1 von 35

Entwurf

Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs:

Die Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl. Nr. L 345 vom 23.12.2008 S. 75, CELEX-Nr.: 32008L0114, (im Folgenden: ECI-RL) sah ein Verfahren für die Ausweisung europäischer kritischer Infrastrukturen (ausschließlich) im Energie- und Verkehrssektor vor, deren Störung oder Zerstörung erhebliche grenzüberschreitende Auswirkungen in mindestens zwei Mitgliedstaaten hätte. Eine im Jahr 2019 durchgeführte Evaluierung der ECI-RL hat jedoch gezeigt, dass aufgrund des zunehmend vernetzten und grenzüberschreitenden Charakters von Tätigkeiten, bei denen kritische Infrastrukturen genutzt werden, Schutzmaßnahmen einzelner Objekte zur Verhinderung sämtlicher Störungen nicht ausreichen. Die Europäische Kommission kam daher zum Schluss, dass ein Ansatz verfolgt werden müsse, der sowohl die bessere Berücksichtigung von Risiken ermöglicht als auch die Rolle und Verpflichtungen von kritischen Einrichtungen als Erbringer von für das Funktionieren des Binnenmarktes wesentlichen Diensten einheitlich festlegt.

Vor diesem Hintergrund wurden am 16. Dezember 2020 im Rahmen der EU-Cybersicherheitsstrategie neue legislative Vorschläge mit dem Ziel präsentiert, die Widerstandsfähigkeit von Einrichtungen, die essenzielle gesellschaftliche Funktionen oder wirtschaftliche Tätigkeiten im Binnenmarkt erbringen, gegen Risiken und Bedrohungen zu erhöhen.

Nach dem erfolgreichen Abschluss der Verhandlungen wurden die Rechtstexte am 27. Dezember 2022 als Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl. Nr. L 333 vom 27.12.2022 S. 164, CELEX-Nr.: 32022L2557, (im Folgenden: RKE-RL) sowie als Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148, ABl. Nr. L 333 vom 27.12.2022 S. 80, CELEX-Nr.: 32022L2555, (im Folgenden: NIS-2-RL) im EU-Amtsblatt veröffentlicht und sind beide Richtlinien am 16. Jänner 2023 in Kraft getreten.

Mit der RKE-RL wurde die ECI-RL aufgehoben sowie ersetzt und erfolgte eine Erweiterung sowohl des Anwendungsbereichs als auch des Umfangs der ECI-RL. Die RKE-RL folgt großteils der Systematik der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. Nr. L 194 vom 19.07.2016 S. 1, (im Folgenden: NIS-1-RL), dh. der Vorgängerrichtlinie zur NIS-2-RL. Sie verfolgt dabei einen „All-Gefahren-Ansatz“, was bedeutet, dass sie alle relevanten natürlichen und vom Menschen verursachten Risiken, darunter Unfälle, Naturkatastrophen, feindliche Bedrohungen, einschließlich terroristischer Straftaten, und Notsituationen im Bereich der öffentlichen Gesundheit, wie etwa Pandemien, abdeckt. Darin unterscheidet sie sich erheblich von der ECI-RL, die sich in erster Linie auf den Terrorismus fokussierte.

Anders als die ECI-RL stützt sich die RKE-RL aufgrund ihres Ziels, Anwendungsbereichs und Gegenstands sowie der zunehmenden wechselseitigen Abhängigkeiten und der notwendigen Schaffung einheitlicher Ausgangsbedingungen für kritische Einrichtungen auf Art. 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), BGBl. III Nr. 86/1999, in dem die Angleichung der Rechtsvorschriften zur Verbesserung des Binnenmarkts vorgesehen ist. Die grenzüberschreitenden

wechselseitigen Abhängigkeiten zwischen den Diensten, die über kritische Infrastrukturen in den nunmehr von der Richtlinie umfassten elf Sektoren erbracht werden, führen dazu, dass sich eine Störung in einem Mitgliedstaat auch auf andere Mitgliedstaaten und die gesamte Union auswirken kann. Um sicherzustellen, dass alle entsprechenden Einrichtungen den Resilienzanforderungen dieser Richtlinie unterliegen, und um diesbezügliche zwischenstaatliche Unterschiede zu verringern, wurde es als wichtig erachtet, harmonisierte Vorschriften festzulegen, die eine einheitliche Ermittlung kritischer Einrichtungen in der Union ermöglichen und die es den Mitgliedstaaten dennoch erlauben, den Aufgaben und der Bedeutung dieser Einrichtungen auf nationaler Ebene angemessen Rechnung zu tragen.

Vor dem Hintergrund dieser Ausführungen ist demnach beabsichtigt, durch die RKE-RL einen unionsrechtlichen Rahmen zu schaffen, der im Wesentlichen darauf abzielt, die Resilienz bzw. physische Widerstandsfähigkeit kritischer Einrichtungen, die für wichtige gesellschaftliche Funktionen oder wirtschaftliche Tätigkeiten im Binnenmarkt unerlässliche Dienste erbringen, zu stärken und ihre Schwachstellen zu verringern, indem ein harmonisiertes Mindestmaß an Verpflichtungen festgelegt wird und kohärente sowie gezielte Unterstützungs- und Aufsichtsmaßnahmen vorgesehen werden. Konkret sollen kritische Einrichtungen ihre Fähigkeit verbessern, Sicherheitsvorfälle zu verhindern, sich davor zu schützen, darauf zu reagieren, die Folgen solcher Vorfälle zu begrenzen, Sicherheitsvorfälle zu bewältigen sowie sich von solchen Vorfällen zu erholen. Dabei soll im Sinne eines „All-Gefahren-Ansatzes“ die Resilienz kritischer Einrichtungen gegenüber allen natürlichen und vom Menschen verursachten Risiken sichergestellt werden (siehe auch oben).

Angesichts der Zusammenhänge zwischen Cybersicherheit und physischer Sicherheit wurde der RKE-RL sowie der NIS-2-RL ein möglichst kohärenter „All-Gefahren-Ansatz“ zugrunde gelegt und soll durch eine abgestimmte nationale Umsetzung der beiden Richtlinien die isolierte Betrachtung physischer und digitaler Risiken überwunden werden. Zudem soll eine Verzahnung zwischen RKE- und NIS-Regime samt Informationsaustausch zwischen den zuständigen Behörden erfolgen. Demzufolge sollen etwa kritische Einrichtungen gemäß der RKE-RL automatisch als wesentliche Einrichtungen im Sinne der NIS-2-RL gelten und somit jedenfalls auch einer (strengen) ex-ante Kontrolle durch die NIS-Behörden unterliegen (im Gegensatz zur ex-post Kontrolle bei wichtigen Einrichtungen gemäß Art. 33 Abs. 1 NIS-2-RL). Darüber hinaus sollen die Mitgliedstaaten ua. sicherstellen, dass die nach der RKE-RL und der NIS-2-RL jeweils erforderlichen nationalen Strategien einen politischen Rahmen für die Koordinierung zwischen den zuständigen nationalen Behörden vorsehen. Zudem sollen die zuständigen Behörden eng zusammenarbeiten und Informationen austauschen, insbesondere über die Ermittlung kritischer Einrichtungen sowie über Risiken, Bedrohungen und Vorfälle, die kritische Einrichtungen (potenziell) beeinträchtigen können, über die von kritischen Einrichtungen ergriffenen Cybersicherheitsmaßnahmen und physischen (Resilienz-)Maßnahmen sowie die Ergebnisse der im Hinblick auf diese Einrichtungen durchgeführten behördlichen Aufsichts- und Durchsetzungstätigkeiten. Um einerseits die Aufsichts- und Durchsetzungstätigkeiten der in den beiden Rechtsbereichen zuständigen Behörden zu straffen und andererseits den Verwaltungsaufwand für die betroffenen Einrichtungen so gering wie möglich zu halten, sollten sowohl die Meldeverpflichtungen bei Sicherheitsvorfällen als auch die behördlichen Aufsichts- und Durchsetzungsverfahren harmonisiert werden. Diese Vorgaben erfordern jedenfalls eine eng aufeinander abgestimmte Vorgehensweise bei der innerstaatlichen Umsetzung der RKE-RL und der NIS-2-RL sowie in Folge eine intensive Zusammenarbeit und einen umfassenden Informationsaustausch zwischen den für diese Bereiche national zuständigen Behörden.

Der Anwendungsbereich der RKE-RL umfasst grundsätzlich elf im Anhang der Richtlinie näher determinierte Sektoren, darunter Energie (Strom, Fernwärme und -kälte, Erdöl, Erdgas, Wasserstoff), Verkehr (Luftfahrt, Schienenverkehr, Schifffahrt, Straßenverkehr, Öffentlicher Verkehr), Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, Öffentliche Verwaltung, Weltraum sowie Lebensmittelproduktion, -verarbeitung und -vertrieb.

Vorgesehen ist insbesondere, dass die Mitgliedstaaten eine nationale Strategie zur Verbesserung der Resilienz kritischer Einrichtungen zu erstellen (Art. 4 RKE-RL) und die jeweils zuständigen Behörden regelmäßig Risikobewertungen durchzuführen haben, wobei eine von der Europäischen Kommission in Form eines delegierten Rechtsakts erlassene, nicht erschöpfende Liste wesentlicher Dienste in den im Anhang der RKE-RL genannten Sektoren und Teilsektoren für die Risikobewertungen heranzuziehen ist (Art. 5 RKE-RL). Auf Grundlage dieser Risikobewertungen hat jeder Mitgliedstaat kritische Einrichtungen zu ermitteln, die zumindest einen wesentlichen Dienst erbringen (Art. 6 RKE-RL). Die auf diesem Wege ermittelten kritischen Einrichtungen haben sodann ihrerseits auf Grundlage der Risikobewertungen der Mitgliedstaaten jene Risiken zu bewerten, die die Erbringung ihrer wesentlichen Dienste stören können (Art. 12 RKE-RL). Des Weiteren haben sie geeignete und verhältnismäßige Resilienzmaßnahmen für ihren physischen Schutz zu treffen (Art. 13 RKE-RL; ua. Ergreifung von verhältnismäßigen technischen, sicherheitsbezogenen und organisatorischen Maßnahmen, Erstellung

eines Resilienzplans, Benennung eines Verbindungsbeauftragten) und der zuständigen Behörde Sicherheitsvorfälle, die die Erbringung wesentlicher Dienste erheblich stören oder stören könnten, unverzüglich zu melden (Art. 15 RKE-RL). Ergänzt werden diese Regelungen durch Unterstützungsmaßnahmen der Mitgliedstaaten, etwa die Bereitstellung von Leitfäden und Schulungsmaßnahmen, und ein spezifisches Aufsichts- und Durchsetzungsregime durch die national zuständigen Behörden. Demnach sollen etwa die Resilienzmaßnahmen von der zuständigen nationalen RKE-Behörde bzw. den zuständigen nationalen RKE-Behörden überprüft werden können, die zudem verbindliche Anweisungen zur Beseitigung festgestellter Verstöße erteilen kann bzw. können (Art. 21 RKE-RL). Gegebenenfalls sollen die kritischen Einrichtungen auch durch eine wirksame, verhältnismäßige und abschreckende Sanktionierung zur Einhaltung ihrer Verpflichtungen angehalten werden können (Art. 22 RKE-RL).

In Österreich soll eine Umsetzung der RKE-RL mit dem vorliegenden Bundesgesetz erfolgen.

Die Hauptgesichtspunkte sind im Einzelnen:

- die Benennung einer zuständigen Behörde, die auch die Funktion einer zentralen Anlaufstelle übernehmen soll
- die Festlegung einer nationalen Strategie zur Verbesserung der Resilienz kritischer Einrichtungen
- die Durchführung einer Risikoanalyse durch die zuständige Behörde zur Bewertung sämtlicher natürlicher und vom Menschen verursachter Risiken (im Sinne des „All-Gefahren-Ansatzes“)
- die bescheidmäßige Ermittlung kritischer Einrichtungen auf Basis der nationalen Strategie sowie der durchgeführten Risikoanalyse
- die Festlegung von Unterstützungsmaßnahmen für kritische Einrichtungen durch die zuständige Behörde
- die Verpflichtung kritischer Einrichtungen zur Durchführung von Risikoanalysen, zum Ergreifen von Resilienzmaßnahmen und zur Meldung von Sicherheitsvorfällen
- die Verpflichtung zur Durchführung von Zuverlässigkeitsüberprüfungen durch die zuständige Behörde
- die Festlegung von Aufsichts- und Durchsetzungsmaßnahmen durch die zuständige Behörde zur Überprüfung der Einhaltung der Verpflichtungen der kritischen Einrichtungen und
- die Festlegung eines effektiven Sanktionenregimes

Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung eines diesem Entwurf entsprechenden Bundesgesetzes gründet sich auf Art. 10 Abs. 1 des Bundes-Verfassungsgesetzes (B-VG), BGBl. Nr. 1/1930. In jenen Bereichen, in denen die Länder zur (Ausführungs-)Gesetzgebung und/oder Vollziehung zuständig sind, beruht die Zuständigkeit des Bundes auf der in § 1 Abs. 1 des gegenständlichen Gesetzes geschaffenen Kompetenzgrundlage.

Besonderheiten des Normerzeugungsverfahrens:

Der Entwurf kann im Hinblick auf §§ 1, 4 Abs. 2 sowie § 23 (Verfassungsbestimmungen) gemäß Art. 44 Abs. 1 B-VG vom Nationalrat nur in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen beschlossen werden. Der Entwurf bedarf überdies im Hinblick auf § 1 Abs. 1 (Kompetenzdeckungsklausel) gemäß Art. 44 Abs. 2 B-VG der in Anwesenheit von mindestens der Hälfte der Mitglieder und mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen zu erteilenden Zustimmung des Bundesrates.

Besonderer Teil

Zu § 1 (Kompetenzdeckung):

Das B-VG kennt keinen eigenen Kompetenztatbestand „physische Sicherheit“ oder etwa „Resilienz bzw. Widerstandsfähigkeit kritischer Einrichtungen“. Die Gefahr von Störfällen im Bereich der physischen Sicherheit stellt auch keine „allgemeine Gefahr“, die im Sinne der Rechtsprechung des VfGH unter den Kompetenztatbestand der „Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“ (Art. 10 Abs. 1 Z 7 B-VG) zu subsumieren wäre, dar. Die abzuwehrenden Gefahren nach der RKE-RL reduzieren sich zudem nicht auf ein bestimmtes Verwaltungsgebiet, sondern handelt es sich dabei mit Blick auf die unterschiedlichen „Anbieter“ bzw. Sektoren oder Einrichtungen, die von der RKE-RL umfasst sind, – wie grundsätzlich im Bereich der Netz- und Informationssystemsicherheit – vielmehr um eine materienübergreifende Querschnittsgefahr, deren Abwehr verschiedenen besonderen

Verwaltungsmaterien zuzuordnen ist und die demnach kompetenzrechtlich der Zuständigkeit zur Regelung des jeweiligen Sachgebietes folgt.

Daraus ergibt sich, dass die Vorschriften in diesem Bundesgesetz, mit dem insbesondere die innerstaatliche Umsetzung der RKE-RL erfolgen soll, zwar überwiegend gemäß Art. 10 Abs. 1 B-VG in die Gesetzgebungs- und Vollziehungskompetenz des Bundes fallen, in einigen (Teil-)Sektoren fällt die Umsetzung jedoch in die (Ausführungs-)Gesetzgebung und/oder in die Vollziehung der Länder, weshalb die Begründung einer Kompetenz des Bundes für diese Bereiche verpflichtend einer Verfassungsänderung bedarf.

Vor dem Hintergrund, dass eine statische Kompetenzdeckungsklausel, die lediglich die Erlassung und Aufhebung (sowie die Vollziehung) von Vorschriften zur Bundessache erklärt, jedoch keine Ermächtigung des Bundes zur Änderung dieser Bestimmungen enthält, zur Folge hätte, dass jede auch noch so geringfügige Novelle zum jeweiligen Bundesgesetz (zB Beseitigung von Vollzugsdefiziten) wiederum einer gesonderten Verfassungsänderung bzw. im Verfassungsrang stehenden Kompetenzdeckungsklausel bedürfte (vgl. auch *Janko*, Staats- und Verwaltungsorganisation [2014] 9), soll das gegenständliche Gesetz in Abs. 1 eine dynamische Kompetenzdeckungsklausel enthalten, die auch die Änderung von Vorschriften, wie sie in diesem Bundesgesetz enthalten sind, umfassen soll. Zudem soll abweichend von Art. 102 Abs. 1 B-VG ausdrücklich angeordnet werden, dass die in diesem Bundesgesetz geregelten Angelegenheiten – sofern nicht im Einzelfall (einfachgesetzlich) eine gegenteilige Anordnung erfolgt (vgl. § 5 betreffend die Nichteinhaltung von Verpflichtungen) – in unmittelbarer Bundesverwaltung besorgt werden können.

Vor dem Hintergrund, dass es aufgrund der in Abs. 1 vorgesehenen dynamischen Kompetenzdeckungsklausel zu einer Kompetenzverschiebung zu Gunsten des Bundes kommt, sollen als Ausgleich gemäß Abs. 2 Novellen gewisser Bestimmungen dieses Gesetzesentwurfs an die Zustimmung der Länder geknüpft werden. Demnach sollen Bundesgesetze, mit denen die Bestimmungen gemäß § 5 (Zuständigkeit der Bezirksverwaltungsbehörden für Verwaltungsstrafverfahren bzw. Feststellungen der Nichteinhaltung von Verpflichtungen) und § 6 Abs. 2 (Zuständigkeit der Verwaltungsgerichte der Länder für diesbezügliche Beschwerdeverfahren) geändert werden, nur mit Zustimmung der Länder kundgemacht werden dürfen. Eine Zustimmungspflicht der Länder soll ebenfalls für Bundesgesetze vorgesehen werden, mit denen § 12 Abs. 1 Z 2 (Voraussetzung für die Einstufung als kritische Einrichtung im Sektor öffentliche Verwaltung) sowie § 20 (Aufsichts- und Durchsetzungsmaßnahmen) geändert werden sollen, sofern sich die jeweilige Änderung auf Behörden und sonstige Stellen der öffentlichen Verwaltung der Länder, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, bezieht. Vor dem Hintergrund, dass die Sanktionierung von Stellen der öffentlichen Verwaltung angesichts des grundsätzlich verfassungsrechtlich geltenden Grundsatzes der Unmöglichkeit der Strafbewehrung hoheitlichen Handelns zudem einen besonders sensiblen Regelungsbereich darstellt, soll dasselbe für Bundesgesetze gelten, mit denen § 22 Abs. 6 (Ausnahmebestimmung betreffend das Verwaltungsstrafregime für Stellen der öffentlichen Verwaltung) sowie § 23 (Nichteinhaltung von Verpflichtungen durch Stellen der öffentlichen Verwaltung) geändert werden. Demnach soll für den Fall der beabsichtigten Änderung dieser Bereiche die formelle Zustimmung der Länder eine Voraussetzung für das verfassungsmäßige Zustandekommen der betreffenden bundesgesetzlichen Regelungen sein (Art. 42a B-VG; vgl. auch zB Art. 102 Abs. 1 und 4 B-VG) und in diesem Zusammenhang ein ausreichendes Mitspracherecht der Länder sichergestellt werden.

Zu § 2 (Anwendungsbereich):

Angesichts der sich rasch ändernden Bedrohungslage, etwa im Kontext mit der offensichtlichen Sabotage der Gasinfrastruktur Nord Stream 1 und Nord Stream 2 in der jüngsten Vergangenheit, stehen Einrichtungen, die kritische Infrastrukturen betreiben, in Bezug auf ihre Widerstandsfähigkeit gegen feindliche Handlungen und andere von Menschen verursachte Bedrohungen vor besonderen Herausforderungen, während auch die Gefahren aufgrund natürlicher Faktoren und des Klimawandels zunehmen und mit diesen feindlichen Handlungen zusammenwirken können. Es ist daher wesentlich, dass diese Einrichtungen geeignete Maßnahmen zur Stärkung ihrer Resilienz ergreifen, um auf Gefahren vorbereitet zu sein und entsprechend reagieren zu können.

Die physische Sicherheit dieser Einrichtungen und der von ihnen betriebenen kritischen Infrastrukturen, mit der Dienste im Binnenmarkt erbracht werden, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit, der Sicherheit oder für die Umwelt von entscheidender Bedeutung sind, spielt daher eine zentrale Rolle in der heutigen Gesellschaft. Mit diesem Bundesgesetz sollen demzufolge Maßnahmen festgelegt werden, die ein hohes Resilienzniveau kritischer Einrichtungen in den im Anhang der RKE-RL gelisteten Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, digitale

Infrastruktur, öffentliche Verwaltung auf Bundesebene, Weltraum sowie Lebensmittelproduktion, -verarbeitung und -vertrieb sicherstellen sollen. Die Regelung in Abs. 1 soll den sachlichen Anwendungsbereich des gegenständlichen Bundesgesetzes klar zum Ausdruck bringen.

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 ErwGr 9 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.

Vor dem Hintergrund der einschränkenden Definition der „Einrichtung der öffentlichen Verwaltung“ in Art. 2 Z 10 RKE-RL soll in Abs. 3 vorgesehen werden, dass die Regelungen dieses Bundesgesetzes nicht für den Bereich der Gerichtsbarkeit sowie der Gesetzgebung (vgl. Art. 24 ff B-VG) und die Österreichische Nationalbank gelten sollen, wobei – mit Blick auf das der innerstaatlichen Rechtsordnung zugrunde liegende Verständnis – die Begrifflichkeit „Gerichtsbarkeit“ sowohl jene der ordentlichen (vgl. Art. 82 ff B-VG) als auch der Verwaltungs- (Art. 129 ff B-VG) und Verfassungsgerichtsbarkeit (Art. 137 ff B-VG) umfassen soll.

Der vorgesehene Ausschluss der Gerichtsbarkeit sowie der Gesetzgebung umfasst auch die für diese Bereiche im Rahmen der Verwaltung erbrachten unterstützenden Tätigkeiten, zumal diese auf die Gewährleistung des ordnungsgemäßen Funktionierens dieser Staatsteilgewalten beschränkt sind und daher per se als von der sich aus der RKE-RL ergebenden Ausnahme erfasst angesehen werden können. Daraus ergibt sich auch ohne ausdrückliche gesetzliche Anordnung, dass Angelegenheiten der (kollegialen und monokratischen) Justizverwaltung sowie der Parlamentsdirektion ebenfalls nicht vom Anwendungsbereich dieses Bundesgesetzes umfasst sein sollen. Ungeachtet dessen gewährleistet die Justiz die Resilienz sämtlicher ihrer Einrichtungen (der Gerichtsbarkeit, der Justizverwaltung und des Straf- und Maßnahmenvollzugs) durch interne Risikoanalysen und Krisenbewältigungsstrategien.

Zu § 3 (Begriffsbestimmungen):

In Umsetzung des Art. 2 RKE-RL sollen in dieser Bestimmung Inhalte von bestimmten Begriffen festgelegt werden. Sofern es keiner eigenen Legaldefinition aufgrund nationaler Gegebenheiten bzw. Besonderheiten bedarf, sollen die in Art. 2 RKE-RL geregelten Definitionen direkt übernommen werden. Darüber hinaus sollen – soweit erforderlich – begriffliche Anpassungen erfolgen und zusätzliche Definitionen aufgenommen werden.

Unter „kritische Einrichtung“ (Z 1) soll eine öffentliche oder private Einrichtung zu verstehen sein, die mit Bescheid des Bundesministers für Inneres bei Vorliegen der gesetzlich normierten Voraussetzungen gemäß § 11 als solche eingestuft wurde. Sofern im Gesetzestext auf „kritische“ Einrichtungen Bezug genommen wird, sollen demnach lediglich solche Einrichtungen umfasst sein, bei denen tatsächlich (bereits) eine bescheidmäßige Ermittlung erfolgte.

Vor dem Hintergrund der geopolitischen Entwicklungen, von globaler Reichweite geprägten Krisen und der sich dadurch ständig wandelnden Bedrohungslage (siehe dazu die Ausführungen oben) stehen kritische Einrichtungen, die wesentliche Dienste zur Verfügung stellen, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen etc. von entscheidender Bedeutung sind, in Bezug auf den Schutz ihrer (physischen) Widerstandsfähigkeit vor besonderen Herausforderungen. Die Fähigkeit zur schnellen Reaktion auf diese Bedrohungen erfordert ständige Wachsamkeit und Anpassung an die aktuellen Gegebenheiten. Im Sinne des Selbstschutzgedankens soll „Resilienz“ (Z 2) die Fähigkeit einer kritischen Einrichtung bezeichnen, sich umfassend und in jedem Stadium gegen Sicherheitsvorfälle „abzusichern“.

Bei einem „Sicherheitsvorfall“ (Z 3) soll es sich um ein Ereignis handeln, das die Erbringung eines wesentlichen Dienstes erheblich stört oder stören könnte, wobei bei Beurteilung der Erheblichkeit der (potenziellen) Störung entweder auf die in § 11 Abs. 2 oder in § 17 Abs. 2 angeführten Kriterien Bedacht zu nehmen sein wird, je nachdem, ob es sich im gegebenen Kontext um die Identifizierung kritischer Einrichtungen durch den Bundesminister für Inneres als zuständige Behörde (vgl. § 4) oder die Meldeverpflichtung kritischer Einrichtungen handelt. Ein Sicherheitsvorfall soll – im Sinne des sowohl der RKE-RL als auch diesem Gesetzesentwurf zugrundeliegenden „All-Gefahren-Ansatzes“ –

beispielsweise durch Unfälle, Naturkatastrophen, gesundheitliche Notlagen, wie etwa Pandemien, und hybride sowie feindliche Bedrohungen, einschließlich terroristischer Straftaten, verursacht werden können. Zudem soll in Umsetzung unionsrechtlicher Vorgaben klargestellt werden, dass auch Beeinträchtigungen der verfassungsrechtlichen Grundprinzipien – wie etwa eine Störung der demokratischen rechtsstaatlichen Grundordnung der Republik oder gezielte (physische) Angriffe auf verfassungsmäßige Einrichtungen, um deren Handlungsfähigkeit auszuschalten (zB das Bundeskanzleramt) – das Ausmaß eines Sicherheitsvorfalles annehmen können.

