Entwurf

Erläuterungen

I. Allgemeiner Teil

Mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (im Folgenden: NIS-RL), die am 8. August 2016 in Kraft getreten ist, soll EU-weit ein hohes Sicherheitsniveau der Netz- und Informationssysteme erreicht werden. Vor diesem Hintergrund soll(en) unter anderem die Zusammenarbeit zwischen den Mitgliedstaaten in strategischer und operationeller Hinsicht gestärkt werden, Mitgliedstaaten eine nationale NIS-Strategie erarbeiten, die strategische Ziele, Prioritäten und Maßnahmen enthalten soll, um in den einzelnen Mitgliedstaaten ein hohes Sicherheitslevel der Netz- und Informationssysteme zu erreichen, nationale Behörden und Computer-Notfallteams benannt werden und bestimmte, für das Gemeinwohl wichtige private und öffentliche Anbieter (Betreiber wesentlicher Dienste und digitale Diensteanbieter) zu angemessenen Sicherheitsmaßnahmen und Meldung erheblicher Störfälle verpflichtet werden.

Betreiber eines wesentlichen Dienstes stellen einen Dienst der in Anhang II der NIS-RL genannten und im Folgenden aufgelisteten Sektoren zur Verfügung: Energie (Elektrizität, Erdöl, Erdgas), Verkehr (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr), Bankwesen (Kreditinstitute), Finanzmarktinfrastrukturen (Betreiber von Handelsplätzen, zentrale Gegenparteien), Gesundheitswesen (Einrichtungen der medizinischen Versorgung, einschließlich Krankenhäuser und Privatkliniken), Trinkwasserlieferung und -versorgung (Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“), Digitale Infrastruktur (Internet Exchange Points, DNS-Diensteanbieter, TLD-Name-Registries). Ferner sollen (ohne entsprechende RL-Vorgabe) bestimmte Einrichtungen des Bundes im Rahmen der österreichischen Umsetzung berücksichtigt werden.

Digitale Diensteanbieter sind – ab einer gewissen Größe – sämtliche Anbieter eines Online-Marktplatzes, einer Online-Suchmaschine oder eines Cloud-Computing-Dienstes.

In Österreich wird die NIS-RL mit dem vorliegenden Bundesgesetz (Netz- und Informationssystemsicherheitsgesetz – NISG) umgesetzt. Dabei sollen Aufgaben, die sich aus der NIS-RL ergeben, bereits bestehenden Strukturen übertragen werden. Der Bundeskanzler wird die strategischen Aufgaben wahrnehmen und somit als „strategisches NIS-Büro“ fungieren, der Bundesminister für Inneres wird die operativen Aufgaben wahrnehmen und somit als „operatives NIS-Büro“ fungieren.

Die Hauptgesichtspunkte sind im Einzelnen:

- die Festlegung von Aufgaben und Behördenzuständigkeiten sowie Befugnissen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen;
- die Festlegung einer nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;
- die Ermittlung der vom Anwendungsbereich konkret erfassten Betreiber wesentlicher Dienste anhand der in einer Verordnung noch näher zu definierenden Teilsektoren und Faktoren;
- die Regelung zweier Arten von Verpflichtungen für die ermittelten Betreiber wesentlicher Dienste, die digitalen Diensteanbieter und Einrichtungen des Bundes: Diese haben a) angemessene Sicherheitsvorkehrungen für ihre Netz- und Informationssysteme vorzusehen und b) Sicherheitsvorfälle an die zuständigen Stellen zu melden;

- die Überprüfung der Einführung geeigneter Sicherheitsvorkehrungen und Einhaltung der Meldepflicht. Während bei Betreibern wesentlicher Dienste diese Überprüfungen jederzeit – zumindest aber alle drei Jahre – durchgeführt werden können, ist dies bei digitalen Diensteanbietern nur im Anlassfall zulässig;
- die Einrichtung von Computer-Notfallteams und Festlegung der Aufgaben, die diesen zukommen sollen;
- die Regelung von Strukturen, Aufgaben und Befugnissen im Falle der Cyberkrise;
- die Festlegung von Sanktionen bei Nichteinhaltung der nach diesem Bundesgesetz einzuhaltenden Pflichten.

Zuständigkeit des Bundes

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 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 5 B-VG.

In jenen Bereichen, in denen die Länder zur Vollziehung zuständig sind, beruht die Zuständigkeit des Bundes auf der in § 1 NISG geschaffenen Kompetenzgrundlage.

II. Besonderer Teil

Zu § 1 (Verfassungsbestimmung):

Die Vorschriften in diesem Bundesgesetz, mit dem insb. die NIS-RL 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-RL gemäß Art. 12 B-VG in die Ausführungsgesetzgebungs- und Vollziehungszuständigkeit der Länder bzw. gemäß Art. 11 B-VG in die Vollziehungszuständigkeit der Länder oder gemäß Art. 15 Abs. 1 B-VG in die Gesetzgebungs- und Vollziehungszuständigkeit der Länder:

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 um das Rettungswesen handelt, in die Gesetzgebungs- und Vollziehungszuständigkeit der Länder (Art. 15 Abs. 1 B-VG).

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.

Die in Aussicht genommene Begründung einer Zuständigkeit des Bundeskanzlers und des Bundesministers für Inneres ist für jene Bereiche, in denen die Länder zur Gesetzgebung bzw. Vollziehung zuständig sind, nach geltender Verfassungsrechtslage nicht zulässig und bedarf daher einer Verfassungsänderung.

Zu § 2 (Gegenstand und Ziele des Gesetzes):

Netz- und Informationssysteme mit den zugehörigen Diensten spielen eine zentrale Rolle in der heutigen Gesellschaft. Für wirtschaftliche und gesellschaftliche Tätigkeiten ist es daher von entscheidender Bedeutung, dass sie 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.

In Abs. 1 wird der sachliche Anwendungsbereich des NISG festgelegt. Umfasst sind Betreiber wesentlicher Dienste (§ 3 Z 8) aus den in Abs. 1 Z 1 bis 7 genannten Sektoren, Anbieter digitaler Dienste (§ 3 Z 10) und Einrichtungen des Bundes (§ 3 Z 15). Die in Abs. 1 genannten Sektoren werden in der Verordnung, die gemäß § 14 Abs. 4 zu erlassen ist, noch weiter konkretisiert, insbesondere werden in dieser Verordnung auch die betroffenen Teilsektoren und die darin erbrachten wesentlichen Dienste genannt. Beispielsweise fallen in den Sektor Energie die Teilsektoren Elektrizität, Erdöl und Erdgas und in den Sektor Verkehr die Teilsektoren Luftverkehr, Schienenverkehr, Schifffahrt und Straßenverkehr. Der Betrieb von Rechenzentren fällt unter keinen der genannten Sektoren, ist aber im Rahmen einer Dienstleisterstellung für die Betreiber wesentlicher Dienste von den Verpflichtungen (zB sind angemessene und geeignete Sicherheitsvorkehrungen zu ergreifen) grundsätzlich mitumfasst.

Die betroffenen Einrichtungen des Bundes sind die Bundesministerien, die Gerichtshöfe des öffentlichen Rechts (VfGH und VwGH), der Rechnungshof, die Volksanwaltschaft, die Präsidentschaftskanzlei und die Parlamentsdirektion, mitsamt all ihren Organisationseinheiten und der damit verbundenen technischen Infrastruktur. Diese Liste von Einrichtungen orientiert sich insbesondere an der dem Sicherheitspolizeirecht bekannten Begrifflichkeit der verfassungsmäßigen Einrichtungen, ist jedoch beschränkt auf Einrichtungen, die dem Bund zuzuordnen und in § 3 Z 15 aufgelistet sind. Mit der Aufnahme dieser Einrichtungen des Bundes geht das vorliegende Bundesgesetz bei der Betroffenheit von öffentlichen Stellen ausdrücklich über den Anwendungsbereich der NIS-RL hinaus. Dies ist erforderlich, weil alle genannten Einrichtungen, also Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes, gleichermaßen das Funktionieren des Gemeinwesens gewährleisten und für die Daseinsvorsorge daher von hoher Bedeutung sind: Der Ausfall eines Dienstes in einem dieser Bereiche kann unter Umständen die öffentliche Sicherheit oder die Funktionsfähigkeit staatlicher Einrichtungen gefährden und zu Versorgungsengpässen führen. Die Funktionsfähigkeit staatlicher Einrichtungen kann auch insbesondere dann gefährdet sein, wenn ein Sicherheitsvorfall nicht bei der staatlichen Einrichtung selbst, sondern bei einem Energieversorger auftritt, von dessen Dienst die betroffene Einrichtung bei der Erbringung der eigenen Leistung abhängig ist.

