2638 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP

Bericht

des Ausschusses für innere Angelegenheiten

über den Antrag 4129/A der Abgeordneten Dr. Christian Stocker, David Stögmüller, Kolleginnen und Kollegen betreffend ein Bundesgesetz, mit dem ein Netz- und Informationssystemsicherheitsgesetz 2024 erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden

Die Abgeordneten Dr. Christian **Stocker**, David **Stögmüller**, Kolleginnen und Kollegen haben den gegenständlichen Initiativantrag am 13. Juni 2024 im Nationalrat eingebracht und wie folgt begründet:

„I. Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs

Mit diesem Bundesgesetz sollen das Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 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 abbilden 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 vom 20. Mai 2021 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 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), 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 2024 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 2024):

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 und die Aufgaben der Cybersicherheitsbehörde, der Computer-Notfallteams (CSIRTs), der unabhängigen Stellen und der unabhängigen Prüfer. Ferner werden die nationale 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 Verwaltungsstraftatbestände 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), BGBl. 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 B-VG,
- ‚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 Vollziehung zuständig sind, beruht die Zuständigkeit des Bundes auf der in § 1 des Gesetzesentwurfs geschaffenen Kompetenzgrundlage, welche im Wesentlichen jener der in § 1 NISG entspricht.

Besonderheiten des Normerzeugungsverfahrens:

Der Entwurf kann im Hinblick auf Artikel 1 (§§ 1, 46 Abs. 2 und 51 Abs. 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 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.

II. Besonderer Teil

Zu Artikel 1: Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024)

Zu § 1 (Verfassungsbestimmung)

Die Vorschriften in diesem Bundesgesetz, mit dem insbesondere die NIS-2-Richtlinie umgesetzt werden soll, fallen überwiegend gemäß Art. 10 B-VG in die Gesetzgebungs- und Vollziehungszuständigkeit des Bundes.

In den folgenden (Teil-)Sektoren fällt jedoch die Umsetzung der NIS-2-Richtlinie gemäß Art. 11 B-VG in die Vollziehungszuständigkeit der Länder bzw. gemäß Art. 12 B-VG in die Ausführungsgesetzgebungs- und Vollziehungszuständigkeit der Länder oder gemäß Art. 15 Abs. 1 B-VG in die Gesetzgebungs- und Vollziehungszuständigkeit der Länder:

Der Teilsektor ‚Elektrizität' fällt – ausgenommen länderübergreifende Starkstromleitungen – unter den Kompetenztatbestand ‚Elektrizitätswesen, soweit es nicht unter Art. 10 fällt' (Art. 12 Abs. 1 Z 5 B-VG) und ist somit in Ausführungsgesetzgebung und Vollziehung Landessache.

Der Teilsektor ‚Straßenverkehr' fällt unter den Kompetenztatbestand ‚Straßenpolizei' (Art. 11 Abs. 1 Z 4 B-VG) und ist somit in Vollziehung Landessache.

Der Teilsektor ‚Schifffahrt' fällt, soweit sie sich auf die Binnenschifffahrt – ausgenommen Donau, Bodensee, Neusiedlersee und auf Grenzstrecken sonstiger Grenzgewässer – bezieht, unter den Kompetenztatbestand ‚Binnenschifffahrt hinsichtlich Schifffahrtsanlagen' bzw. ‚Strom- und Schifffahrtspolizei auf Binnengewässern' (Art. 11 Abs. 1 Z 6 B-VG) und ist somit in Vollziehung Landessache.

Der Sektor ‚Gesundheitswesen' fällt, soweit es sich um Krankenanstalten handelt, unter den Kompetenztatbestand ‚Heil- und Pflegeanstalten' (Art. 12 Abs. 1 Z 1 B-VG) und ist somit in Ausführungsgesetzgebung und Vollziehung Landessache, soweit es sich aber um das Rettungswesen handelt, in die Gesetzgebungs- und Vollziehungszuständigkeit der Länder (Art. 15 Abs. 1 B-VG).

Jene neuen (Teil-)Sektoren, die durch die NIS-2-Richtlinie erfasst sind, wie beispielsweise der Teilsektor ‚Fernwärme- und kälte' oder der Sektor ‚Abfallbewirtschaftung', fallen zum Teil in die Gesetzgebungs- und Vollziehungszuständigkeit der Länder (Art. 15 Abs. 1 B-VG).

Ausgehend von dieser Beurteilung ergibt sich, dass die Vorschriften in diesem Bundesgesetz zwar überwiegend gemäß Art. 10 Abs. 1 B-VG in die Gesetzgebungs- und Vollziehungskompetenz des Bundes fallen, in einigen (Teil-)Sektoren fällt die Umsetzung jedoch in die (Ausführungs-)Gesetzgebung

und/oder in die Vollziehung der Länder, weshalb die Begründung einer Kompetenz des Bundes für diese Bereiche verpflichtend einer Verfassungsänderung bedarf.

Vor dem Hintergrund, dass eine statische Kompetenzdeckungsklausel, die lediglich die Erlassung und Aufhebung (sowie die Vollziehung) von Vorschriften zur Bundessache erklärt, jedoch keine Ermächtigung des Bundes zur Änderung dieser Bestimmungen enthält, zur Folge hätte, dass jede auch noch so geringfügige Novelle zum jeweiligen Bundesgesetz (zB Beseitigung von Vollzugsdefiziten) wiederum einer gesonderten Verfassungsänderung bzw. im Verfassungsrang stehenden Kompetenzdeckungsklausel bedürfte (vgl. auch *Janko*, Staats- und Verwaltungsorganisation [2014] 9), soll das gegenständliche Gesetz in Abs. 1 eine dynamische Kompetenzdeckungsklausel enthalten, die auch die Änderung von Vorschriften, wie sie in diesem Bundesgesetz enthalten sind, umfassen soll. Zudem soll abweichend von Art. 102 Abs. 1 B-VG ausdrücklich angeordnet werden, dass die in diesem Bundesgesetz geregelten Angelegenheiten – sofern nicht im Einzelfall (einfachgesetzlich) eine gegenteilige Anordnung erfolgt (vgl. § 44 Abs. 1) – in unmittelbarer Bundesverwaltung besorgt werden können.Zur unionsrechtskonformen Umsetzung dieser Vorgaben ist es zwingend erforderlich, dass der Bundesminister für Inneres seine 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). Nach der Rechtsprechung des VfGH sind oberste Organe jedoch gegenüber keinem anderen Organ weisungsgebunden und besteht keine sachlich in Betracht kommende Oberbehörde (vgl. VfGH 11.3.1959, B 179/58). Oberste Organe dürfen zudem nicht an Willenserklärungen anderer Organe gebunden werden (vgl. VfSlg. 19.827/2013) und darf die Kontrolle der Rechtmäßigkeit des Handelns eines obersten Organes nicht einer anderen Verwaltungsbehörde übertragen werden (vgl. VfSlg. 13.626/1993). Folglich bedarf es für die – unionsrechtlich verpflichtend vorgesehene – Aufsichts- und Durchsetzungsbefugnisse des Bundesministers für Inneres gegenüber obersten Organen einer entsprechenden verfassungsrechtlichen Grundlage, die mit Abs. 2 geschaffen werden soll. Demnach soll der Bundesminister für Inneres als Cybersicherheitsbehörde (in Anlehnung an die Regelung in § 35 Abs. 2 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999) dazu ermächtigt sein, seine Befugnisse nach diesem Bundesgesetz auch gegenüber den in Art. 19 B-VG genannten obersten Organen der Vollziehung auszuüben, soweit in diesem Bundesgesetz nicht anderes bestimmt ist. Wesentlich ist, dass damit kein Weisungsrecht des Bundesministers für Inneres gegenüber obersten Organen der Vollziehung verbunden sein soll.

Vor dem Hintergrund, dass es aufgrund der in Abs. 1 vorgesehenen dynamischen Kompetenzdeckungsklausel zu einer Kompetenzverschiebung zu Gunsten des Bundes kommt, sollen gemäß Abs. 3 Änderungen der Bestimmungen gemäß §§ 17, 24 Abs. 2 Z 2, Abs. 3 und 5, § 44 Abs. 1, § 45 Abs. 5 sowie § 46 nur mit Zustimmung der Länder kundgemacht werden dürfen, sofern sich diese Änderungen auf Behörden und sonstige Stellen der öffentlichen Verwaltung der Länder, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, beziehen. Sollten geplante Änderungen der in der Norm angeführten Bestimmungen die Interessen der Länder betreffen, ist demnach die formelle Zustimmung der Länder eine Voraussetzung für das verfassungsmäßige Zustandekommen dieser bundesgesetzlichen Regelungen (Art. 42a B-VG; vgl. auch zB Art. 102 Abs. 1 und 4 B-VG). Damit wird in diesem Zusammenhang ein ausreichendes Mitspracherecht der Länder sichergestellt. Festgehalten wird, dass die Einbeziehung der Länder durch den Bund bereits in die Vorbereitung von Gesetzesvorhaben angesichts ihrer Betroffenheit regelmäßig angezeigt sein wird.

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 (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 S. 15 vom 17.04.2019 textuell übernommen:

‚Cybersicherheit' (dort: Art. 2 Nr. 1), ‚IKT-Produkt' (Art. 2 Nr. 12), ‚IKT-Dienst' (Art. 2 Nr. 13), ‚IKT-Prozess' (Art. 2 Nr. 14) und ‚Cyberbedrohung' (Art. 2 Nr. 8).

Folgende Begriffe werden aus der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 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 übernommen: ‚Vertrauensdienst' (dort: Art. 3 Nr. 16), Vertrauensdiensteanbieter (Art. 3 Nr. 19) und qualifizierter Vertrauensdiensteanbieter (Art. 3 Nr. 20), ‚Qualifizierte elektronische Signaturerstellungseinheit' (dort: Art. 3 Nr. 23), ‚Qualifizierte elektronische Siegelerstellungseinheit' (dort: Art. 3 Nr. 32), ‚Konformitätsbewertungsstelle' (Art. 3 Nr. 18), ‚vertrauenswürdige Systeme eines Vertrauensdiensteanbieters' (dort: Art. 24 Abs. 2 Buchstabe e und f).

Die Begriffsbestimmungen von ‚Online-Marktplatz', ‚Online-Suchmaschine' und ‚Cloud-Computing', ‚Internet-Knoten', ‚Rechenzentrumsdienste', ‚Content Delivery Network' und ‚Forschungseinrichtung' werden in der Anlage 1 definiert, da auf diese Begriffe im Gesetz nicht Bezug genommen wird.

‚Netz- und Informationssysteme' (Z 1; Art. 6 Nr. 1 NIS-2-Richtlinie) sind Kommunikationsnetze, wie sie auch in § 4 Z 1 des Telekommunikationsgesetzes 2021 (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 Nr. 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 Nr. 3 NIS-2-Richtlinie) umfasst die Cybersicherheit im Sinne des Art. 2 Nr. 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 Nr. 36 NIS-2-Richtlinie) im Sinne des § 4 Z 9 des Telekommunikationsgesetzes 2021 (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 Nr. 37 NIS-2-Richtlinie) umfasst Kommunikationsdienste im Sinne des § 4 Z 4 des Telekommunikationsgesetzes 2021 (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 Nr. 2 der Verordnung (EU) 2015/2120 ‚Internetzugangsdienste' im Sinne der Begriffsbestimmung des Artikels 2 Abs. 2, Nr. 2 der Verordnung (EU) 2015/2120,
- 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 Nr. 37 NIS-2-Richtlinie identisch.

Der Begriff ‚IKT-Produkt' (Z 6; Art. 6 Nr. 12 NIS-2-Richtlinie) im Sinne des Art. 2 Nr. 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 Nr. 13 NIS-2-Richtlinie) im Sinne des Art. 2 Nr. 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 Nr. 14 NIS-2-Richtlinie) im Sinne des Art. 2 Nr. 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 Nr. 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 Nr. 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 natürliche oder juristische Personen oder Personengesellschaften, die in eigenem Namen Rechte ausüben und Pflichten unterliegen können (Rechts- und Handlungsfähigkeit).

Der Begriff ‚Leitungsorgan' (Z 11) beschreibt eine oder mehrere natürliche Personen, die nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte einer Einrichtung oder innerhalb der Einrichtung zur Überwachung der Geschäftsführung berufen sind. Leitungsorgane wesentlicher und wichtiger Einrichtungen sind gemäß Art. 20 NIS-2-Richtlinie durch die Mitgliedstaaten unmittelbar zu verpflichten, die zur Einhaltung von Art. 21 NIS-2-Richtlinie ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen, ihre Umsetzung zu überwachen und sicherzustellen, dass diese für Verstöße gegen diese Verpflichtungen durch die betreffenden Einrichtungen verantwortlich gemacht werden können.

Im Bereich der öffentlichen Verwaltung wird sich die Einstufung als Einrichtung von der Funktion als Leitungsorgan häufig nicht trennen lassen, sofern Einrichtung und Leitungsorgan eine Einheit bilden. So kann beispielsweise ein Bundesminister als wesentliche Einrichtung im Sinne dieses Bundesgesetzes einzustufen sein und wäre dieser zusätzlich als Leitungsorgan zu qualifizieren.

Eine Legaldefinition für ‚Leitungsorgane' fehlt in der NIS-2-Richtlinie. Die Richtlinie verfolgt das Ziel, Cybersicherheit zu einer der zentralen Agenden der Leitung und der Geschäftsführung von wesentlichen und wichtigen Einrichtungen zu machen. Leitungsorgane sind in die Risikomanagementmaßnahmen einzubeziehen, haben diese zu genehmigen und deren Umsetzung zu überwachen. In Ermangelung einer Legaldefinition in der NIS-2-Richtlinie, wird diese im Bundesgesetz national ergänzt.

Die Definition des Bundesgesetzes zielt darauf ab, die tatsächliche Leitungs- und Geschäftsführungsebene zu erfassen. Aus diesem Grund ist die Vertretungsbefugnis bewusst nicht als Kriterium angeführt und wird stattdessen an die Geschäftsführung und die Überwachung der Geschäftsführung angeknüpft. 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 oder zur Überwachung der Geschäftsführung berufen ist. Ein Leitungsorgan wäre etwa der Vorstand, der Geschäftsführer oder der Aufsichtsrat der jeweiligen Einrichtung.

Der Begriff ‚DNS-Diensteanbieter' (Domainnamensystem – DNS) (Z 12; Art. 6 Nr. 20 NIS-2-Richtlinie) bezeichnet Einrichtungen, die öffentlich zugängliche rekursive Dienste zur Auflösung von Domänennamen für Internet-Endnutzer oder autoritative Dienste zur Auflösung von Domänennamen 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, der eine bestimmte Domäne oberster Stufe (Top Level Domain – TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domänennamen 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 Nr. 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 Nr. 16 NIS-2-Richtlinie) sind juristische Personen oder eingetragene Personengesellschaften, die einen digitalen Dienst im Sinne des § 3 Z 1 E-Commerce-Gesetz (ECG) 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 Nr. 24 NIS-2-Richtlinie) im Sinne des Art. 3 Nr. 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 diese Dienste betreffenden Zertifikaten oder
- Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder
- Bewahrung von diese Dienste 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 Nr. 25 NIS-2-Richtlinie). Hingegen versteht man unter einem ‚qualifizierten Vertrauensdienstanbieter' (Z 18; Art. 6 Nr. 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 Nr. 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 Nr. 32 der Verordnung (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 Buchstabe e und f der Verordnung (EU) Nr. 910/2014 entsprechen.

‚Anbieter verwalteter Dienste' (Managed Service Provider, Z 23; Art. 6 Nr. 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 Nr. 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 Nr. 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 Nr. 40 NIS-2-Richtlinie nach § 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 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl. L 333 vom 27.12.2022 S. 164 (im Folgenden: Richtlinie (EU) 2022/2557).

Der Begriff ‚Risiko' (Z 26; Art. 6 Nr. 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 Nr. 10 NIS-2-Richtlinie) im Sinne des Art. 2 Z 8 der Verordnung (EU) Nr. 2019/881 (Rechtsakt 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 Nr. 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 Nr. 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 Nr. 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 großes Ausmaßes' (Z 31; Art. 6 Nr. 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 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 nach 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 nach 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 § 4 (Cybersicherheitsbehörde)

Art. 8 Abs. 1 und 2 der NIS-2-Richtlinie sieht vor, dass Mitgliedstaaten eine oder mehrere Behörden für die Cybersicherheit und die in Kapitel VII der NIS-2-Richtlinie genannten Aufsichtsaufgaben zuständiger

Behörden benennt oder sie einrichtet, welche die Anwendung dieser Richtlinie auf nationaler Ebene überwachen. § 4 setzt Art. 8 Abs. 1 NIS-2-Richtlinie um und richtet eine Cybersicherheitsbehörde ein.

Während das NISG noch eine Aufgabenverteilung auf zwei Behörden (eine strategische und eine operative NIS-Behörde) vorsah, werden diese Aufgaben nunmehr von einer Behörde wahrgenommen. Die bisherige Aufteilung der ‚strategischen' Angelegenheiten der Netz- und Informationssystemsicherheit auf den Bundeskanzler und der ‚operativen' Angelegenheiten auf den Bundesminister für Inneres setzte einen ständigen Dialog zur Aufgabenerfüllung voraus. Die Erfahrungen anderer Mitgliedstaaten, in denen die behördlichen Aufgaben der NIS-1-Richtlinie auf mehr als eine Behörde verteilt waren, haben gezeigt, dass ein erhöhter Verwaltungsaufwand durch ressortübergreifende Prozesse erzeugt wird und diese Aufteilung einer effizienten Aufgabenerfüllung entgegenstehen kann. Hinzu kommt, dass Parallelstrukturen einerseits aus budgetärer Sicht, andererseits auch in Hinblick auf den Fachkräftemangel im Bereich der IT-Sicherheit hintangehalten werden sollten. Die Vereinigung der Aufgaben im Bereich der Netz- und Informationssystemsicherheit nach der NIS-2-Richtlinie innerhalb einer Behörde erscheint daher zweckmäßig.

Die Cybersicherheitsbehörde übernimmt somit 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. 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 der Kooperationsgruppe, 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 sowie Beaufsichtigung von CSIRTs gemäß § 8 Abs. 2 und § 10;
12. Zulassung sowie Kontrolle der Einhaltung der Erfordernisse unabhängiger Stellen und unabhängiger Prüfer gemäß § 7;
13. Ausübung der Aufsichts- und Durchsetzungsmaßnahmen gegenüber wesentlichen und wichtigen Einrichtungen gemäß den §§ 38 und 39;
14. Entgegennahme, Analyse und Weiterleitung von Meldungen gemäß § 34, § 37 sowie gemäß § 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; § 14) erstellt und durch die Bundesregierung erlassen. Die Koordination der Erstellung erfolgt durch die Cybersicherheitsbehörde.

Sowohl die strategische als auch die operativen Koordinierungsstrukturen (§§ 12 bis 14) werden vom Bundesminister für Inneres 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 §§ 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 (anderen Mitgliedstaaten, NIS-Kooperationsgruppe und CSIRTs-Netzwerk) betrieben.

Der Bundesminister für Inneres betreibt das bei ihm eingerichtete GovCERT (§ 8 Abs. 4). Ferner übernimmt er die Aufgaben der Ermächtigung und Beaufsichtigung von allen CSIRTs (§ 8 Abs. 2).

Unabhängige Stellen und unabhängige Prüfer werden durch die Cybersicherheitsbehörde zugelassen und die Einhaltung der Erfordernisse kontrolliert (§ 7). In diesem Zusammenhang legt der Bundesminister für Inneres durch Verordnung Erfordernisse und Kriterien sowie das Verfahren zur Zulassung von unabhängigen Stellen und unabhängigen Prüfern 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. §§ 12ff, 20).

Mit dem Abs. 2 wird das Verhältnis der Cybersicherheitsbehörde zu jener Behörde, die in Durchführung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates und vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU)

2016/1011, ABl. Nr. 333 vom 27.12.2022 S. 1 (Verordnung 2022/2554), die innerstaatlich zuständige Behörde ist, geregelt. Da die Verordnung 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 2022/2554 innerhalb des dortigen Anwendungsbereichs als zuständige Behörde gilt.

Abs. 3 sieht vor, dass der Bundesminister für Inneres den jährlichen Bericht zur Cybersicherheit dem National- und Bundesrat vorzulegen hat. Zusätzlich erstellt der Bundesminister für Inneres eine Übersicht in anonymisierter Form über die eingelangten Meldungen nach § 34 (Berichtspflichten) und § 37 (Freiwillige Meldung relevanter Informationen) gegliedert nach Sektoren sowie die Höhe des Aufwandsersatzes gemäß § 8 Abs. 6 und legt diese Informationen dem Bericht zur Cybersicherheit bei. Dies dient der Information der Legislativorgane.

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 jährlichen 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 gem. Art. 7 Abs. 1 Buchstabe. i und Abs. 4 der Verordnung (EU) 2021/887 sollten in strukturierter Form erfolgen, um eine rasche Bearbeitung zu ermöglichen. Daher können seitens der Cybersicherheitsbehörde gewisse Modalitäten zur Antragstellung vorgesehen werden.