Als „Beinahe-Sicherheitsvorfall“ (Z 4) soll ein Ereignis verstanden werden, das zwar noch nicht die Schwelle eines Sicherheitsvorfalls gemäß Z 3 erreicht hat, jedoch das Potenzial aufweist, einen solchen hervorzurufen. Die Definition soll demnach auf ein dem Sicherheitsvorfall vorgelagertes Stadium abstellen.

Als Beispiele für „kritische Infrastrukturen“ (Z 5) können etwa die Umspannwerke von Stromnetzbetreibern (zB der Netz Niederösterreich GmbH) oder das Schienennetz sowie die Bahnhöfe der Österreichischen Bundesbahnen (ÖBB) dienen. Ausschlaggebend ist jedoch, dass nur solche „Infrastrukturen“ als kritisch betrachtet werden sollen, die für die Erbringung eines wesentlichen Dienstes (Z 6) erforderlich sind. Im Ergebnis sollen demnach jene Infrastrukturen erfasst sein, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen etwa auf die öffentliche Gesundheit, Sicherheit oder wichtige wirtschaftliche Tätigkeiten haben würden. Wenngleich die Definition von „kritischen Infrastrukturen“ im Sinne der RKE-RL mit jener von „kritischen Infrastrukturen“ im Sinne des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991, nicht deckungsgleich ist, wird zumindest teilweise eine Orientierung an den gemäß § 22 Abs. 1 Z 6 SPG zu schützenden Einrichtungen erfolgen können.

„Wesentlich“ sollen „Dienste“ sein (Z 6), die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, wichtiger wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit oder der Erhaltung der Umwelt von entscheidender Bedeutung sind. Dabei soll es sich in erster Linie um jene Dienste handeln, die – nicht erschöpfend – in der Delegierten Verordnung (EU) 2023/2450 der Europäischen Kommission zur Ergänzung der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates durch eine Liste wesentlicher Dienste, ABl. Nr. L 2023/2450 vom 30.10.2023, auf Grundlage von Art. 5 Abs. 1 RKE-RL sowie darüber hinaus allenfalls aufgrund einer Verordnung des Bundesministers für Inneres innerhalb der im Anhang der RKE-RL gelisteten Sektoren und Teilsektoren festgelegt wurden.

Im Sinne der in der RKE-RL vorgesehenen Begriffsdefinition soll als „Risiko“ (Z 7) das Potenzial für – durch einen Sicherheitsvorfall verursachte – Verluste oder Störungen zu verstehen sein, wobei das Ausmaß eines solchen Verlusts bzw. einer solchen Störung und die Eintrittswahrscheinlichkeit eines Sicherheitsvorfalls berücksichtigt werden sollen. Das Risiko stellt demnach das Produkt aus dem potenziell möglichen Schaden (schädlichen Auswirkungen), der aus dem unerwünschten Ereignis resultiert, und der damit verbundenen Eintrittswahrscheinlichkeit dar.

Voraussetzung für Maßnahmen zur Erhöhung der Resilienz ist die Identifikation der Vulnerabilität kritischer Infrastrukturen gegenüber Risiken. Vor dem Hintergrund, dass im deutschen Sprachgebrauch der in der RKE-RL vorgesehene Begriff der „Risikobewertung“ enger gefasst wird und den Prozess zur Bestimmung der Art und des Ausmaßes eines Risikos nicht abdeckt, soll im gegenständlichen Umsetzungsgesetz in unionsrechtskonformer Weise auf den sämtliche Elemente abdeckenden Terminus „Risikoanalyse“ abgestellt werden. Die „Risikoanalyse“ (Z 8) soll demnach das systematische Verfahren zur Bestimmung eines Risikos darstellen und identifizierte Risiken und deren Eintrittswahrscheinlichkeit korrekt und verständlich beschreiben, die Eintrittswahrscheinlichkeit ermitteln und die potenziellen Auswirkungen auf kritische Einrichtungen anhand von Risikokriterien darlegen. Die Risikoanalyse soll sich somit mit der Fragestellung beschäftigen, welche Auswirkungen Gefahren auf Betrieb und Leistungserbringung kritischer Einrichtungen haben und stellt diese somit die korrekte und verständliche Beschreibung von identifizierbaren Risiken sowie die Ermittlung von Eintrittswahrscheinlichkeit und Darstellung der Auswirkungen anhand von Risikokriterien dar (dh. Identifikation der Verletzbarkeit kritischer Infrastrukturen gegenüber Risiken). Sie umfasst demzufolge auch den Prozess des Vergleichs und der Priorisierung von Risiken in Bezug auf deren Wirkung auf die „kritische Dienstleistung“ und sollen im Rahmen der Risikobewertung Entscheidungen hinsichtlich der Notwendigkeit von geänderten und zusätzlichen Maßnahmen zur Risikobehandlung getroffen werden. Wesentlich ist, dass sie im Sinne eines gesamtheitlichen Ansatzes eine Beurteilung sämtlicher „Risiken“ (Z 7) umfassen soll, insbesondere solche sektorübergreifender oder grenzüberschreitender Art und unabhängig davon, ob deren Ursache auf höhere Gewalt oder den Menschen zurückzuführen ist, wobei als Beispiele Unfälle, Naturkatastrophen, gesundheitliche Notlagen, hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich

terroristischer Straftaten, genannt werden können. Wesentlich ist in diesem Zusammenhang, dass Risiken in der Regel nicht statisch sind, sondern einem dynamischen Prozess unterliegen. Ein wichtiger Aspekt in einem Risikomanagementprozess ist somit die ständige Risikoüberwachung bzw. -überprüfung.

Während vom Terminus „Mitgliedstaat“ (Z 9) jeder Staat, der Vertragspartei des Vertrags über die Europäische Union (EUV) in der Fassung BGBl. III Nr. 132/2009 ist, umfasst sein soll, sollen alle anderen Staaten als „Drittstaaten“ (Z 10) gelten.

„Einrichtungen“ (Z 11) sollen den potenziellen Adressatenkreis der Rechte und Pflichten nach diesem Bundesgesetz abbilden und sollen darunter sowohl natürliche und juristische Personen als auch eingetragene Personengesellschaften zu verstehen sein. Vor dem Hintergrund, dass auch Behörden, etwa Bundesminister, unter bestimmten Voraussetzungen unter das RKE-Regime fallen können, diese jedoch mangels (selbständiger) Rechtsfähigkeit in aller Regel keine juristischen Personen sind, sollen darüber hinaus auch Stellen der öffentlichen Verwaltung ausdrücklich genannt werden. Der Terminus ist bewusst sehr weit gefasst und soll neben Behörden auch sonstige Stellen der öffentlichen Verwaltung, wie insbesondere ausgegliederte Rechtsträger privaten oder öffentlichen Rechts, umfassen. Wesentlich ist in diesem Zusammenhang jedoch, dass nur jene Einrichtungen in den Anwendungsbereich dieses Bundesgesetzes und somit unter das RKE-Regime fallen sollen, die der Bundesminister für Inneres bei Vorliegen der gesetzlich normierten Voraussetzungen gemäß § 11 bescheidmäßig als „kritisch“ eingestuft hat.

Vorgesehen ist, dass im Rahmen der zu treffenden Resilienzmaßnahmen kritischer Einrichtungen auch „Resilienzpläne“ mit einer nachvollziehbaren und strukturierten Aufbereitung von geeigneten und verhältnismäßigen technischen, sicherheitsbezogenen und organisatorischen Maßnahmen zur Gewährleistung der Resilienz (Z 12) zu erstellen sowie an den Bundesminister für Inneres zu übermitteln sind (vgl. § 15 Abs. 3 des gegenständlichen Entwurfs). Die inhaltlichen Komponenten dieses Dokuments sollen durch die Begriffsbestimmung festgeschrieben werden.

Im Rahmen der Aufsichts- und Durchsetzungsmaßnahmen soll der Bundesminister für Inneres in Umsetzung der unionsrechtlichen Vorgabe in Art. 21 Abs. 1 lit. b RKE-RL gemäß § 20 Abs. 1 von kritischen Einrichtungen die Durchführung von „Audits“ verlangen können. Dabei soll es sich um eine systematische Überprüfung der Einhaltung der Verpflichtungen gemäß den §§ 14 und 15 durch qualifizierte Stellen (§ 21) handeln (zB durch einen Bewertungsbesuch), wobei die Ergebnisse zu dokumentieren und vorgeschlagene Korrekturmaßnahmen in einem Prüfbericht aufgelistet werden sollen. Wesentlich ist, dass die Prüftätigkeit in Unabhängigkeit von der zu überprüfenden kritischen Einrichtung erfolgen soll (Z 13).

Zu § 4 (Zuständige Behörde):

In Abs. 1 erfolgt die Festlegung des Bundesministers für Inneres als zuständige Behörde im Sinne des Art. 9 Abs. 1 RKE-RL und soll demnach vor dem Hintergrund, dass die gesamte Expertise in einer Behörde konzentriert werden soll, mit Blick auf eine effektive und effiziente Verwaltungsführung die ausschließliche Zuständigkeit zur Vollziehung des gegenständlichen Gesetzes – mit Ausnahme des Sanktionsregimes (vgl. § 5) – bei der RKE-Behörde liegen. Daraus ergibt sich, dass der Bundesminister für Inneres als „RKE-Behörde“ die Behördenfunktion auch im Hinblick auf kritische Einrichtungen in den Sektoren Bankwesen und Finanzmarktinfrastrukturen sowie digitale Infrastruktur übernehmen soll (so etwa die Unterstützungs- und Vorsorgemaßnahmen gemäß § 13; zur unionsrechtlichen Zulässigkeit dieser Zuständigkeitsbegründung vgl. Art. 9 Abs. 1 Unterabsatz 2 RKE-RL).

Gemäß Art. 9 Abs. 4 RKE-RL sind die Mitgliedstaaten dazu verpflichtet, die zuständige Behörde mit erforderlichen Befugnissen auszustatten, um die ihnen übertragenen Aufgaben wirksam und effizient zu erfüllen. Zudem sind die Mitgliedstaaten gemäß Art. 21 RKE-RL dazu verpflichtet, die zuständige Behörde unter Wahrung des Grundsatzes der Verhältnismäßigkeit mit spezifischen Befugnissen auszustatten, um die ordnungsgemäße Anwendung und Durchsetzung der gemäß dieser Richtlinie erlassenen nationalen Rechtsvorschriften in Bezug auf kritische Einrichtungen sicherzustellen. Zur unionsrechtskonformen Umsetzung dieser Vorgaben ist es zwingend erforderlich, dass der Bundesminister für Inneres sämtliche Befugnisse nach diesem Bundesgesetz auch gegenüber den in Art. 19 B-VG bezeichneten obersten Organen der Vollziehung ausüben kann, wie etwa die Ermittlung als kritische Einrichtung sowie die Ausübung der Aufsichts- und Durchsetzungsbefugnisse gemäß § 20, sofern diese mit Bescheid als kritisch eingestuft wurden.

Nach der Rechtsprechung des VfGH sind oberste Organe jedoch gegenüber keinem anderen Organ weisungsgebunden und besteht keine sachlich in Betracht kommende Oberbehörde (vgl. VfGH 11.3.1959, B 179/58). Oberste Organe dürfen zudem nicht an Willenserklärungen anderer Organe gebunden werden (vgl. VfSlg. 19.827/2013) und darf die Kontrolle der Rechtmäßigkeit des Handelns eines obersten Organes nicht einer anderen Verwaltungsbehörde übertragen werden (vgl.

VfSlg. 13.626/1993). Folglich bedarf es für die – unionsrechtlich verpflichtend vorgesehene – Ausübung von Befugnissen gegenüber obersten Organen einer entsprechenden verfassungsrechtlichen Grundlage, die mit Abs. 2 geschaffen werden soll. Demnach soll der Bundesminister für Inneres als zuständige RKE-Behörde (in Anlehnung an die Regelung in § 35 Abs. 2 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999) dazu ermächtigt sein, seine Befugnisse nach diesem Bundesgesetz auch gegenüber den in Art. 19 B-VG genannten obersten Organen der Vollziehung auszuüben, soweit in diesem Bundesgesetz nicht anderes bestimmt ist. Zu beachten ist, dass damit jedoch kein Weisungsrecht des Bundesministers für Inneres gegenüber obersten Organen der Vollziehung verbunden sein soll. Vor dem Hintergrund der Tatsache, dass – im Gegensatz zum Sektor „Öffentliche Verwaltung“ – in den sonstigen von der RKE-RL umfassten Sektoren etwa auch Einrichtungen (vgl. § 3 Z 11) der Länder wesentliche Dienste erbringen können, bezieht sich die Regelung auf sämtliche obersten Organe der Vollziehung und kann insofern keine Einschränkung auf Bundesorgane erfolgen.

Im Sinne eines effizienten Vollzugs kann es sich als sinnvoll erweisen, die Landespolizeidirektionen mit der Durchführung einzelner Aufgaben, bei denen etwa eine Anwesenheit vor Ort erforderlich ist (zB Vor-Ort-Kontrollen gemäß § 20 Abs. 3), zu beauftragen und sich regelmäßig darüber berichten zu lassen, um einen österreichweiten koordinierten Vollzug sicherzustellen. In Abs. 3 soll daher eine entsprechende Rechtsgrundlage geschaffen und vorgesehen werden, dass der Bundesminister für Inneres der Landespolizeidirektion diesbezügliche auf die jeweils übertragenen Aufgaben bezogene Berichtspflichten vorschreiben kann (vgl. die damit im Zusammenhang stehende Ermächtigung zur Datenübermittlung an Sicherheitsbehörden zur Wahrnehmung der Aufgaben nach diesem Bundesgesetz gemäß § 7 Abs. 2).

Gemäß Art. 9 Abs. 2 RKE-RL in Zusammenschau mit ErwGr 23 zur RKE-RL hat jeder Mitgliedstaat zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation auf Unionsebene sowie mit Blick auf die effektive Umsetzung der RKE-RL eine zentrale Anlaufstelle zu benennen oder einzurichten, wobei diese auch innerhalb einer zuständigen Behörde angesiedelt sein kann. Dementsprechend soll in Abs. 4 vorgesehen werden, dass dem Bundesminister für Inneres auch diese Funktion zukommt. Klargestellt werden soll, dass er auch als Verbindungsstelle zu den zentralen Anlaufstellen der anderen Mitgliedstaaten der Europäischen Union, zur Gruppe für die Resilienz kritischer Einrichtungen gemäß Art. 19 RKE-RL sowie zur Europäischen Kommission fungieren und – vor dem Hintergrund der gemäß Art. 9 Abs. 2 letzter Satz RKE-RL eingeräumten Option – die Zusammenarbeit mit Drittstaaten sicherstellen soll.

Zu § 5 (Nichteinhaltung von Verpflichtungen):

In § 5 soll die Klarstellung erfolgen, dass die Bezirksverwaltungsbehörden – sohin in mittelbarer Bundesverwaltung – für die Führung von Verwaltungsstrafverfahren gemäß § 22 sowie die Feststellung der Nichteinhaltung der Verpflichtungen gemäß § 23 zuständig sind.

Angemerkt wird, dass mit Blick auf die erforderliche Expertise zum Zwecke der Zuständigkeitskonzentration mit Landesgesetz die sprengelübergreifende Zusammenarbeit von Bezirksverwaltungsbehörden vorgesehen werden kann („Kompetenzzentren“; vgl. etwa § 1 des Landesgesetzes über die Kooperation zwischen Bezirksverwaltungsbehörden in Oberösterreich, LGBl. Nr. 103/2018, sowie § 2a des Gesetzes vom 14. Februar 1977 über die Organisation der Bezirkshauptmannschaften, LGBl. Nr. 11/1977).

Zu § 6 (Beschwerdeverfahren):

Die Abgrenzung der Zuständigkeiten zwischen den Verwaltungsgerichten ergibt sich zwar bereits ex constitutione (vgl. Art. 131 B-VG). Vor dem Hintergrund der Regelung im vorgeschlagenen § 1 soll im Sinne der Rechtssicherheit jedoch gemäß Abs. 1 die sachliche Zuständigkeit des Bundesverwaltungsgerichts für Beschwerden gegen Bescheide des Bundesministers für Inneres sowie wegen Verletzung seiner Entscheidungspflicht klargestellt werden (vgl. Art. 131 Abs. 2 B-VG).

Im Hinblick darauf, dass die Bezirksverwaltungsbehörde als „Sanktionsbehörde“ fungieren und das Verwaltungsstrafverfahren sowie das Verfahren betreffend die Nichteinhaltung von Verpflichtungen gegenüber Stellen der öffentlichen Verwaltung demnach in mittelbarer Bundesverwaltung vollzogen werden soll (vgl. § 5), soll in Abs. 2 zudem die Klarstellung erfolgen, dass die Verwaltungsgerichte der Länder für Beschwerden gegen Bescheide der Bezirksverwaltungsbehörden sowie wegen Verletzung ihrer Entscheidungspflicht zuständig sein sollen (vgl. Art. 131 Abs. 1 B-VG).

Zu § 7 (Datenverarbeitung):

In dieser Bestimmung soll die vom Bundesminister für Inneres geführte Datenverarbeitung verankert und insbesondere durch Nennung von Betroffenenkreis, Datenarten und Löschungsfristen näher determiniert werden. Diese Ermächtigung zur Datenverarbeitung soll den Bundesminister für Inneres in die Lage versetzen, den ihm gesetzlich übertragenen Aufgaben auch tatsächlich nachkommen zu können sowie

österreichweit mögliche Bedrohungen und Gefahren ehestmöglich zu erkennen, damit eine rasche Reaktion sowie Gewährleistung bzw. Wiederherstellung der Resilienz möglich ist. Zudem soll durch diese Regelung auch die unionsrechtlich vorgesehene enge Zusammenarbeit sowie der erforderliche Informationsaustausch mit der in Umsetzung des Art. 8 Abs. 1 NIS-2-RL innerstaatlich für die NIS-Agenden zuständigen Behörde bzw. den zuständigen Behörden, etwa betreffend Risiken, Bedrohungen und Vorfälle, die kritische Einrichtungen beeinträchtigen, abgebildet werden. Nur auf diese Weise ist es möglich, das Ziel der RKE-RL, konkret die Resilienz bzw. physische Widerstandsfähigkeit kritischer Einrichtungen zu stärken und ihre Schwachstellen zu verringern, zu erreichen.

In Abs. 1 soll demnach normiert werden, dass der Bundesminister für Inneres als Verantwortlicher gemäß Art. 4 Z 7 in Verbindung mit Art. 24 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 04.05.2016 S. 1, in der Fassung der Berichtigung ABl. Nr. L 74 vom 04.03.2021 S. 35, (im Folgenden: DSGVO) ermächtigt ist, die erforderlichen Kontakt- (zB Telefonnummer, Mailadresse, Anschrift) und Identitätsdaten (zB Namen, Geschlecht, Geburtsdatum, Rechtsform, Firma, Firmenbuchnummer, vertretungsbefugte Organe) bescheidmäßig ermittelter kritischer Einrichtungen samt dem Sektor und Teilsektor, in dem diese ihren wesentlichen Dienst erbringen, die von diesen kritischen Einrichtungen erbrachten wesentlichen Dienste, die Standorte und Versorgungsgebiete kritischer Infrastrukturen sowie Kontaktdaten der namhaft gemachten zentralen Kontaktstellen sowie von Ansprechpersonen zu verarbeiten (Z 1).

Zudem ist es für die ordnungsgemäße Erfüllung der im Rahmen dieses Bundesgesetzes übertragenen Aufgaben notwendig, Daten zu Cybersicherheitsrisiken, Cyberbedrohungen, Cybersicherheitsvorfällen, aber vor allem auch zu nicht cyberbezogenen Risiken, Bedrohungen, Beinahe-Sicherheitsvorfällen und Sicherheitsvorfällen, die kritische Einrichtungen betreffen, zu verarbeiten und soll zu diesem Zweck eine eindeutige und ausreichende Rechtsgrundlage geschaffen werden (Z 2). Intention dieser Regelung ist es auch, den in der RKE-RL vorgesehenen erforderlichen umfassenden Informationsaustausch und dadurch die intensive Zusammenarbeit mit den NIS-Behörden sicherzustellen (siehe dazu auch die Übermittlungsermächtigung gemäß Abs. 2 Z 3).

Zur effektiven und effizienten Aufgabenwahrnehmung nach diesem Bundesgesetz ist es überdies erforderlich, Daten zu den durchgeführten Risikoanalysen und getroffenen Resilienzmaßnahmen sowie vorgenommenen Meldungen kritischer Einrichtungen bei Sicherheitsvorfällen, aber auch den angeordneten bzw. getroffenen Aufsichts- und Durchsetzungsmaßnahmen zu verarbeiten (Z 3). Ziel dieser Datenverarbeitungsermächtigung ist es, die im gegenständlichen Bundesgesetz vorgesehenen Maßnahmen, die sowohl präventiver als auch reaktiver Natur sind, effektiv und erfolgreich durchführen zu können.

Eine wesentliche Einschränkung der von der Ermächtigung umfassten Datenarten ergibt sich aus dem Zweck der Verarbeitung: Klargestellt wird, dass für eine Verarbeitung nur jene personenbezogenen Daten in Betracht kommen, die vom Bundesminister für Inneres für die Aufgabenerfüllung (zB zur Durchführung von Aufsichtsmaßnahmen, aber auch für unionsrechtlich vorgeschriebene Datenübermittlungen insbesondere an die Europäische Kommission) relevant sind.

In Abs. 2 bis 4 sollen insbesondere die Übermittlungsempfänger der gemäß Abs. 1 verarbeiteten Daten ausgewiesen werden.

In Abs. 2 ist vorgesehen, dass Übermittlungen einerseits an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege (Z 1) sowie an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege (Z 2) zulässig sind. Durch die Übermittlungsermächtigung an Sicherheitsbehörden „zur Wahrnehmung der Aufgaben nach diesem Bundesgesetz“ (Z 1) soll insbesondere sichergestellt werden, dass den Landespolizeidirektionen, die gemäß dem vorgeschlagenen § 4 Abs. 3 mit der Durchführung einzelner Aufgaben nach diesem Bundesgesetz betraut werden können, auch die zur Aufgabenwahrnehmung erforderlichen Daten zur Verfügung gestellt werden können. Andererseits soll durch die Ermächtigung in Z 3 gewährleistet werden, dass eine Datenübermittlung auch an Dienststellen inländischer Behörden zulässig sein soll, jedoch nur insoweit, als dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe darstellt. Die diesbezügliche Einschränkung bzw. Konkretisierung ergibt sich demnach wieder aus dem Zweck der Verarbeitung („wesentliche Voraussetzung zur Wahrnehmung der ihnen gesetzlich übertragenen Aufgaben“) und ergeben sich die gesetzlichen Aufgaben (und damit auch die Datenarten) wiederum aus den jeweiligen zur Anwendung gelangenden Materiengesetzen. Durch diese Regelung soll auch die in Art. 9 Abs. 5 RKE-RL vorgesehene Zusammenarbeit mit anderen nationalen Behörden, insbesondere denjenigen, „die für den Katastrophenschutz, die Strafverfolgung und den Schutz personenbezogener

Daten zuständig“ sind, sichergestellt werden und soll die Möglichkeit einer Übermittlung an jene Behörden, die gemäß Art. 8 Abs. 1 der NIS-2-RL als zuständige Behörden benannt wurden, bestehen.

Vor dem Hintergrund, dass der Begriff der „Übermittlung“ technologieneutral ist (vgl. auch ErwGr 15 zur DSGVO) und in der vorgeschlagenen Regelung nicht vorgesehen ist, in welcher Form die Übermittlung der Daten erfolgen soll, sollen Datenübermittlungen auch in Form der Einräumung und Inanspruchnahme einer Abfrageberechtigung stattfinden können (vgl. in diesem Zusammenhang auch § 22b Abs. 4 des Passgesetzes 1992, BGBl. Nr. 839/1992, wonach die „Einräumung einer Möglichkeit zum automatisierten Abruf der personenbezogenen Daten“ als eine mögliche Form der Übermittlung normiert ist).

Übermittlungsermächtigungen von Daten aus dem sicherheitspolizeilichen Bereich (zB hinsichtlich des „strafrechtsakzessorischen“ Schutzes kritischer Infrastruktur) ergeben sich hingegen unmittelbar aus den Regelungen im SPG bzw. sind diese im Staatsschutz- und Nachrichtendienst-Gesetz (SNG), BGBl. I Nr. 5/2016, (vgl. etwa § 53a Abs. 1a iVm Abs. 5a SPG betreffend Daten aus der SKI-Datenbank bzw. § 12 Abs. 1 iVm Abs. 4 SNG betreffend Daten aus der SNG-Analyseanwendung) ausreichend abgebildet.

Zum Zwecke der Gewährleistung der grenzüberschreitenden Zusammenarbeit soll in Abs. 3 vorgesehen werden, dass der Bundesminister für Inneres zudem ermächtigt ist, die gemäß Abs. 1 verarbeiteten Daten an die Europäische Kommission, andere Mitgliedstaaten, die Gruppe für die Resilienz kritischer Einrichtungen (vgl. Art. 19 RKE-RL) sowie Drittstaaten (vgl. damit im Zusammenhang auch Art. 44 DSGVO) zu übermitteln. Diese Ermächtigung soll jedoch nur insoweit bestehen, als dies zur Erfüllung einer in der RKE-RL ausdrücklich vorgesehenen Informationsverpflichtung erforderlich ist. Die Verpflichtung ergibt sich demnach aus zwingenden unionsrechtlichen Vorgaben (vgl. in diesem Zusammenhang etwa Art. 5 Abs. 2 und 4, Art. 7 Abs. 2, Art. 9 Abs. 3, Art. 11, Art. 15 Abs. 1 letzter Satz und Abs. 3, Art. 17 Abs. 2, Art. 18 Abs. 3 und Abs. 4 Unterabsatz 2 und 4 und Art. 18 Abs. 10 RKE-RL). In dieser Regelung findet sich zudem eine entsprechende Ermächtigung zur (Weiter-)Verarbeitung entsprechender von der Europäischen Kommission, anderen Mitgliedstaaten sowie Drittstaaten übermittelten Daten durch den Bundesminister für Inneres.