Um ein hohes Sicherheitsniveau von Netz- und Informationssystemen zu erreichen, werden in diesem Bundesgesetz insbesondere die in Abs. 2 genannten Maßnahmen vorgesehen. Neben den Verpflichtungen die Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes treffen, werden eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen, Behördenzuständigkeiten und -befugnisse sowie Koordinationsstrukturen für den Bereich der Netz- und Informationssystemsicherheit und die Aufgaben und Anforderungen der Computer-Notfallteams festgelegt.

Zu § 3 (Begriffsbestimmungen):

In § 3 werden Begriffsbestimmungen festgelegt. Wo es keiner nationalen Legaldefinition bedarf, sollen die in Art. 4 NIS-RL geregelten Definitionen direkt übernommen werden; darüber hinaus sollen begriffliche Anpassungen und zusätzliche Definitionen vorgenommen werden.

Netz- und Informationssysteme (Z 1) sind elektronische Kommunikationsnetze, wie sie auch in § 3 Z 11 Telekommunikationsgesetz 2003 (TKG 2003) definiert werden. Darüber hinaus versteht man darunter aber auch räumlich verteilte, digitale Hochgeschwindigkeitsverarbeitungsvorrichtungen zur technischen

Unterstützung der Erhebung, Verarbeitung, Speicherung, Wartung, Nutzung, Weitergabe, Verbreitung oder Disposition von Informationen. Auch die Daten, die in einem solchen elektronischen Kommunikationsnetz oder Vorrichtung verarbeitet werden, sind von dem Begriff umfasst.

Der Begriff der Netz- und Informationssystemsicherheit (NIS) (Z 2) umfasst nicht nur die Fähigkeit von Netz- und Informationssystemen, Sicherheitsvorfälle abzuwehren, sondern auch die Fähigkeit, Sicherheitsvorfällen präventiv vorzubeugen, eine bereits entstandene Störung zu beseitigen und möglichst rasch den Normalbetrieb wieder herzustellen. NIS trägt dazu bei, Gefährdungen zu erkennen, bewerten und verfolgen, die Fähigkeit zu stärken, Störungen zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wiederherzustellen.

Die Abkürzung „NIS-RL“ (Z 3) für die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union hat sich gemeinsam mit der Abkürzung „NIS“ für die Sicherheit von Netz- und Informationssystemen im Sprachgebrauch eingebürgert und soll daher auch in diesem Bundesgesetz verwendet werden.

Die NIS-Büros (Z 4) sind beim Bundeskanzler und dem Bundesminister für Inneres eingerichtet. Ihnen kommen die sich aus der Umsetzung der NIS-RL ergebenden Aufgaben nach diesem Bundesgesetz zu. Während der Bundeskanzler vornehmlich strategische Aufgaben wahrnimmt, kommen dem Bundesminister für Inneres hauptsächlich operative Aufgaben zu. Bereits bestehende und in anderen Gesetzen geregelte Aufgaben und Verpflichtungen im jeweiligen Zuständigkeitsbereich bleiben von diesem Bundesgesetz unberührt.

Auf Basis sowie unter Einbindung bereits bestehender, operativer Strukturen wird eine neue Struktur zur Koordination auf der operativen Ebene (OpKoord) (Z 5) geschaffen. In ihrem Rahmen soll insbesondere ein periodisches und anlassbezogenes Lagebild erstellt, erörtert und aktualisiert sowie über zu treffende Maßnahmen auf der operativen Ebene beraten werden. Darüber hinaus soll durch Sammeln, Bündeln, Auswerten und Weitergeben von relevanten Informationen ein kontinuierlicher Überblick über die aktuelle Situation im Bereich der NIS gewährleistet sein. Dabei ist auch die Wirtschaft in geeigneter Form einzubinden und zu informieren. Der permanent und gemeinsam erarbeitete Status zur Situation im Bereich der NIS soll allen Beteiligten als Grundlage für zu treffende planerische, präventive und reaktive Maßnahmen dienen.

Ein Sicherheitsvorfall (Z 6) liegt vor, wenn eine erhebliche Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen zu einem Ausfall oder einer Einschränkung der Verfügbarkeit des betriebenen Dienstes geführt hat. Dieser Dienst ist ein wesentlicher Dienst gemäß § 3 Z 8 iVm § 14 Abs. 2, ein digitaler Dienst gemäß § 3 Z 9 oder ein Dienst, den eine Einrichtung des Bundes erbringt. Damit ein Sicherheitsvorfall im Sinne dieser Definition vorliegt, muss der Dienst für einen längeren Zeitraum vollständig (und nicht nur teilweise) ausgefallen sein (1. Fall). Ein Sicherheitsvorfall liegt auch dann vor, wenn er zwar nicht zu einem vollständigen Ausfall des betriebenen Dienstes, aber zu einer Einschränkung der Verfügbarkeit dieses Dienstes geführt hat (2. Fall). Bei der Beurteilung, ob eine Störung erheblich und somit ein Sicherheitsvorfall ist, 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. Mit Verordnung (§ 14 Abs. 4) können die Parameter für beide Fälle konkretisiert werden.

Im Rahmen des gegenständlichen Gesetzes stellt ein Risiko (Z 7) eine potentielle Gefahrensituation dar, die durch Umstände oder Ereignisse ausgelöst wird, die nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssysteme haben können. Ein Risiko bedarf einer gewissen Qualität, die sich aus der Eintrittswahrscheinlichkeit der Gefahr und der Schwere der Auswirkungen ergibt, sowie eines konkreten Anknüpfungspunkts für das Netz- und Informationssystem der betroffenen natürlichen oder juristischen Person. Ein zeitnaher Angriff auf ein Computersystem mit einer neuen Schadsoftware kann zB eine Risikosituation auslösen, aber auch die Auswirkungen eines Sicherheitsvorfalls (Z 6).

Betreiber wesentlicher Dienste (Z 8) sind private oder öffentliche Einrichtungen, die einen wesentlichen Dienst in einem der in § 2 Abs. 1 genannten Sektoren erbringen. Die Bereitstellung dieses Dienstes muss zu einem überwiegenden Teil von Netz- und Informationssystemen abhängig sein. Dies ist in der Regel dann der Fall, wenn Produktionsprozesse oder die Auslieferung von Leistungen an den Endkunden automationsunterstützt erfolgen.

Digitale Dienste (Z 9) sind Dienste der Informationsgesellschaft, also ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst (§ 1 Abs. 1 Z 2 Notifikationsgesetz 1999), insbesondere der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und

Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern. Die NIS-RL schränkt den Anwendungsbereich auf drei ganz bestimmte digitale Dienste – Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste – ein.

