

Erläuterungen

Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs:

Mit diesem Bundesgesetz sollen das Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) erlassen und das Telekommunikationsgesetz 2021 (TKG 2021), BGBI. I Nr. 190/2021, und das Gesundheitstelematikgesetz 2012 (GTelG 2012), BGBI. I Nr. 111/2012, geändert werden.

Die zunehmende Durchdringung nahezu aller Bereiche der Gesellschaft und des täglichen Lebens mit digitaler Technologie bietet erhebliche Chancen und Möglichkeiten. Gleichzeitig wird die Gesellschaft dadurch aber auch angreifbarer und abhängiger von der Vertraulichkeit, Verfügbarkeit und Integrität von digital verarbeiteten und gespeicherten Informationen, mit anderen Worten: von der Sicherheit im Cyberraum. Staaten, Gruppierungen, aber auch kriminellen Akteuren eröffnen sich immer neue Wege, die digitale Vernetzung für Spionage, Sabotage oder andere kriminelle Aktivitäten nutzbar zu machen. Dabei können schon die Fähigkeiten einzelner krimineller Individuen genügen, um Cyberangriffe mit im Vorfeld nicht abschätzbaren Folgen für die Sicherheit Österreichs durchzuführen. Immer mehr österreichische Unternehmen wurden in den vergangenen Jahren Opfer von Cyberattacken, wie insbesondere von Datenverschlüsselungsangriffen (Ransomware-Attacken) und Angriffen auf die Verfügbarkeit ihrer IT-Systeme (DDoS-Attacken) (für eine nähere Darstellung der Cyberlage im Jahr 2022 siehe den Bericht Cybersicherheit für das Jahr 2022). Im Lichte dieser Entwicklungen wird deutlich, dass moderne Demokratien ein entsprechendes organisatorisches, personelles und finanzielles Fundament benötigen, um die wachsende Bedeutung von Cybersicherheit gesamtstaatlich abilden zu können.

Aufgrund der seit Jahren rapide zunehmenden Bedeutung von Cybersicherheit hat die Europäische Union (EU) mehrere Rechtsakte erlassen, die der unionsweiten Erhöhung der Cybersicherheit dienen. Mit der Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren, ABl. Nr. L 202 vom 08.06.2021 S. 1, wird das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit eingerichtet und sieht in diesem Zusammenhang die Benennung von nationalen Koordinierungszentren durch die Mitgliedstaaten vor. Mit der 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-Richtlinie), welche am 16. Jänner 2023 in Kraft getreten ist, wird unter anderem eine erhebliche Steigerung der zu beaufsichtigenden Einrichtungen sowie eine erhebliche Ausweitung des Aufgabenspektrums der NIS-Behörden vorgesehen.

Das NISG 2026 errichtet das nationale Koordinierungszentrum für Cybersicherheit gemäß der Verordnung (EU) 2021/887 und setzt die NIS-2-Richtlinie um.

Aufbau des Entwurfs des Art. 1 (Netz- und Informationssystemsicherheitsgesetz 2026):

Zum 1. Hauptstück:

Das 1. Hauptstück enthält allgemeine Bestimmungen, einschließlich einer Verfassungsbestimmung betreffend die Kompetenz des Bundes für die in diesem Bundesgesetz geregelten Angelegenheiten. Ferner werden in diesem Hauptstück Gegenstand und Ziel des Gesetzes und die Begriffsbestimmungen festgelegt.

Zum 2. Hauptstück:

Das 2. Hauptstück definiert die Strukturen zur Schaffung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus, die Einrichtung einer dem Bundesminister für Inneres unmittelbar nachgeordneten Cybersicherheitsbehörde und die Aufgaben der Cybersicherheitsbehörde, der Computer-Notfallteams (CSIRTs), der unabhängigen Stellen und der unabhängigen Prüfer. Ferner werden die nationalen Koordinierungsstrukturen, die nationale Cybersicherheitsstrategie, das Management von Cybersicherheitsvorfällen großen Ausmaßes, die national eingesetzten IKT-Lösungen sowie die Zusammenarbeit auf nationaler und internationaler Ebene geregelt.

Zum 3. Hauptstück:

Das 3. Hauptstück definiert wesentliche und wichtige Einrichtungen (als zentrale Normadressaten) und legt ihre sowie die Pflichten von Einrichtungen, die Domänennamenregistrierungsdienste erbringen,

einschließlich der Aufsicht und Durchsetzung dieser Pflichten durch die Cybersicherheitsbehörde, fest. Darüber hinaus wird der rechtliche Rahmen für den freiwilligen Informationsaustausch zur Erhöhung der Cybersicherheit geschaffen.

Zum 4. Hauptstück:

Das 4. Hauptstück schafft die Grundlage der Datenverarbeitung und -übermittlung und begrenzt diese durch eine klare Definition der Zwecke und Modalitäten der Verarbeitung.

Zum 5. Hauptstück:

Das 5. Hauptstück legt Rahmenbedingungen zur Verhängung von Geldstrafen sowie die konkreten Verwaltungsstrafatbestände fest.

Zum 6. Hauptstück:

Das 6. Hauptstück enthält einerseits klarstellende Bestimmungen zu den personenbezogenen Bezeichnungen innerhalb des Gesetzes sowie zu den mit diesem Gesetz umgesetzten Rechtsakten der Europäischen Union und zu den im Gesetz verwendeten Verweisungen und regelt andererseits die Vollziehung des Gesetzes sowie das Verhältnis zum Netz- und Informationssystemsicherheitsgesetzes (NISG), BGBI. I Nr. 111/2018, einschließlich das Inkrafttreten des Gesetzes, das Außerkrafttreten des NISG samt Übergangsbestimmungen.

Kompetenzgrundlage:

Die Zuständigkeit des Bundes zur Gesetzgebung und Vollziehung beruht auf den Kompetenztatbeständen:

- „Börsewesen“ gemäß Art. 10 Abs. 1 Z 5 des Bundes-Verfassungsgesetzes (B-VG), BGBI. Nr. 1/1930,
- „Bankwesen“ gemäß Art. 10 Abs. 1 Z 5 B-VG,
- „Angelegenheiten des Gewerbes und der Industrie“ gemäß Art. 10 Abs. 1 Z 8 B-VG,
- „Verkehrswesen bezüglich der Eisenbahnen“ gemäß Art. 10 Abs. 1 Z 9 B-VG,
- „Verkehrswesen bezüglich der Luftfahrt“ gemäß Art. 10 Abs. 1 Z 9 B-VG,
- „Verkehrswesen bezüglich der Schifffahrt“ bzw. „Strom- und Schifffahrtspolizei“ gemäß Art. 10 Abs. 1 Z 9 B-VG,
- „Fernmeldewesen“ gemäß Art. 10 Abs. 1 Z 9 B-VG,
- „Starkstromwegerecht, soweit sich die Leitungsanlage auf zwei oder mehrere Länder erstreckt“ gemäß Art. 10 Abs. 1 Z 10 B-VG),
- „Wasserrecht“ gemäß Art. 10 Abs. 1 Z 10 B-VG,
- „Bergwesen“ gemäß Art. 10 Abs. 1 Z 10 B-VG und
- „Gesundheitswesen“ gemäß Art. 10 Abs. 1 Z 12 B-VG.

Die Zuständigkeit des Bundes zur Gesetzgebung beruht, neben der Kompetenzdeckungsklausel im vorgesehenen § 1, auf den Kompetenztatbeständen

- „Straßenpolizei“ gemäß Art. 11 Abs. 1 Z 4 B-VG und
- „Binnenschifffahrt hinsichtlich der Schifffahrtsanlagen“ sowie „Strom- und Schifffahrtspolizei auf Binnengewässern“ gemäß Art. 11 Abs. 1 Z 6 B-VG.

Die Zuständigkeit des Bundes zur Grundsatzgesetzgebung beruht auf den Kompetenztatbeständen

- „Heil- und Pflegeanstalten“ gemäß Art. 12 Abs. 1 Z 1 B-VG und
- „Elektrizitätswesen, soweit es nicht unter Art. 10 fällt“ gemäß Art. 12 Abs. 1 Z 2 B-VG.

In jenen Bereichen, in denen die Länder zur (Ausführungs-)Gesetzgebung und/oder Vollziehung zuständig sind, beruht die Zuständigkeit des Bundes auf der in § 1 des Gesetzesentwurfs geschaffenen Kompetenzgrundlage.

Besonderheiten des Normerzeugungsverfahrens:

Der Entwurf kann im Hinblick auf die §§ 1, 46 Abs. 2 und § 51 Abs. 1 des Artikels 1 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 und bedarf überdies im Hinblick auf § 1 Abs. 1 des Artikels 1 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 Artikel 1 (Netz- und Informationssystemsicherheitsgesetz 2026 – NISG 2026)

Zu § 1 (Verfassungsbestimmung):

Das B-VG kennt keinen eigenen Kompetenztatbestand „Cybersicherheit“ oder etwa „Netz- und Informationssystemsicherheit“. Die Gefahr von Störfällen im Bereich der Cybersicherheit 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 abzuwendenden Gefahren nach der NIS-2-Richtlinie 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 NIS-2-Richtlinie umfasst sind, vielmehr um eine materienübergreifende Querschnittsgefahr, deren Abwehr verschiedenen besonderen Verwaltungsmaterien zuzuordnen ist und die demnach kompetenzrechtlich der Zuständigkeit zur Regelung des jeweiligen Sachgebietes folgt. Hinsichtlich jener Sektoren, die bereits vom NIS-1-Regime erfasst waren, begründet die (dynamische) Kompetenzdeckungsklausel in § 1 NISG seit ihrem Inkrafttreten am 29. Dezember 2018 eine ausschließliche Zuständigkeit des Bundes zur Gesetzgebung und Vollziehung in Bezug auf den diesbezüglichen Regelungsgegenstand.

Anders als Kompetenztatbestände beziehen sich Kompetenzdeckungsklauseln nicht auf durch abstrakte Begriffe umschriebene Angelegenheiten, sondern auf konkrete „Bezugsvorschriften“, die den Inhalt der Kompetenz bilden (vgl. Neudorfer, Kompetenzdeckungsklauseln außerhalb des B-VG, in Schmid ua., Auf dem Weg zum hypermodernen Rechtsstaat? 2011, 111 [128 f]), sodass diese anders (und im Ergebnis enger) auszulegen sind als herkömmliche Kompetenztatbestände. Von Relevanz ist die Ermittlung des Inhalts von Kompetenzdeckungsklauseln nur bei „dynamischen“ Kompetenzdeckungsklauseln, die auch zu einer Änderung des auf sie gestützten Gesetzes ermächtigen. Der Verfassungsgerichtshof vertritt dazu die Ansicht, dass Änderungen eines Gesetzes, die sich auf die Kompetenzdeckungsklausel stützen sollen, nicht etwa nur den Regelungsgegenstand des Gesetzes betreffen sollen, sondern mit dem „System“ des Gesetzes übereinzustimmen haben (VfSlg. 8337/1978). Daraus folgt, dass die Einbeziehung neuer Sektoren nach dem NIS-2-Regime (wie auch die Ausdehnung der Regelungen auf neue Gefahren) nicht auf die Kompetenzdeckungsklausel des § 1 NISG gestützt werden kann, sondern es diesfalls wieder einer kompetenzrechtlichen Deckung durch Verfassungsbestimmung bedarf.

Daraus ergibt sich, dass die Vorschriften in diesem Bundesgesetz, mit dem insbesondere die innerstaatliche Umsetzung der NIS-2-Richtlinie 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 diesem Hintergrund soll in § 1 Abs. 1 vorgesehen werden, dass die Erlassung, Aufhebung sowie Vollziehung von Vorschriften, wie sie in diesem Bundesgesetz enthalten sind, auch in den Belangen Bundessache sind, hinsichtlich deren das B-VG etwas anderes bestimmt. Änderungen dieses Bundesgesetzes sollen hingegen nicht von der im vorgeschlagenen § 1 Abs. 1 enthaltenden statischen Kompetenzdeckungsklausel umfasst sein, was zur Folge hat, dass jede Novelle zu diesem Bundesgesetz (zB Beseitigung von Vollzugsdefiziten) wiederum einer gesonderten Verfassungsänderung bzw. im Verfassungsrang stehenden Kompetenzdeckungsklausel bedarf (vgl. auch Janko, Staats- und Verwaltungsorganisation [2014] 9). 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. etwa § 44 Abs. 1) – in unmittelbarer Bundesverwaltung besorgt werden können.

Aus einer Zusammenschau der Regelungen in der NIS-2-Richtlinie (vgl. Art. 8 Abs. 5 NIS-2-Richtlinie sowie Art. 32 und 33 NIS-2-Richtlinie) ergibt sich, dass die Mitgliedstaaten dazu verpflichtet sind, die zuständige Behörde mit erforderlichen Befugnissen auszustatten, um die ihnen übertragenen Aufgaben wirksam und effizient zu erfüllen sowie die ordnungsgemäße Anwendung und Durchsetzung der gemäß dieser Richtlinie erlassenen nationalen Rechtsvorschriften in Bezug auf wesentliche und wichtige Einrichtungen sicherzustellen. Daher ist es erforderlich, dass die Cybersicherheitsbehörde ihre Aufsichts- und Durchsetzungsbefugnisse auch gegenüber den in Art. 19 B-VG bezeichneten obersten Organen der

Vollziehung ausüben kann, sofern diese als wesentliche oder wichtige Einrichtungen gelten (vgl. §§ 24 ff).

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 Organs nicht einer anderen Verwaltungsbehörde übertragen werden (vgl. VfSlg. 13.626/1993). Folglich bedarf es für die – unionsrechtlich vorgesehene – Ausübung von Befugnissen gegenüber obersten Organen einer entsprechenden verfassungsrechtlichen Grundlage, die mit Abs. 2 geschaffen werden soll. Demnach soll die Cybersicherheitsbehörde (in Anlehnung an die Regelung in § 35 Abs. 2 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999) dazu ermächtigt sein, ihre 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. Wesentlich ist, dass von dieser Regelung lediglich die Befugnisse der Cybersicherheitsbehörde gemäß § 26 zur bescheidmäßigen Einstufung wesentlicher oder wichtiger Einrichtungen sowie gemäß den §§ 38 und 39 zur Setzung von Aufsichts- und Durchsetzungsmaßnahmen umfasst sein sollen und damit keinesfalls ein Weisungsrecht im Sinne des Art. 20 B-VG der Cybersicherheitsbehörde gegenüber obersten Organen der Vollziehung verbunden sein soll. Durch den statischen Verweis auf die Befugnisse, wie sie in diesem Bundesgesetz enthalten sind, soll klargestellt werden, dass lediglich (geringfügige) Anpassungen der einzelnen einfachgesetzlichen (Aufsichts-/Durchsetzungs-)Befugnisse, die zu keiner Erweiterung bzw. Ausdehnung der Befugnisse führen, von der verfassungsrechtlichen Grundlage abgedeckt sind.

Zu § 2 (Gegenstand und Ziel des Gesetzes):

Netz- und Informationssysteme mit den zugehörigen Diensten sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil der heutigen Gesellschaft geworden. Diese Entwicklung hat zu einer Ausweitung der Cyberbedrohungslage geführt und neue Herausforderungen mit sich gebracht. Für wirtschaftliche und gesellschaftliche Tätigkeiten ist es von entscheidender Bedeutung, dass die Netz- und Informationssysteme verlässlich und sicher sind. Mit diesem Bundesgesetz werden daher Maßnahmen festgelegt, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen der Einrichtungen, die in den Anwendungsbereich fallen, erreicht werden soll.

Seit Inkrafttreten 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-Richtlinie) und deren nationalen Umsetzung sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz erzielt worden. Die Verpflichtungen nach der NIS-1-Richtlinie wurden in den Mitgliedstaaten der Europäischen Union jedoch auf sehr unterschiedliche Weise umgesetzt, was zu einer Fragmentierung des Binnenmarkts führte und insbesondere die grenzüberschreitende Erbringung von Diensten beeinträchtigte. Aus diesem Grund wurde die NIS-1-Richtlinie durch die NIS-2-Richtlinie ersetzt.

Mit der NIS-2-Richtlinie wird der Anwendungsbereich auf einen größeren Teil der Wirtschaft ausgeweitet, um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die im Binnenmarkt für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind.

In § 2 wird der sachliche Anwendungsbereich beschrieben. Das Bundesgesetz hat zum Ziel, das Cybersicherheitsniveau allgemein, jedoch insbesondere in den in § 2 angeführten Sektoren (näher definiert in den Anlagen 1 und 2 dieses Gesetzes), zu erhöhen.

Dieses Ziel soll durch verpflichtende Risikomanagementmaßnahmen (§ 32; vgl. Art. 21 NIS-2-Richtlinie) und Berichtspflichten (§ 34; vgl. Art. 23 NIS-2-Richtlinie) für wesentliche und wichtige Einrichtungen (§ 24), innerhalb der in Z 1 bis 18 genannten Sektoren, durch die Etablierung nationaler und internationaler Strukturen sowie durch die Einbindung anderer Einrichtungen, wie etwa Einrichtungen, die Domänennamenregistrierungsdienste (§ 29) erbringen, erreicht werden.

Die in Z 1 bis Z 18 genannten Sektoren werden in Anlage 1 (Sektoren mit hoher Kritikalität) und Anlage 2 (Sonstige kritische Sektoren) näher bestimmt. Insbesondere werden in Anlage 1 und 2 auch die betroffenen Teilsektoren und die darin enthaltene Art der Einrichtung angeführt.

Zu § 3 (Begriffsbestimmungen):

In § 3 werden die maßgeblichen Begriffsbestimmungen festgelegt. Soweit möglich und sinnvoll, wird auf einschlägige nationale Legaldefinitionen zurückgegriffen. Die Begriffsbestimmungen des Art. 6 NIS-2-

Richtlinie werden weitgehend auch im Rahmen der nationalen Umsetzung übernommen. Einzelne Begriffe, wie etwa das nicht in der NIS-2-Richtlinie definierte „Leitungsorgan“, sind zu ergänzen.

Soweit eine Begriffsbestimmung aus Art. 6 NIS-2-Richtlinie schlichtweg auf die Definition eines anderen europäischen Rechtsakts verweist, wird diese Definition im Sinne der Rechtsklarheit und zur Vermeidung von Verweisungen (insbesondere dynamischer Verweisungen auf europäisches Recht) textuell übernommen.

Folgende Begriffe werden aus der Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (im Folgenden: Rechtsakt zur Cybersicherheit), ABl. Nr. L 151 vom 07.06.2019 S. 15, textuell übernommen:

„Cybersicherheit“ (dort: Art. 2 Z 1), „IKT-Produkt“ (Art. 2 Z 12), „IKT-Dienst“ (Art. 2 Z 13), „IKT-Prozess“ (Art. 2 Z 14) und „Cyberbedrohung“ (Art. 2 Z 8).

Folgende Begriffe werden aus der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 257 vom 28.8.2014 S. 73, in der Fassung der Berichtigung ABl. Nr. L 23 vom 29.01.2015 S. 19, übernommen: „Vertrauensdienst“ (dort: Art. 3 Z 16), Vertrauensdiensteanbieter (Art. 3 Z 19) und qualifizierter Vertrauensdiensteanbieter (Art. 3 Z 20), „Qualifizierte elektronische Signaturerstellungseinheit“ (dort: Art. 3 Z 23), „Qualifizierte elektronische Siegelerstellungseinheit“ (dort: Art. 3 Z 32), „Konformitätsbewertungsstelle“ (Art. 3 Z 18), „vertrauenswürdige Systeme eines Vertrauensdiensteanbieters“ (dort: Art. 24 Abs. 2 lit. e und f).

Die Begriffsbestimmungen von „Online-Marktplatz“, „Online-Suchmaschine“ und „Cloud-Computing“, „Internet-Knoten“, „Rechenzentrumsdienste“, „Content Delivery Network“ und „Forschungseinrichtung“ werden in den Anlagen 1 und 2 definiert, da auf diese Begriffe im Gesetz nicht Bezug genommen wird.

„Netz- und Informationssysteme“ (Z 1; Art. 6 Z 1 NIS-2-Richtlinie) sind Kommunikationsnetze, wie sie auch in § 4 Z 1 TKG 2021 definiert werden. Darunter ist auch ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte zu verstehen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder digitale Daten, die von den – in den lit. a und b genannten – Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden.

Der Begriff der „Sicherheit von Netz- und Informationssystemen“ (Z 2, Art. 6 Z 2 NIS-2-Richtlinie) umfasst die Fähigkeit, alle Ereignisse, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können, abzuwehren.

Der Begriff der „Cybersicherheit“ (Z3; Art. 6 Z 3 NIS-2-Richtlinie) umfasst die Cybersicherheit im Sinne des Art. 2 Z 1 des Rechtsakts zur Cybersicherheit. Darunter versteht man alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.

Ein „öffentliches Kommunikationsnetz“ (Z 4; Art. 6 Z 36 NIS-2-Richtlinie) im Sinne des § 4 Z 9 TKG 2021 beschreibt ein Kommunikationsnetz, das ganz oder überwiegend dem öffentlichen Anbieten von Kommunikationsdiensten dient, die die Übertragung von Informationen zwischen Netzabschlusspunkten ermöglichen.

Der Begriff „Kommunikationsdienst“ (Z 5; Art. 6 Z 37 NIS-2-Richtlinie) umfasst Kommunikationsdienste im Sinne des § 4 Z 4 TKG 2021. Diese sind unabhängig vom Sitz des Anbieters im räumlichen Geltungsbereich gewöhnlich gegen Entgelt über Kommunikationsnetze erbrachte elektronische Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen, es sei denn, es handelt sich um eine geringfügige Nebendienstleistung:

- „Internetzugangsdienste“ im Sinne der Begriffsbestimmung des Artikels 2 Abs. 2 Z 2 der Verordnung (EU) 2015/2120 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union, ABl. Nr. L 310 vom 26.11.2015 S. 1,
- interpersonelle Kommunikationsdienste und
- Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden.

Der „Kommunikationsdienstes“ des § 4 Z 4 TKG 2021 ist auf „elektronische“ Dienste beschränkt und daher mit dem „elektronischen Kommunikationsdienst“ des Art. 6 Z 37 NIS-2-Richtlinie identisch.

Der Begriff „IKT-Produkt“ (Z 6; Art. 6 Z 12 NIS-2-Richtlinie) im Sinne des Art. 2 Z 12 des Rechtsakts zur Cybersicherheit bezeichnet ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems.

Der Begriff „IKT-Dienst“ (Z 7; Art. 6 Z 13 NIS-2-Richtlinie) im Sinne des Art. 2 Z 13 des Rechtsakts zur Cybersicherheit umfasst einen Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht.

Der Begriff „IKT-Prozess“ (Z 8; Art. 6 Z 14 NIS-2-Richtlinie) im Sinne des Art. 2 Z 14 des Rechtsakts zur Cybersicherheit umfasst jegliche Tätigkeiten, mit denen ein IKT-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll.

Der Begriff „Schwachstelle“ (Z 9; Art. 6 Z 15 NIS-2-Richtlinie) beschreibt eine Schwäche, eine Anfälligkeit oder eine Fehlfunktion von IKT-Produkten oder IKT-Diensten, durch deren Ausnutzung in Netz- und Informationssystemen erhebliche Störungen und Schäden verursacht werden können.

Der Begriff der „Einrichtung“ (Z 10; Art. 6 Z 38 NIS-2-Richtlinie) wird in der NIS-2-Richtlinie weit definiert und umfasst natürliche Personen sowie inländische und ausländische juristische Personen, sofern diese nach dem an ihrem Sitz geltenden nationalen Recht anerkannt sind sowie eingetragene Personengesellschaften. Als Einrichtung gelten jedoch nur solche natürlichen oder juristischen Personen oder Personengesellschaften, die in eigenem Namen Rechte ausüben und Pflichten unterliegen können (Rechts- und Handlungsfähigkeit).

Der Begriff „Leitungsorgan“ (Z 11) soll natürliche Personen beschreiben, die nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte einer Einrichtung berufen sind. Vor dem Hintergrund, dass sich in der NIS-2-Richtlinie keine Legaldefinition betreffend die Begrifflichkeit „Leitungsorgane“ findet, sollen entsprechend der Intention der diesbezüglich unionsrechtlichen Vorgaben (zu den explizit die Leitungsorgane wesentlicher und wichtiger Einrichtungen betreffenden Verpflichtungen vgl. Art. 20 NIS-2-Richtlinie sowie die in § 31 vorgeschlagene Regelung) jene natürlichen Personen umfasst sein, die auf Geschäftsführungs- bzw. Vorstandsebene in den jeweiligen Einrichtungen zuständig sind.

Eine eingeschränkte Befugnis zur Vertretung nach außen (etwa eine Prokura) etabliert noch kein „Leitungsorgan“. Folglich ist die Position eines „Chief Information Security Officer (CISO)“ für sich genommen noch kein Leitungsorgan. Es ist jedoch denkbar, dass jene Person, die die Rolle des CISO in einem Unternehmen einnimmt, auch nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte berufen ist.

Der Begriff „DNS-Diensteanbieter“ (Domainnamensystem – DNS) (Z 12; Art. 6 Z 20 NIS-2-Richtlinie) bezeichnet Einrichtungen, die öffentlich zugängliche rekursive Dienste zur Auflösung von Domänenamen für Internet-Endnutzer oder autoritative Dienste zur Auflösung von Domänenamen erbringen. Dieses Bundesgesetz ist nicht auf Root-Namenserver anwendbar. Unter Dritte gemäß lit. b sind insbesondere Domaininhaber zu verstehen. „Domainnamensystem“ oder „DNS“ bezeichnet ein verteiltes hierarchisches Verzeichnissystem, das die Identifizierung von Diensten und Ressourcen im Internet ermöglicht und es Endnutzergeräten erlaubt, Internet-Routing- und Konnektivitätsdienste zu nutzen, um diese Dienste und Ressourcen zu erreichen.

Der Begriff „Namenregister der Domäne oberster Stufe“ oder „TLD-Namenregister“ (Z 13) bezeichnet eine Einrichtung, die eine bestimmte Domäne oberster Stufe (Top Level Domain – TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domänenamen unterhalb der TLD, sowie für den technischen Betrieb der TLD, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namenserver, zuständig ist, unabhängig davon, ob der Betrieb durch die Einrichtung selbst erfolgt oder ausgelagert wird, jedoch mit Ausnahme von Situationen, in denen TLD-Namen von einem Register nur für seine eigenen Zwecke verwendet werden.

Eine „Einrichtung, die Domänennamen-Registrierungsdienste erbringt“ (Z 14; Art. 6 Z 22 NIS-2-Richtlinie) ist ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa Wiederverkäufer oder Anbieter von Datenschutz- oder Proxy-Registrierungsdiensten.

„Anbieter digitaler Dienste“ (Z 15; Art. 6 Z 16 NIS-2-Richtlinie) sind juristische Personen oder eingetragene Personengesellschaften, die einen digitalen Dienst im Sinne des § 3 Z 1 des E-Commerce-Gesetzes (ECG), BGBl. I Nr. 152/2001 erbringen. Ein digitaler Dienst im Sinne des § 3 Z 1 ECG ist ein – in der Regel gegen Entgelt – elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst. Darunter sind insbesondere der Online-Vertrieb von Waren und Dienstleistungen,

Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen sowie Datenabfragemöglichkeiten zu verstehen. Erfasst sind auch Dienste, die Informationen über ein elektronisches Netz übermitteln, den Zugang zu einem solchen vermitteln oder die Informationen des Nutzers speichern.

„Vertrauensdienste“ (Z 16; Art. 6 Z 24 NIS-2-Richtlinie) im Sinne des Art. 3 Z 19 der Verordnung (EU) Nr. 910/2014 sind elektronische Dienste, die in der Regel gegen Entgelt erbracht werden und alternativ aus

- Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, und Diensten für die Zustellung elektronischer Einschreiben sowie von diesen Diensten betreffenden Zertifikaten oder
- Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder
- Bewahrung von diesen Diensten betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten bestehen.

Werden solche Vertrauensdienste von einer natürlichen oder juristischen Person erbracht, so versteht man darunter einen „Vertrauensdiensteanbieter“ (Z 17; Art. 6 Z 25 NIS-2-Richtlinie). Hingegen versteht man unter einem „qualifizierten Vertrauensdiensteanbieter“ (Z 18; Art. 6 Z 27 NIS-2-Richtlinie) einen Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der Status eines qualifizierten Anbieters verliehen wurde. Dabei prüft die Aufsichtsstelle, ob der Vertrauensdienst die Anforderung der Verordnung (EU) Nr. 910/2014 erfüllt. Die Definition des „qualifizierten Vertrauensdienstes“ als „ein Vertrauensdienst, der die einschlägigen Anforderungen der Verordnung (EU) Nr. 910/2014 erfüllt“ konnte unterbleiben.

Eine „qualifizierte elektronische Signaturerstellungseinheit“ (Z 19) im Sinne des Art. 3 Z 23 der Verordnung (EU) Nr. 910/2014 ist eine elektronische Signaturerstellungseinheit, die die Anforderungen des Anhangs II der genannten Verordnung erfüllt.

Eine „qualifizierte elektronische Siegelerstellungseinheit“ (Z 20) im Sinne des Art. 3 Z 32 der (EU) Nr. 910/2014 bezeichnet eine elektronische Siegelerstellungseinheit, die die Anforderungen des Anhangs II der genannten Verordnung erfüllt.

Unter „Konformitätsbewertungsbericht“ (Z 21) ist ein Konformitätsbewertungsbericht im Sinne des Art. 20 Abs. 1 der Verordnung (EU) Nr. 910/2014 zu verstehen.

„Vertrauenswürdige Systeme eines Vertrauensdiensteanbieters“ (Z 22) sind Systeme und Produkte, die den Erfordernissen gem. Art. 24 Abs. 2 lit. e und f der Verordnung (EU) Nr. 910/2014 entsprechen.

„Anbieter verwalteter Dienste“ (Managed Service Provider, Z 23; Art. 6 Z 39 NIS-2-Richtlinie) eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, die entweder in den Räumlichkeiten der Kunden oder aus der Ferne erbringt. Zum besseren Verständnis wird die auch im deutschsprachigen Raum gebräuchlichere Bezeichnung „Managed Service Provider“ als Klammerausdruck beigefügt.

„Anbieter verwalteter Sicherheitsdienste“ (Z 24; Art. 6 Z 40 NIS-2-Richtlinie) ein Anbieter verwalteter Dienste, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt.

Als „Vertreter“ (Z 25; Art. 6 Z 34 NIS-2-Richtlinie) ist eine natürliche oder juristische Person zu verstehen, die befugt ist, im Auftrag der in § 3 Z 25 aufgezählten Einrichtungen, die nicht in der Union niedergelassen sind, zu handeln. Bietet daher ein DNS-Diensteanbieter, eine Einrichtung, die Domänennamen-Registrierungsdienste erbringt, ein TLD-Namenregister, ein Anbieter von Cloud-Computing-Diensten, ein Anbieter von Rechenzentrumsdiensten, ein Betreiber von Inhaltszustellnetzen, ein Anbieter verwalteter Dienste, ein Anbieter verwalteter Sicherheitsdienste oder ein Anbieter von einem Online-Marktplatz, einer Online-Suchmaschine oder einer Plattform für Dienste sozialer Netzwerke Dienste innerhalb der Union an, ist aber nicht in der Union niedergelassen, so haben diese Einrichtungen einen Vertreter in der Union zu benennen.

Die Begriffe der Z 26 bis 31 stehen in einem engen Zusammenhang und beschreiben unterschiedliche Eskalationsstufen bzw. Verwirklichungen eines „Risikos“. Die deutsche Übersetzung dieser Begriffe in der NIS-2-Richtlinie erreicht nicht die erforderliche Trennschärfe. Im Gesetz wird daher „Vorfall“, „Sicherheitsvorfall“ und „Cybersicherheitsvorfall“, einheitlich als „Cybersicherheitsvorfall“ bezeichnet (so wird der „Beinahe-Vorfall“ des Art. 6 Z 40 NIS-2-Richtlinie gemäß § 3 Z 25 ein „Beinahe-Cybersicherheitsvorfall“). Die Verwendung von „Cybersicherheitsvorfall“ erlaubt ferner eine

Abgrenzung des nicht-cyberbezogenen Sicherheitsvorfalls gemäß Art. 2 Nr. 3 der 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 (im Folgenden: Richtlinie (EU) 2022/2557).

Der Begriff „Risiko“ (Z 26; Art. 6 Z 9 NIS-2-Richtlinie) bezeichnet das Potenzial für Verluste oder Störungen, die durch einen Cybersicherheitsvorfall verursacht werden, welches als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Cybersicherheitsvorfalls zum Ausdruck gebracht wird.

Eine „Cyberbedrohung“ (Z 27; Art. 6 Z 10 NIS-2-Richtlinie) im Sinne des Art. 2 Z 8 des Rechtsakts zur Cybersicherheit bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

Eine „erhebliche Cyberbedrohung“ (Z 28; Art. 6 Z 11 NIS-2-Richtlinie) hingegen umfasst eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Einrichtung oder die Nutzer solcher Systeme erheblich zu beeinträchtigen, indem sie erheblichen materiellen oder immateriellen Schaden verursacht.

Ein „Beinahe-Cybersicherheitsvorfall“ (Z 29; Art. 6 Z 5 NIS-2-Richtlinie) ist ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt haben könnte. Ein Eintritt muss folglich nicht vorliegen.

Ein „Cybersicherheitsvorfall“ (Z 30; Art. 6 Z 6 NIS-2-Richtlinie) liegt dann vor, wenn ein Ereignis zu einer Beeinträchtigung der die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, geführt hat. Bei der Beurteilung, ob ein Cybersicherheitsvorfall vorliegt, sind insbesondere die Anzahl der betroffenen Nutzer, die Dauer der Störung, die geografische Ausbreitung der Störung sowie die Auswirkung auf wirtschaftliche oder gesellschaftliche Tätigkeiten zu berücksichtigen.

Ein „Cybersicherheitsvorfall großen Ausmaßes“ (Z 31; Art. 6 Z 7 NIS-2-Richtlinie) beschreibt einen Cybersicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats der Europäischen Union übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten der Europäischen Union hat. Cybersicherheitsvorfälle großen Ausmaßes können sich je nach Ursache und Auswirkung verschärfen und zu echten Krisen entwickeln. Dadurch kann das reibungslose Funktionieren des Binnenmarkts verhindert werden oder ernsthafte, die öffentliche Sicherheit betreffende Risiken für Einrichtungen und Bürger darstellen.

Der „Innere Kreis der Operativen Koordinierungsstruktur (IKDOK)“ (Z 32) ist eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen. Das NISG schuf bereits auf Basis, sowie unter Einbindung bereits bestehender, operativer Strukturen eigene Koordinierungsstrukturen. Diese etablierten operativen Koordinierungsstrukturen werden in den §§ 13 und 14 fortgeführt.

Der äußere Kreis ist die „Struktur zur Koordination auf der operativen Ebene“ (OpKoord) (Z 33), welche sich aus dem IKDOK und den CSIRTs zusammensetzt. Anlassbezogen kann die OpKoord um weitere Teilnehmer auch erweitert werden.

Die „Kooperationsgruppe“ (Z 34; vgl. Art. 14 NIS-2-Richtlinie) und das CSIRTs-Netzwerk (Z 35; vgl. Art. 15 NIS-2-Richtlinie) sind zwei europäische Gremien, die mit der NIS-2-Richtlinie eingerichtet wurden und der verstärkten Kooperation und dem Informationsaustausch zwischen den Mitgliedstaaten der Europäischen Union im Bereich der Netz- und Informationssystemsicherheit dienen. Diese Gremien wurden vor Inkrafttreten dieses Bundesgesetzes eingerichtet und tagen seither regelmäßig. Während die Kooperationsgruppe gemäß Art. 14 NIS-2-Richtlinie hauptsächlich strategische Themen behandelt, verbessert das CSIRTs-Netzwerk gemäß Art. 15 NIS-2-Richtlinie die operative Zusammenarbeit der europäischen CSIRTs.

Zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union wird ein Europäisches Netzwerk der Verbindungsorganisationen für Cyberkrisen (European Cyber Crises Liaison Organisation Network, kurz: EU-CyCLONe) eingerichtet (Z 36; vgl. Art. 16 NIS-2-Richtlinie).

