres dargestellt werden.

Die Verwendung dieser Vorlagen und Muster sollte jedoch weiterhin freiwillig erfolgen, um Unterschieden im Risikomanagement Rechnung tragen zu können.

Zu Z 7: Die Doppelrolle der Behörde wird hier deutlich: einerseits ist die Behörde jene Instanz, die Sachverhalte hinsichtlich der Einleitung von Strafverfahren anzeigt, andererseits ist sie berufen,

Beratungstätigkeiten, insbesondere betreffend die Beurteilung bereits durchgeführter Risikoanalysen, durchzuführen. Hier bedarf es einer Nachschärfung, da die Verpflichtung der kritischen Einrichtungen zur Übermittlung von Informationen und diversen Unterlagen bei Nichtentsprechen einer Selbstanzeige gleichkommt. Alternativ könnte die Trennung der Kompetenzen in unterschiedliche Behörden überlegt werden.

Zu Z 8: In den Erläuterungen wäre zu ergänzen, dass bei Durchführung von langfristigen strategischen Analysen betreffend Bedrohungen der physischen Sicherheit und Sicherheitsvorfällen, den im jeweiligen Wirkungsbereich betroffenen Bundesministerien, den betroffenen Ländern sowie den in Betracht kommenden Interessenvertretungen Gelegenheit zur Äußerung zu geben ist.

Auch lässt die Formulierung hinsichtlich der Äußerungsmöglichkeit von betroffenen Bundesministerien, Ländern sowie in Betracht kommenden Interessensvertretungen „bei Bedarf" zu viel Spielraum, da dies voraussetzt, dass die entsprechenden Fachexpertisen in der Behörde vorhanden sind. Angeregt wird, eine Beiziehung der betreffenden Stellen vorzusehen.

Zu Z 9: § 13 Z 9 sollte auch die Beratung bei der Auswahl der am besten geeigneten Fördertöpfe und/oder Forschungsprojekte umfassen. Überlegt werden könnte auch ein Kostenersatz für Maßnahmen, die aufgrund von RKE- Bestimmungen gesetzt werden müssen, die sich betriebswirtschaftlich aber nicht darstellen lassen.

Zu § 14 Abs. 1 und § 15 Abs. 1

Diese Bestimmungen enthalten Fristen für die Risikoanalyse (§ 14 Abs. 1: neun Monate ab bescheidmäßiger Einstufung, längstens jedoch alle vier Jahre) und für technische, sicherheitsbezogene und organisatorische Maßnahmen (§ 15 Abs. 1: zehn Monate nach bescheidmäßiger Einstufung). Diese Fristen erscheinen nicht stimmig (ab bescheidmäßiger Einstufung unterscheiden sich die Fristen nur um einen Monat). Es wäre zu bedenken, dass die Maßnahmen auf der Grundlage der Risikoanalyse zu treffen sind und es zu Überschneidungen kommen kann.

Die in § 14 Abs. 1 enthaltene Frist von neun Monaten ab bescheidmäßiger Einstufung für die Durchführung einer Risikoanalyse erscheint darüber hinaus jedenfalls zu kurz (vgl. auch die Ausführungen zu § 11 Abs. 10). Es sollte eine deutliche Verlängerung vorgesehen werden. Ebenso erscheint die Frist, die aufbereiteten Ergebnisse längstens binnen eines Monats an den Bundesminister für Inneres zu übermitteln, zu kurz, weshalb angeregt wird, diese auf zumindest drei Monate zu verlängern. Die Erstellung und die Aufbereitung der notwendigen Dokumente, erfordert einen nicht zu unterschätzenden Zeitaufwand, der in der vorgeschlagenen Frist nicht adäquat abgedeckt werden kann.

Hinsichtlich der Möglichkeit, bestehende oder aufgrund anderer rechtlicher Verpflichtungen erstellte Dokumente im Rahmen der Risikoanalyse zu verwenden, sofern sie den Anforderungen gemäß § 14 Abs. 1 und 2 gleichwertig sind, wird angemerkt, dass eine zu restriktive Auslegung der „Gleichwertigkeit" durch die Aufsichtsbehörde vermieden werden sollte, um unnötige Doppelarbeit zu verhindern. So könnte der Bundesminister für Inneres in diesem Zusammenhang z.B. bescheidmäßig geeignete Maßnahmen klar und transparent auftragen.