In Abs. 4 soll die gesetzliche Grundlage für die Ermächtigung des Bundesministers für Inneres geschaffen werden, zum Zweck der Erfüllung der Unterstützungs- und Vorsorgeaufgaben gemäß § 13 Z 12 sachdienliche Folgeinformationen (Daten gemäß § 17 Abs. 5) an die von einem Risiko, Beinahe-Sicherheitsvorfall oder Sicherheitsvorfall betroffenen kritischen Einrichtungen zu übermitteln (zu den Begriffsbestimmungen vgl. § 3). Intention dieser Regelung ist es ebenfalls, wirksam und rasch auf Sicherheitsvorfälle reagieren zu können und somit ein hohes Resilienzniveau sicherzustellen, damit wesentliche Dienste dauerhaft bzw. ohne maßgebliche Unterbrechungen zur Verfügung gestellt werden können.

Auch nach Rechtskraft eines Bescheids gemäß § 11 Abs. 9, durch den die Einstufung einer Einrichtung als „kritisch“ aufgehoben wird, können Umstände eintreten, die die Heranziehung der gemäß den Abs. 1 bis 4 zu dieser Einrichtung verarbeiteten Daten erforderlich machen (zB für eine wirksame Reaktion auf Sicherheitsvorfälle aufbauend auf „Vorerfahrungen“). Es kann sich daher als schwierig erweisen, im Vorhinein zu beurteilen, zu welchem Zeitpunkt genau diese Daten nicht mehr erforderlich sein werden. Demnach soll unter Berücksichtigung des in der DSGVO vorgesehenen Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) sowie mit Blick auf den Verhältnismäßigkeitsgrundsatz (§ 1 Abs. 2 DSG) aber auch vor dem Hintergrund der Wichtigkeit der Aufrechterhaltung eines hohen Resilienzniveaus betreffend wesentliche Dienste in Abs. 5 vorgesehen werden, dass die gemäß den Abs. 1 bis 4 verarbeiteten Daten spätestens zehn Jahre nach (rechtskräftiger) Aufhebung des Bescheids gemäß § 11 Abs. 1 zu löschen sind.

Vor dem Hintergrund, dass die DSGVO von spezifischen Regelungen betreffend die Protokollierung Abstand nimmt, wird vorgeschlagen, in Abs. 6 eine Protokollierungsdauer von drei Jahren vorzusehen.

Gemäß Art. 21 Abs. 1 DSGVO hat der Betroffene das Recht, aus Gründen, die sich aus seiner besonderen Situation ergeben, jederzeit gegen die Verarbeitung der ihn betreffenden personenbezogenen Daten Widerspruch zu erheben. Darüber hinaus hat der Betroffene gemäß Art. 18 Abs. 1 DSGVO das Recht, unter näher normierten Voraussetzungen die Einschränkung der Verarbeitung zu verlangen. Ein solches, dem Betroffenen durch die DSGVO in genereller Weise eingeräumtes Widerspruchsrecht sowie das Recht auf Einschränkung der Verarbeitung kann jedoch gemäß Art. 23 DSGVO zur Sicherstellung einer der in Abs. 1 lit. a bis j genannten Zwecke durch nationale Bestimmungen beschränkt werden, sofern eine solche Beschränkung notwendig und verhältnismäßig ist. Von einer solchen Beschränkung soll in Abs. 7 für sämtliche nach dem gegenständlichen Bundesgesetz verarbeiteten Daten Gebrauch gemacht werden.

Für einen geordneten Vollzug des gegenständlichen Bundesgesetzes und zur Sicherstellung eines hohen Resilienzniveaus bezüglich der umfassten wesentlichen Dienste ist für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, wichtiger wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und

Sicherheit und die Erhaltung der Umwelt die Verarbeitung personenbezogener Daten kritischer Einrichtungen in dem gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne immer ein überwiegendes schutzwürdiges öffentliches Interesse an der Datenverarbeitung vor. Es ist daher erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO für alle nach diesem Bundesgesetz verarbeiteten personenbezogenen Daten vorzusehen. Eine Einzelfallabwägung, wie sie in Art. 21 Abs. 1 DSGVO vorgesehen ist, hätte überdies zur Folge, dass im Falle eines Widerspruchs durch die betroffene kritische Einrichtung eine weitere Datenverarbeitung mit Ausnahme der Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern die Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass die Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte eine Betroffene demnach verhindern, dass sie betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben (zB Aufsichtsmaßnahmen gegenüber kritischen Einrichtungen) – zumindest für die Dauer der Prüfung des Antrags – verarbeitet werden dürfen. Zur Aufrechterhaltung der öffentlichen Ordnung und Sicherheit als allgemeines öffentliches Interesse und zur Sicherstellung der mit der Verarbeitung personenbezogener Daten Betroffener verbundenen Kontroll-, Überwachungs- und Ordnungsfunktionen (siehe auch Art. 23 Abs. 1 lit. h DSGVO) ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der der Behörde übertragenen Aufgaben jedoch – bis zu deren gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Die Datenverarbeitung ist demnach – auch mit Blick auf die geopolitischen Entwicklungen sowie die aktuellen Bedrohungsszenarien – Grundvoraussetzung für die Aufrechterhaltung der gesamtstaatlichen Resilienz. Im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung wäre die Besorgung der Aufgaben nach diesem Bundesgesetz und ein geordneter, sparsamer und effizienter Vollzug sowie die Gewährleistung der physischen Sicherheit kritischer Einrichtungen nicht mehr möglich und würde diese Möglichkeit – etwa bei Einrichtungen, die die erforderlichen Resilienzmaßnahmen nicht ergriffen haben – auch eine erhebliche Missbrauchsgefahr mit sich bringen. Darüber hinaus liegt der Verarbeitung von bestimmten Daten eine unionsrechtliche Verpflichtung zugrunde. Der generelle Ausschluss der Rechte gemäß den Art. 18 und 21 DSGVO ist daher unerlässlich.

Ist die Verarbeitung unrechtmäßig bzw. benötigt der Verantwortliche die Daten nicht länger, sind die personenbezogenen Daten angesichts der strengen Zweckbindung ihrer Verarbeitung sowie des erhöhten Anspruchs an behördliche Register oder Dateisysteme, ausschließlich rechtmäßig verarbeitete personenbezogene Daten zu enthalten, umgehend zu löschen und soll es nicht möglich sein, dass die Betroffene lediglich die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. b und lit. c DSGVO verlangt.

Den für den Ausschluss des Widerspruchsrechts bzw. des Rechts auf Einschränkung der Verarbeitung einschlägigen Vorgaben des Art. 23 Abs. 2 DSGVO wird entsprechend Rechnung getragen. So ergeben sich aus den gesetzlichen Vorgaben zur Verarbeitung von personenbezogenen Daten nach diesem Bundesgesetz für den Ausschluss der Rechte gemäß den Art. 18 und 21 DSGVO insbesondere sowohl der Umfang der vorgenommenen Beschränkung und die Kategorien der betreffenden personenbezogenen Daten (siehe dazu die taxative Auflistung der Datenarten gemäß Abs. 1) als auch der für deren Verarbeitung Verantwortliche (vgl. Abs. 1), die Zwecke (vgl. etwa Abs. 2 bis 4) sowie die jeweiligen Speicherfristen (vgl. Abs. 5 und 6). Der Ausschluss des Rechts auf Widerspruch gegen die Verarbeitung von personenbezogenen Daten bezieht sich überdies selbstverständlich ausschließlich auf jene Daten, die in Übereinstimmung mit den gesetzlichen und unionsrechtlichen Vorgaben in rechtskonformer Weise verarbeitet werden. Den Betroffenen bleibt es zudem auch bei Ausschluss des Widerspruchsrechts sowie des Rechts auf Einschränkung der Verarbeitung unbenommen, hinsichtlich der Verarbeitung von sie betreffenden unrichtigen personenbezogenen Daten, unrechtmäßig verarbeiteten personenbezogenen Daten oder personenbezogenen Daten, deren Verarbeitung für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig ist, von ihrem Recht auf Berichtigung und Löschung gemäß den Art. 16 bis 17 DSGVO Gebrauch zu machen. Durch den Ausschluss der Rechte gemäß den Art. 18 und 21 DSGVO entsteht für die Betroffene daher auch kein Rechtsschutzdefizit. Als grundrechtsschützende Maßnahme und in Umsetzung des Art. 23 Abs. 2 lit. h DSGVO ist im letzten Satz vorgesehen, dass die Betroffenen in geeigneter Weise hierüber zu informieren sind. Ausdrücklich steht es der Behörde dabei frei, diese Information nicht an jede einzelne Betroffene individuell, sondern an „die Betroffenen“ in deren Gesamtheit zu richten. Die Information kann daher auch in allgemeiner Weise erteilt werden (zB auf der Homepage). Zudem soll auch die in Abs. 6 vorgesehene Protokollierungs- und Aufbewahrungspflicht insbesondere dazu dienen, Missbrauch sowie unrechtmäßige Zugänge zu bzw. unrechtmäßige Übermittlungen von personenbezogenen Daten hintanzuhalten.

Die Ausführungen lassen erkennen, dass das in der DSGVO vorgesehene Recht auf Widerspruch sowie das Recht auf Einschränkung der Verarbeitung in einem Spannungsverhältnis zur gesetzlich angeordneten Datenverarbeitung stehen. Die Bestimmung stellt demzufolge eine ausgewogene Abwägung zwischen den administrativen Interessen sowie dem Schutz der Betroffenen vor der Verarbeitung unrichtiger und unrechtmäßig verarbeiteter Daten dar und soll den unionsrechtskonformen Vollzug des gegenständlichen Gesetzes sowie die Funktionalität und die ordnungsgemäße Führung der vorgesehenen Datenverarbeitung gewährleisten.

Zu § 8 (Veröffentlichung von Sicherheitsvorfällen):

In Umsetzung von Art. 15 Abs. 4 letzter Satz RKE-RL, wonach die Mitgliedstaaten die Öffentlichkeit zu informieren haben, wenn sie zu der Ansicht gelangen, dass dies im öffentlichen Interesse gelegen ist, soll in dieser Bestimmung eine Ermächtigung des Bundesministers für Inneres vorgesehen werden, – nach verpflichtender vorheriger Anhörung der von einem Sicherheitsvorfall betroffenen kritischen Einrichtungen – personenbezogene Kontakt- und Identitätsdaten sowie sonstige erforderliche Informationen, die mit der Meldung zu einem Sicherheitsvorfall in Zusammenhang stehen, (zB mögliche Angreifer, Bezeichnung der betroffenen kritischen Einrichtungen, voraussichtliche Dauer, negative Auswirkungen) zu dem Zweck zu veröffentlichen, die Öffentlichkeit über Sicherheitsvorfälle zu unterrichten (vgl. in diesem Zusammenhang auch Art. 23 Abs. 7 NIS-2-RL, der unter bestimmten Voraussetzungen eine Information der Öffentlichkeit über erhebliche Sicherheitsvorfälle vorsieht). Diese Möglichkeit soll jedoch nur dann bestehen, sofern entweder die Sensibilisierung der Öffentlichkeit mit Blick auf die Verhütung sowie Bewältigung von Sicherheitsvorfällen erforderlich ist oder ein anderweitiges öffentliches Interesse an der Offenlegung besteht. Wesentlich ist, dass es sich bei dem Begriff „öffentliches Interesse“ um einen unbestimmten Rechtsbegriff handelt, dessen Auslegung nach höchstgerichtlicher Judikatur jedoch nicht dazu führen kann, dass unter diesen Begriff auch der Schutz von Einzelinteressen zu subsumieren wäre. Denn das öffentliche Interesse umfasst nur den Schutz bzw. das Schutzbedürfnis der Allgemeinheit (vgl dazu etwa auch VwSlg. 3316 F/1965). Aus der unmittelbaren Anwendbarkeit der DSGVO ergibt sich insbesondere, dass die Veröffentlichtung personenbezogener Daten selbstverständlich nur im unbedingt erforderlichen Ausmaß unter Beachtung der Grundsätze der Verhältnismäßigkeit und Datenminimierung erfolgen darf (vgl. etwa Art. 5 Abs. 1 lit. c DSGVO).

Zudem ist vorgesehen, dass der Veröffentlichung eine Interessenabwägung voranzugehen hat, in der die Auswirkungen der Offenlegung auf die Betroffenen zu berücksichtigen sind. Vor dem Hintergrund, dass davon auszugehen ist, dass die mit einer Meldung zu einem Sicherheitsvorfall im Zusammenhang stehenden Daten auch „sensible“ Informationen enthalten können (zB im Hinblick auf Sicherheitsvorfälle bei Einrichtungen der öffentlichen Verwaltung oder etwa Geschäftsgeheimnisse privater Einrichtungen), soll die ausdrückliche Klarstellung erfolgen, dass die Veröffentlichung nur insoweit – dh. in jenem Ausmaß bzw. Umfang – erfolgen darf, als diese keine Gefahr für die öffentliche Ordnung oder Sicherheit oder für die nationale Sicherheit darstellt (vgl. in diesem Zusammenhang auch die in § 23 vorgesehene Einschränkung). Unter „nationale Sicherheit“ wird üblicherweise die innere und äußere Staatssicherheit (zB militärische Landesverteidigung, Schutz der verfassungsmäßigen Einrichtungen) verstanden und können darunter Angelegenheiten der Außen-, Sicherheits- und Verteidigungspolitik verstanden werden (vgl. in diesem Zusammenhang auch § 2 des Bundesgesetzes über die Errichtung des Nationalen Sicherheitsrates, BGBl. I Nr. 122/2001). Im Fall einer Gefährdung dieser Schutzgüter wären wohl (nach einer Einzelfallabwägung) lediglich allgemeine Informationen über das Vorliegen eines Sicherheitsvorfalls öffentlich bekannt zu machen (zB ohne konkrete Rückschlüsse auf allfällige Sicherheitsmängel etc.).

Vor dem Hintergrund, dass sowohl andere Bundesministerien als auch die Länder von Sicherheitsvorfällen betroffen sein können, soll im Sinne einer raschen Reaktionsfähigkeit sowie mit Blick auf die rasche Eindämmung allfälliger Folgen in Abs. 2 zudem eine Verpflichtung des Bundesministers für Inneres, die im jeweiligen Wirkungsbereich betroffenen Bundesministerien sowie die betroffenen Länder über das Vorliegen eines Sicherheitsvorfalls zu informieren, statuiert werden.

Zu § 9 (Strategie für die Resilienz kritischer Einrichtungen):

Mit dieser Bestimmung soll Art. 4 RKE-RL umgesetzt werden. Zur Gewährleistung eines umfassenden Ansatzes in Bezug auf die Resilienz kritischer Einrichtungen (vgl. auch ErwGr 13 zur RKE-RL) soll die Strategie für die Resilienz kritischer Einrichtungen die für ein hohes Resilienzniveau erforderlichen strategischen Ziele und politischen Maßnahmen festlegen, wobei nach Möglichkeit auf bereits bestehenden sektorbezogenen Strategien, Plänen oder sonstigen vergleichbaren Dokumenten aufgebaut werden sollte. Wesentlich ist, dass die Strategie im Sinne eines umfassenden Gefahrenansatzes einen Rahmen für die Koordinierung von cyberbezogenen Risiken, Cyberbedrohungen und Cybersicherheitsvorfällen im Sinne der NIS-2-RL und von physischen Risiken, Bedrohungen und

Sicherheitsvorfällen im Sinne der RKE-RL, einschließlich der Wahrnehmung von Aufsichtsaufgaben, beinhalten soll.

Zur Erfüllung dieser unionsrechtlichen Vorgaben soll in Abs. 1 vorgesehen werden, dass der Bundesminister für Inneres verpflichtet ist, für die Bundesregierung eine derartige Strategie vorzubereiten und diese anlassbezogen, längstens jedoch alle vier Jahre, anzupassen, und soll den im jeweiligen Wirkungsbereich betroffenen Bundesministerien, den betroffenen Ländern sowie den in Betracht kommenden Interessenvertretungen (zB Wirtschaftskammer Österreich, Industriellenvereinigung, Österreichische Apothekerkammer, Österreichische Ärztekammer) Gelegenheit gegeben werden, sich vorab dazu zu äußern (zB schriftlich). Wie in der RKE-RL vorgesehen soll ein erstmaliger Beschluss der Bundesregierung spätestens bis zum 17. Jänner 2026 erfolgen (zur Relevanz der Strategie im Rahmen der Ermittlung kritischer Einrichtungen vgl. die Erläuterungen zu § 11 Abs. 1). Im Sinne der Transparenz wird es zudem grundsätzlich angezeigt sein, die von der Bundesregierung beschlossene Strategie zu veröffentlichen (etwa auf der Homepage des Bundesministeriums für Inneres) und entspricht diese Vorgangsweise auch der geübten Praxis.

Entsprechend den Vorgaben des Art. 4 Abs. 2 RKE-RL sollen in Abs. 2 folgende Mindestinhalte der Strategie aufgelistet werden:

- strategische Ziele (samt etwaiger Prioritäten) zur Verbesserung der Resilienz kritischer Einrichtungen, insbesondere unter Berücksichtigung grenzüberschreitender und sektorübergreifender, aber etwa auch sonstiger gegenseitiger Abhängigkeiten (Z 1)
- einen Steuerungsrahmen zur Verwirklichung der Ziele gemäß Z 1, insbesondere eine Beschreibung der Aufgaben der an der Umsetzung der Strategie beteiligten Akteure, wie etwa der jeweiligen Behörden (zB von den Sektoren betroffene Bundesminister oder Behörden, die gemäß Art. 46 der Verordnung [EU] 2022/2554 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen [EG] Nr. 1060/2009, [EU] Nr. 648/2012, [EU] Nr. 600/2014, [EU] Nr. 909/2014 und [EU] Nr. 2016/1011, ABl. Nr. L 333 vom 27.12.2022 S. 1, national als zuständige Behörden benannt oder eingerichtet wurden), kritischer Einrichtungen oder sonstiger Akteure (zB Interessenvertretungen; Z 2)
- eine Beschreibung der Maßnahmen zur Verbesserung der Resilienz kritischer Einrichtungen samt Beschreibung der Risikoanalyse gemäß § 10, wobei die konkreten Maßnahmen auf Grundlage der strategischen Ziele gemäß Z 1 zu beschreiben sein werden (Z 3)
- eine Beschreibung des behördlichen Verfahrens zur Ermittlung kritischer Einrichtungen gemäß § 11, dh. insbesondere wesentlicher Verfahrensschritte des verwaltungsbehördlichen Ermittlungsverfahrens, die der Feststellung des entscheidungsrelevanten Sachverhalts dienen (zB sofern zweckmäßig Befassung relevanter Interessenvertretungen sowie der jeweiligen in Betracht kommenden Einrichtungen im Sinne des Grundsatzes des Parteiengehörs; Z 4)
- eine Beschreibung der geplanten Unterstützungs- und Vorsorgemaßnahmen gemäß § 13 (zB Umfang sowie Verfahren) samt Maßnahmen zur Verbesserung der Zusammenarbeit zwischen dem öffentlichen Sektor und dem privaten Sektor sowie öffentlichen und privaten Einrichtungen (Z 5)
- eine Auflistung der zuständigen Behörden und insbesondere der an der Umsetzung der Strategie beteiligten Bundesministerien, Länder sowie Interessenvertretungen (für Beispiele siehe die Erläuterungen zu Abs. 1; Z 6)
- einen Ablauf bzw. politischen Rahmen für die Koordinierung zwischen den Bereichen der Resilienz kritischer Einrichtungen sowie Netz- und Informationssystemsicherheit zum Zweck des Informationsaustausches über Cybersicherheitsrisiken, Cyberbedrohungen und Cybersicherheitsvorfälle sowie über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle und für die Wahrnehmung der Aufsichtsaufgaben (zur erforderlichen Zusammenarbeit mit der NIS-Behörde vgl. auch die Erläuterungen zum Allgemeinen Teil; Z 7)
- eine Beschreibung von Maßnahmen (zB Einlasskontrollen), die – sofern sie bereits ergriffen wurden – den Verpflichtungen gemäß den §§ 14 bis 17 durch kleine und mittlere Unternehmen im Sinne des Anhangs der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl. Nr. L 124 vom 20.05.2003 S. 36, die gemäß § 11 als kritische Einrichtungen eingestuft wurden, entsprechen (Z 8).

Als Element einer starken Einbindung des Nationarats soll in Abs. 3 zudem vorgesehen werden, dass der Bundesminister für Inneres die gemäß Abs. 1 beschlossene Strategie innerhalb von drei Monaten ab Beschlussfassung an den Nationalrat zu übermitteln hat.

Zu § 10 (Risikoanalyse durch den Bundesminister für Inneres):

Ein maßgeblicher Inhalt einer Risikoanalyse besteht in der korrekten und verständlichen Beschreibung von identifizierten Risiken sowie der Ermittlung von Eintrittswahrscheinlichkeit und Darstellung der Auswirkungen anhand von Risikokriterien. Die Risikoanalyse beschäftigt sich vor allem mit der Fragestellung, welche Gefahren welche Auswirkungen auf den Betrieb und die Leistungserbringung kritischer Infrastrukturen haben oder haben könnten (vgl. auch § 3 Z 7 und 8). Strategisches Ziel der RKE-RL ist die Erhöhung der Resilienz kritischer Einrichtungen (vgl. dazu auch oben). Um dieses Ziel erreichen zu können, ist die Identifikation der Vulnerabilität kritischer Einrichtungen gegenüber Risiken maßgeblich. Nur auf diese Weise ist es möglich, Schwachstellen zu erkennen und zielgerichtete Maßnahmen zur Steigerung der Resilienz zu ergreifen.

Diesen Überlegungen zufolge soll in Umsetzung des Art. 5 RKE-RL dem Bundesminister für Inneres als zuständige Behörde gemäß Abs. 1 die Aufgabe zukommen, auf Grundlage der seitens der Europäischen Kommission – und allenfalls weiterer aufgrund einer Verordnung des Bundesministers für Inneres – festgelegten wesentlichen Dienste gemäß § 3 Z 6 spätestens bis zum 17. Jänner 2026 und im Anschluss anlassbezogen, längstens jedoch alle vier Jahre eine Risikoanalyse (vgl. § 3 Z 8) durchzuführen. Im Rahmen dieser Risikoanalyse soll zudem eine Aufschlüsselung nach den im Anhang der RKE-RL gelisteten Sektoren und Teilsektoren erfolgen, was bedeutet, dass sowohl eine gesamtstaatliche Bewertung als auch eine Bewertung auf „Branchenebene“ durchgeführt werden soll.

Mit Blick auf den der RKE-RL zugrunde liegenden „All-Gefahren-Ansatz“ ist es wesentlich, dass diese Bewertung sämtliche Risiken, die sich auf die Erbringung wesentlicher Dienste auswirken könnten, zu berücksichtigen hat, unabhängig davon, ob sie auf höhere Gewalt oder den Menschen zurückzuführen sind. Zu diesen Risiken können etwa Unfälle, Naturkatastrophen, Pandemien sowie hybride und andere feindliche Bedrohungen, einschließlich terroristischer Straftaten, gezählt werden (vgl. auch ErwGr 15 zur RKE-RL sowie die umfassende Definition des Begriffs „Risiko“ in § 3 Z 7).

Diese Risikoanalyse soll wiederum seitens der Behörde bei der Ermittlung kritischer Einrichtungen gemäß § 11 (vgl. dazu auch die Erläuterungen zu § 11 Abs. 1) sowie bei der Unterstützung kritischer Einrichtungen gemäß § 13 im Rahmen des Ergreifens von Resilienzmaßnahmen Beachtung finden.

Gemäß Abs. 2 sollen bei Durchführung der Risikoanalyse andere allgemeine sowie sektorspezifische Risikoanalysen aufgrund einschlägiger Rechtsakte der Union zu berücksichtigen sein und ist eine entsprechende demonstrative Auflistung vorgesehen. Darüber hinaus sollen jedoch auch sonstige für die Durchführung der Risikoanalyse maßgebliche Informationen herangezogen werden (arg: „insbesondere“).

Zudem ist – in Umsetzung der Regelung in Art. 5 Abs. 2 RKE-RL – vorgesehen, dass auch die entsprechenden Risiken, die sich aus dem Ausmaß der Abhängigkeit zwischen den im Anhang genannten Sektoren, einschließlich dem Ausmaß der Abhängigkeit dieser Sektoren gegenüber in anderen Mitgliedstaaten und Drittstaaten ansässigen Einrichtungen ergeben, sowie die Auswirkungen, die ein in einem Sektor auftretender Sicherheitsvorfall (vgl. dazu § 11 Abs. 1 Z 4 in Verbindung mit Abs. 2) auf andere Sektoren haben kann, einbezogen werden (Z 3). Schließlich sollen – sofern vorhanden – sämtliche gemäß § 17 gemeldeten Informationen über Sicherheitsvorfälle in die Analyse aufgenommen werden (Z 4).

Die relevanten Elemente der Risikoanalyse sollen den kritischen Einrichtungen gemäß Abs. 3 in anonymisierter Form zur Verfügung gestellt werden. Wesentlich ist demnach, dass keine Zuweisung allfälliger personenbezogener Daten zu einer identifizierten oder identifizierbaren Einrichtung erfolgen kann.