Zu § 7 (Unabhängige Stellen und unabhängige Prüfer)

Mit § 7 soll das im NISG bestehende Institut der qualifizierten Stellen mit systemischen Anpassungen in das neue NISG 2024 überführt werden, zumal sich dieses in der Vergangenheit gut bewährt hat, und sollen die Aufgaben und Befugnisse der unabhängigen Stellen an die Anforderungen der NIS-2-Richtlinie angepasst werden.

Demnach sollen gemäß Abs. 1 als ‚unabhängige Stellen' juristische Personen oder eingetragene Personengesellschaften mit Niederlassung in Österreich definiert werden, die sich zur Prüfung der Risikomanagementmaßnahmen wesentlicher und wichtiger Einrichtungen gemäß § 33 Abs. 2 und 3 zumindest eines unabhängigen Prüfers (vgl. dazu die Erläuterungen zu Abs. 5) zu bedienen haben.

Gemäß Abs. 2 soll die Zulassung als unabhängige Stelle durch Bescheid der Cybersicherheitsbehörde erfolgen, sofern die in einer Verordnung des Bundesministers für Inneres festzulegenden Anforderungen gemäß Abs. 9 Z 1 erfüllt sind, und sollen der Cybersicherheitsbehörde zur Überprüfung der Einhaltung dieser Anforderungen entsprechende Aufsichtsmaßnahmen, wie sie im vorgeschlagenen § 38 Abs. 1 in Bezug auf wesentliche und wichtige Einrichtungen vorgesehen sind, zukommen.

Werden die Anforderungen gemäß Abs. 9 Z 1 nicht eingehalten, soll die Cybersicherheitsbehörde gemäß Abs. 3 verpflichtet sein, die Zulassung als unabhängige Stelle bescheidmäßig zu widerrufen, es sei denn, die Nichteinhaltung der Anforderungen liegt außerhalb des Einflussbereichs der betreffenden unabhängigen Stelle (zB höhere Gewalt). Um Missbrauch hintanzuhalten, soll im Falle eines bescheidmäßigen Widerrufs für die unabhängige Stelle eine ‚Sperrfrist' von einem Jahr ab Rechtskraft des Bescheides vorgesehen werden und soll demnach erst nach Ablauf dieser Sperrfirst ein neuerlicher Antrag gemäß Abs. 2 gestellt werden können.

Wesentlich ist, dass unabhängige Stellen dazu verpflichtet sein sollen, als unabhängige Prüfer nur solche natürlichen Personen einzusetzen, die von der Cybersicherheitsbehörde gemäß Abs. 5 zugelassen wurden (Abs. 4).

Hintergrund dieser Bestimmung ist Folgender: Gemäß § 3 der Verordnung über qualifizierte Stellen (QuaSteV), BGBl. II Nr. 226/2019, haben qualifizierte Stellen ‚befähigte sicherheitsüberprüfte Prüfer' einzusetzen. Die Anforderungen an diese Prüfer sind in § 4 QuaSteV geregelt. Die Erfüllung dieser Anforderungen sind derzeit durch die qualifizierte Stelle gegenüber dem Bundesminister für Inneres bei der Antragstellung nachzuweisen, welcher diese ausschließlich im Rahmen des § 18 Abs. 1 NISG prüfte. Die fehlende Eignung eines Prüfers konnte sich daher ausschließlich auf die Eignung (oder Nichteignung) der unabhängigen Stelle (nicht aber auf den Prüfer selbst) auswirken. Das Institut der qualifizierten Stellen war daher dahingehend zu überarbeiten, dass auch die Erfüllung der Voraussetzungen zur Aufnahme der Tätigkeit eines Prüfers durch die Cybersicherheitsbehörde überprüft werden kann. Dies erlaubt eine durchgängige Qualitätskontrolle, die im Hinblick auf die verantwortungsvolle Aufgabe der unabhängigen Prüfer notwendig ist.

Vergleichbare Prüfsysteme, in denen einzelne Stellen bzw. Prüfer zwischen den normunterworfenen Einrichtungen und der Behörde zwischengeschaltet sind, finden sich etwa im Wirtschaftstreuhandberufsgesetz 2017 (WTBG 2017), BGBl. I Nr. 137/2017, im Abschlussprüfer-Aufsichtsgesetz (APAG), BGBl. I Nr. 83/2016, im Umweltmanagementgesetz (UMG), BGBl. I Nr. 96/2001, oder in der Fachkundebeurteilungsverordnung (FachKBV), BGBl. II Nr. 37/2007.

In Abs. 5 soll festgelegt werden, welche Voraussetzungen für die Zulassung als unabhängiger Prüfer vorliegen müssen. So soll der Antragsteller gemäß Z 1 über eine vor nicht länger als drei Jahren durchgeführte Sicherheitsüberprüfung auf begründetes Ersuchen einer unabhängigen Stelle oder sonstigen Einrichtung nach §§ 55 ff des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991, für den Zugang zu geheimer Information nachzuweisen haben. Weiters soll der Antragsteller gemäß Z 2 über ein österreichisches Reifeprüfungszeugnis, ein österreichisches Diplomprüfungszeugnis, ein österreichisches Zeugnis über die Berufsreifeprüfung über einschlägige berufliche Qualifikation oder diesen durch völkerrechtliche Vereinbarung gleichwertige Zeugnisse verfügen. Diese Bestimmung orientiert sich an § 64 des Universitätsgesetzes 2002 (UG) BGBl. I Nr. 120/2002. Der Nachweis über eine einschlägige berufliche Qualifikation durch ein Zeugnis gemäß § 26 Berufsausbildungsgesetz – BAG, BGBl. Nr. 142/1969, als erbracht gilt. Nach Z 3 soll zudem eine facheinschlägige Berufserfahrung von mindestens drei Jahren im Ausmaß von zumindest zwanzig Wochenstunden im Bereich der Überprüfung von oder Beratung in verantwortlicher Position über Informationssicherheitsmanagementsystemen, Cybersicherheitsmanagementsystemen und Sicherheitslösungen im IT-/OT-Umfeld. Gemäß Z 4 soll zudem erforderlich sein, dass der Antragsteller gegenüber der Cybersicherheitsbehörde seine Eignung zur Überprüfung der Umsetzung von Risikomanagementmaßnahmen durch den Nachweis ausreichender theoretischer Fachkenntnisse sowie ausreichender praktischer Fähigkeiten in organisatorischer und technischer Hinsicht nachgewiesen hat. Der Bundesminister für Inneres soll mit Verordnung nähere Regelungen zum Verfahren und zu den Inhalten des Eignungsnachweises festlegen können (Abs. 9 Z 2).

Wesentlich ist, dass sämtliche Voraussetzungen gemäß Abs. 5 Z 1 bis 4 im Zeitpunkt der Entscheidung kumulativ vorliegen müssen und demnach ein Antrag gemäß Abs. 5 durch Bescheid zurück- oder abzuweisen sein soll, wenn die normierten Voraussetzungen nicht vorliegen oder erbracht werden können.

Da davon auszugehen ist, dass nicht nur für die Erteilung der Zulassung praktische Erfahrung maßgeblich ist, sondern auch für die ordnungsgemäße weitere Ausübung der Funktion als unabhängiger Prüfer, wird in Abs. 6 vorgeschlagen, die Zulassung zu entziehen, wenn der Betroffene in einem Zeitraum von fünf Jahren nicht für die Durchführung von zumindest zwei Prüfungen von wesentlichen oder wichtigen

Einrichtungen (§ 33 Abs. 2 und 3) herangezogen wurde (Z 1) oder der Cybersicherheitsbehörde im Rahmen ihrer Aufsichtsmaßnahmen erkennbar wird, dass der unabhängige Prüfer nicht mehr über die nötigen Fertigkeiten und Fähigkeiten zur Prüfung der Umsetzung der Risikomanagementmaßnahmen verfügt, was insbesondere dann der Fall sein wird, wenn er im Zusammenhang mit Prüfungen wiederholt mangelhaft vorgegangen ist (Z 2).

In diesen Fällen und auch, wenn die Durchführung der Sicherheitsüberprüfung gemäß Abs. 5 Z 1 mehr als drei Jahre zurückliegt, soll die Cybersicherheitsbehörde die Zulassung als unabhängiger Prüfer zu widerrufen haben (Z 3).

Nach einem Widerruf der Zulassung soll die betroffene natürliche Person erst nach Ablauf eines Jahres ab Rechtskraft des Widerrufs einen neuerlichen Antrag auf Zulassung als unabhängiger Prüfer stellen können.

Die Cybersicherheitsbehörde soll gemäß Abs. 7 eine Liste mit den zugelassenen unabhängigen Stellen und unabhängigen Prüfern zu führen und wesentlichen und wichtigen Einrichtungen sowie unabhängigen Stellen in geeigneter Weise zur Verfügung zu stellen haben. Diese Liste soll es wesentlichen und wichtigen Einrichtungen bzw. unabhängigen Stellen erlauben, aus den zugelassenen unabhängigen Stellen bzw. aus den zugelassenen unabhängigen Prüfern frei wählen zu können.

Wesentlich ist, dass die Cybersicherheitsbehörde an das Ergebnis einer externen Überprüfung durch unabhängige Stellen bzw. unabhängige Prüfer nicht gebunden sein soll, sondern soll dieses als Teil ihrer Entscheidungsgrundlage der freien Beweiswürdigung unterliegen. Die abschließende Beurteilung der gemäß § 33 Abs. 2 und 3 umgesetzten Risikomanagementmaßnahmen soll demnach allein der zuständigen Cybersicherheitsbehörde obliegen.

Gemäß Abs. 8 sollen unabhängige Prüfer über bekanntgewordene Tatsachen und Erkenntnisse, die im Rahmen der Prüfung der Umsetzung von Risikomanagementmaßnahmen auftreten und deren Geheimhaltung im Interesse der jeweiligen geprüften Einrichtungen geboten ist, zur Verschwiegenheit verpflichtet sein. Dies soll auch für Personen gelten, denen im Zuge ihrer Tätigkeit bei einer unabhängigen Stelle solche Tatsachen und Erkenntnisse bekanntwerden.

In Abs. 9 soll eine Verordnungsermächtigung des Bundesministers für Inneres zur Festlegung der Anforderungen an unabhängige Stellen (Z 1) sowie der Inhalte des Eignungsnachweises gemäß Abs. 5 Z 4 vorgesehen werden. Gemäß Z 3 soll der Bundesminister für Inneres zudem Pauschalsätze für die Zulassung als unabhängige Stelle oder als unabhängiger Prüfer festlegen können, die dem durchschnittlichen Aufwand der jeweiligen Zulassung entsprechen.

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, sind ein oder mehrere Computer-Notfallteams, auch CSIRTs (Cybersecurity Incident Response Teams) genannt, einzurichten. Diese unterliegen der Aufsicht des Bundesministers für Inneres (§ 10).

Die CSIRTs sind mit der Bewältigung von Cybersicherheitsvorfällen betraut. Zu den Hauptaufgaben der CSIRTs zählen auch die Entgegennahme von Meldungen gemäß §§ 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 nach § 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) – z. B. 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, sind sie, sofern es sich dabei um private Einrichtungen handelt, für diese Tätigkeiten als Beliehene anzusehen. CSIRTs können grundsätzlich auch bei einer Behörde eingerichtet werden, wenn dies für einen bestimmten Sektor sinnvoll erscheint. Die Feststellung der Eignung und die Erteilung der Ermächtigung erfolgt mittels konstitutiven Bescheids. Wird dieser Bescheid befristet erlassen, so ist die Eignung vor einer neuerlichen Erlassung neuerlich zu prüfen. Unabhängig von einer solchen Befristung kann die Cybersicherheitsbehörde diese Ermächtigung beim Wegfall der Anforderungen (vgl. § 10 Abs. 7) widerrufen.

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 (z. B. 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 (z. B. 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 CSIRTs 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 beim Bundesminister für Inneres eingerichtete GovCERT die Aufgaben eines sektorspezifischen CSIRTs für Behörden und sonstige Stellen der öffentlichen Verwaltung, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen (sowohl auf Bundes-, Landes- und Gemeindeebene), wahrzunehmen haben.

Die Entscheidung über die Ermächtigung des nationalen und etwaiger sektorenspezifischer CSIRTs sind vom Bundesminister für Inneres in geeigneter Form (z. B. 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. 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 sektorenspezifischen 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 anonymer 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 (z. B. 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 der §§ 42, 43 werden auch für CSIRTs explizite datenschutzrechtliche Grundlagen geschaffen. Im Kontext dieser Bestimmungen ist auch auf ErwGr 49 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 vom 4.5.2016 S. 1 (Datenschutz-Grundverordnung; 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.

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 Abs. 1 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 dem Bundesminister für Inneres 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 nach § 11 Abs. 1

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

Mitarbeiter von CSIRTs sind über bekanntgewordene Tatsachen und Erkenntnisse, die im Rahmen der Wahrnehmung der Aufgaben nach § 8 auftreten und deren Geheimhaltung im Interesse der jeweiligen geprüften Einrichtungen geboten ist, zur Verschwiegenheit verpflichtet (Abs. 4).

Zu § 10 (Aufsicht)

Die Aufsicht der gemäß § 8 Abs. 2 oder 3 eingerichteten CSIRTs liegt bei dem Bundesminister für Inneres. In Ausübung dieses Aufsichtsrechts hat dieser ein Weisungsrecht gegenüber den CSIRTs. Der Bundesminister für Inneres ist ebenso ermächtigt, 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 Vertrauensdienstegesetz (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 jährlichen 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 jährlichen Berichts zur Cybersicherheit;
4. Erstellung einer eigenen Geschäftsordnung.

Die CSS setzt sich aus je einem zur selbstständigen Behandlung von Angelegenheiten ermächtigten fachkundigen Vertreterder dem Nationalen Sicherheitsrat angehörenden Bundesminister (§ 3 Abs. 1 des Bundesgesetzes über die Errichtung eines Nationalen Sicherheitsrates, BGBl. 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 des Bundesministers für Inneres 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, sind Teilnehmer des OpKoord zur Verschwiegenheit verpflichtet, sofern in der Sitzung nichts anders beschlossen wird. Die Verpflichtung zur Verschwiegenheit gilt nicht für jene Mitglieder der OpKoord, die im IKDOK vertreten sind, da diese ohnehin bereits der Amtsverschwiegenheit 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 Zusammenschau 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 der Bundesminister für Inneres für die Erfüllung seiner 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 Bundesgesetzes, mit dem IKT-Lösungen und IT-Verfahren bundesweit konsolidiert werden (IKT-Konsolidierungsgesetz – 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 Ereignisse 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 des Bundesministers für Inneres 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 den Bundesminister für Inneres 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, z. B. 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 der Bundesminister für Inneres durch Abs. 3 – welche im Grunde § 13 Abs. 2 NISG idF BGBl. 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 der Bundesminister für Inneres 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 dem Bundesminister für Inneres 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 BGBl. 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 vom Bundesminister für Inneres technisch betrieben und dem Bundeskanzler sowie dem Bundesminister für Landesverteidigung bereitgestellt werden. Es handelt sich dabei um ein Dateisystem (Art. 4 Nr. 6 DSGVO), für welches 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 Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999 sein sollen (Abs. 2).

Anders als in § 11 Abs. 3 NISG idF BGBl. 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 BGBl. I Nr. 111/2018 entspricht. Für die Organisation des IKDOK und zur Wahrnehmung der Aufgaben des IKDOK (z. B. die Erörterung und Aktualisierung von entsprechend themenspezifischen Lagebildern) kann der Bundesminister für Inneres 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, 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 und (EU) 2018/1139, 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, 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 Luftfahrtsicherheitsgesetz 2011 (LSG 2011), BGBl. 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 des Signatur- und Vertrauensdienstegesetzes (SVG), BGBl. I Nr. 50/2016, der nationalen Regulierungsbehörde nach § 194 TKG 2021 sowie der KommAustria nach § 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 Staatsanwaltschaften und Gerichte ermächtigt sind, der Cybersicherheitsbehörde nach Maßgabe des § 76 Abs. 4 der Strafprozeßordnung (StPO), BGBl. 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 der 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-Dienstanbieter 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 nach § 194 TKG 2021 und die KommAustria nach § 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 Abhilfemaßnahmen 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 den Bundesminister für Inneres über den Umstand der Einstellung eines Verfahrens zu informieren (Abs. 3). Die Bestimmung orientiert sich an § 117f Abs. 3 des Ärztegesetzes 1998 (ÄrzteG 1998), BGBl. 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 betreffenden 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 ihren 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 Verschlusssache 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).

Abs. 1 führt an, dass die Cybersicherheitsbehörde an Peer Reviews teilnehmen kann und beinhaltet eine Liste an Punkten, von denen zumindest einer im Zuge eines solchen Peer Reviews umfasst sein muss.

Die Teilnahme von ENISA und der Europäischen Kommission in der Rolle eines Beobachters ist in Abs. 2 geregelt.

Gemäß Abs. 3 ist vor Beginn der Peer Review durch die Teilnehmer ihr Umfang, einschließlich allfälliger ermittelter Probleme, festzulegen. Auch auf die Verlässlichkeit und etwaige Verschwiegenheits- und Geheimhaltungspflichten wird eingegangen, um den angebrachten Umgang mit etwaigen, im Zuge des Peer Reviews erlangten, Daten sicherzustellen.

Abs. 4 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. 5 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 (z. B. Vertrauensdiensteanbieter; vgl. Art. 2 Abs. 2 Buchstabe a-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 Buchstabe b, d, e und f NIS-2-Richtlinie umgesetzt. Art. 3 Abs. 1 Buchstabe e iVm Art. 2 Abs. 2 Buchstaben b-e NIS-2-Richtlinie, wird in § 26 (Größenunabhängige Einstufung als wesentliche oder wichtige Einrichtung) eingehend geregelt. Im Zeitpunkt der Erstellung des NISG 2024 lag noch kein Entwurf des Bundesgesetzes, mit dem Richtlinie (EU) 2022/2557 umgesetzt wird, vor, weshalb die entsprechende Formulierung gewählt wurde.

Abs. 1 Z 2 legt in Umsetzung des Art. 3 Abs. 2 Buchstabe c NIS-2-Richtlinie fest, dass Anbieter öffentlicher elektronischer Kommunikationsnetze sowie Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste bereits dann als wesentliche Einrichtung gelten, wenn sie 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 Buchstabe a der 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 Buchstabe 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 nach § 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 Buchstabe 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-RL – 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 als ein oberstes Organ der Vollziehung eingerichtet 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.

Als maßgebliche definitorische Einschränkung ist eine Einrichtung nur dann als Einrichtungen 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) nationale Sicherheit einschließlich der militärischen Landesverteidigung, die öffentliche Sicherheit oder die Strafverfolgung, fassen, sowie Einrichtungen der Gerichtsbarkeit, einschließlich der kollegialen und monokratischen Justizverwaltung, Einrichtungen der Gesetzgebung, einschließlich der Präsidentschaftskanzlei, 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. Daraus ergibt sich auch ohne ausdrückliche gesetzliche Anordnung, dass Angelegenheiten der Gerichtsbarkeit, einschließlich der kollegialen und monokratischen Justizverwaltung, sowie der Parlamentsdirektion ebenfalls nicht vom Anwendungsbereich dieses Bundesgesetzes umfasst 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 nach 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 nach § 24 Abs. 5). Dies bedeutet auch, dass die Aufsicht über IKT-Drittdienstleister (auch) der Cybersicherheitsbehörde obliegt.

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 vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, in der Fassung ABl. Nr. L 124 vom 20.5.2003 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 in der Fassung ABl. Nr. L 124 vom 20.5.2003 S. 36 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 (einzeln 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 0000 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 Buchstaben b-e NIS-2-Richtlinie um, welche in Zusammenschau mit Art. 3 Abs. 1 Buchstabe 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 Buchstabe 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 größenunabhängige Einstufung (§ 26 Abs. 3; Art. 2 Abs. 2 Buchstaben b-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 Buchstaben b-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 StGB 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 Buchstaben 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 Buchstabe 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 Buchstabe 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' nach 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, dem Bundesminister für Inneres 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 Zustellbevollmächtiger 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 setzt einerseits Art. 3 Abs. 3 und 4 und andererseits Art. 27 NIS-2-Richtlinie um. 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.

Die Einrichtungen haben sich innerhalb von drei Monaten ab Inkrafttreten dieses Bundesgesetzes bei der Cybersicherheitsbehörde zu registrieren und dabei die in Abs. 2 aufgelisteten Angaben bekanntzugeben. 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, haben sich unverzüglich, jedenfalls aber innerhalb von drei Monaten ab Erfüllung der jeweiligen Voraussetzungen zu registrieren. 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), BGBl. 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 sind die Einrichtungen gemäß Abs. 4 verpflichtet, 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 hat 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.

In Abs. 6 soll das im Rahmen des NISG etablierte Institut der ‚Kontaktstelle' aufgrund positiver Erfahrungen im gezielten Informationsaustausch zwischen Behörde und betroffenen Unternehmen weiter bestehen 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-Namensregister 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 Buchstabe c der Verordnung (EU) 2016/679 dar. In Abs. 2 werden die Informationen festgelegt, die von den TLD-Namensregister 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-Namensregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sind gemäß Abs. 4 weiters verpflichtet, unverzüglich nach der Registrierung eines Domänennamens 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-Namensregister 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)

Mit dieser Bestimmung wird Art. 20 der NIS-2-Richtlinie umgesetzt und sieht vor, dass Leitungsorgane wesentlicher und wichtiger Einrichtungen die Einhaltung der Risikomanagementmaßnahmen nach § 32

sicherzustellen und zu beaufsichtigen haben. Dies umfasst auch die Aufgabe entsprechende Richtlinien und Vorgaben (siehe unten, § 32) zu billigen (vgl. Art. 20 Abs. 1 NIS-2-Richtlinie).