Der „Überwachungsbeauftragte“ (Z 37) ist ein Mitarbeiter der Cybersicherheitsbehörde, der für den gemäß § 39 Abs. 3 Z 2 festgelegten Zeitraum die Einhaltung der Risikomanagementmaßnahmen (§ 32) und der Berichtspflichten (§ 34) einer wesentlichen Einrichtung überprüft. Die Bestellung eines Überwachungsbeauftragten erfolgt mit Bescheid der Cybersicherheitsbehörde gegenüber jener wesentlichen Einrichtung, die mit der Pflichterfüllung (§§ 32 und 34) säumig ist. In diesem Bescheid werden jedenfalls der Zeitraum der Überwachung und die Pflichten der wesentlichen Einrichtungen, deren Einhaltung der Überwachungsbeauftragte zu überwachen hat, klar festgelegt. Der Überwachungsbeauftragte leitet die zuständigen Personen der wesentlichen Einrichtung im Rahmen seiner Aufgaben an, und gibt dahingehend Hilfestellung, wie diese Pflichten vollständig erfüllt werden können. Der Überwachungsbeauftragte verfolgt das Ziel, gemeinsam mit der Einrichtung möglichst dauerhafte und klare Prozesse zu etablieren und Hilfestellung zu geben, sodass zukünftig alle Pflichten gemäß den §§ 32 und 34 effizient erfüllt werden können. Darüber hinaus überwacht der Überwachungsbeauftragte die Einhaltung dieser Prozesse. Zwischen dem Überwachungsbeauftragten und den für die Pflichterfüllung der wesentlichen Einrichtung zuständigen Personen wird nach Möglichkeit für den definierten Zeitraum ein ständiger Dialog etabliert. So kann die jeweilige Einrichtung von den Anleitungen des Überwachungsbeauftragten abweichen, sofern sich das Ziel der effizienten Erfüllung der Pflichten gemäß den §§ 32 und 34 auch auf andere Weise erfüllen lässt und dies etwa den Unternehmensabläufen besser entspricht oder aus anderen Gründen geboten erscheint. Dabei werden gegebenenfalls gemeinsam Lösungen erarbeitet, welche sich insbesondere auch an der Verhältnismäßigkeit und dem bestehenden Risiko orientieren. Sofern die Einrichtung jedoch ohne Begründung die erarbeiteten Prozesse nicht einhält, hat dies der Überwachungsbeauftragte der Cybersicherheitsbehörde unverzüglich weiterzuleiten.

Zu § 3a (Bundesamt für Cybersicherheit):

Während das NISG für Angelegenheiten der Netz- und Informationssystemsicherheit noch eine Aufgabenverteilung auf zwei Behörden vorsieht und dem Bundeskanzler die strategischen und dem Bundesminister für Inneres die operativen Agenden überträgt, soll mit Blick auf eine effektive und effiziente Verwaltungsführung sowie im Sinne einer schlanken Richtlinienumsetzung die ausschließliche Zuständigkeit zur Vollziehung des gegenständlichen Gesetzes bei einer Behörde liegen. Die Vereinigung der Aufgaben im Bereich der Netz- und Informationssystemsicherheit scheint zudem auch aus budgetärer Sicht sowie mit Blick auf den Fachkräftemangel im Bereich der IT-Sicherheit zweckmäßig, zumal dadurch auch eine Vermeidung von Doppelgleisigkeiten bzw. Parallelstrukturen erfolgt.

In Abs. 1 soll demnach das Bundesamt für Cybersicherheit eingerichtet werden und soll dieses in Umsetzung des Art. 8 Abs. 1 NIS-2-Richtlinie als Cybersicherheitsbehörde fungieren. Dabei soll es sich um eine monokratisch eingerichtete und dem Bundesminister für Inneres unmittelbar nachgeordnete Behörde mit bundesweiter Zuständigkeit handeln (Abs. 2) und soll vor dem Hintergrund, dass die gesamte Expertise in einer Behörde konzentriert werden soll, die ausschließliche Zuständigkeit zur Vollziehung des gegenständlichen Gesetzes – mit Ausnahme des Sanktionsregimes (vgl. §§ 44 ff) – bei der Cybersicherheitsbehörde liegen. Im Sinne einer klaren Abgrenzung zum Bereich der Sicherheitsverwaltung soll zudem gesetzlich ausdrücklich angeordnet werden, dass die Cybersicherheitsbehörde organisatorisch außerhalb der Generaldirektion für die öffentliche Sicherheit angesiedelt ist.

Die Regelung in Abs. 3 soll als Element einer starken Einbindung des Nationalrats sicherstellen, dass der Direktor sowie dessen Stellvertreter den zuständigen Ausschüssen des Nationalrats auf deren Wunsch Auskünfte aus dem jeweiligen Aufgabenbereich erteilen. Damit soll klargestellt werden, dass dem Direktor sowie dessen Stellvertreter in Ausschusssitzungen das Wort erteilt werden kann (vgl. § 18 Abs. 2 des Geschäftsordnungsgesetzes 1975, BGBI. Nr. 410/1975, [im Folgenden: GOG]) und die Ausschüsse des Nationalrats die Möglichkeit haben, den Direktor und dessen Stellevertreter als Auskunftspersonen zur Äußerung einzuladen (vgl. § 40 Abs. 1 GOG). Durch diese Regelung soll das Interpellationsrecht jedoch nicht berührt werden.

Im Falle von klassifizierten Informationen werden in einem Ausschuss wie üblich die Regelungen zur Vertraulichkeit angewendet (siehe § 37a GOG). Dies bedeutet einerseits, dass die Beratungen im Ausschuss für vom Bundesamt für Cybersicherheit als in den Stufen 1 und 2 oder ESM-Verschlussachen nach dem Informationsordnungsgesetz (InfOG), BGBI. I Nr. 102/2014, klassifizierte Informationen jedenfalls gemäß § 37a Abs. 3 GOG vertraulich sind. Werden in einem Ausschuss klassifizierte Informationen der Stufen 3 und 4 verwendet, so ist dieser Ausschuss gemäß § 37a Abs. 4 GOG geheim.

Zu § 3b (Organisation):

Dem Bundesamt für Cybersicherheit soll gemäß Abs. 1 ein Direktor vorstehen. Aus den vorgeschlagenen Bestimmungen gemäß § 3a Abs. 3, § 3b Abs. 2 sowie § 4 Abs. 4 ergibt sich, dass die Aufgaben des Direktors im Fall seiner Verhinderung durch einen Stellvertreter wahrzunehmen sein sollen.

In Abs. 2 sollen in Anbetracht der hohen Komplexität des Bereichs der Netz- und Informationssystem- bzw. Cybersicherheit sowie zur Sicherstellung der erforderlichen fachlichen Expertise bestimmte Qualifikationen bzw. Erfordernisse für die Ernennung zum Direktor und Stellvertreter festgelegt werden. Demnach soll vorgesehen werden, dass ein abgeschlossenes facheinschlägiges Hochschulstudium im Sinne der Z 1.12 der Anlage 1 des Beamten-Dienstrechtsgesetzes 1979 (BDG 1979), BGBI. Nr. 333/1979, erforderlich ist, wobei insbesondere ein abgeschlossenes juristisches oder technisches Hochschulstudium (etwa im Bereich der IT-Technik) in Betracht kommen wird. Diese Voraussetzung soll somit etwa durch Erwerb eines entsprechenden Diplom-, Master- oder Doktorgrades gemäß § 87 Abs. 1 des Universitätsgesetzes 2002 (UG), BGBI. I Nr. 120/2002, oder eines akademischen Grades gemäß § 6 Abs. 2 des Fachhochschulgesetzes (FHG), BGBI. Nr. 340/1993, aufgrund des Abschlusses eines Fachhochschul-Masterstudiengangs oder eines Fachhochschul-Diplomstudiengangs erfüllt werden können. Zudem soll es einer zumindest fünfjährigen einschlägigen Berufserfahrung bedürfen, sodass sichergestellt ist, dass nur spezifisch qualifizierte Personen zum Direktor (bzw. zum Stellvertreter) ernannt werden können.

Die Ausschreibung der Funktionen als Direktor sowie Stellvertreter soll nach den herkömmlichen Bestimmungen des Ausschreibungsgesetzes 1989 (AusG), BGBI. Nr. 85/1989, erfolgen. Um aufgrund der Sensibilität der Funktionen auch eine umfassende Beurteilung der Eignung der Bewerber für die Funktion des (stellvertretenden) Direktors sicherzustellen, soll bei der Bestellung der Mitglieder der Begutachtungskommission darauf Bedacht genommen werden, dass ein Mitglied von dem für Telekommunikation zuständigen Bundesminister bestellt wird.

In Abs. 3 soll vorgesehen werden, dass die Zentrale des Bundesamts in Wien verortet ist. Im Sinne eines effizienten Vollzugs kann es sich als sinnvoll erweisen, dass etwa zur Wahrnehmung bestimmter Aufgaben (zB Vor-Ort-Kontrollen) eine Anwesenheit vor Ort erforderlich ist. Demnach soll eine entsprechende Rechtsgrundlage geschaffen werden und der Direktor zur Wahrnehmung einzelner Aufgaben gemäß dem vorgeschlagenen § 4 Abs. 1 befugt sein, bei Bedarf Außenstellen einzurichten, wobei die Inanspruchnahme dieser Befugnis an den Grundsätzen der Zweckmäßigkeit und Wirtschaftlichkeit sowie einer effizienten und verwaltungsökonomischen Aufgabenwahrnehmung zu messen sein wird. In der Möglichkeit zur Errichtung von Außenstellen im gesamten Bundesgebiet liegt auch ein erheblicher Vorteil gegenüber einer allfälligen Ansiedelung direkt in der Zentralstelle, zumal bei einer solchen Ausgestaltung die Einrichtung von Außenstellen aufgrund verfassungsrechtlicher Vorgaben nicht möglich wäre (vgl. insbesondere Art. 5 und Art. 77 B-VG). Im Sinne eines einheitlichen und bundesweit koordinierten Aufgabenvollzugs soll der Direktor überdies (mittels Weisung) von den Außenstellen verlangen können, dass ihm diese laufend oder zu bestimmten Zeitpunkten direkt über den Fortgang einer Angelegenheit zu berichten haben.

Bei den Abs. 4 und 5 soll es sich um Regelungen betreffend die Organisation des Bundesamtes handeln und soll demnach mit Blick auf eine rasche und zweckmäßige Geschäftsbehandlung die Zahl der Organisationseinheiten im Bundesamt und in den Außenstellen einschließlich der Aufteilung der Geschäfte in einer vom Direktor zu erlassenden Geschäftseinteilung festzulegen sein (Abs. 4). Der Direktor soll überdies verpflichtet sein, für eine qualitätssichernde Aus- und Fortbildung der Mitarbeiter zu sorgen (Abs. 5).

Vor dem Hintergrund, dass es sich bei der Cybersicherheit von Netz- und Informationssystemen um eine sensible Materie handelt, soll im Sinne umfassender Transparenz – angelehnt an § 7 des Gesetzes über das Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung (BAK-G), BGBI. I Nr. 72/2009 – vorgesehen werden, dass Weisungen des Bundesministers für Inneres an den Direktor des Bundesamts schriftlich zu erteilen und zu begründen sowie im Sinne größtmöglicher Transparenz in einem halbjährlichen Bericht gesammelt zu veröffentlichen sind (Abs. 6).

Vor dem Hintergrund, dass bestimmte Beamte und Vertragsbedienstete des Bundesministeriums für Inneres künftig der Cybersicherheitsbehörde zur dauernden Dienstleistung zugewiesen werden sollen, soll in Abs. 7 vorgesehen werden, dass all jene Beamten und Vertragsbediensteten, die zum Stichtag – das ist der Tag vor Inkrafttreten des gegenständlichen Bundesgesetzes (vgl. § 51 Abs. 1 und 2) – dem Personalstand des Bundesministeriums für Inneres angehören und die gemäß der zu diesem Zeitpunkt geltenden Geschäftseinteilung der Organisationseinheit „Netz- und Informationssystemsicherheit“ zugewiesen sind, ab Inkrafttreten dieses Bundesgesetzes übergeleitet werden. Die Festlegung des Stichtags ist erforderlich, um zu gewährleisten, dass die Cybersicherheitsbehörde zeitgerecht über das

erforderliche Personal verfügt. Durch das Abstellen auf die Zugehörigkeit zu einer bestimmten Organisationseinheit zu einem bestimmten Zeitpunkt soll eine klare und transparente Regelung getroffen werden, die sicherstellt, dass für Beamte und Vertragsbedienstete klar erkennbar ist, aufgrund welcher Kriterien die Zuweisung zur Cybersicherheitsbehörde erfolgt.

Zu § 4 (Aufgaben der Cybersicherheitsbehörde):

Die Cybersicherheitsbehörde soll die strategischen und operativen Aufgaben, die sich aus der Umsetzung der NIS-2-Richtlinie ergeben und jene, die sich aus der bisherigen Umsetzung der NIS-1-Richtlinie etabliert haben, übernehmen. Dies beinhaltet die folgenden Aufgaben:

1. Koordination der Erstellung der Österreichischen Strategie für Cybersicherheit (ÖSCS) gemäß § 15;
2. Leitung der Koordinierungsstrukturen (CSS, IKDOK und OpKoord) gemäß den §§ 12 bis 14;
3. Regelmäßige Erstellung und Weiterleitung von Lagebildern und zusätzlich relevanter Informationen gemäß den §§ 12 bis 14;
4. Erstellung, Analyse und Weitergabe von zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur Vorbeugung von Cybersicherheitsvorfällen
5. Ausübung der Funktion der nationalen Behörde für das Management von Cybersicherheitsvorfällen großen Ausmaßes gemäß § 16;
6. Ausübung der Funktion des Nationalen Koordinierungszentrums für Cybersicherheit gemäß § 6;
7. Vertretung von Österreich in EU-weiten und internationalen Gremien betreffend die Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen, insbesondere in der Kooperationsgruppe, dem EU-CyCLONe sowie dem Europäischen Kompetenznetz und Zentrum für Cybersicherheit (ECCC), unbeschadet der Zuständigkeit des Bundesministers für europäische und internationale Angelegenheiten;
8. Konsultation und Zusammenarbeit mit den zuständigen Behörden anderer Mitgliedstaaten der Europäischen Union gemäß § 22;
9. Betrieb der zentralen Anlaufstelle gemäß § 5;
10. Betrieb des GovCERT gemäß § 8 Abs. 4;
11. Ermächtigung von CSIRTs gemäß § 8 Abs. 2 und Abs. 3;
12. Zulassung unabhängiger Prüfer gemäß § 7 Abs. 2 und 3;
13. Ausübung der Aufsichts- und Durchsetzungsmaßnahmen gegenüber wesentlichen und wichtigen Einrichtungen gemäß den §§ 38 und 39;
14. Entgegennahme, Analyse und Weiterleitung von Meldungen gemäß den §§ 34 und 37 sowie § 8 Abs. 1 Z 7.
15. Betrieb von IKT-Lösungen gemäß den §§ 17, 18 und 19.

Die Nationale Cybersicherheitsstrategie (Österreichische Strategie für Cybersicherheit, kurz: ÖSCS; § 15) wird unter maßgeblicher Mitwirkung der Cyber Sicherheit Steuerungsgruppe (CSS; § 12) erstellt und durch die Bundesregierung erlassen. Die Koordination der Erstellung erfolgt durch die Cybersicherheitsbehörde.

Sowohl die strategischen als auch die operativen Koordinierungsstrukturen (§§ 12 bis 14) werden von der Cybersicherheitsbehörde geleitet. Diese Leitung ist eine organisatorische (etwa die Aussendung und Einberufung von Sitzungen nach vorangehender Koordinierung, Festlegung der Tagesordnung und Worterteilung). Die Eigenständigkeit der an diesen Koordinierungsstrukturen teilnehmenden obersten Organe wird damit nicht berührt.

Neben der Leitung übernimmt die Cybersicherheitsbehörde die Erstellung von Lagebildern und zusätzlicher einschlägiger Informationen und leitet diese im Rahmen der Koordinierungsstrukturen (§§ 12 bis 14) weiter.

Über die Koordinierungsstrukturen hinaus arbeitet die Cybersicherheitsbehörde mit den CSIRTs und jenen Behörden zusammen, mit denen erwartungsgemäß Überschneidungen innerhalb der Aufgabenerfüllung auftreten (§ 20 Abs. 1 und 2). Dabei werden jedenfalls alle zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur Vorbeugung von Cybersicherheitsvorfällen gemäß § 20 Abs. 2 ausgetauscht.

Die Cybersicherheitsbehörde übt die Funktion der nationalen Behörde für das Management von Cybersicherheitsvorfällen großen Ausmaßes gemäß § 16 aus. Bisher war der Bundesminister für Inneres bereits gemäß §§ 24 und 25 NISG mit der operativen Leitung und der Koordination des Cyberkrisenmanagements betraut.

Die Cybersicherheitsbehörde nimmt ferner die Aufgaben eines nationalen Koordinierungszentrums für Cybersicherheit wahr (§ 6).

Der Cybersicherheitsbehörde kommt die Vertretung der Republik Österreich in EU-weiten und internationalen Gremien betreffend die Cybersicherheit zu. Dazu gehören insbesondere die „Horizontal Working Party on Cyber Issues (HWP Cyber)“, die „European Union Agency for Cybersecurity (ENISA)“ soweit sie den Themenbereich Cybersicherheit betreffen.

Davon unberührt bleibt die Vertretung Österreichs durch andere Ministerien in EU-weiten und internationalen Gremien in deren Wirkungsbereich, beispielsweise die Zuständigkeit des Bundesministers für europäische und internationale Angelegenheiten für Cyberdiplomatie oder des Bundesministers für Landesverteidigung für die internationale militärische Zusammenarbeit in Angelegenheiten der Sicherheit von Netz- und Informationssystemen sowie die Zuständigkeit des Bundeskanzlers in Hinsicht auf Cybersicherheitszertifizierungen. Bei interdisziplinären Arbeitsgruppen (keine klare Trennung zwischen Cybersicherheit oder Cybersicherheitszertifizierung) findet eine Abdeckung der Arbeitsgruppen durch Vertreter beider Ressorts (x+1) statt.

Im engen Zusammenhang mit der Teilnahme an internationalen Gremien steht die Zusammenarbeit der Cybersicherheitsbehörde mit den zuständigen Behörden anderer Mitgliedstaaten (§ 22).

Um die Kooperation und Kommunikation zwischen den Mitgliedstaaten im Bereich der Sicherheit von Netz- und Informationssystemen für operative Zwecke innerstaatlich zu zentralisieren und zu vereinfachen, wird in der Cybersicherheitsbehörde eine zentrale Anlaufstelle (§ 5) als Verbindungsstelle nach innen sowie nach außen (zu anderen Mitgliedstaaten, zur NIS-Kooperationsgruppe und zum CSIRTS-Netzwerk) betrieben.

Die Cybersicherheitsbehörde betreibt das bei ihr eingerichtete GovCERT (§ 8 Abs. 4). Ferner übernimmt sie die Aufgaben der Ermächtigung und Beaufsichtigung von allen CSIRTS (§ 8 Abs. 2 und 3 sowie § 10).

Unabhängige Prüfer werden durch die Cybersicherheitsbehörde zugelassen (§ 7). In diesem Zusammenhang legt die Cybersicherheitsbehörde durch Verordnung etwa nähere Regelungen zu den erforderlichen Fachkenntnissen und Fähigkeiten fest.

Als zentrale Aufgabe der Cybersicherheitsbehörde kommt dieser die Aufsicht der Einhaltung der in diesem Gesetz vorgeschriebenen Risikomanagementmaßnahmen (§ 32) und Berichtspflichten (§ 34) für wesentliche und wichtige Einrichtungen zu. Die Einhaltung der Pflichten von wesentlichen und wichtigen Einrichtungen nach diesem Bundesgesetz ist somit durch die Cybersicherheitsbehörde gemäß § 38 zu beaufsichtigen und erforderlichenfalls entsprechend § 39 durchzusetzen.

Neben der zentralen Anlaufstelle fungiert die Cybersicherheitsbehörde auch als Meldesammelstelle aller CSIRTS (§ 34 Abs. 1). Dabei werden die von den CSIRTS eingehenden Meldungen über Cyberbedrohungen, Beinahe-Cybersicherheitsvorfälle und Cybersicherheitsvorfälle entgegengenommen und entsprechend analysiert, um in regelmäßigen Abständen Lagebilder zu erstellen sowie die Meldungen und die Lagebilder mitsamt relevanter hilfreicher Zusatzinformationen an die betroffenen innerstaatlichen Behörden und Stellen weiterzuleiten (vgl. §§ 12 ff sowie § 20).

Mit dem Abs. 2 wird das Verhältnis der Cybersicherheitsbehörde zu jener Behörde, die in Durchführung der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnung (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABI. Nr. L 333 vom 27.12.2022 S. 1 die innerstaatlich zuständige Behörde ist, geregelt. Da die Verordnung (EU) 2022/2554 gegenüber der NIS-2-Richtlinie einen sektorspezifischen Rechtsakt der Europäischen Union (gemäß Art. 4 NIS-2-Richtlinie; § 27) in Bezug auf Finanzunternehmen darstellt (ErwGr 28 NIS-2-Richtlinie), wird in Abs. 2 klargestellt, dass jene zuständige Behörde für die Verordnung (EU) 2022/2554 innerhalb des dortigen Anwendungsbereichs als zuständige Behörde gilt.

Gemäß Abs. 3 soll im Sinne einer starken Einbindung des National- und Bundesrats vorgesehen werden, dass der Bundesminister für Inneres diesen den halbjährlichen Bericht zur Cybersicherheit gemeinsam mit einer Übersicht der eingelangten Meldungen gemäß § 34 (Berichtspflichten) und § 37 (Freiwillige Meldung relevanter Informationen) in anonymisierter Form und gegliedert nach Sektoren sowie die Höhe des Aufwandsersatzes gemäß § 8 Abs. 6 vorzulegen hat. Wesentlich ist, dass von der Berichtspflicht auch die seitens der Cybersicherheitsbehörde gemäß § 34 Abs. 9 übermittelten Informationen zu erheblichen Cybersicherheitsvorfällen sowie zu freiwilligen Meldungen, die gemäß § 21 Abs. 2 erfolgten Meldungen an die Datenschutzbehörde sowie die gemäß § 39 Abs. 9 übermittelten Informationen zu den ergriffenen Aufsichts- und Durchsetzungsmaßnahmen umfasst sein sollen.

Insbesondere vor dem Hintergrund des allfälligen Zugangs zu sensiblen Informationen im Rahmen ihrer Tätigkeiten soll in Abs. 4 vorgesehen werden, dass sich sämtliche Mitarbeiter der Cybersicherheitsbehörde – einschließlich des Direktors und seines Stellvertreters – vor Beginn ihrer Tätigkeit einer Sicherheitsüberprüfung gemäß den §§ 55 bis 55b des Sicherheitspolizeigesetzes (SPG), BGBI. Nr. 566/1991, für den Zugang zu geheimer Information zu unterziehen haben, die alle drei Jahre zu wiederholen sein soll. Durch den Verweis auf § 55a Abs. 4 dritter und vierter Satz SPG soll die Klarstellung erfolgen, dass unter gewissen Voraussetzungen Sicherheitsüberprüfungen auch vor Ablauf der dreijährigen Frist durchgeführt werden können.

Zu § 5 (Zentrale Anlaufstelle der Cybersicherheitsbehörde):

In Umsetzung des Art. 8 Abs. 3 der NIS-2-Richtlinie wird in der Cybersicherheitsbehörde eine zentrale Anlaufstelle eingerichtet. Gemäß Abs. 1 hat die zentrale Anlaufstelle als operative Verbindungsstelle die grenzüberschreitende Zusammenarbeit und Kommunikation mit den zuständigen Stellen in den anderen Mitgliedstaaten der Europäischen Union, der Kooperationsgruppe, EU-CyCLONe und dem CSIRTS-Netzwerk zu gewährleisten. Darüber hinaus hat die zentrale Anlaufstelle gemäß Abs. 2 eingehende Meldungen und Anfragen unmittelbar an die Mitglieder des IKDOK und die CSIRTS (Z 1) sowie Angaben aus dem Register der Einrichtungen (vgl. § 29 Abs. 6) an die ENISA weiterzuleiten (Z 2) und die zentralen Anlaufstellen in anderen Mitgliedstaaten der Europäischen Union über einen Cybersicherheitsvorfall mit grenzüberschreitenden Auswirkungen, die von diesem potentiell betroffen sind sowie die ENISA (vgl. § 34 Abs. 5) zu unterrichten (Z 3).

Die zentrale Anlaufstelle ersetzt nicht die direkte Kommunikation der CSIRTS im Rahmen des CSIRTS-Netzwerkes, sondern stellt sicher, dass es immer einen Kommunikationsweg zwischen anderen Mitgliedstaaten und den Koordinierungsstrukturen in Österreich gibt.

Zu § 6 (Nationales Koordinierungszentrum für Cybersicherheit):

In § 6 wird das nationale Koordinierungszentrum für Cybersicherheit eingerichtet, womit zugleich auch die Vorgaben des Art. 6 der Verordnung (EU) 2021/887 durchgeführt werden. Durch die Schaffung eines Koordinierungs- und Kompetenzzentrums ist es möglich, der Gesellschaft, Verwaltung, Wirtschaft und Wissenschaft ein breitgestreutes und zugleich spezialisiertes Wissen über Cybersicherheit zur Verfügung zu stellen. Auf diese Weise wird ein wesentlicher Beitrag zur Erhöhung der gesamtstaatlichen Resilienz Österreichs geleistet.

Die Cybersicherheitsbehörde nimmt die Aufgaben des nationalen Koordinierungszentrums für Cybersicherheit wahr, welches die in Art. 7 Verordnung (EU) 2021/887 genannten Tätigkeiten umfasst. Darüber hinaus koordiniert das Nationale Koordinierungszentrum für Cybersicherheit die öffentlich-private Zusammenarbeit im Bereich der Cybersicherheit sowie die Erstellung eines halbjährlichen Berichts zur Cybersicherheit.

Das Nationale Koordinierungszentrum für Cybersicherheit nimmt als Schnittstelle zwischen dem öffentlichen und dem privaten Sektor verschiedene Aufgaben im Bereich der Bewusstseinsbildung, Stärkung von Cyberkompetenzen und Prävention von Cybersicherheitsvorfällen, aber auch im Bereich der Beratung zum Forschungs- und Förderbedarf und zu den Forschungs- und Förderprioritäten im Bereich Cybersicherheit wahr.

Anträge von Einrichtungen zur Aufnahme in die Europäische Kompetenzgemeinschaft gemäß Art. 7 Abs. 1 lit. i und Abs. 4 der Verordnung (EU) 2021/887 sollen in strukturierter Form erfolgen, um eine rasche Bearbeitung zu ermöglichen. Daher soll die Möglichkeit bestehen, dass seitens der Cybersicherheitsbehörde gewisse Modalitäten zur Antragstellung vorgegeben werden. Mit dem Ziel, allfälligen Antragstellern einen möglichst niederschwelligen Zugang zur Europäischen Kompetenzgemeinschaft zu ermöglichen bzw. in diesem Zusammenhang allfällige Hemmschwellen für die jeweils in Betracht kommenden Einrichtungen zu vermeiden und mit Blick auf die Minimierung des mit der Bearbeitung solcher Anträge verbundenen Verwaltungsaufwands soll eine Befreiung von sämtlichen Gebühren gemäß dem Gebührengesetz 1957 (GebG), BGBI. Nr. 267/1957, vorgesehen werden. Zudem sollen Verwaltungsabgaben des Bundes für Amtshandlungen im Zusammenhang mit diesen Anträgen nicht zu entrichten sein (vgl. die Bundesverwaltungsabgabenverordnung 1983, BGBI. Nr. 24/1983).

Zu § 7 (Unabhängige Stellen und unabhängige Prüfer):

Mit gegenständlicher Bestimmung soll das im NISG bestehende Institut der qualifizierten Stellen und deren Prüfer mit systemischen Anpassungen in das NIS-2-Regime überführt werden, zumal sich dieses in der Vergangenheit gut bewährt hat. Zudem soll eine Anpassung der Aufgaben der unabhängigen Stellen und unabhängigen Prüfer an die Anforderungen der NIS-2-Richtlinie erfolgen. Im Unterschied zum

bisherigen Regime soll der Fokus der behördlichen Zulassung und Qualitätskontrolle nun auf die unabhängigen Prüfer gelegt werden.

Vor dem Hintergrund, dass sich im NIS-1-Regime die fehlende Eignung eines Prüfers ausschließlich auf die Zulassung bzw. Eignung (oder Nichteignung) der unabhängigen Stelle (nicht aber auf den Prüfer selbst) auswirken konnte, war das Institut der qualifizierten Stellen dahingehend zu überarbeiten, dass nunmehr mit Blick auf eine durchgängige Qualitätskontrolle die Erfüllung der Voraussetzungen zur Aufnahme der Tätigkeit eines Prüfers durch die Cybersicherheitsbehörde überprüft werden können soll, was insbesondere im Hinblick auf die verantwortungsvolle Aufgabe der unabhängigen Prüfer erforderlich scheint. Vergleichbare Prüfsysteme finden sich etwa im Wirtschaftstreuhandberufsgesetz 2017 (WTBG 2017), BGBI. I Nr. 137/2017, im Abschlussprüfer-Aufsichtsgesetz (APAG), BGBI. I Nr. 83/2016, im Umweltmanagementgesetz (UMG), BGBI. I Nr. 96/2001, oder in der Fachkundbeurteilungsverordnung (FachKBV), BGBI. II Nr. 37/2007.

Diesen Überlegungen zufolge sollen gemäß Abs. 1 als „unabhängige Stellen“ juristische Personen oder eingetragene Personengesellschaften mit Niederlassung in Österreich oder in einem anderen EU-Mitgliedstaat definiert werden, die sich zur Prüfung der Umsetzung der Risikomanagementmaßnahmen wesentlicher und wichtiger Einrichtungen gemäß § 33 Abs. 2 zumindest eines unabhängigen Prüfers bedienen. Für den Fall, dass eine natürliche Person die Tätigkeit als unabhängiger Prüfer selbstständig ausübt (zB bei einem Ein-Personen-Unternehmen), soll diese aus Gleichbehandlungsüberlegungen gleichzeitig als unabhängige Stelle gelten. Wesentlich ist, dass eine Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit durch die unabhängige Stelle voraussetzen soll.

Vor dem Hintergrund, dass die Prüfung der Umsetzung der Risikomanagementmaßnahmen eine besonders verantwortungsvolle Aufgabe darstellt, die ein entsprechendes Maß an fachlicher Kompetenz und vorhandener Erfahrung erfordert, sollen in Abs. 2 die Voraussetzungen, die eine natürliche Person für die Zulassung als unabhängiger Prüfer erfüllen muss, festgelegt werden. Demnach soll der Antragsteller gemäß Z 1 über ein österreichisches Reifeprüfungszeugnis, ein österreichisches Diplomprüfungszeugnis, ein österreichisches Zeugnis über die Berufsreifeprüfung, ein aufgrund völkerrechtlicher Vereinbarung gleichwertiges Zeugnis (vgl. dazu etwa § 64 des Universitätsgesetzes 2002 – UG, BGBI. I Nr. 120/2002) oder eine einschlägige berufliche Qualifikation verfügen.

Gemäß Z 2 soll zudem eine facheinschlägige Berufserfahrung von durchgängig mindestens drei Jahren im Ausmaß von zumindest zwanzig Wochenstunden im Bereich der Cybersicherheit (zB im Bereich der Überprüfung von Informationssicherheitsmanagementsystemen, Cybersicherheitsmanagementsystemen und Sicherheitslösungen im IT-/OT-Umfeld oder diesbezügliche Beratung in verantwortlicher Position) vorliegen, die durch Zeugnisse gemäß § 39 des Angestelltengesetzes (AngG), BGBI. Nr. 292/1921, oder in gleichwertiger Form (zB durch Projektbestätigungen oder Auftragsbestätigungen durch Dritte, die Tätigkeiten im Bereich der Cybersicherheit im geforderten zeitlichen Ausmaß darlegen) nachgewiesen werden soll.

Gemäß Z 3 soll es zudem erforderlich sein, dass der Antragsteller gegenüber der Cybersicherheitsbehörde seine Eignung zur Prüfung der Umsetzung von Risikomanagementmaßnahmen durch den Nachweis ausreichender theoretischer Fachkenntnisse sowie ausreichender praktischer Fähigkeiten zur Durchführung von Prüfhandlungen in organisatorischer und technischer Hinsicht im Rahmen einer Eignungsprüfung erbringt. Damit soll gewährleistet werden, dass die Eignung bzw. Kompetenz zur Durchführung von Prüfungen unter Berücksichtigung des Stands der Technik den gegenwärtigen Prüfstandards im Bereich der Cybersicherheit entspricht.

Wesentlich ist, dass sämtliche Voraussetzungen gemäß Abs. 2 Z 1 bis 3 im Zeitpunkt der Entscheidung kumulativ vorliegen sollen und demnach ein Antrag gemäß Abs. 2 durch Bescheid zurück- oder abgewiesen werden soll, wenn die normierten Voraussetzungen nicht vorliegen oder erbracht werden können. Unabhängig von der fehlenden gesetzlichen Anordnung bleibt es in diesem Zusammenhang der jeweiligen unabhängigen Stelle unbenommen, angemessene Sicherheitsvorkehrungen, etwa eine Verpflichtung zur Vornahme von Sicherheitsüberprüfungen gemäß den §§ 55 bis 55b SPG bei unabhängigen Prüfern vorzusehen.

Im Hinblick darauf, dass davon auszugehen ist, dass nicht nur für die Erteilung der Zulassung als unabhängiger Prüfer, sondern auch für die ordnungsgemäße Ausübung dieser Funktion praktische Erfahrungen maßgeblich sind, wird in Abs. 3 vorgeschlagen, dass die Zulassung seitens der Cybersicherheitsbehörde zu entziehen ist, wenn durch den unabhängigen Prüfer innerhalb der letzten fünf Jahre nicht zumindest eine Prüfung der Umsetzung von Risikomanagementmaßnahmen von wesentlichen oder wichtigen Einrichtungen erfolgte (Z 1) oder aufgrund etwa der Qualität der durchgeföhrten Prüfungen bzw. gesetzten Prüfhandlungen erkennbar wird, dass der jeweilige unabhängige Prüfer nicht mehr über die notwendige theoretische oder fachliche Eignung zur Prüfung der Umsetzung der

Risikomanagementmaßnahmen gemäß Abs. 2 Z 3 verfügt (Z 2). Nach rechtskräftiger Entziehung der Zulassung soll die betroffene Person erst nach Ablauf eines Jahres einen neuerlichen Antrag auf Zulassung als unabhängiger Prüfer stellen können. Dadurch soll sichergestellt werden, dass die theoretische und fachliche Eignung der unabhängigen Prüfer und somit auch die Qualität der Prüfungen auf einem hohen Niveau bleiben.

Um wesentlichen und wichtigen Einrichtungen einen Überblick über unabhängige Prüfer geben zu können, soll die Cybersicherheitsbehörde gemäß Abs. 4 eine diesbezügliche Liste mit den Kontaktdaten von unabhängigen Prüfern (zB Name, Erreichbarkeitsdaten wie E-Mailadresse und allfällige Zugehörigkeit zu einer unabhängigen Stelle) führen und diese den wesentlichen und wichtigen Einrichtungen in geeigneter Weise (zB in elektronischer Form) zur Verfügung stellen.

Vor dem Hintergrund, dass davon auszugehen ist, dass unabhängige Prüfer im Zuge der Durchführung von Prüfungen mitunter vertrauliche Informationen über die jeweiligen wesentlichen und wichtigen Einrichtungen erlangen werden, soll in Abs. 5 vorgesehen werden, dass unabhängige Prüfer über die im Rahmen der Durchführung von Prüfungen bekanntgewordenen Informationen zur vertraulichen Behandlung verpflichtet sind, sofern deren Geheimhaltung im Interesse der jeweiligen wesentlichen und wichtigen Einrichtungen geboten ist. Dies soll sinngemäß auch für sonstige Personen gelten, denen im Zuge ihrer Tätigkeit bei einer unabhängigen Stelle solche Informationen bekanntwerden. Das kann zB Mitarbeiter von unabhängigen Stellen betreffen, die keine unabhängigen Prüfer per se sind, aber im Zuge von Prüfungen administrativ unterstützen.

In Abs. 6 soll eine Verordnungsermächtigung der Cybersicherheitsbehörde zur Festlegung der Inhalte und der Form der Eignungsprüfung gemäß Abs. 2 Z 3 (Z 1) sowie zur Festlegung von Pauschalsätzen für Verwaltungsabgaben für die Zulassung als unabhängiger Prüfer (Z 2) vorgesehen werden (vgl. in diesem Zusammenhang auch die Erläuterungen zu Abs. 3). Um in diesem Zusammenhang eine umfassende und zeitgerechte Einbindung der künftigen Normadressaten sicherzustellen, sollte angestrebt werden, diese Verordnung vor Erlassung einem Begutachtungsverfahren zu unterziehen. Im Sinne eines nahtlosen Übergangs von NIS-1 auf NIS-2 vgl. die Übergangsbestimmungen in § 51 Abs. 7 und 8.

Zu § 8 (Zweck und Aufgaben der Computer-Notfallteams):

Um Cybersicherheitsvorfälle, Cyberbedrohungen und Risiken zu verhüten und zu erkennen, darauf zu reagieren und um ihre Auswirkungen abzuschwächen sowie um eine effiziente Zusammenarbeit auf Unionsebene zu gewährleisten, ist vorgesehen, dass ein oder mehrere Computer-Notfallteams, auch CSIRTs (Cybersecurity Incident Response Teams) genannt, einzurichten sind. Diese sollen der Aufsicht der Cybersicherheitsbehörde unterliegen (§ 10).