Zu § 11 (Ermittlung kritischer Einrichtungen):

Die Maßnahmen der Mitgliedstaaten zur Ermittlung kritischer Einrichtungen und zur Gewährleistung ihrer Resilienz sollen einem risikobasierten Ansatz folgen, bei dem diejenigen Einrichtungen im Fokus stehen, die für die Erfüllung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten am bedeutendsten sind (vgl. auch ErwGr 15 zur RKE-RL). Um sicherzustellen, dass alle entsprechenden Einrichtungen auch tatsächlich den Resilienzanforderungen der RKE-RL unterliegen, wurden auf unionsrechtlicher Ebene harmonisierte Vorschriften festgeschrieben, die einerseits eine einheitliche Ermittlung kritischer Einrichtungen in der gesamten Union sicherstellen und es andererseits ermöglichen, den Aufgaben und der Bedeutung dieser Einrichtungen auf nationaler Ebene angemessen Rechnung zu tragen (vgl. ErwGr 16 zur RKE-RL).

Mit gegenständlicher Bestimmung soll Art. 6 RKE-RL umgesetzt werden. Gemäß Abs. 1 soll der Bundesminister für Inneres verpflichtet sein, sämtliche kritischen Einrichtungen für jede der im Anhang der RKE-RL angeführten Kategorie von Einrichtungen der gelisteten Sektoren und Teilsektoren mit Bescheid als kritisch einzustufen. Wesentlich ist, dass die bescheidmäßige Einstufung unter Heranziehung

der gemäß § 9 erstellten Strategie sowie der gemäß § 10 durchgeführten Risikoanalyse erfolgen soll, die erstmalig spätestens bis zum 17. Jänner 2026 von der Bundesregierung zu beschließen bzw. vom Bundesminister für Inneres durchzuführen sein soll (vgl. dazu die vorgeschlagenen Regelungen in § 9 Abs. 1 sowie § 10 Abs. 1 sowie die unionsrechtlichen Verpflichtungen gemäß Art. 4 Abs. 1 RKE-RL bzw. Art. 5 Abs. 1 RKE-RL). Darauf basierend soll die RKE-Behörde in einem weiteren Schritt die erstmalige Einstufung – wie es sich aus Art. 6 Abs. 1 RKE-RL ergibt – längstens bis zum 17. Juli 2026 vorzunehmen haben, wobei Einrichtungen an der Feststellung des für die Einstufung als kritische Einrichtung maßgeblichen Sachverhalts mitzuwirken haben sollen (vgl. in diesem Zusammenhang die Regelung in § 11 Abs. 10, wonach kritische Einrichtungen auch verpflichtet sein sollen, Änderungen des für die Einstufung maßgeblichen Sachverhalts unverzüglich bekanntzugeben). Damit soll im Sinne der Rechtsprechung des VwGH zu § 39 Abs. 2 des Allgemeinen Verwaltungsverfahrensgesetzes 1991 (AVG), BGBl. Nr. 51/1991, klargestellt werden, dass mit dem Grundsatz der Amtswegigkeit des Verwaltungsverfahrens die Pflicht der Parteien, an der Ermittlung des Sachverhalts mitzuwirken, korrespondiert, was gerade dort von Bedeutung ist, wo ein Sachverhalt nur im Zusammenwirken mit der Partei geklärt werden kann, weil die Behörde außerstande ist, sich die Kenntnis von ausschließlich in der Sphäre der Partei liegenden Umständen von Amts wegen zu beschaffen (vgl. VwGH 18.07.2023, Ra 2022/10/0093). Die Anforderungen an die Mitwirkungspflicht in amtswegig eingeleiteten Verfahren sind zwar grundsätzlich weniger streng als jene im Antragsverfahren (vgl. VwGH 09.04.2013, 2011/04/0001), jedoch werden auch im Verfahren zur Ermittlung kritischer Einrichtungen regelmäßig Informationen seitens der Einrichtungen benötigt werden, damit eine tatsachenbasierte Einstufung erfolgen kann.

Um den Aufgaben und der Bedeutung der jeweiligen Einrichtungen Rechnung zu tragen, soll es für die Einstufung erforderlich sein, dass seitens der in Betracht kommenden Einrichtung bestimmte Kriterien kumulativ erfüllt werden. Demnach ist vorgesehen, dass eine Einrichtung zunächst nur dann als „kritisch“ einzustufen ist, sofern sie in Österreich tätig ist (Z 1), was bedeutet, dass sie Tätigkeiten ausübt, die für den betreffenden wesentlichen Dienst bzw. für die betreffenden wesentlichen Dienste erforderlich sind (vgl. ErwGr 16 zur RKE-RL).

Zudem soll nur dann eine Ermittlung möglich sein, wenn sich deren kritische Infrastruktur (zB Umspannwerk, Pipeline, Raffinerie) im Inland befindet (Z 2). Auch wenn in vielen Fällen der Ort der Niederlassung der kritischen Einrichtung derselbe wie jener sein wird, an dem die Dienstleistungen erbracht werden oder an dem sich die kritische Infrastruktur befindet, ist es wesentlich, dass der Ort der Niederlassung als solcher nicht entscheidend sein soll. Demnach ist es nicht zwingend erforderlich, dass auch eine Niederlassung in Österreich besteht, sondern ist lediglich ausschlaggebend, dass tatsächlich Dienstleistungen in Österreich erbracht werden und auch kritische Infrastrukturen im Inland vorhanden sind.

Die zu ermittelnde Einrichtung hat zudem einen wesentlichen Dienst oder mehrere wesentliche Dienste (vgl. dazu die Definition in § 3 Z 6) zu erbringen (Z 3). Ob dieser wesentliche Dienst (zB Elektrizitätsversorgung im Sektor „Energie“, Erbringung von Gesundheitsdienstleistungen im Sektor „Gesundheit“, Erbringung von Vertrauensdiensten im Sektor „digitale Infrastruktur“; vgl. dazu auch die Delegierte Verordnung [EU] 2023/2450), in Österreich erbracht wird, soll hingegen – im Gegensatz zu den in Z 1 und Z 2 gelisteten Voraussetzungen, die explizit auf das Inland abstellen – irrelevant sein. Damit soll der Intention, Einrichtungen zu schützen, die Tätigkeiten im Binnenmarkt erbringen, die insbesondere für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen von entscheidender Bedeutung sind, Rechnung getragen werden und die zunehmend verflochtene Unionswirtschaft Berücksichtigung finden.

Des Weiteren soll lediglich dann eine Einstufung als kritische Einrichtung erfolgen, wenn – aufgrund ihrer Bedeutung für die Daseinsvorsorge – ein Sicherheitsvorfall im Sinne einer erheblichen Störung (vgl. die Definition in § 3 Z 3 sowie die in Abs. 2 festgelegten Parameter) eintreten könnte (Z 4).

Liegen die in Abs. 1 festgelegten Voraussetzungen nicht oder (auch nur) teilweise nicht vor, soll keine Verpflichtung (und auch keine Möglichkeit) zur Ermittlung kritischer Einrichtungen in dem entsprechenden Sektor oder Teilsektor bestehen (siehe auch ErwGr 16 zur RKE-RL). Im Hinblick darauf, dass etwa der in Anhang II der NIS-2-RL genannte Sektor „Forschung“ im Anhang zur RKE-RL nicht aufgelistet ist, können Einrichtungen in diesem Sektor (zB Einrichtungen im Bildungs-, Hochschul- oder Forschungsbereich) nicht als kritische Einrichtungen ermittelt werden.

Zur Bestimmung des Ausmaßes einer durch einen Sicherheitsvorfall verursachten Störung wurden in Art. 7 Abs. 1 RKE-RL Kriterien festgelegt. Um Anstrengungen der Mitgliedstaaten betreffend die Ermittlung der Betreiber wesentlicher Dienste im Sinne der NIS-1-RL und die diesbezüglich gewonnenen

Erfahrungen zu nutzen, erfolgte dabei eine enge Anlehnung an jene in der NIS-1-RL gelisteten Parameter (vgl. auch ErwGr 18 zur RKE-RL).

Im Hinblick auf die Beurteilung, ob ein Sicherheitsvorfall gemäß Abs. 1 Z 4 die erhebliche Störung bei der Erbringung der wesentlichen Dienste verursachen würde, sollen in Umsetzung der in Art. 7 RKE-RL vorgesehenen Regelung die in Abs. 2 taxativ gelisteten Parameter zu berücksichtigen sein. Dazu zählen die Zahl der Nutzer eines von der jeweiligen Einrichtung erbrachten wesentlichen Dienstes gemäß Abs. 1 Z 3 (Z 1) sowie das Ausmaß der Abhängigkeit anderer im Anhang der RKE-RL gelisteter Sektoren sowie Teilsektoren von einem von der Einrichtung erbrachten wesentlichen Dienst (Z 2). Vor dem Hintergrund, dass schwere Krisen, wie etwa die COVID-19-Pandemie, gezeigt haben, wie wichtig es ist, die Sicherheit von Lieferketten zu gewährleisten, und diese auch die negativen wirtschaftlichen und gesellschaftlichen Auswirkungen sowohl auf etliche Sektoren als auch auf grenzüberschreitender Ebene vor Augen geführt haben, ist es essenziell, dass im Rahmen der Bestimmung des Ausmaßes der Abhängigkeit anderer Sektoren und Teilsektoren von wesentlichen Diensten einer kritischen Einrichtung auch die Auswirkungen auf Lieferketten mitberücksichtigt werden (vgl. ErwGr 18 zur RKE-RL). Zudem sollen die möglichen Auswirkungen von Sicherheitsvorfällen im Sinne von Ausmaß und Dauer auf bestimmte taxativ genannte Rechtsgüter Berücksichtigung finden (Z 3) und soll auch der Marktanteil der jeweiligen Einrichtung auf dem Markt für wesentliche Dienste oder für die betreffenden wesentlichen Dienste in die Beurteilung miteinbezogen werden (Z 4). Vor dem Hintergrund, dass etwa auch die Wirtschaft, die Freizügigkeit und die Sicherheit der Unionsbürger vom ordnungsgemäßen Funktionieren der kritischen Infrastrukturen abhängen, sollen in diesem Zusammenhang auch potenzielle Bedrohungen durch ausländische Beteiligungen an kritischen Infrastrukturen in der Union anerkannt werden (vgl. ErwGr 19 zur RKE-RL). Demnach soll das von einem Sicherheitsvorfall potenziell betroffene geografische Gebiet, einschließlich etwaiger grenzüberschreitender Auswirkungen, Berücksichtigung finden und soll in diesem Zusammenhang auch auf allfällige Schwachstellen, die aus der Abgeschiedenheit bestimmter geografischer Gebiete, wie insbesondere Bergregionen oder sonstige isolierte Gebiete, resultieren, Bedacht genommen werden (Z 5). Des Weiteren ist vorgesehen, dass die Bedeutung der Einrichtung für die Aufrechterhaltung des wesentlichen Dienstes in die Beurteilung einbezogen werden soll, wobei die Verfügbarkeit alternativer Mittel für die Erbringung des jeweiligen wesentlichen Dienstes angemessen zu berücksichtigen sein wird (Z 6).

In diesem Zusammenhang ist zu beachten, dass eine Festlegung von (innerstaatlichen) Schwellenwerten (vgl. dazu auch Art. 7 Abs. 2 lit. c RKE-RL) lediglich zur Spezifizierung jener Einrichtungen möglich ist, die für die Daseinsvorsorge von einer solchen entscheidenden Bedeutung sind, sodass eine Störung bei der Erbringung eines wesentlichen Dienstes das Ausmaß der Erheblichkeit im Sinne eines Sicherheitsvorfalls annehmen würde. Im Hinblick darauf, dass betreffend die Festlegung wesentlicher Dienste im Gegensatz zur NIS-1-RL für das RKE-Regime ein delegierter Rechtsakt der Europäischen Kommission erlassen wurde (siehe dazu oben sowie § 3 Z 6), ist hingegen eine Einschränkung bzw. eine Adaptierung wesentlicher Dienste etwa in Form von Schwellenwerten (vgl. die Regelungen in der Netz- und Informationssystemsicherheitsverordnung [NISV], BGBl. II Nr. 215/2019) nicht zulässig (sehr wohl aber eine Ausdehnung, vgl. ErwGr 41 zur RKE-RL).

Die Verpflichtungen kritischer Einrichtungen zum Treffen von Resilienzmaßnahmen (§ 15) sowie die Meldeverpflichtungen (§ 17) sollen gemäß Abs. 3 nach Ablauf von zehn Monaten nach rechtskräftiger Ermittlung (vgl. § 13 des Verwaltungsgerichtsverfahrensgesetzes – VwGVG, BGBl. I Nr. 33/2013) gemäß Abs. 1 gelten (vgl. auch Art. 6 Abs. 3 Unterabsatz 2 RKE-RL). Die Verpflichtung zur Durchführung von Risikoanalysen gemäß § 14 soll im Gegensatz dazu bereits innerhalb von neun Monaten nach rechtskräftiger Einstufung als kritische Einrichtung bestehen (vgl. dazu die vorgeschlagene Regelung in § 14 Abs. 1 sowie die unionsrechtliche Verpflichtung gemäß Art. 12 Abs. 1 RKE-RL).

Im Interesse der Wirksamkeit, Effizienz, Kohärenz und Rechtssicherheit (vgl. auch ErwGr 16 zur RKE-RL) soll gemäß Abs. 4 vorgesehen werden, dass kritische Einrichtungen im gemäß Abs. 1 zu erlassenden Bescheid sowohl über ihre Verpflichtung zur Bekanntgabe einer zentralen Kontaktstelle und einer Ansprechperson (Abs. 6), eines Zustellungsbevollmächtigten gemäß § 9 des Zustellgesetzes (ZustG), BGBl. Nr. 200/1982, (Abs. 7), eines verantwortlichen Beauftragten gemäß § 9 VStG (Abs. 8) und von Änderungen des für die Einstufung maßgeblichen Sachverhalts (Abs. 10 zweiter Satz), zur Durchführung einer Risikoanalyse (§ 14) sowie zum Ergreifen von Resilienzmaßnahmen (§ 15) als auch zur Meldung von Sicherheitsvorfällen (§ 17) zu informieren sind. Zudem sollen sie darüber in Kenntnis zu setzen sein, dass eine Verpflichtung zur Mitteilung besteht, sofern die jeweilige kritische Einrichtung für oder in mindestens sechs Mitgliedstaaten wesentliche Dienste erbringt (§ 19 Abs. 1). Diese Information soll selbstverständlich auch den Zeitpunkt umfassen, ab dem die Verpflichtungen gemäß den §§ 14, 15, 17 und 19 Abs. 1 auf sie Anwendung finden (vgl. Abs. 3 sowie § 14 Abs. 1).

Mit der NIS-2-RL werden Einrichtungen im Sektor digitale Infrastruktur, die für eine Einstufung als kritische Einrichtungen im Sinne der RKE-RL in Frage kommen könnten, verpflichtet, geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit von Netz- und Informationssystemen zu beherrschen, sowie erhebliche Sicherheitsvorfälle und Cyberbedrohungen zu melden. Vor dem Hintergrund, dass Gefahren für die Sicherheit von Netz- und Informationssystemen unterschiedliche Ursachen haben können, wird in der NIS-2-RL ebenfalls ein gefahrenübergreifender Ansatz angewandt, der sowohl die Resilienz von Netz- und Informationssystemen als auch die physischen Komponenten und das physische Umfeld dieser Systeme umfasst (vgl. auch ErwGr 20 zur RKE-RL). Da die in der NIS-2-RL diesbezüglich festgelegten Anforderungen mit Blick auf Inhalt und Umfang den entsprechenden Verpflichtungen aus der RKE-RL zumindest gleichwertig sind, sollen die in Abs. 6 sowie den §§ 14, 15, 17 und 19 festgelegten Verpflichtungen aus dem RKE-Bereich für Einrichtungen im Sektor digitale Infrastruktur nicht gelten. Zudem ist die Resilienz von Einrichtungen in den Sektoren Bankwesen und Finanzmarktinfrastrukturen durch die in Rechtsvorschriften der Union enthaltenen umfassenden Anforderungen für Finanzunternehmen ebenfalls vollumfänglich abgedeckt (vgl. ErwGr 20 und 21 zur RKE-RL). Um Doppelarbeit und unnötigen Verwaltungsaufwand zu vermeiden, ist daher in Art. 8 RKE-RL eine entsprechende Ausnahmebestimmung für die in diesen Bereichen bzw. Sektoren tätigen kritischen Einrichtungen vorgesehen (vgl. auch die Erläuterungen zu § 18 Abs. 3). Durch die Regelung in Abs. 5 soll demnach sichergestellt werden, dass kritische Einrichtungen in den im Anhang der RKE-RL gelisteten Sektoren Bankwesen, Finanzmarktinfrastrukturen und digitale Infrastruktur gleichzeitig mit Bescheiderlassung auch darüber zu informieren sind, dass die Verpflichtungen gemäß Abs. 6 (Bekanntgabe einer zentralen Kontaktstelle sowie einer Ansprechperson) sowie gemäß den §§ 14 (Risikoanalyse), 15 (Resilienzmaßnahmen), 17 (Meldepflicht bei Sicherheitsvorfällen) und 19 (allfällige Mitteilungspflicht sowie zusätzliche Verpflichtungen für kritische Einrichtungen von besonderer europäischer Bedeutung) auf sie keine Anwendung finden.

Um die Zusammenarbeit zu erleichtern und zur Sicherstellung einer schnellen Reaktionsfähigkeit, raschen Erreichbarkeit sowie funktionierenden Kommunikation zwischen dem Bundesminister für Inneres sowie den jeweiligen kritischen Einrichtungen sollen in Umsetzung der Regelung in Art. 13 Abs. 3 RKE-RL nach Abs. 6 kritische Einrichtungen dem Bundesminister für Inneres innerhalb von zwei Wochen nach Rechtskraft des Ermittlungsbescheides eine zentrale Kontaktstelle (samt Erreichbarkeiten), beispielsweise ein Funktionspostfach, sowie eine Ansprechperson als direkte Kommunikationsschiene namhaft zu machen bzw. – sofern eine derartige „Stelle“ noch nicht besteht – einzurichten haben und sollen jegliche die zentrale Kontaktstelle oder die namhaft gemachte Ansprechperson betreffenden Änderungen ohne Aufschub, längstens jedoch binnen zwei Wochen bekanntzugeben sein. Wesentlich ist, dass die Erreichbarkeit der zentralen Kontaktstelle sowie des „Verbindungsbeauftragten“ während des Zeitraums, in dem die betreffende kritische Einrichtung ihre wesentlichen Dienste erbringt, gewährleistet ist. Über diese Verpflichtung soll ebenfalls im Bescheid gemäß Abs. 1 zu informieren sein.

Das ZustG regelt die physische und elektronische Zustellung von behördlichen und (verwaltungs-)gerichtlichen Dokumenten an deren Adressaten (Näheres vgl. *Bumberger/Schmid*, Praxiskommentar zum Zustellgesetz [2018] § 1 ZustG) und hat der Bundesgesetzgeber – aufgrund des Bedürfnisses nach Erlassung einheitlicher Vorschriften – die Bedarfskompetenz nach Art. 11 Abs. 2 B-VG durch Erlassung dieses Gesetzes in Anspruch genommen. Wird demnach keine (abweichende) materienspezifische Regelung vorgenommen, finden die Regelungen des ZustG (automatisch) Anwendung. Vor dem Hintergrund der Tatsache, dass eine Niederlassung im Inland nicht erforderlich sein soll, um als kritische Einrichtung eingestuft werden zu können (vgl. dazu die Erläuterungen zu Abs. 1), soll in Abs. 7 insofern eine materienspezifische Abweichung von § 10 Abs. 1 ZustG vorgenommen werden, als kritische Einrichtungen, die über keine Abgabestelle (vgl. § 2 Z 4 ZustG) im Inland verfügen, dem Bundesminister für Inneres verpflichtend einen Zustellungsbevollmächtigten gemäß § 9 ZustG namhaft zu machen haben. Eine derartige Abweichung ist zur richtlinienkonformen Umsetzung zwingend erforderlich (vgl. Art. 11 Abs. 2 zweiter Halbsatz B-VG), um sicherzustellen, dass auch gegenüber kritischen Einrichtungen ohne Abgabestelle im Inland eine wirksame Zustellung von behördlichen Dokumenten (zB des konstitutiven Ermittlungsbescheids) erfolgen kann. Durch den Verweis auf § 9 ZustG ist auch § 9 Abs. 2 letzter Satz ZustG anwendbar, wonach das Erfordernis des Hauptwohnsitzes im Inland nicht für Staatsangehörige von EWR-Vertragsstaaten gilt, falls Zustellungen durch Staatsverträge mit dem Vertragsstaat des Wohnsitzes des Zustellungsbevollmächtigten oder auf andere Weise sichergestellt sind.

Von seiner Bedarfskompetenz gemäß Art. 11 Abs. 2 B-VG hat der Bundesgesetzgeber auch durch die Erlassung des VStG Gebrauch gemacht. § 9 VStG regelt die verwaltungsstrafrechtliche Verantwortlichkeit bei Tatbegehung von juristischen Personen oder eingetragenen Personengesellschaften und wird statutarischen Vertretungsorganen die Möglichkeit zu einer Verantwortlichkeitsübertragung

durch Bestellung sogenannter „verantwortlicher Beauftragter“ eingeräumt (vgl. *Lewisch/Fister/Weilguni*, Verwaltungsstrafgesetz [2023] § 9 Rz 1). In Anbetracht der Tatsache, dass auch jene Einrichtungen vom RKE-Regime umfasst sind, die – wie bereits oben erläutert – nicht zwangsläufig eine Niederlassung im Inland haben (vgl. auch die Erläuterungen zu Abs. 1), solche Einrichtungen jedoch nach den Vorgaben der RKE-RL ebenso zu beaufsichtigen sowie zu sanktionieren sind, ist es aufgrund der unionsrechtlichen Vorgaben (sowie im Hinblick darauf, dass sich eine diesbezügliche Zusammenarbeit insbesondere mit Drittstaaten als schwierig erweisen kann) unbedingt erforderlich, dass eine verpflichtende Benennung eines verantwortlichen Beauftragten erfolgt, um die strafrechtliche Verantwortlichkeit solcher Einrichtungen sicherzustellen. Als Abweichung zur Regelung in § 9 Abs. 2 VStG (wonach die Möglichkeit zur Bestellung verantwortlicher Beauftragter besteht) soll demzufolge in Abs. 8 bereits gesetzlich normiert werden, dass kritische Einrichtungen ohne Niederlassung im Inland dem Bundesminister für Inneres verpflichtend einen verantwortlichen Beauftragten gemäß § 9 VStG zu benennen haben, dem die Verantwortung für die Einhaltung der Verwaltungsvorschriften nach diesem Bundesgesetz obliegt. Betreffend die Voraussetzungen soll ein Verweis auf die Regelungen in § 9 VStG erfolgen, was bedeutet, dass der Verantwortliche insbesondere lediglich eine Person mit Hauptwohnsitz im Inland oder in einem EWR-Vertragsstaat sein kann, die strafrechtlich verfolgt werden kann, ihrer Bestellung nachweislich zugestimmt hat und der für den ihrer Verantwortung unterliegenden klar abzugrenzenden Bereich eine entsprechende Anordnungsbefugnis zugewiesen ist (vgl. § 9 Abs. 4 VStG). Da in § 9 Abs. 4 VStG auf den „Hauptwohnsitz“ (und nicht den „Sitz“) abgestellt wird, leitet der VwGH mit Blick auf die Gesetzesterminologie ab, dass nur die Bestellung natürlicher Personen als verantwortliche Beauftragte in Betracht kommen kann (vgl. VwGH 16.5.2011, 2009/17/0185).

In Abs. 9 soll eine gesetzliche Grundlage dafür geschaffen werden, den Bescheid gemäß Abs. 1 aufzuheben, sobald die erforderlichen Voraussetzungen nachträglich wegfallen. Wesentlich ist, dass ein solcher „Aufhebungsbescheid“ unverzüglich nach Kenntnisnahme des Wegfalls der für die Einstufung maßgeblichen Voraussetzungen durch den Bundesminister für Inneres zu erlassen sein soll, zumal kritische Einrichtungen aufgrund ihrer Verpflichtungen nach diesem Bundesgesetz insbesondere finanziellen sowie personellen Belastungen ausgesetzt sind. Ab dem Zeitpunkt der Zustellung dieses „Aufhebungsbescheids“ sollen die in diesem Bundesgesetz für kritische Einrichtungen vorgesehenen Verpflichtungen für die jeweilige Einrichtung keine Anwendung mehr finden.

Vor dem Hintergrund der in Art. 6 Abs. 3 RKE-RL vorgesehenen Regelung soll in Abs. 10 normiert werden, dass den Bundesminister für Inneres die Verpflichtung trifft, eine Liste mit den ermittelten kritischen Einrichtungen zu erstellen, diese in regelmäßigen Abständen, längstens jedoch alle vier Jahre zu überprüfen und allenfalls bei Bedarf anzupassen. Für diese Zwecke soll – auch mit Blick auf die im Rahmen des Einstufungsverfahrens vorgesehene Mitwirkungspflicht gemäß Abs. 1 – vorgesehen werden, dass (bereits) als kritisch eingestufte Einrichtungen verpflichtet sind, dem Bundesminster für Inneres für die Einstufung maßgebliche Änderungen (zB bei Erbringung weiterer wesentlicher Dienste) unverzüglich (zur Auslegung des Begriffs „unverzüglich“ vgl. die Erläuterungen zu § 14 Abs. 1) bekanntzugeben.

Zu § 12 (Kritische Einrichtungen im Sektor öffentliche Verwaltung):

Gemäß der in Art. 2 Z 10 RKE-RL angeführten Begriffsdefinition in Zusammenschau mit dem Anhang zur RKE-RL gilt als eine „Einrichtung der öffentlichen Verwaltung“ eine als solche in einem Mitgliedstaat nach nationalem Recht anerkannte Einrichtung von Zentralregierungen, mit Ausnahme der Justiz, der Parlamente und der Zentralbanken. Diese Regelung definiert demnach „Einrichtungen der öffentlichen Verwaltung“ und legt kumulative Voraussetzungen fest, die erfüllt werden müssen, damit solche Einrichtungen unter das RKE-Regime fallen. Wesentlich ist, dass die Verpflichtung, Einrichtungen der öffentlichen Verwaltung in den Anwendungsbereich einzubeziehen, im Gegensatz zur NIS-2-RL, die – nach einer risikobasierten Bewertung – allenfalls auch Einrichtungen der öffentlichen Verwaltung auf „regionaler Ebene“ (verpflichtend) umfasst, auf Einrichtungen der öffentlichen Verwaltung der „Zentralregierung“ beschränkt ist (vgl. Sektor 9. „Öffentliche Verwaltung“ gemäß dem Anhang zur RKE-RL).