Auch die in § 15 Abs. 1 statuierte Frist von zehn Monaten nach bescheidmäßiger Einstufung zur Setzung von Maßnahmen im geforderten Umfang in bestimmten Fällen wird als deutlich zu kurz eingeschätzt. Beispielhaft kann angeführt werden, dass bei Ergreifen bestimmter Maßnahmen die Einholung von Sachverständigengutachten, eine Ausschreibung oder Ähnliches notwendig sein kann. In Abhängigkeit von den budgetären Planungen und den Budgetierungsintervallen können insbesondere bei großen Arealen oder einer hohen Anzahl an Standorten, die gesichert werden müssen, die verfügbaren Ressourcen nicht ausreichen. Darüber hinaus stellen spezifische technische Maßnahmen hohe Anforderungen an die technische Planungsphase, den Beschaffungsprozess und letztlich auch die bauliche Umsetzung. Es wird daher angeregt, die zeitliche Vorgabe von zehn Monaten für die Erstellung eines Maßnahmenplans zu präzisieren. Dieser Plan sollte auch die Möglichkeit beinhalten, die Umsetzung über einen längeren Zeitraum zu realisieren. Eine Verlängerung der Frist auf mindestens 18 Monate wird angeregt.

Angemerkt wird, dass auch die in § 20 Abs. 1 enthaltene Ermächtigung seitens des Bundesministers für Inneres innerhalb einer angemessenen Frist Nachweise für das Erfüllen der Anforderungen der §§ 14 und 15 bzw. die in § 20 Abs. 5 vorgesehene bescheidmäßige Nachbesserung in angemessener Frist für betroffene Einrichtungen nicht die Möglichkeit inkludiert, für Maßnahmen entsprechende Umsetzungszeitrahmen mit nachvollziehbarer Begründung vorzusehen.

In den Erläuterungen zu § 15 wird zudem angeführt, dass auch ohne ausdrückliche Anordnung Resilienzmaßnahmen dem Stand der Technik entsprechen sollen. Dies entspricht nicht der bisherigen in Österreich gelebten Praxis (vgl. z. B. den Bereich Brandschutz), das Erreichen von Schutzzielen zu verfolgen, was nicht zwingend die Umsetzung des letzten Standes der Technik bedeutet. Diese Forderung könnte womöglich als unverhältnismäßig angesehen werden. Sie ist mit Kosten für Betreiber*innen kritischer Infrastruktur verbunden. Es wird angeregt die Formulierung in den Erläuterungen anzupassen.

Bei der Organisation und Teilnahme an Sicherheitsüberprüfungen sowie Übungen zur Überprüfung der Notfallpläne sollte (in den Materialien) darauf verwiesen werden, dass diese bereits in vielen Branchen eingespielte Praxis darstellen, auf die aufgebaut werden kann.

Darüber hinaus wäre auch in § 14 Abs. 1 und § 15 Abs. 1 - analog zu § 11 Abs. 6 RKEG - jeweils auf die Rechtskraft des Bescheides i. S. d. § 11 RKEG abzustellen.

Zu § 14 Abs. 2

Um konkret auf die Wechselwirkungen eingehen zu können, müssen auch die konkreten wesentlichen Dienste der anderen Sektoren hinreichend bekannt sein. Auch die zugehörigen Risikoanalysen können wesentlich beim Erkennen von Wechselwirkungen hilfreich sein. Hier stellt sich die Frage, wie die entsprechenden Unterlagen den jeweiligen Unternehmen bekannt gemacht werden bzw. wer die Informationsdrehscheibe(n)-Funktion übernimmt.

Zu § 15

Zu Abs. 2 Z 4: Es ist unklar, wie die Berücksichtigung alternativer Lieferketten z. B. bei Komplettausfall eines Krankenhauses seitens der Betreiber*in von Statten gehen soll.