Die CSIRTs sind mit der Bewältigung von Cybersicherheitsvorfällen betraut. Zu den Hauptaufgaben der CSIRTs zählen auch die Entgegennahme von Meldungen gemäß den §§ 34 und 37 (Abs. 1 Z 7) und deren Weiterleitung an zuständige Behörden, wesentliche und wichtige Einrichtungen und andere einschlägige Interessensträger (Abs. 1 Z 2). Die CSIRTs sind damit die Erstanlaufstelle für alle in den Anwendungsbereich dieses Bundesgesetzes fallenden Einrichtungen, die von einem Cybersicherheitsvorfall betroffen sind. Die Zuständigkeit zur Entgegennahme von Meldungen erstreckt sich auf Cybersicherheitsvorfälle, die eine Meldepflicht gemäß § 34 für wesentliche und wichtige Einrichtungen auslösen, sowie andere Cybersicherheitsvorfälle, Cyberbedrohungen und Beinahe-Cybersicherheitsvorfälle, die freiwillig gemeldet werden (§ 37). CSIRTs sind in Österreich bedeutende Ansprechpartner im Bereich Cybersicherheit und betreuen im Rahmen ihrer Tätigkeit nicht nur wesentliche und wichtige Einrichtungen. Das nationale CSIRT soll daher im Rahmen der ihm zur Verfügung stehenden Ressourcen beispielsweise auch Frühwarnungen und Alarmmeldungen für KMU (kleine und mittlere Unternehmen) oder auch für eine breitere Öffentlichkeit, die auch Privatpersonen umfasst, herausgeben können (Abs. 1 Z 2).

Zusätzlich nehmen CSIRTs noch weitere technische Aufgaben wahr (Abs. 1 Z 1 bis 5 und 8). Dazu gehören etwa die Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Cybersicherheitsvorfällen, die Erhebung und Analyse forensischer Daten sowie die Ausgabe von Warnungen oder Alarmmeldungen, wenn Informationen über Cyberbedrohungen, Schwachstellen und Cybersicherheitsvorfälle bekannt werden. Diese Informationen können etwa von Dritten (anderen CSIRTs, Herstellern, Sicherheitsforschern, Dienstleistern, Non-Profit-Organisationen etc.) stammen oder sie können von den CSIRTs selbst, etwa durch aktive Informationseinholung (auf Schwachstellen oder Fehlkonfigurationen), ermittelt werden. Die CSIRTs sollten in der Lage sein, auf Ersuchen einer wesentlichen oder wichtigen Einrichtung die mit dem Internet verbundenen Anlagen innerhalb und außerhalb der Geschäftsräume zu überwachen, um das organisatorische Gesamtrisiko der Einrichtung für neu ermittelte Sicherheitslücken in der Lieferkette oder kritische Schwachstellen zu ermitteln, zu verstehen und zu verwalten. Die Einrichtung sollte dazu angehalten werden, dem CSIRT mitzuteilen, ob

es eine privilegierte Verwaltungsschnittstelle betreibt, da dies die Geschwindigkeit der Durchführung von Abhilfemaßnahmen beeinträchtigen könnte.

Ebenso wie auch die Cybersicherheitsbehörde haben CSIRTs, bei einem hohen Arbeitsaufkommen Aufgaben danach zu priorisieren, ob diese für die Schaffung oder Aufrechterhaltung eines hohen Cybersicherheitsniveaus besonders drängend sind oder nicht. Daher können bei der Durchführung der Überprüfungen die CSIRTs auf Grundlage eines risikobasierten Ansatzes bestimmten Aufgaben Vorrang einräumen.

Sofern erforderlich können auch allgemeine Handlungsempfehlungen an die betroffenen Einrichtungen ausgegeben werden. Ist eine wesentliche oder wichtige Einrichtung von einem Cybersicherheitsvorfall betroffen, so wird sie von einem CSIRT bei der ersten allgemeinen technischen Reaktion unterstützt. In der Regel handelt es sich dabei um konkrete Handlungsanweisungen und Informationen, um den aktuellen Cybersicherheitsvorfall abzuwehren und die negativen Auswirkungen dadurch möglichst gering zu halten. Nur in Ausnahmefällen können CSIRTs nach Möglichkeit und Ermessen auch vor Ort eine technische Unterstützung leisten.

Darüber hinaus beteiligen sich alle CSIRTs am europäischen CSIRTs-Netzwerk (Abs. 1 Z 6) – zB durch Eintragung auf E-Mail-Verteilerlisten oder Teilnahme in grenzüberschreitenden Arbeitsgruppen – und nehmen an der OpKoord teil (§ 14 Abs. 1).

Da CSIRTs (schlicht) hoheitliche Aufgaben wahrnehmen sollen, sollen sie, sofern es sich dabei um private Einrichtungen handelt, für diese Tätigkeiten als Beliebte anzusehen sein. CSIRTs sollen grundsätzlich auch bei einer Behörde eingerichtet werden können, wenn dies für einen bestimmten Sektor sinnvoll erscheint. Die Feststellung der Eignung und die Erteilung der Ermächtigung soll mittels konstitutiven Bescheids erfolgen. Wird dieser Bescheid befristet erlassen, so soll die Eignung vor einer neuerlichen Erlassung neuerlich zu prüfen sein. Unabhängig von einer solchen Befristung soll die Cybersicherheitsbehörde diese Ermächtigung beim Wegfall der Anforderungen (vgl. § 10 Abs. 7) widerrufen können.

Das gemäß Abs. 2 ermächtigte nationale CSIRT ist darüber hinaus auf Ersuchen einer wesentlichen Einrichtung zur proaktiven nicht intrusiven Überprüfung öffentlich zugänglicher Netz- und Informationssysteme berechtigt. Dabei kann zeitgleich nur eine Einrichtung die Funktion des nationalen CSIRTs wahrnehmen. Eine solche Überprüfung darf keine nachteiligen Auswirkungen auf das Funktionieren der Dienste der betroffenen wesentlichen oder wichtigen Einrichtungen haben. Da auch eine proaktive nicht intrusive Überprüfung öffentlich zugänglicher Netz- und Informationssysteme einen Aufwand für die überprüfte Einrichtung darstellen kann (zB ein Fehlalarm wird ausgelöst und Ressourcen gebunden), sind solche Überprüfungen, die sich auf spezifische Einrichtungen beziehen, dieser vorab nach Möglichkeit anzukündigen und in ihren Auswirkungen möglichst gering zu halten. Davon ist abzusehen, sofern der Zweck der Überprüfung (zB Abwehr einer Gefahr und Alarmierung) ansonsten vereitelt würde oder die Ankündigung mangels eines konkreten Adressaten faktisch nicht möglich ist.

Werden bei einer solchen Überprüfung anfällige oder unsicher konfigurierte Netz- und Informationssysteme ermittelt, sind die jeweiligen Einrichtungen darüber zu unterrichten. Solange kein nationales CSIRT besteht, hat das GovCERT (Abs. 4) die Aufgaben des nationalen CSIRTs wahrzunehmen.

Zur Unterstützung der wesentlichen und wichtigen Einrichtungen soll bei Bedarf für die einzelnen Sektoren jeweils ein sektorenspezifisches CSIRT eingerichtet werden können, etwa, wenn mit dem gemäß Abs. 2 ermächtigten nationalen CSIRT nicht das Auslangen gefunden werden kann (Abs. 3). Diese verfügen über das notwendige Fachwissen aus dem jeweiligen Sektor und können den wesentlichen und wichtigen Einrichtungen die bestmögliche technische Unterstützung im Rahmen der Bewältigung von Vorfällen und Cybersicherheitsvorfällen bieten. Gibt es kein sektorenspezifisches CSIRT für einen bestimmten Sektor fallen die jeweiligen Aufgaben dem nationalen CSIRT zu. Das nationale CSIRT ist also grundsätzlich für alle NIS-unterworfenen Einrichtungen zuständig und hat die Aufgabe, die einem CSIRT nach diesem Bundesgesetz zukommen, sektorenübergreifend zu erfüllen. Sollte auch kein nationales CSIRT eingerichtet sein (weil beispielsweise dessen Eignung und Ermächtigung zu widerrufen war), so übernimmt das GovCERT (Abs. 4) dessen Aufgabe in Bezug auf das Meldewesen.

Gemäß Abs. 4 soll das bei der Cybersicherheitsbehörde eingerichtete GovCERT die Aufgaben eines sektorspezifischen CSIRTs für Einrichtungen der öffentlichen Verwaltung wahrzunehmen haben.

Die Entscheidungen über die Ermächtigungen des nationalen und etwaiger sektorenspezifischer CSIRTS sind von der Cybersicherheitsbehörde in geeigneter Form (zB auf einer Website) zu veröffentlichen. Diese Veröffentlichung beinhaltet auch die Kontakt- und Identitätsdaten des jeweiligen CSIRT.

Gemäß Abs. 6 soll dem nationalen CSIRT sowie den allenfalls ermächtigten sektorspezifischen CSIRTs vom Bund ein Ersatz für die bei Erfüllung ihrer Aufgaben gemäß Abs. 1 sowie § 11 Abs. 1 entstandenen Kosten gebühren. Die genaue Höhe dieses Kostenersatzes soll auf Grundlage einer transparenten internen Kostenrechnung unter Zugrundelegung der Prinzipien der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit nach dem Grundsatz der Kostendeckung festzulegen sein. Wesentlich ist, dass bei Festlegung des Kostenersatzes die Verhältnismäßigkeit der Kostenbelastung für die öffentliche Hand zu beachten sein wird. Diese Regelung soll im Einklang mit dem Unionsrecht stehen, verhältnismäßig und diskriminierungsfrei sein und den unterschiedlichen Ansätzen für die Bereitstellung sicherer Dienste Rechnung tragen (ErwGr 46 NIS-2-Richtlinie).

Abs. 7 erlaubt es sektorspezifischen CSIRTs, auf Ersuchen betroffener Einrichtungen, die Analyse und Bewertung von Unregelmäßigkeiten, die durch eine bei dieser wesentlichen oder wichtigen Einrichtung eingerichteten IKT-Lösung gemäß § 17 erkannt wurden, vorzunehmen und die zu diesem Zweck notwendigerweise zu verarbeitenden Daten zu verarbeiten. Dies schließt auch die Verarbeitung von personenbezogenen Daten gemäß § 42 ein, sofern eine Analyse auf Basis vollständig alterner Datensätze nicht möglich oder zielführend ist.

Abs. 8 nimmt auf den Austausch von Informationen innerhalb sektorspezifischer und sektorübergreifender Zusammenschlüsse wichtiger und wesentlicher Einrichtungen gemäß § 36 Bezug und verpflichtet CSIRTs, mit diesen Einrichtungen zusammenzuarbeiten und Informationen auszutauschen (zB im Rahmen eines Information Sharing and Analysis Centers – ISACs).

Wegen der Bedeutung der internationalen Zusammenarbeit im Bereich Cybersicherheit sollten die CSIRTs sich zusätzlich zum CSIRTs-Netzwerk an anderen internationalen Kooperationsnetzen beteiligen können.

Mit den Bestimmungen gemäß den §§ 42 und 43 werden auch für CSIRTs explizite datenschutzrechtliche Grundlagen geschaffen. Im Kontext dieser Bestimmungen ist auch auf ErwGr 49 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) hinzuweisen. Darin wird ausgeführt, dass die Verarbeitung von personenbezogenen Daten durch Behörden, CSIRTs, Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellt, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, das heißt soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solch berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of Service“-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

Zur Erfüllung ihrer Aufgaben sollten die CSIRTs und die zuständigen Behörden daher in der Lage sein, Informationen, einschließlich personenbezogener Daten, mit nationalen CSIRTs oder zuständigen Behörden von Drittländern auszutauschen, sofern die Bedingungen des Datenschutzrechts der Union für die Übermittlung personenbezogener Daten an Drittländer, unter anderem gemäß Art. 49 DSGVO, erfüllt sind.

In Abs. 12 soll vorgesehen werden, dass die Cybersicherheitsbehörde verpflichtet ist, die Ermächtigung gemäß Abs. 2 und 3 zu widerrufen, sofern eine der Anforderungen gemäß § 9 Abs. 1 nicht mehr erfüllt wird.

Zu § 9 (Anforderungen und Eignung von CSIRTs):

CSIRTs erfüllen zentrale Aufgaben im Bereich der Cybersicherheit, insbesondere sind sie für die Entgegennahme von Meldungen sowie deren Weiterleitung verantwortlich. Es ist daher erforderlich, dass CSIRTs technische und organisatorische Anforderungen aufweisen können (Abs. 1). Diese Anforderungen an CSIRTs werden durch Art. 11 NIS-2-Richtlinie vorgegeben. Diese betreffen die Sicherheit, Belastbarkeit und Verfügbarkeit ihrer Kommunikationskanäle, um die Kontaktaufnahme mit anderen Einrichtungen sowie die eigene Erreichbarkeit jederzeit garantieren zu können (Z 1). Auch ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen muss vorhanden (Z 2) und die Vertraulichkeit und Vertrauenswürdigkeit ihrer Tätigkeit gewährleistet sein (Z 3) sowie die

Betriebskontinuität, die sowohl im personellen, technischen als auch im infrastrukturellen Bereich sichergestellt werden (Z 4 und 5). Die NIS-2-Richtlinie verlangt in diesem Zusammenhang eine „ständige Bereitschaft“ (Art. 11 Abs. 1 Buchstabe e NIS-2-Richtlinie), worunter eine rund um die Uhr Rufbereitschaft zu verstehen ist. Z 6 verpflichtet CSIRTs die Pflichten der §§ 32 und 34 auch selbst entsprechend zu erfüllen und Risikomanagementmaßnahmen umzusetzen und erhebliche Sicherheitsvorfälle (direkt an die Cybersicherheitsbehörde) zu melden. Darüber hinaus ist sicherzustellen, dass die bei einem CSIRT angestellten Personen über die notwendige fachliche Eignung verfügen und sich vor Beginn ihrer Tätigkeit für den Zugang zu geheimer Information einer Sicherheitsüberprüfung nach den Bestimmungen des SPG unterzogen haben (Z 4 und 7). Zum Nachweis der Unterstützung aus dem Sektor kommen beispielsweise finanzielle, personelle oder sonstige Ressourcen (Bereitstellung von IT-Infrastruktur) in Frage (Z 8). Sollten sich Umstände, die zur Ermächtigung geführt haben, nachträglich ändern, so hat das betroffene CSIRT dies unverzüglich der Cybersicherheitsbehörde anzuzeigen. (Abs. 2).

Zur Wahrnehmung ihrer gesetzlichen Aufgaben sollten CSIRTs Kooperationsbeziehungen mit einschlägigen Interessenträgern des Privatsektors zu pflegen. Zur Erleichterung dieser Zusammenarbeit haben die CSIRTs die Annahme und Anwendung gemeinsamer oder standardisierter Vorgehensweisen, Klassifizierungssysteme und Taxonomien für

1. Verfahren zur Bewältigung von Cybersicherheitsvorfällen,
2. das Krisenmanagement und
3. die koordinierte Offenlegung von Schwachstellen gemäß § 11 Abs. 1

zu fördern. Dies umfasst auch die Förderung von einschlägigen nationalen und europäischen Forschungsprojekten.

Mitarbeiter von CSIRTs sollen über bekanntgewordene Tatsachen und Erkenntnisse, die im Rahmen der Wahrnehmung der Aufgaben nach diesem Bundesgesetz auftreten und deren Geheimhaltung im Interesse der jeweiligen geprüften Einrichtungen geboten ist, zur Geheimhaltung verpflichtet sein (Abs. 4).

Zu § 10 (Aufsicht):

Die Aufsicht der gemäß § 8 Abs. 2 oder 3 eingerichteten CSIRTs soll bei der Cybersicherheitsbehörde liegen. In Ausübung dieses Aufsichtsrechts soll diese ein Weisungsrecht gegenüber den CSIRTs haben. Die Cybersicherheitsbehörde soll ebenso ermächtigt sein, die CSIRTs und deren gesetzliche Voraussetzungen zu überprüfen, Mängel festzustellen und gegebenenfalls die Ermächtigung zu widerrufen.

Zu § 11 (Koordinierte Offenlegung von Schwachstellen):

Mit dieser Bestimmung wird Art. 12 NIS-2-Richtlinie umgesetzt. Das nationale CSIRT hat gemäß Abs. 1 die von natürlichen oder juristischen Personen gemeldeten Schwachstellen von IKT-Produkten oder IKT-Diensten entgegenzunehmen. Auf Ersuchen des Melders oder des Herstellers bzw. Anbieters fungiert das nationale CSIRT als Vermittler und ermöglicht einen Austausch zwischen diesen. Darüber hinaus hat das nationale CSIRT die von einer Schwachstelle betroffenen Einrichtungen zu ermitteln und zu kontaktieren (Z 1), den Melder zu unterstützen (Z 2) und Zeitpläne für die Offenlegung der Schwachstelle auszuhandeln und das Vorgehen bei Schwachstellen, die mehrere Einrichtungen betreffen, zu koordinieren (Z 3). Abs. 2 stellt klar, dass die Meldung einer Schwachstelle an das nationale CSIRT auch anonym erfolgen kann und verpflichtet das nationale CSIRT hinsichtlich einer gemeldeten Schwachstelle Folgemaßnahmen durchzuführen. Soweit eine gemeldete Schwachstelle erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten der Europäischen Union hat, obliegt dem nationalen CSIRT die Zusammenarbeit mit den übrigen CSIRTs im Rahmen des CSIRTS-Netzwerks (Abs. 3). Abs. 4 regelt, dass die Aufsichtsstelle gemäß § 12 des Signaturen- und Vertrauensdienstegesetzes (SVG), BGBl. I Nr. 50/2016, über Schwachstellen, die eine qualifizierte elektronische Signaturerstellungseinheit, eine qualifizierte elektronische Siegelerstellungseinheit oder ein vertrauenswürdiges System eines Vertrauensdiensteanbieters betreffen, zu informieren ist. Diese Information hat unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme der Schwachstelle durch das nationale CSIRT zu erfolgen.

Zu § 12 (Cyber Sicherheit Steuerungsgruppe):

Die Cyber Sicherheit Steuerungsgruppe (CSS) ist das zentrale, strategisch-planende Organ der Cybersicherheit in Österreich. Sie entwickelt und koordiniert sämtliche Maßnahmen der Österreichischen Strategie für Cybersicherheit (ÖSCS). Darüber hinaus überwacht sie die Umsetzung der ÖSCS (Monitoring), aktualisiert den Maßnahmenkatalog und erstellt einen halbjährlichen Bericht zur Cybersicherheit.

Der CSS kommen folgende Aufgaben zu:

1. Mitwirkung bei der Entwicklung und Koordination der ÖSCS gemäß § 15 Abs. 1;
2. Beobachtung der Umsetzung der ÖSCS (Monitoring);
3. Mitwirkung bei der Erstellung eines halbjährlichen Berichts zur Cybersicherheit;
4. Erstellung einer eigenen Geschäftsordnung.

Die CSS setzt sich aus je einem zur selbstständigen Behandlung von Angelegenheiten ermächtigten fachkundigen Vertreter der dem Nationalen Sicherheitsrat angehörenden Bundesminister (§ 3 Abs. 1 des Bundesgesetzes über die Errichtung eines Nationalen Sicherheitsrates, BGBI. I Nr. 122/2001) sowie der für Telekommunikation und Digitalisierung zuständigen Bundesminister zusammen. Ein Vertreter der Präsidentschaftskanzlei ist berechtigt, an den Sitzungen der CSS mit beratender Stimme teilzunehmen (Abs. 3). Themenorientiert kann die CSS um Vertreter anderer Einrichtungen im Sektor der öffentlichen Verwaltung erweitert werden („CSS+“), insbesondere, wenn diese selbst oder ihr Wirkungsbereich von Maßnahmen der ÖSCS betroffen sind (Abs. 4).

Es sei klargestellt, dass unabhängig von der Leitung der CSS, die Verantwortlichkeiten der zuständigen obersten Organe des Bundes unberührt bleiben. Inhaltliche Zuständigkeiten und die Letztverantwortung sollen demnach beim jeweils zuständigen Ressort verbleiben. Ein Durchgriffsrecht der Cybersicherheitsbehörde auf andere Ressorts oder eine Kompetenzverschiebung ist mit dieser Regelung – auch aus verfassungsrechtlichen Gründen – nicht beabsichtigt und sollen demzufolge auch keine diesbezüglichen (inhaltlichen) Verantwortlichkeiten auf das CSS (oder andere Koordinierungsstrukturen) übergehen.

Zu § 13 (Innerer Kreis der Operativen Koordinierungsstruktur – IKDOK):

Die operativen Koordinierungsstrukturen, die bereits durch das NISG etabliert wurden, werden mit den §§ 13 und 14 fortgeführt. Diese operativen Koordinierungsstrukturen bestehen aus einem „Inneren Kreis“ und einem „Äußeren Kreis“. Der Innere Kreis der Operativen Koordinierungsstruktur (IKDOK; § 3 Z 28) ist eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen. Mit der Einrichtung der operativen Koordinierungsstrukturen kommt es zu keinen Verschiebungen der inhaltlichen Zuständigkeiten und die Letztverantwortung soll demnach beim jeweils zuständigen Ressort verbleiben (vgl. Erläuterung zu § 12).

Im Rahmen des IKDOK wird das von der Cybersicherheitsbehörde erstellte Lagebild über Risiken, Cyberbedrohungen und Cybersicherheitsvorfälle sowie Erkenntnisse, die gemäß § 17 Abs. 1 und 2 (Betrieb von IKT-Lösungen) gewonnen wurden, erörtert. Der Austausch von klassifizierten Informationen zwischen den Teilnehmern ist zur Wahrnehmung der Aufgaben nach Maßgabe ihrer Zuständigkeiten zulässig.

Zu § 14 (Operative Koordinierungsstruktur – OpKoord):

Im Rahmen der Operativen Koordinierungsstruktur (OpKoord), die sich aus dem IKDOK und den CSIRTs zusammensetzt, wird das gesamtheitliche Lagebild betreffend die Cybersicherheit erörtert.

Die OpKoord kann darüber hinaus um Vertreter von wesentlichen und wichtigen Einrichtungen sowie sonstigen Teilnehmern erweitert werden, wenn deren Wirkungsbereich von einem Cybersicherheitsvorfall, einer Cyberbedrohung oder einem Beinahe-Cybersicherheitsvorfall betroffen ist („erweiterte OpKoord“). Dies kann auch Einrichtungen umfassen, die nicht in den Anwendungsbereich der NIS-2-Richtlinie fallen.

Aufgrund der Sensibilität der Informationen, die im Rahmen der Erörterung des gesamtheitlichen Lagebildes ausgetauscht werden, sollen Teilnehmer des OpKoord zur Geheimhaltung verpflichtet sein, sofern in der Sitzung nichts anders beschlossen wird. Die Verpflichtung zur Geheimhaltung soll nicht für jene Mitglieder der OpKoord gelten, die im IKDOK vertreten sind, da diese ohnehin bereits sonstigen gesetzlichen (zB dienstrechtlichen) Geheimhaltungspflichten unterliegen.

Die näheren Regelungen über das Zusammenwirken der Teilnehmer des OpKoord, d.h. konkret zwischen jenen Einrichtungen, die im IKDOK (§ 13) vertreten sind und jenen, die ausschließlich im OpKoord vertreten sind, wird durch die Teilnehmer des IKDOK geregelt. Die Festlegung einer solchen Geschäftsordnung, die insbesondere die Einberufung von Sitzungen und die Zusammensetzung regeln kann, erfolgt im Einvernehmen.

In Abs. 5 wird festgelegt, dass die an der OpKoord teilnehmenden Einrichtungen (einschließlich der privaten Akteure) personenbezogene Daten zum Zweck der Organisation des OpKoord und zur Wahrnehmung der Aufgaben gemäß Abs. 1 verarbeiten dürfen, soweit dies hiefür erforderlich ist.

Zu § 15 (Nationale Cybersicherheitsstrategie):

Mit dieser Bestimmung wird Art. 7 NIS-2-Richtlinie umgesetzt, welcher die Erlassung einer Cybersicherheitsstrategie durch die Mitgliedstaaten und deren wesentliche Inhalte vorschreibt.

Die Strategie baut innerstaatlich auf der bereits bestehenden Österreichischen Strategie für Cyber Sicherheit (ÖSCS) aus dem Jahr 2021 auf. Die ÖSCS soll auf Basis des § 15 weiterentwickelt werden und mit Rücksicht auf die Vorgaben des § 15 einen Rahmen mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen in Österreich vorgeben.

Abs. 1 sieht vor, dass die Cybersicherheitsbehörde die Erstellung der ÖSCS koordiniert (vgl. § 4 Abs. 1 Z 1) und die Cyber Sicherheit Steuerungsgruppe (CSS) einzubinden ist. Bereits bisher leisteten die Mitglieder der CSS einen maßgeblichen Beitrag bei der Erstellung der ÖSCS 2021. Die Cybersicherheitsstrategie umfasst insbesondere strategische Ziele und angemessene Politik- und Regulierungsmaßnahmen, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen im Bundesgebiet erreicht und aufrechterhalten werden soll, weshalb diese durch die Bundesregierung erlassen wird.

Zu § 16 (Management von Cybersicherheitsvorfällen großen Ausmaßes):

Diese Bestimmung setzt Art. 9 NIS-2-Richtlinie um. Aus Zwecken der Begriffsklarheit wird anstelle der in der NIS-2-Richtlinie verwendeten Synonyme „Cybersicherheitsvorfälle großen Ausmaßes und Krisen“ lediglich der Begriff „Cybersicherheitsvorfall großen Ausmaßes“ verwendet.

Die Cybersicherheitsbehörde ist als zentrale Behörde im Bereich der Cybersicherheit auch für das Management von Cybersicherheitsvorfällen großen Ausmaßes zuständig. Dies beinhaltet die Teilnahme am EU-CyCLONe (§ 3 Z 36) und dessen Unterstützung bei der Aufgabenerfüllung (§ 4 Abs. 1 Z 5 und 7).

Wie in § 3 Z 31 definiert, setzt ein Cybersicherheitsvorfall großen Ausmaßes einen Cybersicherheitsvorfall (§ 3 Z 30) voraus, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat. Erreicht ein solcher Cybersicherheitsvorfall – für sich genommen oder in Zusammensetzung mit einschlägigen Cyberbedrohungen, Risiken oder anderen Cybersicherheitsvorfällen bzw. Beinahe-Cybersicherheitsvorfällen – dieses Ausmaß, so wird die Cybersicherheitsbehörde im Rahmen des Abs. 1 tätig.

Die Beurteilung, ob ein Cybersicherheitsvorfall großen Ausmaßes vorliegt, erfolgt somit holistisch und nicht bloß anhand des konkreten Cybersicherheitsvorfalls. So kann ein Cybersicherheitsvorfall bereits für sich genommen mehrere Mitgliedstaaten betreffen (etwa bei grenzüberschreitend tätigen Unternehmen), aber ebenso kann ein Cybersicherheitsvorfall einer wesentlichen/wichtigen Einrichtung in Österreich, eine Schwachstelle/ein Risiko und damit eine Cyberbedrohung für eine Einrichtung in einem oder mehreren anderen Mitgliedstaaten der europäischen Union zur Folge haben. In beiden Fällen hat der Cybersicherheitsvorfall Auswirkungen auf zwei Mitgliedstaaten der Europäischen Union.

Wird ein Cybersicherheitsvorfall als einer „großen Ausmaßes“ erkannt, ist dies von der Cybersicherheitsbehörde im Rahmen des EU-CyCLONe zu erörtern. Die Feststellung, dass ein „Cybersicherheitsvorfall großen Ausmaßes“ vorliegt, ist nicht eigens kundzumachen.

Die Cybersicherheitsbehörde hat gemäß Abs. 2 verschiedene präventive Maßnahmen zu setzen, um ein effizientes Management von Cybersicherheitsvorfällen großen Ausmaßes zu ermöglichen. Dies beinhaltet das Ermitteln von Kapazitäten, Mittel und Verfahren, die im Fall eines Cybersicherheitsvorfalls großen Ausmaßes eingesetzt werden können (unter Berücksichtigung des aktuellen Lagebildes der Koordinierungsstrukturen) und darauf aufbauend, die Verabschiedung eines nationalen Plans für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes. Dieser Plan (Abs. 3) hat insbesondere Folgendes zu beschreiben:

1. die Ziele der nationalen Vorsorgenmaßnahmen und -tätigkeiten;
2. die Aufgaben und Zuständigkeiten der Behörden für das Management von Cybersicherheitsvorfällen großen Ausmaßes;
3. die Verfahren für das Management von Cybersicherheitsvorfällen großen Ausmaßes, einschließlich deren Integration in den nationalen Rahmen für das allgemeine Krisenmanagement, und die Kanäle für den Informationsaustausch;
4. die nationalen Vorsorgemaßnahmen, einschließlich Übungen und Ausbildungsmaßnahmen;
5. die einschlägigen öffentlichen und privaten Interessenträger und die betroffene Infrastruktur;

6. die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und Regelungen, die gewährleisten sollen, dass sich die Republik Österreich wirksam am koordinierten Management von Cybersicherheitsvorfällen großen Ausmaßes auf Unionsebene beteiligen und dieses unterstützen kann.

Die Cybersicherheitsbehörde übermittelt die einschlägigen Informationen über den gemäß Abs. 3 erstellten Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes sowohl an die Europäische Kommission als auch an das EU-CyCLONe. Von den übermittelten Informationen sind jedoch jene Informationen auszunehmen, wenn und soweit dies aus Gründen der nationalen Sicherheit erforderlich ist.

Zu § 17 (Betrieb von IKT-Lösungen):

In Abs. 1 soll generell dargestellt werden, dass die Cybersicherheitsbehörde für die Erfüllung ihrer behördlichen Aufgaben nach diesem Bundesgesetz IKT-Lösungen zu betreiben hat. Dabei kann der Begriff IKT-Lösung als Gesamtheit aller informationstechnologischen Maßnahmen und technischen Mittel, die erforderlich sind, um Nutzern Funktionen und Informationen automationsunterstützt zur Verfügung zu stellen, verstanden werden (vgl. § 1 Abs. 2 Z 1 des IKT-Konsolidierungsgesetzes – IKTKonG, BGBl. I Nr. 35/2012). Unter dem Betrieb von IKT-Lösungen in diesem Sinne wird insbesondere auch der Betrieb eines sogenannten Cyber Hubs und einer nationalen SOC-Plattform verstanden.

Eine spezielle Ausprägung solcher IKT-Lösungen findet sich in Abs. 2, welche im Grunde § 13 Abs. 1 NISG idF BGBl. I Nr. 111/2018 entspricht. Es handelt sich dabei um IKT-Lösungen, die der frühzeitigen Erkennung von Risiken, Cyberbedrohungen oder Cybersicherheitsvorfällen betreffend die Netz- und Informationssysteme der Teilnehmer an diesen IKT-Lösungen dienen. Durch entsprechend konfigurierte und vor bzw. innerhalb der Netzwerke der Teilnehmer implementierte Sensorik (Software) können Angriffe, das Vorgehen des jeweiligen Angreifers im Netz des Teilnehmers und seine Kommunikation mit Schadsoftware erkannt werden. Es erfolgt dabei weder eine Analyse von Daten innerhalb des Teilnehmernetzwerkes, noch ist die Überwachung von Internet-Backbones (leistungsstarkes Netzwerk, das die „Internet-Service-Provider“ [ISPs] weltweit miteinander verbindet) vorgesehen. Verschlüsselte Daten, die die Sensorik passieren, werden von dieser nicht entschlüsselt. Darüber hinaus kann ein Austausch von relevanten Cyber-Bedrohungsinformationen und sicherheitsrelevanten Ereignissen durch direkte Verbindung zwischen qualifizierten IKT-Sicherheitsteams (insbesondere Security Operations Center, kurz SOC) des Betreibers und der Teilnehmer oder von diesen herangezogenen Dienstleistern erfolgen.

Wesentliche Einrichtungen – insbesondere Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene – und wichtige Einrichtungen sollen freiwillig am Betrieb teilnehmen können, wobei die Teilnahme mittels Vertrag geregelt wird. Gegenstand eines solchen Vertrages können beispielsweise Teilnahmemodalitäten, Austauschmodalitäten von Erkenntnissen, die Örtlichkeit der zu implementierenden Sensorik, technische Spezifikationen (wie etwa Schnittstellen), Regelungen zur Informations- und Datensicherheit oder nähere Bestimmungen zur Datenverarbeitung sein. Dem Teilnehmer soll hierbei die Möglichkeit gegeben werden, zu bestimmen, wo die Sensorik in seinem Netz platziert wird und welche Daten übermittelt werden.

Weiters ist vorgesehen, dass dem Bund für die Teilnahme am Frühwarnsystem ein Kostenersatz in Form eines Pauschalbetrags gebührt, dessen Zusammensetzung und Höhe nach Maßgabe der durchschnittlichen Kosten durch eine Verordnung der Cybersicherheitsbehörde festgelegt werden soll. Dabei sollen insbesondere die Anschaffungskosten der IKT-Lösungen sowie deren jährliche Wartungs- bzw. Instandhaltungskosten berücksichtigt werden.

Der Betrieb der IKT-Lösungen durch die Cybersicherheitsbehörde umfasst neben deren Instandhaltung (das heißt Installation, Sicherstellung der Funktionalität, Wartung etc.) und Management auch die Führung einer „Threat Intelligence“ (TI), die als zentrale Datenbank Informationen zu aktuellen Bedrohungen aufbereitet und die IKT-Lösungen mit jenen Erkennungsmustern („Indicators of Compromise“, kurz IOC) zu Bedrohungen über technische Schnittstellen speist, die von diesen in den aus- und eingehenden Datenströmen der Teilnehmer automatisiert oder teilautomatisiert erkannt werden sollen. Basierend auf IOC ist es für die IKT-Lösungen möglich, Unregelmäßigkeiten zu erkennen (IOC-basiertes Frühwarnsystem). Ob es sich bei einer Unregelmäßigkeit auch tatsächlich um eine Störung handelt, die eine Alarmierung und entsprechende Behandlung nach sich zieht, kann erst nach eingehender Analyse und Bewertung entschieden werden, wofür primär der jeweilige Teilnehmer bzw. dessen qualifiziertes IKT-Sicherheitsteam (insbesondere SOC) zuständig ist. Der Betreiber unterhält ebenso ein SOC zur Unterstützung von SOC der Teilnehmer und zur Qualitätssicherung des Systems. Im Falle einer Alarmierung ist, unabhängig von der internen Behandlung der Störung durch den jeweiligen Teilnehmer,

jedenfalls eine Weiterleitung des entsprechenden Alarms (darüber, dass etwas passiert ist) inklusive zusammenhängender Informationen (der Kontext darüber, was den Alarm ausgelöst hat, zB bestimmte IOC) an den Betreiber zur Analyse und Bewertung sowie Aufnahme in die TI und auch Verarbeitung im Lagebildprozess des IKDOK vorgesehen. Auch Informationen zu aufgetretenen Fehlalarmen werden an den Betreiber übermittelt. Eine solche Weiterleitung einer Alarmierung an den Betreiber stellt keine Meldung (freiwillig oder verpflichtend) eines Cybersicherheitsvorfalls im Sinne dieses Bundesgesetzes dar.

Zudem ist die Cybersicherheitsbehörde durch Abs. 3 – welche im Grunde § 13 Abs. 2 NISG idF BGBI. I Nr. 111/2018 entspricht – ermächtigt, IKT-Lösungen, zu betreiben oder (bloß) zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen. Das können bspw. sog. „Honeypots“ und „Sinkholes“ sein.

Unter dem Überbegriff „Honeypots“, der auch „Honeypot“-ähnliche Ansätze, wie zB „Honeynets“ umfasst, versteht man vermeintlich verwundbare Systeme bzw. Systemteile, die in ihrer primären Anwendungsform zwar vom Internet aus verfügbar sind, dort aber nicht offensiv publiziert werden. Nebenbei können sie aber auch in internen Netzen eingesetzt werden, um Angreifer leichter zu erkennen. „Honeypots“ sind nicht real verwundbar, sondern zeichnen Angriffsversuche lediglich auf und geben dem Angreifer dadurch das Gefühl, einen erfolgreichen Angriff durchgeführt zu haben. Ihre primäre Aufgabe liegt darin, die Vorgehensweise von Angreifern zu analysieren sowie die angewandten Angriffsmethoden zu erkennen.

„Sinkholes“ hingegen sind insbesondere für die Erkennung von Botnetzen erforderlich, von denen eine wesentliche Gefahr für die Netz- und Informationssystemsicherheit in Österreich ausgeht. Ein Botnetz ist ein Zusammenschluss von netzwerkfähigen Geräten, die mit Schadsoftware infiziert sind und über einen oder mehrere sogenannte „C2-Server“ (Command and Control Server) kontrolliert und missbräuchlich verwendet werden können. „Sinkholes“ stellen Maßnahmen dar, die dahingehend Abhilfe schaffen, dass sie den Datenverkehr zwischen infizierten netzwerkfähigen Geräten und C2-Servern analysieren. Sie bieten somit die Möglichkeit, Botnetze entsprechend zu untersuchen und die Kommunikation zwischen infizierten Geräten und C2-Servern so einzuschränken, dass kein Schaden verursacht werden kann. IKT-Lösungen wie zB „Sinkholes“ können dadurch genutzt werden, indem die Cybersicherheitsbehörde solche nicht unbedingt von sich aus physisch betreibt, sondern auch nur auf den Datenverkehr von bei Dritten installierten Sinkholes nach deren auf freiwilliger Basis erteilten Einwilligung Zugriff bekommt.