Durch die Regelung in Abs. 1 soll diese unionsrechtliche Bestimmung innerstaatlich abgebildet und sollen – abweichend von den im vorgeschlagenen § 11 Abs. 1 Z 1 bis 4 vorgesehenen Kriterien – im Sektor der öffentlichen Verwaltung auf Bundesebene Einrichtungen (nur) dann als kritisch ermittelt werden, wenn die in Z 1 bis 4 gelisteten kumulativen Voraussetzungen vorliegen. Die übrigen in § 11 vorgesehenen Bestimmungen sollen hingegen anwendbar sein (etwa die Verpflichtung zur Mitwirkung gemäß § 11 Abs. 1 vorletzter Satz). Wesentlich ist, dass der unionsrechtliche Terminus „Zentralregierung“ mit Blick auf den im B-VG abgebildeten österreichischen (föderalen) Staatsaufbau als die Ebene des „Bundes“ zu verstehen ist, weshalb eine innerstaatliche Einschränkung auf Einrichtungen der öffentlichen Verwaltung auf Bundesebene erfolgen soll. Die „regionale“ (Länder) und „lokale Ebene“

(Gemeinden) soll hingegen – in Übereinstimmung mit der RKE-RL – nicht vom RKE-Regime umfasst sein.

Vorgesehen ist, dass eine Einrichtung (vgl. dazu die Begriffsbestimmung in § 3 Z 11, wonach als „Einrichtung“ nicht nur natürliche und juristische Personen sowie eingetragene Personengesellschaften, sondern auch Stellen der öffentlichen Verwaltung, zB Bundesminister, gelten sollen) im Sektor der öffentlichen Verwaltung auf Bundesebene nur dann als kritisch zu ermitteln ist, wenn sie zum Zweck eingerichtet (zB im Sinne von gesetzlich eingerichtet oder gegründet) wurde, im öffentlichen Interesse (vgl. zu der Begrifflichkeit auch die Erläuterungen zu § 8) liegende Aufgaben nicht gewerblicher Art zu erfüllen (Z 1).

Unter „im öffentlichen Interesse liegende Aufgaben“ ist ein gewisser Kernbereich von Agenden (etwa im Bereich der Daseinsvorsorge) zu verstehen, die im Interesse des Gemeinwohls vom Staat als Träger des Interesses der Gesamtheit besorgt wird. Im Vordergrund dabei steht nicht ausschließlich die Förderung von Einzelinteressen, sondern die Förderung von gemeinsamen Interessen der Gesamtbevölkerung oder von einzelnen Bevölkerungsgruppen. Eine diesbezügliche Orientierung bieten etwa Art. 14 und 106 Abs. 2 AEUV samt einschlägiger Judikatur des EuGH. Dass bei der Erfüllung derartiger öffentlicher Aufgaben wirtschaftliche Grundsätze zu beachten sind (vgl. etwa Art. 126b Abs. 5 B-VG), steht einer Ausrichtung auf das Allgemeininteresse nicht entgegen.

Eine weitere kumulative Voraussetzung nach Z 1 für die Qualifikation als Einrichtung der öffentlichen Verwaltung ist die Besorgung von „Aufgaben nicht gewerblicher Art“. Das Kriterium der „nicht gewerblichen Art“ soll den Begriff der im öffentlichen Interesse liegenden Aufgaben im Sinne dieser Bestimmung präzisieren und führt somit zu einer weiteren Begriffseinschränkung. Das Vorliegen von im öffentlichen Interesse liegenden Aufgaben nicht gewerblicher Art ist objektiv zu beurteilen und schließt der Begriff demnach nicht Aufgaben aus, die von Privatunternehmen erfüllt werden können. Das Vorliegen eines entwickelten Wettbewerbs und insbesondere der Umstand, dass die jeweilige Einrichtung auf dem betreffenden Markt im Wettbewerb steht, stellt (nur) ein Indiz dafür dar, dass es sich um eine Aufgabe gewerblicher Art handelt.

Hinsichtlich der Beurteilungskriterien der Erfüllung von „Aufgaben nicht gewerblicher oder gewerblicher Art“ wird auf eine Gesamtbetrachtung abzustellen sein, bei der insbesondere folgende Aspekte zu berücksichtigen sind: Die Tatsache, dass keine Gewinnerzielungsabsicht verfolgt wird, ist ein Indiz für das Vorliegen einer „Aufgabe nicht gewerblicher Art“, da eine „gewerbliche Tätigkeit“ grundsätzlich auf die Erwirtschaftung eines unternehmerischen Gewinns ausgerichtet ist. Der EuGH verneint jedoch das Vorliegen einer Gewinnerzielungsabsicht selbst dann, wenn die Tätigkeit zwar zu Gewinnen führen würde, das Erzielen des Gewinnes jedoch nicht den Hauptzweck der Einrichtung darstellt (EuGH 22.5.2003, C-18/07 [*Korhonen*] Rz 54). Unter einer Einrichtung, die Aufgaben „gewerblicher Art“ besorgt, ist hingegen eine Einrichtung zu verstehen, die in Konkurrenz mit privaten Wirtschaftstreibenden unter den gleichen Bedingungen (dh. unter Beachtung der gleichen wirtschaftlichen Regeln) wie diese am allgemeinen Wirtschaftsleben (Marktwettbewerb) teilnimmt und das wirtschaftliche Risiko (Insolvenzrisiko) ihres Handelns trägt. Das Fehlen wirtschaftlicher Risikotragung (Verlustausgleich durch die öffentliche Hand) oder das Tätigwerden nach anderen als Leistungs-, Effizienz- und Wirtschaftskriterien sind Indizien einer Aufgabenerfüllung nicht gewerblicher Art. Eine Teilnahme am regulären Wirtschaftsleben ist wohl dann nicht anzunehmen, wenn eine staatliche Kontrolle oder die Möglichkeit einer Einflussnahme auf die Unternehmensgebarung nach staatsspezifischen Kriterien erfolgen kann, gleichgültig auf welche Art diese verwirklicht wird.

Daraus ergibt sich für die Frage, ob die Kriterien nach Z 1 erfüllt werden, dass auf die Nähe der jeweiligen Einrichtung zum originär staatlichen Tätigkeitsbereich abzustellen ist. Weisen die Tätigkeiten der Einrichtungen demnach kommerziellen Charakter mit Gewinnerzielungsabsicht auf oder verfolgt die jeweilige Einrichtung private Einzelinteressen, soll sie von dieser Bestimmung nicht umfasst sein und demnach nicht unter den Sektor der öffentlichen Verwaltung fallen. Es wird daher im Ergebnis insbesondere zu beurteilen sein, ob die Einrichtung an den gleichen wirtschaftlichen Zielsetzungen ausgerichtet ist wie die Tätigkeit anderer Wirtschaftsteilnehmer.

Als weiteres (kumulatives) Kriterium soll die Einrichtung gemäß Z 2 – in Anlehnung an die österreichische Terminologie sowie die innerstaatliche verfassungsrechtliche Ausgestaltung – zur Erfüllung von Angelegenheiten der Bundesverwaltung berufen sein und zusätzlich alternativ entweder Rechtspersönlichkeit besitzen (zB Gesellschaften mit beschränkter Haftung, Anstalten öffentlichen Rechts) oder als Bundesbehörde eingerichtet worden sein (zB Bundesminister). Aufgrund der Anknüpfung an „Angelegenheiten der Bundesverwaltung“ soll klargestellt werden, dass – im Einklang mit der RKE-RL, die auf die „Zentralregierung“ abstellt (siehe dazu oben) – etwa die Ebene der Landesverwaltung nicht umfasst ist. Durch das (alternative) Abstellen auf die „Einrichtung als

Bundesbehörden“ soll zudem bewusst eine Anlehnung an Art. 10 Abs. 1 Z 16 B-VG erfolgen und durch die Umschreibung der Organisationskompetenz (vgl auch *Muzak*, Bundes-Verfassungsrecht[6] [2020] Art. 10 Rz 86) ein organisatorischer Behördenbegriff zum Ausdruck gebracht werden, zumal nach dem RKE-Regime die „Organisation“ an sich eine resiliente Umgebung bzw. (organisationsrechtliche) Rahmenbedingungen zu schaffen hat und diese Verpflichtung nicht an die Aufgabenwahrnehmung per se anknüpft. Daraus ergibt sich, dass ausschließlich organisatorisch als Bundesbehörde eingerichtete Behörden umfasst sein sollen; Landesbehörden, die bloß funktional als Bundesbehörden fungieren, sollen hingegen ausgeschlossen sein.

Vor dem Hintergrund der Tatsache, dass die „regionale“ sowie „lokale“ Ebene im Sektor öffentliche Verwaltung nicht vom RKE-Regime umfasst sein soll (siehe oben), soll in Z 2 ausdrücklich klargestellt werden, dass die Gebietskörperschaften Länder und Gemeinden nicht unter die Begriffsdefinition fallen. Zudem soll eine ausdrückliche Ausnahme für Gemeindeverbände geschaffen werden.

Eine weitere Einschränkung ergibt sich durch Z 3. Demnach sollen nur jene Einrichtungen zu ermitteln sein, die – alternativ – der Aufsicht des Bundes unterstehen (erster Fall) oder die an die Weisungen eines obersten Organs des Bundes gebunden sind (zweiter Fall) oder die ein Leitungs- oder Aufsichtsorgan (wer darunter zu subsumieren ist vgl. die entsprechenden Materiengesetze, dazu zählen etwa Geschäftsführer oder Aufsichtsräte; vgl. zB § 70 des Aktiengesetzes [AktG], BGBl. Nr. 98/1965; § 15 des GmbH-Gesetzes [GmbHG], RGBl. Nr. 58/1906) haben, das mehrheitlich aus Mitgliedern besteht, die von Bundesbehörden oder von anderen auf Bundesebene eingerichteten Körperschaften des öffentlichen Rechts eingesetzt worden sind (dritter Fall) oder die überwiegend im Eigentum des Bundes stehen (vierter Fall), wobei bei letzter Variante hinsichtlich der Terminologie mit Blick auf eine kongruente Ausgestaltung eine Anknüpfung an die verfassungsrechtlich vorgesehenen parlamentarischen Kontrollrechte (vgl. Art. 52 Abs. 2 B-VG) bzw. an die Rechnungshofkontrolle (vgl. Art. 126b Abs. 2 B-VG) erfolgte. Vor dem Hintergrund der Regelung in Art. 19 B-VG, wonach oberste Organe der Vollziehung sowohl keinem anderen Organ gegenüber weisungsgebunden sind (vgl. VfSlg. 9536/1982; vgl. auch VfSlg. 6885/1972) als auch keine sachlich in Betracht kommende Oberbehörde in Frage kommt (vgl. VfSlg. 3506/1959, 4259/1962), soll – aufgrund innerstaatlicher Besonderheiten und im Sinne einer unionsrechtskonformen Umsetzung – zudem vorgesehen werden, dass auch dann eine bescheidmäßige Ermittlung erfolgen kann, sofern die Einrichtung ein – zu den obersten Organen des Bundes zählendes – Mitglied der Bundesregierung (Art. 69 B-VG) ist (letzter Fall).

Abschließend soll in Z 4 normiert werden, dass lediglich jene Einrichtungen ermittelt werden sollen, die ermächtigt sind, im Rahmen ihrer gesetzlich übertragenen Aufgaben in Vollziehung von Unionsrecht im eigenen Namen Bescheide mit Auswirkungen auf den Binnenmarkt bzw. die Grundfreiheiten zu erlassen. Generelle Rechtsakte (Verordnungen) hingegen sollen – in Anlehnung an Art. 2 Z 10 lit. d RKE-RL, der auf „Entscheidungen“ Bezug nimmt – von dieser Regelung nicht umfasst sein. Im Hinblick darauf, dass etwa Dienststellen oder Abteilungen einer Bundesbehörde mangels Behördenfunktion nicht befugt sind, Bescheide im eigenen Namen zu erlassen, soll auch keine Möglichkeit bestehen, diese gesondert als kritische Einrichtungen im Sektor öffentliche Verwaltung zu ermitteln.

Die RKE-RL berührt nicht die Zuständigkeit der Mitgliedstaaten und ihrer Behörden hinsichtlich der Verwaltungsautonomie sowie ihre Verantwortung für den Schutz der nationalen Sicherheit und Verteidigung oder ihre Befugnis zum Schutz anderer wesentlicher staatlicher Funktionen, insbesondere in Bezug auf die öffentliche Sicherheit, die territoriale Unversehrtheit und die Aufrechterhaltung der öffentlichen Ordnung (vgl. ErwGr 11 zur RKE-RL). Der Ausschluss von Einrichtungen der öffentlichen Verwaltung vom Anwendungsbereich dieser Richtlinie gilt daher gemäß Art. 1 Abs. 6 RKE-RL für Einrichtungen, deren Tätigkeiten überwiegend in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten, ausgeübt werden. Einrichtungen der öffentlichen Verwaltung, deren Tätigkeiten nur geringfügig mit diesen Bereichen zusammenhängen, sollen hingegen in den Anwendungsbereich fallen (vgl. ErwGr 11 zur RKE-RL).

Die Regelung in Abs. 2 soll diese unionsrechtlich vorgesehene Ausnahme abbilden und soll demnach vorgesehen werden, dass Einrichtungen im Sektor der öffentlichen Verwaltung, deren Wirkungsbereiche überwiegend die nationale Sicherheit einschließlich der militärischen Landesverteidigung, die öffentliche Sicherheit oder die Strafverfolgung (einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten) umfassen, nicht unter die Bestimmungen dieses Bundesgesetzes fallen. Wenngleich die militärische Landesverteidigung als Teil der nationalen Sicherheit von der in Abs. 2 vorgeschlagenen Ausnahme ohnehin mitumfasst ist (vgl. dazu auch die Erläuterungen zu § 8), soll diese im Sinne der Rechtssicherheit ausdrückliche Erwähnung finden, zumal auch in Art. 1 Abs. 6 RKE-RL ausdrücklich zwischen den Bereichen der nationalen Sicherheit und der Verteidigung differenziert wird. Vor dem Hintergrund der Regelung in Art. 9a B-VG, wonach der Begriff der „umfassenden Landesverteidigung“

auch die geistige, zivile und wirtschaftliche Landesverteidigung umfasst, soll überdies mit Blick auf die Intention der Regelung und im Sinne der innerstaatlichen Terminologie eine Einschränkung der Ausnahmebestimmung auf die von der nationalen Sicherheit umfasste „militärische Landesverteidigung“ erfolgen.

Zur Ausnahme für „Justiz, Parlamente und Zentralbanken“ siehe die Erläuterungen zu § 2 Abs. 3.

Zu § 13 (Unterstützungs- und Vorsorgemaßnahmen):

Unbeschadet der eigenen rechtlichen Verantwortung kritischer Einrichtungen, die in der vorliegenden Richtlinie enthaltenen Verpflichtungen einzuhalten, sind Mitgliedstaaten gemäß Art. 10 RKE-RL dazu verpflichtet, diese beim Ausbau ihrer Resilienz zu unterstützen und sollte dadurch übermäßigem Verwaltungsaufwand vorgebeugt werden (vgl. ErwGr 25 zur RKE-RL). Diese Unterstützung kann insbesondere die Entwicklung von Leitfäden und Methoden, die Unterstützung der Organisation von Übungen zur Überprüfung der Resilienz sowie die Beratung und Bereitstellung von Schulungen für das Personal kritischer Einrichtungen umfassen.

Mit gegenständlicher Bestimmung soll Art. 10 RKE-RL umgesetzt und die Verpflichtung des Bundesministers für Inneres, kritische Einrichtungen bei der Verbesserung ihrer Resilienz zu unterstützen sowie mit diesen Informationen austauschen, festgeschrieben werden.

In einer beispielhaften Aufzählung soll eine Auflistung allfälliger Unterstützungs- und Vorsorgemaßnahmen erfolgen. Diese umfassen insbesondere die Entwicklung und Bereitstellung von generellen Empfehlungen und Leitfäden für kritische Einrichtungen zur Prävention von Sicherheitsvorfällen und Reduktion von Risiken sowie die Zurverfügungstellung von etwa Vorlagen und Mustern für Risikoanalysen und Resilienzpläne (Z 1) sowie die Beratung beim Ergreifen von Resilienzmaßnahmen (Z 6). Damit könnte es einerseits kritischen Einrichtungen erleichtert werden, ihren Verpflichtungen gemäß den §§ 14 und 15 nachzukommen, andererseits kann auf diese Weise auch eine Angleichung der vorzulegenden Dokumente bewirkt werden, was eine effizientere Vorgehensweise auf Vollzugsebene ermöglicht. Als weitere Beispiele sind etwa die Beratung bei der Festlegung von Resilienzmaßnahmen und der Organisation von und Mitwirkung an Sicherheitsübungen sowie Übungen zur Überprüfung der Notfallpläne (Z 2), die Beratung und Durchführung von Schulungen für das Personal kritischer Einrichtungen (Z 3), die Bereitstellung von Informationen zum Thema physische Sicherheit sowie die Organisation und Durchführung von Kampagnen zur Bewusstseinsbildung und Sensibilisierung insbesondere für physische Bedrohungen sowie zur Stärkung und Erweiterung von Fähigkeiten und Kenntnissen im Bereich der physischen Sicherheit (Z 4) und die Übermittlung von Frühwarnungen („early warnings“) an kritische Einrichtungen, sofern ein Risiko vorliegt, sowie von sonstigen sektorspezifischen Informationen (Z 5) genannt. Vor dem Hintergrund, dass es oftmals wohl nicht eindeutig sein wird, ob bereits bestehende Risikoanalysen gemäß § 14 Abs. 3 oder Resilienzmaßnahmen gemäß § 15 Abs. 5 zumindest gleichwertig sind, wäre es – vor allem mit Blick auf die Eingrenzung allfälliger Verwaltungsstrafverfahren – ebenfalls sehr hilfreich, diesbezügliche Beratungen durchzuführen (Z 7). Weitere mögliche Unterstützungsmaßnahmen stellen die Durchführung von langfristigen strategischen Analysen betreffend Bedrohungen der physischen Sicherheit und Sicherheitsvorfälle (Z 8), die Beratung der in ihrem Wirkungsbereich betroffenen Bundesminister und öffentlichen Einrichtungen zum Forschungs- und Förderbedarf und zu den Forschungs- und Förderprioritäten im Bereich der physischen Sicherheit (Z 9), die Verfolgung von Entwicklungen und gegebenenfalls Mitarbeit an der Er- und Überarbeitung von Normen mit Bezug auf die physische Sicherheit (Z 10), die Mitwirkung und Teilnahme an nationalen, europäischen und internationalen Forschungs- und Förderprojekten und -programmen auf dem Gebiet der physischen Sicherheit (Z 11) sowie die Übermittlung sachdienlicher Folgeinformationen gemäß § 17 Abs. 5 sowie die Information der Öffentlichkeit gemäß § 8 dar (Z 12). Die entsprechende Datenverarbeitungsermächtigung findet sich in der in § 7 Abs. 4 vorgeschlagenen Regelung.

Durch die vorgesehenen Unterstützungsmaßnahmen soll es möglich sein, kritischen Einrichtungen ein breitgestreutes und zugleich spezialisiertes Wissen im RKE-Bereich zur Verfügung zu stellen und soll dadurch ein wesentlicher Beitrag zur Erhöhung der gesamtstaatlichen Resilienz Österreichs geleistet werden. Die RKE-Behörde soll demnach als Schnittstelle zwischen dem öffentlichen und privaten Sektor verschiedene Aufgaben etwa im Bereich der Bewusstseinsbildung, Stärkung entsprechender Kompetenzen und Prävention von Sicherheitsvorfällen wahrnehmen.

Zu § 14 (Risikoanalyse durch kritische Einrichtungen):

Kritischen Einrichtungen sollten die potenziellen Verluste oder Störungen, denen sie ausgesetzt sind, in ihrer Gesamtheit bekannt sein, weshalb gemäß Art. 12 RKE-RL eine entsprechende Verpflichtung (auch) kritischer Einrichtungen vorgesehen ist, eine Risikoanalyse durchzuführen. Diese Analyse hat sich auf

alle Ereignisse zu beziehen, die die Erbringung ihrer wesentlichen Dienste stören und demnach zu einem Sicherheitsvorfall (§ 3 Z 3) führen könnten (vgl. auch ErwGr 28 zur RKE-RL).

Mit der gegenständlichen Bestimmung soll Art. 12 RKE-RL umgesetzt werden. Damit kritische Einrichtungen auch tatsächlich Kenntnis über die sie betreffenden Risiken (vgl. die Definition in § 3 Z 7) haben, sind Gefahren zu beschreiben bzw. zu identifizieren, deren Eintrittswahrscheinlichkeit zu ermitteln und Auswirkungen anhand von Risikokriterien darzustellen. Als Gefahren kommen etwa Naturgefahren (Hochwasser, Sturm, Erdbeben etc.), intentionale Gefahren (Sabotage, Spionage, Gewalthandlungen etc.), anthropogene Gefahren (Abhängigkeiten von ausländischen Technologien, fehlendes Fachpersonal, Verschuldungskrise etc.) und technische Gefahren (fehlerhafte Software, manipulierte bzw. unsichere Hardware, Datenmissbrauch etc.) in Betracht. Demnach soll in Abs. 1 vorgesehen werden, dass kritische Einrichtungen erstmals innerhalb von neun Monaten nach Rechtskraft des Bescheids gemäß § 11 und im Anschluss anlassbezogen (etwa bei Änderungen der maßgeblichen Risikofaktoren), längstens jedoch alle vier Jahre, eine Risikoanalyse (vgl. die Definition in § 3 Z 8) durchzuführen haben. Aus § 11 Abs. 1 iVm §12 Abs. 1 ergibt sich, dass auch kritische Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene (§ 12) von dieser Verpflichtung umfasst sein sollen. Als Grundlage für die Risikoanalyse durch kritische Einrichtungen soll die durch den Bundesminister für Inneres gemäß § 10 durchzuführende Risikoanalyse dienen.

Die Risikoanalyse hat demzufolge auch mit Blick auf den der RKE-RL zugrunde liegenden All-Gefahren-Ansatz allen entsprechenden natürlichen und vom Menschen verursachten Gefahren bzw. Ereignissen, die zu einem Sicherheitsvorfall führen könnten, einschließlich grenzüberschreitenden oder sektorübergreifenden Ereignissen, Unfällen, Naturkatastrophen, gesundheitlichen Notlagen, hybriden und anderen feindlichen Bedrohungen, Rechnung zu tragen und auch dem „Stand der Technik“ zu entsprechen (vgl. in diesem Zusammenhang auch die in § 13 Z 1 vorgesehene Möglichkeit zur Unterstützung der kritischen Einrichtungen durch Bereitstellung von Vorlagen für eine Risikoanalyse).

Kritische Einrichtungen sollen zudem verpflichtet sein, die Ergebnisse ihrer Risikoanalyse unverzüglich, längstens jedoch binnen eines Monats, an den Bundesminister für Inneres zu übermitteln. Mit Blick auf die Regelungen in § 20 ist wesentlich, dass die Ergebnisse übersichtlich und in strukturierter Form aufbereitet sind, damit diese auch der behördlichen Überprüfung zugrunde gelegt werden können. Bei der vorgesehenen „unverzüglichen“ Übermittlung soll von einem Handeln „so bald als möglich“, „ohne unnötigen Aufschub“ bzw. „ohne schuldhaftes Zögern“ auszugehen sein (vgl. VwGH 10.10.2014, Ro 2014/02/0020), wobei eine „Maximalfrist“ von einem Monat vorgesehen sein soll.

In Abs. 2 soll zudem vorgesehen werden, dass die Risikoanalyse das Ausmaß der Abhängigkeit anderer im Anhang der RKE-RL gelisteter Sektoren von dem wesentlichen Dienst, der von der kritischen Einrichtung (gegebenenfalls auch in benachbarten Mitgliedstaaten oder Drittstaaten) erbracht wird, und das Ausmaß der Abhängigkeit der kritischen Einrichtung von den wesentlichen Diensten, die von anderen Einrichtungen in anderen Sektoren erbracht werden, zu berücksichtigen hat, zumal solche Interdependenzen weitreichende Folgen nach sich ziehen könnten.

Haben kritische Einrichtungen aufgrund von Verpflichtungen aus anderen Rechtsakten Risikoanalysen vorgenommen oder entsprechende Dokumente erstellt, die für die Risikoanalyse durch kritische Einrichtungen nach dem RKE-Regime relevant sind, sollen diese Bewertungen und Dokumente verwendet werden können, um die in der vorliegenden Richtlinie hinsichtlich der Risikoanalyse durch kritische Einrichtungen festgelegten Anforderungen zu erfüllen. Bei der Wahrnehmung ihrer Aufsichtsfunktion soll gemäß Art. 12 Abs. 2 Unterabsatz 2 RKE-RL die Möglichkeit der zuständigen Behörde bestehen, eine bestehende Risikoanalyse, die den Anforderungen des Art. 12 RKE-RL entspricht, als vollständig oder teilweise den Verpflichtungen nach diesem Artikel entsprechend zu erklären (vgl. auch ErwGr 28 zur RKE-RL).