Zu Abs. 3: Die Frist von einem Monat für die Übermittlung des Resilienzplanes wird jedenfalls als zu kurz erachtet. Eine Fristverlängerung auf mindestens drei Monate wird angeregt.

Zu Abs. 4: Ein System zur Qualitätssicherung setzt die Verwertung entsprechender Erkenntnisse voraus und ist daher nur nach eingetretenem Anlassfall (vgl. Abs. 1) sinnvoll. Es wird angeregt, diese Bedingung zusätzlich in den Gesetzeswortlaut aufzunehmen. Angemerkt wird, dass die RKE-RL eine solche Qualitätssicherung generell nicht vorsieht.

Zu § 16

§ 16 normiert die Möglichkeit der Zuverlässigkeitsüberprüfung für Personen, die in sensiblen Bereichen kritischer Einrichtungen tätig sind oder eine entsprechende Tätigkeit anstreben.

Angemerkt wird, dass die vorgesehene Datenverarbeitung - zumal auch Daten über strafrechtliche Verurteilungen und Strafdaten umfasst sind - einen tiefen Eingriff in die Rechte und Freiheiten natürlicher Personen darstellt.

Abs. 1 bedarf daher im Sinne der Grundsätze der Zweckbindung und der Datenminimierung (Art. 5 Abs. 1 lit. b, c Datenschutz-Grundverordnung - DSGVO) sowie des besonderen Schutzes der gegenständlichen personenbezogenen Daten gem. Art. 10 DSGVO einer klareren Definition, in welchen Fällen die gegenständliche Zuverlässigkeitsprüfung zulässig ist.

Zum Zweck der gemäß Abs. 2 ff durchzuführenden Übermittlung (auch ist eine sichere Übermittlungsart zu wählen!) personenbezogener Daten an den Bundesminister für Inneres bedarf es der vor- und nachbereitenden Verarbeitung der gegenständlichen Personendaten durch die kritische Einrichtung. Rechtsnorm und Erläuterung sehen lediglich eine Einwilligung der betroffenen Person zur Überprüfung durch den Bundesminister für Inneres sowie zur wechselseitigen Übermittlung der entsprechenden Datenarten vor. Eine solche Einwilligung kann nur im Sinne des Art. 6 Abs. 1 lit. a DSGVO zur Verarbeitung der personenbezogenen Daten verstanden werden. Diese muss jedoch freiwillig sein. Die betroffene Person muss die echte und freie Wahl haben, ob sie in die Verarbeitung ihrer Daten einwilligt. Im beruflichen Kontext kann jedoch die Einwilligung zur Verarbeitung von Daten von Bewerber*innen oder Arbeitnehmer*innen in den meisten Fällen keine Rechtsgrundlage bilden, weil es (zumeist) am Erfordernis der echten und freien Wahl fehlt.

Die hier gesetzlich vorgesehene Einwilligung kann - wie schon die Problematik der in § 55 ff SPG normierten Einwilligung in eine Sicherheitsüberprüfung gezeigt hat - in der Praxis in vielen Fällen nicht die datenschutzrechtlichen Voraussetzungen erfüllen.

Art. 10 DSGVO erfordert für die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Strafdaten die Schaffung einer entsprechenden Rechtsnorm. Zudem weisen

auch Überlegungen zum Widerrufsrecht (Art. 7 Abs. 3 DSGVO) bzw. den Betroffenenrechten gemäß Art. 15 ff DSGVO auf diese Notwendigkeit hin. Die Schaffung einer Rechtsnorm, welche die Verarbeitung personenbezogener Daten gemäß § 16 Abs. 2 ff RKEG inklusive des Ergebnisses der Überprüfung gemäß § 16 Abs. 6 leg. cit. durch die kritische Einrichtung zulässt, ist erforderlich. Im Sinne der Schaffung von Rechtssicherheit für die kritische Einrichtung wird diese Rechtsnorm auch Aufbewahrungsfristen zu enthalten haben.

Zudem wird aufgrund der „Kann"-Bestimmung bezüglich der Wiederholung der Zuverlässigkeitsüberprüfung nach drei Jahren angeregt, diese Formulierung zu konkretisieren, da ansonsten Unklarheit hinsichtlich der Gültigkeit von bestehenden Zuverlässigkeitsüberprüfungen besteht.