Daraus gewonnene Erkenntnisse dienen insbesondere als Grundlage für eine aktuelle Lageeinschätzung durch den IKDOK (§ 13 Abs. 2). Neben der Cybersicherheitsbehörde kommt auch dem GovCERT innerhalb seines Zuständigkeitsbereichs die Befugnis zu, solche IKT-Lösungen zu betreiben oder zu nutzen, um zu wichtigen Informationen der aktuellen Gefährdungslage zu gelangen.

Zu § 18 (Meldeanalysesystem):

In dieser Bestimmung wird die Einrichtung des „Meldeanalysesystems“ vorgesehen, welches im Grunde § 11 NISG idF BGBI. I Nr. 111/2018 entspricht.

Bei diesem System handelt es sich um IKT-Lösungen und IT-Verfahren, in welchen Inhalte von Meldungen über Risiken, Cyberbedrohungen und Cybersicherheitsvorfälle sowie Erkenntnissen, die aus dem Betrieb von IKT-Lösungen zur Vorbeugung von insbesondere Cybersicherheitsvorfällen (§ 17 Abs. 2 und 3) gewonnen wurden, verarbeitet werden. Ein IT-Verfahren kann als ein Bestandteil einer IKT-Lösung verstanden werden, der über Informationstechnologie als Service genutzt wird (vgl. § 1 Abs. 2 Z 2 IKTKonG). Hinsichtlich der im Rahmen des Meldeanalysesystems verarbeiteten Daten kann diesbezüglich auf § 42 Abs. 2 verwiesen werden. Der Zweck des Betriebs des Meldeanalysesystems liegt in der Analyse und damit zusammenhängenden Bewertung von Risiken, Cyberbedrohungen und Cybersicherheitsvorfällen für Netz- und Informationssysteme und der Unterstützung der Erstellung von Lagebildern (Abs. 1).

Das Meldeanalysesystem soll von der Cybersicherheitsbehörde technisch betrieben und dem Bundesminister für Inneres, dem Bundeskanzler sowie dem Bundesminister für Landesverteidigung bereitgestellt werden. Es handelt sich dabei um ein Dateisystem (Art. 4 Nr. 6 DSGVO), für welches die Cybersicherheitsbehörde, der Bundeskanzler, der Bundesminister für Inneres und der Bundesminister für Landesverteidigung gemeinsam datenschutzrechtliche Verantwortliche gemäß Art. 4 Nr. 7 in Verbindung mit Art. 26 DSGVO bzw. § 47 DSG sein sollen (Abs. 2).

Anders als in § 11 Abs. 3 NISG idF BGBI. I Nr. 111/2018 soll die Erfüllung der datenschutzrechtlichen Pflichten nach der DSGVO und dem 3. Hauptstück DSG gegenüber Betroffenen jedem Verantwortlichen hinsichtlich jener Daten obliegen, die im Zusammenhang mit den von ihm geführten Verfahren oder den von ihm gesetzten Maßnahmen verarbeitet werden (Abs. 3).

Zu § 19 (IKDOK-Plattform):

In dieser Bestimmung wird die Einrichtung der „IKDOK-Plattform“ vorgesehen, welche im Grunde § 12 NISG idF BGBI. I Nr. 111/2018 entspricht. Für die Organisation des IKDOK und zur Wahrnehmung der Aufgaben des IKDOK (zB die Erörterung und Aktualisierung von entsprechend themenspezifischen Lagebildern) kann die Cybersicherheitsbehörde eine IKT-Lösung betreiben. Im Falle des Betriebs einer solchen IKT-Lösung ist diese den im IKDOK vertretenen Ressorts bereitzustellen (Abs. 1).

Der Bundesminister für Inneres, die Cybersicherheitsbehörde, der Bundeskanzler, der Bundesminister für Landesverteidigung und der Bundesminister für europäische und internationale Angelegenheiten sind im Falle des Betriebs gemeinsam datenschutzrechtliche Verantwortliche gemäß Art. 4 Nr. 7 in Verbindung mit Art. 26 DSGVO bzw. § 47 DSG. Hinsichtlich der in der IKDOK-Plattform verarbeiteten Datenkategorien kann auf § 42 Abs. 2 verwiesen werden (Abs. 2).

Die Erfüllung der datenschutzrechtlichen Pflichten nach der DSGVO und dem 3. Hauptstück DSG gegenüber Betroffenen soll jedem Verantwortlichen hinsichtlich jener Daten obliegen, die im Zusammenhang mit den von ihm geführten Verfahren oder den von ihm gesetzten Maßnahmen verarbeitet werden (Abs. 3).

Zu § 20 (Zusammenarbeit auf nationaler Ebene):

Zur wirksamen Erfüllung der Aufgaben und Pflichten der Cybersicherheitsbehörde und der CSIRTs, wird in Abs. 1 deren Zusammenarbeit festgelegt. Abs. 2 der Bestimmung setzt Art. 13 Abs. 4 NIS-2-Richtlinie um, wonach die Mitgliedstaaten dafür sorgen sollen, dass zwischen den zuständigen Behörden, zentralen Anlaufstellen sowie CSIRTs und den Strafverfolgungsbehörden, den nationalen Behörden gemäß den Verordnungen (EG) Nr. 300/2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002, ABl. Nr. L 91 vom 09.04.2008 S. 72, und der Verordnung (EU) 2018/1139 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates, ABl. Nr. L 212 vom 22.08.2018 S. 1, den Aufsichtsstellen gemäß der Verordnung (EU) Nr. 910/2014, den gemäß der Verordnung (EU) 2022/2554 zuständigen Behörden, den nationalen Regulierungsbehörden gemäß der Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation, ABl. Nr. L 321 vom 17.12.2018 S. 36, den gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden sowie im Rahmen anderer sektorspezifischer Rechtsakte der Union innerhalb des jeweiligen Mitgliedstaats zuständiger Behörden eine angemessene Zusammenarbeit stattfinden kann.

Demnach hat die Cybersicherheitsbehörde für die Erfüllung ihrer gesetzlichen Aufgaben und Pflichten insbesondere mit der Kriminalpolizei, den Staatsanwaltschaften und den Gerichten, den Behörden, die das Luftfahrt Sicherheitsgesetz 2011 (LSG 2011), BGBI. I Nr. 111/2010, vollziehen, den Behörden, die als zuständige nationale Aufsichtsbehörde bzw. zuständige nationale Behörde im Sinne der Verordnung (EU) 2018/1139 sowie deren delegierten Rechtsakte und Durchführungsrechtsakte benannt sind, den Behörden, welche innerstaatlich die Einhaltung der Verordnung (EU) 2022/2554 sicherstellen, der Aufsichtsstelle gemäß § 12 SVG, der nationalen Regulierungsbehörde gemäß § 194 TKG 2021 sowie der KommAustria gemäß § 199 TKG 2021 zusammenzuarbeiten.

Die Cybersicherheitsbehörde hat in diesem Zusammenhang zu prüfen, ob eine Zusammenarbeit mit den in Abs. 2 genannten Behörden zur Erfüllung ihrer gesetzlichen Aufgaben und Pflichten erforderlich ist. Die Bestimmung sieht darüber hinaus vor, dass Informationen über relevante Umstände, die auch personenbezogene Daten beinhalten können und im Aufgabenbereich der jeweiligen Behörden liegen und deren Übermittlung der Erhöhung der Cybersicherheit dient, anlassbezogen ausgetauscht werden können. Abs. 7 stellt jedoch klar, dass ein Informationsaustausch mit der Aufsichtsstelle gemäß Abs. 2 Z 4 jedenfalls dann zu erfolgen hat, wenn es sich um Risiken, Cyberbedrohungen und Cybersicherheitsvorfälle eines Vertrauensdiensteanbieters handelt, oder die Angelegenheiten Schwachstellen gemäß § 11 Abs. 4 betreffen.

In Abs. 3 wird festgelegt, dass Kriminalpolizei, Staatsanwaltschaften und Gerichte ermächtigt sind, der Cybersicherheitsbehörde nach Maßgabe des § 76 Abs. 4 der Strafprozeßordnung 1975 (StPO), BGBI. Nr. 631/1975, ermittelte personenbezogene Daten zu übermitteln, soweit eine Weiterverarbeitung dieser Daten durch die Cybersicherheitsbehörde für die Erfüllung ihrer gesetzlichen Aufgaben und Pflichten nach diesem Bundesgesetz erforderlich ist. In Abs. 4 wird in Umsetzung der Bestimmung gemäß Art. 13 Abs. 5 NIS-2-Richtlinie festgelegt, dass die Cybersicherheitsbehörde mit den zuständigen nationalen Behörden, der noch umzusetzenden Richtlinie (EU) 2022/2557, hinsichtlich der Identifizierung kritischer

Einrichtungen im Sinne der Richtlinie (EU) 2022/2557 sowie hinsichtlich Risiken, Cyberbedrohungen und Sicherheitsvorfällen aber auch hinsichtlich nicht cyberbezogener Risiken, Bedrohungen und Sicherheitsvorfällen zusammenarbeiten und wesentliche Informationen, insbesondere zu den als Reaktion auf diese Risiken, Bedrohungen und Sicherheitsvorfälle ergriffenen Maßnahmen austauschen soll.

Abs. 5 legt Informationspflichten der Cybersicherheitsbehörde gegenüber jener Behörde, die in Umsetzung des Art. 9 Richtlinie (EU) 2022/2557 als zuständige Behörde benannt oder eingerichtet wurde, fest. Demnach hat die Cybersicherheitsbehörde von Aufsichts- und Durchsetzungsmaßnahmen, die sie gegenüber Einrichtungen gemäß § 24 Abs. 1 Z 1 lit. f setzen will, zu unterrichten.

In Abs. 6 wird jener Behörde, die in Umsetzung des Art. 9 Richtlinie (EU) 2022/2557 als zuständige Behörde benannt oder eingerichtet wurde, die Möglichkeit eingeräumt, die Cybersicherheitsbehörde um die Ausübung von Aufsichts- und Durchsetzungsmaßnahmen gegenüber Einrichtungen, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden, zu ersuchen. Die Cybersicherheitsbehörde hat jene Aufsichts- und Durchsetzungsmaßnahmen sodann zu setzen.

Die Informationspflicht des Abs. 5 gilt gemäß Abs. 7 entsprechend auch für Aufsichts- und Durchsetzungsmaßnahmen, welche gegenüber wesentlichen und wichtigen Einrichtungen, die als IKT-Dritt Dienstleister gemäß Art. 31 der Verordnung (EU) 2022/2554 benannt wurden, gesetzt werden sollen. In diesem Fall hat die Cybersicherheitsbehörde das gemäß Art. 32 Abs. 1 der Verordnung (EU) 2022/2554 eingerichtete Überwachungsforum zu unterrichten.

Die letztgenannten Bestimmungen dienen dazu, die diesbezüglichen Vorgaben aus Art 32 Abs. 9 und 10 NIS-2-Richtlinie und Art. 21 Abs. 5 zweiter Satz der Richtlinie (EU) 2022/2557 umzusetzen, um eine sinnvolle Koordinierung der Aufsichtstätigkeiten zwischen den dafür zuständigen Behörden vorzusehen.

Abs. 8 sieht vor, dass ein Informationsaustausch mit der Aufsichtsstelle gemäß Abs. 2 Z 4 jedenfalls in Angelegenheiten zu erfolgen hat, die Risiken, Cyberbedrohungen und Cybersicherheitsvorfälle eines Vertrauensdiensteanbieters oder Schwachstellen einer qualifizierten elektronischen Signaturerstellungseinheit, einer qualifizierten elektronischen Siegelerstellungseinheit oder der vertrauenswürdigen Systeme eines Vertrauensdiensteanbieters betreffen.

Abs. 9 sieht vor, dass die Cybersicherheitsbehörde vor der Durchführung von Aufsichts- und Durchsetzungsmaßnahmen gegenüber Betreibern gemäß § 4 Z 25 TKG 2021 und Anbietern gemäß § 4 Z 36 TKG 2021 die nationale Regulierungsbehörde gemäß § 194 TKG 2021 und die KommAustria gemäß § 199 TKG 2021 zu unterrichten hat. Dies soll verhindern, dass zur Gewährleistung des gebotenen Cybersicherheitsniveaus von mehreren Behörden Durchsetzungsmaßnahmen vorgenommen werden.

Zu § 21 (Zusammenarbeit mit der Datenschutzbehörde):

Art. 13 Abs. 4 NIS-2-Richtlinie legt fest, dass die Mitgliedstaaten zur wirksamen Erfüllung der Aufgaben und Pflichten der nationalen Behörden für eine angemessene Zusammenarbeit mit der Datenschutzbehörde sorgen sollen. Art. 35 NIS-2-Richtlinie enthält darüber hinaus spezifische Regelungen, wie mit Verstößen, die mit Verletzungen des Schutzes personenbezogener Daten einhergehen, umgegangen werden soll. Um eine angemessene Zusammenarbeit zu gewährleisten, insbesondere bei der Bearbeitung und der Anordnung von Abwehr- und Abhelfemaßnahmen von Cybersicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO und § 36 Abs. 2 Z 1 DSG führen, soll die Möglichkeit eines Informationsaustausches zwischen der Cybersicherheitsbehörde und der Datenschutzbehörde geschaffen werden. Vor dem Hintergrund der Bestimmung des Art. 35 Abs. 2 NIS-2-Richtlinie, wonach keine Geldbuße für einen Verstoß verhängt werden darf, wenn die Datenschutzbehörde bereits eine Geldbuße für diesen Verstoß verhängt hat, soll die Datenschutzbehörde die Cybersicherheitsbehörde über die Verhängung einer solchen Geldbuße durch Übermittlung einer Ausfertigung des Straferkenntnisses gegenüber einer wesentlichen oder wichtigen Einrichtung informieren. Ebenso hat die Datenschutzbehörde die Cybersicherheitsbehörde über den Umstand der Einstellung eines Verfahrens zu informieren (Abs. 3). Die Bestimmung orientiert sich an § 117 f Abs. 3 des Ärztegesetzes 1998 (ÄrzteG 1998), BGBI. I Nr. 169/1998.

Zu § 22 (Internationale Zusammenarbeit):

Die Bestimmung setzt Art. 37 NIS-2-Richtlinie um. Wenn eine Einrichtung Dienste in mehr als einem Mitgliedstaat erbringt oder ihre Netz- und Informationssysteme in einem anderen Mitgliedstaat als demjenigen angesiedelt sind, in dem sie Dienste erbringt, soll die Cybersicherheitsbehörde mit den zuständigen Behörden im betreffenden Mitgliedstaat zusammenarbeiten (Abs. 1). In Abs. 2 wird die Zusammenarbeit näher definiert:

1. über die zentralen Anlaufstellen unterrichtet die Cybersicherheitsbehörde die zuständigen Behörden in den anderen betroffenen Mitgliedstaaten über die Aufsichts- und Durchsetzungsmaßnahmen und konsultiert sie zu diesen;
2. die Cybersicherheitsbehörde kann eine andere zuständige Behörde ersuchen, Aufsichts- oder Durchsetzungsmaßnahmen zu ergreifen;
3. auf begründetes Ersuchen einer anderen zuständigen Behörde leistet die Cybersicherheitsbehörde der ersuchenden Behörde in einem ihnen zur Verfügung stehenden Ressourcen angemessenen Umfang Rechtshilfeersuchen, damit die Aufsichts- oder Durchsetzungsmaßnahmen wirksam, effizient und kohärent durchgeführt werden können. Die Rechtshilfeersuchen kann die Erteilung von Auskünften und die Durchführung von Aufsichtsmaßnahmen, einschließlich der Durchführung von Vor-Ort-Kontrollen, externen Aufsichtsmaßnahmen und gezielten Überprüfungen umfassen.

Sofern die Cybersicherheitsbehörde zur Unterstützung von einer zuständigen Behörde in einem anderen Mitgliedstaat aufgefordert wird, regelt Abs. 3, unter welchen Umständen die Cybersicherheitsbehörde ein solches Amtshilfeersuchen ablehnen darf. In Abs. 4 wird der Cybersicherheitsbehörde schließlich ermöglicht, gemeinsame Aufsichtsmaßnahmen mit der zuständigen Behörde eines anderen Mitgliedstaats durchzuführen, wenn dies im gegenseitigen Einvernehmen geschieht.

Zu § 23 (Peer Reviews):

Die Bestimmung setzt Art. 19 NIS-2-Richtlinie um und soll zu einem verbesserten Informationsaustausch zwischen der Cybersicherheitsbehörde und den nationalen Behörden in den Mitgliedstaaten beitragen, wobei dieser Austausch, insbesondere von „best practices“, den Reifegrad der Mitgliedstaaten im Bereich der Cybersicherheit verbessern soll.

Art. 19 NIS-2-Richtlinie sieht vor, dass die Kooperationsgruppe bis zum 17. Jänner 2025 mit Unterstützung der Kommission und der ENISA und gegebenenfalls des CSIRTs-Netzwerks die Methode und die organisatorischen Aspekte der Peer Reviews festlegen wird, um aus gemeinsamen Erfahrungen zu lernen, das gegenseitige Vertrauen zu stärken, ein hohes gemeinsames Cybersicherheitsniveau zu erreichen und die für die Umsetzung dieser Richtlinie erforderlichen Cybersicherheitsfähigkeiten und -konzepte der Mitgliedstaaten zu verbessern. Die Teilnahme an Peer Reviews ist freiwillig. Die Peer Reviews werden von Sachverständigen für Cybersicherheit durchgeführt. Die Sachverständigen für Cybersicherheit werden von mindestens zwei Mitgliedstaaten benannt, die sich von dem überprüften Mitgliedstaat unterscheiden. Die Methode muss objektive, nichtdiskriminierende, faire und transparente Kriterien umfassen, anhand deren die Mitgliedstaaten Sachverständige für Cybersicherheit benennen, die für die Durchführung der Peer Reviews infrage kommen (Art. 19 Abs. 1 und 2 NIS-2-Richtlinie).

Die Peer Reviews umfassen physische oder virtuelle Besuche am Standort sowie abseits des Standorts den Austausch von Informationen. Im Einklang mit dem Grundsatz der guten Zusammenarbeit stellt der Mitgliedstaat, der Gegenstand der Peer Review ist, den benannten Sachverständigen für Cybersicherheit die für die Bewertung erforderlichen Informationen zur Verfügung, vorbehaltlich der Rechtsvorschriften der Union oder der Mitgliedstaaten über den Schutz vertraulicher oder als Verschlussache eingestufter Informationen und der Wahrung grundlegender Funktionen des Staates wie der nationalen Sicherheit. Die Kooperationsgruppe entwickelt in Zusammenarbeit mit der Kommission und der ENISA geeignete Verhaltenskodizes zur Untermauerung der Arbeitsmethoden der benannten Sachverständigen für Cybersicherheit. Sämtliche durch die Peer Review erlangten Informationen dürfen nur zu diesem Zweck verwendet werden. Die an der Peer Review beteiligten Sachverständigen für Cybersicherheit geben keine sensiblen oder vertraulichen Informationen, die im Laufe der Peer Review erlangt wurden, an Dritte weiter (Art. 19 Abs. 6 NIS-2-Richtlinie).

Nachdem sie einer Peer Review unterzogen wurden, dürfen innerhalb von zwei Jahren nach Abschluss der Peer Review in diesem Mitgliedstaat keine weiteren Peer Reviews zu denselben Aspekten, die in einem Mitgliedstaat überprüft wurden, durchgeführt werden, es sei denn, der Mitgliedstaat beantragt etwas anderes oder es wird auf Vorschlag der Kooperationsgruppe etwas anderes vereinbart (Art. 19 Abs. 7 NIS-2-Richtlinie).

Gemäß Abs. 1 soll die Cybersicherheitsbehörde an Peer Reviews teilnehmen können.

In Abs. 2 soll auf die Verlässlichkeit und etwaige Geheimhaltungspflichten eingegangen werden, um den angebrachten Umgang mit etwaigen, im Zuge des Peer Reviews erlangten, Daten sicherzustellen.

Abs. 3 bezieht sich auf Art. 19 Abs. 8 NIS-2-Richtlinie. Demnach stellen Mitgliedstaaten sicher, dass jegliches Risiko eines Interessenkonflikts im Zusammenhang mit den benannten Sachverständigen für Cybersicherheit den anderen Mitgliedstaaten, der Kooperationsgruppe, der Kommission und der ENISA vor Beginn der Peer Review offengelegt wird. Der Mitgliedstaat, der Gegenstand der Peer Review ist,

kann Einwände gegen die Benennung bestimmter Sachverständiger für Cybersicherheit erheben, wenn er dem benennenden Mitgliedstaat stichhaltige Gründe mitteilt.

Abs. 4 setzt Art. 19 Abs. 9 NIS-2-Richtlinie um. Demnach erstellen die an Peer Reviews beteiligten Sachverständigen für Cybersicherheit Berichte über die Ergebnisse und Schlussfolgerungen der Peer Reviews. Die einer Peer Review unterliegenden Mitgliedstaaten können zu den sie betreffenden Berichtsentwürfen Stellung nehmen; diese Stellungnahmen werden den Berichten beigefügt. Die Berichte enthalten Empfehlungen zur Verbesserung der im Rahmen der Peer Review behandelten Aspekte. Die Berichte werden gegebenenfalls der Kooperationsgruppe und dem CSIRTS-Netzwerk vorgelegt. Ein einer Peer Review unterliegender Mitgliedstaat kann beschließen, seinen Bericht oder eine redigierte Fassung davon öffentlich zugänglich zu machen.

Zu § 24 (Wesentliche und wichtige Einrichtungen):

In Umsetzung der NIS-2-Richtlinie wird zwischen wesentlichen und wichtigen Einrichtungen unterschieden. Die Einstufung als wesentliche oder wichtige Einrichtung ist von zwei Faktoren abhängig:

- ob eine Einrichtung zumindest einem der Sektoren des § 2, die in den Anlagen 1 und 2 dieses Bundesgesetzes näher spezifiziert werden, zuzuordnen ist und
- ob sie ein mittleres oder großes Unternehmen ist (sofern die Einstufung als wichtige oder wesentliche Einrichtung nicht bereits größenunabhängig erfolgt).

Die NIS-2-Richtlinie gibt somit im Grundsatz ein klares System vor, wonach die Einstufung als wesentliche oder wichtige Einrichtung anhand der zwei oben genannten Faktoren (Sektoren und Unternehmensgröße; letzteres als „size-cap-rule“ bezeichnet) erfolgt. Von diesem Grundsatz wird jedoch vereinzelt abgewichen. So werden einzelne (Teil-)Sektoren in der NIS-2-Richtlinie unabhängig von der Unternehmensgröße in den Anwendungsbereich einbezogen bzw. als wesentliche/wichtige Einrichtung eingestuft (zB Vertrauensdiensteanbieter; vgl. Art. 2 Abs. 2 lit. a bis f NIS-2-Richtlinie sowie deren Abs. 3 und 4).

Anstelle eines zweistufigen Vorgehens, wie es in Art. 2 und 3 der NIS-2-Richtlinie vorgesehen ist, ist für die Einstufung als wesentliche oder wichtige Einrichtung nach diesem Bundesgesetz ausschließlich § 24 maßgeblich. Dabei geht die engere Definition der wesentlichen Einrichtungen jener der wichtigen Einrichtungen vor.

Als „wesentliche Einrichtungen“ gelten gemäß Abs. 1 Z 1 unabhängig von der Größe der Einrichtung qualifizierte Vertrauensdiensteanbieter, Namenregister der Domäne oberster Stufe (TLD Namenregister), DNS-Diensteanbieter, Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene, Einrichtungen, die von der Cybersicherheitsbehörde als wesentliche Einrichtung eingestuft wurden (§ 26 Abs. 1) sowie Einrichtungen, die als kritische Einrichtungen iSD Richtlinie (EU) 2022/2557 ermittelt wurden. Damit werden Art. 3 Abs. 1 lit. b, d, e und f NIS-2-Richtlinie umgesetzt. Art. 3 Abs. 1 lit. e iVm Art. 2 Abs. 2 lit. b bis e NIS-2-Richtlinie, wird in § 26 (Größenunabhängige Einstufung als wesentliche oder wichtige Einrichtung) eingehend geregelt.

Abs. 1 Z 2 legt in Umsetzung des Art. 3 Abs. 2 lit. c NIS-2-Richtlinie fest, dass Anbieter öffentlicher elektronischer Kommunikationsnetze sowie Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste bereits dann als wesentliche Einrichtung gelten, wenn sie jeweils ein „mittleres“ Unternehmen (vgl. § 25 Abs. 3) betreiben.

Mit Abs. 1 Z 3 wird festgelegt, dass jene Einrichtungen, die der Anlage 1 dieses Gesetzes zuzuordnen sind und nicht bereits in den Z 1 und 2 angeführt sind, nur dann als wesentliche Einrichtung gelten, wenn diese Einrichtungen ein großes Unternehmen (vgl. § 25 Abs. 2) betreiben. Damit wird Art. 3 Abs. 1 lit. a NIS-2-Richtlinie umgesetzt.

Von der Möglichkeit bei der Umsetzung der NIS-2-Richtlinie die bisherigen „Betreiber wesentlicher Dienste“ (§ 3 Z 9, 10 des bisher geltenden NISG) gemäß Art. 3 Abs. 1 lit. g NIS-2-Richtlinie pauschal als wesentliche Einrichtungen einzustufen, wird abgesehen. Mit der NIS-2-Richtlinie entfällt die Anknüpfung an den „wesentlichen Dienst“ vollständig. Stattdessen wird die gesamte Einrichtung, abhängig von den bereits einleitend zu dieser Bestimmung erläuterten Faktoren zur Gänze als wesentliche oder als wichtige Einrichtung eingestuft. Auch sind die Risikomanagementmaßnahmen (§ 32) und die Berichtspflichten (§ 34) nicht auf bestimmte Dienste der Einrichtung beschränkt, sondern es hat eine wesentliche oder wichtige Einrichtung für alle Dienste die dort vorgeschriebenen Pflichten zu erfüllen. Hinsichtlich der von den Einrichtungen betriebenen Dienste können diese Pflichten jedoch unterschiedlich ausfallen, wie sich ein Blick auf das risikobasierte Vorgehen gemäß § 32 Abs. 1 und die Schwelle des „erheblichen“ Cybersicherheitsvorfalls bei der Berichtspflicht gemäß § 34 Abs. 1 iVm § 35 zeigt.

In Abs. 2 werden die wichtigen Einrichtungen definiert. Demnach gelten Einrichtungen, die nicht als wesentliche Einrichtung und auch nicht größenunabhängig als wichtige Einrichtung qualifiziert werden können, nur dann als wichtige Einrichtung, wenn sie sowohl ein (mindestens) mittleres Unternehmen (§ 25 Abs. 3) betreiben und andererseits dieses einem der Sektoren der Anlagen 1 und 2 zugeordnet werden kann („Auffangklausel“).

Größenunabhängig werden als wichtige Einrichtungen gemäß § 24 Abs. 2 Z 3 jene Einrichtungen eingestuft, die gemäß Art. 2 NIS-2-Richtlinie größenunabhängig in den Anwendungsbereich fallen, jedoch nicht bereits als wesentliche Einrichtungen zu qualifizieren sind, sofern diese in den Anlage 1 und 2 angeführt sind. Einrichtungen im Sektor der öffentlichen Verwaltung auf Landesebene gemäß Abs. 5 sind ebenso größenunabhängig als wichtige Einrichtungen zu qualifizieren.

Einrichtungen, die Domänennamenregistrierungsdienste erbringen, sind weder wesentliche noch wichtige Einrichtungen.

Aus Abs. 1 und 2 ergibt sich im Umkehrschluss, dass Einrichtungen, die nicht zumindest ein mittleres Unternehmen (vgl. § 25 Abs. 3) betreiben und nicht aufgrund einer der größenunabhängigen Einstufungen bereits als wesentliche oder wichtige Einrichtung gelten, den Pflichten nach diesem Bundesgesetz (mit Ausnahme der Registrierungspflicht, die auch für Einrichtungen, die Domänennamenregistrierungsdienste erbringen, gilt) nicht unterliegen.

Abs. 3 definiert die Einrichtung im Sektor der öffentlichen Verwaltung gemäß Art. 6 Nr. 35 NIS-2-Richtlinie für das nationale Recht. Art. 2 Abs. 2 lit. f NIS-2-Richtlinie sieht vor, dass die NIS-2-Richtlinie für Einrichtungen im Sektor der öffentlichen Verwaltung unabhängig von der Größe der Einrichtungen gilt, sofern es sich dabei um

- von einem Mitgliedstaat gemäß nationalem Recht definierte Einrichtung der öffentlichen Verwaltung der Zentralregierung oder
- von einem Mitgliedstaat gemäß nationalem Recht definierte Einrichtung im Sektor der öffentlichen Verwaltung auf regionaler Ebene, die nach einer risikobasierten Bewertung Dienste erbringt, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte, handelt.

Die europäischen Begriffe („Zentralregierung“ und „regionale Ebene“) sind mit Blick auf den österreichischen Staatsaufbau nach der Bundesverfassung als „Bund“ und „Länder“ zu verstehen (Art. 2 iVm 10 ff B-VG).

Ferner können Mitgliedstaaten gemäß Art. 2 Abs. 5 NIS-2-Richtlinie vorsehen, dass Einrichtungen im Sektor der öffentlichen Verwaltung auf lokaler Ebene in den Anwendungsbereich der nationalen Umsetzungsrechtsakte fallen können.

Von der Möglichkeit, Einrichtungen im Sektor der öffentlichen Verwaltung auf „lokaler Ebene“ (innerstaatlich als „Gemeinden“ zu verstehen) in den Anwendungsbereich aufzunehmen (Art. 2 Abs. 5 NIS-2-Richtlinie), wurde kein Gebrauch gemacht. Da Wien im Rahmen der Verwaltungsorganisation insofern eine Sonderstellung einnimmt, als es primär als Gemeinde organisiert und erst auf zweiter Ebene als Land eingerichtet ist (vgl. Koprivnikar, Art. 108 B-VG, in Kneihs/Lienbacher, Rill-Schäffer-Kommentar Bundesverfassungsrecht, 11. Lfg. [2011], Rz 8f), bedarf es in diesem Fall einer differenzierten Betrachtung, zumal die „lokale Ebene“ – in Übereinstimmung mit der NIS-2-Richtlinie – vom Sektor der öffentlichen Verwaltung nicht umfasst sein soll. Neben den Gemeinden gelten auch Bildungseinrichtungen, insbesondere Schulen und Universitäten bzw. Hochschulen, nicht als wesentliche oder wichtige Einrichtungen.

Als Einrichtungen im Sektor der öffentlichen Verwaltung sollen gemäß Abs. 3 Einrichtungen gelten, die

1. zum Zweck eingerichtet wurden, im öffentlichen Interesse liegende Aufgaben nicht gewerblicher Art zu erfüllen,
2. der Aufsicht des Bundes oder eines Landes unterstehen oder an die Weisungen eines obersten Organs gebunden sind oder ein Leitungs- oder Aufsichtsorgan haben, das mehrheitlich aus Mitgliedern besteht, die von Bundes- oder Landesbehörden oder von anderen auf Bundes- oder Landesebene eingerichteten Körperschaften des öffentlichen Rechts eingesetzt worden sind, oder an denen der Bund oder ein Land mit mindestens 50 vH des Stamm-, Grund- oder Eigenkapitals beteiligt ist oder Mitglieder der Bundesregierung sind und
3. ermächtigt sind, im Rahmen ihrer gesetzlich übertragenen Aufgaben Bescheide zu erlassen, die Rechte Einzelner im grenzüberschreitenden Personen-, Waren, Dienstleistungs- oder Kapitalverkehr berühren,

mit Ausnahme der Gemeinden sowie Gemeindeverbände.

Vor dem Hintergrund, dass der Bundespräsident ex constitutione kein Mitglied der Bundesregierung darstellt (vgl. Z 2), soll dieser auch nicht vom Anwendungsbereich umfasst sein (und damit auch nicht die Präsidentschaftskanzlei).

Als maßgebliche definitorische Einschränkung ist eine Einrichtung nur dann als Einrichtung im Sektor der öffentlichen Verwaltung zu qualifizieren, wenn sie – neben den vorgenannten Voraussetzungen – ferner berechtigt ist, Bescheide zu erlassen, die Rechte Einzelner im grenzüberschreitenden Personen-, Waren-, Dienstleistungs- oder Kapitalverkehr berühren (§ 24 Abs. 3 Z 3).

Wesentlich ist, dass es sich bei dieser Bestimmung um eine Legaldefinition handeln soll, die isoliert betrachtet keinen eigenen normativen Gehalt aufweist, zumal Einrichtungen, die lediglich die Voraussetzungen gemäß Abs. 3 erfüllen, per se – ohne Hinzutreten der in Abs. 4 und 5 normierten Voraussetzungen – weder als wesentliche noch als wichtige Einrichtungen gelten sollen.

In Abs. 4 und 5 wird demnach der Sektor der öffentlichen Verwaltung für die Bundes- und die Landesebene konkretisiert.

Für Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene wird in Abs. 4 festgelegt, dass davon nur jene Einrichtungen erfasst werden sollen, die die Voraussetzungen gemäß Abs. 3 erfüllen und zudem zur Besorgung von Angelegenheiten der Bundesverwaltung berufen sind und (alternativ) entweder als Bundesbehörden eingerichtet wurden oder Rechtspersönlichkeit besitzen. Die Voraussetzungen gemäß Abs. 3 und 4 sollen sohin kumulativ vorliegen müssen, damit eine Einstufung als Einrichtung im Sektor der öffentlichen Verwaltung auf Bundesebene erfolgt. Damit werden sowohl organisatorische Bundesbehörden als auch ausgegliederte Rechtsträger mit eigener Rechtspersönlichkeit erfasst, sofern diese zur Besorgung von Angelegenheiten der Bundesverwaltung berufen sind. Um einen einheitlichen und effizienten Vollzug im Bereich des Sektors der öffentlichen Verwaltung auf Bundesebene zu gewährleisten und somit die Prüfung der Registrierung gemäß § 29 Abs. 2 durch die Cybersicherheitsbehörde zu erleichtern, sollen die übrigen Mitglieder der Bundesregierung verpflichtet sein, der Cybersicherheitsbehörde erstmalig innerhalb einer Frist von drei Monaten ab Inkrafttreten dieses Bundesgesetzes und sodann anlassbezogen, wenn diesbezügliche Änderungen (Wegfall von oder Hinzukommen neuer Einrichtungen) eintreten, eine Liste mit den in ihren Wirkungsbereich fallenden Einrichtungen (zB ausgegliederte Rechtsträger) zur Verfügung zu stellen, wobei längstens jedoch alle drei Jahre eine aktualisierte Liste übermittelt werden soll. Wesentlich ist, dass die Verpflichtungen der jeweiligen Einrichtungen gemäß § 29 Abs. 2 bis 4 davon unberührt bleiben sollen.

In Abs. 5 sollen zunächst jene organisatorischen Landesbehörden abschließend aufgelistet werden, die auf Basis einer bereits vorgenommenen risikobasierten Bewertung jedenfalls – dh. unabhängig vom Vorliegen der Voraussetzungen gemäß Abs. 3 – als Einrichtungen im Sektor der öffentlichen Verwaltung auf Landesebene qualifiziert werden sollen und soll es sich dabei um die Ämter der Landesregierungen und die Bezirkshauptmannschaften handeln. Daneben sollen als Einrichtungen im Sektor der öffentlichen Verwaltung auf Landesebene jene Einrichtungen erfasst werden, die zusätzlich zu den Voraussetzungen des Abs. 3 sowohl Rechtspersönlichkeit besitzen als auch zur Besorgung von Angelegenheiten der Landesverwaltung berufen sind. Neben diesen ausdrücklich genannten organisatorischen Landesbehörden sollen somit auch ausgegliederte Einrichtungen erfasst werden, die in Angelegenheiten der Landesverwaltung entsprechend hoheitlich tätig werden (vgl. Abs. 3 Z 3).

Abs. 6 setzt die Ausnahmen für bestimmte staatliche Bereiche vom Anwendungsbereich der NIS-2-Richtlinie um (Art. 2 Abs. 7 und Art. 6 Nr. 35 NIS-2-Richtlinie). Demnach gelten Einrichtungen im Sektor der öffentlichen Verwaltung, deren Wirkungsbereiche überwiegend (vgl. ErwGr 8 NIS-2-Richtlinie) die nationale Sicherheit einschließlich der militärischen Landesverteidigung, die öffentliche Sicherheit oder die Strafverfolgung umfassen, sowie Einrichtungen der Gerichtsbarkeit, einschließlich der kollegialen und monokratischen Justizverwaltung, Einrichtungen der Gesetzgebung, einschließlich der Parlamentsdirektion, der Rechnungshof, der Volksanwaltschaft und die Österreichische Nationalbank nicht als wesentliche oder wichtige Einrichtungen.