Eine Verletzung dieser Pflichten hat die schadenersatzrechtliche Haftung für schuldhaft verursachten Schaden, der der Einrichtung dadurch entstanden ist, zur Folge.

Um der Pflicht nach § 31 Abs. 1 nachkommen zu können, haben sich die Leitungsorgane wesentlicher und wichtiger Einrichtungen die notwendigen Fähigkeiten im Bereich der Cybersicherheit in Form von Schulungen anzueignen. Darüber hinaus sind auch den übrigen Mitarbeitern – abhängig von ihrem jeweiligen Arbeitsbezug mit Netz- und Informationssystemen – von den Einrichtungen regelmäßige Cybersicherheitsschulungen anzubieten. Die Einrichtung hat dafür Sorge zu tragen, dass 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. Dies ist in Umsetzung des Art. 21 Abs. 2 Buchstabe g NIS-2-Richtlinie auch gemäß § 32 Abs. 1 iVm Punkt 6 der Anlage 3 dieses Bundesgesetzes ein Teilbereich der gebotenen Risikomanagementmaßnahmen.

Zu § 32 (Risikomanagementmaßnahmen im Bereich der Cybersicherheit)

Mit dieser Bestimmung wird Art. 21 der NIS-2-Richtlinie umgesetzt.

Abs. 1 regelt, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen in den Bereichen der Anlage 3 umzusetzen haben. Diese Risikomanagementmaßnahmen müssen Risiken für die Sicherheit der Netz- und Informationssysteme, die für den Betrieb oder die Erbringung ihrer Dienste genützt werden, sowie Auswirkungen von Cybersicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste entsprechend adressieren.

In der zugehörigen Anlage 3 werden jene Bereiche aufgelistet, welche den Normunterworfenen als thematischer Rahmen für die Umsetzung der Risikomanagementmaßnahmen dienen soll. Die Definition und Struktur der Bereiche sind stark an Ausarbeitungen auf europäischer Ebene im Rahmen der Kooperationsgruppe (vgl. § 3 Z 34) angelehnt.

Eine organisatorische Risikomanagementmaßnahme im Bereich der Netzwerksicherheit wäre beispielweise eine von der dafür innerhalb der Einrichtung zuständigen und verantwortlichen Stelle in Kraft gesetzte Richtlinie, welche diesbezügliche Prozesse und Vorgaben definiert. Dabei ist nicht ausgeschlossen, dass – im Fall von Unternehmensgruppen – für die innerhalb der jeweiligen Einrichtung geltenden Vorgaben und Prozesse auch Richtlinien übernommen und in Kraft gesetzt werden, die von innerhalb dieser Gruppe übergeordneten Unternehmen (etwa der Konzernmutter) vorgegeben sind. Diese Richtlinien sind gegebenenfalls für die jeweilige Einrichtung zu ergänzen. Entsprechendes gilt für Einrichtungen im Sektor der öffentlichen Verwaltung.

Eine technische Risikomanagementmaßnahme stellt unter anderem der Einsatz von technischen Lösungen, wie etwa Firewalls zum Kontrollieren und Absichern des Übergangs zwischen unterschiedlichen Netzwerkbereichen dar. Das Vorsehen einer für den Betrieb einer solchen technischen Lösung notwendigen fachkundigen Betriebsmannschaft wäre beispielsweise eine operative Risikomanagementmaßnahme in diesem Bereich. Durch Abs. 2 soll klargestellt werden, dass bei der Umsetzung von Risikomanagementmaßnahmen weitere relevante Aspekte von wesentlichen und wichtigen Einrichtungen zu beachten sind:

Zunächst wird den betroffenen Einrichtungen auferlegt, ein dem bestehenden Risiko angemessenes Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten, was den risikobasierten Ansatz bei der Umsetzung von Risikomanagementmaßnahmen unterstreicht (Abs. 2 Z 1).

Hierbei sind der Stand der Technik und gegebenenfalls einschlägigen nationalen, europäischen und internationalen Normen sowie Best-Practices entsprechend zu berücksichtigen (lit. a). Unter den hierbei erwähnten Normen sind insbesondere solche gemäß Art. 2 Nr. 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung zu verstehen. Best-Practices können in diesem Zusammenhang als sich bewährte Verfahren und Methoden bei der Umsetzung von Risikomanagementmaßnahmen verstanden werden. Zudem sollten, aus der Umsetzung von dem Stand der Technik und gegebenenfalls einschlägigen nationalen, europäischen und internationalen Normen sowie bewährte Verfahren(allgemein bewährte Verfahren und Methoden) berücksichtigenden Risikomanagementmaßnahmen keine unverhältnismäßigen finanziellen und administrativen Belastungen für wesentliche und wichtige Einrichtungen entstehen, weshalb die Kosten der Umsetzung (lit. b) der Risikomanagementmaßnahmen in einem angemessenen Verhältnis zum bestehenden Risiko bzw. den bestehenden Risiken stehen sollten, denen das betreffende Netz- und Informationssystem ausgesetzt ist.

Da Gefahren für die Sicherheit von Netz- und Informationssystemen unterschiedliche Ursachen haben können, ist es von großer Relevanz, dass die umzusetzenden Risikomanagementmaßnahmen auf einem gefahrenübergreifenden Ansatz beruhen (Abs. 2 Z 2). Dieser zielt darauf ab, dass Netz- und Informationssysteme und ihr physisches Umfeld vor Ereignissen wie beispielsweise Diebstahl, Feuer, Überschwemmungen, Telekommunikations- oder Stromausfällen oder vor unbefugtem physischen Zugang zu Informationen und Datenverarbeitungsanlagen einer wesentlichen oder wichtigen Einrichtung geschützt werden. Dementsprechend ist daher auch die physische Sicherheit und die Sicherheit des Umfelds von Netz- und Informationssystemen zu berücksichtigen, indem Maßnahmen zum Schutz dieser Systeme vor Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen einbezogen werden. In diesem Zusammenhang sollten sich die wesentlichen und wichtigen Einrichtungen im Rahmen ihrer Risikomanagementmaßnahmen beispielsweise auch mit der Sicherheit des Personals befassen und über angemessene Konzepte für die Zugangskontrolle verfügen.

Besonders wichtig ist die Bewältigung von Risiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten, z. B. Anbietern von Datenspeicherungs- und -verarbeitungsdiensten oder Anbietern von verwalteten Sicherheitsdiensten und Softwareherstellern, betreffen, da sich die Vorfälle häufen, bei denen Einrichtungen Opfer von Cyberangriffen werden und es böswilligen Akteuren gelingt, die Sicherheit der Netz- und Informationssysteme zu beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Diensten Dritter ausgenutzt werden. Wesentliche und wichtige Einrichtungen haben daher Schwachstellen von unmittelbaren Lieferanten und Anbietern sowie die Gesamtqualität und Widerstandsfähigkeit der Produkte und Dienste, die darin enthaltenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Cybersicherheitsverfahren ihrer Lieferanten und Anbieter, einschließlich der Sicherheit deren Entwicklungsprozesse, zu bewerten und zu berücksichtigen, um die Sicherheit ihrer Lieferketten gewährleisten zu können (Abs. 2 Z 3). Beispielsweise hat eine wesentliche oder wichtige Einrichtung Risiken und Abhängigkeiten, die sich aus den Beziehungen zu einem unmittelbaren Diensteanbieter ergeben, zu identifizieren, zu bewerten und entsprechend zu behandeln, aber auch bei der Auswahl von neuen Lieferanten oder Anbietern oder bei vertraglichen Vereinbarungen generell die zuvor genannten Aspekte zu berücksichtigen.

Bei der Bewertung der verhältnismäßigen Umsetzung von Risikomanagementmaßnahmen (Abs. 3) sind Faktoren wie das Ausmaß der Risikoexposition der 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. Aufgrund der Tatsache, dass innerhalb einer Einrichtung diese Faktoren wie beispielsweise Risikoexposition oder Schweregrad der Auswirkung von Cybersicherheitsvorfällen auf ihre Dienste nicht für alle Netz- und Informationssysteme zwingend identisch sein werden, werden sich innerhalb einer Einrichtung voraussichtlich unterschiedliche Verhältnismäßigkeiten ergeben und daraus unterschiedliche Ausprägungen bei der Umsetzung von spezifischen Risikomanagementmaßnahmen ableiten lassen.

Nach Abs. 4 hat der Bundesminister für Inneres mit Verordnung die Risikomanagementmaßnahmen in den Themengebietender Anlage 3 hinsichtlich technischer, operativer und organisatorischer Anforderungen präzisierend festzulegen. Darüber hinaus kann der Bundesminister für Inneres sektorspezifische Anforderungen an diese Risikomanagementmaßnahmen ebenfalls mit Verordnung festlegen. Diese Spezifizierungen dienen dazu, den Normunterworfenen einen klaren Rahmen vorzugeben, innerhalb dessen Risikomanagementmaßnahmen verhältnismäßig, geeignet und dem Risiko angemessen umzusetzen. Dabei sind überdies der Stand der Technik, gegebenenfalls die einschlägigen Normen und Best-Practices sowie die Kosten der Umsetzung zu berücksichtigen. Die dem Betriebsrat sowie sonstigen Betroffenen zustehenden (Mitbestimmungs-)Rechte, insbesondere jene nach dem Arbeitsverfassungsgesetz sowie der DSGVO, bleiben unberührt.

Zu § 33 (Nachweis der Wirksamkeit von Risikomanagementmaßnahmen)

Sowohl wesentliche als auch wichtige Einrichtungen haben der Cybersicherheitsbehörde sechs Monate nach diesbezüglicher Aufforderung eine Aufstellung der von ihnen umgesetzten Risikomanagementmaßnahmen zu übermitteln (Selbstdeklaration), wobei die Übermittlung in strukturierter Form nach den Vorgaben der Cybersicherheitsbehörde (etwa hinsichtlich notwendiger Inhalte, Format bzw. Struktur oder Art der Übermittlung) erfolgen soll (Abs. 1). Die Vorgehensweise ist insbesondere Art. 31 Abs. 2 NIS-2-Richtlinie entnommen, nach dem den zuständigen Behörden der Mitgliedstaaten eingeräumt werden kann, ihre Aufsichtsaufgaben zu priorisieren und diese Priorisierung auf einem risikobasierten Ansatz beruhen soll. (Teil-)Sektorale Risikoanalysen der Cybersicherheitsbehörde können beispielsweise als Basis für die Aufforderung der Übermittlung einer Selbstdeklaration dienen. Durch die Regelungen in Abs. 2 und 3 soll zudem das von der NIS-2-Richtlinie vorgesehene differenzierte Aufsichtssystem – wesentliche Einrichtungen sind ex ante, wichtige Einrichtungen ex post zu kontrollieren – aufgegriffen werden:

Wesentliche Einrichtungen sollen ab der Aufforderung durch die Cybersicherheitsbehörde drei Jahre Zeit haben, den in ihrer Selbstdeklaration angegebenen Umsetzungsstand der Risikomanagementmaßnahmen der Behörde nachzuweisen. Vorgesehen ist, dass dies durch Übermittlung eines Prüfberichts als Resultat einer Prüfung durch eine unabhängige Stelle geschieht und soll die Übermittlung nach den Vorgaben der Cybersicherheitsbehörde in strukturierter Form zu erfolgen haben (als Beispiele für derartige Vorgaben siehe auch die Erläuterungen zu Abs. 1). Ein solcher Prüfbericht soll die Wirksamkeit der umgesetzten Risikomanagementmaßnahmen zu beschreiben haben, geht dabei gegebenenfalls auf festgestellte Mängel eingehen und einen diese adressierenden Maßnahmenplan enthalten. Wesentlich ist, dass ein Prüfbericht von einem Leitungsorgan sowohl der wesentlichen Einrichtung als auch der unabhängigen Stelle sowie den eingesetzten unabhängigen Prüfern zu unterzeichnen sein soll (Abs. 2).

Im Gegensatz dazu sollen wichtige Einrichtungen nur bei Vorliegen von Nachweisen oder sonstigen Hinweisen und Informationen, wie etwa Angaben in ihrer Selbstdeklaration, Medienberichten oder Meldungen, die der Cybersicherheitsbehörde nahelegen, dass die jeweilige wichtige Einrichtung ihrer Verpflichtung zur Umsetzung der Risikomanagementmaßnahmen mutmaßlich nicht nachkommt, die Umsetzung der Risikomanagementmaßnahmen mittels einer Prüfung durch eine unabhängige Stelle und durch Übermittlung eines Prüfberichts nachzuweisen haben. Für den Prüfbericht sollen die gleichen Regelungen wie oben gelten, allein der Fristenlauf beginnt nicht mit der Aufforderung zur Selbstdeklaration, sondern der Aufforderung zur Übermittlung eines Prüfberichts durch die Cybersicherheitsbehörde (Abs. 3).

Die Kosten der Prüfung durch die unabhängige Stelle sollen grundsätzlich von der wesentlichen bzw. wichtigen Einrichtung zu tragen sein, außer die Cybersicherheitsbehörde trifft in hinreichend begründeten Fällen eine anderslautende Entscheidung (Abs. 4).

Um sicherzustellen, dass die Behörde ihre Aufsichtsmaßnahme gemäß § 38 Abs. 1 Z 1 letzter Fall sinnvoll ausüben kann, haben wesentliche und wichtige Einrichtungen der Cybersicherheitsbehörde geplante Prüfungen spätestens einen Monat vor Beginn der Durchführung bekanntzugeben und dabei auch einen Prüfplan nach den Vorgaben der Cybersicherheitsbehörde zu übermitteln, in dem erkennbar ist, zu welchem Zeitpunkt oder zu welchen Zeitpunkten die unabhängige Stelle durch welche unabhängigen Prüfer und an welchen Örtlichkeiten der jeweiligen Einrichtung prüfen wird (Abs. 5).

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 sektorenspezifischen 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 Sicherheitsvorfalles soll nicht dazu führen, dass die meldende Einrichtung die Ressourcen von Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen – was vorrabgig 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 §§ 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 Buchstabe 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 nach § 37, die von diesen Einrichtungen ergangen sind.

Zu § 35 (Erheblicher Cybersicherheitsvorfall)

Mit dieser Bestimmung wird Art. 23 Abs. 3 NIS-2-Richtlinie umgesetzt und präzisiert, wann ein Cybersicherheitsvorfall als nach § 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 BGBl. 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.

Der Bundesminister für Inneres 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 aus wesentliche und wichtige Einrichtungen)

Mit dieser Bestimmung sollen Art. 32 und 33 NIS-2-Richtlinie derart umgesetzt werden, dass die darin angeführten Aufsichtsmaßnahmen und diese betreffende 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. Auch hier ist wieder der Unterschied im Aufsichtssystem zwischen wesentlichen und wichtigen Einrichtungen abgebildet:

Während die aufgezählten Maßnahmen bezüglich wesentlicher Einrichtungen jederzeit vorgenommen werden können, darf sie die Cybersicherheitsbehörde hinsichtlich wichtiger Einrichtungen – wie analog in

§ 33 Abs. 3 geregelt – 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 nach § 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. Darüber hinaus kann die Cybersicherheitsbehörde die in Abs. 1 angeführten Aufsichtsmaßnahmen auch gegenüber unabhängigen Stellen ergreifen, um die Einhaltung der an diese gestellten Anforderungen kontrollieren zu können (vgl. § 7 Abs. 3).

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 sowie hinsichtlich der Anforderungen von unabhängigen Stellen 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, die Prüfer von unabhängigen Stellen bei ihren Prüfhandlungen im Rahmen von Prüfungen bei wesentlichen oder wichtigen Einrichtungen kontrollierend zu begleiten (‚Witnessaudits'). Dies ist ein wichtiges Instrument, mit dem nicht nur die Einhaltung der Verpflichtungen durch die jeweils kontrollierte Einrichtung, sondern auch die Qualität der Prüfhandlungen von unabhängigen Prüfern durch die Cybersicherheitsbehörde beurteilt werden kann.

Die Cybersicherheitsbehörde ist zudem befugt, bei wesentlichen und wichtigen Einrichtungen sowie unabhängigen Stellen 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. 1 Z 14 dar.

Die Cybersicherheitsbehörde ist ebenfalls befugt, von wesentlichen und wichtigen Einrichtungen sowie unabhängigen Stellen 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 (z. B. Richtlinien), Unterlagen und Protokolle zu operativen Vorgängen (z. B. Protokolle durchgeführter Wartungstätigkeiten) aber auch technische Detailinformationen (z. B. 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 (z. B. 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 der Verordnung (EU) 2019/881 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 sowie Abs. 5 und Art. 33 Abs. 4 lit. a bis g 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. 1a).

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

Mit dieser Bestimmung wird Art. 24 NIS-2-Richtlinie umgesetzt.

Zu § 41 (Beschwerdeverfahren)

Diese Bestimmung legt fest, dass gegen Bescheide des Bundesministers für Inneres und wegen Verletzung seiner Entscheidungspflicht Beschwerde an das Verwaltungsgericht 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 bis § 43) werden datenschutzrechtliche Bestimmungen zur Verarbeitung von personenbezogenen Daten gemäß Art. 4 Nr. 2 DSGVO und § 36 Datenschutzgesetz (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, 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 Buchstabe b DSGVO), der Datenminimierung (Art. 5 Abs. 1 Buchstabe 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 AS-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 Abs. 2 und § 34 Abs. 4 sowie § 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 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 Buchstabe d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 Buchstabe a oder Buchstabe 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.

Zu § 43 (Datenübermittlungen)

Der Bundeskanzler, der Bundesminister für Inneres, 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 abzuwehrende 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.

Der Bundesminister für Inneres kann gemäß Abs. 2 darüber hinaus personenbezogene Daten an bestimmte ausländische Sicherheitsbehörden und Sicherheitsorganisationen (§ 2 Abs. 2 und 3 Polizeikooperationsgesetz) 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 BGBl. I Nr. 111/2018. Hinsichtlich der Übermittlung in Drittstaaten sind die Vorgaben des Kapitels 5 der DSGVO sowie von §§ 58 f DSG einzuhalten.

Der Bundesminister für Inneres 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 Analaufstellen 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 Einrichtungengemäß § 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, sind Verwaltungsstrafen von den Bezirksverwaltungsbehörden als zuständige Behörden nach den verfahrensrechtlichen Bestimmungen des Verwaltungsstrafgesetzes 1991 – VStG, BGBl. Nr. 52/1991, zu verhängen. Angemerkt wird, dass mit Blick auf die erforderliche Expertise zum Zwecke der Zuständigkeitskonzentration mit Landesgesetz die sprengelübergreifende Zusammenarbeit von Bezirksverwaltungsbehörden vorgesehen werden kann (‚Kompetenzzentren'; vgl. etwa § 1 des Landesgesetzes über die Kooperation zwischen Bezirksverwaltungsbehörden in Oberösterreich, LGBl. Nr. 103/2018, sowie § 2a des Gesetzes vom 14. Februar 1977 über die Organisation der Bezirkshauptmannschaften, LGBl. Nr. 11/1977).

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 der Bundesminister für Inneres 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 des Bundesministers für Inneres 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 dem Bundesminister für Inneres 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. 1a angeordnet werde, 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. 7).

Die Verhängung von Geldstrafen gegen juristische Personen oder gegen eingetragene Personengesellschaften orientiert sich an § 99d BWG. Unter Berücksichtigung des Doppelstrafverbots und in Orientierung an § 30 Abs. 3 DSG kann von der Bestrafung eines Verantwortlichen gemäß § 9 VStG abgesehen werden, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person oder die eingetragene Personengesellschaft verhängt wird (Abs. 2, 3 und 4).

Abs. 5 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 Buchstabe i DSGVO war, keine Geldbuße nach Art. 34 der vorliegenden Richtlinie verhängen. Dem soll durch die Regelung in Abs. 6 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 Risikomanagamentmaßnahmen 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-Namensregistern und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, hinsichtlich der Führung bzw. Erteilung von Zugang zu der gemäß Abs. 30 zu führenden Datenbank zum Gegenstand.

Wesentlich ist, dass die Abs. 1 bis 4 auf Behörden, Organe sowie Einrichtungen und sonstige Stellen der öffentlichen Verwaltung, unabhängig davon, ob sie hoheitlich oder im Rahmen der Privatwirtschaftsverwaltung eingerichtet oder tätig sind, keine Anwendung finden sollen (vgl. Abs. 5). Die Formulierung ‚Behörden und sonstige Stellen der öffentlichen Verwaltung, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen' soll an § 30 Abs. 5 DSG angelehnt werden, wobei keine Einschränkung auf öffentliche Stellen, ‚die im gesetzlichen Auftrag handeln' erfolgen soll. Klargestellt ist daher, dass neben der Hoheitsverwaltung auch die gesamte Privatwirtschaftsverwaltung von dieser Regelung umfasst sein soll. Organwalter 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 Organwalter (im Rahmen der Privatwirtschaftsverwaltung, vgl. VwGH vom 21.10.1992, 92/10/0111 in Bezug auf den Bürgermeister einer Gemeinde; siehe auch VfGH 25.6.2015, E 473/2015) – in Frage kommen.