Demnach soll in Abs. 3 angeordnet werden, dass den Anforderungen gemäß dieser Bestimmung insoweit – ganz oder teilweise – entsprochen wird, als von der kritischen Einrichtung aufgrund anderer rechtlicher Verpflichtungen (diese können entweder innerstaatlich oder unionsrechtlich vorgesehen sein; vgl. ErwGr 27 zur RKE-RL) Risikoanalysen durchgeführt wurden, die hinsichtlich der Anforderungen zumindest gleichwertig sind. Diesbezüglich ist kein eigenes Bescheidverfahren vorgesehen, sondern soll die Überprüfung der Gleichwertigkeit im Rahmen der Aufsichtsmaßnahmen erfolgen. Ergibt sich im Rahmen der Überprüfung, dass die in dieser Bestimmung normierten Anforderungen nicht oder nicht vollständig erfüllt werden und auch aufgrund anderer rechtlicher Verpflichtungen keine Risikoanalyse durchgeführt wurde, die einer Gleichwertigkeitsprüfung standhält, soll nach § 20 Abs. 5 vorgegangen werden, wonach der Bundesminister für Inneres der kritischen Einrichtung bescheidmäßig aufzutragen hat, innerhalb einer angemessenen Frist und nachweislich erforderliche und verhältnismäßige Maßnahmen zu ergreifen, die zur Herstellung des rechtmäßigen Zustands erforderlich sind. In diesem

Zusammenhang wird auf die in § 13 Z 7 vorgesehene Möglichkeit zur Unterstützung bei der Beurteilung, ob die Anforderungen bereits bestehender Risikoanalysen gleichwertig sind, verwiesen (vgl. auch die Erläuterungen zu § 13).

Auch ohne ausdrückliche Anordnung soll selbstverständlich auch die Möglichkeit bestehen, bereits bestehende bzw. aufgrund anderer rechtlicher Verpflichtungen erstellte Dokumente im Rahmen der Risikoanalyse heranzuziehen.

Zu beachten ist in diesem Zusammenhang, dass selbstverständlich auch die zeitlichen Anforderungen gemäß Abs. 1 erfüllt sein müssen.

Zu § 15 (Resilienzmaßnahmen kritischer Einrichtungen):

In Art. 13 RKE-RL ist vorgesehen, dass kritische Einrichtungen technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu ergreifen haben, die mit Blick auf die sie betreffenden Risiken angemessen und geeignet sind. Ziel dieser Maßnahmen ist es, Sicherheitsvorfälle zu verhindern, sich davor zu schützen, sie abzuwehren, darauf zu reagieren, die Folgen solcher Vorfälle zu begrenzen, Sicherheitsvorfälle zu bewältigen sowie sich von diesen zu erholen (ErwGr 29 zur RKE-RL).

In Umsetzung von Art. 13 RKE-RL soll in Abs. 1 vorgesehen werden, dass sämtliche kritische Einrichtungen (vgl. dazu die Erläuterungen zu § 14) basierend auf den seitens des Bundesministers für Inneres bereitgestellten Elementen der gemäß § 10 durchgeführten Risikoanalyse sowie den Ergebnissen der gemäß § 14 durchgeführten Risikoanalyse geeignete und verhältnismäßige Maßnahmen technischer, sicherheitsbezogener und organisatorischer Art (lediglich; im Gegensatz zur NIS-2-RL, vgl. Art. 21 NIS-2-RL) in Bezug auf die von ihnen bereitgestellten wesentlichen Dienste (zur Definition vgl. § 3 Z 6) zu treffen haben. Diese Maßnahmen sollen dazu dienen, die physische Sicherheit bzw. Resilienz sicherzustellen und haben kritische Einrichtungen demnach die Fähigkeit zu besitzen, Sicherheitsvorfällen (vgl. § 3 Z 3) vorzubeugen, diese zu erkennen, abzuwehren sowie zu beseitigen. Vorgesehen ist zudem, dass kritische Einrichtungen einen Resilienzplan mit einer nachvollziehbar aufbereiteten Auflistung dieser Maßnahmen (vgl. § 3 Z 12) zu erstellen haben, der gemäß Abs. 3 in geeigneter Form unverzüglich, längstens jedoch binnen eines Monats, nach erstmaliger Erstellung sowie im Anschluss anlassbezogen (zB bei Adaptierungen) an den Bundesminister für Inneres zu übermitteln sein soll (zur Auslegung des Begriffs „unverzüglich“ vgl. die Erläuterungen zu § 14 Abs. 1).

Resilienzmaßnahmen nach Abs. 1 haben – wie bereits näher erläutert – geeignet und verhältnismäßig zu sein und soll dadurch insbesondere ein „risikobasierter Ansatz“ verfolgt werden. Einzelheiten und Umfang dieser Maßnahmen sollen demnach die „besondere Situation“ (vgl. auch ErwGr 29 zur RKE-RL) der betreffenden Einrichtung auf angemessene und verhältnismäßige Weise widerspiegeln. Damit ein einheitlicher Ansatz der Union gefördert wird, ist beabsichtigt, dass die Kommission nach Konsultation der Gruppe für die Resilienz kritischer Einrichtungen nicht verbindliche Leitlinien erlässt, in denen solche technischen, sicherheitsbezogenen und organisatorischen Maßnahmen näher ausgeführt werden. Arbeiten zu diesem Thema auf europäischer Ebene sollen jedenfalls Berücksichtigung finden. Darüber hinaus sollen auch allfällige bereits bestehende und etablierte internationale Standards beachtet werden.

Auch ohne ausdrückliche Anordnung sollen Resilienzmaßnahmen dem Stand der Technik entsprechen.

Basierend auf der Regelung in Art. 6 Abs. 3 Unterabsatz 2 RKE-RL soll vorgesehen werden, dass die Resilienzmaßnahmen innerhalb von zehn Monaten nach bescheidmäßiger Einstufung zu treffen sind.

In Abs. 2 soll eine abstrakte Festlegung möglicher Resilienzmaßnahmen erfolgen. Normiert werden soll, dass es sich dabei insbesondere um jene Maßnahmen handeln soll, die erforderlich sind, um

- das Auftreten von Sicherheitsvorfällen zu verhindern, unter Berücksichtigung von Maßnahmen zur Katastrophenvorsorge und zum Umgang mit dem Klimawandel (Z 1),
- einen angemessen physischen Schutz der kritischen Infrastrukturen und der Räumlichkeiten der kritischen Einrichtungen (mit Bezug zum wesentlichen Dienst, vgl. Abs. 1) zu gewährleisten, wie das Aufstellen von Zäunen und Absperrungen sowie die Einführung von Instrumenten und Verfahren für die Überwachung der Umgebung, die Verwendung von Detektionsgeräten sowie die Durchführung von Zugangskontrollen (Z 2),
- Sicherheitsvorfälle abzuwehren, diese zu bewältigen und die Auswirkungen solcher Vorfälle gering zu halten, unter Berücksichtigung von Risiko- und Krisenmanagementmaßnahmen sowie Notfallplänen bzw. vorgegebener Abläufe im „Alarmfall“ (Z 3),
- nach Sicherheitsvorfällen die Fortsetzung oder rasche Wiederaufnahme des wesentlichen Dienstes zu gewährleisten, unter Berücksichtigung von Maßnahmen zur Aufrechterhaltung des Betriebs (zB Sicherstellung einer Notstromversorgung) bzw. alternativer Lieferketten (Z 4),

- angemessene personelle Sicherheitsvorkehrungen zu gewährleisten, insbesondere die Festlegung von Anforderungen an die Ausbildung sowie die Qualifikation des Personals und die Identifizierung von kritischen Funktionen samt Festlegung von Zugangsberechtigungen, etwa zu Räumlichkeiten, kritischen Infrastrukturen sowie sensiblen Informationen, sowie Verpflichtungen zur Vornahme von Zuverlässigkeitsüberprüfungen für bestimmte „Kategorien“ von Personal, das die Anforderungen gemäß dem vorgeschlagenen § 16 Abs. 1 Z 1 oder 2 erfüllt (dh. vor allem jenes Personal, das ein entsprechendes „Sicherheitsrisiko“ darstellt), unter Berücksichtigung des Personals externer Dienstleister, (Z 5) und
- das betroffene Personal insbesondere durch Schulungsmaßnahmen bzw. Qualifikationen oder Übungen im Hinblick auf die Steigerung der Resilienz zu sensibilisieren (Z 6).

Wesentlich ist, dass eine Sicherheitsüberprüfung gemäß den §§ 55 bis 55b SPG, eine Verlässlichkeitsprüfung gemäß den §§ 23 und 24 des Militärbefugnisgesetzes (MBG), BGBl. I Nr. 86/2000, oder eine Zuverlässigkeitsüberprüfung gemäß § 134a des Luftfahrtgesetzes (LFG), BGBl Nr. 253/1957, als einer Zuverlässigkeitsüberprüfung gemäß dem vorgeschlagenen § 16 (im Folgenden: ZÜP) grundsätzlich gleichwertig zu betrachten ist und wird daher regelmäßig kein Bedarf für die Durchführung einer ZÜP bestehen, sofern die jeweilige Überprüfung nicht länger als drei Jahre zurückliegt und keine Anhaltspunkte vorliegen, wonach die betroffene Person nicht mehr zuverlässig sein könnte. Damit soll es kritischen Einrichtungen ermöglicht werden, ihren Personalentscheidungen bestimmte gleichwertige Überprüfungen zugrunde zu legen (vgl. dazu außerdem auch die Erläuterungen zu § 16 Abs. 1 und 6).

Vorgesehen ist zudem in Abs. 4, dass kritische Einrichtungen hinsichtlich der getroffenen Resilienzmaßnahmen ein ausreichendes Qualitätsmanagement sicherzustellen haben. Demnach soll nicht nur die Verpflichtung bestehen, Resilienzpläne zu erstellen, sondern sollte etwa auch angedacht werden, in angemessenen Zeitabständen Übungen abzuhalten sowie diese zu evaluieren und zu dokumentieren. Die Resilienzpläne sollten demnach in angemessenen Zeitabständen auf ihre Aktualität sowie auf Schwachstellen geprüft und bei Bedarf aktualisiert werden, wobei insbesondere auch Erfahrungen aus vergangenen Sicherheitsvorfällen bzw. aus entsprechenden Übungen zu berücksichtigen sein werden. Wesentlich ist, dass auch bei einem Sicherheitsvorfall so lange wie möglich die für die Bevölkerung notwendigen Leistungen erbracht werden können.

Vergleichbar mit der in § 14 Abs. 3 vorgeschlagenen Regelung soll in Abs. 5 normiert werden, dass der in gegenständlicher Bestimmung vorgesehenen Verpflichtung zum Treffen von Resilienzmaßnahmen insoweit entsprochen wird, als von der kritischen Einrichtung aufgrund anderer rechtlicher Verpflichtungen Resilienzmaßnahmen ergriffen wurden, die hinsichtlich der in Abs. 1 genannten technischen, sicherheitsbezogenen und organisatorischen Anforderungen zumindest gleichwertig sind. Sind demnach kritische Einrichtungen aufgrund von Bestimmungen des Unionsrechts oder des nationalen Rechts verpflichtet, Maßnahmen zur Gewährleistung ihrer eigenen Resilienz zu ergreifen, sollen diese Anforderungen bei der Beurteilung, ob die kritische Einrichtung die in Abs. 1 normierten Verpflichtungen eingehalten hat, angemessen und in entsprechendem Ausmaß berücksichtigt werden (vgl. dazu auch ErwGr 27 zur RKE-RL). Hat demnach die kritische Einrichtung bereits technische, sicherheitsbezogene und organisatorische Maßnahmen zur Verbesserung ihrer Resilienz ergriffen, so sollen diese, um Doppelbelastungen zu vermeiden, entsprechende Berücksichtigung finden (siehe auch ErwGr 30 zur RKE-RL), wobei die Überprüfung der Gleichwertigkeit im Rahmen der Aufsichtsmaßnahmen aufgrund einer Einzelfallbeurteilung erfolgen soll (vgl. dazu auch die Erläuterungen zu § 14 Abs. 3 sowie die in § 13 Z 7 vorgesehene Möglichkeit zur Unterstützung bei der Beurteilung, ob die Anforderungen bereits bestehender Resilienzmaßnahmen gleichwertig sind).

Haben kritische Einrichtungen Dokumente (zB Resilienzpläne) erstellt, die für die in Abs. 1 genannten Maßnahmen relevant sind, soll selbstverständlich auch die Möglichkeit bestehen, diese zur Erfüllung der in dieser Regelung vorgesehenen Verpflichtung heranzuziehen (vgl. Art. 13 Abs. 2 RKE-RL).

Wie zu § 14 Abs. 3 erläutert soll die Anerkennung gleichwertiger Maßnahmen jedoch keine dauerhafte Entbindung von den Verpflichtungen zur Folge haben, sondern soll nach wie vor die in Abs. 1 vorgesehene Aktualisierungspflicht Beachtung finden.

Zu § 16 (Zuverlässigkeitsüberprüfungen):

Die gegenständliche Bestimmung dient der Umsetzung von Art. 14 RKE-RL. Gemäß ErwGr 32 zur RKE-RL obliegt es den Mitgliedstaaten, als Teil der sicherheitsbezogenen Maßnahmen zur Gewährleistung der Resilienz kritischer Einrichtungen die Bedingungen, unter denen eine kritische Einrichtung Anträge auf Durchführung von ZÜP bestimmter Personen stellen darf, festzulegen. Zu diesem Zweck sollen seitens der kritischen Einrichtung Kategorien von Personal zu benennen sein, die eine ZÜP durchlaufen müssen (vgl. § 15 Abs. 2 Z 5), weil sie entweder über einen Zugang auf ihre Räumlichkeiten, Informationen oder

Kontrollsysteme verfügen, eine Funktion mit einem solchen Zugriff anstreben oder sonstige sensible Funktionen für kritische Einrichtungen wahrnehmen oder anstreben (vgl. Abs. 1).

Um unter Berücksichtigung von Art. 14 Abs. 2 RKE-RL zu gewährleisten, dass ZÜP stets „verhältnismäßig und strikt auf das Notwendige“ beschränkt bleiben, soll sich die Erforderlichkeit der Durchführung zusätzlich aus der Risikoanalyse gemäß § 10 zu erschließen haben. Bei Vorliegen einer der in § 15 Abs. 2 Z 5 abschließend genannten gleichwertigen Überprüfungen wird – vorbehaltlich einer abweichenden Einschätzung durch die kritische Einrichtung – in der Regel kein Anlass für die Durchführung einer ZÜP bestehen, sofern die Überprüfung nicht länger als drei Jahre zurückliegt und keine Anhaltspunkte bestehen, wonach die betroffene Person nicht mehr zuverlässig sein sollte (vgl. dazu außerdem auch die Erläuterungen zu § 15 Abs. 2 Z 5). Der maßgebliche Zeitraum von drei Jahren ab dem Überprüfungszeitpunkt entspricht der Geltungsdauer der ZÜP und ist daher auch hinsichtlich der prinzipiell jährlich zu wiederholenden ZÜP nach § 134a LFG heranzuziehen, zumal diese in ihrem Umfang der ZÜP nach diesem Gesetzesentwurf weitestgehend entspricht.

Zwecks Durchführung der ZÜP soll die kritische Einrichtung dem Bundesminister für Inneres zusätzlich zu den für die Überprüfung erforderlichen personenbezogenen Daten ein begründetes Ersuchen zu übermitteln haben. In diesem Ersuchen soll insbesondere dargelegt werden, inwiefern die zu überprüfende Person eine sensible Funktion für die kritische Einrichtung wahrnimmt oder wahrnehmen soll und allenfalls warum trotz Vorliegens einer aufrechten ZÜP oder einer gleichwertigen Überprüfung gemäß § 15 Abs. 2 Z 5 eine erneute Antragstellung vor Ablauf der Dreijahresfrist erforderlich ist.

Die einzelfallbezogene Abwägung, ob eine Person basierend auf einer Risikoanalyse einer ZÜP zu unterziehen ist, soll der kritischen Einrichtung selbst obliegen. Es bleibt allerdings der Behörde vorbehalten, eine nachprüfende Kontrolle des Antrages vorzunehmen und die Durchführung der ZÜP insbesondere dann abzulehnen, wenn sich im Rahmen der Prüfung herausstellen sollte, dass bereits eine in § 15 Abs. 2 Z 5 genannte gleichwertige Überprüfung vorliegt und das Ersuchen keine Ausführungen hinsichtlich der Erforderlichkeit einer erneuten Überprüfung enthält. Zuvor sollte allerdings der kritischen Einrichtung, wie auch bei Vorliegen sonstiger formeller Mängel, im Rahmen eines Verbesserungsauftrags die Behebung des Mangels ermöglicht werden. Im Falle der Ablehnung eines Ersuchens oder eines nicht erfüllten Verbesserungsauftrages soll die Behörde verpflichtet sein, die zuvor überwiesene Gebühr für die Durchführung der ZÜP (vgl. Abs. 7) jedenfalls rückzuerstatten.

Vorgesehen ist, dass das Ersuchen sowie die in Abs. 2 angeführten personenbezogenen Daten der zu überprüfenden Person dem Bundesminister für Inneres im elektronischen Weg über einen sicheren Kommunikationskanal strukturiert zu übermitteln sein sollen. Die gewählte Formulierung orientiert sich an § 16 Abs. 6 des Finanzmarkt-Geldwäschegesetzes (FM-GwG), BGBl. I Nr. 118/2016, und soll insbesondere ein möglichst hohes Datensicherheitsniveau sowie eine rasche Bearbeitung der Anträge gewährleisten. Der zu verwendende Kommunikationskanal (zB ein bereitgestelltes Online-Formular) soll den kritischen Einrichtungen rechtzeitig, beispielsweise durch Veröffentlichung auf der öffentlich zugänglichen Homepage des Bundesministeriums für Inneres, zur Kenntnis zu bringen sein und soll der Bundesminister für Inneres vor dem Hintergrund der unmittelbaren Anwendbarkeit des Art. 32 DSGVO insbesondere dazu verpflichtet sein, bei Bereitstellung der technischen Voraussetzungen den diesbezüglichen Anforderungen Rechnung zu tragen, etwa durch technische oder organistorische Vorkehrungen gegen unbefugte Zugriffe sowie Dokumentationspflichten. Dem Ersuchen soll zudem die ausdrückliche Einwilligung der betroffenen Person zur Überprüfung ihrer Daten sowie Rückmeldung des Ergebnisses dieser Überprüfung an die kritische Einrichtung anzuschließen sein. Die seitens der Einrichtung zu übermittelnden Datenkategorien entsprechen weitestgehend jenen, die gemäß § 134a LFG zum Zweck der Durchführung einer Zuverlässigkeitsüberprüfung vorzulegen sind, wobei auf vereinzelte Parameter – wie beispielsweise Aus- und Weiterbildungen – mangels Relevanz für die behördliche Überprüfung verzichtet wurde.

Im Zuge der Überprüfung der Zuverlässigkeit soll sich die Behörde mit Blick auf die unionsrechtlichen Vorgaben in Art. 14 Abs. 3 RKE-RL jedenfalls durch Abgleich der übermittelten personenbezogenen Daten mit dem beigefügten Identitätsnachweis der Identität der zu überprüfenden Person vergewissern. Zudem soll sie die Landespolizeidirektion Wien um eine Abfrage des Europäischen Strafregisterinformationssystems (ECRIS) nach Maßgabe des Rahmenbeschlusses 2009/315/JI über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten, ABl. Nr. L 93 vom 07.04.2009 S. 23, geändert durch die Richtlinie (EU) 2019/884 zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS), sowie zur Ersetzung des Beschlusses 2009/316/JI des Rates, ABl. Nr. L 151 vom 07.06.2019 S. 143, zu ersuchen und allfällige vorgelegte ausländische Strafregisterbescheinigungen zu sichten haben. Demnach soll etwa in Abs. 4 explizit angeordnet werden, dass nicht nur Strafregisterauskünfte gemäß § 9

des Strafregistergesetzes 1968 einzuholen sind (vgl. Abs. 5), sondern im Zuge der Überprüfung der Zuverlässigkeit auch eine Nutzung des ECRIS (sowohl in Bezug auf Unionsbürger als auch Drittstaatsangehörige) zu erfolgen hat. Über die expliziten Anforderungen der RKE-RL hinaus sollen zusätzlich die in Abs. 5 angeführten Umstände, die zumindest abstrakt geeignet sind, die Zuverlässigkeit der zu überprüfenden Person in Zweifel zu ziehen, durch Abfrage der polizeilichen Evidenzen und Datenbanken sowie Anfrage an die Strafjustiz abzuklären sein, wobei die von dieser Ermächtigung umfassten Datenarten durch die strenge Zweckbindung der Verarbeitung (Überprüfung der Zuverlässigkeit) hinreichend bestimmt beschrieben werden (vgl. Abs. 3). Zur Möglichkeit der Sicherheitsbehörden und damit auch des Bundesministers für Inneres, sich bei der Dokumentation aller Amtshandlungen und Verwaltung von Dienststücken im Rahmen der Wahrnehmung gesetzlich übertragener Aufgaben der automationsunterstützten Datenverarbeitung zu bedienen vgl. § 13a Abs. 1 SPG.

Mit dem gemäß Abs. 6 seitens des Bundesministers für Inneres an die kritische Einrichtung übermittelten Ergebnis der Überprüfung soll per se keine Bewertung der Zuverlässigkeit der überprüften Person erfolgen. Vielmehr soll die kritische Einrichtung durch Mitteilung allfälliger im Rahmen der Überprüfung zu Tage getretener (sicherheitspolizeilicher) Bedenken in die Lage versetzt werden, eine fundierte, einzelfallbezogene Beurteilung dahingehend durchzuführen, ob die mitgeteilten Bedenken im Hinblick auf die von der überprüften Person wahrgenommene oder angestrebte sensible Funktion ein Sicherheitsrisiko innerhalb der Organisation der kritischen Einrichtung begründen.

Angelehnt an die Regelung in § 55b Abs. 5 SPG soll in Abs. 7 vorgesehen werden, dass Zuverlässigkeitsüberprüfungen einer Gebührenpflicht unterliegen und soll der dem Bund für die Überprüfung der Zuverlässigkeit gebührende Pauschalbetrag nach Maßgabe der durchschnittlichen Aufwendungen mit Verordnung des Bundesministers für Inneres festzulegen sein. Vor dem Hintergrund, dass es im Falle einer an Behörden und sonstige Stellen der öffentlichen Verwaltung adressierten Gebührenpflicht wohl großteils zu einer Umverteilung finanzieller Mittel innerhalb des Budgets kommen würde (vgl. dazu auch die Erläuterungen zu § 23), sollen diese von der Verpflichtung zur Entrichtung der Gebühr befreit sein (vgl. auch die Bestimmung gemäß § 2 des Gebührengesetzes 1957, BGBl. Nr. 267/1957, sowie die Regelung gemäß § 55a Abs. 2 Z 3 und Z 3a iVm § 55b Abs. 5 SPG, wonach lediglich Unternehmen, die um Durchführung einer Sicherheitsüberprüfung ersucht haben, deren Kosten zu tragen haben).

Zu § 17 (Meldepflicht für kritische Einrichtungen):

Mit gegenständlicher Bestimmung soll ein Prozess für die Meldung bestimmter Sicherheitsvorfälle im Sinne des Art. 15 RKE-RL etabliert werden, um dem Bundesminister für Inneres als zuständige RKE-Behörde eine rasche und angemessene Reaktion sowie einen umfassenden Überblick über die Auswirkungen, Art und Ursache sowie möglichen Folgen dieser Sicherheitsvorfälle zu ermöglichen. Demnach sollen kritische Einrichtungen gemäß Abs. 1 dazu verpflichtet sein, bei Vorliegen der Voraussetzungen gemäß Abs. 2 – soweit dies aus operativer Sicht möglich ist – Sicherheitsvorfälle unverzüglich, längstens jedoch binnen 24 Stunden nach Kenntnis dem Bundesminister für Inneres zu melden und soll eine ausführliche Folgemeldung längstens binnen eines Monats nach der Erstmeldung zu erfolgen haben (vgl. Art. 15 Abs. 1 RKE-RL). Wesentlich ist, dass die Erstmeldung Informationen beinhalten sollte, die unbedingt erforderlich sind, um den Bundesminister für Inneres über den Sicherheitsvorfall und – soweit möglich – über die mutmaßliche Ursache in Kenntnis zu setzen und bei Bedarf Hilfe in Anspruch nehmen zu können, während die Folgemeldung die Erstmeldung ergänzen und einen vollständigeren Überblick über den Sicherheitsvorfall bieten soll (vgl. ErwGr 33 zur RKE-RL). Durch das Abstellen auf die Möglichkeit „aus operativer Sicht“ soll sichergestellt werden, dass die Ressourcen der kritischen Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen Vorrang haben und diese durch die Pflicht zur Übermittlung der Erstmeldung nicht beeinträchtigt werden sollen.

Der Systematik des Art. 15 RKE-RL zufolge haben kritische Einrichtungen – im Unterschied zu Art. 6 Abs. 2 lit. c iVm Art. 7 RKE-RL – die Erheblichkeit einer Störung anhand der in Art. 15 Abs. 1 lit. a bis c RKE-RL festgelegten Parameter, die zur Auslösung der Meldepflicht führen, selbständig zu beurteilen. Um kritischen Einrichtungen diese Beurteilung zu ermöglichen, soll der Bundesminister für Inneres gemäß Abs. 2 verpflichtet sein, durch Verordnung nähere Regelungen zum Vorliegen von Sicherheitsvorfällen, die eine Meldepflicht gemäß Abs. 1 auslösen, festzulegen. Dabei soll dieser bestimmte Kriterien zu berücksichtigen haben, wie etwa die Zahl bzw. den prozentuellen Anteil der vom Sicherheitsvorfall betroffenen Nutzer des erbrachten wesentlichen Diensts (Z 1), die Dauer der Störung (Z 2) sowie das vom Sicherheitsvorfall betroffene geografische Gebiet (Z 3), wobei regionalen Gegebenheiten, wie insbesondere dem Umstand einer allenfalls isolierten Lage bzw. Region (etwa im Bereich der Alpen) besonders Rechnung zu tragen sein soll (vgl. auch Art. 15 Abs. 1 lit. a bis c RKE-RL).