Anbieter digitaler Dienste (Z 10) sind juristische Personen, die einen solchen digitalen Dienst in Österreich anbieten und eine Hauptniederlassung in Österreich haben oder einen Vertreter (Z 11) in Österreich namhaft gemacht haben. Explizit ausgenommen sind natürliche Personen, Kleinstunternehmen und kleine Unternehmen (Unternehmen mit weniger als 50 Mitarbeitern und einem Jahresumsatz bzw. einer Jahresbilanz von unter 10 Mio. Euro). Anbieter digitaler Dienste ohne Hauptniederlassung in der Europäischen Union sind verpflichtet, einen Vertreter (Z 11) in einem Mitgliedstaat namhaft zu machen. Dieser handelt im Auftrag des digitalen Diensteanbieters und ist die Kontaktstelle für die zuständigen Stellen in den Mitgliedstaaten.

Ein Online-Marktplatz (Z 12) ermöglicht es Verbrauchern und Unternehmern, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern abzuschließen, und ist als solcher der endgültige Bestimmungsort für den Abschluss dieser Verträge. Er erstreckt sich nicht auf Online-Dienste, die lediglich als Vermittler für Drittdienste fungieren und durch die letztlich ein Vertrag geschlossen werden kann. Er erstreckt sich deshalb nicht auf Online-Dienste, die die Preise für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern miteinander vergleichen und den Nutzer anschließend an den bevorzugten Unternehmer weiterleiten, damit er das Produkt dort kauft. Die von einem Online-Marktplatz bereitgestellten IT-Dienste können die Verarbeitung von Transaktionen, die Aggregation von Daten oder die Erstellung von Nutzerprofilen einschließen. Als Online-Stores tätige Application-Stores, die den digitalen Vertrieb von Anwendungen oder Software-Programmen von Dritten ermöglichen, sind Online-Marktplätze im weiteren Sinn.

Eine Online-Suchmaschine (Z 13) ermöglicht es dem Nutzer, Suchen grundsätzlich auf allen Websites anhand einer Abfrage zu einem beliebigen Thema vorzunehmen. Sie kann alternativ dazu auf Websites in einer bestimmten Sprache beschränkt sein. Die Definition des Begriffs „Online-Suchmaschine“ erstreckt sich nicht auf Suchfunktionen, die auf den Inhalt einer bestimmten Website beschränkt sind, und zwar unabhängig davon, ob die Suchfunktion durch eine externe Suchmaschine bereitgestellt wird. Sie erstreckt sich auch nicht auf Online-Dienste, die Preise für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern vergleichen und den Nutzer anschließend an den bevorzugten Unternehmer weiterleiten.

Cloud-Computing-Dienste (Z 14) umfassen eine breite Palette von Tätigkeiten, die auf unterschiedliche Weise erbracht werden können. Für die Zwecke der NIS-RL und dieses Bundesgesetzes sind unter dem Begriff „Cloud-Computing-Dienste“ Dienste zu verstehen, die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen. Zu diesen Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Speicher, Anwendungen und Dienste. Der Begriff „skalierbar“ bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. Der Begriff „elastischer Pool“ wird verwendet, um die Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die verfügbaren Ressourcen je nach Arbeitsaufkommen rasch auf- bzw. abgebaut werden können. Der Begriff „gemeinsam nutzbar“ wird verwendet, um die Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst von derselben elektronischen Einrichtung erbracht wird.

Einrichtungen des Bundes sind die Bundesministerien, die Gerichtshöfe des öffentlichen Rechts (VfGH und VwGH), der Rechnungshof, die Volksanwaltschaft, die Präsidentschaftskanzlei und die Parlamentsdirektion, mitsamt all ihren Organisationseinheiten und der damit verbundenen technischen Infrastruktur (Z 15). Der zuständige Bundesminister kann weitere Dienststellen durch Verordnung bestimmen. Die Einrichtungen des Bundes sind für die Funktionsfähigkeit des (Rechts-)Staates und daher für das Gemeinwesen und die Daseinsvorsorge der Bevölkerung von hoher Bedeutung. Sie sollen daher in den Anwendungsbereich dieses Bundesgesetzes aufgenommen werden.

Die Kooperationsgruppe (Z 16) und das CSIRT-Netzwerk (Z 17) sind zwei Gremien, die auf europäischer Ebene unmittelbar aufgrund der NIS-RL eingerichtet wurden und insbesondere der verstärkten Kooperation, dem Informationsaustausch und der Zusammenarbeit zwischen den Mitgliedstaaten der Europäischen Union im Bereich der NIS dienen. Diese Gremien wurden vor Inkrafttreten dieses Bundesgesetzes eingerichtet und tagen seither in regelmäßigen Intervallen. Während die

Kooperationsgruppe hauptsächlich strategische Themen behandelt, ist das CSIRT-Netzwerk für operative Themen zuständig.

Führt ein Sicherheitsvorfall zu einer schweren Anomalie im Cyberraum und stellt diese Anomalie eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen dar, spricht man von einer Cyberkrise (Z 18). In einem solchen Fall tritt das Cyberkrisenmanagement (Z 19) in Kraft, welches besondere Koordinationsmechanismen zur Bewältigung einer Cyberkrise umfasst.

Zu § 4 (Aufgaben des Bundeskanzlers):

Die Aufgaben des Bundeskanzlers sind hauptsächlich strategischer Natur und umfassen Tätigkeiten wie die Koordination einer Strategie zur Sicherheit von Netz- und Informationssystemen oder die Vertretung Österreichs in EU-weiten und internationalen Gremien. Diese Aufgaben hat der Bundeskanzler schon vor Inkrafttreten dieses Gesetzes im Rahmen seines gesetzlich übertragenen Wirkungsbereichs erledigt. Davon unberührt bleibt die Vertretung Österreichs durch andere Ministerien in EU-weiten und internationalen Gremien in deren Wirkungsbereich, beispielsweise die Zuständigkeit des Bundesministeriums für Inneres für Cyberkriminalität oder des Bundesministeriums für Europa, Integration und Äußeres etwa im Bereich der Cyberdiplomatie.

Die Strategie und der jährliche Bericht zur Sicherheit von Netz- und Informationssystemen (Z 1) setzen auf der bereits bestehenden Österreichischen Strategie für Cyber Sicherheit (ÖSCS) aus dem Jahr 2013 auf. Die Strategie für die Sicherheit von Netz- und Informationssystemen soll die ÖSCS weiterentwickeln und mit Rücksicht auf die europäischen Vorgaben aus der NIS-RL einen Rahmen mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen in Österreich vorgeben. Ein Bericht zum Thema Cyber Sicherheit wurde bereits vor Inkrafttreten dieses Bundesgesetzes auf Grundlage der ÖSCS jährlich erstellt und soll unter der Koordination des Bundeskanzleramtes auch weiterhin jährlich erscheinen.

Auf EU-Ebene wurde mit der Kooperationsgruppe ein strategisches Gremium zur Erleichterung der strategischen Zusammenarbeit, zum Informationsaustausch, zum Aufbau von Vertrauen und zur Erreichung eines hohen gemeinsamen Sicherheitsniveaus zwischen den Mitgliedstaaten eingerichtet. Als Aufgaben obliegen ihr unter anderem die Bereitstellung strategischer Leitlinien für das CSIRT-Netzwerk, Erörterung der Modalitäten für die Berichterstattung über die Meldungen von Sicherheitsvorfällen, Erörterung der Fähigkeiten und Abwehrbereitschaft der Mitgliedstaaten, Erörterung von Normen und Spezifikation mit Vertretern der einschlägigen europäischen Normungsorganisationen, Austausch von besten Praktiken (in Bezug auf Meldepflichten, Schulungen, Forschung und Entwicklung, etc.), Erörterung der durchgeführten Arbeiten im Zusammenhang mit Übungen für die Sicherheit von Netz- und Informationssystemen etc. Neben der Vertretung Österreichs in der Kooperationsgruppe obliegt dem Bundeskanzler ferner die Vertretung Österreichs in anderen EU-weiten und internationalen Gremien für Netz- und Informationssystemsicherheit (Z 2), denen strategische Aufgaben zugewiesen sind, wie zB die „Horizontal Working Party on Cyber Issues“. Im Vorfeld dieser Gremien ist jeweils die grundlegende Position der Republik Österreich zu koordinieren.