Zu § 17

Zu Abs. 1 und 2: Abs. 1 normiert eine Meldepflicht kritischer Einrichtungen „bei Erfüllung der Voraussetzungen gemäß Abs. 2". Die Meldepflicht umfasst eine Erst- und eine Folgemeldung. Abs. 2 trägt dem Bundesminister für Inneres die Erlassung einer Verordnung auf, in der geregelt werden soll, wann ein Sicherheitsvorfall eine Meldepflicht gemäß Abs. 1 auslöst. Zum Verhältnis von Erst- und Folgemeldung lassen sich den Erläuterungen nähere Informationen entnehmen. Dabei wird aber nicht gesagt, welche Mindestinformationen die Erstmeldung enthalten muss. Eine diesbezügliche Ergänzung in den Erläuterungen wird angeregt.

Weiters ist anzumerken, dass Sicherheitsvorfälle mit Auswirkungen auf die Erbringung der kritischen Leistung sowohl Meldungen nach NISG als auch RKEG zur Folge haben können. Während die Meldung nach NISG im Gesundheitsbereich z. B. an Health CERT zur erfolgen hat, ist die Meldung nach dem RKEG gemäß § 17 RKEG an den Bundesminister für Inneres zu richten. Es haben somit in einer Krisensituation innerhalb relativ kurzer Fristen Meldungen an zwei separate Stellen zu erfolgen. Angeregt wird, die Meldung an eine einzelne Stelle oder eine Priorisierung der Meldungen vorzusehen.

Zu Abs. 2: Angeregt wird bei Z 1 zu berücksichtigen, dass innerhalb der Sektoren auch eine gegenseitige Hilfestellung möglich ist, sodass zwar eine prognostizierte Anzahl von Personen betroffen ist, aber durch getroffene Gegenmaßnahmen eine Kompensation erfolgen kann. Zu Z 2 wird angeregt, eine Meldung erst ab einer entsprechenden Dauer des Sicherheitsvorfalles schlagend werden zu lassen und diese sektorspezifisch zu definieren.

Zu Abs. 3: Es ist vorgesehen, dass Informationen, die erforderlich sind, um grenzüberschreitende Auswirkungen des Sicherheitsvorfalls zu bestimmen, ebenfalls zu übermitteln sind.

Um zeitnah betroffene andere Sektoren bzw. deren Einrichtungen kritischer Infrastruktur seitens des Bundesministers für Inneres informieren zu können, wird hier auch die Angabe von sektorübergreifenden Auswirkungen angeregt.

Zu Abs. 4: Die in § 17 Abs. 4 statuierte Frist von zwei Monaten für den Abschlussbericht wird als zu kurz angesehen. Oft benötigt z. B. die Ursachenermittlung eines Vorfalls umfangreiche

Untersuchungen und die Einholung von Sachverständigengutachten. All dies erfordert ein angemessenes Maß an Zeit. Angeregt wird eine Fristverlängerung auf mindestens sechs Monate vorzusehen.

Zu Abs. 5: § 17 Abs. 5 RKEG dient der Umsetzung des Art. 15 Abs. 4 RKE-RL. Dieser sieht vor, dass die zuständige Behörde der betreffenden kritischen Einrichtung die Informationen „sobald wie möglich" zu übermitteln hat. Vor diesem (wohl auch bereits unionsrechtlich gebotenen) Hintergrund sollte § 17 Abs. 5 RKEG wie folgt lauten:

„(5) Der Bundesminister für Inneres ist verpflichtet, auf Grundlage einer Meldung gemäß Abs. 1 den vom Sicherheitsvorfall betroffenen kritischen Einrichtungen sachdienliche Informationen, insbesondere über die wirksame Abwehr und Bewältigung des betreffenden Sicherheitsvorfalls, ***sobald wie möglich*** *zur Verfügung zu stellen."*

Zu § 18 Abs. 3

In den Erläuterungen wird angeführt, dass für die kritischen Einrichtungen in den Sektoren digitale Infrastruktur, Bankwesen und Finanzmarktinfrastrukturen u. a. auch das Aufsichts- und Durchsetzungs- bzw. Sanktionsregime gemäß den vorgeschlagenen §§ 20 bis 23 nicht zur Anwendung gelangen soll. Die §§ 20 bis 23 sind in § 18 Abs. 3 nicht angeführt und wären daher zu ergänzen.