In Abs. 3 soll die Präzisierung erfolgen, welche Informationen zum Sicherheitsvorfall an den Bundesminister für Inneres übermittelt werden sollen (vgl. Art. 15 Abs. 2 RKE-RL). Wesentlich ist, dass die Anforderungen an die Meldepflichten kritischer Einrichtungen insbesondere in der Erstphase eines Sicherheitsvorfalles nicht überspannt werden sollten, zumal der Ergreifung von Sofortmaßnahmen zur raschen Bewältigung des Sicherheitsvorfalls Priorität eingeräumt werden sollte (vgl. ErwGr 33 zur RKE-RL sowie die in Abs. 1 vorgesehene allfällige Einschränkung der Meldepflicht).

Gemäß Abs. 4 sollen kritische Einrichtungen dem Bundesminister für Inneres unverzüglich Informationen über erst zu einem späteren Zeitpunkt bekannt gewordene Umstände zu einem Sicherheitsvorfall, einschließlich die Information über dessen Beendigung, zu übermitteln haben. Zudem sollen diese dazu verpflichtet sein, nach Beendigung eines Sicherheitsvorfalls unverzüglich (vgl. die Erläuterungen zu § 14), längstens jedoch binnen zwei Monaten einen Abschlussbericht zu übermitteln. Diese Berichtspflicht soll als „Feedback-Mechanismus“ insbesondere dazu dienen, die ergriffenen Abwehr- bzw. Bewältigungsmaßnahmen zu evaluieren, um damit die Vorbereitung auf künftige Sicherheitsvorfälle zu verbessern und die Resilienz insgesamt zu stärken (vgl. damit im Zusammenhang auch § 15 Abs. 4 betreffend die Einrichtung eines Qualitätsmanagements). Bei zeitnaher Beendigung eines Sicherheitsvorfalls wäre es allenfalls denkbar, Folgemeldung und Abschlussbericht in einer Meldung zusammenzufassen, sofern diese über sämtliche Inhalte verfügt sowie die vorgesehenen Fristen eingehalten werden.

In Abs. 5 soll – in Umsetzung der Regelung in Art. 15 Abs. 4 RKE-RL – die Verpflichtung des Bundesministers für Inneres vorgesehen werden, die vom Sicherheitsvorfall betroffenen kritischen Einrichtungen zu unterstützen, indem er diesen basierend auf den in der Meldung enthaltenen Angaben sachdienliche Informationen – insbesondere zur Abwehr und Bewältigung des betreffenden Sicherheitsvorfalls – bereitstellt (vgl. damit im Zusammenhang auch die in § 13 Z 12 vorgesehenen Unterstützungsmaßnahmen).

Zu § 18 (Ausnahmen von Verpflichtungen für kritische Einrichtungen):

Gemäß Art. 1 Abs. 3 RKE-RL finden die Bestimmungen dieser Richtlinie, einschließlich der in Kapitel IV festgelegten Anordnungen über Aufsicht und Durchsetzung, insoweit keine Anwendung, als kritische Einrichtungen bereits auf Grund sektorspezifischer Rechtsakte der Union Maßnahmen zur Verbesserung ihrer Resilienz zu ergreifen haben. Voraussetzung ist, dass die jeweiligen sektorspezifischen Anforderungen von den Mitgliedstaaten als den entsprechenden Verpflichtungen nach der RKE-RL zumindest gleichwertig anerkannt sind. In diesem Fall sollen demnach lediglich die in den jeweiligen Unionsrechtsakten festgelegten Bestimmungen zur Anwendung kommen, um Doppelarbeit und unnötigen Aufwand in Fällen zu vermeiden, in denen kritische Einrichtungen bereits durch andere bestehende sektorale Rechtsvorschriften der Union zur Ergreifung resilienzfördernder Maßnahmen verpflichtet sind (vgl. ErwGr 10 zur RKE-RL).

Damit dem Gleichwertigkeitserfordernis entsprochen wird, ist es wesentlich, dass die Anforderungen in dem jeweiligen sektorspezifischen Rechtsakt der Union mindestens den Anforderungen der in der RKE-RL vorgesehenen Bestimmungen entsprechen oder sogar darüber hinausgehen, was bedeutet, dass die sektorspezifischen Bestimmungen im Vergleich dazu etwa inhaltlich detaillierter sein können. Zudem ist es essenziell, dass die Verpflichtungen jedenfalls den von der RKE-RL erfassten gefahrenübergreifenden Ansatz abdecken und sollten die zu treffenden Maßnahmen geeignet sein, die Unterbrechung der Erbringung wesentlicher Dienste durch die kritische Einrichtung zu verhindern, sich davor zu schützen, die Unterbrechung abzuwehren, darauf zu reagieren, die Folgen zu begrenzen, die Unterbrechung zu bewältigen oder sich davon zu erholen.

Dementsprechend soll in Abs. 1 festgelegt werden, dass die Anforderungen gemäß § 15 (Resilienzmaßnahmen) insoweit nicht anwendbar sein sollen, als kritische Einrichtungen bereits aufgrund sektorspezifischer Unionsrechtsakte zur Ergreifung gleichwertiger Maßnahmen für die Erbringung eines wesentlichen Dienstes verpflichtet sind (Z 1). Wesentlich soll außerdem sein, dass diese Verpflichtungen ein zumindest gleichwertiges Resilienzniveau gewährleisten oder sogar darüber hinausgehen (Z 2). Um kritischen Einrichtungen die Beurteilung zu erleichtern, ob und inwieweit sie von Verpflichtungen nach diesem Bundesgesetz ausgenommen sind, soll der Bundesminister für Inneres verpflichtet sein, über die jeweiligen sektorspezifischen Bestimmungen sowie das Ausmaß der Gleichwertigkeit auf der Homepage des Bundesministeriums für Inneres zu informieren. Sind die Anforderungen gemäß § 15 nicht anwendbar und die jeweiligen kritischen Einrichtungen demnach von den Verpflichtungen ausgenommen, sollen selbstverständlich auch die in § 20 normierten behördlichen Aufsichts- und Durchsetzungsmaßnahmen in demselben Ausmaß keine Anwendung finden.

In Abs. 2 sollen die Kriterien näher präzisiert werden, die bei der Beurteilung der Gleichwertigkeit zu berücksichtigen sind. Demnach soll darauf Bedacht zu nehmen sein, dass die jeweiligen

sektorspezifischen Bestimmungen insgesamt ein zumindest gleich hohes Schutzniveau mit Blick auf die Resilienz kritischer Einrichtungen bieten.

Da in den Sektoren digitale Infrastruktur, Bankwesen und Finanzmarktinfrastrukturen auf Grund einschlägiger Unionsrechtsakte bereits ein ausreichend hohes Resilienzniveau kritischer Einrichtungen gewährleistet ist, soll – ebenfalls zur Vermeidung von Doppelarbeit und unnötigem Aufwand – in Abs. 3 vorgesehen werden, dass § 11 Abs. 6 bis 8 sowie §§ 14, 15, 17 und 19 für die in diesen Sektoren ermittelten kritischen Einrichtungen nicht gelten sollen (vgl. auch Art. 8 RKE-RL sowie ErwGr 21 zur RKE-RL) und soll demnach etwa auch die Bestimmung gemäß § 16 (Zuverlässigkeitsüberprüfungen) nicht anwendbar sein, zumal es sich hierbei um eine Resilienzmaßnahme gemäß § 15 Abs. 2 Z 5 handeln soll. Über diesen Umstand sollen die betreffenden Einrichtungen in dem gemäß § 11 Abs. 1 zu erlassenden Bescheid belehrt werden (§ 11 Abs. 5; vgl. Art. 6 Abs. 3 Unterabsatz 1 RKE-RL). Da Einrichtungen in diesen Sektoren demnach nicht den in diesem Bundesgesetz vorgesehenen Verpflichtungen unterliegen sollen, soll folglich auch das Aufsichts- und Durchsetzungs- bzw. Sanktionsregime gemäß den vorgeschlagenen §§ 20 bis 23 nicht zur Anwendung gelangen.

Zu § 19 (Kritische Einrichtungen von besonderer europäischer Bedeutung):

Da kritische Einrichtungen als Teil eines immer stärker verflochtenen Dienstleistungs- und Infrastrukturnetzes wesentliche Dienste regelmäßig auch im Hoheitsgebiet anderer Mitgliedstaaten erbringen und diesen demnach eine unverzichtbare Rolle bei der Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten im Binnenmarkt zukommt, unterstreicht die RKE-RL die besondere Bedeutung jener kritischen Einrichtungen, die wesentliche Dienste für oder in sechs oder mehr Mitgliedstaaten zur Verfügung stellen, weshalb diese spezifische Unterstützung auf Unionsebene erhalten sollen (vgl. ErwGr 35 zur RKE-RL).

In Umsetzung des Art. 17 Abs. 2 RKE-RL soll in Abs. 1 daher vorgesehen werden, dass kritische Einrichtungen den Bundesminister für Inneres unverzüglich darüber zu informieren haben, dass sie wesentliche Dienste für oder in mindestens sechs Mitgliedstaaten erbringen. Diese Mitteilungspflicht soll mit Eintritt der formellen Rechtskraft eines gemäß § 11 Abs. 1 erlassenen Bescheids entstehen bzw. falls die Voraussetzungen erst zu einem späteren Zeitpunkt vorliegen, ab diesem. In dieser Mitteilung soll auch anzugeben sein, um welche wesentlichen Dienste es sich jeweils handelt und in welchen Mitgliedstaaten diese erbracht werden. Fallen die Voraussetzungen nachträglich weg, sollen kritische Einrichtungen den Bundesminister für Inneres auch darüber zu informieren haben. Zwar sieht die RKE-RL eine Informationspflicht bei Wegfall der Voraussetzungen nicht ausdrücklich vor, jedoch scheint eine solche erforderlich, zumal mit der Einstufung als kritische Einrichtung von besonderer europäischer Bedeutung besondere Rechtsfolgen bzw. spezifische Verpflichtungen einhergehen (vgl. Abs. 3 und 4).

Wesentlich ist, dass es nach der Systematik der RKE-RL der Europäischen Kommission obliegt, nach Erhalt der Informationen gemäß Abs. 1 und entsprechender Konsultation der involvierten Mitgliedstaaten festzustellen, ob es sich um eine kritische Einrichtung von besonderer europäischer Bedeutung handelt. Ist dies der Fall, hat sie diesen Umstand den zuständigen Behörden mitzuteilen (vgl. Art. 17 Abs. 3 RKE-RL). Gemäß Abs. 2 soll der Bundesminister für Inneres sodann dazu verpflichtet sein, eine solche Mitteilung der Europäischen Kommission über die Einstufung als kritische Einrichtung von besonderer europäischer Bedeutung unverzüglich an die jeweilige kritische Einrichtung weiterzuleiten und diese über ihre Verpflichtungen gemäß den Abs. 3 und 4, einschließlich des Zeitpunkts, ab dem diese gelten, zu unterrichten. Die Übermittlung der Mitteilung und der „Rechtsbelehrung“ sollten tunlichst zeitgleich erfolgen, zumal kritische Einrichtungen bereits ab dem Zeitpunkt der Zustellung der Mitteilung über ihre Einstufung an die Verpflichtungen gemäß den Abs. 3 und 4 gebunden sein sollen (vgl. Art. 17 Abs. 4 RKE-RL). Die Wirksamkeit der Zustellung soll sich nach den allgemeinen Regeln des ZustG richten.

Wenngleich die RKE-RL keine entsprechende Informationspflicht festlegt, scheint im Hinblick darauf, dass mit der Einstufung als kritische Einrichtung von besonderer Bedeutung für Europa spezifische Rechtsfolgen verbunden sind (vgl. dazu sogleich unten), eine Information der Europäischen Kommission durch den Bundesminister für Inneres auch über den Wegfall der Voraussetzungen angezeigt. Widerruft die Europäische Kommission in weiterer Folge die Einstufung als kritische Einrichtung von besonderer Bedeutung für Europa, soll der Bundesminister für Inneres diese Mitteilung sowie die Information, dass die Verpflichtungen gemäß den Abs. 3 und 4 ab wirksamer Zustellung der Mitteilung nicht mehr erfüllt werden müssen, ebenfalls unverzüglich an die jeweilige Einrichtung weiterzuleiten haben.

Gemäß Art. 18 RKE-RL hat die Europäische Kommission Beratungsmissionen zur Bewertung der Maßnahmen, die eine kritische Einrichtung von besonderer Bedeutung für Europa in Erfüllung ihrer Verpflichtungen gemäß den Vorgaben der RKE-RL ergriffen hat, zu organisieren und unterliegen die auf diesem Wege überprüften kritischen Einrichtungen besonderen Verpflichtungen, die in den Abs. 3 und 4 abgebildet werden sollen. So sollen kritische Einrichtungen von besonderer Bedeutung für Europa gemäß

Abs. 3 dazu verpflichtet sein, Beratungsmissionen Zugang zu ihren kritischen Infrastrukturen (darunter fallen etwa Systeme und Anlagen, die der Bereitstellung ihrer wesentlichen Dienste dienen) im erforderlichen Ausmaß zu ermöglichen sowie Einsicht in relevante Unterlagen und Informationen zu gewähren (vgl. Art. 18 Abs. 7 RKE-RL). Die RKE-RL weist in diesem Zusammenhang ausdrücklich darauf hin, dass Beratungsmissionen den jeweiligen nationalen Rechtsvorschriften – etwa über die Bedingungen für den Zugang zu den entsprechenden Räumlichkeiten oder Dokumenten – unterliegen sollen (vgl. ErwGr 36 zur RKE-RL).

Gemäß Abs. 4 sollen kritische Einrichtungen von besonderer Bedeutung für Europa zudem verpflichtet sein, den Bundesminister für Inneres über Maßnahmen zu unterrichten, die aufgrund einer Empfehlung der Europäischen Kommission gemäß Art. 18 Abs. 4 Unterabsatz 3 RKE-RL ergriffen wurden. Daraus ergibt sich, dass die überprüften kritischen Einrichtungen eine entsprechende Stellungnahme der Europäischen Kommission prüfen, bewerten und gegebenenfalls den darin zum Ausdruck gebrachten Empfehlungen gebührend Rechnung tragen sollen (vgl. Art. 18 Abs. 4 Unterabsatz 4 RKE-RL).

Zu § 20 (Aufsichts- und Durchsetzungsmaßnahmen):

Gemäß Art. 21 RKE-RL sind die Mitgliedstaaten dazu verpflichtet, die zuständige Behörde unter Wahrung des Grundsatzes der Verhältnismäßigkeit mit spezifischen Befugnissen auszustatten, um die ordnungsgemäße Anwendung und Durchsetzung der gemäß dieser Richtlinie erlassenen nationalen Vorschriften in Bezug auf kritische Einrichtungen sicherzustellen (vgl. dazu auch die Erläuterungen zu § 4 Abs. 2). Demnach sollen die Mitgliedstaaten solche Maßnahmen vorsehen, die erforderlich sind, um die Erfüllung der jeweiligen Verpflichtung durch die betreffende kritische Einrichtung sicherzustellen, wobei insbesondere deren wirtschaftliche Leistungsfähigkeit sowie die Schwere des Verstoßes berücksichtigt werden sollen. Die der zuständigen Behörde übertragenen Befugnisse sollen zudem mit angemessenen und wirksamen Garantien einhergehen, die national im Einklang mit der Charta der Grundrechte der Europäischen Union festgelegt werden sollen (vgl. auch ErwGr 40 zur RKE-RL).

Wie bereits in den Erläuterungen zu § 4 Abs. 2 näher ausgeführt ist es zur unionsrechtskonformen Umsetzung zwingend erforderlich, dass der Bundesminister für Inneres seine Befugnisse nach diesem Bundesgesetz – und damit insbesondere auch jene im Rahmen des Aufsichts- und Durchsetzungsregimes – gegenüber sämtlichen gemäß §§ 11 und 12 mit Bescheid als kritisch eingestuften Einrichtungen und somit gegebenenfalls auch gegenüber den in Art. 19 B-VG bezeichneten obersten Organen der Vollziehung ausüben kann. Dabei gilt es zu beachten, dass das Aufsichts- und Durchsetzungsregime auf Einrichtungen im Sektor der öffentlichen Verwaltung (und damit auch oberste Organe der Vollziehung), deren Wirkungsbereiche überwiegend die nationale Sicherheit einschließlich der militärischen Landesverteidigung, die öffentliche Sicherheit oder die Strafverfolgung umfassen, keine Anwendung finden soll, zumal diese gemäß dem vorgeschlagenen § 12 Abs. 2 nicht den Bestimmungen dieses Bundesgesetzes unterliegen.

In den Abs. 1 bis 4 sollen die einzelnen dem Bundesminister für Inneres im Rahmen der Aufsicht und Durchsetzung übertragenen Befugnisse festgelegt werden. So soll dieser gemäß Abs. 1 – unbeschadet der in § 14 Abs. 1 sowie § 15 Abs. 3 normierten „proaktiven“ Übermittlungspflichten – befugt sein, von kritischen Einrichtungen zu verlangen, die Erfüllung der Verpflichtungen gemäß den §§ 14 und 15 innerhalb einer angemessenen Frist nachzuweisen, soweit dies zur Wahrnehmung seiner Aufgaben nach diesem Bundesgesetz erforderlich ist (vgl. auch die unionsrechtlichen Vorgaben in Art. 21 Abs. 2 lit. a und b RKE-RL). Dabei sollen der Zweck der Überprüfung sowie Art und Umfang der erforderlichen Informationen bereits aus dem „Auskunftsverlangen“ klar hervorgehen (vgl. Art. 21 Abs. 2 Unterabsatz 2 RKE-RL). Im Zuge einer solchen Überprüfung soll der Bundesminister für Inneres allenfalls auch die Gleichwertigkeit von Risikoanalysen und Resilienzmaßnahmen, die aufgrund anderer rechtlicher Verpflichtungen durchgeführt wurden, zu beurteilen haben (vgl. § 14 Abs. 3 sowie § 15 Abs. 5). Zudem soll der Bundesminister für Inneres von kritischen Einrichtungen die Durchführung von Audits (§ 3 Z 13) durch qualifizierte Stellen gemäß § 21 verlangen können (vgl. Art. 21 Abs. 1 lit. b RKE-RL). Wesentlich ist, dass der Bundesminister für Inneres an das Ergebnis eines Audits nicht gebunden sein soll, sondern soll dieses als Teil seiner Entscheidungsgrundlage der freien Beweiswürdigung unterliegen. Die abschließende Beurteilung der Umsetzung der Verpflichtungen gemäß §§ 14 und 15 soll demnach allein dem Bundesminister für Inneres als zuständige Behörde obliegen.

In Abs. 2 soll die korrespondierende Nachweispflicht kritischer Einrichtungen näher präzisiert werden und sollen demnach dem Bundesminister für Inneres auf Verlangen sämtliche zur Überprüfung der Anforderungen gemäß den §§ 14 und 15 erforderliche Informationen sowie der Prüfbericht über durchgeführte Audits zu übermitteln sein.

In Umsetzung des Art. 21 Abs. 1 lit. a RKE-RL soll der Bundesminister für Inneres zur Überprüfung der ergriffenen Resilienzmaßnahmen (§ 15) gemäß Abs. 3 dazu ermächtigt sein, Vor-Ort-Kontrollen der

kritischen Infrastrukturen sowie jener Räumlichkeiten von kritischen Einrichtungen vorzunehmen, die der Erbringung eines wesentlichen Dienstes dienen. Die Zulässigkeit dieser Kontrollen soll demnach im Sinne der Verhältnismäßigkeit und Erforderlichkeit ausschließlich auf solche Bereiche beschränkt sein, die einen unmittelbaren Konnex zur Erbringung eines wesentlichen Dienstes aufweisen. Der Bundesminister für Inneres soll überdies die beabsichtigte Durchführung einer Vor-Ort-Kontrolle vorab ankündigen und werden bei Festlegung des Termins wohl berechtigte Interessen der jeweiligen kritischen Einrichtung zu berücksichtigen sein. Die Vorankündigung von Vor-Ort-Kontrollen ist insbesondere auch deshalb angezeigt, um der jeweiligen kritischen Einrichtung in Anbetracht ihrer umfangreichen Mitwirkungspflichten Gelegenheit zu geben, Vorsorge für entsprechende personelle Ressourcen zu treffen. So sollen kritische Einrichtungen zunächst verpflichtet sein, dem Bundesminister für Inneres auf sein Verlangen das gefahrlose Betreten und Besichtigen ihrer kritischen Infrastrukturen und Räumlichkeiten – soweit erforderlich – zu ermöglichen sowie die relevanten Informationen zu erteilen und Einschau in einschlägige Unterlagen und Aufzeichnungen zu gewähren. Wesentlich ist, dass kritische Einrichtungen aktiv an einer solchen Überprüfung, insbesondere durch die Bereitstellung fachkundigen Personals, mitwirken sollen. Im Sinne des Grundsatzes der Verhältnismäßigkeit soll der Bundesminister für Inneres die Überprüfung nur auf das unbedingt erforderliche Ausmaß beschränken, wobei er unter möglichster Schonung der Rechte der jeweiligen kritischen Einrichtung sowie Dritter, etwa im Hinblick auf die Wahrung von Betriebsgeheimnissen, vorgehen soll.

Art. 6 Abs. 2 RKE-RL legt bestimmte Kriterien fest, die bei der Ermittlung kritischer Einrichtungen zu berücksichtigen sind. Demnach muss die Einrichtung ua. im Bundesgebiet tätig sein und über eine kritische Infrastruktur im Inland verfügen. Eine inländische Niederlassung stellt hingegen keine Voraussetzung für die Einstufung als kritische Einrichtung dar. Daher soll der Bundesminister für Inneres im Hinblick auf kritische Einrichtungen, die ihre Niederlassung in einem anderen Mitgliedstaat haben, ermächtigt sein, die zuständige Behörde dieses Mitgliedstaates zu ersuchen, eine Überprüfung nach Abs. 3 vorzunehmen und das Ergebnis als Entscheidungsgrundlage heranzuziehen (Abs. 4). Voraussetzung für ein solches Ersuchen soll sein, dass die Vornahme von Vor-Ort-Kontrollen durch die zuständige Behörde des jeweiligen Mitgliedstaates erforderlich ist, um die Einhaltung der Verpflichtungen gemäß § 15 umfassend überprüfen zu können. Aus der Zusammenschau mit den Maßnahmen gemäß Abs. 3 ergibt sich, dass sich das Ersuchen (ebenfalls) nur auf solche Räumlichkeiten bzw. Bereiche beziehen soll, die der Erbringung des wesentlichen Dienstes dienen.

Gelangt der Bundesminister für Inneres im Zuge der Überprüfungen gemäß den Abs. 1 bis 4 zu dem Ergebnis, dass die in den §§ 14 und 15 festgelegten Anforderungen an die Risikoanalyse bzw. an die Resilienzmaßnahmen nicht bzw. nicht ordnungsgemäß erfüllt werden (zB Nichtberücksichtigung des All-Gefahren-Ansatzes), soll gemäß Abs. 5 die jeweilige kritische Einrichtung mit Bescheid dazu verpflichtet werden, binnen einer angemessenen Frist notwendige und verhältnismäßige Maßnahmen nachweislich zu ergreifen (vgl. Art. 21 Abs. 3 RKE-RL). Damit soll der jeweiligen kritischen Einrichtung ausreichend Gelegenheit zur Herstellung des rechtmäßigen Zustandes gegeben werden und soll erst die Nichtbefolgung eines rechtskräftigen Bescheids gemäß Abs. 5 als Verwaltungsübertretung strafbar sein (vgl. dazu die Erläuterungen zu § 22).

Wesentlich ist, dass der Bundesminister für Inneres die in den Abs. 1 bis 3 vorgesehenen Aufsichts- und Durchsetzungsmaßnahmen nicht mit Zwangsgewalt durchsetzen kann. Zuwiderhandlungen gegen die in diesen Bestimmungen normierten Informations- bzw. Mitwirkungspflichten begründen jedoch eine Verwaltungsübertretung (vgl. § 22) bzw. haben diese bei Stellen der öffentlichen Verwaltung eine bescheidmäßige Feststellung der Pflichtverletzung zur Folge (vgl. § 23) und steht kritischen Einrichtungen gegen diesbezügliche Bescheide jeweils der Rechtsweg zum zuständigen Landesverwaltungsgericht offen, womit dem in Art. 21 Abs. 4 RKE-RL postulierten Anspruch auf effektiven Rechtsschutz hinreichend Rechnung getragen wird (vgl. § 6 Abs. 2).

Zu § 21 (Qualifizierte Stellen):

In Abs. 1 soll festgelegt werden, welche Voraussetzungen erforderlich sind, um gemäß § 20 Abs. 1 als qualifizierte Stelle zur Durchführung von Audits (§ 3 Z 13) fungieren zu können. Demnach soll es sich bei einer qualifizierten Stelle um eine natürliche oder juristische Person oder eingetragene Personengesellschaft handeln, die ihre Niederlassung entweder in Österreich oder in einem anderen Mitgliedstaat der Europäischen Union hat und aufgrund eines begründeten schriftlichen Antrags mit Bescheid des Bundesministers für Inneres zur Durchführung von Audits berechtigt wurde. Bereits im Antrag soll das Vorliegen sämtlicher Voraussetzungen, insbesondere jener gemäß Abs. 2, ausführlich dargelegt werden.