Der Bundeskanzler soll auch die Rolle einer zentralen Schnittstelle des Staates zu Gesellschaft, Wirtschaft und Wissenschaft im Bereich der Netz- und Informationssystemsicherheit einnehmen (Z 3). Beispiele für die öffentlich-private Zusammenarbeit sind die Cyber Security Plattform (CSP), die aus der ÖSCS entspringt, und die „contractual public-private partnership (cPPP) on cyber security“, die von der Europäischen Kommission und der European Cyber Security Organisation (ECSO) am 5. Juli 2016 unterzeichnet wurde.

Zur Beurteilung, ob eine erhebliche Störung eines betriebenen Dienstes vorliegt und es sich daher um einen Sicherheitsvorfall (§ 3 Z 6) handelt, sind die in § 3 Z 6 lit. a bis d genannten Parameter zu berücksichtigen. Der Bundeskanzler kann gemäß § 16 Abs. 7 mit Verordnung, im Einvernehmen mit dem Bundesminister für Inneres, Kriterien für diese Parameter festlegen (Z 4).

Betrifft ein Sicherheitsvorfall mehrere vom Anwendungsbereich dieses Bundesgesetzes umfasste Sektoren, so obliegt es dem Bundeskanzler, die Öffentlichkeit über diesen Vorfall zu informieren (Z 5). Dabei ist darauf abzustellen, ob das Ausmaß des Sicherheitsvorfalls derart schwerwiegend ist, dass daran ein öffentliches Interesse bestehen kann und die Veröffentlichung der Informationen daher gerechtfertigt erscheint.

Dem Bundeskanzler kommt gemäß § 14 Abs. 1 die Aufgabe zu, die vom Anwendungsbereich dieses Bundesgesetzes umfassten Betreiber wesentlicher Dienste zu ermitteln (Z 6). Der Bundeskanzler führt und aktualisiert eine Liste der betroffenen „wesentlichen Dienste“ und übermittelt diese an die Europäische Kommission.

Mit Verordnung legt der Bundeskanzler, im Einvernehmen mit dem Bundesminister für Inneres, Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste, die jedenfalls zur Gewährleistung der Anforderungen nach § 15 Abs. 1 geeignet sind, fest (Z 7). Dabei sind die Arbeiten zu diesem Thema, die auf europäischer Ebene bereits durchgeführt wurden, insbesondere jene der Kooperationsgruppe, zu berücksichtigen und auf bestehende und international anerkannte Standards zurückzugreifen.

Hat ein Anbieter digitaler Dienste (§ 3 Z 10) seine Hauptniederlassung in Österreich, so fällt dieser in die Zuständigkeit österreichischer Behörden. Befinden sich aber die Netz- und Informationssysteme dieses Anbieters digitaler Dienste in einem anderen Mitgliedstaat, so ist vorgesehen, dass der Bundeskanzler Konsultationen mit den zuständigen Behörden dieses anderen Mitgliedstaates vornimmt (Z 8). Dies ist insbesondere dann notwendig, wenn es erforderlich erscheint, die getroffenen Sicherheitsmaßnahmen für diese Netz- und Informationssysteme vor Ort zu überprüfen.

Zu § 5 (Aufgaben des Bundesministers für Inneres):

Dem Bundesminister für Inneres kommt vorrangig eine zentrale Rolle im operativen Bereich zu, wobei sich das Aufgabenspektrum von koordinierenden, kommunikativen bis hin zu analysierenden und kontrollierenden Aufgaben erstreckt.

Um die Kooperation und Kommunikation zwischen den Mitgliedstaaten im Bereich der Sicherheit von Netz- und Informationssystemen innerstaatlich zu zentralisieren und zu vereinfachen, wird beim Bundesminister für Inneres eine zentrale Anlaufstelle bzw. SPOC (Single Point Of Contact) als Verbindungsstelle nach innen sowie nach außen (anderen Mitgliedstaaten, Kooperationsgruppe und CSIRT-Netzwerk) geschaffen und betrieben (Z 1; vgl. auch § 6). Organisatorisch betrachtet, wird die zentrale Anlaufstelle im Cyber Security Center (CSC) des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung eingerichtet.

Die neu geschaffenen Strukturen OpKoord (§ 3 Z 5 sowie § 7 Abs. 2) und IKDOK (§ 7 Abs. 1) werden vom Bundesminister für Inneres operativ koordiniert (Z 2), wobei dieser gemäß § 7 Abs. 3 ermächtigt ist, nähere Regelungen zum Zusammenwirken der Koordinierungsstrukturen (zB die Einberufung von Sitzungen, die Zusammensetzung, die Entscheidungsfindung) im Rahmen einer Geschäftsordnung zu treffen.

Neben der zentralen Anlaufstelle (SPOC) fungiert das CSC auch als Meldesammelstelle aller nationalen Meldestellen (Computer-Notfallteams). Dabei werden die von den Computer-Notfallteams eingehenden Meldungen über Sicherheitsvorfälle (§§ 16, 18 Abs. 2 und § 19 Abs. 2) und Störungen (§§ 19 Abs. 3 und 20) sowie die von der Finanzmarktaufsichtsbehörde (FMA) eingehenden Meldungen über schwerwiegende Betriebs- oder Sicherheitsvorfälle (§ 17 Abs. 2) 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. Da die OpKoord gemäß § 7 Abs. 2 zur Erörterung eines gesamtheitlichen Lagebildes eingerichtet wird, ist insbesondere diese auf die zuvor Bezug genommenen Informationen angewiesen (Z 3).

Der Bundesminister für Inneres ist zudem für die Erstellung und Weitergabe von zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur Vorbeugung von Sicherheitsvorfällen zuständig. Diese präventive Kompetenz ist erforderlich, um entsprechende Warnungen oder Handlungsempfehlungen im Vorhinein weitergeben zu können, und das Ziel des Gesetzes, ein möglichst hohes Niveau an Netz- und Informationssystemsicherheit, zu erreichen (Z 4).

Das CSC ist gemäß §§ 15 und 18 ermächtigt, die Sicherheitsvorkehrungen, die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste zu treffen haben, zu überprüfen. Auch wird vom CSC evaluiert, ob den Meldepflichten gemäß §§ 16 und 18 nachgekommen wird (Z 5).

Gegebenenfalls kann die Öffentlichkeit über einzelne Sicherheitsvorfälle nach Anhörung des von einem Sicherheitsvorfall betroffenen Betreibers wesentlicher Dienste vom Bundesminister für Inneres unterrichtet werden, wenn dies zur Bewältigung des konkreten Sicherheitsvorfalls oder der Vorbeugung zukünftiger Sicherheitsvorfälle notwendig ist oder die Offenlegung auf sonstige Weise im öffentlichen Interesse liegt (Z 6; § 16 Abs. 6).

Im Fall einer Cyberkrise kommt dem Bundesminister für Inneres darüber hinaus die operative Leitung und Koordination des Cyberkrisenmanagements zu (Z 7; §§ 21 f).

Zu § 6 (Zentrale Anlaufstelle):

In Umsetzung des Art. 8 Abs. 3 NIS-RL wird eine sogenannte zentrale Anlaufstelle (Single Point of Contact – SPOC) eingerichtet, die gemäß § 5 Z 1 vom Bundesminister für Inneres betrieben wird (Abs. 1).