Darüber hinaus wird in diesem Zusammenhang nochmals auf die Notwendigkeit einer bestmöglichen Abstimmung bzw. Harmonisierung der Gesetzesentwürfe zur Umsetzung der NIS-2-RL und der RKE-RL hingewiesen.

Zu § 20

Zu Abs. 1 und Abs. 2: Anstelle der in Abs. 1 vorgesehenen „*angemessenen*" Frist wird angeregt auf Basis des ermittelten Risikos und des Zeitaufwands etwaig umzusetzender Investitionen konkrete Fristen anzuführen, z. B. bei geringem Risiko: 12-24 Monate, bei mittlerem Risiko: 6 - 18 Monate).

Die Durchführung von Audits sollte hingegen - im Sinne eines abgestuften Vorgehens - erst dann verlangt werden können, wenn weitere von der kritischen Einrichtung angeforderte Nachweise nicht ausreichen, um beurteilen zu können, ob die Resilienzmaßnahmen i. S. d. § 15 RKEG ausreichend umgesetzt sind. Der Auditauftrag sollte in Bescheidform, unter Angabe der konkreten Infrastruktur (§ 3 Z 5 RKEG), der Auditkriterien, sowie der zu erlangenden Nachweise i. S. d. ÖNORM 19011[5] ergehen.

Zu Abs. 3: Zwar ist angeführt, dass Vor-Ort-Kontrollen „unter möglichster Schonung der Rechte der betroffenen Einrichtung und Dritter auszuüben" sind, es wird aber dennoch angeregt zu ergänzen, dass auch der Betrieb der Einrichtung nicht gestört werden soll, somit also Priorität gegenüber der Kontrolle hat.

Zu § 21

[5] https://www.austrian-standards.at/de/shop/onorm-en-iso-19011-2018-11-01~p2445239.

Angemerkt wird, dass in § 7 des Entwurfs des NISG 2024 im Gegensatz zum gegenständlichen Gesetzesentwurf von „unabhängigen Stellen und unabhängigen Prüfern" gesprochen wird. Darüber hinaus wird in § 51 Z 2 lit. 3 des Entwurfs des NISG 2024 die Verordnung über qualifizierte Stellen außer Kraft gesetzt.

Angesichts der Bedeutung der Cybersicherheit für die Resilienz kritischer Einrichtungen und im Sinne der Einheitlichkeit sollte möglichst dafür gesorgt werden, dass die Umsetzungen der NIS-2-RL und der RKE-RL kohärent sind.

Vor dem Hintergrund, dass einer qualifizierten Stelle die Berechtigung zur Durchführung von Audits auch entzogen werden kann, wird vorgeschlagen, dass über den Umstand eines möglichen Entzugs der Berechtigung auch die kritischen Einrichtungen entsprechend informiert werden, um nicht frustrierte Prüfaufwände zu erzeugen. Frustrierte Aufwände entstehen etwa dann, wenn die Berechtigung zur Durchführung eines Audits in einem laufenden Audit entzogen und die kritische Einrichtung die Prüfung erneut durchführen müsste, da der Auditor nicht mehr als qualifizierte Stelle gilt. Dies insbesondere vor dem Hintergrund, dass Audits teils über einen sehr langen Zeitraum (mehrere Jahre) durchgeführt werden. Angeregt wird § 21 Abs. 5 RKEG wie folgt anzupassen:

„(5) Bei Wegfall oder Nichteinhaltung der gemäß Abs. 2 normierten Erfordernisse ist die qualifizierte Stelle vom Bundesminister für Inneres darauf hinzuweisen, dass sie diese binnen einer angemessenen Frist nachweislich zu erfüllen hat. Wird dieser Nachweis nicht innerhalb der festgelegten Frist erbracht, hat der Bundesminister für Inneres den Bescheid gemäß Abs. 1 zu widerrufen ***und wird die qualifizierte Stelle von der Liste iSd Abs. 6 gestrichen. Die qualifizierte Stelle hat die von ihr geprüften, kritischen Einrichtungen umgehend sowohl über die Einleitung eines Verfahrens zum Widerruf als auch über den erfolgten Widerruf des Bescheides und die Streichung von der Liste zu informieren****."*

Zum Audit: Die ÖNORM 19011 definiert den Begriff des Audits wie folgt:

„Audit systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen (…) und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die Auditkriterien (…) erfüllt sind."