ErwGr 8 NIS-2-Richtlinie führt hierzu unter anderem Folgendes aus:

„...Für die Zwecke dieser Richtlinie gelten Einrichtungen mit Regulierungskompetenzen nicht als Einrichtungen, die Tätigkeiten im Bereich der Strafverfolgung ausüben, und sind demnach nicht aus diesem Grunde vom Anwendungsbereich dieser Richtlinie ausgenommen. Einrichtungen der öffentlichen Verwaltung, die gemäß einer internationalen Übereinkunft gemeinsam mit einem Drittland gegründet wurden, sind vom Anwendungsbereich dieser Richtlinie ausgenommen. Diese Richtlinie gilt nicht für diplomatische und konsularische Vertretungen der Mitgliedstaaten in Drittländern oder für deren Netz-

und Informationssysteme, sofern sich diese Systeme in den Räumlichkeiten der Mission befinden oder für Nutzer in einem Drittland betrieben werden.“

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 NIS-2-Richtlinie ergebenden Ausnahme erfasst angesehen werden können. Es soll daher klargestellt werden, dass Angelegenheiten der kollegialen und monokratischen Justizverwaltung sowie der Parlamentsdirektion ebenfalls nicht vom Anwendungsbereich dieses Bundesgesetzes umfasst sind. Ungeachtet dieser Ausnahme gewährleistet die Justiz die Netz- und Informationssystemsicherheit sämtlicher ihrer Einrichtungen (der Gerichtsbarkeit, der Justizverwaltung einschließlich der Zentralleitung und des Straf- und Maßnahmenvollzugs) durch interne Risikoanalysen und Krisenbewältigungsstrategien. Durch den pauschalen Verweis auf den Bereich der Gerichtsbarkeit ergibt sich auch ohne ausdrückliche gesetzliche Anordnung, dass die Ausnahme die Staatsanwaltschaften umfassen soll (vgl. Art. 90a B-VG, wonach Staatsanwälte Organe der Gerichtsbarkeit sind).

Die (optionalen) weiteren Ausnahmen gemäß Art. 2 Abs. 8 NIS-2-Richtlinie wurden aufgrund der fehlenden Anwendungsfälle der ersten Variante und der praktischen Umsetzungshürden für die zweite Variante der leg cit nicht wahrgenommen.

Darüber hinaus sind Einrichtungen des Universitäts-, Hochschul- und Schulwesens vom Anwendungsbereich ausgenommen. Als „Bildungseinrichtungen“ sind diese bereits aus dem Sektor „Forschung“ ausgenommen. Dies ergibt sich aus der Legaldefinition der „Forschungseinrichtung“ in Art. 6 Z 41 NIS-2-Richtlinie, „die [...] Bildungseinrichtungen nicht einschließt“. Der ausdrückliche Ausschluss von Bildungseinrichtungen aus dem Sektor „Forschung“ in der NIS-2-Richtlinie würde konterkariert, wenn diese ohnehin als Einrichtung im Sektor der öffentlichen Verwaltung zu qualifizieren wäre. Daher waren diese ausdrücklich auszunehmen. Von der Möglichkeit des Art. 2 Abs. 5 NIS-2-Richtlinie, Bildungseinrichtungen dennoch in den Anwendungsbereich aufzunehmen, wird kein Gebrauch gemacht.

Die Ausnahmen gemäß Abs. 6 kommen für Vertrauensdiensteanbieter nicht zur Anwendung (vgl. Art. 2 Abs. 9 NIS-2-Richtlinie).

Abs. 7 regelt das Verhältnis dieses Bundesgesetzes gegenüber der Verordnung (EU) Nr. 2022/2554 und der nationalen Durchführungsrechtsakte und ordnet an, dass die dortigen Bestimmungen gegenüber jenen dieses Bundesgesetzes vorgehen („lex specialis“; vgl. Art. 1 Abs. 2 Verordnung (EU) Nr. 2022/2554). Jene Einrichtungen, die gemäß Art. 2 Abs. 4 Verordnung (EU) Nr. 2022/2554 im Rahmen der innerstaatlichen Durchführung von deren Anwendungsbereich ausgenommen wurden, sind vom Anwendungsbereich dieses Bundesgesetzes ausgenommen.

Abs. 8 ordnet an, dass IKT-Drittdienstleister iSd Art. 3 Nr. 23 der Verordnung (EU) Nr. 2022/2554 auch den Bestimmungen dieses Bundesgesetzes unterliegen (Ausnahme von lex-specialis-Regelung gemäß § 24 Abs. 5). Dies bedeutet auch, dass die Aufsicht über IKT-Drittdienstleister (auch) der Cybersicherheitsbehörde obliegt.

Im Sinne eines vollumfänglichen gesamtstaatlichen Ansatzes soll in Abs. 9 mit Blick auf aktuelle Entwicklungen sowie die damit verbundene „Vorbildfunktion“ die Klarstellung erfolgen, dass (auch) der Bundesminister für Inneres, die Bundesministerin für Justiz und der Bundesminister für Landesverteidigung – die in besonders sensiblen „staatlichen“ Bereichen tätig sind – im jeweiligen Wirkungsbereich sowie der Präsident des Nationalrats im Bereich der diesem zustehenden Verwaltungsangelegenheiten (vgl. auch Art. 30 Abs. 3 und 6 B-VG) die notwendigen internen Vorehrungen zu treffen haben und demnach über Strukturen für die Sicherstellung eines hohen Cybersicherheitsniveaus verfügen. Da diese Einrichtungen angesichts der in Art. 2 Abs. 7 NIS-2-Richtlinie vorgesehenen Ausnahmeregelungen (vgl. auch Abs. 6) dem NIS-Regime grundsätzlich nicht unterliegen, sollen folglich auch die Regelungen betreffend die Aufsicht und Durchsetzung sowie Sanktionierung wesentlicher und wichtiger Einrichtungen gemäß den vorgeschlagenen §§ 38 und 39 sowie den §§ 45 und 46 nicht zur Anwendung gelangen.

Zu § 25 (Ermittlung der Unternehmensgröße):

In § 25 wird die Ermittlung der Unternehmensgrößen „mittleres Unternehmen“ und „großes Unternehmen“ beschrieben. Diese erfolgt auf Basis der Empfehlung der Kommission (2003/361/EG) betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl. Nr. L 124 vom 20.05.2003 S. 36 (Empfehlung 2003/361/EG), wie in Art. 2 Abs. 1 NIS-2-Richtlinie vorgesehen. Die in der Empfehlung 2003/361/EG definierten Unternehmensgrößen werden innerstaatlich

in zahlreichen Bundesgesetzen herangezogen und sind als allgemein anerkannte Referenzgrößen anzusehen.

Die Ermittlung der Unternehmensgröße ist aufgrund der in der NIS-2-Richtlinie grundsätzlich geltenden allgemeinen Größenschwelle („size-cap-rule“) für die Einstufung als wesentliche oder wichtige Einrichtung gemäß § 24 von Bedeutung. Andere Unternehmensgrößen als das „mittlere Unternehmen“ oder das „große Unternehmen“ können für die Zwecke dieses Bundesgesetzes außer Acht bleiben. Unternehmen, die weder als großes noch als mittleres Unternehmen gelten, können lediglich dann als wesentliche oder wichtige Einrichtung qualifiziert werden, wenn die jeweilige Art des Unternehmens größenunabhängig als wesentliche oder wichtige Einrichtung gilt (siehe § 24).

Um zu ermitteln, ob ein „großes Unternehmen“ (Abs. 2) oder ein „mittleres Unternehmen“ (Abs. 3) vorliegt, sind folgende Faktoren heranzuziehen: Die Mitarbeiteranzahl, der Jahresumsatz sowie die Jahresbilanz. Diese werden jeweils anhand der Vorgaben in Art. 1 bis 6 (mit Ausnahme des Art. 3 Abs. 4) des Anhangs der Empfehlung 2003/361/EG berechnet.

Die Mitarbeiteranzahl wird in Jahresvollzeitäquivalenten (Art. 5 des Anhangs der Empfehlung 2003/361/EG) berechnet und umfasst

- a) Lohn- und Gehaltsempfänger;
- b) für das Unternehmen tätige Personen, die in einem Unterordnungsverhältnis zu diesem stehen und nach nationalem Recht Arbeitnehmern gleichgestellt sind;
- c) mitarbeitende Eigentümer;
- d) Teilhaber, die eine regelmäßige Tätigkeit in dem Unternehmen ausüben und finanzielle Vorteile aus dem Unternehmen ziehen.

Auszubildende oder in der beruflichen Ausbildung stehende Personen, die einen Lehr- bzw. Berufsausbildungsvertrag haben, sind in der Mitarbeiterzahl nicht berücksichtigt. Die Dauer des Mutterschafts- bzw. Elternurlaubs wird nicht mitgerechnet.

Als „großes Unternehmen“ (Abs. 2) gilt ein Unternehmen jedenfalls, wenn es zumindest 250 Mitarbeiter beschäftigt.

Als „mittleres Unternehmen“ (Abs. 3) gilt ein Unternehmen, wenn es zumindest 50 Mitarbeiter beschäftigt, aber noch nicht die Voraussetzungen eines „großen Unternehmens“ erreicht.

Ebenso kann die Größenschwelle zum mittleren Unternehmen oder zum großen Unternehmen dadurch überschritten werden, dass ein bestimmter Jahresumsatz und eine bestimmte Jahresbilanz erreicht wird.

So gilt ein Unternehmen auch dann als großes Unternehmen, wenn es einen Jahresumsatz von über 50 Millionen Euro erzielt und sich die Jahresbilanz auf über 43 Millionen Euro beläuft.

Sofern ein Unternehmen nicht als großes Unternehmen gilt, ist es ein mittleres Unternehmen, wenn dessen Jahresumsatz über 10 Millionen Euro beträgt und dessen Jahresbilanz sich auf über 10 Millionen Euro beläuft.

Zu beachten ist, dass bei der Berechnung der obigen Werte nicht bloß jene des eigenen Unternehmens, sondern auch jene der mit dem Unternehmen verbundenen Unternehmen und (anteilig) jene der Partnerunternehmen hinzugerechnet werden.

Als verbundene Unternehmen gelten gemäß Art. 3 Abs. 2 des Anhangs der Empfehlung 2003/361/EG Unternehmen, die zueinander in einer der folgenden Beziehungen stehen:

- a) ein Unternehmen hält die Mehrheit der Stimmrechte der Aktionäre oder Gesellschafter eines anderen Unternehmens;
- b) ein Unternehmen ist berechtigt, die Mehrheit der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsgremiums eines anderen Unternehmens zu bestellen oder abzuberufen;
- c) ein Unternehmen ist gemäß einem mit einem anderen Unternehmen abgeschlossenen Vertrag oder aufgrund einer Klausel in dessen Satzung berechtigt, einen beherrschenden Einfluss auf dieses Unternehmen auszuüben;
- d) ein Unternehmen, das Aktionär oder Gesellschafter eines anderen Unternehmens ist, übt gemäß einer mit anderen Aktionären oder Gesellschaftern dieses anderen Unternehmens getroffenen Vereinbarung die alleinige Kontrolle über die Mehrheit der Stimmrechte von dessen Aktionären oder Gesellschaftern aus.

Sofern sich die vorgenannten Investoren nicht direkt oder indirekt in die Verwaltung des betroffenen Unternehmens einmischen – unbeschadet der Rechte, die sie in ihrer Eigenschaft als Aktionäre oder

Gesellschafter besitzen – besteht die Vermutung, dass kein beherrschender Einfluss ausgeübt wird (vgl. Art. 3 Abs. 2 der Empfehlung 2003/361/EG).

Unternehmen, die durch ein oder mehrere andere Unternehmen, oder einem der in Abs. 2 genannten Investoren, untereinander in einer der in Unterabsatz 1 genannten Beziehungen stehen, gelten ebenfalls als verbunden.

Unternehmen, die durch eine natürliche Person oder eine gemeinsam handelnde Gruppe natürlicher Personen miteinander in einer dieser Beziehungen stehen, gelten gleichermaßen als verbundene Unternehmen, sofern diese Unternehmen ganz oder teilweise in demselben Markt oder in benachbarten Märkten tätig sind.

Als benachbarter Markt gilt der Markt für ein Produkt oder eine Dienstleistung, der dem betreffenden Markt unmittelbar vor- oder nachgeschaltet ist.

Als Partnerunternehmen gelten gemäß Art. 3 Abs. 2 des Anhangs der Empfehlung 2003/361/EG alle Unternehmen, die nicht als verbundene Unternehmen gelten und zwischen denen folgende Beziehung besteht:

Ein Unternehmen (das vorgeschaltete Unternehmen) hält – allein oder gemeinsam mit einem oder mehreren verbundenen Unternehmen – 25 % oder mehr des Kapitals oder der Stimmrechte eines anderen Unternehmens (des nachgeschalteten Unternehmens).

Ein Unternehmen gilt jedoch weiterhin als eigenständig, auch wenn der Schwellenwert von 25 % erreicht oder überschritten wird, sofern es sich um folgende Kategorien von Investoren handelt und unter der Bedingung, dass diese Investoren nicht (einzelne oder gemeinsam) mit dem betroffenen Unternehmen verbunden sind:

- a) staatliche Beteiligungsgesellschaften, Risikokapitalgesellschaften, natürliche Personen bzw. Gruppen natürlicher Personen, die regelmäßig im Bereich der Risikokapitalinvestition tätig sind ("Business Angels") und die Eigenmittel in nicht börsennotierte Unternehmen investieren, sofern der Gesamtbetrag der Investition der genannten „Business Angels“ in ein und dasselbe Unternehmen 125 000 EUR nicht überschreitet;
- b) Universitäten oder Forschungszentren ohne Gewinnzweck;
- c) institutionelle Anleger einschließlich regionaler Entwicklungsfonds;
- d) autonome Gebietskörperschaften mit einem Jahreshaushalt von weniger als 10 Millionen Euro und weniger als 5000 Einwohnern.

Die Berechnung der Unternehmensgröße lässt sich anhand folgender Beispiele verdeutlichen:

Beschäftigt ein Unternehmen 70 Mitarbeiter, erzielt jedoch einen Jahresumsatz und eine Jahresbilanz von nur neun Millionen Euro, so ist dieses nach der Empfehlung 2003/361/EG aufgrund der Überschreitung der Mitarbeiteranzahl für Kleinunternehmen als mittleres Unternehmen einzustufen (und unterliegt damit potentiell dem Anwendungsbereich dieses Bundesgesetzes).

Beschäftigt ein Unternehmen 49 Mitarbeiter, erzielt jedoch einen Jahresumsatz und eine Jahresbilanz von 15 Millionen Euro, so ist dieses ebenfalls als mittleres Unternehmen einzustufen, da das Kriterium des Jahresumsatzes und jenes der Jahresbilanz überschritten wird. Sollte entweder der Jahresumsatz oder die Jahresbilanz im vorliegenden Beispiel maximal 10 Millionen Euro betragen, würde jedoch ein Kleinunternehmen vorliegen, da bei diesem – wie oben erwähnt – einer dieser beiden Werte überschritten werden darf.

Ein Großunternehmen ist ein Unternehmen, das zumindest 250 Mitarbeiter beschäftigt oder einen Jahresumsatz von über 50 Millionen Euro erzielt und dessen Jahresbilanz über 43 Millionen Euro übersteigt.

Sieht man sich dies anhand eines Beispiels an, so lässt sich Folgendes feststellen: Ein Unternehmen, welches 260 Mitarbeiter beschäftigt, jedoch unter 10 Millionen Euro umsetzt, ist ein Großunternehmen. Ein Unternehmen, das 249 Mitarbeiter beschäftigt und einen Jahresumsatz von über 50 Millionen Euro erzielt und dessen Jahresbilanz sich auf über 43 Millionen Euro beläuft, ist ebenfalls als Großunternehmen anzusehen.

Die Europäische Union stellt mehr Informationen bezüglich der Kriterien und der Berechnung der Schwellenwerte zur Verfügung, hier kann auf den Benutzerleitfaden zur Definition von KMU verwiesen werden, welcher Einzelheiten und Erläuterungen zur KMU Definition enthält.

In Abs. 4 soll die durch ErwGr 16 der NIS-2-Richtlinie eröffnete Möglichkeit aufgegriffen werden, eine möglicherweise unverhältnismäßige Zusammenrechnung der Daten einer Einrichtung mit jenen ihrer

Partner- und verbundenen Unternehmen bei bestehender „technischer“ Unabhängigkeit der Einrichtung von diesen zu unterbinden.

Zu § 26 (Größenunabhängige Einstufung als wesentliche oder wichtige Einrichtung):

Diese Bestimmung setzt Art. 2 Abs. 2 lit. b bis e NIS-2-Richtlinie um, welche in Zusammenschau mit Art. 3 Abs. 1 lit. e und Abs. 2 NIS-2-Richtlinie zu lesen ist. Demnach sind unabhängig von ihrer Größe auch jene Einrichtungen vom Anwendungsbereich der NIS-2-Richtlinie umfasst, die in einem der Sektoren der Anhänge I oder II der NIS-2-Richtlinie (umgesetzt in den Anlagen 1 und 2 dieses Bundesgesetzes) tätig sind und

1. es sich bei der Einrichtung in einem Mitgliedstaat um den einzigen Anbieter eines Dienstes handelt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist;
2. sich eine Störung des von der Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;
3. eine Störung des von der Einrichtung erbrachten Dienstes zu einem wesentlichen Systemrisiko führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte oder
4. die Einrichtung aufgrund der besonderen Bedeutung, die sie auf nationaler oder regionaler Ebene für den betreffenden Sektor oder die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren in dem Mitgliedstaat hat, kritisch ist.

Aus Art. 3 Abs. 1 lit. e und Abs. 2 NIS-2-Richtlinie ergibt sich, dass Mitgliedstaaten diese Einrichtungen entweder als wichtige Einrichtungen oder als wesentliche Einrichtungen einzustufen haben. Wenngleich das Vorliegen der Gründe für die größerenunabhängige Einstufung (§ 26 Abs. 3; Art. 2 Abs. 2 lit. b bis e NIS-2-Richtlinie) im gebundenen Ermessen der Mitgliedstaaten liegt, ist die Prüfung, ob diese Gründe für bestimmte Einrichtungen vorliegen, durch die Cybersicherheitsbehörde verpflichtend durchzuführen, um den Bestimmungen des Art. 2 Abs. 2 lit. b bis e NIS-2-Richtlinie Geltung zu verschaffen.

Die Einstufung als „kritisch“ gemäß Abs. 3 Z 4 ist vergleichbar mit dem Begriff der „kritischen Infrastruktur“ gemäß § 22 Abs. 1 Z 6 SPG und § 74 Z 11 des Strafgesetzbuches (StGB), BGBl. Nr. 60/1974, zu deuten. Als „Systemrisiko“ (Abs. 3 Z 3) ist ein Risiko zu verstehen, dessen Verwirklichung nicht nur Auswirkung auf die Einrichtung selbst, sondern auch auf andere Einrichtungen (wesentliche, wichtige und auch sonstige Einrichtungen) hat. Ein Beispiel für ein „Systemrisiko“ wäre die Störung einer Einrichtung im Sektor Energie, die aufgrund der hohen Vernetzung innerhalb dieses Sektors in der europäischen Union in der Regel grenzübergreifende Auswirkungen hat.

Zu § 27 (Ausnahmen von Verpflichtungen für wesentliche oder wichtige Einrichtungen aufgrund sektorspezifischer Rechtsakte der Union):

Die Bestimmung überführt Art. 4 NIS-2-Richtlinie in das nationale Recht, der das Verhältnis der NIS-2-Richtlinie (und damit auch deren Umsetzung in das nationale Recht) zu anderen Unionsrechtsakten regelt, die sektorspezifische Cybersicherheitsmaßnahmen vorsehen. Art. 4 NIS-2-Richtlinie regelt, dass in jenen Fällen, in denen wesentliche oder wichtige Einrichtungen gemäß sektorspezifischer Rechtsakte der Union entweder Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder erhebliche Sicherheitsvorfälle melden müssen, die einschlägigen Bestimmungen der NIS-2-Richtlinie, einschließlich der Bestimmungen über Aufsicht und Durchsetzung in Kapitel VII, keine Anwendung auf solche Einrichtungen finden, sofern diese sektorspezifischen Bestimmungen jenen der NIS-2-Richtlinie zumindest gleichwertig sind.

Art. 4 NIS-2-Richtlinie ordnet somit ausdrücklich an, dass speziellere Bestimmungen zu Cybersicherheitsmaßnahmen, die ein zumindest gleichwertiges Cybersicherheitsniveau zu jenen der NIS-2-Richtlinie bewirken, vorgehen (als „lex specialis“). Nach dem Wortlaut des Art. 4 NIS-2-Richtlinie wird nicht ein ganzer Rechtsakt, sondern vielmehr einzelne Bestimmungen aus den sektorspezifischen Rechtsakten vorrangig angewandt.

Dementsprechend soll in Abs. 1 festgelegt werden, dass die Anforderungen gemäß § 32 (Risikomanagementmaßnahmen im Bereich der Cybersicherheit) und § 34 (Berichtspflichten) insoweit (dh. entweder zur Gänze oder teilweise) nicht anwendbar sein sollen, als wesentliche oder wichtige Einrichtungen bereits auf Grund sektorspezifischer Rechtsakte der Union entsprechenden Verpflichtungen unterliegen (Z 1). Wesentlich soll außerdem sein, dass diese Verpflichtungen jenen nach diesem Bundesgesetz gleichwertig sind oder sogar darüber hinausgehen (Z 2).

In Abs. 2 soll in Umsetzung der Regelung in Art. 4 Abs. 2 der NIS-2-Richtlinie festgelegt werden, unter welchen Voraussetzungen die Verpflichtungen der sektorspezifischen unionsrechtlichen Bestimmung als

gleichwertig gelten. Um wesentlichen oder wichtigen Einrichtungen die Beurteilung zu erleichtern, soll die Cybersicherheitsbehörde dazu verpflichtet sein, über die jeweiligen sektorspezifischen Bestimmungen sowie das Ausmaß der Gleichwertigkeit auf der Homepage der Cybersicherheitsbehörde zu informieren. In diesem Zusammenhang wird es angezeigt sein, dass die Cybersicherheitsbehörde die auf Grundlage von Art. 4 Abs. 3 NIS-2-Richtlinie zu erlassenden Leitlinien der Kommission heranzieht.

Zu § 28 (Territorialität):

Die Bestimmung setzt Art. 26 NIS-2-Richtlinie um und regelt den örtlichen Anwendungsbereich dieses Bundesgesetzes.

Art. 26 Abs. 1 NIS-2-Richtlinie sieht grundsätzlich vor, dass Einrichtungen der Zuständigkeit jenes Mitgliedstaats der Europäischen Union unterliegen, in dem sie niedergelassen sind, sofern nicht eine der Ausnahmen der lit. a bis c leg. cit. vorliegt. Das Kriterium der Niederlassung im Sinne dieser Richtlinie setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Zuständigkeit eines jeweiligen Mitgliedstaates der Europäischen Union ist somit nicht exklusiv. Jeder Mitgliedstaat, in dessen Staatsgebiet eine Einrichtung eine Niederlassung betreibt, ist daher für die Einhaltung der Vorgaben der NIS-2-Richtlinie zuständig.

Gemäß Art. 26 Abs. 1 lit. a NIS-2-Richtlinie unterliegen – abweichend von der vorgenannten Grundregel – Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste der Zuständigkeit jenes Mitgliedstaats der Europäischen Union, in dem sie ihre Dienste erbringen. Das Bundesgesetz ist daher gemäß Abs. 2 Z 1 auf diese anwendbar, sofern sie ihre Dienste in Österreich erbringen.

Die Ausnahme des Art. 26 Abs. 1 lit. b und Abs. 2 NIS-2-Richtlinie wird in Abs. 2 Z 2 und Abs. 3 umgesetzt. Für die davon betroffenen sogenannten „grenzübergreifenden Einrichtungen“ („cross-border-entities“) wird – in Abweichung vom Grundsatz der gemeinsamen Zuständigkeit mehrerer Mitgliedstaaten im Fall von mehreren Niederlassungen (Abs. 1) – vorgesehen, dass lediglich ein Mitgliedstaat innerhalb der Europäischen Union zuständig ist, und zwar jener in dem sich die Hauptniederlassung der Einrichtung (dazu unten) befindet.

Zu diesen grenzübergreifenden Einrichtungen zählen DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke.

Hauptniederlassung im Sinne des Abs. 2 Z 2 lit. a ist jene Niederlassung, in der die Entscheidungen im Zusammenhang mit den Risikomanagementmaßnahmen vorwiegend getroffen werden. Nur wenn dies nicht eindeutig bestimmt werden kann oder wenn diese Entscheidungen nicht in der Europäischen Union getroffen werden, so gilt als Hauptniederlassung subsidiär jene Niederlassung, in der die Risikomanagementmaßnahmen ergriffen werden. Kann dies ebenso wenig festgestellt werden (oder liegt diese außerhalb der Union) so gilt die „Hauptniederlassung“ in jenem Mitgliedstaat gelegen, in der die Einrichtung die höchste Beschäftigtenzahl in der Europäischen Union hat.

Die Anschrift der Hauptniederlassung ist von der Einrichtung im Rahmen der Registrierung gemäß § 29 anzugeben.

Sofern eine grenzübergreifende wesentliche oder wichtige Einrichtung gemäß Abs. 2 Z 2 keine Niederlassung in der Europäischen Union hat, jedoch Dienste innerhalb der Union anbietet, hat sie einen Vertreter in der Union zu benennen. Dieser Vertreter muss in einem der Mitgliedstaaten der Europäischen Union niedergelassen sein, in denen die Dienste angeboten werden. Die Einrichtung unterliegt dann der Zuständigkeit jenes Mitgliedstaates, in dem der Vertreter niedergelassen ist. Lediglich in Fällen, in denen kein solcher Vertreter benannt wurde, ist die Zuständigkeit jedes Mitgliedstaates, in dem die Einrichtung Dienste erbringt, eröffnet.

Dies bedeutet, dass eine der vorgenannten „grenzübergreifenden Einrichtungen“ gemäß Abs. 2 Z 2, die keine Niederlassung in der Europäischen Union besitzt (und damit auch keine „Hauptniederlassung“ gemäß Abs. 2 Z 2 lit. a), sofern sie keinen zur Empfangnahme von Dokumenten befugten Vertreter mit Hauptwohnsitz im Inland hat, der Cybersicherheitsbehörde einen Zustellbevollmächtigten gemäß § 9 des Zustellgesetzes (ZustG), BGBl. Nr. 200/1982, namhaft zu machen hat. Dies gilt nur dann, sofern sie einen solchen Vertreter nicht bereits in einem anderen Mitgliedstaat der Europäischen Union benannt hat. (Abs. 4 erster Satz). Wurde kein Zustellbevollmächtigter benannt, gelten für die wesentliche oder wichtige Einrichtung die Bestimmungen nach diesem Hauptstück und die Cybersicherheitsbehörde kann nach dem 4. Abschnitt dieses Hauptstücks vorgehen (Abs. 4 zweiter Satz).

Einrichtungen im Sektor der öffentlichen Verwaltung, unterliegen der Zuständigkeit jenes Mitgliedstaats der Europäischen Union, der sie gegründet hat. Entsprechend sieht Abs. 2 Z 3 für Einrichtungen im Sektor der öffentlichen Verwaltung im Sinne des § 24 Abs. 3 die alleinige Zuständigkeit Österreichs vor, unabhängig von ihrem Niederlassungsort innerhalb der Europäischen Union.

Gemäß Abs. 5 lässt die Benennung eines Vertreters durch eine in Abs. 2 Z 2 genannte Einrichtung rechtliche Schritte, die gegen die Einrichtung selbst eingeleitet werden könnten, unberührt.

Gemäß Abs. 6 kann die Cybersicherheitsbehörde aufgrund von Rechtshilfeersuchen von anderen Mitgliedstaaten der Europäischen Union zu einer in den Abs. 1 und 2 genannten Einrichtung, die in Österreich Dienste anbietet oder ein Netz- und Informationssystem betreibt (im Umfang des Rechtshilfeersuchens) geeignete Aufsichts- und Durchsetzungsmaßnahmen nach diesem Bundesgesetz in Bezug auf die betreffende Einrichtung ergreifen. § 22 gilt in diesem Zusammenhang sinngemäß.

Zu § 29 (Register der Einrichtungen):

Die Bestimmung soll einerseits Art. 3 Abs. 3 und 4 und andererseits Art. 27 NIS-2-Richtlinie umsetzen. Das Register der wesentlichen und wichtigen Einrichtungen sowie der Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, soll der Cybersicherheitsbehörde einen Überblick über die in den Anwendungsbereich des Bundesgesetzes fallenden Einrichtungen verschaffen.

In Abs. 3 soll vorgesehen werden, dass sich die Einrichtungen innerhalb von drei Monaten ab Inkrafttreten dieses Bundesgesetzes bei der Cybersicherheitsbehörde zu registrieren und dabei die in Abs. 2 aufgelisteten Angaben bekanntzugeben haben. Unter den in Z 2 angeführten Kontaktdaten sind beispielsweise Telefonnummern und E-Mail-Adressen zu verstehen. Einrichtungen, die erst nach diesem Zeitpunkt als wesentliche oder wichtige Einrichtungen gelten, sollen sich unverzüglich, jedenfalls aber innerhalb von drei Monaten ab Erfüllung der jeweiligen Voraussetzungen zu registrieren haben. Vorgesehen ist, dass die in Abs. 2 aufgelisteten Angaben der Cybersicherheitsbehörde im elektronischen Weg über einen sicheren Kommunikationskanal strukturiert zu übermitteln sein sollen (vgl. auch die Formulierung gemäß § 16 Abs. 6 des Finanzmarkt-Geldwäschegesetzes – FM-GWG, BGBI. I Nr. 118/2016). Der zu verwendende Kommunikationskanal (zB ein bereitgestelltes Online-Formular) soll wesentlichen und wichtigen Einrichtungen rechtzeitig, beispielsweise durch Veröffentlichung auf einer öffentlich zugänglichen Homepage, zur Kenntnis zu bringen sein. Es könnte allenfalls angedacht werden, eine elektronische Übermittlung über das Unternehmensserviceportal vorzusehen.

Zur Gewährleistung der Aktualität des Registers sollen – in Umsetzung der Regelungen in Art. 3 Abs. 4 UAbs. 2 sowie Art. 27 Abs. 3 NIS-2-Richtlinie – die Einrichtungen gemäß Abs. 4 verpflichtet sein, der Cybersicherheitsbehörde Änderungen hinsichtlich der Angaben zu Namen, Anschrift und Sektor unverzüglich, in jedem Fall aber innerhalb von zwei Wochen ab dem Tag der Änderung, und hinsichtlich der Angaben zu den Mitgliedstaaten, in denen sie Dienste erbringen, zu den IP-Adressbereichen, zur Anschrift der Hauptniederlassung und zu Informationen über die in § 25 angeführten Schwellenwerte unverzüglich, in jedem Fall aber innerhalb von drei Monaten ab dem Tag der Änderung mitzuteilen. In Entsprechung der Bestimmung des Art. 27 Abs. 4 NIS-2-Richtlinie soll die zentrale Anlaufstelle gemäß Abs. 5 die Registerdaten betreffend DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke an die ENISA weiterzuleiten haben.

In Abs. 6 soll das im Rahmen des NISG etablierte Institut der „Kontaktstelle“ aufgrund positiver Erfahrungen im gezielten Informationsaustausch zwischen Behörde und betroffenen Unternehmen weiterbestehen und präzisiert werden. Um auch in einem Vorfallsszenario einen direkten Kommunikationskanal mit der Behörde zu haben, empfiehlt es sich, dass die Kontaktstelle im Rahmen ihrer regulären Geschäfts- bzw. Betriebszeiten auch außerhalb dieser erreichbar ist.

Zu § 30 (Datenbank der Domänennamen-Registrierungsdaten):

Die Bestimmung setzt Art. 28 NIS-2-Richtlinie um, wonach TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, verpflichtet werden sollen, korrekte und vollständige Datenbanken mit Domänennamen-Registrierungsdaten („WHOIS-Daten“) zu führen. Zu diesem Zweck sollen TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, mindestens eine Kontaktmöglichkeit des Domäneninhabers überprüfen. Die Verarbeitung stellt eine rechtliche Verpflichtung im Sinne von Art. 6 Abs. 1 lit. c DSGVO dar. In Abs. 2 werden die Informationen festgelegt, die von den TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, zu speichern sind. Gemäß Abs. 3 haben die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Vorgaben und Verfahren,

einschließlich Überprüfungsverfahren, die die Aktualität der Daten gewährleisten sollen, festzulegen, die sie öffentlich zugänglich zu machen haben. Die TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sind gemäß Abs. 4 weiters verpflichtet, unverzüglich nach der Registrierung eines Domänenamens die nicht personenbezogenen Domänennamen-Registrierungsdaten öffentlich zugänglich zu machen. Berechtigten Zugangsnachfragern, das sind insbesondere die Sicherheitsbehörden, die kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichte sowie CERTs oder CSIRTS, haben TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, im Einklang mit dem Datenschutzrecht, innerhalb von 72 Stunden nach Eingang eines Antrags, Zugang zu den personenbezogenen Daten zu gewähren. Die Verpflichtung zur Überprüfung dieser Anträge muss in verhältnismäßiger Weise ausgelegt werden und ist somit nicht zwangsläufig als Überprüfung jedes einzelnen Antrags zu verstehen, sondern erlaubt auch eine stichprobenartige Überprüfung (Abs. 5). Zur Verringerung des Arbeits- und Verwaltungsaufwandes und zur Vermeidung einer doppelten Erhebung der Daten (soweit technisch möglich), sollen die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, gemäß Abs. 6 angehalten werden, miteinander zusammenzuarbeiten.

Zu § 31 (Governance):

In Umsetzung von Art. 20 NIS-2-Richtlinie soll mit dieser Bestimmung vorgesehen werden, dass Leitungsorgane wesentlicher und wichtiger Einrichtungen die Einhaltung der Risikomanagementmaßnahmen gemäß § 32 sicherzustellen und zu beaufsichtigen haben. Dies soll auch die Aufgabe, entsprechende Richtlinien und Vorgaben (vgl. § 32) zu billigen, umfassen (vgl. Art. 20 Abs. 1 NIS-2-Richtlinie).

Wesentlich ist, dass die Verletzung der Pflichten durch Leitungsorgane keine Verwaltungsstrafe für diese zur Folge haben soll, zumal sich die vorgeschlagenen Verwaltungsstrafen ausschließlich gegen die Einrichtung selbst richten (siehe die Erläuterungen zu § 45). Eine Verletzung der Pflichten durch Leitungsorgane kann jedoch zu einer Schadenersatzpflicht führen, sofern die Voraussetzungen dafür erfüllt sind.

Voraussetzung für jeden Schadenersatzanspruch ist der Eintritt eines Schadens, der rechtswidrig und schulhaft verursacht wurde. Für eine allfällige Haftung ist daher vor allem die Frage relevant, ob das jeweilige Leitungsorgan sorgfaltswidrig gehandelt hat und diese Pflichtwidrigkeit für den eingetretenen Schaden letztlich ursächlich war. Sofern einem Leitungsorgan demnach hinsichtlich der Nichteinhaltung der Pflichten aus dem gegenständlichen Bundesgesetz durch die jeweilige Einrichtung kein Schuldvorwurf gemacht werden kann (zB weil ihm die Einflussmöglichkeiten fehlen oder es bei einem rechtswidrigen Beschluss überstimmt wurde), haftet dieses nicht.

Um der Pflicht nach Abs. 1 nachkommen zu können, sollen sich die Leitungsorgane wesentlicher und wichtiger Einrichtungen die notwendigen Fähigkeiten im Bereich der Cybersicherheit in Form von Schulungen anzueignen haben. Darüber hinaus sollen auch den übrigen Mitarbeitern – abhängig von ihrem jeweiligen Arbeitsbezug mit Netz- und Informationssystemen – von den Einrichtungen regelmäßige Cybersicherheitsschulungen anzubieten sein. Die Einrichtung soll dafür Sorge zu tragen haben, dass ihre Mitarbeiter ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie gegebenenfalls Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste erwerben. Dabei soll es sich in Umsetzung des Art. 21 Abs. 2 lit. g NIS-2-Richtlinie auch gemäß § 32 Abs. 4 lit. g um einen Teilbereich der gebotenen Risikomanagementmaßnahmen handeln.