Die zentrale Anlaufstelle dient der Gewährleistung und Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation zwischen den Mitgliedstaaten der Europäischen Union im Bereich der Sicherheit von Netz- und Informationssystemen. Um eine effektive Umsetzung der NIS-RL zu ermöglichen, ist es notwendig, dass jeder Mitgliedstaat – unbeschadet sektorenbezogener regulatorischer Vereinbarungen – eine nationale zentrale Anlaufstelle benennt, die für die Koordinierung im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist. Im Rahmen der grenzüberschreitenden Zusammenarbeit können der Kooperationsgruppe – zum Zwecke der wirksamen Information der Mitgliedstaaten und der Europäischen Kommission – auch zusammenfassende Berichte (samt Informationen über die Anzahl der eingegangenen Meldungen, Angaben über die Art der gemeldeten Sicherheitsvorfälle, wie zB die Arten der Sicherheitsverletzungen, deren Schwere und Dauer etc.) vorgelegt werden, wobei jedenfalls darauf zu achten ist, dass kein Personenbezug hergestellt werden kann, um die Vertraulichkeit der Meldungen und der Identität der Betreiber wesentlicher Dienste oder Anbieter digitaler Dienst zu wahren.

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

Eingehende Meldungen, Anfragen oder sonstige Informationen aus den anderen Mitgliedstaaten, die an die zentrale Anlaufstelle herangetragen werden, sind von dieser unmittelbar im Rahmen des IKDOK (siehe hierzu § 7) an dessen Mitglieder und an die zuständigen Computer-Notfallteams (§ 12) weiter zu verteilen, wenn dies zur Erfüllung der Aufgaben des jeweiligen NIS-Büros (§§ 4 ff) oder des Computer-Notfallteams erforderlich ist (Abs. 2 Z 1). Das zuständige NIS-Büro oder das Computer-Notfallteam übernimmt in Folge die weitere Behandlung.

Betrifft ein nationaler Sicherheitsvorfall einen oder mehrere Mitgliedstaaten der Europäischen Union, unternimmt die zentrale Anlaufstelle zudem die Unterrichtung der zentralen Anlaufstellen in anderen Mitgliedstaaten (Abs. 2 Z 2; vgl. auch §§ 16 Abs. 5, 18 Abs. 3 und 19 Abs. 4).

Zu § 7 (Koordinierungsstrukturen):

Auf Basis sowie unter Einbindung bestehender operativer Strukturen wird eine neue Struktur zur Koordination auf der operativen Ebene (OpKoord) (§ 3 Z 5) geschaffen. Diese Koordinierungsstruktur besteht aus einem sogenannten „Inneren Kreis“ und einem „Äußeren Kreis“. Die Arbeiten im Rahmen der OpKoord werden unter Einbindung der Ressorts und operativer Strukturen aus Wirtschaft und Forschung vom Bundesminister für Inneres koordiniert (Public Private Partnership).

Der Innere Kreis der operativen Koordinierungsstruktur (IKDOK) setzt sich aus Vertretern jener Behörden, denen nach den Bestimmungen der §§ 4 und 5 Aufgaben zugewiesen werden (NIS-Büros; Abs. 1) sowie des Bundesministeriums für Landesverteidigung und des Bundesministeriums für Europa, Integration und Äußeres (BMEIA), zusammen. Für den Bundeskanzler sind dies beispielsweise Vertreter des GovCERT, für den Bundesminister für Inneres beispielsweise Vertreter des Cyber Crime Competence Center (C 4) sowie des Cyber Security Center (CSC) und für den Bundesminister für Landesverteidigung beispielsweise Vertreter des MilCERT (Military Cyber Emergency Readiness Team), des Heeres-Nachrichtenamtes (HNaA) und des Cyber Verteidigungszentrum (CVZ). Die Einbindung des BMEIA ist von besonderer Bedeutung, da Sicherheitsvorfälle in der Regel einen Auslandsbezug aufweisen und sich daraus eine außenpolitisch relevante Situation ergeben kann. Die erforderliche Fachexpertise in Bereichen wie Cyberdiplomatie kann dabei für die Beurteilung eines Sicherheitsvorfalls innerhalb dieses Gremiums notwendig sein. Im Rahmen des IKDOK soll das durch den Bundesminister für Inneres erstellte Lagebild gemeinsam erörtert und aktualisiert werden und auch die Möglichkeit bestehen, klassifizierte Informationen zwischen diesen Behörden auszutauschen. Darüber hinaus sollen auch die Erkenntnisse, die sich aus den gemäß § 9 Abs. 1 beim Bundesminister für Inneres betriebenen technischen Einrichtungen zur frühzeitigen Erkennung von Störungen oder Unregelmäßigkeiten von Netz- und Informationssystemen (Indicators of Compromise [IOC]-basiertes Frühwarnsystem) ergeben, diskutiert werden. Dasselbe gilt für die Erkenntnisse, die sich aus den gemäß § 9 Abs. 2 beim Bundesminister für Inneres sowie gemäß § 12 Abs. 4 beim Bundeskanzler (GovCERT) betriebenen technischen Einrichtungen zur Erkennung von Mustern von Angriffen auf Netz- und Informationssysteme („Honeypots“ und „Sinkholes“), ergeben. Der permanent und gemeinsam erarbeitete Status zur Situation im Bereich NIS soll allen Beteiligten als Grundlage für zu treffende planerische, präventive und reaktive Maßnahmen dienlich sein. Dem IKDOK kommt auch die Aufgabe zu, den Koordinationsausschuss (§ 22) durch Erstellung von anlassbezogenen Lagebildern und technische Expertise zu unterstützen (§ 22 Abs. 3).

Darüber hinaus werden zur Erörterung eines gesamtheitlichen Lagebilds in einem zweiten Kreis Vertreter der Computer-Notfallteams eingebunden. Bei Bedarf können auch Vertreter anderer Ressorts und anderer Einrichtungen des Bundes eingebunden werden, wenn deren gesetzliche Wirkungsbereiche betroffen sind, sowie Vertreter aus Wirtschaft (insbesondere Betreiber wesentlicher Dienste oder digitale Diensteanbieter) und Forschung.

Die näheren Regelungen für die Zusammenarbeit im Rahmen der Koordinierungsstrukturen (OpKoord und IKDOK) können vom BMI in einer Geschäftsordnung festgelegt werden (Abs. 3). Dies umfasst insbesondere Regelungen zur Einberufung von Sitzungen, die Zusammensetzung sowie die Entscheidungsfindung.

Zu § 8 (Strategie für die Sicherheit von Netz- und Informationssystemen):

Gemäß Art. 7 NIS-RL hat jeder Mitgliedstaat eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen, in der die strategischen Ziele und angemessene Politik- und Regulierungsmaßnahmen bestimmt werden, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht und aufrechterhalten werden soll. Dabei sollen insbesondere folgende Aspekte berücksichtigt werden:

a) die Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;
b) ein Steuerungsrahmen zur Erreichung der Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen, einschließlich der Aufgaben und Zuständigkeiten der staatlichen Stellen und der anderen einschlägigen Akteure;
c) die Bestimmung von Maßnahmen zur Abwehrbereitschaft, Reaktion und Wiederherstellung, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;
d) eine Aufstellung der Ausbildungs-, Aufklärungs- und Schulungsprogramme im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;
e) eine Angabe der Forschungs- und Entwicklungspläne im Zusammenhang mit der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;
f) ein Risikobewertungsplan zur Bestimmung von Risiken;
g) eine Liste der verschiedenen Akteure, die an der Umsetzung der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen beteiligt sind.

In Österreich kann dabei auf der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) aufgebaut werden, die im Jahr 2013 von der Bundesregierung verabschiedet wurde. Die ÖSCS ist ein umfassendes und proaktives Konzept zum Schutz des Cyberraums und der Menschen im virtuellen Raum unter Gewährleistung ihrer Menschenrechte. Ihr Ziel ist es die Sicherheit und Widerstandskraft der österreichischen Infrastrukturen und Leistungen im Cyberraum zu verbessern. Die ÖSCS leitet sich aus der Österreichischen Sicherheitsstrategie (Beschluss durch den Nationalrat im Juli 2013) ab und orientiert sich an den Prinzipien des Programms zum Schutz kritischer Infrastrukturen (Beschlüsse der Bundesregierung vom März 2008 und November 2014).