§ 3 Z 13 RKEG definiert ein „Audit" wie folgt:

„eine systematische und unabhängige Überprüfung der Einhaltung der Verpflichtungen gemäß den §§ 14 und 15, insbesondere durch einen Bewertungsbesuch, samt Dokumentation der Ergebnisse und Auflistung vorgeschlagener Korrekturmaßnahmen (§ 21) in einem Prüfbericht durch qualifizierte Stellen."

Von einem Audit i. S. d. ÖNORM nicht erfasst sind (wie die obigen Definitionen zeigen) Korrekturmaßnahmen. Damit Korrekturmaßnahmen vorgeschlagen werden könnten, sind die Grundsätze der Verhältnismäßigkeit i. S. d. § 15 RKEG zu berücksichtigen. Da die qualifizierte Stelle die Verhältnismäßigkeit nicht bewerten kann, kann diese auch keine Korrekturmaßnahmen vorschlagen. Darüber hinaus ist weder im NISG noch im NISG 2024 in diesem Zusammenhang vorgesehen, dass ein

Prüfergebnis auch Korrekturmaßnahmen zu enthalten hat.[6] Es würde sich um eine Art „*gold plating*" handeln, da diese Anforderung in Art. 21 Abs. 1 lit. b RKE-RL schlicht nicht vorgesehen ist, gleichzeitig würden die Auditkosten merklich erhöht werden.

Darüber hinaus wird angeregt die maximale Auditdauer (in Personentagen) im Bescheid etwa im Lichte der Norm ISO 27006 mitanzugeben.[7]

Die bescheidmäßige Ausgestaltung der Auditkriterien bzw. des Auditumfangs erscheint auch deshalb notwendig, da i. S. d. § 18 RKEG eine kritische Einrichtung durch sektorspezifische Rechtsakte über ein zumindest gleichwertiges Resilienzniveau verfügen kann, was dazu führt, dass diesfalls § 15 RKEG nicht anwendbar und somit keinem Audit (§ 3 Z 13 RKEG) zugänglich ist. Zur klaren Abgrenzung des Audits (auch für die qualifizierte Stelle) erscheint eine Eingrenzung daher notwendig.

Zu §22

Zu Abs. 1 Z 1: Vgl. die Anmerkung zu § 11 Abs. 6.

Zu Abs. 1 Z 10 und Z 11: Hier sollten Ausnahmen hinzugefügt werden für den Fall, dass das Betreten bzw. Besichtigen aus unvorhersehbaren Gründen nicht möglich ist bzw. den laufenden Betrieb nachteilig beeinträchtigen könnte. Beispielsweise könnte trotz vorangegangener Ankündigung (Terminvereinbarung) just unmittelbar davor ein sicherheitsrelevanter Vorfall eintreten oder es etwa zu einem (kurzfristigen) Personalausfall kommen, sodass die Personalkapazität der Aufrechterhaltung des Betriebes bzw. Ergreifung entsprechender Maßnahmen Priorität gegenüber der Kontrolle einzuräumen ist (siehe hierzu auch die Anmerkung zu § 20 Abs. 3)

Zu Abs. 2: Auch wenn Art. 22 der RKE-RL Sanktionen vorsieht, die „wirksam, verhältnismäßig und abschreckend" sind, erscheint ein Strafmaß von 7 Mio. Euro dennoch äußerst hoch. Anders als bei der NIS-2-RL wird hier seitens der EU-Richtlinie kein Mindestmaß für die vorzusehende Höchststrafe determiniert (wie auch in den Erläuterungen zu § 22 zutreffend bemerkt wird).