Zu § 32 (Risikomanagementmaßnahmen im Bereich der Cybersicherheit):

In Art. 21 NIS-2-Richtlinie ist vorgesehen, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen zu ergreifen haben, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

In Umsetzung des Art. 21 NIS-2-Richtlinie soll in Abs. 1 vorgesehen werden, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige Risikomanagementmaßnahmen in technischer, operativer und organisatorischer Hinsicht umzusetzen haben. Diese Risikomanagementmaßnahmen sollen dazu dienen, die Sicherheit der Netz- und Informationssysteme, die für den Betrieb oder die Erbringung ihrer Dienste genutzt werden, sicherzustellen sowie Auswirkungen von Cybersicherheitsvorfällen auf die Nutzer ihrer Dienste und auf andere Dienste bestmöglich zu verhindern. Ein Beispiel für eine Risikomanagementmaßnahme in organisatorischer Hinsicht wäre etwa eine von der jeweiligen Einrichtung intern verabschiedete Richtlinie zur Netzwerksicherheit, die diesbezügliche Prozesse und

Vorgaben definiert, wobei im Fall von Unternehmensgruppen auch angedacht werden könnte, auf die entsprechenden Richtlinien des übergeordneten Unternehmens (etwa der Konzernmutter) zu verweisen bzw. diese für anwendbar zu erklären und diese bei Bedarf allenfalls zu ergänzen oder zu adaptieren (dies soll auch auf Einrichtungen im Sektor der öffentlichen Verwaltung zutreffen). Als Risikomanagementmaßnahme in technischer Hinsicht käme beispielsweise der Einsatz technischer Lösungen in Betracht, etwa Firewalls zur Kontrolle und Sicherung des Übergangs zwischen unterschiedlichen Netzwerkbereichen, und kann die Bereitstellung der für den Betrieb einer solchen technischen Lösung notwendigen fachkundigen Betriebsmannschaft als Beispiel für eine Risikomanagementmaßnahme in operativer Hinsicht angeführt werden.

In Abs. 2 soll klargestellt werden, dass die Risikomanagementmaßnahmen ein dem bestehenden Risiko angemessenes Cybersicherheitsniveau zu gewährleisten haben, wobei der Stand der Technik, gegebenenfalls einschlägige nationale, europäische und internationale Normen, wie insbesondere jene gemäß Art. 2 Nr. 1 der Verordnung (EU) Nr. 1025/2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates, ABl. Nr. L 316 vom 14.11.2012 S. 12, sowie bewährte Verfahren und Methoden im Rahmen der Umsetzung von Risikomanagementmaßnahmen („Best-Practices“) und die von den betroffenen Einrichtungen zu tragenden Kosten zu berücksichtigen sein sollen (vgl. Art. 21 Abs. 1 NIS-2-Richtlinie).

Wesentlich ist, dass den betroffenen Einrichtungen aus der Umsetzung von Risikomanagementmaßnahmen keine unverhältnismäßigen finanziellen und administrativen Belastungen erwachsen sollen, weshalb die Kosten der Umsetzung in einem angemessenen Verhältnis zu den bestehenden Risiken für das jeweils betroffene Netz- und Informationssystem stehen soll.

Vor dem Hintergrund, dass die Anforderungen an die Sicherheit von Netz- und Informationssystemen aufgrund der spezifischen Risikoexposition der Einrichtung nicht für alle Netz- und Informationssysteme der Einrichtung zwingend identisch ausgestaltet werden müssen, wird sich die Beurteilung der Verhältnismäßigkeit von Risikomanagementmaßnahmen an den jeweiligen Gegebenheiten innerhalb einer Einrichtung auszurichten haben und werden daraus allenfalls unterschiedliche Ausprägungen bei der Umsetzung von spezifischen Risikomanagementmaßnahmen abzuleiten sein. Dementsprechend soll in Abs. 3 vorgesehen werden, dass bei der Beurteilung der Verhältnismäßigkeit der Risikomanagementmaßnahmen das Ausmaß der Risikoexposition der jeweiligen Einrichtung sowie ihrer Dienste, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Cybersicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen sind.

Wesentlich ist, dass die umzusetzenden Risikomanagementmaßnahmen auf einem gefahrenübergreifenden Ansatz beruhen, zumal die Gefahren für die Sicherheit von Netz- und Informationssystemen verschiedene Ursachen haben können. Demnach soll in Abs. 4 klargestellt werden, dass die Risikomanagementmaßnahmen auf Grundlage des der NIS-2-Richtlinie zugrundeliegenden „All-Gefahren-Ansatzes“ festzulegen sind, der im Ergebnis darauf abzielt, Netz- und Informationssysteme einschließlich ihres physischen Umfelds vor Cybersicherheitsvorfällen zu schützen. Zu diesem Zweck sollen die Risikomanagementmaßnahmen gewissen Anforderungen entsprechen und sollen – in Umsetzung des Art. 21 Abs. 2 NIS-2-Richtlinie – demonstrativ aufgelistete Mindestinhalte festgelegt werden.

Demzufolge soll bei Festlegung der Risikomanagementmaßnahmen etwa auf die Sicherheit der Lieferketten, einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern (zB Anbieter von Datenspeicherungs- und -verarbeitungsdiensten oder von verwalteten Sicherheitsdiensten oder Softwarehersteller), unter Berücksichtigung der spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter, der Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, sowie der Ergebnisse der gemäß Art. 22 Abs. 1 NIS-2-Richtlinie durchgeföhrten koordinierten Risikobewertungen, Bedacht zu nehmen sein (lit. d), da zuletzt vermehrte Cyberangriffe auf die Netz- und Informationssysteme wesentlicher und wichtiger Einrichtungen durch Ausnutzung von Schwachstellen im Zusammenhang mit Produkten und Diensten Dritter beobachtet werden konnten. Zur Gewährleistung der Sicherheit von Lieferketten ist es daher essenziell, dass etwa (potenzielle) Schwachstellen von unmittelbaren Lieferanten und Anbietern sowie die Gesamtqualität und Widerstandsfähigkeit ihrer Produkte und Dienste mitbedacht werden. Zu diesem Zweck könnte es beispielsweise erforderlich sein, Risiken und Abhängigkeiten, die sich aus den Beziehungen wesentlicher oder wichtiger Einrichtungen zu

einem unmittelbaren Diensteanbieter ergeben, zu identifizieren, zu bewerten und entsprechend zu behandeln, und diese Aspekte auch bei der Auswahl neuer Lieferanten bzw. Anbieter sowie im Rahmen vertraglicher Vereinbarungen entsprechend zu beachten.

In Abs. 5 soll die Ermächtigung der Cybersicherheitsbehörde vorgesehen werden, durch Verordnung nähere Anforderungen an die Risikomanagementmaßnahmen gemäß Abs. 4 festzulegen. Dabei sollen insbesondere die von der Europäischen Kommission auf Grundlage des Art. 21 Abs. 5 NIS-2-Richtlinie hinsichtlich einzelner Sektoren oder bestimmter Arten von Einrichtungen erlassenen Durchführungsrechtsakte zur Festlegung technischer und methodischer Anforderungen an Risikomanagementmaßnahmen auch auf andere Sektoren oder Arten von Einrichtungen – allenfalls unter Berücksichtigung sektorspezifischer Besonderheiten – für anwendbar erklärt werden können, sofern diese auch in Bezug auf in anderen Sektoren tätige Einrichtungen geeignete Maßnahmen beinhalten. In diesem Zusammenhang käme etwa die Durchführungsverordnung (EU) 2024/2690 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltzzustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt, ABl. Nr. L vom 18.10.2024, in Betracht.

Um eine umfassende und zeitgerechte Einbindung der betroffenen Sektoren sicherzustellen, ist mit Blick auf eine effiziente und kohärente Umsetzung der NIS-2-Richtlinie angedacht, diese Verordnung vor Erlassung einem Begutachtungsverfahren zu unterziehen. Auf diese Weise soll der breiten Öffentlichkeit jedenfalls die Möglichkeit zur Stellungnahme gegeben werden, um durch deren Mitwirkung zu sachgerechten Ergebnissen zu gelangen.

Zu § 33 (Nachweis der Wirksamkeit von Risikomanagementmaßnahmen):

Unter Berücksichtigung von Art. 31 Abs. 2 NIS-2-Richtlinie soll durch gegenständliche Regelung ein modulares Prüfsystem in Bezug auf wesentliche und wichtige Einrichtungen etabliert werden, bestehend aus einer sogenannten „Selbstdeklaration“ und den Nachweisen der organisatorischen, operativen sowie technischen Umsetzung von Risikomanagementmaßnahmen gemäß dem vorgeschlagenen § 32. Dieses adaptierte Prüfsystem soll zwar das bisher geltende Prüfsystem nach dem NISG ablösen, aber dessen Grundintention – insbesondere die Heranziehung von qualifizierten nunmehr unabhängigen Stellen als Prüfstellen – und die sich aus dem bisherigen Vollzug ergebenden Erfahrungswerte im Rahmen dieses Bundesgesetzes einfließen lassen.

Mit Abs. 1 soll die Selbstdeklaration als neuer Mechanismus eingeführt werden, demzufolge sowohl wesentliche als auch wichtige Einrichtungen innerhalb einer „festen“ Frist von zwölf Monaten nach Eintritt der Registrierungspflicht gemäß § 29 Abs. 2 – diese beginnt mit dem Zeitpunkt, ab dem die jeweilige Einrichtung die Voraussetzungen einer wesentlichen oder wichtigen Einrichtung erfüllt – gewisse Informationen hinsichtlich umgesetzter Risikomanagementmaßnahmen der Cybersicherheitsbehörde nach deren Vorgaben in strukturierter Form übermitteln sollen. Der Mechanismus der Selbstdeklaration soll der Cybersicherheitsbehörde einen initialen Überblick über den Stand der Umsetzung von Risikomanagementmaßnahmen durch wesentliche und wichtige Einrichtungen bieten und zudem ermöglichen, das Aufsichtssystem der Cybersicherheitsbehörde an die individuellen und sektoralen Gegebenheiten entsprechend risikobasiert anzupassen. Der Schwerpunkt der Informationen soll dabei insbesondere auf den genutzten Netz- und Informationssystemen (zB über eingesetzte Systemkomponenten und die Systemlandschaft der jeweiligen Einrichtung), auf der Sicherheit der Lieferketten (zB über das Umfeld der und den Umgang mit unmittelbaren Dienstleister/n und Anbieter/n der jeweiligen Einrichtung) sowie den individuellen Ergebnissen der für die generelle Umsetzung von Risikomanagementmaßnahmen durch die jeweilige Einrichtung notwendig durchzuführenden Risikoanalyse liegen. Die diesbezüglichen konkreten Inhalte sowie die Art und strukturierte Form der Übermittlung (zB in elektronischer Form wie einem Webformular, einem elektronischen Format oder einer entsprechenden Dokumentenvorlage) sollen durch die Cybersicherheitsbehörde vorgegeben und etwa auf der Internetseite der Cybersicherheitsbehörde verfügbar gemacht werden.

In Abs. 2 soll die Intention des bisherigen Prüfsystems (insbesondere § 17 Abs. 3 NISG) übernommen sowie an die Anforderungen und den Umfang der NIS-2-Richtlinie hinsichtlich der Adressaten angepasst werden. Hierbei soll grundlegend zwischen einem Nachweis der organisatorischen sowie operativen Umsetzung und einem Nachweis der technischen Umsetzung von Risikomanagementmaßnahmen

unterschieden werden, die innerhalb eines gewissen gesetzlich vorgegebenen Zeitraums abhängig vom Zeitpunkt der Aufforderung durch die Cybersicherheitsbehörde zu übermitteln sein sollen.

Der Nachweis der organisatorischen sowie operativen Umsetzung von Risikomanagementmaßnahmen gemäß § 32 soll durch eine von einer unabhängigen Stelle durchgeführte organisatorische Prüfung nach den Vorgaben der Cybersicherheitsbehörde erfolgen. Eine organisatorische Prüfung soll dabei als eine systematische Überprüfung der Struktur, Prozesse, Dokumente (Standards, Sicherheitsrichtlinien, Verfahrensanweisungen) und Verantwortlichkeiten eines Informationssicherheitsmanagementsystems (ISMS) betrachtet werden, die die Wirksamkeit von Risikomanagementmaßnahmen bewertet. Ein Schwerpunkt soll hierbei auf dem Risikomanagementprozess aufgrund seiner Relevanz als Bewertungsgrundlage liegen.

Alternativ zu einer organisatorischen Prüfung kann die jeweilige Einrichtung auch einschlägige gültige Zertifikate als Nachweis der organisatorischen sowie operativen Umsetzung von Risikomanagementmaßnahmen vorlegen. Unter Berücksichtigung von insbesondere Art. 25 NIS-2-Richtlinie sollen diese Zertifikate auf etablierten europäischen und internationalen Normen im Sinne der Verordnung (EU) Nr. 1025/2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates, ABl. Nr. L 316 vom 14.11.2012 S. 12, beruhen und unter den entsprechenden Rahmenbedingungen (zB entsprechend gewählter Scope der Zertifizierung) die Anwendung von solchen einschlägigen Normen, zB jene der ISO 27001-Serie, ermöglichen. Vor dem Hintergrund der qualitativen Unterscheidung zwischen wesentlichen und wichtigen Einrichtungen durch die NIS-2-Richtlinie sollen wesentliche Einrichtungen diesen Nachweis innerhalb von zwei Monaten ab dem Zeitpunkt der Aufforderung durch die Cybersicherheitsbehörde erbringen, wichtige Einrichtungen hingegen innerhalb von zwei Jahren nach Aufforderung durch die Cybersicherheitsbehörde.

Der Nachweis der technischen Umsetzung von Risikomanagementmaßnahmen gemäß § 32 soll durch eine von einer unabhängigen Stelle durchgeführte technische Prüfung nach den Vorgaben der Cybersicherheitsbehörde generell innerhalb von zwei Jahren ab dem Zeitpunkt der Aufforderung durch die Cybersicherheitsbehörde erfolgen. Bei einer technischen Prüfung wird einerseits eine technische Einsichtnahme bzw. Inspektion von Systemkonfigurationen durchgeführt, um die Einhaltung von Härtungsmaßnahmen, Berechtigungsvergaben und des Minimalitätsprinzips sicherzustellen. Andererseits erfolgt sie durch die Durchführung eines Penetrationstests, der Taktiken, Techniken, Verfahren und Werkzeuge realer Angreifer, die als echte Cyberbedrohung empfunden werden, nachbildet und in einem kontrollierten Rahmen auf die produktiven Netz- und Informationssysteme oder auf repräsentative Testsysteme dieser angewendet wird. Der Anwendungsbereich des Penetrationstests ist aus der Risikoanalyse der Einrichtung derart abzuleiten, dass die umfassten Netz- und Informationssysteme und die Intensität ihrer Prüfung die Relevanz in der Erbringung der Dienste der Einrichtung widerspiegelt. Das Szenario eines „Assumed Breach“ (Annahme, dass ein böswilliger Angreifer bereits Zugang zu mindestens einem niederprivilegierten Teilnehmer des internen Netzwerks erlangt hat) wird jedenfalls abgedeckt. Um das Risiko für die Einrichtung zu minimieren und die Effektivität des Penetrationstests zu maximieren, ist ein geeigneter Mix aus „Black“, „Grey“ und „Whitebox“ Testansätzen zu wählen. Ein Penetrationstest dient vor allem zur Aufdeckung von Schwachstellen „in der Breite“ des Systems. Die Ergebnisse (sowie der Umfang und Zeitraum) dieser Überprüfung sind für einen sachverständigen Dritten nachvollziehbar zu dokumentieren. Feststellungen aus den Penetrationstests werden aus Geschäftsrisikosicht bewertet. Die Bewertung und eine abgeleitete Maßnahmenbehandlung zu den einzelnen Feststellungen werden mindestens bei mittlerer bis sehr hoher Kritikalität in Bezug auf die Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit dokumentiert.

Sowohl organisatorische als auch technische Prüfungen bzw. deren Ergebnisse sollen dabei nicht länger als zwei Jahre zurückliegen dürfen, um eine gewisse Aktualität der Feststellungen gewährleisten zu können.

Zudem soll die Unterscheidung der Intensität der Aufsicht über wesentliche und wichtige Einrichtungen entsprechend abgebildet werden (vgl. ErwGr. 122 zur NIS-2-Richtlinie sowie Art. 31 Abs. 1 NIS-2-Richtlinie). Demnach soll gegenüber wichtigen Einrichtungen – ähnlich wie bei den sonstigen Aufsichts- und Durchsetzungsmaßnahmen gemäß dem vorgeschlagenen § 38 Abs. 2 – nur dann eine Aufforderung durch die Cybersicherheitsbehörde möglich sein, wenn diese Informationen oder Hinweise erlangt, die einen Gesetzesverstoß der jeweiligen Einrichtung nahelegen, womit eine anlassbezogene Ex-post-Aufsicht über wichtige Einrichtungen etabliert werden soll. Im Gegensatz dazu sieht die NIS-2-Richtlinie hinsichtlich wesentlicher Einrichtungen grundsätzlich eine von Anlassfällen unabhängige Ex-ante-

Aufsicht vor, weshalb diese jederzeit von der Cybersicherheitsbehörde dazu aufgefordert werden können sollen, einen entsprechenden Nachweis zu erbringen.

Wesentlich ist, dass die erstmalige Aufforderung zum Nachweis einer organisatorischen, operativen oder technischen Umsetzung von Risikomanagementmaßnahmen durch die Cybersicherheitsbehörde sowohl in Bezug auf wesentliche als auch wichtige Einrichtungen erstmalig nach Ablauf von zwei Jahren ab Inkrafttreten dieses Bundesgesetzes zulässig sein soll, um insbesondere die Modularität des Prüfsystems mit initialer Selbstdeklaration zu unterstreichen.

Wesentlich ist, dass gesetzlich kein bestimmter Prüfzyklus vorgesehen werden soll, sondern soll die Cybersicherheitsbehörde befugt sein, wesentliche Einrichtungen in regelmäßigen an die Bedrohungslage angepassten Abständen zu Prüfungen aufzufordern. Diese Systematik soll industrie- bzw. branchenübliche Prüfzyklen berücksichtigen und den Einrichtungen Flexibilität bei der Planung von Audits ermöglichen. Zudem soll damit die geforderte Regelmäßigkeit von „Sicherheitsprüfungen“ („security audits“) gemäß Art. 32 Abs. 2 lit. b NIS-2-Richtlinie abgebildet und durch die Berücksichtigung der Bedrohungslage auch der in Art. 31 Abs. 2 NIS-2-Richtlinie vorgesehene risikobasierte Ansatz sichergestellt werden.

Über eine Prüfung durch eine unabhängige Stelle nach Abs. 2 soll gemäß Abs. 3 ein für Sachkundige nachvollziehbarer, die Prüfhandlungen und Prüfergebnisse dokumentierender Prüfbericht verfasst werden. In diesem soll vor allem dargestellt werden, ob und inwieweit Risikomanagementmaßnahmen von der jeweiligen wesentlichen oder wichtigen Einrichtung umgesetzt wurden und wirksam sind. Bei allenfalls festgestellten Mängeln soll in einem Maßnahmenplan auch auf deren zukünftige Behebung einzugehen sein. Ein solcher Maßnahmenplan hat sich schon im Rahmen des Vollzugs des NISG bewährt und kann der Cybersicherheitsbehörde insbesondere beim weiteren Vorgehen im Zusammenhang mit anderen ihr zur Verfügung stehenden Aufsichts- und Durchsetzungsmaßnahmen als Orientierung dienen. Wesentlich ist, dass die Cybersicherheitsbehörde an das Ergebnis einer Prüfung durch unabhängige Prüfer nicht gebunden sein soll, sondern die Prüfung im Rahmen der Überprüfung der umgesetzten Risikomanagementmaßnahmen als Teil ihrer Entscheidungsgrundlage der freien Beweiswürdigung unterliegen. Die abschließende Beurteilung der gemäß § 32 umgesetzten Risikomanagementmaßnahmen soll demnach allein der zuständigen Cybersicherheitsbehörde obliegen. Um einer der Stoßrichtungen der NIS-2-Richtlinie zu entsprechen und demnach Kenntnis über die aktuellen Verhältnisse und etwaige Mängel im Bereich der Cybersicherheit einer wesentlichen oder wichtigen Einrichtung auch in deren höchsten Entscheidungsebenen zu schaffen und auch aufgrund gängiger Praxis in anderen Prüfregimen, etwa im Bereich der Wirtschaftsprüfung, soll ein Prüfbericht auf Seiten der jeweiligen Einrichtung durch die Leitungsorgane (vgl. die in § 3 Z 11 vorgeschlagene Begriffsdefinition) zu unterzeichnen sein. Ebenfalls aufgrund gängiger Praxis und aus Gründen der Nachvollziehbarkeit soll auf Seiten der jeweiligen unabhängigen Stelle der Prüfbericht von den jeweiligen unabhängigen Prüfern zu unterzeichnen sein. Konkretere Form- und Inhaltserfordernisse bezüglich eines Prüfberichts sowie Einzelheiten zu dessen Übermittlung sollen sich aus Vorgaben und etwa Formularen auf der Internetseite der Cybersicherheitsbehörde ergeben.

Mit Abs. 4 soll Art. 32 Abs. 2 UAbs. 3 zweiter Satz bzw. Art. 33 Abs. 2 UAbs. 3 zweiter Satz NIS-2-Richtlinie umgesetzt werden, wonach die Kosten von Prüfungen durch unabhängige Stellen von der geprüften Einrichtung zu tragen sind, es sei denn, die Cybersicherheitsbehörde trafe in hinreichend begründeten Fällen amtswegig eine anderslautende Entscheidung.

Mit der in Abs. 5 festgelegten Verpflichtung von wesentlichen und wichtigen Einrichtungen, Prüfpläne einen Monat vor der jeweils geplanten Prüfung an die Behörde zu übermitteln, soll die Möglichkeit geschaffen werden, dass während einer Prüfung einer wesentlichen oder wichtigen Einrichtung durch einen unabhängigen Prüfer von Mitarbeitern der Cybersicherheitsbehörde sogenannte „Witness-Audits“ (Beobachtungsaudits) durchgeführt werden. So soll sichergestellt werden, dass Prüfungen mit der nötigen Qualität durchgeführt werden können und die Eignung der jeweiligen unabhängigen Prüfer auch im Hinblick auf § 7 Abs. 3 Z 2 laufend kontrolliert werden kann. Auch soll die Behörde dadurch einen generellen Überblick erlangen können, welche Einrichtungen jeweils aktuell durch unabhängige Stellen geprüft werden. Konkrete Vorgaben bezüglich der Übermittlung und Anforderungen an Inhalt und Form eines solchen Prüfplans sollen etwa auf der Internetseite der Cybersicherheitsbehörde verfügbar gemacht werden.

Zu § 34 (Berichtspflichten):

Mit dieser Bestimmung wird Art. 23 NIS-2-Richtlinie (mit Ausnahme von dessen Abs. 3; siehe § 35) umgesetzt.

Abs. 1 regelt die grundsätzliche Pflicht wesentlicher und wichtiger Einrichtungen dem für sie zuständigen sektorenpezifischen CSIRT oder den für sie zuständigen sektorspezifischen CSIRTS, in Ermangelung

eines solchen an das nationale CSIRT, unverzüglich jeden erheblichen Cybersicherheitsvorfall (§ 35) zu melden. Das CSIRT hat die Meldung unverzüglich an die Cybersicherheitsbehörde weiterzuleiten. Die unverzügliche Meldung setzt die technische Erreichbarkeit der Meldesysteme voraus. Eine Meldung kann daher nur dann unverzüglich erfolgen, sofern dies aus technischen Gegebenheiten möglich ist.

Der Inhalt der Meldung über einen erheblichen Sicherheitsvorfall wird in Abs. 2 geregelt. Dabei wird zwischen einer ersten Frühwarnung, der Meldung, dem Zwischenbericht und dem Abschlussbericht (bzw. Fortschrittsbericht) unterschieden. Die Frühwarnung (Z 1) hat unverzüglich, spätestens jedoch innerhalb von 24 Stunden zu erfolgen. Die Meldung (Z 2) hat ebenfalls unverzüglich, spätestens jedoch innerhalb von 72 Stunden zu erfolgen (mit Ausnahme von Vertrauensdiensteanbietern, für die auch hier die maximale Frist von 24 Stunden gilt). Zwischenberichte (Z 3) sind auf Ersuchen des CSIRTs ebenfalls unverzüglich zu erbringen (allerdings ohne statischer maximaler Frist). Der Abschlussbericht (Z 4) ist spätestens ein Monat nach der Meldung gemäß Z 2 zu übermitteln. Soweit der Cybersicherheitsvorfall zum Zeitpunkt der Fälligkeit der Vorlage des Abschlussberichts gemäß Z 4 noch andauert, haben die betreffenden Einrichtungen bis zu diesem Zeitpunkt einen Fortschrittsbericht zu übermitteln, wobei der Abschlussbericht bis spätestens ein Monat nach Beendigung der Vorfallsbehandlung übermittelt werden muss (Z 5).

Die Frühwarnung soll lediglich die Informationen enthalten, die erforderlich sind, um das CSIRT über den Sicherheitsvorfall zu unterrichten und es der betreffenden Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. Gegebenenfalls soll in der Frühwarnung angegeben werden, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall durch rechtswidrige oder böswillige Handlungen verursacht wurde oder ob diese grenzüberschreitende Auswirkungen hat. Die Verpflichtung zur Übermittlung der Frühwarnung oder die anschließende Meldung eines Sicherheitsvorfallen soll nicht dazu führen, dass die meldende Einrichtung die Ressourcen von Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen – was vorrangig behandelt werden sollte – umlenken müssen, um zu verhindern, dass die Verpflichtung zur Meldung von Sicherheitsvorfällen entweder dazu führt, das Ressourcen für die Bewältigung erheblicher Sicherheitsvorfälle umgelenkt oder die diesbezüglichen Maßnahmen der Einrichtungen auf andere Weise beeinträchtigt werden.

Mit Abs. 3 wird die Unterrichtung der Empfänger der Dienste durch die wesentliche oder wichtige Einrichtung geregelt (Art. 23 Abs. 1 zweiter Satz NIS-2-Richtlinie).

Mit Abs. 4 wird Abs. 23 Abs. 5 NIS-2-Richtlinie umgesetzt. Demnach übermittelt das CSIRT der meldenden Einrichtung unverzüglich (spätestens 24 Stunden nach Eingang der Frühwarnung) eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Cybersicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operative Beratung für die Durchführung möglicher Abhilfemaßnahmen. Ferner leistet das CSIRT der betreffenden Einrichtung auf Ersuchen zusätzliche technische Unterstützung. Darüber hinaus gibt das CSIRT, sofern bei dem erheblichen Cybersicherheitsvorfall ein krimineller Hintergrund vermutet wird, Orientierungshilfen für die Meldung des Cybersicherheitsvorfalls an die Strafverfolgungsbehörden.

Mit Abs. 5 wird Art. 23 Abs. 6 NIS-2-Richtlinie umgesetzt. Demnach unterrichtet die Cybersicherheitsbehörde im Wege der zentralen Anlaufstelle unverzüglich die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten der Europäischen Union und ENISA über den erheblichen Cybersicherheitsvorfall, sofern dieser zwei oder mehr Mitgliedstaaten betrifft. Dies stellt auch einen Fall des Cybersicherheitsvorfalls großen Ausmaßes (§ 3 Z 31) dar. Darüber hinaus definiert Abs. 5 den Inhalt dieser Mitteilung, wonach diese die gemäß Abs. 2 erhaltenen Informationen zu enthalten hat.

Mit Abs. 6 wird Art. 23 Abs. 7 NIS-2-Richtlinie umgesetzt. Demnach kann die Cybersicherheitsbehörde – nach Anhörung der von einem erheblichen Cybersicherheitsvorfall betroffenen Einrichtungen – personenbezogene Daten gemäß den §§ 42 und 43 nach erfolgter Interessenabwägung bezüglich der Auswirkungen auf die Betroffenen zu dem Zweck veröffentlichen, die Öffentlichkeit über erhebliche Cybersicherheitsvorfälle zu unterrichten. Dies setzt voraus, dass die Sensibilisierung der Öffentlichkeit zur Verhütung oder zur Bewältigung von erheblichen Cybersicherheitsvorfällen erforderlich ist, oder die Offenlegung des erheblichen Cybersicherheitsvorfalls auf sonstige Weise im (überwiegenden) öffentlichen Interesse liegt. Im Hinblick der Veröffentlichung ist darauf zu achten, dass es nur zur Veröffentlichung jener personenbezogenen Daten kommt, die für den Zweck der Auswirkungen auf die Betroffenen erforderlich sind. Bei der Abwägung ist auf den Verhältnismäßigkeitsgrundsatz gemäß § 1 Abs. 2 DSG und den Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO Bedacht zu nehmen.

Mit Abs. 7 wird Art. 23 Abs. 10 NIS-2-Richtlinie umgesetzt. Demnach hat die Cybersicherheitsbehörde jener Behörde, die in Umsetzung des Art. 9 Richtlinie (EU) 2022/2557 national als zuständige Behörde benannt oder eingerichtet wurde, Informationen über erhebliche Cybersicherheitsvorfälle, erhebliche

Cyberbedrohungen und Beinahe-Cybersicherheitsvorfälle zur Verfügung zu stellen, die nach Abs. 1 von Einrichtungen, die im Sinne der Richtlinie (EU) 2022/2557 als kritische Einrichtungen gelten, gemeldet wurden. Dies gilt auch für freiwillige Meldungen gemäß § 37, die von diesen Einrichtungen ergangen sind.

Angesichts der Relevanz von Netz- und Informationssystemen wesentlicher und wichtiger Einrichtungen für wichtige gesellschaftliche und wirtschaftliche Funktionen ist ein umfassender Informationsfluss zum Bundesminister für Inneres insbesondere in Anbetracht seiner politischen und rechtlichen Letztverantwortung als zuständiges oberstes Organ essenziell. Vor diesem Hintergrund soll gemäß Abs. 9 eine halbjährliche Berichtspflicht der Cybersicherheitsbehörde im Hinblick auf eingetretene erhebliche Cybersicherheitsvorfälle vorgesehen werden, die auch jene Informationen umfassen soll, die gemäß den Abs. 1, 5, 7 und 8, gemäß § 8a Abs. 3 GTelG 2012 sowie gemäß § 37 zur Verfügung gestellt wurden. Wesentlich ist, dass diese Informationen im Sinne einer starken Einbindung des Gesetzgebers und zur Sicherstellung einer umfassenden Transparenz sodann vom Bundesminister für Inneres (als zuständiges oberstes Organ) an den National- sowie Bundesrat übermittelt werden sollen (vgl. dazu die Erläuterungen zu § 4 Abs. 3).

Zu § 35 (Erheblicher Cybersicherheitsvorfall):

Mit dieser Bestimmung wird Art. 23 Abs. 3 NIS-2-Richtlinie umgesetzt und präzisiert, wann ein Cybersicherheitsvorfall als gemäß § 34 meldepflichtiger „erheblicher Cybersicherheitsvorfall“ einzustufen ist.

Gemäß Art. 23 Abs. 3 NIS-2-Richtlinie gilt ein Cybersicherheitsvorfall als erheblich, wenn dieser

1. schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder
2. andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Dieser Grundsatz, gemeinsam mit den in ErwGr 101 der NIS-2-Richtlinie genannten Kriterien wird in Abs. 1 festgeschrieben.

Die in Abs. 2 genannten und bei Beurteilung der Erheblichkeit zu berücksichtigenden Kriterien sind jenen Kriterien nachempfunden, die bereits für die Beurteilung eines „Sicherheitsvorfalls“ nach dem NISG idF BGBI. I Nr. 111/2018 (§ 3 Z 6) zu berücksichtigen waren. Demnach sind bei der Beurteilung der Erheblichkeit von Cybersicherheitsvorfällen die betroffenen Netz- und Informationssysteme und deren Bedeutung für die Erbringung der nach Art der jeweiligen wesentlichen oder wichtigen Einrichtung gemäß § 24 in Verbindung mit Anlage 1 und 2 erbrachten Dienste (z. B. Dienste, die sich aufgrund der Art. Verteilernetzbetreiber [Elektrizität] erbracht werden), die Schwere und die technischen Merkmale der Cyberbedrohung und sämtliche zugrundeliegende Schwachstellen, die ausgenutzt werden, sowie die Erfahrungen der Einrichtung mit ähnlichen Vorfällen zu berücksichtigen. Zusätzlich sind darüber hinaus stets unternehmens- und sektorspezifische Faktoren zu berücksichtigen, sofern solche vorliegen.

Die Cybersicherheitsbehörde kann gemäß Abs. 3 mit Verordnung weitere Kriterien und nähere Regelungen zu Abs. 2 für das Vorliegen eines erheblichen Cybersicherheitsvorfalls festlegen. Dabei können sektorspezifische Faktoren berücksichtigt werden. Diese Spezifizierung durch Verordnung orientiert sich an den jeweiligen aktuellen tatsächlichen Gegebenheiten. Dies kann unter anderem auch eine Änderung der Rechtsansichten der Mitgliedstaaten über die Erheblichkeit von Sicherheitsvorfällen (für bestimmte Sektoren) umfassen.

Zu § 36 (Vereinbarungen über den Austausch von Informationen zur Cybersicherheit):

Mit dieser Bestimmung wird Art. 29 NIS-2-Richtlinie umgesetzt. Wesentliche und wichtige Einrichtungen sowie Einrichtungen, die nicht in den Anwendungsbereich des Bundesgesetzes fallen, sollen gemäß Abs. 1 zur Verhinderung, Aufdeckung und Bewältigung von Cybersicherheitsvorfällen (Z 1) sowie zur Erhöhung des Cybersicherheitsniveaus (Z 2) relevante Informationen austauschen können. Bei diesen Informationen kann es sich beispielsweise um Schwachstellen oder Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten oder um Cybersicherheitswarnungen handeln.

Der Austausch solcher Informationen, bei denen es sich notwendigerweise auch um sensible Informationen handeln kann, hat gemäß Abs. 2 auf der Grundlage von Vereinbarungen zu erfolgen, bei deren Ausarbeitung die Cybersicherheitsbehörde die Einrichtungen auf deren Wunsch gemäß Abs. 3 zu unterstützen hat. Wesentliche und wichtige Einrichtungen haben gemäß Abs. 4 die Cybersicherheitsbehörde über den Abschluss bzw. den Rücktritt von Vereinbarungen zu unterrichten, um die Nachvollziehbarkeit dieses Informationsaustausches zu gewährleisten.

Zu § 37 (Freiwillige Meldung relevanter Informationen):

Mit dieser Bestimmung wird Art. 30 NIS-2-Richtlinie umgesetzt. Einrichtungen der Sektoren nach Anlage 1 und 2 sollen die Möglichkeit haben, an das für sie zuständige sektorale CSIRT, in Ermangelung eines solchen an das nationale CSIRT, Cybersicherheitsvorfälle, Cyberbedrohungen und Beinahe-Cybersicherheitsvorfälle freiwillig melden zu können (Abs. 1). Einrichtungen, die nicht in den Anwendungsbereich dieses Bundesgesetzes fallen, können ebenso mit Cybersicherheitsvorfällen, Cyberbedrohungen und Beinahe-Cybersicherheitsvorfällen konfrontiert sein. Die freiwillige Meldung solcher Risiken sollte im öffentlichen Interesse auf freiwilliger Basis ebenfalls möglich sein, da sie für ein gesamtstaatliches und vollständiges Lagebild essentiell ist (Abs. 2). Zuständig für jene Einrichtungen, die nicht in den Anwendungsbereich fallen, ist das das nationale CSIRT.

Der Meldeweg unterscheidet sich nicht von jenem für eine verpflichtende Meldung. Auch freiwillige Meldungen ergehen direkt an das zuständige CSIRT, welches diese zusammenfasst und an die Cybersicherheitsbehörde weiterleitet. Diese Weiterleitung hat allerdings nicht unverzüglich zu erfolgen, sondern kann etwa auch erst mit einer gewissen zeitlichen Verzögerung und zusammengefasst mit anderen gleichartigen Meldungen erfolgen. Die Nennung der Identität der freiwillig meldenden Einrichtung kann dabei auf Verlangen entfallen.

Die freiwillige Meldung kann Angaben zum Risiko oder der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zum Sektor der Einrichtung enthalten. Da der Inhalt von freiwilligen Meldungen für ein gesamtstaatliches und vollständiges Lagebild einen unerlässlichen Bestandteil bildet, sollen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen die Kontakt- und Identitätsdaten der meldenden Einrichtung sowie technische Daten von Personen, die mit einer Meldung zu einem Risiko, Vorfall oder Cybersicherheitsvorfall in Zusammenhang stehen, an das zuständige CSIRT übermittelt werden können.

Zu § 38 (Aufsichtsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen):

Mit dieser Bestimmung sollen die Art. 32 und 33 NIS-2-Richtlinie derart umgesetzt werden, dass die darin angeführten Aufsichtsmaßnahmen und diese betreffenden Vorgaben in Bezug auf wesentliche und wichtige Einrichtungen zur besseren Verständlichkeit für den Normunterworfenen in einer Bestimmung zusammengefasst werden. Neben der in § 33 (Nachweis der Wirksamkeit von Risikomanagementmaßnahmen) festgelegten Vorgehensweise werden in den Abs. 1 und 2 jene Aufsichtsmaßnahmen angeführt, welche der Cybersicherheitsbehörde ermöglichen sollen, die Einhaltung der sich aus dem Bundesgesetz ergebenden Verpflichtungen möglichst effektiv und ohne unverhältnismäßige Eingriffe zu beaufsichtigen. Wesentlich ist in diesem Zusammenhang die Unterscheidung zwischen wesentlichen und wichtigen Einrichtungen:

Während die aufgezählten Maßnahmen bezüglich wesentlicher Einrichtungen jederzeit vorgenommen werden können, darf sie die Cybersicherheitsbehörde hinsichtlich wichtiger Einrichtungen nur dann ergreifen, wenn sie durch Nachweise oder sonstige Hinweise und Informationen davon Kenntnis erlangt, dass eine wichtige Einrichtung mutmaßlich ihren Verpflichtungen nach diesem Bundesgesetz nicht nachkommt. Ein diesbezüglicher Nachweis kann beispielsweise die Selbstdeklaration gemäß § 33 Abs. 1 darstellen. Die angeführten Hinweise oder Informationen könnten beispielsweise der Cybersicherheitsbehörde von anderen Behörden, Einrichtungen, Bürgern oder Medien zur Verfügung gestellt werden oder aus anderen Quellen oder öffentlich zugänglichen Informationen herrühren oder sich aus anderen Tätigkeiten der Cybersicherheitsbehörde bei der Wahrnehmung ihrer Aufgaben ergeben.