Auf Basis der ÖSCS ist es daher gemäß § 4 Z 1 Aufgabe des Bundeskanzlers, die Weiterentwicklung dieser Strategie vor dem Hintergrund der in der NIS-RL genannten Aspekte zu koordinieren, damit eine neue Strategie zur Sicherheit für Netz- und Informationssysteme in Österreich verabschiedet werden kann.

Diese Strategie ist der Europäischen Kommission bekanntzugeben (Abs. 2). Sollten Elemente der Strategie auch Aspekte der nationalen Sicherheit betreffen, so können diese Elemente dabei weggelassen werden.

Zu § 9 (Befugnisse zur Vorbeugung von Sicherheitsvorfällen):

Durch Abs. 1 wird vorgesehen, dass der Bundesminister für Inneres zur Erfüllung der Aufgabe gemäß § 5 Z 4 („Erstellung und Weitergabe von zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur Vorbeugung von Sicherheitsvorfällen“) ermächtigt ist, als Ergänzung der vorhandenen proaktiven Sicherheitsmaßnahmen technische Einrichtungen zu betreiben, um Störungen oder Unregelmäßigkeiten von Netz- und Informationssystemen frühzeitig zu erkennen und somit die Netz- und Informationssystemsicherheit in Österreich zu stärken (IOC-basiertes Frühwarnsystem). Dabei folgt Österreich dem Vorbild einiger europäischer Länder, wie zB Spanien, Schweiz, Finnland, Dänemark oder Niederlande.

Auch wenn eine Kompromittierung von sensitiven Netzwerken (zB Netzwerke von Unternehmen) oft nicht gänzlich verhindert werden kann, ist es wichtig, die Zeitspanne zwischen der Durchführung und der Erkennung einer Kompromittierung zu minimieren, um rasch dagegen vorgehen zu können und Schäden

möglichst gering zu halten. Durch entsprechend konfigurierte und vor den Netzwerken der Teilnehmer platzierte technische Einrichtungen können Angriffe, das Vorgehen des jeweiligen Angreifers im Netz des Teilnehmers und seine Kommunikation mit Schadsoftware erkannt werden. Diese Einrichtungen werden explizit außerhalb des Netzwerkes des Teilnehmers angebracht. 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 technische Einrichtung passieren, werden von diesem nicht entschlüsselt. Im österreichischen Früwarnsystem wird der Betrieb der eingesetzten technischen Einrichtungen durch den Bundesminister für Inneres (konkret: „Cyber Security Center“, CSC) für den zivilen Bereich durchgeführt.

Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen des Bundes sollen freiwillig am zivilen Betrieb durch das CSC teilnehmen können, wobei die Teilnahme und auch das Ausmaß der Datenverarbeitung mittels Rahmenverträgen geregelt werden. Dem Teilnehmer soll dabei die Möglichkeit gegeben werden, zu bestimmen, welche Daten übermittelt werden, wohingegen ein gänzlicher Ausschluss der Datenübermittlung nicht möglich ist.

Außerdem 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 ist beabsichtigt, insbesondere die Anschaffungskosten der technischen Einrichtungen sowie deren jährliche Wartungs- bzw. Instandhaltungskosten zu berücksichtigen.

Der Betrieb der technischen Einrichtungen 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 technischen Einrichtungen mit jenen Erkennungsmustern (IOC) zu Bedrohungen über technische Schnittstellen speist, die von diesen in den aus- und eingehenden Datenströmen der Teilnehmer automatisch erkannt werden sollen.

Die TI bekommt Bedrohungsinformationen aus unterschiedlichen Quellen. Diese sind stellenweise mit einer Klassifizierung versehen und können daher einem Teilnehmer nicht ohne weiteres zugänglich gemacht werden. Dennoch ist es erforderlich, dass die Frühwarneinrichtungen, die zwar technisch vor den Netzwerken, aber physisch in der Infrastruktur der Teilnehmer installiert werden, solche klassifizierten IOC zur Erkennung von Unregelmäßigkeiten heranziehen. Dies wird durch einen sogenannten „Black Box“-Betrieb ermöglicht, das heißt der jeweilige Teilnehmer bekommt, abgesehen von einem eingeschränkten Zugriff über eine technische Schnittstelle, um bestimmte Daten auszulesen, keine Möglichkeit, auf klassifizierte IOC, die in den technischen Einrichtungen verarbeitet werden, zuzugreifen. Dadurch kann die Information solcher IOC zur Erkennung von Unregelmäßigkeiten genutzt und trotzdem ihre Klassifizierung gewahrt werden.

Basierend auf IOC ist es für die technischen Einrichtungen 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 „Security Operation Center“ (SOC, eine IT-Sicherheitsabteilung, die durch den Teilnehmer selbst oder einen externen Dienstleister bereitgestellt wird) zuständig ist. Zudem bietet § 12 Abs. 3 die Möglichkeit, dass Betreiber wesentlicher Dienste sektorenspezifische Computer-Notfallteams beauftragen können, die Analyse und Bewertung von Unregelmäßigkeiten vorzunehmen. Anbieter digitaler Dienste können das nationale Computer-Notfallteam (§ 12 Abs. 3 letzter Satz), Einrichtungen des Bundes das GovCERT (§ 12 Abs. 4 zweiter Satz) dazu beauftragen.

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) inkl. zusammenhängender Informationen (der Kontext darüber, was den Alarm ausgelöst hat, zB bestimmte IOC) an den Betreiber zur Analyse und Bewertung sowie Aufnahme in die TI und 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 Sicherheitsvorfalls im Sinne dieses Gesetzes dar, unabhängig davon, ob die gefundene Unregelmäßigkeit auf einem klassifizierten oder einem nicht klassifizierten IOC basiert.

Zudem ist durch Abs. 2 der Bundesminister für Inneres zur Erfüllung der Aufgabe gemäß § 5 Z 4 ermächtigt, technische Einrichtungen, das heißt „Honeypots“ und „Sinkholes“, zu betreiben oder (bloß) zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen.

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. Daraus gewonnene Erkenntnisse dienen insbesondere als Grundlage für eine aktuelle Lageeinschätzung durch den IKDOK (§ 7 Abs. 1).

„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. Im Gegensatz zu „Honeypots“ werden „Sinkholes“ nur insofern genutzt, als der Bundesminister für Inneres „Sinkholes“ nicht von sich aus physisch betreibt, sondern nur auf den Datenverkehr von bei Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und Einrichtungen des Bundes installierten Sinkholes Zugriff bekommt.

Sowohl bei „Honeypots“ als auch bei „Sinkholes“ ist die Aufzeichnung und Verarbeitung zweckentsprechender Informationen erforderlich, um Angriffsquellen und Angriffsziele zu erkennen und analysieren zu können (§ 10 Abs. 2 letzter Satz).

Neben dem Bundesminister für Inneres kommt gemäß § 12 Abs. 4 letzte Satz auch dem GovCERT innerhalb seines Zuständigkeitsbereichs die Befugnis zu, „Honeypots“ zu betreiben oder „Sinkholes“ zu nutzen, um zu wichtigen Informationen der aktuellen Gefährdungslage zu gelangen.

Zu § 10 (Datenverarbeitung):

Die Behörden, bei denen NIS-Büros eingerichtet sind, sollen gemäß Abs. 1 explizit ermächtigt sein, personenbezogene Daten, die zur Wahrnehmung sämtlicher Aufgaben gemäß §§ 4 und 5 erforderlich sind, im Rahmen ihrer Aktenverwaltung für Zwecke der Dokumentation und zur Nachvollziehbarkeit der Tätigkeit zu verarbeiten (zentrale Informationssammlung). Beim Verarbeiten von personenbezogenen Daten ist jedenfalls der Grundsatz der Verhältnismäßigkeit zu beachten.