Zu Abs. 6: Diese Bestimmung sieht vor, dass § 22 keine Anwendung findet auf Behörden und sonstige Stellen der öffentlichen Verwaltung, insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen. Es wird vorgeschlagen, diesbezüglich die Formulierung des Gesetzesentwurfs zu § 45 Abs. 5 NISG 2024, Stand Juni 2024, zu übernehmen.

Zu § 23

Zum angewandten Prinzip des „naming and shaming" wird angemerkt, dass dies insbesondere im Bereich der öffentlichen Verwaltung zweckwidrig und überschießend erscheint. Auch birgt es - trotz des letzten Satzes dieser Bestimmung - die Gefahr, vulnerable Stellen potentiellen „Gefährder*innen"

[6] § 17 Abs. 3 letzter Satz NISG sieht in diesem Zusammenhang folgendes vor: „*der durchgeführten Überprüfungen durch qualifizierte Stellen, einschließlich der dabei aufgedeckten Sicherheitsmängel an den Bundesminister für Inneres*".

[7] Es ist davon auszugehen, dass eine vergleichsweise geringe Anzahl von Audits durchzuführen sein wird, was wohl dazu führen wird, dass unter den qualifizierten Stellen kein Wettbewerb stattfinden wird. Kritische Einrichtungen wären ohne Angabe der maximalen Auditdauer vom Gutdünken der qualifizierten Stelle abhängig.

kenntlich zu machen. Diesbezüglich wäre auf eine verhältnismäßige Maßnahmensetzung bzw. Ausgestaltung Bedacht zu nehmen.

Zu § 24

Es darf (nochmals) darauf hingewiesen werden, dass die Behörde einerseits Beratungsagenden wahrnimmt, andererseits auch Sachverhalte hinsichtlich der Einleitung von Strafverfahren anzuzeigen hat. Jegliche Anfragen kritischer Einrichtungen in bestimmten Umsetzungsfällen könnten hier bereits einen Verdacht einer Verwaltungsübertretung auslösen und kämen einer Selbstanzeige gleich. Es wird angeregt, die Trennung der beiden Kompetenzen im Gesetz zu berücksichtigen.

Weitere Anmerkungen

Sensible Dokumente wie z. B. Risikoanalysen oder Resilienzpläne könnten Informationen enthalten, die im Falle einer verpflichtenden Veröffentlichung oder Beauskunftung negative Einflüsse auf die Resilienz kritischer Einrichtungen haben. Eine Prüfung der Anwendbarkeit von § 6 Informationsfreiheitsgesetz, BGBl. I Nr. 5/2024, und entsprechende Klarstellungen in den Erläuterungen werden daher angeregt.

Zu den Kosten

Die Umsetzung der Resilienzmaßnahmen (§ 15 RKEG) und die Aufrechterhaltung der Resilienz (§ 3 Z 2 RKEG) samt Qualitätssicherungsmaßnahmen (§ 15 Abs. 4 RKEG) geht für die kritischen Einrichtungen mit erheblichen Kosten einher.

Angemerkt wird, dass mit den durch dieses Gesetz vorgesehenen Resilienzmaßnahmen neben dem Resilienzniveau für den Geschäftsbetrieb auch Maßnahmen zu treffen sind, die für gewöhnlich der Staat im Rahmen der Daseinsvorsorge für die Bevölkerung erbringt. Es könnte daher überlegt werden diesbezüglich eine Kostenerstattungsregel in § 15 RKEG aufzunehmen.

Zum Zweck der Reduzierung des Umsetzungs- und Betriebsaufwandes wäre es wichtig, die Pflichten des NISG 2024 und des RKEG inhaltlich zusammenzuführen, um einen optimalen Schutz der kritischen Infrastruktur und der Sicherheit der Netz- und Informationssysteme gewährleisten zu können. Zur Sicherstellung einer einfachen Rechtsanwendung sollten die Vorgaben für kritische Infrastrukturen zur physischen Sicherheit im RKEG und zur Informationssicherheit im NISG 2024 umfassend aufeinander abgestimmt werden.