Zu § 46 (Nichteinhaltung von Verpflichtungen durch Stellen der öffentlichen Verwaltung):

Angelehnt an die im vorgeschlagenen § 44 Abs. 1 normierte Anzeigepflicht des Bundesministers für Inneres 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 dem Bundesminister für Inneres festgelegt werden.

Vor dem Hintergrund, dass unter bestimmten Voraussetzungen auch Behörden und sonstige Stellen der öffentlichen Verwaltung vom Anwendungsbereich der NIS-2-RL umfasst sind, bedarf es zur unionsrechtskonformen Umsetzung des Art. 36 NIS-2-RL eines wirksamen alternativen Sanktionsmechanismus im Sinne dieser Bestimmung. Wesentlich ist, dass es sich bei den Adressaten des alternativen Sanktionsmechanismus in Abs. 2 um jene des § 45 Abs. 5 handeln soll. Die zuständige Bezirksverwaltungsbehörde soll demnach bescheidmäßig die Nichteinhaltung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen festzustellen haben. Wesentlich ist, dass die Bezirksverwaltungsbehörde mit diesem Bescheid eine angemessene Frist für die Herstellung des rechtmäßigen Zustandes anzuordnen haben soll. Wird dem Bescheid nicht ordnungsgemäß innerhalb der angeordneten Frist entsprochen, soll die Bezirksverwaltungsbehörde nach Eintritt der formellen Rechtskraft des Bescheides 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. Dabei soll die Bezirksverwaltungsbehörde darauf Bedacht zu nehmen haben, dass die Veröffentlichung keine Gefahr für die öffentliche Ordnung oder Sicherheit darstellt und sollen allenfalls bloß jene Informationen über die Nichteinhaltung von Verpflichtungen nach diesem Bundesgesetz öffentlich bekannt gemacht werden, die keine konkreten Rückschlüsse auf die mit der Pflichtverletzung einhergehenden Sicherheitsmängel zulassen.

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-RL hinreichend Genüge getan.

Zur Anwendbarkeit dieser Bestimmung sowohl auf den Bereich der Hoheitsverwaltung als auch der Privatwirtschaftsverwaltung siehe auch die Erläuterungen zu § 45 Abs. 5.

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 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, 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 ist grundsätzlich der Bundesminister für Inneres betraut, da dieser die Aufgaben der Cybersicherheitsbehörde wahrnimmt (§ 50 Abs. 1 Z 4).

Davon abweichend obliegt der Bundesregierung (Z 1) die Vollziehung dieses Bundesgesetzes hinsichtlich der Erlassung der nationalen Cybersicherheitsstrategie (§ 15 Abs. 1).

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

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

Dem Bundesminister für Inneres obliegt nach Abs. 2 die Besorgung der allgemeinen Angelegenheiten der in § 4 Abs. 1 genannten Aufgaben, worunter auch die legistische Tätigkeit zu verstehen ist.

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

Mit dieser Bestimmung wird das Inkrafttreten dieses Gesetzes, das Außerkrafttreten des NISG und der auf dessen Grundlage erlassenen Verordnungen sowie der Übergang vom NISG auf das NISG 2024 geregelt. Das NISG 2024 tritt mit 1. Juni 2025 in Kraft. Bis zu diesem Zeitpunkt ist die NIS-2-Richtlinie im nationalen Recht der Mitgliedstaaten umzusetzen.

Verordnungen auf Grund dieses Bundesgesetzes können bereits ab dem auf seine Kundmachung folgenden Tag erlassen werden. Ab diesem Zeitpunkt ist das Gesetz in Geltung. Allerdings treten die Bestimmungen des Gesetzes jedenfalls mit 1. Juni 2025 in Kraft. Um ein Auseinanderfallen der Geltung und des Inkrafttretens der Verordnungsermächtigung mit jenem des Gesetzes zu vermeiden, wird das Inkrafttreten der Verordnung frühestens für den 1. Juni 2025 vorgesehen. Um eine rasche Umsetzung des Gesetzes und Konkretisierung der darin getroffenen Vorgaben zu gewährleisten, sind alle vorbereitenden Maßnahmen bereits ab dem Zeitpunkt der Geltung des Gesetzes (dem der Kundmachung dieses Bundesgesetzes folgenden Tag) zu setzen, soweit sie nicht bereits erfolgt sind.

Das NISG, Netz- und Informationssystemsicherheitsverordnung (NISV), BGBl. II Nr. 215/2019, und die Verordnung über qualifizierte Stellen (QuaSteV), BGBl. II Nr. 226/2019, treten mit Ablauf des 1. Juni 2025 außer Kraft.

Hinsichtlich der Wirksamkeit von Bescheiden, die auf Basis des NISG erlassen wurden, wird festgelegt, dass diese mit Inkrafttreten dieses Bundesgesetzes gegenstandslos werden. Von der Möglichkeit der Ermittlung aller Betreiber wesentlicher Dienste als wesentliche Einrichtung, wurde in Hinblick auf Art. 7

B-VG kein Gebrauch gemacht. Betreiber wesentlicher Dienste § 16 Abs. 1 NISG sind jedoch in der Regel nunmehr als wesentliche Einrichtungen gemäß § 24 Abs. 1 dieses Bundesgesetzes zu qualifizieren.

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.

In Anlage 1 Punkt 1 lit. a (Sektor ‚Energie', Subsektor ‚Elektrizität') wird in der 4. Variante (‚Erzeuger') festgelegt, dass als relevante Arten der Einrichtung darunter lediglich Erzeuger im Sinne des § 7 Abs. 1 Z 17 ElWOG fallen, 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', Subsektor ‚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 Bundesgesetz zur Festlegung einheitlicher Standards beim Infrastrukturaufbau für alternative Kraftstoffe, BGBl. 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 Nr. 39 Verordnung (EU) 2023/1804 ‚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 Nr. 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 Nr. 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 Mobilitätsdiensleister 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', Subsektor ‚Fernwärme') wird die Art der Einrichtung als Betreiber von Fernwärme oder Fernkälte im Sinne des Artikels 2 Nummer 19 der Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates 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 Buchstabe g der Richtlinie 2011/24/EU (Patientenmobilitätsrichtlinie) als maßgebliche Art der Einrichtung definiert. Zum Begriff des ‚Gesundheitsdienstleisters' kann auf Anlage 1 der Gesundheitstelematikverordnung 2013 (GTelV 2012) 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), Apotheken sowie Einrichtungen des Rettungswesens.

Demnach handelt es sich bei dem Großteil der in der Anlage 1 der Gesundheitstelematikverordnung 2013 (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 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 Buchstabe g der Richtlinie 2011/24/EU 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, GZ: KII-2/91, 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') wird die maßgebliche Art der Einrichtung unter anderem danach definiert, dass Unternehmen ausgeschlossen sind, ‚für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist'. Eine Wirtschaftstätigkeit ist jedenfalls eine wirtschaftliche Tätigkeit. Nicht wirtschaftliche Tätigkeiten scheiden für die Ermittlung dieses Sektors aus. Da die NIS-2-Richtlinie nicht von mehreren ‚Hauptwirtschaftstätigkeiten' ausgeht (arg: ‚ihre' Hauptwirtschaftstätigkeit), ist sohin darauf abzustellen, ob das Unternehmen unter Berücksichtigung aller wirtschaftlichen Tätigkeiten die Abfallbewirtschaftung die primäre Tätigkeit darstellt, mit der die Wirtschaftlichkeit ihres Handelns sichergestellt ist.

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 des Europäischen Parlaments und des Rates vom 18. Dezember 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. L 396 vom 30.12.2006 S. 1 (im Folgenden REACH-Verordnung) angeführt sind. Hersteller gemäß Art. 3 Nr. 9 REACH-Verordnung bezeichnet natürliche oder juristische Person mit Sitz in der Gemeinschaft, die in der Gemeinschaft einen Stoff herstellt. Händler gemäß Art. 3 Nr. 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 entweder im Großhandel tätig ist oder in der industriellen Produktion und Verarbeitung. Wird eine Einrichtung entweder im Großhandel oder in der industriellen Produktion und Verarbeitung tätig, 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. Letztverwender) verkaufen.

Zur Anlage 3 (Risikomanagementmaßnahmen-Bereiche)

Die Anlage 3 beschreibt jene Bereiche, in denen wesentliche und wichtige Einrichtungen gemäß § 32 verpflichtend geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen zu ergreifen haben. Dadurch sollen die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, beherrscht werden und die Auswirkungen von Cybersicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste verhindert oder möglichst geringgehalten werden.

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. 4):

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 Zusammenschau mit Abs. 4 – die KommAustria), mit Verordnung nähere 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 2024 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 Finanzen und dem Bundesminister für Inneres 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 § 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. xx):

Bei der vorgeschlagenen Änderung handelt es sich um eine erforderliche Anpassung der geltenden Bestimmungen des GTelG 2012 an das NISG 2024.

Abs. 2 stellt klar, dass das Austrian HealthCERT hinkünftig für den Sektor Gesundheitswesen gemäß § 2 Z 5 NISG 2024 die Aufgaben eines sektorspezifischen CSIRT übernehmen soll. Das Austrian HealthCERT hat die Anforderungen, die gemäß § 9 NISG 2024 an ein Computer-Notfallteam gestellt werden mit Ausnahme der Z 8, zu erfüllen. Außerdem soll klargestellt werden, dass die Bestimmungen aus dem NISG 2024, welche sich auf die Ermächtigung des Bundesminister oder der Bundesministerin für Inneres 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 2024 an ein sektorspezifischen gestellt werden, efüllt, wird ebenfalls bereits mit der gegenständlichen Novelle des GTelG 2012 sichergestellt. Da das

Austrian HealthCERT auch als sektorspezifisches CSIRT iSd NISG 2024 tätig wird, finden desweiteren die Bestimmungen des NISG 2024, welche sich auf sektorspezifische CSIRTs beziehen, Anwendung.

Die Verarbeitung der Daten erfolgt hierbei auf Grundlage des NISG 2024, 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 2024 die dem Sektor Gesundheitswesen gemäß § 2 Z 5 NISG 2024 angehören, verpflichtet werden, die Meldungen nach den §§ 34 und 37 NISG 2024 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 2024 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 2024 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 2024, nach der DSGVO, dem Medizinprodukterecht 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, der Bundesminister für Landesverteidigung, der Bundesminister für europäische und internationale Angelegenheiten und die CSIRTs sind ermächtigt, personenbezogene Daten zu verarbeiten (§ 42 NISG 2024) 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 2024 bzw. aufgrund innerstaatlicher oder internationaler Amtshilfe (§ 43 Abs. 1, 2 und 3 NISG 2024) erforderlich sein.

Die Kategorien der betroffenen personenbezogenen Daten werden in § 42 Abs. 2 bis 6 NISG 2024 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 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 2024 gewonnen wurden, hat der Bundesminister für Inneres gemäß § 18 NISG 2024 ein Meldeanalysesystem zu betreiben. Weiters ist er gemäß § 13 NISG 2024 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 2024 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 Regelungen zur Amtsverschwiegenheit sowie auf anderweitige Verschwiegenheitspflichten darf verwiesen werden (vgl. etwa Art. 20 B-VG, § 46 BDG 1979). Insbesondere ist aufgrund der durchgehenden Protokollierungspflicht (§ 42 Abs. 3) 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 2024).

– ‚Einschränkung der Rechte der betroffenen Personen':

Die Einschränkung der Rechte der betroffenen Personen werden in § 42 Abs. 10 NISG 2024 geregelt und gemessen am Zweck des NISG 2024 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. Gleiches 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 2024 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 internationalem Bereich bei einem Null-Szenario ist extrem erhöht, sodass die Datenschutz-Folgenabschätzung klar positiv ausfällt.

Anlage 1

Sektoren mit hoher Kritikalität		
Sektor	**Teilsektor**	**Art der Einrichtung**
1. Energie	a) Elektrizität	Elektrizitätsunternehmen im Sinne des § 7 Abs. 1 Z 11 Bundesgesetz, mit dem die Organisation auf dem Gebiet der Elektrizitätswirtschaft neu geregelt wird (Elektrizitätswirtschafts- und -organisationsgesetz 2010 - ElWOG 2010, im Folgenden: ElWOG) StF: BGBl. I Nr. 110/2010, sofern diese Versorger gemäß § 7 Abs. 1 Z 74 ElWOG sind
		Verteilernetzbetreiber im Sinne des § 7 Abs. 1 Z 76 ElWOG
		Übertragungsnetzbetreiber im Sinne des § 7 Abs, 1 Z 70 ElWOG
		Erzeuger im Sinne des § 7 Abs 1 Z 17 ElWOG, sofern es sich bei diesen Tätigkeiten um die gewerbliche oder berufliche Haupttätigkeit handelt
		Nominierte Strommarktbetreiber im Sinne des Art. 2 Z 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt, ABl. L 158 vom 14.6.2019 S. 54 (im Folgenden: Verordnung 2019/943)
		Marktteilnehmer im Sinne des Art. 2 Z 25 Verordnung 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Art. 2 Z 18, 20 und 59 der Richtlinie (EU)

		2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU, ABl. L 158 vom 14.6.2019 S. 125 anbieten
		Betreiber von Ladepunkten im Sinne des Art. 2 Z 39 der Verordnung (EU) 2023/1804 Verordnung (EU) 2023/1804 des Europäischen Parlaments und des Rates vom 13. September 2023 über den Aufbau der Infrastruktur für alternative Kraftstoffe und zur Aufhebung der Richtlinie 2014/94/EU, ABl. L 234 vom 22.9.2023, S. 1–47
	b) Fernwärme und -kälte	Betreiber von Fernwärme oder Fernkälte im Sinne des Art. 2 Z 19 Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates, ABl. L 328 vom 21.12.2018 S. 82, idF ABl. L 311 vom 25.9.2020 S. 11
	c) Erdöl	Betreiber von Erdöl-Fernleitungen
		Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
		Zentrale Erdölbevorratungsstellen im Sinne des § 9 Bundesgesetz über die Haltung von Mindestvorräten an Erdöl und Erdölprodukten (Erdölbevorratungsgesetz 2012 – EBG 2012) BGBl. I Nr. 78/2012
	d) Erdgas	Versorgungsunternehmen (‚Versorger') im Sinne des § 7 Abs. 1 Z 68 Bundesgesetz, mit dem Neuregelungen auf dem Gebiet der Erdgaswirtschaft erlassen werden (Gaswirtschaftsgesetz 2011, im Folgenden: GWG), BGBl. I Nr. 107/2011
		Verteilernetzbetreiber im Sinne des § 7 Abs. 1 Z 72 GWG
		Fernleitungsnetzbetreiber im Sinne des § 7 Abs. 1 Z 20 GWG
		Betreiber einer Speicheranlage (‚Speicherunternehmen') im Sinne des § 7 Abs. 1 Z 58 GWG
		Betreiber einer LNG-Anlage im Sinne des Art. 2 Nr. 12 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG, ABl. L 211 vom 14.8.2009 S. 94
		Erdgasunternehmen im Sinne des § 7 Abs. 1 Z 16 GWG
		Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
	e) Wasserstoff	Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung
2. Verkehr	a) Luftverkehr	Luftfahrtunternehmen im Sinne des Art. 3 Nr. 4 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002, ABl. L 97 vom 9.4.2008 S. 72, die zu gewerblichen Zwecken eingesetzt werden
		Flughafenleitungsorgane im Sinne des § 3 Z 2 Bundesgesetz über die Festlegung von Flughafenentgelten (Flughafenentgeltegesetz – FEG), BGBl. I Nr. 41/2012, Flughäfen im Sinne des § 3 Z 1 FEG, einschließlich der in Anhang II Abschnitt 2 der

		Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU, ABl. L 348 vom 20.12.2013, S. 1 angeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
		Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Art. 2 Z 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums (‚Rahmenverordnung'), ABl. L 96 vom 31.3.2004 S. 1 bereitstellen
	b) Schienenverkehr	Infrastrukturbetreiber im Sinne des Art. 3 Z 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates vom 21. November 2012 zur Schaffung eines einheitlichen europäischen Eisenbahnraums, ABl. L 343 vom 14.12.2012 S. 32
		Eisenbahnunternehmen im Sinne des § 1b EisbG, einschließlich Betreiber einer Serviceeinrichtung im Sinne des § 62a Abs 1 EisbG
	c) Schifffahrt	Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/200411 für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe
		Leitungsorgane von Häfen im Sinne des Art. 3 Z 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen, ABl. L 310 vom 25.11.2005 S. 28, einschließlich ihrer Hafenanlagen im Sinne des Art. 2 Z 11 der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen, ABl. L 129 vom 29.4.2004 S. 6, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben
		Betreiber von Schiffverkehrsdiensten im Sinne des Art. 3 lit o der Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates vom 27. Juni 2002 über die Einrichtung eines gemeinschaftlichen Überwachungs- und Informationssystems für den Schiffsverkehr und zur Aufhebung der Richtlinie 93/75/EWG des Rates, ABl. L 208 vom 5.8.2002 S. 10
	d) Straßenverkehr	Straßenverkehrsbehörden im Sinne des Art. 2 Z 12 der Delegierten Verordnung (EU) 2015/962 der Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste, ABl. L 157 vom 23.6.2015 S. 21, die für Verkehrsmanagement- und Verkehrssteuerung verantwortlich sind, mit Ausnahme von öffentlichen Stellen, für die das Verkehrsmanagement oder der Betrieb intelligenter

		Verkehrssysteme nur ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist
		Betreiber intelligenter Verkehrssysteme im Sinne des § 2 Z 1 Bundesgesetz über die Einführung intelligenter Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (IVS-Gesetz – IVS-G), BGBl. I Nr. 38/2013
3. Bankwesen		Kreditinstitute im Sinne des Art. 4 Z 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012, ABl. L 176 vom 27.6.2013 S. 1
4. Finanzmarkt-infrastrukturen		Betreiber von Handelsplätzen im Sinne des § 1 Z 26 Wertpapieraufsichtsgesetz 2018 – WAG 2018, BGBl. I Nr. 107/2017.
		Zentrale Gegenparteien im Sinne des Art. 2 Z 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister, ABl. L 201 vom 27.7.2012 S. 1
5. Gesundheitswesen		Gesundheitsdienstleister im Sinne des Art. 3 lit. g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung, ABl. L 88 vom 4.4.2011 S. 45
		EU-Referenzlaboratorien im Sinne des Art. 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU, ABl. L 314 vom 6.12.2022 S. 26
		Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des § 1 Abs. 1 Bundesgesetz vom 2. März 1983 über die Herstellung und das Inverkehrbringen von Arzneimitteln (Arzneimittelgesetz – AMG), BGBl. Nr. 185/1983 ausüben
		Einrichtungen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen
		Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Art. 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte, ABl. L 20 vom 31.1.2022 S. 1 (‚Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit‘) eingestuft werden
6. Trinkwasser		Lieferanten von und Unternehmen der Versorgung mit ‚Wasser für den menschlichen Gebrauch‘ im Sinne des § 3 Z 2 Bundesgesetz über Sicherheitsanforderungen und weitere Anforderungen an Lebensmittel, Gebrauchsgegenstände und kosmetische Mittel zum Schutz der Verbraucherinnen und Verbraucher

		(Lebensmittelsicherheits- und Verbraucherschutzgesetz – LMSVG) BGBl. I Nr. 13/2006, jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist
7. Abwasser		Unternehmen, die kommunales, häusliches oder industrielles Abwasser im Sinne des Art. 2 Nr. 1, 2 und 3 der Richtlinie 91/271/EWG des Rates vom 21. Mai 1991 über die Behandlung von kommunalem Abwasser, ABl. L 135 vom 30.5.1991 S. 40 sammeln, entsorgen oder behandeln, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung, oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist
8. Digitale Infrastruktur		Betreiber von Netzeinrichtungen, die die Zusammenschaltung von mehr als zwei unabhängigen Netzen (autonomen Systemen) ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr, der nur der Zusammenschaltung autonomer Systeme dient und weder voraussetzt, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; noch den betreffenden Datenverkehr verändert oder anderweitig beeinträchtigt (‚Internet-Knoten' oder , Internet Exchange Point – ‚IXP')
		DNS-Diensteanbieter, ausgenommen Betreiber von Root-Nameserver
		‚Namenregister der Domäne oberster Stufe' (TLD-Namenregister)
		Anbieter von Diensten, die auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind (‚Cloud-Computing-Dienstes')
		Anbieter von Diensten, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden (‚Rechenzentrumsdienste'), mit Ausnahme von Rechenzentrumsdiensten, die ausschließlich von der betroffenen Einrichtung betrieben und genutzt werden.
		Betreiber von Netzen dezentraler Server zur Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder schnellen Zustellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern (‚Inhaltszustellnetzen' oder ‚Content Delivery Network')
		Vertrauensdiensteanbieter
		Anbieter öffentlicher elektronischer Kommunikationsnetze oder
		Anbieter von Kommunikationsdiensten, soweit deren