Da die Durchführung von Audits zur Überprüfung der Einhaltung der Verpflichtungen gemäß den §§ 14 und 15 eine besonders verantwortungsvolle Aufgabe darstellt, die in der Regel mit einem Zugang zu

besonders sensiblen Informationen einhergeht, sollen qualifizierte Stellen gemäß Abs. 2 selbst sicherheitsüberprüft sein bzw. – bei juristischen Personen – im Rahmen der Personalauswahl dazu verpflichtet sein, lediglich sicherheitsüberprüfte Prüfer einzusetzen. Zudem soll sichergestellt werden, dass Sicherheitsvorkehrungen (etwa in Bezug auf die physische Sicherheit sowie betreffend ihre Netz- und Informationssysteme) erfüllt werden, für die Durchführung von Audits geeignete technische und organisatorische Hilfsmittel (zB IT-Anwendungen) Verwendung finden und die qualifizierte Stelle über ein System zur Qualitätssicherung verfügt. Der Bundesminister für Inneres soll ermächtigt werden, diese Anforderungen mit Verordnung näher festzulegen und soll die diesbezügliche Verordnungsermächtigung zudem die Festlegung näherer verfahrensrechtlicher Bestimmungen sowie – mit Blick auf eine verwaltungsökonomische standardisierte und strukturierte Vorgehensweise – Regelungen hinsichtlich Form und Inhalt des Prüfberichts umfassen.

Um sicherzustellen, dass die gemäß Abs. 2 festgelegten Erfordernisse von qualifizierten Stellen auch tatsächlich erfüllt werden, soll dem Bundesminister für Inneres gemäß Abs. 3 die Befugnis übertragen werden, diesbezügliche Auskünfte zu verlangen und Einschau in für die Überprüfung relevante Unterlagen zu nehmen. Zudem soll der Bundesminister für Inneres dazu ermächtigt sein, Vor-Ort-Kontrollen durchzuführen, wobei diese der jeweiligen qualifizierten Stelle zuvor anzukündigen sein sollen. Bei der Festlegung des Termins sollte tunlichst auf das Einvernehmen mit der jeweiligen qualifizierten Stelle hingewirkt werden, zumal aufgrund des Verweises auf § 20 Abs. 3 zweiter bis vierter Satz umfangreiche Mitwirkungspflichten bestehen sollen und dementsprechend seitens der zu überprüfenden Stelle für die Bereitstellung ausreichender (personeller) Ressourcen gesorgt werden muss (vgl. die Erläuterungen zu § 20 Abs. 3).

In Abs. 4 soll vorgesehen werden, dass qualifizierte Stellen jede Änderung der Erfordernisse gemäß Abs. 2 sowie deren Wegfall dem Bundesminister für Inneres unverzüglich bekannt zu geben haben (zur Beurteilung der „Unverzüglichkeit“ vgl. die Erläuterungen zu § 14).

Erfüllt eine qualifizierte Stelle eine oder mehrere der gemäß Abs. 2 bzw. in einer allfälligen Verordnung festgelegten Erfordernisse nicht mehr, soll diese vom Bundesminister für Inneres dazu aufgefordert werden, binnen einer angemessenen Frist diesen Zustand nachweislich zu beheben. Lässt die qualifizierte Stelle diese Frist ungenützt verstreichen bzw. wird den Anforderungen nicht zur Gänze nachweislich entsprochen, soll der Bundesminister für Inneres dazu verpflichtet sein, den Bescheid gemäß Abs. 1 zu widerrufen (Abs. 5). Der rechtskräftige Widerruf soll zur Folge haben, dass die jeweilige qualifizierte Stelle ihren „Status“ verliert und folglich nicht mehr zur Durchführung von Audits herangezogen werden kann.

Wesentlich ist, dass kritische Einrichtungen in der Auswahl einer (bescheidmäßig berechtigten) qualifizierten Stelle frei sein sollen und die Kosten der Durchführung von Audits selbst zu tragen haben. Vor dem Hintergrund, dass sie demnach eine Übersicht über die berechtigten qualifizierten Stellen benötigen, soll der Bundesminister für Inneres gemäß Abs. 6 dazu verpflichtet sein, eine aktuelle Liste mit den berechtigten qualifizierten Stellen zu führen und den kritischen Einrichtungen in geeigneter Weise zur Verfügung zu stellen. Diese Liste kann beispielsweise auf der öffentlich zugänglichen Homepage des Bundesministeriums für Inneres bereitgestellt werden.

Qualifizierte Stellen werden im Zuge der Durchführung von Audits gemäß Abs. 1 mitunter vertrauliche Informationen über die jeweiligen kritischen Einrichtungen erlangen. Daher soll in Abs. 7 vorgesehen werden, dass qualifizierte Stellen über die im Rahmen der Durchführung von Audits bekanntgewordenen Tatsachen und Erkenntnisse zur Verschwiegenheit verpflichtet sind, sofern deren Geheimhaltung im Interesse der jeweiligen kritischen Einrichtungen geboten ist. Dies soll sinngemäß auch für das seitens der qualifizierten Stelle eingesetzte Personal gelten.

Zu § 22 (Verwaltungsstrafverfahren):

Mit dieser Bestimmung soll Art. 22 RKE-RL umgesetzt werden, der die Mitgliedstaaten dazu verpflichtet, „wirksame, verhältnismäßige und abschreckende“ Sanktionen bei Verstößen gegen die sich aus der RKE-RL ergebenden Verpflichtungen zu erlassen.

Die Strafen sollen hinsichtlich ihrer Höhe je nach Schweregrad bzw. Unrechtsgehalt der Verwaltungsübertretungen differenziert ausgestaltet werden. Angesichts der engen Zusammenhänge zwischen physischer Sicherheit und Cybersicherheit scheint – insbesondere mit Blick auf eine (ebenfalls) entsprechend hohe Durchschlagskraft des RKE-Regimes – eine Orientierung am NIS-2-Strafregime angezeigt, zumal die RKE-RL keine Vorgaben zur Verhängung von Geldbußen beinhaltet.

In Abs. 1 sollen zunächst jene Verwaltungsübertretungen festgelegt werden, die weniger schwerwiegende Auswirkungen auf die Resilienz kritischer Einrichtungen befürchten lassen. Dabei soll es sich insbesondere um die Verletzung allgemeiner Melde- sowie Mitwirkungspflichten kritischer Einrichtungen

bzw. qualifizierter Stellen handeln und soll ein solcher Verstoß – angelehnt an die Strafdrohung des Netz- und Informationssystemsicherheitsgesetzes (NISG), BGBl. I Nr. 111/2018 – von der zuständigen Bezirksverwaltungsbehörde mit einer Geldstrafe bis zu 50 000 Euro, im Wiederholungsfall bis zu 100 000 Euro zu bestrafen sein. Demnach soll eine Verwaltungsübertretung begehen, wer entgegen § 11 Abs. 6 keine Kontaktstelle oder keine Ansprechperson benennt bzw. diesbezügliche Änderungen nicht rechtzeitig bekannt gibt. Da die Bekanntgabe eines Zustellungsbevollmächtigten gemäß § 9 ZustG seitens kritischer Einrichtungen ohne Abgabestelle in Österreich notwendig ist, um eine rasche und rechtlich wirksame Zustellung wichtiger behördlicher Erledigungen nach diesem Bundesgesetz zu ermöglichen (vgl. § 11 Abs. 7), soll eine Verletzung dieser Mitteilungspflicht ebenfalls unter (Verwaltungs-)Strafe gestellt werden. Wie bereits zu § 11 Abs. 8 näher erläutert müssen auch jene Einrichtungen, die keine Niederlassung im Inland haben, zur vollständigen Umsetzung der unionsrechtlichen Vorgaben verpflichtet und bei Nichteinhaltung dieser Verpflichtungen sanktioniert werden können. Vor diesem Hintergrund soll auch die Nichtbekanntgabe eines verantwortlichen Beauftragten gemäß § 9 VStG entgegen der in § 11 Abs. 8 normierten Mitteilungspflicht als Verwaltungsübertretung strafbar sein (Z 2). Die Z 3, 4 und 5 sollen die nicht unverzügliche Bekanntgabe von Änderungen des für die Einstufung maßgeblichen Sachverhalts (vgl. § 11 Abs. 10), die nicht fristgerechte und nicht geeignete Übermittlung der Risikoanalyse (vgl. § 14 Abs. 1) sowie des Resilienzplans (vgl. § 15 Abs. 3) unter Strafe stellen und soll durch Z 6 die Nichteinrichtung eines Systems zur Qualitätssicherung (vgl. § 15 Abs. 4) ebenfalls zur Verwaltungsübertretung erklärt werden. Die Z 7 und 8 sollen die Verletzung von Mitteilungs- bzw. Mitwirkungspflichten kritischer Einrichtungen von besonderer Bedeutung für Europa sanktionieren. Da der Bundesminister für Inneres bei der Ausübung seiner Aufsichts- und Durchsetzungsmaßnahmen gemäß § 20 regelmäßig auf die Kooperation bzw. aktive Mitwirkung der zu überprüfenden kritischen Einrichtung angewiesen sein wird, sollen nach Z 9 und 10 Zuwiderhandlungen gegen die Verpflichtungen gemäß § 20 Abs. 2 und 3 ebenfalls unter Strafe gestellt werden. Z 11 und 12 richten sich hingegen an qualifizierte Stellen als deren Adressaten und erklären Zuwiderhandlungen gegen die Verpflichtungen gemäß § 21 Abs. 3 sowie die Nichtvornahme einer Mitteilung gemäß § 21 Abs. 4 zur Verwaltungsübertretung. Zudem soll ein Verstoß gegen die Verpflichtung zur vertraulichen Behandlung gemäß § 21 Abs. 7 unter Verwaltungsstrafe gestellt werden (Z 13).

Bei den in Abs. 2 normierten Verwaltungsübertretungen handelt es sich angesichts ihrer potenziellen Auswirkungen auf die Resilienz kritischer Einrichtungen und die damit verbundene gesamtstaatliche Bedeutung um besonders schwerwiegende Verstöße und soll die Begehung aus spezial- und generalpräventiven Erwägungen mit einer entsprechend hohen Geldstrafe bedroht sein, wobei in diesem Zusammenhang eine Orientierung am Strafrahmen gemäß dem NIS-2-Regime erfolgen soll. Demnach soll für die Begehung einer Verwaltungsübertretung gemäß Abs. 2 von der zuständigen Bezirksverwaltungsbehörde eine Geldstrafe von bis zu 7 Mio. Euro (vgl. § 19 Abs. 2 VStG) festzulegen sein. Im Zusammenhang mit der Festsetzung hoher Verwaltungsstrafen hat der VfGH zur Frage der Verfassungskonformität des § 99d des Bankwesengesetzes (BWG), idF BGBl I Nr. 184/2013, in Abkehr von seiner bisherigen Rechtsprechung bereits ausgesprochen, dass sich die Höhe der angedrohten Sanktion im Ergebnis als kein taugliches Mittel für die Abgrenzung des gerichtlichen Strafrechts und des Verwaltungsstrafrechts erweist (vgl. VfSlg. 20.231/2017). Demnach soll gemäß Abs. 2 eine Verwaltungsübertretung begehen, wer den in einem rechtskräftigen Bescheid gemäß § 20 Abs. 5 angeordneten Maßnahmen nicht ordnungsgemäß nachkommt (Z 1). Wesentlich ist, dass Entscheidungsgrundlage der zuständigen Bezirksverwaltungsbehörde allein die Frage sein soll, ob die in einem solchen (Leistungs-)Bescheid des Bundesministers für Inneres angeordneten Maßnahmen von der jeweiligen kritischen Einrichtung vollständig und fristgerecht umgesetzt wurden, wobei der Eintritt der (formellen) Rechtskraft dieses Bescheids Voraussetzung für die Verhängung einer Verwaltungsstrafe sein soll. Demnach soll ein Verstoß gegen die Anforderungen an die Risikoanalyse bzw. die Resilienzmaßnahmen gemäß den §§ 14 oder 15 für sich genommen (noch) keine Verwaltungsübertretung begründen, sondern erst die Nichtbefolgung eines rechtskräftigen Bescheids des Bundesministers für Inneres gemäß § 20 Abs. 5. In Z 2 sollen Verstöße gegen Meldepflichten im Zusammenhang mit Sicherheitsvorfällen gemäß § 17 Abs. 1, 3 und 4 für strafbar erklärt werden.

Gemäß den Abs. 3 und 4 soll – neben dem subsidiären („sofern die Verwaltungsvorschriften nicht anderes bestimmen“) Regime der strafrechtlichen Verantwortlichkeit juristischer Personen gemäß § 9 VStG – unter bestimmten Voraussetzungen auch eine unmittelbare Verantwortlichkeit und Sanktionierung von juristischen Personen sowie eingetragenen Personengesellschaften ermöglicht werden, wobei sich die Formulierung an § 30 DSG orientiert. Demnach soll die Bezirksverwaltungsbehörde unter den Voraussetzungen der Abs. 3 und 4 Geldstrafen gegen eine juristische Person oder eingetragene Personengesellschaft verhängen können. Da das VStG lediglich das Verfahren für die Strafbarkeit natürlicher Personen normiert, ist vor dem Hintergrund der unionsrechtlichen Vorgabe, dass Sanktionen wirksam, verhältnismäßig und abschreckend sein müssen

und Geldstrafen dementsprechend hoch festzusetzen sein werden, die Abweichung vom Regime des § 9 VStG zur vollständigen Umsetzung des Art. 22 RKE-RL erforderlich.

In Anlehnung an § 30 Abs. 3 DSG und damit es in keinem Fall zu einer Doppelbestrafung kommen kann, soll die zuständige Bezirksverwaltungsbehörde gemäß Abs. 5 von der Bestrafung eines Verantwortlichen gemäß § 9 VStG abzusehen haben, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person oder eingetragene Personengesellschaft verhängt wurde.

In Abs. 6 soll ausdrücklich klargestellt werden, dass die Abs. 1 bis 5 auf Behörden und sonstige Stellen der öffentlichen Verwaltung keine Anwendung finden, was bedeutet, dass diese Einrichtungen nicht unter die Verwaltungsstraftatbestände fallen können. Betreffend die Formulierung „Behörden und sonstige Stellen der öffentlichen Verwaltung, insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen“ soll eine Anlehnung an § 30 Abs. 5 DSG erfolgen, wobei jedoch – davon abweichend – keine Einschränkung auf Stellen, „die im gesetzlichen Auftrag handeln“ erfolgen soll. Daraus ergibt sich, dass neben der Hoheitsverwaltung auch die gesamte Privatwirtschaftsverwaltung, für die es keiner besonderen gesetzlichen Ermächtigung bedarf, von dieser Regelung umfasst sein soll. Der Terminus „sonstige Stellen der öffentlichen Verwaltung“ ist bewusst sehr weit gefasst. Organwalter sollen nicht unmittelbare Adressaten der sich aus dem gegenständlichen Gesetz ergebenden Verpflichtungen sein (vgl. §§ 11 und 12). Vor dem Hintergrund, dass Behörden selbst von Verwaltungsstrafen ausgenommen sein sollen, kann auch keine verwaltungsstrafrechtliche Verantwortlichkeit der nach außen vertretungsbefugten Personen – also der Organwalter (im Rahmen der Privatwirtschaftsverwaltung, vgl. VwGH vom 21.10.1992, 92/10/0111 in Bezug auf den Bürgermeister einer Gemeinde; siehe auch VfGH 25.6.2015, E 473/2015) – in Frage kommen.

Zu § 23 (Nichteinhaltung von Verpflichtungen durch Stellen der öffentlichen Verwaltung):

Vor dem Hintergrund, dass unter bestimmten Voraussetzungen auch Behörden und sonstige – insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete – Stellen der öffentlichen Verwaltung vom Anwendungsbereich der RKE-RL umfasst sind und demnach eine Einstufung als kritische Einrichtungen in Betracht kommt, bedarf es zur unionsrechtskonformen Umsetzung des Art. 22 RKE-RL eines wirksamen Sanktionsmechanismus im Sinne dieser Bestimmung. In der österreichischen Rechtsordnung ist die Möglichkeit der Verhängung von Geldstrafen gegenüber Behörden grundsätzlich nicht vorgesehen, zumal diese selbst keine Rechtsträger sind und demnach keine Rechtspersönlichkeit besitzen. Vielmehr haften die hinter diesen Behörden stehenden Rechtsträger und deren Organe (Bund, Länder, Gemeinden, sonstige Körperschaften und Anstalten des öffentlichen Rechts) im Rahmen der Amts- und Organhaftung für Schäden, die im Zuge hoheitlicher Vollziehung verursacht wurden. Zudem scheint die Sinnhaftigkeit einer Umverteilung finanzieller Mittel innerhalb des Budgets, zu der es bei der Verhängung von Geldstrafen gegenüber Behörden kommen würde, höchst fraglich und wäre damit allenfalls eine Gefährdung der gesetzlichen Aufgabenerfüllung zu befürchten (vgl. auch *Bresich/Riedl* in *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl*, Datenschutzgesetz [2018] § 30 Rz 15). Auch bei den Bundesministern als oberste Organe des Bundes handelt es sich um keine juristischen Personen und sind diese demnach auch nicht gemäß § 9 VStG zur Einhaltung der Verwaltungsvorschriften im Bereich des hoheitlichen Gesetzesvollzugs berufen. Der VfGH hat hierzu vielmehr in allgemeiner Weise ausgesprochen, dass eine „verwaltungsstrafrechtliche Strafbarkeit“ eines obersten Verwaltungsorgans für Handlungen im Rahmen des hoheitlichen Gesetzesvollzugs von vornherein nicht in Betracht kommt (vgl. VfGH 25.6.2013, E 473/2015). Die unionsrechtskonforme Umsetzung der RKE-RL erfordert jedoch einen Sanktionsmechanismus auch gegenüber Behörden und sonstige Stellen der öffentlichen Verwaltung, einschließlich obersten Organen der Vollziehung.

Auf Unionsebene finden sich Vorschriften, die die Veröffentlichung von Rechtsverstößen vorsehen (vgl. etwa Art. 60 der Richtlinie [EU] 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung [EU] Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl. Nr. L 141 vom 05.06.2015 S. 73, Art. 34 der Verordnung [EU] 596/2014 über Marktmissbrauch [Marktmissbrauchsverordnung] und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission, ABl. Nr. L 173 vom 12.06.2014 S. 1, oder Art. 9 der Verordnung [EU] 2023/1092 zur Änderung der Verordnung [EG] Nr. 2157/1999 über das Recht der Europäischen Zentralbank, Sanktionen zu verhängen [EZB/1999/4] [EZB/2023/13], ABl. Nr. L 146 vom 06.06.2013 S. 15). Den Erwägungsgründen dieser Rechtsvorschriften kann entnommen werden, dass die Veröffentlichung abschreckend wirken soll (vgl. etwa ErwGr 73 zur Marktmissbrauchsverordnung).

Vor dem Hintergrund, dass Geldstrafen gegenüber Behörden den Anforderungen des Art. 22 RKE-RL mangels Wirksamkeit und Abschreckung wohl nicht entsprechen würden (bloße Umverteilung finanzieller Mittel), bedarf es folglich einer alternativen Sanktionsmöglichkeit, die mit der gegenständlichen Verfassungsbestimmung normiert werden soll. Demnach sollen keine Geldbußen gegen Behörden – unabhängig davon, ob diese im Sektor öffentliche Verwaltung oder in einem anderen Sektor als kritische Einrichtung ermittelt werden – verhängt werden dürfen (vgl. dazu die Erläuterungen zu § 22 Abs. 6). Die zuständige Bezirksverwaltungsbehörde soll stattdessen nach den Bestimmungen des AVG bescheidmäßig die Nichteinhaltung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen festzustellen und eine angemessene Frist für die Herstellung des rechtmäßigen Zustandes anzuordnen haben. Wird dem Bescheid nicht ordnungsgemäß innerhalb der angeordneten Frist entsprochen, soll die Bezirksverwaltungsbehörde nach Eintritt der formellen Rechtskraft des Bescheids – angelehnt an die oben angeführten unionsrechtlichen Vorschriften – dazu verpflichtet sein, die Nichteinhaltung der Verpflichtungen in einer Weise zu veröffentlichen, die geeignet scheint, einen möglichst weiten Personenkreis zu erreichen. In Frage käme etwa eine Verbreitung der Informationen über Hörfunk oder Fernsehen sowie auf der Homepage der zuständigen Bezirksverwaltungsbehörde. Dabei soll die Bezirksverwaltungsbehörde darauf Bedacht zu nehmen haben, dass die Veröffentlichung keine Gefahr für die öffentliche Ordnung oder Sicherheit oder für die nationale Sicherheit (vgl. dazu auch die Erläuterungen zu § 8 Abs. 1) darstellt und sollen dementsprechend allenfalls lediglich allgemeine Informationen über das Vorliegen einer Verwaltungsübertretung öffentlich bekannt gemacht werden, die keine konkreten Rückschlüsse auf die von der Pflichtverletzung betroffenen physischen Gegebenheiten und damit einhergehende Sicherheitsmängel zulassen. Von der (Verfassungs-)Bestimmung sollen neben Behörden auch sonstige Stellen der öffentlichen Verwaltung (insbesondere ausgegliederte Rechtsträger privaten oder öffentlichen Rechts) umfasst sein, da die Verhängung von Geldstrafen auch in diesen Fällen allenfalls eine bloße Umverteilung finanzieller Mittel zur Folge hätte und zu einer Gefährdung der gesetzlichen Aufgabenerfüllung führen könnte.

Der Sanktionscharakter dieser Regelung soll in dem durch die Veröffentlichung entstehenden öffentlichen und politischen Druck auf die jeweilige Behörde bzw. sonstige Stelle der öffentlichen Verwaltung zum Ausdruck kommen und wird damit dem Effizienz- und Verhältnismäßigkeitsgebot des Art. 22 RKE-RL hinreichend Genüge getan.

Zu § 24 (Verständigungspflichten):

Gemäß § 25 Abs. 3 VStG sind die Gerichte und Verwaltungsbehörden nicht verpflichtet, der Strafbehörde die Begehung einer Verwaltungsübertretung anzuzeigen, wenn die Bedeutung des strafrechtlich geschützten Rechtsgutes und die Intensität seiner Beeinträchtigung durch die Tat gering sind. Den Materialien lässt sich entnehmen, dass es sich dabei lediglich um eine partielle Einschränkung von allfälligen in anderen Gesetzen vorgesehenen Anzeigepflichten handeln soll und demnach mit dieser Bestimmung selbst keine Anzeigepflicht normiert wird (vgl. ErläutRV 2009 BlgNr. 24. GP 19). Um vor dem Hintergrund einer unionsrechtskonformen Umsetzung eine wirksame Sanktionierung sicherzustellen (vgl. Art. 22 RKE-RL) und eine ordnungsgemäße Führung von Strafverfahren nach diesem Bundesgesetz zu gewährleisten, soll daher vorgesehen werden, dass der Bundesminister für Inneres Sachverhalte, die den Verdacht einer Verwaltungsübertretung gemäß § 22 Abs. 1 oder 2 begründen, der zuständigen Bezirksverwaltungsbehörde zur Anzeige zu bringen hat.

Wesentlich ist, dass die Anwendbarkeit der Bestimmung des § 25 Abs. 3 VStG, die vom Bundesgesetzgeber auf Grundlage der Bedarfskompetenz nach Art. 11 Abs. 2 B-VG erlassen wurde, von der im vorgeschlagenen Abs. 1 statuierten Anzeigepflicht des Bundesministers für Inneres im Hinblick auf Verwaltungsübertretungen gemäß § 22 Abs. 1 und 2 zwar grundsätzlich unberührt bleibt. Angesichts der Bedeutung der physischen Sicherheit von Einrichtungen, die für wichtige gesellschaftliche Funktionen oder wirtschaftliche Tätigkeiten im Binnenmarkt unerlässliche Dienste erbringen, wird jedoch für die Anwendbarkeit des § 25 Abs. 3 VStG häufig kein Raum sein und bedarf es zudem vor dem Hintergrund des Art. 22 RKE-RL einer unionsrechtskonformen und damit wohl restriktiven Anwendung dieser Bestimmung im Vollzug.

Die vorliegende Verständigungspflicht durch die Bezirksverwaltungsbehörden soll auch im Hinblick auf die Nichteinhaltung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen durch Behörden und sonstige Stellen der öffentlichen Verwaltung, insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, zur Anwendung gelangen.

In Abs. 2 soll zudem angeordnet werden, dass die Bezirksverwaltungsbehörde dem Bundesminister für Inneres einen jährlichen Bericht über eingeleitete Verwaltungsstrafverfahren sowie Verfahren gemäß § 23 sowie die Gründe für eine allenfalls unterbliebene Einleitung oder Einstellung nach standardisierten Vorgaben innerhalb einer bestimmten Frist zu erstatten hat. Diese Berichtspflicht soll einerseits die

einheitliche Auslegung und Anwendung dieses Bundesgesetzes erleichtern und andererseits den Anforderungen des Art. 22 RKE-RL Rechnung tragen.

Zu § 25 (Umsetzung von Rechtsakten der EU):

Klargestellt wird, dass mit diesem Bundesgesetz die Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG, ABl. Nr. L 333 vom 27.12.2022 S. 164, CELEX-Nr.: 32022L2557, umgesetzt wird.

Zu § 29 (Übergangsbestimmungen):

Da die RKE-RL den Mitgliedstaaten zahlreiche Verpflichtungen auferlegt, für deren Erfüllung umfassende organisatorische und personelle Maßnahmen erforderlich sind, soll der Zeitraum zwischen Kundmachung und Aufgabenwahrnehmung durch den Bundesminister für Inneres genutzt und dementsprechend in Abs. 1 normiert werden, dass bereits ab dem der Kundmachung dieses Bundesgesetzes folgenden Tag alle für die Ermöglichung einer zeitgerechten Aufgabenwahrnehmung durch den Bundesminister für Inneres erforderlichen vorbereitenden Maßnahmen organisatorischer und personeller Natur zu setzen sind.

Vor dem Hintergrund, dass der vorliegende Entwurf die nähere Ausgestaltung einzelner Vorgaben der RKE-RL einer Verordnung des Bundesministers für Inneres vorbehält, soll in Abs. 2 vorgesehen werden, dass Verordnungen auf Grund dieses Bundesgesetzes und seiner Novellen bereits ab dem Tag der Kundmachung dieses Bundesgesetzes bzw. der betreffenden künftigen Novelle erlassen werden können, wobei sie frühestens mit dem Inkrafttreten der jeweiligen Bestimmungen in Kraft treten sollen.