So hat der Bundeskanzler insbesondere jene personenbezogenen Daten zu verarbeiten, die für die Ermittlung der Betreiber wesentlicher Dienste gemäß § 14 Abs. 1 erforderlich sind. Solche Daten können Name, Firmenname oder Adresse der jeweils betroffenen Einrichtung sein, die einen wesentlichen Dienst im Sinne des § 14 Abs. 2 betreibt. Darüber hinaus werden auch jene personenbezogenen Daten verarbeitet, die im Zuge der Bekanntgabe einer Kontaktstelle im Sinne des § 14 Abs. 3 übermittelt werden. Dabei handelt es sich zB um Name, E-Mail-Adresse und Telefonnummer der als Kontaktstelle bzw. Kontaktperson benannten Personen.

Der Bundesminister für Inneres ist ermächtigt, jene personenbezogenen Daten zu verarbeiten, die zur Wahrnehmung sämtlicher Aufgaben gemäß § 5 erforderlich sind. Darunter fallen insbesondere jene personenbezogenen Daten, die für die Entgegennahme von Meldungen über Sicherheitsvorfälle und sonstige Störungen relevant sind, wie Daten des Einmelders, der Kontaktperson, des Opfers, des Angreifers und des entsprechenden Sachverhalts. Das sind insbesondere Namen, Anschriften, Telefonnummern, E-Mail-Adressen und sonstige den Sachverhalt spezifizierende technische Daten (zB IP-Adressen).

Zusätzlich zu der Datenverarbeitung gemäß Abs. 1 ist der Bundesminister für Inneres gemäß Abs. 2 explizit ermächtigt, im Rahmen einer speziellen Datenverarbeitung („Analysedatei“) zur Erfüllung seiner spezifischen Aufgaben gemäß § 5 Z 4 und 5 Identifikations- und Erreichbarkeitsdaten von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste (zB Namen, Anschriften, Telefonnummern, E-Mail-Adressen von zuständigen Kontaktpersonen, aber auch Unternehmensdaten, wie Name, Anschrift und Sektorenzugehörigkeit des jeweiligen Betreibers wesentlicher Dienste oder Anbieters digitaler Dienste) zu verarbeiten. Im Zusammenhang mit der Überprüfung von Sicherheitsvorkehrungen und der Einhaltung der Meldepflicht von Betreibern wesentlicher Dienste und Anbietern digitaler Dienste ist zudem die Verarbeitung von Daten über die Aufstellung vorhandener Sicherheitsvorkehrungen, mögliche aufgedeckte Sicherheitsmängel, Ergebnisse der Einschau in die Netz- und Informationssysteme und dazugehörige Unterlagen (zB Audit-Reports) sowie mögliche ausgesprochene Empfehlungen umfasst.

Darüber hinaus dürfen gemäß Abs. 2 vom Bundesminister für Inneres Daten gemäß § 9 Abs. 1 und 2 sowie Verwaltungsdaten verarbeitet werden. Zu den Daten bzw. zweckentsprechenden Informationen, die gemäß § 9 Abs. 1 und 2 gewonnen werden, zählen insbesondere technische personenbezogene Daten, wie IP-Adressen der zugreifenden Systeme bzw. Personen, verwendete Ports und IP-Adressen von Angriffszielen, Host-Namen (eindeutige Bezeichnung eines Rechners im Netzwerk), Hashes (Prüfziffern für die Erkennung von Schadsoftware), übermittelter Network-Dump (Aufzeichnung des Netzwerkverkehrs), URL (Identifikation und Lokalisierung einer Ressource), Ports (Adresskomponenten für die Kommunikation, um Datenpakete einer Anwendung zuzuordnen), Domainnamen (Internetadresse), Whois-Informationen, Zugangsdaten, Log-Files (Protokollierung von Programmabläufen oder Zugriffen auf eine bestimmte Ressource) sowie Metadaten (Header, Schlüssel), aber auch Informationen, die das Verhalten bzw. das Muster eines Angriffs abbilden (zB welche Dateien liegen im Fokus des Angreifers).

Jedes NIS-Büro darf von dem anderen NIS-Büro, den Computer-Notfallteams und den Betreibern wesentlicher Dienste und Anbietern digitaler Dienste Auskünfte verlangen, die sie als wesentliche Voraussetzung zur Erfüllung ihrer Aufgaben benötigt (Abs. 3), wobei die ersuchten Stellen zur unverzüglichen Auskunftserteilung verpflichtet sind. Dabei handelt es sich etwa um Informationen, die für die umfassende Beurteilung eines Sicherheitsvorfalls notwendig sind.

Durch den Entfall des bisherigen § 14 DSG 2000 durch das Datenschutz-Anpassungsgesetz 2018, BGBl. I Nr. 120/2017, und den Umstand, dass die DSGVO keine spezifischen Regelungen über die Protokollierung enthält, soll in Abs. 4 explizit vorgesehen werden, dass jede Abfrage, Übermittlung und Änderung personenbezogener Daten zur besseren Nachvollziehbarkeit und Überprüfbarkeit zu protokollieren ist, wobei die Protokollierungsdauer drei Jahre betragen soll. Bei der Protokollierung der verarbeiteten Daten soll eine Zuordnung von Abfragen, Übermittlungen oder Änderungen zu einem NIS-Büro erfolgen.

Zu § 11 (Gemeinsame Verarbeitung):

Art. 26 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 (im Folgenden: DSGVO) sieht vor, dass wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung festlegen, diese gemeinsam Verantwortliche sind. Da diese Regelung eine Öffnungsklausel enthält, soll in § 12 eine nähere Regelung erfolgen.

Im Rahmen des Art. 26 DSGVO sind der Bundeskanzler, der Bundesminister für Inneres und der Bundesminister für Landesverteidigung als gemeinsam Verantwortliche ermächtigt, in Abs. 1 näher bezeichnete Daten zu verarbeiten. Der Zweck dieser Datenverarbeitung ist die Bewertung von Risiken für Netz- und Informationssysteme sowie die Erstellung eines Lagebilds mittels strategischer oder operativer Analyse in einem Dateisystem (Art. 4 Z 6 DSGVO). Bezüglich des Risikobegriffs ist auf die Ausführungen zu § 3 Z 7 zu verweisen.

Die sogenannte strategische und operative Analyse stellt eine Methode dar, um Ausmaß, Erscheinungsformen und Charakter (Qualität, Quantität und Struktur) von Angriffen auf Netz- und Informationssysteme zu erfassen, mit dem Ziel, Erkenntnisse zu ihren Bewegungen, Entwicklungen und beeinflussbaren Rahmenbedingungen herauszuarbeiten und darauf aufbauend Maßnahmen der Prävention und Abwehr entwickeln zu können. Im Rahmen der strategischen Analyse soll eine abstrakte Übersicht über Status Quo, Ursachen und Entwicklungstendenzen im Cyberraum zu einer bestimmten Zeit und bezogen auf bestimmte Bereiche (zB Cybercrime) erstellt werden. Im Gegensatz dazu werden bei der operativen Analyse Informationen über konkrete Sachverhalte verarbeitet, um einerseits durch Vergleich von Angriffen mit ähnlichem „Muster“ eine Häufung von Angriffen zu erkennen und andererseits in komplexen Fällen neue Ermittlungsansätze zu finden. Das bedeutet, dass sich erst im Zuge der Datenverarbeitung die Wahrscheinlichkeit der erneuten Begehung eines möglichen Angriffs ergibt.