		Dienste öffentlich zugänglich sind
9. Verwaltung von IKT-Diensten (Business-to-Business)		Anbieter verwalteter Dienste (Managed Service Provider - MSP)‘), ausgenommen jener Fälle, in denen diese Dienste ausschließlich von der betroffenen Einrichtung betrieben und genutzt werden
		Anbieter verwalteter Sicherheitsdienste (Managed Security Service Provider - MSSP), ausgenommen jener Fälle, in denen diese Dienste ausschließlich von der betroffenen Einrichtung betrieben und genutzt werden
10. Öffentliche Verwaltung		Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene
		Einrichtungen im Sektor der öffentlichen Verwaltung auf Landesebene
11. Weltraum		Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

Anlage 2

Sonstige kritische Sektoren		
Sektor	**Teilsektor**	**Art der Einrichtung**
1. Post- und Kurierdienste		Postdiensteanbieter gemäß § 3 Z 3 Postmarktgesetz (PMG), BGBl. I Nr. 123/2009 und Anbieter von Kurierdiensten gemäß § 3 Z 4a PMG.
2. Abfallbewirtschaftung		Unternehmen gemäß § 2 Abs. 6 Z 3 und 4 Abfallwirtschaftsgesetz 2002, BGBl. I Nr. 102/2002.
3. Produktion, Herstellung und Handel mit chemischen Stoffen		Unternehmen im Sinne der Art. 3 Z 9 und 14 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 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. L 396 vom 30.12.2006 S. 1, die Stoffe herstellen und die diese Stoffe oder Gemische 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 in die Kategorie 20 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) fallen.
4. Produktion, Verarbeitung und Vertrieb von Lebensmittel		Lebensmittelunternehmen im Sinne des Art. 3 Z 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für

		Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit, ABl. L 31 vom 1.2.2002 S. 1, die im Großhandel und in der industriellen Produktion und Verarbeitung tätig sind.
5. Verarbeitendes Gewerbe/Herstellung von Waren	a) Herstellung von Medizinprodukten und Invitro-Diagnostika	Einrichtungen, die Medizinprodukte im Sinne des Art. 2 Z 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (Text von Bedeutung für den EWR, ABl. L 117 vom 5.5.2017 S. 1 herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Art. 2 Z 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission, ABl. L 117 vom 5.5.2017, S.176 herstellen, mit Ausnahme der bereits unter Anlage 1 Nr. 5 fünfte Variante (‚Einrichtungen, die Medizinprodukte herstellen') fallen
	b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	c) Herstellung von elektronischen Ausrüstungen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	d) Maschinenbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	e) Herstellung von Kraftwagen und Kraftwagenteilen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	f) sonstiger Fahrzeugbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
6. Anbieter digitaler Dienste		Anbieter eines Online-Marktplatzes gemäß § 1 Abs. 4 Z 10 Bundesgesetz gegen den unlauteren Wettbewerb 1984 (UWG), BGBl. Nr. 448/1984.
		Anbieter einer ‚Online-Suchmaschine' im Sinne des Art. 2 Z 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten, ABl. L 186 vom 11.7.2019

		S. 57
		Anbieter einer Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können (‚Dienste sozialer Netzwerke')
7. Forschung		Einrichtungen, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen, die jedoch Bildungseinrichtungen nicht einschließt (‚Forschungseinrichtung')

Anlage 3

Themengebiete der Risikomanagementmaßnahmen	
1. Leitungsorgane	
	a. Rollen und Verantwortlichkeiten der Leitungsorgane
2. Sicherheitsrichtlinien	
	a. Sicherheitsrichtlinien
	b. Funktionen, Aufgaben und Verantwortlichkeiten
3. Risikomanagement	
	a. Risikomanagementrichtlinie und Risikomanagementprozess
	b. Beurteilung der Effektivität von Risikomanagementmaßnahmen
	c. Überwachung der Einhaltung von Vorgaben
	d. Unabhängige Überprüfungen
4. Verwaltung von Vermögenswerten	
	a. Inventarisierung von Vermögenswerten
	b. Klassifikation von Vermögenswerten
	c. Handhabung von Vermögenswerten
	d. Umgang mit Wechseldatenträgern
	e. Rücknahme oder Löschung von Vermögenswerten
5. Personalwesen	
	a. Sicherheit im Personalwesen
	b. Hintergrundüberprüfung
	c. Verfahren bei Beendigung oder Wechsel des Beschäftigungsverhältnisses
	d. Umgang mit Verstößen gegen die Sicherheitsrichtlinie
6. Cybersicherheitskompetenzen und Cybersicherheitsschulungen	
	a. Vermittlung von Cybersicherheitskompetenzen
	b. Cybersicherheitsschulungen
7. Sicherheit von Lieferketten	
	a. Richtlinie zur Sicherheit von Lieferketten
	b. Lieferantenverzeichnis
8. Zugangssteuerung	
	a. Zugangssteuerungsrichtlinie
	b. Verwaltung von Zugriffsberechtigungen
	c. Privilegierte und administrative Zugänge
	d. Systeme und Anwendungen zur Systemadministration
	e. Identifikation
	f. Authentifikation
	g. Multi-Faktor-Authentifikation
9. Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung	
	a. Konfigurationsmanagement
	b. Änderungsmanagement
	c. Umgang mit Schwachstellen und deren Offenlegung
	d. Sicherheitstests

	e. Patchmanagement
	f. Sicherheit bei der Beschaffung von IKT-Diensten und IKT-Produkten
	g. Sichere Softwareentwicklung
	h. Netzwerksegmentierung
	i. Netzwerksicherheit
	j. Schutz vor bösartiger und unautorisierter Software
10. Kryptographie	
	a. Kryptographierichtlinie
11. Umgang mit Cybersicherheitsvorfällen	
	a. Richtlinie zum Umgang mit Cybersicherheitsvorfällen
	b. Überwachung und Protokollierung
	c. Meldung von Ereignissen
	d. Korrelation und Analyse von Ereignissen
	e. Reaktion auf Cybersicherheitsvorfälle
	f. Erkenntnisse nach Cybersicherheitsvorfällen
12. Betriebskontinuitäts- und Krisenmanagement	
	a. Betriebskontinuitätsmanagement und Notfallwiederherstellungspläne
	b. Backup-, Redundanz- und Wiederherstellungsmanagement
	c. Krisenmanagement
13. Umgebungsbezogene und physische Sicherheit	
	a. Sicherheitsperimeter und physische Zutrittskontrollen
	b. Schutz vor umgebungsbezogenen Gefährdungen
	c. Versorgungseinrichtungen

“

Der Ausschuss für innere Angelegenheiten hat den gegenständlichen Initiativantrag in seiner Sitzung am 19. Juni 2024 in Verhandlung genommen und einstimmig die Durchführung eines öffentlichen Hearings gemäß § 37a Abs. 1 Z 3 GOG-NR beschlossen, dem nach § 40 Abs. 1 GOG-NR einstimmig die beiden Experten Mag. Otmar **Lendl** (nationaler und internationaler Liaison Officer für die öffentliche Verwaltung in Österreich und GovCERT Austria) und Sebastian **Kneidinger** (Policy Advisor epicenter.works) beigezogen wurden.

Nach einer einleitenden Stellungnahme des Bundesministers für Inneres Mag. Gerhard **Karner** und Statements der geladenen Experten Mag. Otmar **Lendl** und Sebastian **Kneidinger** beteiligten sich außer der Berichterstatterin Abgeordneten Eva-Maria **Himmelbauer** die Abgeordneten Katharina **Kucharowits**, Mag. Hannes **Amesbauer**, BA, Mag. Georg **Bürstmayr** und Dr. Stephanie **Krisper** an der Debatte. Die aufgeworfenen Fragen wurden von den Experten Mag. Otmar **Lendl** und Sebastian **Kneidinger** und dem Bundesminister für Inneres Mag. Gerhard **Karner** beantwortet.

Nach Beendigung des öffentlichen Hearings gaben die Abgeordnete Katharina **Kucharowits** sowie der Bundesminister für Inneres Mag. Gerhard **Karner** weitere Wortmeldungen ab.

Auf Ersuchen des Ausschusses veranlasste der Präsident des Nationalrates die Abfassung einer auszugsweisen Darstellung über das Hearing. Der Ausschuss beschloss einstimmig, diese gemäß § 39 Abs. 3 GOG-NR zu veröffentlichen (Anlage 1).

Im Zuge der Debatte haben die Abgeordneten Dr. Christian **Stocker** und Michel **Reimon**, MBA einen gesamtändernden Abänderungsantrag eingebracht, der wie folgt begründet war:

„I. Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs

Mit diesem Bundesgesetz sollen das Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 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 abbilden 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 vom 20. Mai 2021 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 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), 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 2024 errichtet das nationale Koordinierungszentrum für Cybersicherheit gemäß der Verordnung (EU) 2021/887 und setzt die NIS-2-Richtlinie um.

Mit dem gegenständlichen Abänderungsantrag soll ein redaktionelles Versehen behoben und demnach klargestellt werden, dass die Anlagen 1 bis 3 normativer Bestandteil des NISG 2024 sind. Damit sind keine inhaltlichen Änderungen verbunden.

Aufbau des Entwurfs des Art. 1 (Netz- und Informationssystemsicherheitsgesetz 2024):

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 und die Aufgaben der Cybersicherheitsbehörde, der Computer-Notfallteams (CSIRTs), der unabhängigen Stellen und der unabhängigen Prüfer. Ferner werden die nationale 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 Verwaltungsstraftatbestände 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), BGBl. 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 B-VG,
- ‘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 Vollziehung zuständig sind, beruht die Zuständigkeit des Bundes auf der in § 1 des Gesetzesentwurfs geschaffenen Kompetenzgrundlage, welche im Wesentlichen jener der in § 1 NISG entspricht.

Besonderheiten des Normerzeugungsverfahrens:

Der Entwurf kann im Hinblick auf Artikel 1 (§§ 1, 46 Abs. 2 und 51 Abs. 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 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.

II. Besonderer Teil

Zu Artikel 1: Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024)

Zu § 1 (Verfassungsbestimmung)

Die Vorschriften in diesem Bundesgesetz, mit dem insbesondere die NIS-2-Richtlinie umgesetzt werden soll, fallen überwiegend gemäß Art. 10 B-VG in die Gesetzgebungs- und Vollziehungszuständigkeit des Bundes.

In den folgenden (Teil-)Sektoren fällt jedoch die Umsetzung der NIS-2-Richtlinie gemäß Art. 11 B-VG in die Vollziehungszuständigkeit der Länder bzw. gemäß Art. 12 B-VG in die Ausführungsgesetzgebungs- und Vollziehungszuständigkeit der Länder oder gemäß Art. 15 Abs. 1 B-VG in die Gesetzgebungs- und Vollziehungszuständigkeit der Länder:

Der Teilsektor ‘Elektrizität’ fällt – ausgenommen länderübergreifende Starkstromleitungen – unter den Kompetenztatbestand ‘Elektrizitätswesen, soweit es nicht unter Art. 10 fällt’ (Art. 12 Abs. 1 Z 5 B-VG) und ist somit in Ausführungsgesetzgebung und Vollziehung Landessache.

Der Teilsektor ‘Straßenverkehr’ fällt unter den Kompetenztatbestand ‘Straßenpolizei’ (Art. 11 Abs. 1 Z 4 B-VG) und ist somit in Vollziehung Landessache.

Der Teilsektor ‘Schifffahrt’ fällt, soweit sie sich auf die Binnenschifffahrt – ausgenommen Donau, Bodensee, Neusiedlersee und auf Grenzstrecken sonstiger Grenzgewässer – bezieht, unter den Kompetenztatbestand ‘Binnenschifffahrt hinsichtlich Schifffahrtsanlagen’ bzw. ‘Strom- und Schifffahrtspolizei auf Binnengewässern’ (Art. 11 Abs. 1 Z 6 B-VG) und ist somit in Vollziehung Landessache.

Der Sektor ‘Gesundheitswesen’ fällt, soweit es sich um Krankenanstalten handelt, unter den Kompetenztatbestand ‘Heil- und Pflegeanstalten’ (Art. 12 Abs. 1 Z 1 B-VG) und ist somit in Ausführungsgesetzgebung und Vollziehung Landessache, soweit es sich aber um das Rettungswesen handelt, in die Gesetzgebungs- und Vollziehungszuständigkeit der Länder (Art. 15 Abs. 1 B-VG).

Jene neuen (Teil-)Sektoren, die durch die NIS-2-Richtlinie erfasst sind, wie beispielsweise der Teilsektor ‘Fernwärme- und kälte’ oder der Sektor ‘Abfallbewirtschaftung’, fallen zum Teil in die Gesetzgebungs- und Vollziehungszuständigkeit der Länder (Art. 15 Abs. 1 B-VG).

Ausgehend von dieser Beurteilung ergibt sich, dass die Vorschriften in diesem Bundesgesetz zwar überwiegend gemäß Art. 10 Abs. 1 B-VG in die Gesetzgebungs- und Vollziehungskompetenz des Bundes fallen, in einigen (Teil-)Sektoren fällt die Umsetzung jedoch in die (Ausführungs-)Gesetzgebung und/oder in die Vollziehung der Länder, weshalb die Begründung einer Kompetenz des Bundes für diese Bereiche verpflichtend einer Verfassungsänderung bedarf.

Vor dem Hintergrund, dass eine statische Kompetenzdeckungsklausel, die lediglich die Erlassung und Aufhebung (sowie die Vollziehung) von Vorschriften zur Bundessache erklärt, jedoch keine Ermächtigung des Bundes zur Änderung dieser Bestimmungen enthält, zur Folge hätte, dass jede auch noch so geringfügige Novelle zum jeweiligen Bundesgesetz (zB Beseitigung von Vollzugsdefiziten) wiederum einer gesonderten Verfassungsänderung bzw. im Verfassungsrang stehenden Kompetenzdeckungsklausel bedürfte (vgl. auch *Janko*, Staats- und Verwaltungsorganisation [2014] 9), soll das gegenständliche Gesetz in Abs. 1 eine dynamische Kompetenzdeckungsklausel enthalten, die auch die Änderung von Vorschriften, wie sie in diesem Bundesgesetz enthalten sind, umfassen soll. Zudem soll abweichend von Art. 102 Abs. 1 B-VG ausdrücklich angeordnet werden, dass die in diesem Bundesgesetz geregelten Angelegenheiten – sofern nicht im Einzelfall (einfachgesetzlich) eine gegenteilige Anordnung erfolgt (vgl. § 44 Abs. 1) – in unmittelbarer Bundesverwaltung besorgt werden können.Zur unionsrechtskonformen Umsetzung dieser Vorgaben ist es zwingend erforderlich, dass der Bundesminister für Inneres seine 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). Nach der Rechtsprechung des VfGH sind oberste Organe jedoch gegenüber keinem anderen Organ weisungsgebunden und besteht keine sachlich in Betracht kommende Oberbehörde (vgl. VfGH 11.3.1959, B 179/58). Oberste Organe dürfen zudem nicht an Willenserklärungen anderer Organe gebunden werden (vgl. VfSlg. 19.827/2013) und darf die Kontrolle der Rechtmäßigkeit des Handelns eines obersten Organes nicht einer anderen Verwaltungsbehörde übertragen werden (vgl. VfSlg. 13.626/1993). Folglich bedarf es für die – unionsrechtlich verpflichtend vorgesehene – Aufsichts- und Durchsetzungsbefugnisse des Bundesministers für Inneres gegenüber

obersten Organen einer entsprechenden verfassungsrechtlichen Grundlage, die mit Abs. 2 geschaffen werden soll. Demnach soll der Bundesminister für Inneres als Cybersicherheitsbehörde (in Anlehnung an die Regelung in § 35 Abs. 2 des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999) dazu ermächtigt sein, seine Befugnisse nach diesem Bundesgesetz auch gegenüber den in Art. 19 B-VG genannten obersten Organen der Vollziehung auszuüben, soweit in diesem Bundesgesetz nicht anderes bestimmt ist. Wesentlich ist, dass damit kein Weisungsrecht des Bundesministers für Inneres gegenüber obersten Organen der Vollziehung verbunden sein soll.

Vor dem Hintergrund, dass es aufgrund der in Abs. 1 vorgesehenen dynamischen Kompetenzdeckungsklausel zu einer Kompetenzverschiebung zu Gunsten des Bundes kommt, sollen gemäß Abs. 3 Änderungen der Bestimmungen gemäß §§ 17, 24 Abs. 2 Z 2, Abs. 3 und 5, § 44 Abs. 1, § 45 Abs. 5 sowie § 46 nur mit Zustimmung der Länder kundgemacht werden dürfen, sofern sich diese Änderungen auf Behörden und sonstige Stellen der öffentlichen Verwaltung der Länder, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen, beziehen. Sollten geplante Änderungen der in der Norm angeführten Bestimmungen die Interessen der Länder betreffen, ist demnach die formelle Zustimmung der Länder eine Voraussetzung für das verfassungsmäßige Zustandekommen dieser bundesgesetzlichen Regelungen (Art. 42a B-VG; vgl. auch zB Art. 102 Abs. 1 und 4 B-VG). Damit wird in diesem Zusammenhang ein ausreichendes Mitspracherecht der Länder sichergestellt. Festgehalten wird, dass die Einbeziehung der Länder durch den Bund bereits in die Vorbereitung von Gesetzesvorhaben angesichts ihrer Betroffenheit regelmäßig angezeigt sein wird.

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 (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 S. 15 vom 17.04.2019 textuell übernommen:

‘Cybersicherheit’ (dort: Art. 2 Nr. 1), ‘IKT-Produkt’ (Art. 2 Nr. 12), ‘IKT-Dienst’ (Art. 2 Nr. 13), ‘IKT-Prozess’ (Art. 2 Nr. 14) und ‘Cyberbedrohung’ (Art. 2 Nr. 8).

Folgende Begriffe werden aus der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 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 übernommen: ‘Vertrauensdienst’ (dort: Art. 3 Nr. 16), Vertrauensdiensteanbieter (Art. 3 Nr. 19) und qualifizierter Vertrauensdiensteanbieter (Art. 3 Nr. 20), ‘Qualifizierte elektronische Signaturerstellungseinheit’ (dort: Art. 3 Nr. 23), ‘Qualifizierte elektronische Siegelerstellungseinheit’ (dort: Art. 3 Nr. 32), ‘Konformitätsbewertungsstelle’ (Art. 3 Nr. 18), ‘vertrauenswürdige Systeme eines Vertrauensdiensteanbieters’ (dort: Art. 24 Abs. 2 Buchstabe e und f).

Die Begriffsbestimmungen von ‘Online-Marktplatz’, ‘Online-Suchmaschine’ und ‘Cloud-Computing’, ‘Internet-Knoten’, ‘Rechenzentrumsdienste’, ‘Content Delivery Network’ und ‘Forschungseinrichtung’ werden in der Anlage 1 definiert, da auf diese Begriffe im Gesetz nicht Bezug genommen wird.

‘Netz- und Informationssysteme’ (Z 1; Art. 6 Nr. 1 NIS-2-Richtlinie) sind Kommunikationsnetze, wie sie auch in § 4 Z 1 des Telekommunikationsgesetzes 2021 (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 Nr. 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 Nr. 3 NIS-2-Richtlinie) umfasst die Cybersicherheit im Sinne des Art. 2 Nr. 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 Nr. 36 NIS-2-Richtlinie) im Sinne des § 4 Z 9 des Telekommunikationsgesetzes 2021 (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 Nr. 37 NIS-2-Richtlinie) umfasst Kommunikationsdienste im Sinne des § 4 Z 4 des Telekommunikationsgesetzes 2021 (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 Nr. 2 der Verordnung (EU) 2015/2120 ‘Internetzugangsdienste’ im Sinne der Begriffsbestimmung des Artikels 2 Abs. 2, Nr. 2 der Verordnung (EU) 2015/2120,
- 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 Nr. 37 NIS-2-Richtlinie identisch.

Der Begriff ‘IKT-Produkt’ (Z 6; Art. 6 Nr. 12 NIS-2-Richtlinie) im Sinne des Art. 2 Nr. 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 Nr. 13 NIS-2-Richtlinie) im Sinne des Art. 2 Nr. 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 Nr. 14 NIS-2-Richtlinie) im Sinne des Art. 2 Nr. 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 Nr. 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 Nr. 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 natürliche oder juristische Personen oder Personengesellschaften, die in eigenem Namen Rechte ausüben und Pflichten unterliegen können (Rechts- und Handlungsfähigkeit).

Der Begriff ‘Leitungsorgan’ (Z 11) beschreibt eine oder mehrere natürliche Personen, die nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte einer Einrichtung oder innerhalb der Einrichtung zur Überwachung der Geschäftsführung berufen sind. Leitungsorgane wesentlicher und wichtiger Einrichtungen sind gemäß Art. 20 NIS-2-Richtlinie durch die Mitgliedstaaten unmittelbar zu verpflichten, die zur Einhaltung von Art. 21 NIS-2-Richtlinie ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen, ihre Umsetzung zu überwachen und sicherzustellen, dass diese für Verstöße gegen diese Verpflichtungen durch die betreffenden Einrichtungen verantwortlich gemacht werden können.

Im Bereich der öffentlichen Verwaltung wird sich die Einstufung als Einrichtung von der Funktion als Leitungsorgan häufig nicht trennen lassen, sofern Einrichtung und Leitungsorgan eine Einheit bilden. So kann beispielsweise ein Bundesminister als wesentliche Einrichtung im Sinne dieses Bundesgesetzes einzustufen sein und wäre dieser zusätzlich als Leitungsorgan zu qualifizieren.