Im Rahmen der in Abs. 1 Z 1 geregelten Aufsichtsmaßnahme ist die Cybersicherheitsbehörde nach vorangegangener Verständigung der betreffenden Einrichtung befugt, Kontrollen bei wesentlichen und wichtigen Einrichtungen hinsichtlich der Einhaltung der Risikomanagementmaßnahmen gemäß § 32 durchzuführen. Dabei kann die Cybersicherheitsbehörde vor Ort oder aus der Ferne Einschau bzw. Einsicht in Netz- und Informationssysteme sowie relevante Unterlagen nehmen. Außerdem ist die Cybersicherheitsbehörde befugt, unabhängige Stellen bei ihren Prüfhandlungen im Rahmen von Prüfungen bei wesentlichen oder wichtigen Einrichtungen zu begleiten („Witnessaudits“). Dies ist ein wichtiges Instrument, mit dem die Einhaltung der Verpflichtungen durch die jeweils kontrollierte Einrichtung durch die Cybersicherheitsbehörde beurteilt werden kann.

Die Cybersicherheitsbehörde ist zudem befugt, bei wesentlichen und wichtigen Einrichtungen Sicherheitsscans durchzuführen. Das sind beispielsweise proaktive, nicht intrusive Überprüfungen öffentlich zugänglicher Netz- und Informationssysteme. Dabei hat die Cybersicherheitsbehörde von Maßnahmen Abstand zu nehmen, die sich in negativer Weise auf deren jeweilige Netz- und Informationssysteme auswirken könnten (Abs. 1 Z 2). Von einer wesentlichen oder wichtigen Einrichtung eingerichtete Sicherheitsmaßnahmen, wie beispielsweise die Einrichtung von Firewalls, stellen in diesem

Zusammenhang keine Be- oder Verhinderung der Durchführung der Kontrolle im Sinne des § 45 Abs. 4 Z 12 dar.

Die Cybersicherheitsbehörde ist ebenfalls befugt, von wesentlichen und wichtigen Einrichtungen jene Informationen anzufordern, die es ihr erlauben, die Einhaltung bzw. Erfüllung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen überprüfen zu können. Als Informationen können unter anderem Unterlagen zu Vorgaben und Prozessen (zB Richtlinien), Unterlagen und Protokolle zu operativen Vorgängen (zB Protokolle durchgeföhrter Wartungstätigkeiten) aber auch technische Detailinformationen (zB Netzwerklogs) verstanden werden (Abs. 1 Z 3).

Darüber hinaus kann die Cybersicherheitsbehörde von wesentlichen und wichtigen Einrichtungen sämtliche weitere relevanten Informationen anfordern, die zur Erfüllung ihrer Aufsichtsaufgaben erforderlich sind. Dies können beispielsweise Informationen zu geplanten Umsetzungen im Bereich der Risikomanagementmaßnahmen sein (Abs. 1 Z 4). Davon ausgeschlossen sind mandantenabhängige Daten – sowohl Stamm als auch Bewegungsdaten – die im jeweiligen Geschäftsfeld verarbeitet werden. Soweit personenbezogene Daten betroffen sind, ist darauf hinzuweisen, dass entsprechend dem in Art. 5 Abs. 1 lit. b DSGVO festgelegten Zweckbindungsgrundsatz und dem in Art. 5 Abs. 1 lit. c DSGVO festgelegten Datenminimierungsgrundsatz nur solche Daten angefordert werden dürfen, die unmittelbar zur Wahrnehmung der Aufgaben der Cybersicherheitsbehörde erforderlich und für den Zweck angemessen und erheblich sind.

Gegenüber wesentlichen Einrichtungen ist die Cybersicherheitsbehörde zudem explizit befugt, Ad-hoc-Prüfungen, insbesondere, wenn dies aufgrund eines erheblichen Cybersicherheitsvorfalls oder eines anderwärtigen Verstoßes gegen dieses Bundesgesetz, oder zur Überprüfung der Selbstdeklaration gemäß § 33 Abs. 1 notwendig erscheint, durchzuführen (Abs. 1 Z 5).

Zu § 39 (Durchsetzungsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen):

Mit dieser Bestimmung werden die Art. 32 und 33 NIS-2-Richtlinie umgesetzt. Die dort vorgesehenen Durchsetzungsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen werden zur besseren Verständlichkeit für den Normunterworfenen in einer Bestimmung zusammengefasst. Die in der Richtlinie vorgesehenen Maßnahmen werden dabei adaptiert und zusammengefasst, sodass sowohl die Anforderungen der NIS-2-Richtlinie erfüllt als auch die bisherige Vorgangsweise nach dem NISG (Verstoß – Aufforderung – Bescheid und in weiterer Folge allenfalls Sachverhaltsdarstellungen an die Bezirksverwaltungsbehörde) im Wesentlichen weitergeführt wird.

Wird der Cybersicherheitsbehörde im Zuge ihrer Aufsicht erkennbar, dass eine wesentliche oder wichtige Einrichtung ihren Verpflichtungen nach diesem Bundesgesetz nicht nachkommt, hat diese entsprechend der in Abs. 1 bis 4 vorgesehenen Maßnahmen vorzugehen.

Erforderlichenfalls können dabei aber auch angemessene Fristen in Form einer Aufforderung gesetzt werden. Wird einer solchen Aufforderung nicht nachgekommen, hat dies zur Folge, dass die jeweils angeordnete Maßnahme, wie etwa die (vollständige) Umsetzung jeweiliger Risikomanagementmaßnahmen durch die Cybersicherheitsbehörde mit Bescheid gemäß Abs. 2 angeordnet wird.

Die Cybersicherheitsbehörde ist neben dieser Aufforderung etwa von Risikomanagementmaßnahmen dazu befugt, die betreffende Einrichtung aufzufordern, die Nutzer ihrer Dienste und Tätigkeiten (zB ihre Kunden) über eine Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen gegen ebendiese zu verständigen oder die Öffentlichkeit über Aspekte ihres Verstoßes gegen dieses Bundesgesetz zu unterrichten (Abs. 3 Z 1).

Gegenüber wesentlichen Einrichtungen ist die Cybersicherheitsbehörde darüber hinaus befugt, für eine bestimmte Zeit einen Überwachungsbeauftragten für eine wesentliche Einrichtung zu ernennen, der die Umsetzung der Maßnahmen nach Abs. 2 in der jeweiligen Einrichtung sicherstellen soll. Dieser Überwachungsbeauftragte hat ein Mitarbeiter der Cybersicherheitsbehörde zu sein und dessen Aufgaben können beispielsweise die Teilnahme an internen Terminen und Sitzungen der Einrichtung, die Einsicht in Informationen und Dokumente der Einrichtung oder auch die technische Einsicht in Netz- und Informationssysteme umfassen, immer auf jenen Umfang beschränkt, der im Rahmen der Überwachung der mit Bescheid angeordneten Maßnahmen – wie etwa Umsetzungen und Adaptierungen im Bereich der Risikomanagementmaßnahmen und Berichtspflichten – unbedingt erforderlich ist (Abs. 3 Z 2).

Sollte eine wesentliche Einrichtung dem Bescheid nach Abs. 2 innerhalb der angeordneten Frist nicht entsprechen, kann die Cybersicherheitsbehörde von der zuständigen Behörde verlangen, die Zertifizierung oder Genehmigung für einen Teil oder alle von der Einrichtung erbrachten einschlägigen Dienste oder Tätigkeiten auszusetzen oder die nationale Behörde für die Cybersicherheitszertifizierung gemäß Art. 58 des Rechtsakts zur Cybersicherheit oder eine Konformitätsbewertungsstelle zu ersuchen,

die Zertifizierung oder Genehmigung auszusetzen (Abs. 4 Z 1). Zudem kann die Cybersicherheitsbehörde im Falle der Nichtbefolgung eines Bescheides gemäß Abs. 2 einem Leitungsorgan der Einrichtung mit Bescheid untersagen, seine Leitungsaufgaben in dieser wesentlichen Einrichtung wahrzunehmen (Abs. 4 Z 2).

Die Cybersicherheitsbehörde soll – angelehnt an § 70 Abs. 9 des Bankwesengesetzes (BWG), BGBl. Nr. 532/1993 – den Bescheid sowie auch die Aufhebung der Untersagung dem Firmenbuchgericht zur Eintragung in das Firmenbuch zu übermitteln haben. Dadurch soll der Untersagung der Ausübung der Leitungsaufgaben die entsprechende rechtlich relevante Publizität verschafft werden. Die Eintragung stellt eine allgemeine Eintragung nach § 3 Abs. 1 Z 16 des Firmenbuchgesetzes (FBG), BGBl. Nr. 10/1991, dar.

Sobald die jeweilige wesentliche Einrichtung die angeordneten Maßnahmen gemäß Abs. 2 nachträglich umsetzt, sind die gemäß Abs. 4 verhängten vorübergehenden Aussetzungen oder Verbote von der Cybersicherheitsbehörde unverzüglich aufzuheben (Abs. 5).

Wenngleich die Regelungen gemäß Abs. 1 bis 3 auch in Bezug auf Behörden und sonstige Stellen der öffentlichen Verwaltung zur Anwendung gelangen sollen, sollen im Gegensatz dazu die Maßnahmen gemäß Abs. 4 Z 1 und 2 gegenüber diesen Einrichtungen nicht ergriffen werden können (Abs. 6).

In Abs. 7 wurden die entsprechenden Vorgaben aus Art. 32 Abs. 7 NIS-2-Richtlinie übernommen, um sicherzustellen, dass die Cybersicherheitsbehörde bei der Auswahl ihrer Mittel zur Durchsetzung nicht in unverhältnismäßiger Weise vorgeht und von den – gemessen an der österreichischen Rechtsordnung durchaus drastischen Eingriffen – nach der Richtlinie verpflichtend vorzusehenden Maßnahmen nicht überschießend Gebrauch gemacht wird.

Aus dem Wortlaut des Art. 34 Abs. 2 NIS-2-Richtlinie und dem Zusammenspiel mit Art. 32 Abs. 4 lit. i bzw. Art. 33 Abs. 4 lit. h NIS-2-Richtlinie ergibt sich, dass Geldbußen nicht unmittelbar, sondern nur zusätzlich zur Ergreifung zumindest einer (Durchsetzungs-)Maßnahme gemäß Art. 32 Abs. 4 lit. a bis h NIS-2-Richtlinie sowie Abs. 5 und Art. 33 Abs. 4 lit. a bis g NIS-2-Richtlinie verhängt werden können. Dementsprechend soll in Abs. 8 festgelegt werden, dass die Cybersicherheitsbehörde bei Verdacht einer Verwaltungsübertretung – neben der gesetzlich statuierten Anzeigepflicht an die Bezirksverwaltungsbehörde (vgl. dazu die Erläuterungen zu § 44 Abs. 1) – zudem geeignete Durchsetzungsmaßnahmen gemäß Abs. 1 bis 4 zu ergreifen hat (vgl. zudem auch die Erläuterungen zu § 44 Abs. 2).

Gemäß Abs. 9 soll festgelegt werden, dass die Cybersicherheitsbehörde dem Bundesminister für Inneres halbjährlich über die ergriffenen Aufsichts- und Durchsetzungsmaßnahmen zu berichten hat, um die regelmäßige Auseinandersetzung mit bestehenden Prozessen und Abläufen im Rahmen des Aufsichts- und Durchsetzungsregimes sicherzustellen und allfälliges Verbesserungspotenzial aufgreifen zu können. Zur diesbezüglichen Berichtspflicht des Bundesministers für Inneres als oberstes Organ gegenüber dem National- und Bundesrat vgl. die Erläuterungen zu § 4 Abs. 3.

Zu § 40 (Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung):

Mit dieser Bestimmung wird Art. 24 NIS-2-Richtlinie umgesetzt. Wesentlich ist, dass die Regelung lediglich auf „IKT-Produkte, -Dienste und -Prozesse“ abstellt, weshalb IKT-Komponenten, die keine IKT-Produkte darstellen, nicht umfasst sein sollen.

Zu § 41 (Beschwerdeverfahren):

Diese Bestimmung legt fest, dass gegen Bescheide der Cybersicherheitsbehörde und wegen Verletzung ihrer Entscheidungspflicht Beschwerde an das Bundesverwaltungsgericht erhoben werden kann (Abs. 1). Gegen Bescheide der Bezirksverwaltungsbehörden und wegen Verletzung ihrer Entscheidungspflichten in Verwaltungssachen kann Beschwerde an die Verwaltungsgerichte der Länder erhoben werden (Abs. 2).

Zu § 42 (Datenschutzbestimmungen):

Im 4. Hauptstück (§§ 42 und 43) werden datenschutzrechtliche Bestimmungen zur Verarbeitung von personenbezogenen Daten gemäß Art. 4 Nr. 2 DSGVO und § 36 DSG geregelt. Die Bestimmung orientiert sich am Aufbau und der Struktur der Bestimmung im NISG und wird durch die neuen Aufgaben der Cybersicherheitsbehörde ergänzt. Der Bundeskanzler, der Bundesminister für Inneres, die Cybersicherheitsbehörde, der Bundesminister für Landesverteidigung und der Bundesminister für europäische und internationale Angelegenheiten, aber auch die CSIRTs sollen gemäß § 42 Abs. 1 explizit ermächtigt sein, zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen bei der Wahrnehmung ihrer Aufgaben nach diesem Bundesgesetz und zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit die erforderlichen personenbezogenen Daten zu verarbeiten. Beim Verarbeiten von personenbezogenen Daten sind die Grundsätze für die Verarbeitung

personenbezogener Daten, wie insbesondere der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO), der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und der Verhältnismäßigkeitsgrundsatz (§ 1 Abs. 2 DSG) zu beachten.

In Abs. 2 bis 6 werden abschließend die Datenkategorien bestimmt, die von den Abs. 1 bezeichneten datenschutzrechtlichen Verantwortlichen zur Erfüllung ihrer Aufgaben nach diesem Bundesgesetz verarbeitet werden dürfen. Diese umfassen Kontakt- und Identitätsdaten natürlicher und juristischer Personen, wie etwa Vor- und Familienname, Firmenname, Wohnadresse, Firmenadresse, Telefonnummer, E-Mail-Adresse oder User- und Account-Name, technische Daten, wie etwa ASN-Nummer, Domain-Name, Hashes, Host-Name, IP-Adresse, Log-Files, Metadaten, Network-Dump, Ports, Rechnername, RIPE-Handle oder Uniform Resource Locator (URL) und unternehmensbezogene Daten, wie etwa die Anzahl der Mitarbeiter, Bilanzdaten oder Daten aus der Gewinn- und Verlustrechnung, die insbesondere zur Überprüfung der Unternehmensgröße gemäß § 25 für die Cybersicherheitsbehörde erforderlich sind.

Da im Rahmen der Wahrnehmung der Aufgabenerfüllung nicht ausgeschlossen werden kann, dass von der Verarbeitung auch besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO und § 39 DSG betroffen sein können sowie dem Umstand, dass im Rahmen des § 20 Abs. 3, § 44 Abs. 7 iVm § 21 Abs. 3, § 43 Abs. 1 Z 4 und 5, § 44 Abs. 1 und 2 sowie § 34 Abs. 4 und § 46 Abs. 1 personenbezogene Daten im Sinne des Art. 10 DSGVO bzw. § 4 Abs. 3 DSG verarbeitet werden, bestimmt Abs. 7, dass besondere Kategorien personenbezogener Daten und Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen verarbeitet werden dürfen, wenn dies zum Zweck der Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen und der Abwehr von Gefahren für die öffentliche Sicherheit unbedingt erforderlich ist.

In Abs. 8 wird festgelegt, dass für die Erhebung, Abfrage, Übermittlung, Änderung und Löschung von personenbezogenen Daten Protokollaufzeichnungen zu führen und nach drei Jahren zu löschen sind. Abs. 9 sieht vor, dass personenbezogene Daten unverzüglich zu löschen sind, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Im Rahmen der operativen Analyse (vgl. § 18) werden Informationen über konkrete Sachverhalte verarbeitet, um einerseits durch Vergleich von Angriffen mit ähnlichem Muster eine Häufung von Angriffen zu erkennen und andererseits, darauf aufbauend, Maßnahmen der Abwehr und Prävention zu entwickeln. Eine Speicherdauer von fünf Jahren ist in diesem Zusammenhang jedenfalls erforderlich und stellt im Übrigen auch ein ausgewogenes Verhältnis zwischen dem Ziel und den eingesetzten Mitteln dar. Nach Ablauf von fünf Jahren sind die Daten von den Verantwortlichen jedenfalls zu löschen.

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 und § 45 Abs. 3 DSG 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 wird in Abs. 10 für sämtliche nach dem 3. Abschnitt des 2. Hauptstücks, dem 1., 2. und 4. Abschnitt des 3. Hauptstücks verarbeiteten Daten Gebrauch gemacht. Für einen geordneten Vollzug dieser Hauptstücke ist die Verarbeitung personenbezogener Daten im gesetzlich vorgesehenen Maße unerlässlich und liegt in diesem Sinne auch ein überwiegendes schutzwürdiges, öffentliches Interesse an der Datenverarbeitung vor.

Da die Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen, insbesondere im Rahmen der Behandlung der Reaktion auf und Analyse von Cybersicherheitsvorfällen sowie der damit zusammenhängenden Erstellung eines Lagebildes Aspekte der nationalen Sicherheit, der Landesverteidigung und der öffentlichen Sicherheit berühren können, und diese allgemeine öffentliche Interessen darstellen, ist die gesetzlich vorgesehene Verarbeitung der betreffenden Daten zur Erfüllung der den Behörden übertragenen Aufgaben – bis zur gesetzlich vorgesehenen Löschung – zu jedem Zeitpunkt erforderlich. Es ist daher auch erforderlich und sachgerecht, den Ausschluss des Widerspruchsrechts gemäß Art. 21 DSGVO sowie des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO und § 45 Abs. 3 DSG für alle nach dem 3. Abschnitt des 2. Hauptstücks, dem 1., 2. und 4. Abschnitt des 3. Hauptstücks 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 Person eine weitere Datenverarbeitung mit Ausnahme der

Speicherung der Daten bis zum Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung nicht mehr vorgenommen werden dürfte, sofern der Betroffene die Einschränkung der Verarbeitung verlangt (Art. 18 Abs. 1 lit. d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 lit. a oder lit. d DSGVO verlangt. Durch die Ausübung dieser Rechte könnte ein Betroffener demnach verhindern, dass ihn betreffende personenbezogene Daten zur Erfüllung gesetzlicher Aufgaben – zumindest für die Dauer der Prüfung des Antrags – nicht verarbeitet werden dürfen. Weiters wäre im Falle eines Widerspruchs nach Art. 21 DSGVO sowie bei einem Verlangen auf Einschränkung der Verarbeitung nach Art. 18 DSGVO oder § 45 DSG und der – wenn auch nur vorübergehenden – Unzulässigkeit der Weiterverarbeitung die Besorgung der Aufgaben nach diesem Bundesgesetz wesentlich beeinträchtigt. Durch die vorliegenden Bestimmungen wird das Recht auf Löschung unrichtiger und unrechtmäßig verarbeiteter Daten gemäß Art. 17 DSGVO und § 45 DSG nicht berührt.

Gemäß Abs. 11 soll im Sinne der Transparenz und zur Sicherstellung der Rechtmäßigkeit der Datenverarbeitungen angeordnet werden, dass der zuständige Datenschutzbeauftragte einen halbjährlichen Übersichtsbericht über die Datenverarbeitungen (zB Übersicht über Datenübermittlungen gemäß § 43, Inanspruchnahme der Betroffenenrechte) zu veröffentlichen hat.

Zu § 43 (Datenübermittlungen):

Der Bundeskanzler, der Bundesminister für Inneres, die Cybersicherheitsbehörde, der Bundesminister für Landesverteidigung und der Bundesminister für europäische und internationale Angelegenheiten sind berechtigt, Daten, die sie aufgrund der Wahrnehmung ihrer Aufgaben nach diesem Bundesgesetz verarbeitet haben, an militärische Behörden für Zwecke der militärischen Landesverteidigung gemäß Art. 79 Abs. 1 B-VG, an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege sowie an inländische Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist, zu übermitteln. Die Möglichkeit der Übermittlung von personenbezogenen Daten ist angesichts des breiten Charakters der Cyberbedrohungen notwendig. Die abzuwendende Gefahr des Eingriffs in die Netz- und Informationssysteme stellt eine „Querschnittsgefahr“ dar, deren Abwehr verschiedenen besonderen Verwaltungsmaterien zuzuordnen ist. Daher soll die Möglichkeit bestehen, Daten an die inländischen Behörden, die diese – von Cybergefahren bedrohten – besonderen Verwaltungsmaterien vollziehen, zu übermitteln, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist.

Die Cybersicherheitsbehörde kann gemäß Abs. 2 darüber hinaus personenbezogene Daten an bestimmte ausländische Sicherheitsbehörden und Sicherheitsorganisationen (§ 2 Abs. 2 und 3 des Polizeikooperationsgesetzes – PolKG, BGBI. I Nr. 104/1997) sowie Organe der Europäischen Union oder der Vereinten Nationen in Einklang mit den Bestimmungen über die internationale polizeiliche Amtshilfe übermitteln. Diese Bestimmung entspricht § 10 Abs. 4 NISG idF BGBI. I Nr. 111/2018. Hinsichtlich der Übermittlung an Drittstaaten sind die Vorgaben des Kapitels 5 der DSGVO sowie gemäß §§ 58 f DSG einzuhalten.

Die Cybersicherheitsbehörde wird darüber hinaus in Abs. 3 ermächtigt, bestimmte Übermittlungen von personenbezogenen Daten vorzunehmen. Dies umfasst die Übermittlung von personenbezogenen Daten an wesentliche und wichtige Einrichtungen und an mit diesen im Rahmen des Schutzes ihrer Netz- und Informationssysteme zusammenarbeitenden Dritten sowie sonstige Einrichtungen, die von einem Risiko oder Cybersicherheitsvorfall betroffen sind, CSIRTS zur Wahrnehmung ihrer Aufgaben, die ENISA, die zentralen Analysenstellen der von einem erheblichen Cybersicherheitsvorfall betroffenen Mitgliedstaaten, die zuständigen Behörden in der Europäischen Union, der Europäischen Kommission und EU-CYCLONE.

Abs. 4 legt fest, dass die CSIRTS berechtigt sind, Daten zur Erfüllung ihrer Aufgaben an wesentliche und wichtige Einrichtungen gemäß § 8 Abs. 1, 2 und 7 sowie § 34 Abs. 4, an sonstige Einrichtungen und Personen gemäß § 8 Abs. 10, an Teilnehmer des CSIRTS-Netzwerks gemäß § 8 Abs. 1 Z 6, an nationale CSIRTS von Drittländern oder gleichwertigen Stellen oder Sicherheitsdienstleistern gemäß § 8 Abs. 8 sowie an inländische Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist, übermitteln.

Zu § 44 (Allgemeine Bedingungen für die Verhängung von Geldstrafen):

Für Verstöße gegen die Verpflichtungen, die sich aus diesem Bundesgesetz ergeben und in § 45 aufgezählt werden, sollen Verwaltungsstrafen von den Bezirksverwaltungsbehörden als zuständige Behörden nach den verfahrensrechtlichen Bestimmungen des Verwaltungsstrafgesetzes 1991 (VStG), BGBI. Nr. 52/1991, zu verhängen sein. 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, LGBI. Nr. 103/2018, sowie § 2a des Gesetzes vom 14. Februar 1977 über die Organisation der Bezirkshauptmannschaften, LGBI. Nr. 11/1977).

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 eine ordnungsgemäße Führung von Strafverfahren nach diesem Bundesgesetz zu gewährleisten, soll daher in Abs. 1 vorgesehen werden, dass die Cybersicherheitsbehörde Sachverhalte, die den Verdacht einer Verwaltungsübertretung gemäß § 45 Abs. 1 oder 4 begründen, der zuständigen Bezirksverwaltungsbehörde zur Anzeige zu bringen hat (vgl. dazu auch die Erläuterungen zu § 39 Abs. 8).

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 der Cybersicherheitsbehörde im Hinblick auf Verwaltungsübertretungen gemäß § 45 Abs. 1 oder 4 zwar grundsätzlich unberührt bleibt. Angesichts der Bedeutung der Cybersicherheit 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 einer unionsrechtskonformen und damit wohl restriktiven Anwendung dieser Bestimmung im Vollzug.

Zudem soll angeordnet werden, dass die Bezirksverwaltungsbehörde der Cybersicherheitsbehörde einen jährlichen Bericht über eingeleitete Verwaltungsstrafverfahren sowie die Gründe für eine allenfalls unterbliebene Einleitung oder Einstellung nach standardisierten Vorgaben innerhalb einer bestimmten Frist zu erstatten hat.

Vor dem Hintergrund, dass gemäß Art. 34 Abs. 2 iVm Art. 32 Abs. 4 lit. i bzw. Art. 33 Abs. 4 lit. h NIS-2-Richtlinie Geldbußen lediglich zusätzlich zu zumindest einer Durchsetzungsmaßnahme verhängt werden dürfen, soll in Abs. 2 angeordnet werden, dass die Bezirksverwaltungsbehörde die Cybersicherheitsbehörde über von Amts wegen eingeleitete Verwaltungsstrafverfahren zu informieren hat. Damit soll sichergestellt werden, dass die Cybersicherheitsbehörde in jedem Fall Kenntnis über den Verdacht einer Verwaltungsübertretung erlangt und folglich geeignete Durchsetzungsmaßnahmen ergreifen kann (vgl. dazu die Erläuterungen zu § 39 Abs. 8).

Gemäß Abs. 3 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 § 99d BWG orientiert. Demnach soll die Bezirksverwaltungsbehörde unter den Voraussetzungen der Abs. 3 und 4 Geldstrafen gegen eine juristische Person oder eingetragene Personengesellschaft verhängen können, wobei es in ihrem (pflichtgemäßem) Ermessen liegen soll, die jeweilige juristische Person bzw. eingetragene Personengesellschaft als unmittelbare Strafaddressatin zu verfolgen und gegebenenfalls zu bestrafen (vgl. VwGH vom 29.03.2019, Ro 2018/02/0023). Da das VStG lediglich das Verfahren für die Strafbarkeit natürlicher Personen normiert, ist vor dem Hintergrund der unionsrechtlichen Vorgabe gemäß Art. 34 Abs. 1 NIS-2-Richtlinie, wonach die Mitgliedstaaten sicherzustellen haben, dass bei Pflichtverstößen durch wesentliche und wichtige Einrichtungen wirksame, verhältnismäßige und abschreckende Geldbußen (unmittelbar) gegen diese verhängt werden, die Abweichung vom Regime des § 9 VStG zur vollständigen Umsetzung des Art. 34 NIS-2-Richtlinie zwingend 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.

Die Intention der Regelungen gemäß Abs. 3 und 4 soll in Zusammenschau mit Abs. 5 darin liegen, dass bei Vorliegen der in Abs. 3 und 4 gelisteten Voraussetzungen die juristische Person selbst primärer Adressat der Verwaltungssanktion sein und daher – auch mit Blick auf die Vorgaben der NIS-2-Richtlinie (vgl. Art. 34 NIS-2-Richtlinie) – der wirtschaftliche Nachteil der Verwaltungsstrafe vorrangig jene Person treffen soll, die auch den „Nutzen“ gezogen hat. Im Rahmen der Ausübung ihres pflichtgemäßem Ermessens soll die Bezirksverwaltungsbehörde daher die Wertung der Regelung, wonach sich die

Verfolgung primär auf die juristische Person als eigentlichen „Nutzträger“ konzentrieren und die Verwaltungsstrafe in erster Linie die Einrichtung selbst treffen soll, zu berücksichtigen haben.

Abs. 6 soll die Bestimmung des Art. 34 Abs. 3 NIS-2-Richtlinie, wonach bei der Entscheidung über die Verhängung einer Geldbuße und deren Höhe in jedem Einzelfall zumindest die in Art. 32 Abs. 7 NIS-2-Richtlinie genannten Elemente gebührend zu berücksichtigen sind, aufgreifen. Dementsprechend wird hier auf die vergleichbare Bestimmung in § 39 Abs. 7 verwiesen.

Nach Art. 35 Abs. 2 NIS-2-Richtlinie dürfen die zuständigen Behörden für einen Verstoß, der sich aus demselben Verhalten ergibt wie ein Verstoß, der Gegenstand einer verhängten Geldbuße nach Art. 58 Abs. 2 lit. i DSGVO war, keine Geldbuße nach Art. 34 der vorliegenden Richtlinie verhängen. Dem soll durch die Regelung in Abs. 7 entsprochen werden.

Zu § 45 (Verwaltungsstrafbestimmungen):

Die in Abs. 1 aufgelisteten Verwaltungsübertretungen haben insbesondere Verstöße von wesentlichen und wichtigen Einrichtungen betreffend die Durchführung von Cybersicherheitsschulungen, die Setzung von Risikomanagementmaßnahmen sowie die Meldung von erheblichen Cybersicherheitsvorfällen zum Gegenstand.

Die beiden Abs. 2 und 3 legen den Strafrahmen für die Verwirklichung einer Verwaltungsübertretung nach Abs. 1 für wesentliche und wichtige Einrichtungen fest und setzen Art. 34 Abs. 4 und Abs. 5 NIS-2-Richtlinie um.

Abs. 4 hat insbesondere die Missachtung von Duldungs- und Mitwirkungspflichten wesentlicher und wichtiger Einrichtungen sowie Pflichtenverstöße von TLD-Namenregistern und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, hinsichtlich der Führung bzw. Erteilung von Zugang zu der gemäß Abs. 30 zu führenden Datenbank zum Gegenstand.

Aus diesen Regelungen ergibt sich, dass keine Verwaltungsstrafen für Leitungsorgane vorgesehen sind (vgl. auch die Erläuterungen zu § 31) und Verwaltungsstrafen ausschließlich gegen die jeweilige Einrichtung (bzw. die Verantwortlichen gemäß § 9 VStG) gerichtet sein sollen.

Wesentlich ist, dass die Abs. 1 bis 4 auf Behörden, Organe sowie Einrichtungen und sonstige Stellen der öffentlichen Verwaltung, einschließlich der Gebietskörperschaften und unabhängig davon, ob sie hoheitlich oder im Rahmen der Privatwirtschaftsverwaltung eingerichtet oder tätig sind, keine Anwendung finden sollen (vgl. dazu das in § 46 Abs. 2 vorgesehene alternative Sanktionsregime). Daraus ergibt sich, dass neben der Hoheitsverwaltung auch die gesamte Privatwirtschaftsverwaltung von dieser Regelung umfasst sein soll. Organwälter sollen nicht unmittelbare Adressaten der sich aus dem gegenständlichen Gesetz ergebenden Verpflichtungen sein. Vor dem Hintergrund, dass Behörden, Organe sowie Einrichtungen und sonstige Stellen der öffentlichen Verwaltung selbst von Verwaltungsstrafen ausgenommen sein sollen, kann auch keine verwaltungsstrafrechtliche Verantwortlichkeit der nach außen vertretungsbefugten Personen – also der Organwälter (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 § 46 (Nichteinhaltung von Verpflichtungen durch Stellen der öffentlichen Verwaltung):

Angelehnt an die im vorgeschlagenen § 44 Abs. 1 normierte Anzeigepflicht der Cybersicherheitsbehörde soll in Abs. 1 festgelegt werden, dass dieser der jeweils zuständigen Bezirksverwaltungsbehörde auch die Nichteinhaltung von sich aus diesem Bundesgesetz ergebenden Verpflichtungen durch Behörden und sonstige Stellen der öffentlichen Verwaltung anzuzeigen hat und soll eine entsprechende jährliche Berichtspflicht der Bezirksverwaltungsbehörden gegenüber der Cybersicherheitsbehörde festgelegt werden.

Vor dem Hintergrund, dass unter bestimmten Voraussetzungen auch Behörden und sonstige – sowohl in Formen des öffentlichen Rechts als auch des Privatrechts eingerichtete – Stellen der öffentlichen Verwaltung einschließlich der Gebietskörperschaften vom Anwendungsbereich der NIS-2-Richtlinie umfasst sind, bedarf es zur unionsrechtskonformen Umsetzung des Art. 36 NIS-2-Richtlinie eines wirksamen alternativen 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 NIS-2-Richtlinie erfordert jedoch einen Sanktionsmechanismus auch gegenüber Behörden und sonstigen 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 Marktmisbrauch [Marktmisbrauchsverordnung] 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 Marktmisbrauchsverordnung).

Vor dem Hintergrund, dass Geldstrafen gegenüber Behörden den Anforderungen des Art. 36 NIS-2-Richtlinie 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 abweichend von § 45 keine Geldbußen gegen Behörden und sonstige Stellen der öffentlichen Verwaltung, einschließlich der Gebietskörperschaften sowie in Formen des Privatrechts eingerichtete Stellen der öffentlichen Verwaltung, verhängt werden dürfen. Die zuständige Bezirksverwaltungsbehörde soll stattdessen nach den Bestimmungen des Allgemeinen Verwaltungsverfahrensgesetzes 1991 (AVG), BGBL. Nr. 51/1991, bescheidmäßig die Nichteinhaltung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen – sohin in mittelbarer Bundesverwaltung – festzustellen und eine angemessene Frist für die Herstellung des rechtmäßigen Zustandes anzuordnen haben. Wesentlich ist, dass den Bezirksverwaltungsbehörden keine Aufgaben im Rahmen der Aufsicht und Durchsetzung (vgl. etwa die §§ 38 und 39) übertragen werden sollen, sondern einzig die Cybersicherheitsbehörde als „Aufsichtsbehörde“ im Sinne des gegenständlichen Gesetzes fungieren soll. Wird dem Bescheid nicht ordnungsgemäß innerhalb der angeordneten Frist entsprochen, soll die Bezirksverwaltungsbehörde nach Eintritt der formellen Rechtskraft des Bescheides – angelehnt an die oben angeführten unionsrechtlichen Vorschriften – dazu verpflichtet sein, die Nichteinhaltung von Verpflichtungen nach diesem Bundesgesetz 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 öffentlich zugänglichen Homepage der zuständigen Bezirksverwaltungsbehörde. Vor dem Hintergrund der Sensibilität der Informationen ist wesentlich, dass vor Veröffentlichung den jeweiligen betroffenen Behörden und sonstigen Stellen der öffentlichen Verwaltung Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist gegeben werden soll.

Bei der Veröffentlichung selbst soll die Bezirksverwaltungsbehörde darauf Bedacht zu nehmen haben, dass diese keine Gefahr für die öffentliche Ordnung oder Sicherheit oder für die nationale Sicherheit darstellt sowie keine schutzwürdigen Interessen wesentlicher und wichtiger Einrichtungen beeinträchtigt und sollen dementsprechend allenfalls lediglich allgemeine Informationen über das Vorliegen einer Pflichtverletzung öffentlich bekannt gemacht werden, die keine konkreten Rückschlüsse auf bestehende Sicherheitsmängel zulassen. Von der (Verfassungs-)Bestimmung sollen neben Behörden auch sonstige Stellen der öffentlichen Verwaltung einschließlich der Gebietskörperschaften sowie in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen der öffentlichen Verwaltung (insbesondere aus gegliederte Rechtsträger privaten oder öffentlichen Rechts) umfasst sein und soll demnach § 45 nicht zur Anwendung gelangen, 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. Wesentlich ist, 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 weit gefasst und sollen allenfalls auch staatsnahe private und somit ausgegliederte Rechtsträger (vgl. VfGH 5.10.2023, G 265/2022, sowie VfGH 14.12.2023, G 328-335/2022) unter das alternative Sanktionsregime fallen. Organwalter sollen nicht unmittelbare Adressaten der sich aus dem gegenständlichen Gesetz ergebenden Verpflichtungen sein. 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.

Der Sanktionscharakter dieser Bestimmung 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. 36 NIS-2-Richtlinie hinreichend Genüge getan.

Im Hinblick darauf, dass eine Einschränkung auf „als wesentliche oder wichtige Einrichtungen geltende“ Behörden erfolgt, soll etwa die Nichteinhaltung der der Cybersicherheitsbehörde obliegenden Aufgaben (vgl. § 4) nicht unter diese Regelung fallen.