Festzuhalten ist, dass das RKEG (voraussichtlich teils sehr hohe) finanzielle Mehrbelastungen, vor allem in folgenden Themenfeldern, mit sich bringen wird:

Resilienzpläne und Maßnahmen: Der Aufbau einer BCM-Struktur zur Bewältigung der gesetzlichen Vorgaben ist unerlässlich. Dies erzeugt jedenfalls einen Mehrbedarf an Expert*innen (bei allen dem RKEG unterworfenen Einrichtungen). Aus derzeitiger Sicht kann aber nicht beurteilt werden, ob überhaupt eine ausreichende Anzahl von entsprechenden Expert*innen am Markt verfügbar sein wird.

Zuverlässigkeitsüberprüfungen (§ 16): Die dem RKEG unterliegenden Einrichtungen müssen für die Zuverlässigkeitsüberprüfungen einen Pauschalbetrag bezahlen. Daher ist auch bei einer sehr selektiven Vorgehensweise in Bezug auf die Personengruppen und unter Berücksichtigung der Fluktuation sowie des Wiederholungszykluses alle drei Jahre dennoch jährlich beispielsweise bei den Wiener Linien mit einem Aufwand im sechsstelligen Bereich zu rechnen.

Objektschutzmaßnahmen (§ 15 Abs. 2): Bei einem Teil der Standorte mit höherer Kritikalität wird ein zusätzlicher Personaleinsatz notwendig sein. Hier ist z. B. im Fall der Wiener Linien von jährlichen Personal-Mehrkosten in Höhe von mindestens 1,5 Mio. Euro auszugehen.

Darüber hinaus sind an allen Standorten Objektschutzmaßnahmen zu treffen, allerdings in unterschiedlicher Qualität und Ausmaß (aufgrund bereits bestehender Maßnahmen bzw. Kritikalität i. V. m Risikobeurteilung). Diese Mehrbelastung durch die Umsetzung der Maßnahmen (Investitionen über vier Jahre) liegt z. B. nach derzeitigem Stand für alle Standorte der Wiener Linien in einem deutlich zweistelligen Mio. Bereich.

Abschließend muss darauf hingewiesen werden, dass die dem Entwurf beigefügte WFA zwar eine Kostenschätzung für die durch die Zuständigkeit des Bundesministers für Inneres resultierenden Kosten für den Bund enthält, entgegen Art. 1 Abs. 3 der Vereinbarung zwischen dem Bund, den Ländern und den Gemeinden über einen Konsultationsmechanismus und einen künftigen Stabilitätspakt der Gebietskörperschaften, BGBl. I Nr. 35/1999, jedoch keine Darstellung der aus der Zuständigkeit der Bezirksverwaltungsbehörden und Verwaltungsgerichte der Länder für Verwaltungsstrafverfahren nach dem RKEG resultierenden Kosten für die Länder.

Aufgrund der im Entwurf statuierten Zuständigkeit für Verwaltungsstrafverfahren nach dem RKEG ist jedenfalls mit zusätzlichen finanziellen Ausgaben seitens der Länder zu rechnen. Zum aktuellen Zeitpunkt sind diese in Ermangelung einer abschätzbaren Fallzahl jedoch noch nicht konkret quantifizierbar. Dementsprechend muss sich das Land Wien das Recht vorbehalten, in weiterer Folge gemäß Art. 5 Abs. 1 Z 2 der Vereinbarung zwischen dem Bund, den Ländern und den Gemeinden über einen Konsultationsmechanismus und einen künftigen Stabilitätspakt der Gebietskörperschaften, BGBl. I Nr. 35/1999, die Ersatzpflicht des Bundes für die erwachsenden Mehraufwendungen geltend zu machen.

Für den Landesamtsdirektor:

Mag. Mag. Mag. Michael Uhrmacher, LL.M.

Mag.ª Birgit Eisler
Senatsrätin

Ergeht an:

1. Präsidium des Nationalrates
2. alle Ämter der Landesregierungen
3. Verbindungsstelle der Bundesländer
4. MA 64
   mit dem Ersuchen um Weiterleitung
   an die einbezogenen Dienststellen
5. MA 53
   zur Veröffentlichung auf der
   Stadt Wien-Website