Eine Legaldefinition für ‘Leitungsorgane’ fehlt in der NIS-2-Richtlinie. Die Richtlinie verfolgt das Ziel, Cybersicherheit zu einer der zentralen Agenden der Leitung und der Geschäftsführung von wesentlichen und wichtigen Einrichtungen zu machen. Leitungsorgane sind in die Risikomanagementmaßnahmen einzubeziehen, haben diese zu genehmigen und deren Umsetzung zu überwachen. In Ermangelung einer Legaldefinition in der NIS-2-Richtlinie, wird diese im Bundesgesetz national ergänzt.

Die Definition des Bundesgesetzes zielt darauf ab, die tatsächliche Leitungs- und Geschäftsführungsebene zu erfassen. Aus diesem Grund ist die Vertretungsbefugnis bewusst nicht als Kriterium angeführt und wird stattdessen an die Geschäftsführung und die Überwachung der Geschäftsführung angeknüpft. 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 oder zur Überwachung der Geschäftsführung berufen ist. Ein Leitungsorgan wäre etwa der Vorstand, der Geschäftsführer oder der Aufsichtsrat der jeweiligen Einrichtung.

Der Begriff ‘DNS-Diensteanbieter’ (Domainnamensystem – DNS) (Z 12; Art. 6 Nr. 20 NIS-2-Richtlinie) bezeichnet Einrichtungen, die öffentlich zugängliche rekursive Dienste zur Auflösung von Domänennamen für Internet-Endnutzer oder autoritative Dienste zur Auflösung von Domänennamen 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, der eine bestimmte Domäne oberster Stufe (Top Level Domain – TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domänennamen 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 Nr. 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 Nr. 16 NIS-2-Richtlinie) sind juristische Personen oder eingetragene Personengesellschaften, die einen digitalen Dienst im Sinne des § 3 Z 1 E-Commerce-Gesetz (ECG) 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 Nr. 24 NIS-2-Richtlinie) im Sinne des Art. 3 Nr. 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 diese Dienste betreffenden Zertifikaten oder
- Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder
- Bewahrung von diese Dienste 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 Nr. 25 NIS-2-Richtlinie). Hingegen versteht man unter einem ‘qualifizierten Vertrauensdienstanbieter’ (Z 18; Art. 6 Nr. 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 Nr. 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 Nr. 32 der Verordnung (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 Buchstabe e und f der Verordnung (EU) Nr. 910/2014 entsprechen.

‘Anbieter verwalteter Dienste’ (Managed Service Provider, Z 23; Art. 6 Nr. 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 Nr. 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 Nr. 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 Nr. 40 NIS-2-Richtlinie nach § 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 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl. L 333 vom 27.12.2022 S. 164 (im Folgenden: Richtlinie (EU) 2022/2557).

Der Begriff ‘Risiko’ (Z 26; Art. 6 Nr. 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 Nr. 10 NIS-2-Richtlinie) im Sinne des Art. 2 Z 8 der Verordnung (EU) Nr. 2019/881 (Rechtsakt 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 Nr. 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 Nr. 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 Nr. 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 großes Ausmaßes’ (Z 31; Art. 6 Nr. 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 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 nach 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 nach 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 § 4 (Cybersicherheitsbehörde)

Art. 8 Abs. 1 und 2 der NIS-2-Richtlinie sieht vor, dass Mitgliedstaaten eine oder mehrere Behörden für die Cybersicherheit und die in Kapitel VII der NIS-2-Richtlinie genannten Aufsichtsaufgaben zuständiger Behörden benennt oder sie einrichtet, welche die Anwendung dieser Richtlinie auf nationaler Ebene überwachen. § 4 setzt Art. 8 Abs. 1 NIS-2-Richtlinie um und richtet eine Cybersicherheitsbehörde ein.

Während das NISG noch eine Aufgabenverteilung auf zwei Behörden (eine strategische und eine operative NIS-Behörde) vorsah, werden diese Aufgaben nunmehr von einer Behörde wahrgenommen. Die bisherige Aufteilung der ‘strategischen’ Angelegenheiten der Netz- und Informationssystemsicherheit auf den Bundeskanzler und der ‘operativen’ Angelegenheiten auf den Bundesminister für Inneres setzte einen ständigen Dialog zur Aufgabenerfüllung voraus. Die Erfahrungen anderer Mitgliedstaaten, in denen die behördlichen Aufgaben der NIS-1-Richtlinie auf mehr als eine Behörde verteilt waren, haben gezeigt, dass ein erhöhter Verwaltungsaufwand durch ressortübergreifende Prozesse erzeugt wird und diese Aufteilung einer effizienten Aufgabenerfüllung entgegenstehen kann. Hinzu kommt, dass Parallelstrukturen einerseits aus budgetärer Sicht, andererseits auch in Hinblick auf den Fachkräftemangel im Bereich der IT-Sicherheit hintangehalten werden sollten. Die Vereinigung der Aufgaben im Bereich der Netz- und Informationssystemsicherheit nach der NIS-2-Richtlinie innerhalb einer Behörde erscheint daher zweckmäßig.

Die Cybersicherheitsbehörde übernimmt somit 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. 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 der Kooperationsgruppe, 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 sowie Beaufsichtigung von CSIRTs gemäß § 8 Abs. 2 und § 10;
12. Zulassung sowie Kontrolle der Einhaltung der Erfordernisse unabhängiger Stellen und unabhängiger Prüfer gemäß § 7;
13. Ausübung der Aufsichts- und Durchsetzungsmaßnahmen gegenüber wesentlichen und wichtigen Einrichtungen gemäß den §§ 38 und 39;
14. Entgegennahme, Analyse und Weiterleitung von Meldungen gemäß § 34, § 37 sowie gemäß § 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; § 14) erstellt und durch die Bundesregierung erlassen. Die Koordination der Erstellung erfolgt durch die Cybersicherheitsbehörde.

Sowohl die strategische als auch die operativen Koordinierungsstrukturen (§§ 12 bis 14) werden vom Bundesminister für Inneres 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 §§ 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 (anderen Mitgliedstaaten, NIS-Kooperationsgruppe und CSIRTs-Netzwerk) betrieben.

Der Bundesminister für Inneres betreibt das bei ihm eingerichtete GovCERT (§ 8 Abs. 4). Ferner übernimmt er die Aufgaben der Ermächtigung und Beaufsichtigung von allen CSIRTs (§ 8 Abs. 2).

Unabhängige Stellen und unabhängige Prüfer werden durch die Cybersicherheitsbehörde zugelassen und die Einhaltung der Erfordernisse kontrolliert (§ 7). In diesem Zusammenhang legt der Bundesminister für Inneres durch Verordnung Erfordernisse und Kriterien sowie das Verfahren zur Zulassung von unabhängigen Stellen und unabhängigen Prüfern 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. §§ 12ff, 20).

Mit dem Abs. 2 wird das Verhältnis der Cybersicherheitsbehörde zu jener Behörde, die in Durchführung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates und vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABl. Nr. 333 vom 27.12.2022 S. 1 (Verordnung 2022/2554), die innerstaatlich zuständige Behörde ist, geregelt. Da die Verordnung 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 2022/2554 innerhalb des dortigen Anwendungsbereichs als zuständige Behörde gilt.

Abs. 3 sieht vor, dass der Bundesminister für Inneres den jährlichen Bericht zur Cybersicherheit dem National- und Bundesrat vorzulegen hat. Zusätzlich erstellt der Bundesminister für Inneres eine Übersicht in anonymisierter Form über die eingelangten Meldungen nach § 34 (Berichtspflichten) und § 37 (Freiwillige Meldung relevanter Informationen) gegliedert nach Sektoren sowie die Höhe des Aufwandsersatzes gemäß § 8 Abs. 6 und legt diese Informationen dem Bericht zur Cybersicherheit bei. Dies dient der Information der Legislativorgane.

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 jährlichen 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 gem. Art. 7 Abs. 1 Buchstabe. i und Abs. 4 der Verordnung (EU) 2021/887 sollten in strukturierter Form erfolgen, um eine rasche Bearbeitung zu ermöglichen. Daher können seitens der Cybersicherheitsbehörde gewisse Modalitäten zur Antragstellung vorgesehen werden.

Zu § 7 (Unabhängige Stellen und unabhängige Prüfer)

Mit § 7 soll das im NISG bestehende Institut der qualifizierten Stellen mit systemischen Anpassungen in das neue NISG 2024 überführt werden, zumal sich dieses in der Vergangenheit gut bewährt hat, und sollen die Aufgaben und Befugnisse der unabhängigen Stellen an die Anforderungen der NIS-2-Richtlinie angepasst werden.

Demnach sollen gemäß Abs. 1 als ‘unabhängige Stellen’ juristische Personen oder eingetragene Personengesellschaften mit Niederlassung in Österreich definiert werden, die sich zur Prüfung der Risikomanagementmaßnahmen wesentlicher und wichtiger Einrichtungen gemäß § 33 Abs. 2 und 3 zumindest eines unabhängigen Prüfers (vgl. dazu die Erläuterungen zu Abs. 5) zu bedienen haben.

Gemäß Abs. 2 soll die Zulassung als unabhängige Stelle durch Bescheid der Cybersicherheitsbehörde erfolgen, sofern die in einer Verordnung des Bundesministers für Inneres festzulegenden Anforderungen gemäß Abs. 9 Z 1 erfüllt sind, und sollen der Cybersicherheitsbehörde zur Überprüfung der Einhaltung dieser Anforderungen entsprechende Aufsichtsmaßnahmen, wie sie im vorgeschlagenen § 38 Abs. 1 in Bezug auf wesentliche und wichtige Einrichtungen vorgesehen sind, zukommen.

Werden die Anforderungen gemäß Abs. 9 Z 1 nicht eingehalten, soll die Cybersicherheitsbehörde gemäß Abs. 3 verpflichtet sein, die Zulassung als unabhängige Stelle bescheidmäßig zu widerrufen, es sei denn, die Nichteinhaltung der Anforderungen liegt außerhalb des Einflussbereichs der betreffenden unabhängigen Stelle (zB höhere Gewalt). Um Missbrauch hintanzuhalten, soll im Falle eines bescheidmäßigen Widerrufs für die unabhängige Stelle eine ‘Sperrfrist’ von einem Jahr ab Rechtskraft des Bescheides vorgesehen werden und soll demnach erst nach Ablauf dieser Sperrfirst ein neuerlicher Antrag gemäß Abs. 2 gestellt werden können.

Wesentlich ist, dass unabhängige Stellen dazu verpflichtet sein sollen, als unabhängige Prüfer nur solche natürlichen Personen einzusetzen, die von der Cybersicherheitsbehörde gemäß Abs. 5 zugelassen wurden (Abs. 4).

Hintergrund dieser Bestimmung ist Folgender: Gemäß § 3 der Verordnung über qualifizierte Stellen (QuaSteV), BGBl. II Nr. 226/2019, haben qualifizierte Stellen ‘befähigte sicherheitsüberprüfte Prüfer’ einzusetzen. Die Anforderungen an diese Prüfer sind in § 4 QuaSteV geregelt. Die Erfüllung dieser Anforderungen sind derzeit durch die qualifizierte Stelle gegenüber dem Bundesminister für Inneres bei der Antragstellung nachzuweisen, welcher diese ausschließlich im Rahmen des § 18 Abs. 1 NISG prüfte. Die fehlende Eignung eines Prüfers konnte sich daher ausschließlich auf die Eignung (oder Nichteignung)

der unabhängigen Stelle (nicht aber auf den Prüfer selbst) auswirken. Das Institut der qualifizierten Stellen war daher dahingehend zu überarbeiten, dass auch die Erfüllung der Voraussetzungen zur Aufnahme der Tätigkeit eines Prüfers durch die Cybersicherheitsbehörde überprüft werden kann. Dies erlaubt eine durchgängige Qualitätskontrolle, die im Hinblick auf die verantwortungsvolle Aufgabe der unabhängigen Prüfer notwendig ist.

Vergleichbare Prüfsysteme, in denen einzelne Stellen bzw. Prüfer zwischen den normunterworfenen Einrichtungen und der Behörde zwischengeschaltet sind, finden sich etwa im Wirtschaftstreuhandberufsgesetz 2017 (WTBG 2017), BGBl. I Nr. 137/2017, im Abschlussprüfer-Aufsichtsgesetz (APAG), BGBl. I Nr. 83/2016, im Umweltmanagementgesetz (UMG), BGBl. I Nr. 96/2001, oder in der Fachkundebeurteilungsverordnung (FachKBV), BGBl. II Nr. 37/2007.

In Abs. 5 soll festgelegt werden, welche Voraussetzungen für die Zulassung als unabhängiger Prüfer vorliegen müssen. So soll der Antragsteller gemäß Z 1 über eine vor nicht länger als drei Jahren durchgeführte Sicherheitsüberprüfung auf begründetes Ersuchen einer unabhängigen Stelle oder sonstigen Einrichtung nach §§ 55 ff des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991, für den Zugang zu geheimer Information nachzuweisen haben. Weiters soll der Antragsteller gemäß Z 2 über ein österreichisches Reifeprüfungszeugnis, ein österreichisches Diplomprüfungszeugnis, ein österreichisches Zeugnis über die Berufsreifeprüfung über einschlägige berufliche Qualifikation oder diesen durch völkerrechtliche Vereinbarung gleichwertige Zeugnisse verfügen. Diese Bestimmung orientiert sich an § 64 des Universitätsgesetzes 2002 (UG) BGBl. I Nr. 120/2002. Der Nachweis über eine einschlägige berufliche Qualifikation durch ein Zeugnis gemäß § 26 Berufsausbildungsgesetz – BAG, BGBl. Nr. 142/1969, als erbracht gilt. Nach Z 3 soll zudem eine facheinschlägige Berufserfahrung von mindestens drei Jahren im Ausmaß von zumindest zwanzig Wochenstunden im Bereich der Überprüfung von oder Beratung in verantwortlicher Position über Informationssicherheitsmanagementsystemen, Cybersicherheitsmanagementsystemen und Sicherheitslösungen im IT-/OT-Umfeld. Gemäß Z 4 soll zudem erforderlich sein, dass der Antragsteller gegenüber der Cybersicherheitsbehörde seine Eignung zur Überprüfung der Umsetzung von Risikomanagementmaßnahmen durch den Nachweis ausreichender theoretischer Fachkenntnisse sowie ausreichender praktischer Fähigkeiten in organisatorischer und technischer Hinsicht nachgewiesen hat. Der Bundesminister für Inneres soll mit Verordnung nähere Regelungen zum Verfahren und zu den Inhalten des Eignungsnachweises festlegen können (Abs. 9 Z 2).

Wesentlich ist, dass sämtliche Voraussetzungen gemäß Abs. 5 Z 1 bis 4 im Zeitpunkt der Entscheidung kumulativ vorliegen müssen und demnach ein Antrag gemäß Abs. 5 durch Bescheid zurück- oder abzuweisen sein soll, wenn die normierten Voraussetzungen nicht vorliegen oder erbracht werden können.

Da davon auszugehen ist, dass nicht nur für die Erteilung der Zulassung praktische Erfahrung maßgeblich ist, sondern auch für die ordnungsgemäße weitere Ausübung der Funktion als unabhängiger Prüfer, wird in Abs. 6 vorgeschlagen, die Zulassung zu entziehen, wenn der Betroffene in einem Zeitraum von fünf Jahren nicht für die Durchführung von zumindest zwei Prüfungen von wesentlichen oder wichtigen Einrichtungen (§ 33 Abs. 2 und 3) herangezogen wurde (Z 1) oder der Cybersicherheitsbehörde im Rahmen ihrer Aufsichtsmaßnahmen erkennbar wird, dass der unabhängige Prüfer nicht mehr über die nötigen Fertigkeiten und Fähigkeiten zur Prüfung der Umsetzung der Risikomanagementmaßnahmen verfügt, was insbesondere dann der Fall sein wird, wenn er im Zusammenhang mit Prüfungen wiederholt mangelhaft vorgegangen ist (Z 2).

In diesen Fällen und auch, wenn die Durchführung der Sicherheitsüberprüfung gemäß Abs. 5 Z 1 mehr als drei Jahre zurückliegt, soll die Cybersicherheitsbehörde die Zulassung als unabhängiger Prüfer zu widerrufen haben (Z 3).

Nach einem Widerruf der Zulassung soll die betroffene natürliche Person erst nach Ablauf eines Jahres ab Rechtskraft des Widerrufs einen neuerlichen Antrag auf Zulassung als unabhängiger Prüfer stellen können.

Die Cybersicherheitsbehörde soll gemäß Abs. 7 eine Liste mit den zugelassenen unabhängigen Stellen und unabhängigen Prüfern zu führen und wesentlichen und wichtigen Einrichtungen sowie unabhängigen Stellen in geeigneter Weise zur Verfügung zu stellen haben. Diese Liste soll es wesentlichen und wichtigen Einrichtungen bzw. unabhängigen Stellen erlauben, aus den zugelassenen unabhängigen Stellen bzw. aus den zugelassenen unabhängigen Prüfern frei wählen zu können.

Wesentlich ist, dass die Cybersicherheitsbehörde an das Ergebnis einer externen Überprüfung durch unabhängige Stellen bzw. unabhängige Prüfer nicht gebunden sein soll, sondern soll dieses als Teil ihrer Entscheidungsgrundlage der freien Beweiswürdigung unterliegen. Die abschließende Beurteilung der gemäß § 33 Abs. 2 und 3 umgesetzten Risikomanagementmaßnahmen soll demnach allein der zuständigen Cybersicherheitsbehörde obliegen.

Gemäß Abs. 8 sollen unabhängige Prüfer über bekanntgewordene Tatsachen und Erkenntnisse, die im Rahmen der Prüfung der Umsetzung von Risikomanagementmaßnahmen auftreten und deren Geheimhaltung im Interesse der jeweiligen geprüften Einrichtungen geboten ist, zur Verschwiegenheit verpflichtet sein. Dies soll auch für Personen gelten, denen im Zuge ihrer Tätigkeit bei einer unabhängigen Stelle solche Tatsachen und Erkenntnisse bekanntwerden.

In Abs. 9 soll eine Verordnungsermächtigung des Bundesministers für Inneres zur Festlegung der Anforderungen an unabhängige Stellen (Z 1) sowie der Inhalte des Eignungsnachweises gemäß Abs. 5 Z 4 vorgesehen werden. Gemäß Z 3 soll der Bundesminister für Inneres zudem Pauschalsätze für die Zulassung als unabhängige Stelle oder als unabhängiger Prüfer festlegen können, die dem durchschnittlichen Aufwand der jeweiligen Zulassung entsprechen.

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, sind ein oder mehrere Computer-Notfallteams, auch CSIRTs (Cybersecurity Incident Response Teams) genannt, einzurichten. Diese unterliegen der Aufsicht des Bundesministers für Inneres (§ 10).

Die CSIRTs sind mit der Bewältigung von Cybersicherheitsvorfällen betraut. Zu den Hauptaufgaben der CSIRTs zählen auch die Entgegennahme von Meldungen gemäß §§ 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 nach § 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) – z. B. 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, sind sie, sofern es sich dabei um private Einrichtungen handelt, für diese Tätigkeiten als Beliehene anzusehen. CSIRTs können grundsätzlich auch bei einer Behörde eingerichtet werden, wenn dies für einen bestimmten Sektor sinnvoll erscheint. Die Feststellung der Eignung und die Erteilung der Ermächtigung erfolgt mittels konstitutiven Bescheids. Wird dieser Bescheid befristet erlassen, so ist die Eignung vor einer neuerlichen Erlassung neuerlich zu prüfen. Unabhängig von einer solchen Befristung kann die Cybersicherheitsbehörde diese Ermächtigung beim Wegfall der Anforderungen (vgl. § 10 Abs. 7) widerrufen.

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 (z. B. 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 (z. B. 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 CSIRTs 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 beim Bundesminister für Inneres eingerichtete GovCERT die Aufgaben eines sektorspezifischen CSIRTs für Behörden und sonstige Stellen der öffentlichen Verwaltung, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen (sowohl auf Bundes-, Landes- und Gemeindeebene), wahrzunehmen haben.

Die Entscheidung über die Ermächtigung des nationalen und etwaiger sektorenspezifischer CSIRTs sind vom Bundesminister für Inneres in geeigneter Form (z. B. 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. 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 sektorenspezifischen 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 anonymer 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 (z. B. 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 der §§ 42, 43 werden auch für CSIRTs explizite datenschutzrechtliche Grundlagen geschaffen. Im Kontext dieser Bestimmungen ist auch auf ErwGr 49 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 vom 4.5.2016 S. 1 (Datenschutz-Grundverordnung; 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.

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 Abs. 1 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 dem Bundesminister für Inneres 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 nach § 11 Abs. 1

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

Mitarbeiter von CSIRTs sind über bekanntgewordene Tatsachen und Erkenntnisse, die im Rahmen der Wahrnehmung der Aufgaben nach § 8 auftreten und deren Geheimhaltung im Interesse der jeweiligen geprüften Einrichtungen geboten ist, zur Verschwiegenheit verpflichtet (Abs. 4).