Zu § 47 (Personenbezogene Bezeichnungen):

§ 47 dient der Klarstellung, dass alle in diesem Bundesgesetz verwendeten personenbezogenen Bezeichnungen gleichermaßen für alle Geschlechter gelten. Bei der Anwendung der Bezeichnung auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

Zu § 48 (Durchführung und Umsetzung von Rechtsakten der Europäischen Union):

Durch dieses Bundesgesetz wird die NIS-2-Richtlinie umgesetzt und die Verordnung (EU) 2021/887 durchgeführt.

Zu § 49 (Verweisungen):

Verweisungen auf andere Bundesgesetze sind grundsätzlich als Verweisungen auf die jeweils geltende Fassung zu verstehen. Demgegenüber sind Verweisungen, die auf ein Gesetz in einer bestimmten Fassung verweisen, nicht als Verweisungen auf die jeweils geltende Fassung zu verstehen. Verweisungen auf europäische Rechtsakte sind darüber hinaus als Verweisungen auf die zum Zeitpunkt des Inkrafttretens geltende Fassung zu verstehen, sofern die entsprechende Bestimmung nicht ohnehin zur besseren Verständlichkeit direkt in das Gesetz übernommen wurde.

Zu § 50 (Vollziehung):

Mit der Vollziehung dieses Bundesgesetzes soll grundsätzlich der Bundesminister für Inneres betraut werden (§ 50 Z 5).

Davon abweichend soll die Vollziehung hinsichtlich des § 6 Abs. 2, soweit er die Befreiung von den Verwaltungsabgaben des Bundes betrifft, der Bundesregierung und im Übrigen – soweit es sich um Gebühren handelt – dem Bundesminister für Finanzen obliegen (Z 1).

Mit der Vollziehung dieses Bundesgesetzes hinsichtlich der Erlassung der nationalen Cybersicherheitsstrategie (§ 15 Abs. 1) soll die Bundesregierung betraut sein (Z 2).

Die Cyber Sicherheit Steuerungsgruppe (CSS) soll sich aus fachkundigen Vertretern der im Nationalen Sicherheitsrat vertretenen Bundesminister zusammensetzen und soll diesen Bundesministern daher auch die Vollziehung dieses Bundesgesetzes in diesem Zusammenhang obliegen.

Die Aufgaben der operativen Koordinierungsstrukturen des IKDOK und des OpKoord (§§ 13 und 14) sollen von den darin vertretenen Bundesministern gemeinsam vollzogen werden (Z 3 und 4).

Zu § 51 (Inkrafttretens-, Außerkrafttretens- und Übergangsbestimmungen):

Mit dieser Bestimmung sollen das Inkrafttreten des vorgeschlagenen Bundesgesetzes, das Außerkrafttreten des NISG samt der auf dessen Grundlage erlassenen Verordnungen sowie die erforderlichen Übergangsbestimmungen geregelt werden.

Vor dem Hintergrund, dass der vorliegende Entwurf die nähere Ausgestaltung einzelner Bestimmungen einer Verordnung der Cybersicherheitsbehörde vorbehält (vgl. etwa § 35 Abs. 3), soll in Abs. 3 vorgesehen werden, dass Verordnungen auf Grund dieses Bundesgesetzes bereits ab dem Tag der Kundmachung dieses Bundesgesetzes erlassen werden können, wobei sie frühestens mit Inkrafttreten dieses Bundesgesetzes in Kraft treten sollen.

Da die NIS-2-Richtlinie den Mitgliedstaaten zahlreiche Verpflichtungen auferlegt, für deren Erfüllung umfassende organisatorische und personelle Maßnahmen erforderlich sind, soll der Zeitraum zwischen

Kundmachung und Aufgabenwahrnehmung durch die Cybersicherheitsbehörde genutzt und dementsprechend in Abs. 4 normiert werden, dass bereits ab dem der Kundmachung dieses Bundesgesetzes folgenden Tag alle für die Ermöglichung einer zeitgerechten Aufgabenwahrnehmung durch die Cybersicherheitsbehörde erforderlichen vorbereitenden Maßnahmen – etwa organisatorischer und personeller Natur – zu setzen sind.

Gemäß Abs. 5 sollen Bescheide, die gemäß § 15 Abs. 3, § 16 Abs. 1 und § 18 Abs. 1 NISG erlassen wurden, mit Inkrafttreten dieses Bundesgesetzes gegenstandslos werden, sofern nicht Abs. 6 oder 7 zur Anwendung gelangt.

In Abs. 6 soll angeordnet werden, dass das gemäß § 15 Abs. 3 NISG ermächtigte nationale CSIRT die Aufgaben gemäß § 8 Abs. 1 und 3 sowie § 11 bis zur Ermächtigung eines nationalen CSIRTs gemäß § 8 Abs. 2, längstens jedoch für einen Zeitraum von zwei Jahren ab Inkrafttreten dieses Bundesgesetzes, wahrzunehmen hat, wobei die Regelungen betreffend den Kostenersatz gemäß § 8 Abs. 6 sowie die Aufsicht durch die Cybersicherheitsbehörde gemäß § 10 gelten sollen. Dadurch soll angesichts der Relevanz für die Sicherheit von Netz- und Informationssystemen sichergestellt werden, dass die Aufgaben des nationalen CSIRTs bereits ab Inkrafttreten dieses Gesetzesentwurfs uneingeschränkt wahrgenommen werden.

Durch den vorgeschlagenen § 7 soll das im NISG bestehende System der qualifizierten Stellen mit systematischen Anpassungen in das neue NIS-2-Regime überführt werden, wobei jedoch keine „Zulassung“ unabhängiger Stellen erfolgen, sondern der Fokus auf der Sicherstellung der fachlichen Qualität von unabhängigen Prüfern im Rahmen eines bescheidmäßigen Zulassungsverfahrens liegen soll und sollen die diesbezüglichen Parameter durch Verordnung festgelegt werden (vgl. die Erläuterungen zu § 7). Die Regelung in § 33 Abs. 2, wonach der Nachweis der Umsetzung der Risikomanagementmaßnahmen grundsätzlich durch eine von einer unabhängigen Stelle durchgeführte Prüfung zu erfolgen hat, würde im Ergebnis dazu führen, dass solange seitens der Cybersicherheitsbehörde noch keine derartige Verordnung erlassen wurde und – entweder mangels Verordnung oder mangels Antragstellung – (noch) keine bescheidmäßige Zulassung von unabhängigen Prüfern erfolgt ist, ein ordnungsgemäßer Vollzug bzw. Nachweis der Risikomanagementmaßnahmen durch wesentliche und wichtige Einrichtungen nicht möglich wäre. Demnach soll im Sinne eines nahtlosen Übergangs von NIS-1 auf NIS-2 in Abs. 7 eine Übergangsregelung dahingehend erfolgen, dass bisher nach dem NIS-1-Regime bescheidmäßig ermittelte qualifizierte Stellen für eine Übergangszeit als unabhängige Stellen fungieren können und diese Prüfungen demnach anzuerkennen sind, wobei (auch mit Blick auf die Divergenzen zum neuen angedachten Prüfregime) vorgesehen ist, dass qualifizierte Stellen im Rahmen der Prüfungen die bisher von ihnen eingesetzten Prüfer heranzuziehen haben. Diese Schonfrist soll in Kombination mit der in Abs. 8 vorgesehenen Regelung einen ausreichenden Zeitraum für die Etablierung von unabhängigen Stellen und unabhängigen Prüfern zur Verfügung stellen und demnach dem Grundsatz der Rechtssicherheit für die Betroffenen Genüge tun.

Damit im Zusammenhang stehend soll in Abs. 8 die Klarstellung erfolgen, dass Anträge gemäß § 7 Abs. 2 auf Zulassung als unabhängiger Prüfer erst ab dem Zeitpunkt des Inkrafttretens der gemäß § 7 Abs. 6 vorgesehenen Verordnungen möglich sein sollen, zumal in dieser die Festlegung der Inhalte des Prüfverfahrens erfolgen soll.

Um die zeitgerechte Wahrnehmung der Aufgaben nach diesem Bundesgesetz sicherzustellen, soll in Abs. 9 angeordnet werden, dass die Ausschreibung der Funktionen des Direktors und seines Stellvertreters (vgl. § 3b) bereits vor Inkrafttreten dieses Bundesgesetzes zulässig ist.

Zu den Anlagen 1 und 2:

Die Anlagen 1 und 2 überführen die Anhänge I und II der NIS-2-Richtlinie in das nationale Recht.

Gemäß Anlage 1 Punkt 1 lit. a (Sektor „Energie“, Teilsektor „Elektrizität“) erste Variante soll – entsprechend der unionsrechtlichen Vorgaben – festgelegt werden, dass es sich bei den vom Anwendungsbereich umfassten „Elektrizitätsunternehmen“ um solche gemäß § 7 Abs. 1 Z 11 des Elektrizitätswirtschafts- und -organisationsgesetzes 2010 (EIWOG 2010), BGBL. I Nr. 110/2010, handelt, sofern diese als Versorger gemäß § 7 Abs. 1 Z 74 EIWOG 2010 anzusehen sind. Daraus ergibt sich, dass mit einer Photovoltaikanlage ausgestattete Unternehmen, die überschüssige elektrische Energie in das öffentliche Netz gegen Entgelt einspeisen (sogenannte „Überschusseinspeiser“), von der Legaldefinition grundsätzlich nicht umfasst sein sollen, sofern diese elektrische Energie primär für den Eigenbedarf und somit ohne Gewinnerzielungsabsicht erzeugen. Der spätere Verkauf der überschüssigen Energie gegen Entgelt ändert an diesem Umstand nichts, zumal dieser keine Funktion gemäß § 7 Abs. 1 Z 11 EIWOG 2010 darstellt (vgl. VwGH 18.9.2019, Ro 2018/04/0010, Rz 33 ff.).

In Anlage 1 Punkt 1 lit. a (Sektor „Energie“, Teilesktor „Elektrizität“) wird in der vierten Variante („Erzeuger“) festgelegt, dass als relevante Arten der Einrichtung lediglich Erzeuger im Sinne des § 7 Abs. 1 Z 17 ElWOG 2010 zu verstehen sind, sofern es sich bei diesen Tätigkeiten um die gewerbliche oder berufliche Haupttätigkeit handelt. Diese Einschränkung vermeidet ein „ausufern“ des Anwendungsbereichs und harmonisiert die Umsetzung der NIS-2-Richtlinie mit jener des „Green Deals“ der Europäischen Union.

In Anlage 1, Punkt 1 lit. a (Sektor „Energie“, Teilesktor „Elektrizität“) werden in der siebten Variante („Betreiber von Ladepunkten“) festgelegt, dass Betreiber von Ladepunkten, die für die Verwaltung und den Betrieb eines Ladepunkts gemäß § 2 Z 3 des Bundesgesetzes zur Festlegung einheitlicher Standards beim Infrastrukturaufbau für alternative Kraftstoffe, BGBI. I Nr. 38/2018. Hierzu existieren in der Praxis verschiedene Betriebsmodelle: Betreiber (Charge Point Operator kurz CPO), Mobilitätsdienstleister (eMobility Provider kurz EMP oder auch Mobility Service Provider kurz MSP) und Eigentümer. Als „Betreiber einer Ladestation“ wird in Art. 2 Z 39 Verordnung (EU) 2023/1804 über den Aufbau der Infrastruktur für alternative Kraftstoffe und zur Aufhebung der Richtlinie 2014/94/EU, ABl. Nr. L 234 vom 22.09.2023 S. 1, „die für die Verwaltung und den Betrieb eines Ladepunkts zuständige Stelle, die Endnutzern einen Aufladedienst erbringt, auch im Namen und Auftrag eines Mobilitätsdienstleisters“. Ein „Mobilitätsdienstleister“ wird gemäß Art. 2 Z 36 Verordnung (EU) 2023/1804 als eine juristische Person definiert, „die einem Endnutzer gegen Entgelt Dienstleistungen erbringt, einschließlich des Verkaufs von Auflade- oder Betankungsdiensten“. Ein „Aufladedienst“ gemäß Art. 2 Z 53 Verordnung (EU) 2023/1804 bezeichnet den Verkauf oder die Bereitstellung von Strom, einschließlich damit zusammenhängender Dienstleistungen, über einen öffentlich zugänglichen Ladepunkt. Im Wesentlichen ist unter dem Betreiber eines Ladepunktes somit jene Person erfasst, die für die Aufrechterhaltung des Betriebs des Ladepunkts sowohl im Bereich Hardware als auch der Software vorrangig verantwortlich ist. Als Mobilitätsdienstleister können auch jene Dienstleister erfasst werden, die über ein Abonnement das Laden auch an dem betroffenen Ladepunkt ermöglicht.

In Anlage 1, Punkt 1 lit. b (Sektor „Energie“, Teilesktor „Fernwärme“) wird die Art der Einrichtung als Betreiber von Fernwärme oder Fernkälte im Sinne des Art. 2 Z 19 der Richtlinie (EU) 2018/2001 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen, ABl. Nr. L 328 vom 21.12.2018 S. 82, in der Fassung der Berichtigung ABl. Nr. L 311 vom 25.09.2020 S. 11, definiert. Von diesen „Betreibern“ sind „Anbieter“ von Fernwärme bzw. Fernkälte zu unterscheiden, welche Abwärme (etwa Brauereien, Papierindustrie oder ähnliche) in das Fernwärme- oder Fernkältenetz.

In Anlage 1, Punkt 5 (Sektor „Gesundheitswesen“) wird der „Gesundheitsdienstleister“ im Sinne des Art. 3 lit. g der Richtlinie 2011/24/EU über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung ABl. Nr. L 88 vom 04.04.2011 S. 45, (im Folgenden: Patientenmobilitätsrichtlinie) als maßgebliche Art der Einrichtung definiert. Zum Begriff des „Gesundheitsdienstleisters“ kann auf Anlage 1 der Gesundheitstelematikverordnung 2013 (GTelV 2013), BGBI. II Nr. 506/2013, verwiesen werden. Gesundheitsdienstleister sind beispielsweise Ärzte und alle weiteren freiberuflich tätigen Angehörigen von Gesundheitsberufen, wie etwa Physiotherapeuten oder Heilmasseure. Es werden daher insbesondere folgende Einrichtungen als Gesundheitsdienstleister verstanden: Krankenanstalten im Sinne des Krankenanstalten- und Kuranstaltengesetzes (KaKuG), BGBI. Nr. 1/1975, Apotheken sowie Einrichtungen des Rettungswesens.

Demnach handelt es sich bei dem Großteil der in der Anlage 1 GTelV 2013 genannten Gesundheitsdiensteanbieter auch um Gesundheitsdienstleister im Sinn der Patientenmobilitätsrichtlinie. Allerdings sind dort nicht alle dieser Angehörigen der Gesundheitsberufe (als Teil der „Gesundheitsversorgung“) angeführt. Die in der GTelV 2013 in Anlage 1 angeführten Sozialversicherungsträger sind nicht als Gesundheitsdienstleister anzusehen.

In Hinblick auf den ErWGr 14 der Patientenmobilitätsrichtlinie, wonach Dienstleistungen der Langzeitpflege nicht unter Gesundheitsdienstleister im Sinne des Art. 3 lit. g Patientenmobilitätsrichtlinie zu subsumieren sind, wird für die NIS-2-Richtlinie, die sich auf diese Definition stützt, abgeleitet, dass Dienstleistungen der Langzeitpflege und damit einhergehend Einrichtungen der Pflege und Pflegeanstalten nicht von deren Anwendungsbereich umfasst sind.

Für die Abgrenzung zwischen Pflege in einem Pflegeheim und Pflege in einer Krankenanstalt ist darauf abzustellen, ob die Betroffenen eine ständige Pflege, oder aber bloß fallweise einer ärztlichen Betreuung bedürfen. Überwiegt der Pflegeaspekt, liegt ein Pflegeheim vor, überwiegt der Bedarf an ärztlicher Betreuung, eine Krankenanstalt. Hier ist insbesondere auf das Erkenntnis des Verfassungsgerichtshofs vom 16.10.1992, VfSlg 13.237, zu verweisen. Je nach Ausgestaltung der erbrachten Dienstleistungen in einer stationären Einrichtung können diese Einrichtungen in den Anwendungsbereich fallen.

In Anlage 1, Punkt 7 (Sektor „Abwasser“) werden aus der maßgeblichen Art der Einrichtung jene Unternehmen ausgeschlossen, „für die das Sammeln, die Entsorgung oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist“. Als allgemeine Tätigkeit wird jede Tätigkeit des Unternehmens zu verstehen sein, einschließlich jener Bereiche, die für sich genommen nicht wirtschaftlich sind. Als wesentliche Teile der allgemeinen Tätigkeit sind dabei wohl nur jene Teile zu verstehen, die in einer Gesamtbetrachtung des Unternehmens nicht unberücksichtigt bleiben können. Sind jedoch bestimmte Filter- oder Kläranlagen in Ausübung einer Tätigkeit (auch in einem der übrigen Sektoren) vorgesehen und dient diese Anlage vorrangig der Erfüllung dieser Vorgaben, dann ist davon auszugehen, dass es sich um einen „nicht wesentlichen Teil ihrer allgemeinen Tätigkeit“ handelt.

In Anlage 2, Punkt 2 (Sektor „Abfallwirtschaft“) soll die maßgebliche Art der Einrichtung unter anderem danach definiert werden, dass Unternehmen ausgeschlossen sein sollen, für die die Abfallbewirtschaftung nicht ihre „Hauptwirtschaftstätigkeit“ darstellt. Nicht wirtschaftliche Tätigkeiten sollen für die Ermittlung dieses Sektors von vornherein ausscheiden. Da die NIS-2-Richtlinie nicht von mehreren „Hauptwirtschaftstätigkeiten“ ausgeht (arg: „ihre“ Hauptwirtschaftstätigkeit), ist sohin – im Einklang mit den unionsrechtlichen Vorgaben – darauf abzustellen, ob – unter Berücksichtigung aller wirtschaftlichen Tätigkeiten des jeweiligen Unternehmens – die Abfallbewirtschaftung die primäre Tätigkeit darstellt.

In Anlage 2, Punkt 3 (Sektor „Produktion, Herstellung und Handel mit chemischen Stoffen“) umfasst die Art der Einrichtung jene Unternehmen, die in Art. 3 Z 9 und 14 der Verordnung (EG) Nr. 1907/2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Agentur für chemische Stoffe, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EG und 2000/21/EG der Kommission, ABl. Nr. L 396 vom 30.12.2006 S. 1 (im Folgenden REACH-Verordnung) angeführt sind. Hersteller gemäß Art. 3 Z 9 REACH-Verordnung bezeichnet natürliche oder juristische Person mit Sitz in der Gemeinschaft, die in der Gemeinschaft einen Stoff herstellt. Händler gemäß Art. 3 Z 14 REACH-Verordnung bezeichnet eine natürliche oder juristische Person mit Sitz in der Gemeinschaft, die einen Stoff als solchen oder in einem Gemisch lediglich lagert und an Dritte in Verkehr bringt, einschließlich Einzelhändler. Händler und Hersteller sind erfasst, sofern diese Stoffe herstellen und diese Stoffe oder Gemische ferner im Großhandel vertreiben sowie Unternehmen, die Erzeugnisse im Sinne des Art. 3 Z 3 der genannten Verordnung aus diesen Stoffen oder Gemischen produzieren, sofern diese Erzeugnisse in die Kategorie 20 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) fallen.

In Anlage 2, Punkt 4 (Sektor „Produktion, Verarbeitung und Vertrieb von Lebensmitteln“) wird die maßgebliche Art der Einrichtung unter anderem danach definiert, dass diese sowohl im Großhandel tätig ist als auch in der industriellen Produktion und Verarbeitung. Wird eine Einrichtung im Großhandel und in der industriellen Produktion und Verarbeitung tätig (kumulativ), erfüllt sie die Voraussetzung. Der Großhandel ist in Abgrenzung zum Einzelhandel zu verstehen. Die industrielle Produktion und Verarbeitung ist in Abgrenzung zur gewerblichen Produktion vom Grad der Automatisierung und der maschinellen Durchdringung abhängig.

Je nachdem, ob der Abnehmer der Waren an gewerbliche oder nicht gewerbliche Kunden verkauft, wird zwischen Groß- und Einzelhandel unterschieden: Großhandel liegt vor, wenn Marktteilnehmer Waren von Herstellern oder anderen Lieferanten beschaffen und an Wiederverkäufer, Weiterverarbeiter, gewerbliche Verwender oder sonstige Institutionen absetzen. Hingegen liegt Einzelhandel dann vor, wenn Handelsunternehmen die Waren verschiedener Hersteller beschaffen, diese zu einem Sortiment zusammenfügen und an nicht gewerbliche Kunden (Verbraucher bzw. Letzterverwender) verkaufen.

Zu Artikel 2 (Änderung des Telekommunikationsgesetzes 2021)

Zu Z 1 bis 6 (§ 44, § 188 Abs. 5, § 198, § 200 Abs. 1 und 5 sowie § 217 Abs. 5):

Art. 43 NIS-2-Richtlinie legt fest, dass die Art. 40 und 41 der Richtlinie (EU) 2018/1972, welche in Österreich durch die Bestimmung des § 44 TKG 2021 umgesetzt wurden, mit Wirkung vom 18. Oktober 2024 gestrichen werden, weshalb § 44 TKG 2021 entsprechender Anpassung bedarf.

§ 44 Abs. 1 TKG 2021 ermächtigt in der abgeänderten Fassung die Regulierungsbehörde (sowie – in Zusammenshau mit Abs. 4 – die KommAustria), mit Verordnung nähtere Vorgaben über technische und organisatorische Sicherheitsmaßnahmen festzulegen, sofern die in den bestehenden Rechtsvorschriften vorgesehenen Maßnahmen zur Gewährleistung eines hohen Cybersicherheitsniveaus nicht zur Erreichung des in § 1 Abs. 2 Z 4 TKG 2021 genannten Ziels ausreichen (Aufrechterhaltung der Sicherheit der Netze und Dienste). Eine solche Verordnung kann insbesondere speziellere Bestimmungen gegenüber dem NISG 2026 enthalten. Um einer „Normenkollision“ vorzubeugen, wird zunächst die ausdrückliche

Subsidiarität angeordnet. Eine solche Verordnung ist somit nur dann zulässig, wenn die bestehenden Rechtsvorschriften nicht ausreichen, um die Aufrechterhaltung der Sicherheit der Netze und Dienste zu gewährleisten. Dies kann auch dann vorliegen, wenn die bestehenden Vorschriften einer näheren sektorspezifischen Konkretisierung, allenfalls auch unter Einbindung technologiespezifischer Bestimmungen, erfordern. Darüber hinaus wird durch das Erfordernis des Einvernehmens mit dem Bundeskanzler, dem Bundesminister für Wohnen, Kunst, Kultur, Medien und Sport und der Cybersicherheitsbehörde ein kohärentes Vorgehen im Bereich der Cybersicherheit sichergestellt.

Die Verordnung ist ferner unter Bedachtnahme auf die relevanten internationalen Vorschriften, die nationale Cybersicherheitsstrategie, die Art des Netzes oder des Dienstes, die technischen Möglichkeiten, den Schutz personenbezogener Daten und die sonstigen schutzwürdigen Interessen von Nutzern zu erlassen.

Abs. 2 führt im Wesentlichen den bisherigen Abs. 14 fort.

Mit Abs. 3 werden der Regulierungsbehörde darüber hinaus folgende Aufgaben übertragen:

1. Durchführung einer Branchenrisikoanalyse in Zusammenarbeit mit dem Bundeskanzleramt, den Bundesministerien für Finanzen, für Inneres und für Landesverteidigung, dem CSIRT sowie den Betreibern von Fest- und von Mobilfunknetzen in Abständen von jeweils zwei Jahren sowie Erstellung eines Abschlussberichts, der den teilnehmenden Institutionen zur Verfügung zu stellen und unter Beachtung des notwendigen Schutzes kritischer Infrastrukturen in einer bereinigten Version auf der RTR-Website zu veröffentlichen ist;
2. Mitwirkung an der Erstellung eines Mustersicherheitskonzepts für Betreiber gemäß § 4 Z 25 TKG 2021 und Anbieter gemäß § 4 Z 36 TKG 2021;
3. Mitwirkung in Arbeitsgruppen der ENISA sowie der NIS-Kooperationsgruppe.

Abs. 4 sieht als Sonderbestimmung vor, dass eine Verordnung nach Abs. 1 über spezifische technische und organisatorische Cybersicherheitsmaßnahmen in Bezug auf Rundfunknetze und die Übertragung von Rundfunksignalen von der KommAustria zu erlassen ist. Klargestellt wird in Abs. 3, dass der RTR-GmbH im Rahmen ihrer Zuständigkeit nach den §§ 194 ff Aufgaben übertragen werden. Sind von diesen Aufgaben nach Abs. 3 Rundfunknetze oder die Übertragung von Rundfunksignalen betroffen, so ist Einvernehmen mit der KommAustria herzustellen.

Zu Artikel 3 (Änderung des Gesundheitstelematikgesetzes 2012)

Zu Z 1 bis 3 (Inhaltsverzeichnis, § 8a, § 26 Abs. 21):

Bei der vorgeschlagenen Änderung handelt es sich um eine erforderliche Anpassung der geltenden Bestimmungen des GTelG 2012 an das NISG 2026.

Abs. 2 stellt klar, dass das Austrian HealthCERT hinkünftig für den Sektor Gesundheitswesen gemäß § 2 Z 5 NISG 2026 die Aufgaben eines sektorspezifischen CSIRT übernehmen soll. Das Austrian HealthCERT hat die Anforderungen, die gemäß § 9 NISG 2026 an ein Computer-Notfallteam gestellt werden mit Ausnahme der Z 8, zu erfüllen. Außerdem soll klargestellt werden, dass die Bestimmungen aus dem NISG 2026, welche sich auf die Ermächtigung der Cybersicherheitsbehörde zur Einrichtung von sektorspezifischen CSIRTS beziehen, nicht zur Anwendung kommen, da das Austrian HealthCERT bereits auf Grundlage des GTelG 2012 besteht. Dass das Austrian HealthCERT die Anforderungen, welche nach dem NISG 2026 an ein sektorspezifisches CSIRT gestellt werden, erfüllt, wird ebenfalls bereits mit der gegenständlichen Novelle des GTelG 2012 sichergestellt. Da das Austrian HealthCERT auch als sektorspezifisches CSIRT iSd NISG 2026 tätig wird, finden des Weiteren die Bestimmungen des NISG 2026, welche sich auf sektorspezifische CSIRTS beziehen, Anwendung.

Die Verarbeitung der Daten erfolgt hierbei auf Grundlage des NISG 2026, weshalb eine Regelung hierzu im GTelG 2012 nicht erforderlich ist.

Mit dem vorgeschlagenen Abs. 3 sollen die wesentliche und wichtige Einrichtungen gemäß den §§ 24 ff NISG 2026, die dem Sektor Gesundheitswesen gemäß § 2 Z 5 NISG 2026 angehören, verpflichtet werden, die Meldungen nach den §§ 34 und 37 NISG 2026 an das Austrian HealthCERT zu erbringen. Die vorgeschlagene Bestimmung tritt an die Stelle der bisherigen Verpflichtung gemäß Abs. 3. Im Gegensatz zur bisherigen Regelung sind nun wesentliche und wichtige Einrichtungen des Sektor Gesundheit nach dem NISG 2026 umfasst, unabhängig davon, ob es sich dabei um Gesundheitsdiensteanbieter im Sinne des § 2 Z 2 GTelG 2012 handelt. Das Austrian HealthCERT ist hierbei das für den Sektor Gesundheitswesen zuständige Computer-Notfallteam. Die Meldepflichten, die sich aus dem NISG 2026 ergeben, werden durch die gegenständliche Meldung an das Austrian HealthCERT erfüllt, sofern es sich um Meldepflichten im Sektor Gesundheit handelt. Andere

Meldepflichten, wie etwa bezogen auf andere Sektoren nach dem NISG 2026, nach der DSGVO, dem Medizinproduktrecht oder anderen Rechtsgebieten, bleiben hiervon unberührt.

Abs. 4 soll den für das Gesundheitswesen zuständigen Bundesminister oder die zuständige Bundesministerin ermächtigen, dem Austrian HealthCERT mit Verordnung weitere Aufgaben zur Gewährleistung der Sicherheit und der Resilienz von Netz- und Informationssystemen im Gesundheitswesen zu übertragen.

Bereits in der derzeitigen Steuerung der Cybersicherheit und der Cyberresilienz im Gesundheitswesen wurde der CSAeH als das strategische Gremium eingerichtet. Mit dem vorgeschlagenen Abs. 5 wird eine gesetzliche Grundlage geschaffen.

Datenschutz-Folgenabschätzung

Systematische Beschreibung der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten öffentlichen Interessen

Der Bundeskanzler, der Bundesminister für Inneres, die Cybersicherheitsbehörde, der Bundesminister für Landesverteidigung, der Bundesminister für europäische und internationale Angelegenheiten und die CSIRTs sind ermächtigt, personenbezogene Daten zu verarbeiten (§ 42 NISG 2026) und einander zu übermitteln. Eine solche Verarbeitung muss entweder zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen und zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit oder zum Zwecke der Erfüllung der rechtlichen Verpflichtungen aufgrund des NISG 2026 bzw. aufgrund innerstaatlicher oder internationaler Amtshilfe (§ 43 Abs. 1, 2 und 3 NISG 2026) erforderlich sein.

Die Kategorien der betroffenen personenbezogenen Daten werden in § 42 Abs. 2 bis 6 NISG 2026 abschließend festgelegt und umfassen

1. Kontakt- und Identitätsdaten,
2. unternehmensbezogene Daten sowie
3. technische Daten.

Da nicht ausgeschlossen werden kann, dass es im Rahmen der Wahrnehmung der Aufgabenerfüllung auch zur Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO und § 39 DSG kommt sowie dem Umstand, dass im Rahmen des § 20 Abs. 3, § 44 Abs. 6 iVm § 21 Abs. 3, § 43 Abs. 1 Z 4 und 5 sowie § 46 Abs. 1 personenbezogene Daten im Sinne des Art. 10 DSGVO bzw. § 4 Abs. 3 DSG verarbeitet werden, wird in Abs. 7 festgelegt, dass besondere Kategorien personenbezogener Daten und Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen verarbeitet werden dürfen, wenn dies zum Zweck der Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen und der Abwehr von Gefahren für die öffentliche Sicherheit unbedingt erforderlich ist.

Zur Analyse von Meldungen über Risiken, Cyberbedrohungen und Cybersicherheitsvorfälle sowie von Erkenntnissen, die gemäß § 17 Abs. 1 und 2 NISG 2026 gewonnen wurden, hat die Cybersicherheitsbehörde gemäß § 18 NISG 2026 ein Meldeanalysesystem zu betreiben. Weiters ist er gemäß § 13 NISG 2026 ausdrücklich ermächtigt, IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen zu betreiben.

Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

Die Notwendigkeit der Verarbeitung, Übermittlung oder Weiterverarbeitung personenbezogener Daten ergibt sich u.a. aus

1. der EU-rechtlichen Verpflichtung in Rahmen der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. Nr. L 333 vom 27.12.2022 S 80,
2. den auf der NIS-2-Richtlinie fußenden im NISG 2026 normierten Pflichten und
3. erheblichem wichtigem öffentlichem Interesse an der Abwehr und raschen Lösung von Cyberangriffen zur Gewährleistung eines hohen nationalen und internationalen Sicherheitsniveaus von Netz- und Informationssystemen.

Risiken

Als Risiken werden insbesondere in ErwGr 85 der DSGVO unter anderem genannt:

- „physische, materielle oder immaterielle Schäden“, „unbefugte Aufhebung der Pseudonymisierung“, „Rufschädigung“, „Identitätsdiebstahl oder -betrug“, „finanzielle Verluste“, „Verlust der Vertraulichkeit bei Berufsgeheimnissen“ oder „erhebliche wirtschaftliche oder gesellschaftliche Nachteile“:

Diese Risiken beziehungsweise Nachteile sind nahezu ausgeschlossen, weil mit den Strafbestimmungen des vierten bis sechsten sowie zweiundzwanzigsten Abschnittes des Besonderen Teiles des Strafgesetzbuches – StGB, BGBL. Nr. 60/1974, sowie den allenfalls anzuwendenden dienstrechtlichen Bestimmungen, wie beispielsweise dem Disziplinarrecht, wirksame Vorkehrungen gegen die unrechtmäßige Verarbeitung von Daten und somit das Entstehen von physischen, materiellen oder immateriellen Schäden bestehen. Wer die jeweiligen Daten missbraucht, geht angesichts der gerichtlichen Strafdrohung selbst ein sehr hohes Risiko ein. Auf die gesetzlichen Geheimhaltungspflichten darf verwiesen werden (vgl. etwa § 46 BDG 1979). Insbesondere ist aufgrund der durchgehenden Protokollierungspflicht (§ 42 Abs. 8) kein Missbrauch der Daten zu erwarten.

- „Verlust der Kontrolle über personenbezogene Daten“:

Diese Risiken werden dadurch verringert, dass Art. 5 Abs. 2 DSGVO als unmittelbar anwendbaren Grundsatz die Rechenschaftspflicht vorsieht. Die oder der Verantwortliche ist also nicht nur für die Einhaltung des Art. 5 Abs. 1 DSGVO verantwortlich, sondern muss auch dessen Einhaltung nachweisen können, was einzelfallbezogen durch entsprechende Protokollierungen sowie Dokumentation erfolgt.

- „Diskriminierung“:

Dieses Risiko ist durch diverse Diskriminierungsverbote ausgeschlossen und können freiwillige Meldungen auch anonym erfolgen (§ 37 Abs. 3 NISG 2026).

- „Einschränkung der Rechte der betroffenen Personen“:

Die Einschränkung der Rechte der betroffenen Personen werden in § 42 Abs. 10 NISG 2026 geregelt und gemessen am Zweck des NISG 2026 eingeschränkt, da nicht aufgrund der Ausübung des Betroffenenrechtes auf Löschung oder Widerspruch (z. B. der IP-Adresse eines Angreifers) die Möglichkeit der Analyse von Bedrohungsszenarien ausgeschlossen werden soll. Die Beschränkung der Rechte der betroffenen Person im notwendigen und verhältnismäßigen Ausmaß liegt im allgemeinen öffentlichen Interesse und stellt sicher, dass die Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen und zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit möglich ist.

Abhilfemaßnahmen

Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in ErwGr 78 der DSGVO unter anderem genannt:

- „Minimierung der Verarbeitung personenbezogener Daten“ und „Verwendungsbeschränkung“:

Grundsätzlich ist festzuhalten, dass nur ein sehr eingeschränkter Personenkreis Zugang zu personenbezogenen Daten hat, wobei die Verarbeitung bereits durch Art. 5 Abs. 1 Buchstabe c DSGVO eingeschränkt wird.

- „schnellstmögliche Pseudonymisierung personenbezogener Daten“ (siehe auch ErwGr 28 DSGVO):

Die gesetzlichen Bestimmungen stehen einer Pseudonymisierung der erhobenen personenbezogenen Daten durch den Verantwortlichen, soweit die Auflösung des Personenbezuges durch geeignete technische Mittel möglich und gemäß den Grundsätzen in Art. 5 Abs. 1 DSGVO geboten ist, nicht entgegen.

- „Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten“ und „Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen“:

Durch die explizite gesetzliche Regelung der Datenverarbeitung sowie deren Zwecke wird den Anforderungen der Transparenz bereits durch die Kundmachung in hohem Maße Rechnung getragen. Gleichermaßen gilt für die sich unmittelbar aus dem Grundsatz der Rechenschaftspflicht ergebende Protokollierung sowie Dokumentation. Durch die Benennung einer oder eines jeweils zuständigen Datenschutzbeauftragten oder nötigenfalls auch mehrerer Datenschutzbeauftragter gemäß Art. 37 bis 39 DSGVO wird eine direkte Ansprechperson deklariert, der betroffene Personen unter Wahrung der Geheimhaltung und der Vertraulichkeit zu allen Angelegenheiten, die mit der Verarbeitung ihrer

personenbezogener Daten und besonderer Kategorien personenbezogener Daten oder mit der Wahrnehmung ihrer Rechte im Zusammenhang stehen, Fragen stellen können. Außerdem wird durch das gemäß Art. 30 DSGVO zu führende Verzeichnis von Verarbeitungstätigkeiten, das der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist, dargestellt, welche Verarbeitungstätigkeiten jeweils vorgenommen werden und der jeweiligen Zuständigkeit unterliegen.

– „**Datensicherheitsmaßnahmen**“ (ErwGr 83 DSGVO):

Die Verantwortlichen der IKT-Lösungen gemäß §§ 17 bis 19 NISG 2026 sind gemäß Art. 32 DSGVO verpflichtet dem Stand der Technik entsprechende Maßnahmen zu setzen.

Ergebnis

Grundsätzlich bestehen gewisse Risiken, allerdings ist deren Eintritt einerseits nicht sehr wahrscheinlich und sind andererseits zahlreiche, wirksame und auf den jeweiligen Einzelfall bezogene Abhilfemaßnahmen vorgesehen. Das Risiko für die wesentliche Beeinträchtigung öffentlicher Interessen und auch der Datensicherheit im nationalen und internationalen Bereich bei einem Null-Szenario ist extrem erhöht, sodass die Datenschutz-Folgenabschätzung klar positiv ausfällt.