Zu § 10 (Aufsicht)

Die Aufsicht der gemäß § 8 Abs. 2 oder 3 eingerichteten CSIRTs liegt bei dem Bundesminister für Inneres. In Ausübung dieses Aufsichtsrechts hat dieser ein Weisungsrecht gegenüber den CSIRTs. Der Bundesminister für Inneres ist ebenso ermächtigt, 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 Vertrauensdienstegesetz (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 jährlichen 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 jährlichen Berichts zur Cybersicherheit;
4. Erstellung einer eigenen Geschäftsordnung.

Die CSS setzt sich aus je einem zur selbstständigen Behandlung von Angelegenheiten ermächtigten fachkundigen Vertreterder dem Nationalen Sicherheitsrat angehörenden Bundesminister (§ 3 Abs. 1 des Bundesgesetzes über die Errichtung eines Nationalen Sicherheitsrates, BGBl. 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 des Bundesministers für Inneres 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, sind Teilnehmer des OpKoord zur Verschwiegenheit verpflichtet, sofern in der Sitzung nichts anders beschlossen wird. Die Verpflichtung zur Verschwiegenheit gilt nicht für jene Mitglieder der OpKoord, die im IKDOK vertreten sind, da diese ohnehin bereits der Amtsverschwiegenheit 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 Zusammenschau 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 der Bundesminister für Inneres für die Erfüllung seiner 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 Bundesgesetzes, mit dem IKT-Lösungen und IT-Verfahren bundesweit konsolidiert werden (IKT-Konsolidierungsgesetz – 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 Ereignisse 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 des Bundesministers für Inneres 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 den Bundesminister für Inneres 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, z. B. 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 der Bundesminister für Inneres durch Abs. 3 – welche im Grunde § 13 Abs. 2 NISG idF BGBl. 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 der Bundesminister für Inneres 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 dem Bundesminister für Inneres 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 BGBl. 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 vom Bundesminister für Inneres technisch betrieben und dem Bundeskanzler sowie dem Bundesminister für Landesverteidigung bereitgestellt werden. Es handelt sich dabei um ein Dateisystem (Art. 4 Nr. 6 DSGVO), für welches 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 Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999 sein sollen (Abs. 2).

Anders als in § 11 Abs. 3 NISG idF BGBl. 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 BGBl. I Nr. 111/2018 entspricht. Für die Organisation des IKDOK und zur Wahrnehmung der Aufgaben des IKDOK (z. B. die Erörterung und Aktualisierung von entsprechend themenspezifischen Lagebildern) kann der Bundesminister für Inneres 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, 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 und (EU) 2018/1139, 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, 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 Luftfahrtsicherheitsgesetz 2011 (LSG 2011), BGBl. 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 des Signatur- und Vertrauensdienstegesetzes (SVG), BGBl. I Nr. 50/2016, der nationalen Regulierungsbehörde nach § 194 TKG 2021 sowie der KommAustria nach § 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 Staatsanwaltschaften und Gerichte ermächtigt sind, der Cybersicherheitsbehörde nach Maßgabe des § 76 Abs. 4 der Strafprozeßordnung (StPO), BGBl. 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 der 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-Dienstanbieter 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 nach § 194 TKG 2021 und die KommAustria nach § 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 Abhilfemaßnahmen 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 den Bundesminister für Inneres über den Umstand der Einstellung eines Verfahrens zu informieren (Abs. 3). Die Bestimmung orientiert sich an § 117f Abs. 3 des Ärztegesetzes 1998 (ÄrzteG 1998), BGBl. 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 betreffenden 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 ihren 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 Verschlusssache 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).

Abs. 1 führt an, dass die Cybersicherheitsbehörde an Peer Reviews teilnehmen kann und beinhaltet eine Liste an Punkten, von denen zumindest einer im Zuge eines solchen Peer Reviews umfasst sein muss.

Die Teilnahme von ENISA und der Europäischen Kommission in der Rolle eines Beobachters ist in Abs. 2 geregelt.

Gemäß Abs. 3 ist vor Beginn der Peer Review durch die Teilnehmer ihr Umfang, einschließlich allfälliger ermittelter Probleme, festzulegen. Auch auf die Verlässlichkeit und etwaige Verschwiegenheits- und Geheimhaltungspflichten wird eingegangen, um den angebrachten Umgang mit etwaigen, im Zuge des Peer Reviews erlangten, Daten sicherzustellen.

Abs. 4 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. 5 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 (z. B. Vertrauensdiensteanbieter; vgl. Art. 2 Abs. 2 Buchstabe a-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 Buchstabe b, d, e und f NIS-2-Richtlinie umgesetzt. Art. 3 Abs. 1 Buchstabe e iVm Art. 2 Abs. 2 Buchstaben b-e NIS-2-Richtlinie, wird in § 26 (Größenunabhängige Einstufung als wesentliche oder wichtige Einrichtung) eingehend geregelt. Im Zeitpunkt der Erstellung des NISG 2024 lag noch kein Entwurf des Bundesgesetzes, mit dem Richtlinie (EU) 2022/2557 umgesetzt wird, vor, weshalb die entsprechende Formulierung gewählt wurde.

Abs. 1 Z 2 legt in Umsetzung des Art. 3 Abs. 2 Buchstabe c NIS-2-Richtlinie fest, dass Anbieter öffentlicher elektronischer Kommunikationsnetze sowie Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste bereits dann als wesentliche Einrichtung gelten, wenn sie 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 Buchstabe a der 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 Buchstabe 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 nach § 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 Buchstabe 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-RL – 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 als ein oberstes Organ der Vollziehung eingerichtet 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.

Als maßgebliche definitorische Einschränkung ist eine Einrichtung nur dann als Einrichtungen 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) nationale Sicherheit einschließlich der militärischen Landesverteidigung, die öffentliche Sicherheit oder die Strafverfolgung, fassen, sowie Einrichtungen der Gerichtsbarkeit, einschließlich der kollegialen und monokratischen Justizverwaltung, Einrichtungen der Gesetzgebung, einschließlich der Präsidentschaftskanzlei, 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. Daraus ergibt sich auch ohne ausdrückliche gesetzliche Anordnung, dass Angelegenheiten der Gerichtsbarkeit, einschließlich der kollegialen und monokratischen Justizverwaltung, sowie der Parlamentsdirektion ebenfalls nicht vom Anwendungsbereich dieses Bundesgesetzes umfasst 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 nach 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 nach § 24 Abs. 5). Dies bedeutet auch, dass die Aufsicht über IKT-Drittdienstleister (auch) der Cybersicherheitsbehörde obliegt.

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 vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, 2003/361/EG, in der Fassung ABl. Nr. L 124 vom 20.5.2003 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 in der Fassung ABl. Nr. L 124 vom 20.5.2003 S. 36 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 (einzeln 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 0000 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 Buchstaben b-e NIS-2-Richtlinie um, welche in Zusammenschau mit Art. 3 Abs. 1 Buchstabe 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 Buchstabe 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 größenunabhängige Einstufung (§ 26 Abs. 3; Art. 2 Abs. 2 Buchstaben b-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 Buchstaben b-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 StGB 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 Buchstaben 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 Buchstabe 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 Buchstabe 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’ nach 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, dem Bundesminister für Inneres 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 Zustellbevollmächtiger 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 setzt einerseits Art. 3 Abs. 3 und 4 und andererseits Art. 27 NIS-2-Richtlinie um. 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.

Die Einrichtungen haben sich innerhalb von drei Monaten ab Inkrafttreten dieses Bundesgesetzes bei der Cybersicherheitsbehörde zu registrieren und dabei die in Abs. 2 aufgelisteten Angaben bekanntzugeben. 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, haben sich unverzüglich, jedenfalls aber innerhalb von drei Monaten ab Erfüllung der jeweiligen Voraussetzungen zu registrieren. 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), BGBl. 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 sind die Einrichtungen gemäß Abs. 4 verpflichtet, 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 hat 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.

In Abs. 6 soll das im Rahmen des NISG etablierte Institut der ‘Kontaktstelle’ aufgrund positiver Erfahrungen im gezielten Informationsaustausch zwischen Behörde und betroffenen Unternehmen weiter bestehen 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-Namensregister 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 Buchstabe c der Verordnung (EU) 2016/679 dar. In Abs. 2 werden die Informationen festgelegt, die von den TLD-Namensregister 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-Namensregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sind gemäß Abs. 4 weiters verpflichtet, unverzüglich nach der Registrierung eines Domänennamens 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-Namensregister 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)

Mit dieser Bestimmung wird Art. 20 der NIS-2-Richtlinie umgesetzt und sieht vor, dass Leitungsorgane wesentlicher und wichtiger Einrichtungen die Einhaltung der Risikomanagementmaßnahmen nach § 32 sicherzustellen und zu beaufsichtigen haben. Dies umfasst auch die Aufgabe entsprechende Richtlinien und Vorgaben (siehe unten, § 32) zu billigen (vgl. Art. 20 Abs. 1 NIS-2-Richtlinie).

Eine Verletzung dieser Pflichten hat die schadenersatzrechtliche Haftung für schuldhaft verursachten Schaden, der der Einrichtung dadurch entstanden ist, zur Folge.

Um der Pflicht nach § 31 Abs. 1 nachkommen zu können, haben sich die Leitungsorgane wesentlicher und wichtiger Einrichtungen die notwendigen Fähigkeiten im Bereich der Cybersicherheit in Form von Schulungen anzueignen. Darüber hinaus sind auch den übrigen Mitarbeitern – abhängig von ihrem jeweiligen Arbeitsbezug mit Netz- und Informationssystemen – von den Einrichtungen regelmäßige Cybersicherheitsschulungen anzubieten. Die Einrichtung hat dafür Sorge zu tragen, dass 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. Dies ist in Umsetzung des Art. 21 Abs. 2 Buchstabe g NIS-2-Richtlinie auch gemäß § 32 Abs. 1 iVm Punkt 6 der Anlage 3 dieses Bundesgesetzes ein Teilbereich der gebotenen Risikomanagementmaßnahmen.

Zu § 32 (Risikomanagementmaßnahmen im Bereich der Cybersicherheit)

Mit dieser Bestimmung wird Art. 21 der NIS-2-Richtlinie umgesetzt.

Abs. 1 regelt, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen in den Bereichen der Anlage 3 umzusetzen haben. Diese Risikomanagementmaßnahmen müssen Risiken für die Sicherheit der Netz- und Informationssysteme, die für den Betrieb oder die Erbringung ihrer Dienste genützt werden, sowie Auswirkungen von Cybersicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste entsprechend adressieren.

In der zugehörigen Anlage 3 werden jene Bereiche aufgelistet, welche den Normunterworfenen als thematischer Rahmen für die Umsetzung der Risikomanagementmaßnahmen dienen soll. Die Definition

und Struktur der Bereiche sind stark an Ausarbeitungen auf europäischer Ebene im Rahmen der Kooperationsgruppe (vgl. § 3 Z 34) angelehnt.

Eine organisatorische Risikomanagementmaßnahme im Bereich der Netzwerksicherheit wäre beispielweise eine von der dafür innerhalb der Einrichtung zuständigen und verantwortlichen Stelle in Kraft gesetzte Richtlinie, welche diesbezügliche Prozesse und Vorgaben definiert. Dabei ist nicht ausgeschlossen, dass – im Fall von Unternehmensgruppen – für die innerhalb der jeweiligen Einrichtung geltenden Vorgaben und Prozesse auch Richtlinien übernommen und in Kraft gesetzt werden, die von innerhalb dieser Gruppe übergeordneten Unternehmen (etwa der Konzernmutter) vorgegeben sind. Diese Richtlinien sind gegebenenfalls für die jeweilige Einrichtung zu ergänzen. Entsprechendes gilt für Einrichtungen im Sektor der öffentlichen Verwaltung.

Eine technische Risikomanagementmaßnahme stellt unter anderem der Einsatz von technischen Lösungen, wie etwa Firewalls zum Kontrollieren und Absichern des Übergangs zwischen unterschiedlichen Netzwerkbereichen dar. Das Vorsehen einer für den Betrieb einer solchen technischen Lösung notwendigen fachkundigen Betriebsmannschaft wäre beispielsweise eine operative Risikomanagementmaßnahme in diesem Bereich. Durch Abs. 2 soll klargestellt werden, dass bei der Umsetzung von Risikomanagementmaßnahmen weitere relevante Aspekte von wesentlichen und wichtigen Einrichtungen zu beachten sind:

Zunächst wird den betroffenen Einrichtungen auferlegt, ein dem bestehenden Risiko angemessenes Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten, was den risikobasierten Ansatz bei der Umsetzung von Risikomanagementmaßnahmen unterstreicht (Abs. 2 Z 1).

Hierbei sind der Stand der Technik und gegebenenfalls einschlägigen nationalen, europäischen und internationalen Normen sowie Best-Practices entsprechend zu berücksichtigen (lit. a). Unter den hierbei erwähnten Normen sind insbesondere solche gemäß Art. 2 Nr. 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung zu verstehen. Best-Practices können in diesem Zusammenhang als sich bewährte Verfahren und Methoden bei der Umsetzung von Risikomanagementmaßnahmen verstanden werden. Zudem sollten, aus der Umsetzung von dem Stand der Technik und gegebenenfalls einschlägigen nationalen, europäischen und internationalen Normen sowie bewährte Verfahren(allgemein bewährte Verfahren und Methoden) berücksichtigenden Risikomanagementmaßnahmen keine unverhältnismäßigen finanziellen und administrativen Belastungen für wesentliche und wichtige Einrichtungen entstehen, weshalb die Kosten der Umsetzung (lit. b) der Risikomanagementmaßnahmen in einem angemessenen Verhältnis zum bestehenden Risiko bzw. den bestehenden Risiken stehen sollten, denen das betreffende Netz- und Informationssystem ausgesetzt ist.

Da Gefahren für die Sicherheit von Netz- und Informationssystemen unterschiedliche Ursachen haben können, ist es von großer Relevanz, dass die umzusetzenden Risikomanagementmaßnahmen auf einem gefahrenübergreifenden Ansatz beruhen (Abs. 2 Z 2). Dieser zielt darauf ab, dass Netz- und Informationssysteme und ihr physisches Umfeld vor Ereignissen wie beispielsweise Diebstahl, Feuer, Überschwemmungen, Telekommunikations- oder Stromausfällen oder vor unbefugtem physischen Zugang zu Informationen und Datenverarbeitungsanlagen einer wesentlichen oder wichtigen Einrichtung geschützt werden. Dementsprechend ist daher auch die physische Sicherheit und die Sicherheit des Umfelds von Netz- und Informationssystemen zu berücksichtigen, indem Maßnahmen zum Schutz dieser Systeme vor Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen einbezogen werden. In diesem Zusammenhang sollten sich die wesentlichen und wichtigen Einrichtungen im Rahmen ihrer Risikomanagementmaßnahmen beispielsweise auch mit der Sicherheit des Personals befassen und über angemessene Konzepte für die Zugangskontrolle verfügen.

Besonders wichtig ist die Bewältigung von Risiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten, z. B. Anbietern von Datenspeicherungs- und -verarbeitungsdiensten oder Anbietern von verwalteten Sicherheitsdiensten und Softwareherstellern, betreffen, da sich die Vorfälle häufen, bei denen Einrichtungen Opfer von Cyberangriffen werden und es böswilligen Akteuren gelingt, die Sicherheit der Netz- und Informationssysteme zu beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Diensten Dritter ausgenutzt werden. Wesentliche und wichtige Einrichtungen haben daher Schwachstellen von unmittelbaren Lieferanten und Anbietern sowie die Gesamtqualität und Widerstandsfähigkeit der Produkte und Dienste, die darin enthaltenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Cybersicherheitsverfahren ihrer Lieferanten und Anbieter, einschließlich der Sicherheit deren Entwicklungsprozesse, zu bewerten und zu berücksichtigen, um die Sicherheit ihrer Lieferketten gewährleisten zu können (Abs. 2 Z 3). Beispielsweise hat eine wesentliche oder wichtige Einrichtung Risiken und Abhängigkeiten, die sich aus den Beziehungen zu einem unmittelbaren Diensteanbieter ergeben, zu identifizieren, zu bewerten und

entsprechend zu behandeln, aber auch bei der Auswahl von neuen Lieferanten oder Anbietern oder bei vertraglichen Vereinbarungen generell die zuvor genannten Aspekte zu berücksichtigen.

Bei der Bewertung der verhältnismäßigen Umsetzung von Risikomanagementmaßnahmen (Abs. 3) sind Faktoren wie das Ausmaß der Risikoexposition der 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. Aufgrund der Tatsache, dass innerhalb einer Einrichtung diese Faktoren wie beispielsweise Risikoexposition oder Schweregrad der Auswirkung von Cybersicherheitsvorfällen auf ihre Dienste nicht für alle Netz- und Informationssysteme zwingend identisch sein werden, werden sich innerhalb einer Einrichtung voraussichtlich unterschiedliche Verhältnismäßigkeiten ergeben und daraus unterschiedliche Ausprägungen bei der Umsetzung von spezifischen Risikomanagementmaßnahmen ableiten lassen.

Nach Abs. 4 hat der Bundesminister für Inneres mit Verordnung die Risikomanagementmaßnahmen in den Themengebietender Anlage 3 hinsichtlich technischer, operativer und organisatorischer Anforderungen präzisierend festzulegen. Darüber hinaus kann der Bundesminister für Inneres sektorspezifische Anforderungen an diese Risikomanagementmaßnahmen ebenfalls mit Verordnung festlegen. Diese Spezifizierungen dienen dazu, den Normunterworfenen einen klaren Rahmen vorzugeben, innerhalb dessen Risikomanagementmaßnahmen verhältnismäßig, geeignet und dem Risiko angemessen umzusetzen. Dabei sind überdies der Stand der Technik, gegebenenfalls die einschlägigen Normen und Best-Practices sowie die Kosten der Umsetzung zu berücksichtigen. Die dem Betriebsrat sowie sonstigen Betroffenen zustehenden (Mitbestimmungs-)Rechte, insbesondere jene nach dem Arbeitsverfassungsgesetz sowie der DSGVO, bleiben unberührt.

Zu § 33 (Nachweis der Wirksamkeit von Risikomanagementmaßnahmen)

Sowohl wesentliche als auch wichtige Einrichtungen haben der Cybersicherheitsbehörde sechs Monate nach diesbezüglicher Aufforderung eine Aufstellung der von ihnen umgesetzten Risikomanagementmaßnahmen zu übermitteln (Selbstdeklaration), wobei die Übermittlung in strukturierter Form nach den Vorgaben der Cybersicherheitsbehörde (etwa hinsichtlich notwendiger Inhalte, Format bzw. Struktur oder Art der Übermittlung) erfolgen soll (Abs. 1). Die Vorgehensweise ist insbesondere Art. 31 Abs. 2 NIS-2-Richtlinie entnommen, nach dem den zuständigen Behörden der Mitgliedstaaten eingeräumt werden kann, ihre Aufsichtsaufgaben zu priorisieren und diese Priorisierung auf einem risikobasierten Ansatz beruhen soll. (Teil-)Sektorale Risikoanalysen der Cybersicherheitsbehörde können beispielsweise als Basis für die Aufforderung der Übermittlung einer Selbstdeklaration dienen. Durch die Regelungen in Abs. 2 und 3 soll zudem das von der NIS-2-Richtlinie vorgesehene differenzierte Aufsichtssystem – wesentliche Einrichtungen sind ex ante, wichtige Einrichtungen ex post zu kontrollieren – aufgegriffen werden:

Wesentliche Einrichtungen sollen ab der Aufforderung durch die Cybersicherheitsbehörde drei Jahre Zeit haben, den in ihrer Selbstdeklaration angegebenen Umsetzungsstand der Risikomanagementmaßnahmen der Behörde nachzuweisen. Vorgesehen ist, dass dies durch Übermittlung eines Prüfberichts als Resultat einer Prüfung durch eine unabhängige Stelle geschieht und soll die Übermittlung nach den Vorgaben der Cybersicherheitsbehörde in strukturierter Form zu erfolgen haben (als Beispiele für derartige Vorgaben siehe auch die Erläuterungen zu Abs. 1). Ein solcher Prüfbericht soll die Wirksamkeit der umgesetzten Risikomanagementmaßnahmen zu beschreiben haben, geht dabei gegebenenfalls auf festgestellte Mängel eingehen und einen diese adressierenden Maßnahmenplan enthalten. Wesentlich ist, dass ein Prüfbericht von einem Leitungsorgan sowohl der wesentlichen Einrichtung als auch der unabhängigen Stelle sowie den eingesetzten unabhängigen Prüfern zu unterzeichnen sein soll (Abs. 2).

Im Gegensatz dazu sollen wichtige Einrichtungen nur bei Vorliegen von Nachweisen oder sonstigen Hinweisen und Informationen, wie etwa Angaben in ihrer Selbstdeklaration, Medienberichten oder Meldungen, die der Cybersicherheitsbehörde nahelegen, dass die jeweilige wichtige Einrichtung ihrer Verpflichtung zur Umsetzung der Risikomanagementmaßnahmen mutmaßlich nicht nachkommt, die Umsetzung der Risikomanagementmaßnahmen mittels einer Prüfung durch eine unabhängige Stelle und durch Übermittlung eines Prüfberichts nachzuweisen haben. Für den Prüfbericht sollen die gleichen Regelungen wie oben gelten, allein der Fristenlauf beginnt nicht mit der Aufforderung zur Selbstdeklaration, sondern der Aufforderung zur Übermittlung eines Prüfberichts durch die Cybersicherheitsbehörde (Abs. 3).

Die Kosten der Prüfung durch die unabhängige Stelle sollen grundsätzlich von der wesentlichen bzw. wichtigen Einrichtung zu tragen sein, außer die Cybersicherheitsbehörde trifft in hinreichend begründeten Fällen eine anderslautende Entscheidung (Abs. 4).

Um sicherzustellen, dass die Behörde ihre Aufsichtsmaßnahme gemäß § 38 Abs. 1 Z 1 letzter Fall sinnvoll ausüben kann, haben wesentliche und wichtige Einrichtungen der Cybersicherheitsbehörde

geplante Prüfungen spätestens einen Monat vor Beginn der Durchführung bekanntzugeben und dabei auch einen Prüfplan nach den Vorgaben der Cybersicherheitsbehörde zu übermitteln, in dem erkennbar ist, zu welchem Zeitpunkt oder zu welchen Zeitpunkten die unabhängige Stelle durch welche unabhängigen Prüfer und an welchen Örtlichkeiten der jeweiligen Einrichtung prüfen wird (Abs. 5).

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 sektorenspezifischen 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 Sicherheitsvorfalles soll nicht dazu führen, dass die meldende Einrichtung die Ressourcen von Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen – was vorrabgig 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 §§ 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 Buchstabe 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 nach § 37, die von diesen Einrichtungen ergangen sind.

Zu § 35 (Erheblicher Cybersicherheitsvorfall)

Mit dieser Bestimmung wird Art. 23 Abs. 3 NIS-2-Richtlinie umgesetzt und präzisiert, wann ein Cybersicherheitsvorfall als nach § 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 BGBl. 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.

Der Bundesminister für Inneres 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 aus wesentliche und wichtige Einrichtungen)

Mit dieser Bestimmung sollen Art. 32 und 33 NIS-2-Richtlinie derart umgesetzt werden, dass die darin angeführten Aufsichtsmaßnahmen und diese betreffende 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. Auch hier ist wieder der Unterschied im Aufsichtssystem zwischen wesentlichen und wichtigen Einrichtungen abgebildet:

Während die aufgezählten Maßnahmen bezüglich wesentlicher Einrichtungen jederzeit vorgenommen werden können, darf sie die Cybersicherheitsbehörde hinsichtlich wichtiger Einrichtungen – wie analog in § 33 Abs. 3 geregelt – 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 nach § 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. Darüber hinaus kann die Cybersicherheitsbehörde die in Abs. 1 angeführten Aufsichtsmaßnahmen auch gegenüber unabhängigen Stellen ergreifen, um die Einhaltung der an diese gestellten Anforderungen kontrollieren zu können (vgl. § 7 Abs. 3).

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 sowie hinsichtlich der Anforderungen von unabhängigen Stellen 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, die Prüfer von unabhängigen Stellen bei ihren Prüfhandlungen im Rahmen von Prüfungen bei wesentlichen oder wichtigen Einrichtungen kontrollierend zu begleiten (‘Witnessaudits’). Dies ist ein wichtiges Instrument, mit dem nicht nur die Einhaltung der Verpflichtungen durch die jeweils kontrollierte Einrichtung, sondern auch die Qualität der Prüfhandlungen von unabhängigen Prüfern durch die Cybersicherheitsbehörde beurteilt werden kann.

Die Cybersicherheitsbehörde ist zudem befugt, bei wesentlichen und wichtigen Einrichtungen sowie unabhängigen Stellen 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. 1 Z 14 dar.

Die Cybersicherheitsbehörde ist ebenfalls befugt, von wesentlichen und wichtigen Einrichtungen sowie unabhängigen Stellen 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 (z. B. Richtlinien), Unterlagen und Protokolle zu operativen Vorgängen (z. B. Protokolle durchgeführter Wartungstätigkeiten) aber auch technische Detailinformationen (z. B. 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 (z. B. 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 der Verordnung (EU) 2019/881 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 sowie Abs. 5 und Art. 33 Abs. 4 lit. a bis g 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. 1a).

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

Mit dieser Bestimmung wird Art. 24 NIS-2-Richtlinie umgesetzt.

Zu § 41 (Beschwerdeverfahren)

Diese Bestimmung legt fest, dass gegen Bescheide des Bundesministers für Inneres und wegen Verletzung seiner Entscheidungspflicht Beschwerde an das Verwaltungsgericht 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 bis § 43) werden datenschutzrechtliche Bestimmungen zur Verarbeitung von personenbezogenen Daten gemäß Art. 4 Nr. 2 DSGVO und § 36 Datenschutzgesetz (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, 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 Buchstabe b DSGVO), der

Datenminimierung (Art. 5 Abs. 1 Buchstabe 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 AS-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 Abs. 2 und § 34 Abs. 4 sowie § 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 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 Buchstabe d DSGVO). Dasselbe gilt für den Fall, dass der Betroffene die Einschränkung der Verarbeitung gemäß Art. 18 Abs. 1 Buchstabe a oder Buchstabe 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.

Zu § 43 (Datenübermittlungen)

Der Bundeskanzler, der Bundesminister für Inneres, 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 abzuwehrende 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.

Der Bundesminister für Inneres kann gemäß Abs. 2 darüber hinaus personenbezogene Daten an bestimmte ausländische Sicherheitsbehörden und Sicherheitsorganisationen (§ 2 Abs. 2 und 3 Polizeikooperationsgesetz) 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 BGBl. I Nr. 111/2018. Hinsichtlich der Übermittlung in Drittstaaten sind die Vorgaben des Kapitels 5 der DSGVO sowie von §§ 58 f DSG einzuhalten.

Der Bundesminister für Inneres 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 Analaufstellen 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 Einrichtungengemäß § 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, sind Verwaltungsstrafen von den Bezirksverwaltungsbehörden als zuständige Behörden nach den verfahrensrechtlichen Bestimmungen des Verwaltungsstrafgesetzes 1991 – VStG, BGBl. Nr. 52/1991, zu verhängen. Angemerkt wird, dass mit Blick auf die erforderliche Expertise zum Zwecke der Zuständigkeitskonzentration mit Landesgesetz die sprengelübergreifende Zusammenarbeit von Bezirksverwaltungsbehörden vorgesehen werden kann (‘Kompetenzzentren’; vgl. etwa § 1 des Landesgesetzes über die Kooperation zwischen Bezirksverwaltungsbehörden in Oberösterreich, LGBl. Nr. 103/2018, sowie § 2a des Gesetzes vom 14. Februar 1977 über die Organisation der Bezirkshauptmannschaften, LGBl. Nr. 11/1977).

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 der Bundesminister für Inneres 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 des Bundesministers für Inneres 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 dem Bundesminister für Inneres 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. 1a angeordnet werde, 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. 7).

Die Verhängung von Geldstrafen gegen juristische Personen oder gegen eingetragene Personengesellschaften orientiert sich an § 99d BWG. Unter Berücksichtigung des Doppelstrafverbots und in Orientierung an § 30 Abs. 3 DSG kann von der Bestrafung eines Verantwortlichen gemäß § 9 VStG abgesehen werden, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person oder die eingetragene Personengesellschaft verhängt wird (Abs. 2, 3 und 4).

Abs. 5 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 Buchstabe i DSGVO war, keine Geldbuße nach Art. 34 der vorliegenden Richtlinie verhängen. Dem soll durch die Regelung in Abs. 6 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 Risikomanagamentmaßnahmen 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-Namensregistern und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, hinsichtlich der Führung bzw. Erteilung von Zugang zu der gemäß Abs. 30 zu führenden Datenbank zum Gegenstand.

Wesentlich ist, dass die Abs. 1 bis 4 auf Behörden, Organe sowie Einrichtungen und sonstige Stellen der öffentlichen Verwaltung, unabhängig davon, ob sie hoheitlich oder im Rahmen der Privatwirtschaftsverwaltung eingerichtet oder tätig sind, keine Anwendung finden sollen (vgl. Abs. 5). Die Formulierung ‘Behörden und sonstige Stellen der öffentlichen Verwaltung, wie insbesondere in Formen des öffentlichen Rechts sowie des Privatrechts eingerichtete Stellen’ soll an § 30 Abs. 5 DSG

angelehnt werden, wobei keine Einschränkung auf öffentliche Stellen, ‘die im gesetzlichen Auftrag handeln’ erfolgen soll. Klargestellt ist daher, dass neben der Hoheitsverwaltung auch die gesamte Privatwirtschaftsverwaltung von dieser Regelung umfasst sein soll. Organwalter 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 Organwalter (im Rahmen der Privatwirtschaftsverwaltung, vgl. VwGH vom 21.10.1992, 92/10/0111 in Bezug auf den Bürgermeister einer Gemeinde; siehe auch VfGH 25.6.2015, E 473/2015) – in Frage kommen.

Zu § 46 (Nichteinhaltung von Verpflichtungen durch Stellen der öffentlichen Verwaltung):

Angelehnt an die im vorgeschlagenen § 44 Abs. 1 normierte Anzeigepflicht des Bundesministers für Inneres 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 dem Bundesminister für Inneres festgelegt werden.

Vor dem Hintergrund, dass unter bestimmten Voraussetzungen auch Behörden und sonstige Stellen der öffentlichen Verwaltung vom Anwendungsbereich der NIS-2-RL umfasst sind, bedarf es zur unionsrechtskonformen Umsetzung des Art. 36 NIS-2-RL eines wirksamen alternativen Sanktionsmechanismus im Sinne dieser Bestimmung. Wesentlich ist, dass es sich bei den Adressaten des alternativen Sanktionsmechanismus in Abs. 2 um jene des § 45 Abs. 5 handeln soll. Die zuständige Bezirksverwaltungsbehörde soll demnach bescheidmäßig die Nichteinhaltung der sich aus diesem Bundesgesetz ergebenden Verpflichtungen festzustellen haben. Wesentlich ist, dass die Bezirksverwaltungsbehörde mit diesem Bescheid eine angemessene Frist für die Herstellung des rechtmäßigen Zustandes anzuordnen haben soll. Wird dem Bescheid nicht ordnungsgemäß innerhalb der angeordneten Frist entsprochen, soll die Bezirksverwaltungsbehörde nach Eintritt der formellen Rechtskraft des Bescheides 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. Dabei soll die Bezirksverwaltungsbehörde darauf Bedacht zu nehmen haben, dass die Veröffentlichung keine Gefahr für die öffentliche Ordnung oder Sicherheit darstellt und sollen allenfalls bloß jene Informationen über die Nichteinhaltung von Verpflichtungen nach diesem Bundesgesetz öffentlich bekannt gemacht werden, die keine konkreten Rückschlüsse auf die mit der Pflichtverletzung einhergehenden Sicherheitsmängel zulassen.

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-RL hinreichend Genüge getan.

Zur Anwendbarkeit dieser Bestimmung sowohl auf den Bereich der Hoheitsverwaltung als auch der Privatwirtschaftsverwaltung siehe auch die Erläuterungen zu § 45 Abs. 5.

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 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, 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 ist grundsätzlich der Bundesminister für Inneres betraut, da dieser die Aufgaben der Cybersicherheitsbehörde wahrnimmt (§ 50 Abs. 1 Z 4).

Davon abweichend obliegt der Bundesregierung (Z 1) die Vollziehung dieses Bundesgesetzes hinsichtlich der Erlassung der nationalen Cybersicherheitsstrategie (§ 15 Abs. 1).

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

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

Dem Bundesminister für Inneres obliegt nach Abs. 2 die Besorgung der allgemeinen Angelegenheiten der in § 4 Abs. 1 genannten Aufgaben, worunter auch die legistische Tätigkeit zu verstehen ist.

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

Mit dieser Bestimmung wird das Inkrafttreten dieses Gesetzes, das Außerkrafttreten des NISG und der auf dessen Grundlage erlassenen Verordnungen sowie der Übergang vom NISG auf das NISG 2024 geregelt. Das NISG 2024 tritt mit 1. Juni 2025 in Kraft. Bis zu diesem Zeitpunkt ist die NIS-2-Richtlinie im nationalen Recht der Mitgliedstaaten umzusetzen.

Verordnungen auf Grund dieses Bundesgesetzes können bereits ab dem auf seine Kundmachung folgenden Tag erlassen werden. Ab diesem Zeitpunkt ist das Gesetz in Geltung. Allerdings treten die Bestimmungen des Gesetzes jedenfalls mit 1. Juni 2025 in Kraft. Um ein Auseinanderfallen der Geltung und des Inkrafttretens der Verordnungsermächtigung mit jenem des Gesetzes zu vermeiden, wird das Inkrafttreten der Verordnung frühestens für den 1. Juni 2025 vorgesehen. Um eine rasche Umsetzung des Gesetzes und Konkretisierung der darin getroffenen Vorgaben zu gewährleisten, sind alle vorbereitenden Maßnahmen bereits ab dem Zeitpunkt der Geltung des Gesetzes (dem der Kundmachung dieses Bundesgesetzes folgenden Tag) zu setzen, soweit sie nicht bereits erfolgt sind.

Das NISG, Netz- und Informationssystemsicherheitsverordnung (NISV), BGBl. II Nr. 215/2019, und die Verordnung über qualifizierte Stellen (QuaSteV), BGBl. II Nr. 226/2019, treten mit Ablauf des 1. Juni 2025 außer Kraft.

Hinsichtlich der Wirksamkeit von Bescheiden, die auf Basis des NISG erlassen wurden, wird festgelegt, dass diese mit Inkrafttreten dieses Bundesgesetzes gegenstandslos werden. Von der Möglichkeit der Ermittlung aller Betreiber wesentlicher Dienste als wesentliche Einrichtung, wurde in Hinblick auf Art. 7 B-VG kein Gebrauch gemacht. Betreiber wesentlicher Dienste § 16 Abs. 1 NISG sind jedoch in der Regel nunmehr als wesentliche Einrichtungen gemäß § 24 Abs. 1 dieses Bundesgesetzes zu qualifizieren.

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.

In Anlage 1 Punkt 1 lit. a (Sektor ‘Energie’, Subsektor ‘Elektrizität’) wird in der 4. Variante (‘Erzeuger’) festgelegt, dass als relevante Arten der Einrichtung darunter lediglich Erzeuger im Sinne des § 7 Abs. 1 Z 17 ElWOG fallen, 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’, Subsektor ‘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 Bundesgesetz zur Festlegung einheitlicher Standards beim Infrastrukturaufbau für alternative Kraftstoffe, BGBl. 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 Nr. 39 Verordnung (EU) 2023/1804 ‘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 Nr. 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 Nr. 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 Mobilitätsdiensleister 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', Subsektor 'Fernwärme') wird die Art der Einrichtung als Betreiber von Fernwärme oder Fernkälte im Sinne des Artikels 2 Nummer 19 der Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates 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 Buchstabe g der Richtlinie 2011/24/EU (Patientenmobilitätsrichtlinie) als maßgebliche Art der Einrichtung definiert. Zum Begriff des 'Gesundheitsdienstleisters' kann auf Anlage 1 der Gesundheitstelematikverordnung 2013 (GTelV 2012) 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), Apotheken sowie Einrichtungen des Rettungswesens.

Demnach handelt es sich bei dem Großteil der in der Anlage 1 der Gesundheitstelematikverordnung 2013 (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 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 Buchstabe g der Richtlinie 2011/24/EU 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, GZ: KII-2/91, 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') wird die maßgebliche Art der Einrichtung unter anderem danach definiert, dass Unternehmen ausgeschlossen sind, 'für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist'. Eine Wirtschaftstätigkeit ist jedenfalls eine wirtschaftliche Tätigkeit. Nicht wirtschaftliche Tätigkeiten scheiden für die Ermittlung dieses Sektors aus. Da die NIS-2-Richtlinie nicht von mehreren 'Hauptwirtschaftstätigkeiten' ausgeht (arg: 'ihre' Hauptwirtschaftstätigkeit), ist sohin darauf abzustellen, ob das Unternehmen unter Berücksichtigung aller wirtschaftlichen Tätigkeiten die Abfallbewirtschaftung die primäre Tätigkeit darstellt, mit der die Wirtschaftlichkeit ihres Handelns sichergestellt ist.

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 des Europäischen Parlaments und des Rates vom 18. Dezember 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. L 396 vom 30.12.2006 S. 1 (im Folgenden REACH-Verordnung) angeführt sind. Hersteller gemäß Art. 3 Nr. 9 REACH-Verordnung bezeichnet natürliche oder juristische Person mit Sitz in der Gemeinschaft, die in der Gemeinschaft einen Stoff herstellt. Händler gemäß Art. 3 Nr. 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 entweder im Großhandel tätig ist oder in der industriellen Produktion und Verarbeitung. Wird eine Einrichtung entweder im Großhandel oder in der industriellen Produktion und Verarbeitung tätig, 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. Letztverwender) verkaufen.

Zur Anlage 3 (Risikomanagementmaßnahmen-Bereiche)

Die Anlage 3 beschreibt jene Bereiche, in denen wesentliche und wichtige Einrichtungen gemäß § 32 verpflichtend geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen zu ergreifen haben. Dadurch sollen die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, beherrscht werden und die Auswirkungen von Cybersicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste verhindert oder möglichst geringgehalten werden.

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. 4):

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 Zusammenschau mit Abs. 4 – die KommAustria), mit Verordnung nähere 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 2024 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 Finanzen und dem Bundesminister für Inneres 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 § 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. xx):

Bei der vorgeschlagenen Änderung handelt es sich um eine erforderliche Anpassung der geltenden Bestimmungen des GTelG 2012 an das NISG 2024.

Abs. 2 stellt klar, dass das Austrian HealthCERT hinkünftig für den Sektor Gesundheitswesen gemäß § 2 Z 5 NISG 2024 die Aufgaben eines sektorspezifischen CSIRT übernehmen soll. Das Austrian HealthCERT hat die Anforderungen, die gemäß § 9 NISG 2024 an ein Computer-Notfallteam gestellt werden mit Ausnahme der Z 8, zu erfüllen. Außerdem soll klargestellt werden, dass die Bestimmungen aus dem NISG 2024, welche sich auf die Ermächtigung des Bundesminister oder der Bundesministerin für Inneres 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 2024 an ein sektorspezifischen gestellt werden, efüllt, wird ebenfalls bereits mit der gegenständlichen Novelle des GTelG 2012 sichergestellt. Da das Austrian HealthCERT auch als sektorspezifisches CSIRT iSd NISG 2024 tätig wird, finden desweiteren die Bestimmungen des NISG 2024, welche sich auf sektorspezifische CSIRTs beziehen, Anwendung.

Die Verarbeitung der Daten erfolgt hierbei auf Grundlage des NISG 2024, 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 2024 die dem Sektor Gesundheitswesen gemäß § 2 Z 5 NISG 2024 angehören, verpflichtet werden, die Meldungen nach den §§ 34 und 37 NISG 2024 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 2024 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 2024 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 2024, nach der DSGVO, dem Medizinprodukterecht 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, der Bundesminister für Landesverteidigung, der Bundesminister für europäische und internationale Angelegenheiten und die CSIRTs sind ermächtigt, personenbezogene Daten zu verarbeiten (§ 42 NISG 2024) 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 2024 bzw. aufgrund innerstaatlicher oder internationaler Amtshilfe (§ 43 Abs. 1, 2 und 3 NISG 2024) erforderlich sein.

Die Kategorien der betroffenen personenbezogenen Daten werden in § 42 Abs. 2 bis 6 NISG 2024 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 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 2024 gewonnen wurden, hat der Bundesminister für Inneres gemäß § 18 NISG 2024 ein Meldeanalysesystem zu betreiben. Weiters ist er gemäß § 13 NISG 2024 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 2024 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 Regelungen zur Amtsverschwiegenheit sowie auf anderweitige Verschwiegenheitspflichten darf verwiesen werden (vgl. etwa Art. 20 B-VG, § 46 BDG 1979). Insbesondere ist aufgrund der durchgehenden Protokollierungspflicht (§ 42 Abs. 3) 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 2024).

– ‘Einschränkung der Rechte der betroffenen Personen’:

Die Einschränkung der Rechte der betroffenen Personen werden in § 42 Abs. 10 NISG 2024 geregelt und gemessen am Zweck des NISG 2024 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. Gleiches 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 2024 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 internationalem Bereich bei einem Null-Szenario ist extrem erhöht, sodass die Datenschutz-Folgenabschätzung klar positiv ausfällt.“

Bei der Abstimmung wurde der Gesetzentwurf in der Fassung des oben erwähnten Abänderungsantrages der Abgeordneten Dr. Christian **Stocker**, Michel **Reimon**, MBA mit Stimmenmehrheit (**dafür:** V, G, **dagegen:** S, F, N) beschlossen.

Als Ergebnis seiner Beratungen stellt der Ausschuss für innere Angelegenheiten somit den **Antrag**, der Nationalrat wolle dem **angeschlossenen Gesetzentwurf** die verfassungsmäßige Zustimmung erteilen.

Wien, 2024 06 19

Eva-Maria Himmelbauer, BSc	**Dr. Christian Stocker**
Berichterstattung	Obmann

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-06-24T15:35:09+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	