Im Rahmen der gemeinsamen Verarbeitung dürfen insbesondere jene Daten verarbeitet werden, die erforderlich sind, um eine Einrichtung (dies kann eine natürliche oder juristische Person sein), die von einem Sicherheitsvorfall oder einer sonstigen Störung betroffen ist, oder eine Einrichtung, von der eine Gefahr oder sogar ein Angriff ausgeht, zu identifizieren. Dies können etwa Telefonnummern, IP-Adressen, E-Mail-Adressen, Domains/Hostnamen (zB www.beispiel.at), Rechnernamen (zB PC-Mitarbeiter-Eingang-01), URL (zB http://www.beispiel.at/team/name.html), Namen von Herstellern einer betroffenen Komponente (zB Software oder Hardware), Usernamen oder weitere Accountnamen (zB Facebook-Accountname, Twitter-Handle, Skype-ID) sein. Gleichzeitig sind aber auch alle anderen Daten zu verarbeiten, die notwendig sind, um einen Sicherheitsvorfall oder eine sonstige Störung eines betroffenen Dienstes beurteilen und bewerten zu können. Dabei können neben personenbezogenen Daten

auch nicht-personenbezogene Daten, wie etwa Informationen zu Zeit, Ort, Grund und Art des Sicherheitsvorfalls, relevant sein. Ebenso dürfen jene Daten verarbeitet werden, die im Rahmen einer Meldung von der meldenden Einrichtung ebenfalls anzugeben sind. Dies sind etwa Namen, Firmennamen, Adressen, Telefonnummern, E-Mail-Adressen und sonstige Kontaktinformationen. Zudem ist es zulässig, Verwaltungsdaten sowie die aggregierten Erkenntnisse, die gemäß § 9 Abs. 1 und 2 gewonnen werden, gemeinsam zu verarbeiten. Bei den dabei verarbeiteten personenbezogenen Daten ist auf jene Aufzählung der Datenarten (siehe oben in diesem Absatz) zu verweisen, die im Rahmen eines Sicherheitsvorfalls oder einer sonstigen Störung betroffen sein können.

Gemäß Art. 26 Abs. 1 zweiter Satz DSGVO haben mehrere gemeinsam Verantwortliche in einer Vereinbarung festzulegen, wer von ihnen gegenüber der Betroffenen welche Verpflichtungen nach der DSGVO – zB Berichtigungs- und Löschungspflichten – wahrzunehmen hat, es sei denn, eine entsprechende Zuständigkeitsverteilung bzw. Pflichtenzuordnung ist bereits in einer gesetzlichen Vorschrift des Unions- oder des nationalen Rechts vorgesehen. In diesem Sinne soll der vorgeschlagene Abs. 2 die Zuständigkeit zwischen den gemeinsam Verantwortlichen dahingehend aufteilen, dass Auskunfts-, Informations-, Berichtigungs-, Löschungs- und sonstige Pflichten nach der DSGVO von jedem Verantwortlichen nur in Bezug auf jene personenbezogenen Daten zu erfüllen sind, die im Zusammenhang mit den von ihm selbst geführten Verwaltungsverfahren oder den von ihm gesetzten (verfahrensfreien) Maßnahmen verarbeitet werden. Dies erscheint zweckmäßig, weil der in diesem Sinne (ausschließlich) zuständige Verantwortliche am ehesten in der Lage ist, zu beurteilen, ob dem Betroffenen bezüglich der in Rede stehenden Daten tatsächlich ein Informations-, Auskunfts-, Berichtigungs- oder sonstige Anspruch nach der DSGVO zukommt.

Wird ein Recht nach der DSGVO vom Betroffenen – unter Nachweis seiner Identität (vgl. ErwGr 64 zur DSGVO) – bei einem nach dieser Bestimmung unzuständigen Verantwortlichen wahrgenommen, soll direkt durch diesen die Weiterverweisung an den für die Bearbeitung des Gesuchs zuständigen Verantwortlichen erfolgen. Dies soll auch für Fälle gelten, in denen den in Anspruch genommenen Verantwortlichen nur einen Teil der Pflichten nach der DSGVO treffen.

Der vorgeschlagenen Regelung steht Art. 26 Abs. 3 DSGVO nicht entgegen. Nach dieser Bestimmung kann der Betroffene ein Recht aufgrund der DSGVO zwar gegenüber „jedem einzelnen der Verantwortlichen“ geltend machen, und zwar unabhängig von einer zwischen den Verantwortlichen im Rahmen einer Vereinbarung getroffenen Zuständigkeitsverteilung; dies impliziert eine Pflicht des insoweit unzuständigen Verantwortlichen, ein Gesuch des Betroffenen nicht zurückzuweisen, sondern es jedenfalls entgegenzunehmen und an den zuständigen Verantwortlichen weiterzuleiten. Die freie Wahl des Verantwortlichen, gegenüber dem der Betroffene ein Recht nach der DSGVO geltend macht, gilt jedoch nur dann, wenn die Zuständigkeitsverteilung auf einer Vereinbarung zwischen den Verantwortlichen, nicht aber, wenn sie auf einer gesetzlichen Regelung beruht. Verteilt daher wie hier eine gesetzliche Regelung die Zuständigkeiten unter den Verantwortlichen, so ist ein unzuständiger Verantwortlicher nicht gehalten, ein Gesuch des Betroffenen entgegenzunehmen oder weiterzuleiten. Vielmehr kann er den Betroffenen in einem solchen Fall an den zuständigen Verantwortlichen verweisen. Bei dieser Bestimmung handelt es sich lediglich um eine Zuständigkeitsnorm. Die Regelungen der DSGVO zu den inhaltlichen Voraussetzungen der oben genannten Ansprüche und Pflichten gemäß Art. 13 ff bleiben davon unberührt. Macht der Betroffene demnach zB das Recht auf Löschung (Art. 17 DSGVO) geltend, ist durch den in Abs. 2 erster Satz genannten Verantwortlichen jeweils im Einzelfall zu prüfen, ob dieses besteht oder ein Ausnahmetatbestand nach Art. 17 Abs. 3 DSGVO zur Anwendung gelangt, wobei vor allem der Ausnahmetatbestand gemäß lit. b leg. cit. einschlägig sein wird.

Gemäß Art. 28 Abs. 1 DSGVO kann sich der Verantwortliche eines Dritten bedienen, der personenbezogene Daten in seinem Auftrag verarbeitet (Auftragsverarbeiter, Art. 4 Z 8 DSGVO). Der Auftragsverarbeiter im Sinne der DSGVO entspricht im Wesentlichen dem Dienstleister gemäß § 4 Z 5 DSG 2000 und – soweit es sich bei der Datenanwendung derzeit um ein Informationsverbundsystem handelt – dem Betreiber gemäß § 50 Abs. 1 DSG 2000. Gemäß Abs. 3 soll dem Bundesminister für Inneres die Funktion des Auftragsverarbeiters gemäß Art. 4 Z 8 iVm Art. 28 Abs. 1 DSGVO und somit auch die technische Zuständigkeit übertragen werden. Der Bundesminister für Inneres ist in dieser Funktion zudem verpflichtet, die Datenschutzpflichten gemäß Art. 28 Abs. 3 lit. a bis h DSGVO wahrzunehmen.

Die Übermittlung der personenbezogenen Daten, die gemäß Abs. 1 und § 10 Abs. 1 und 2 verarbeitet werden dürfen, ist darüber hinaus für die in Abs. 4 genannten Zwecke zulässig. Dies umfasst neben der Übermittlung an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an militärische Organe und Behörden für Zwecke der militärischen Landesverteidigung gemäß Art. 79 Abs. 1 B-VG, an die Datenschutzbehörde für Zwecke des Art. 33 DSGVO und an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege auch eine Übermittlung an sonstige andere in-

und ausländische Behörden oder Stellen (zB Aufsichtsstellen oder Regulierungsbehörden in einem der in § 2 Abs. 1 genannten Sektoren). Eine Übermittlung an die letztgenannten Stellen ist allerdings nur dann zulässig, wenn dies für diese Stelle zur Aufgabenerfüllung erforderlich ist. Darüber hinaus ist eine Übermittlung dann zulässig, wenn im jeweiligen Materiengesetz eine gesetzliche Grundlage für die Übermittlung dieser Daten besteht.

Hinsichtlich der Protokollierung (Abs. 5) ist auf die Erläuterungen zu § 10 Abs. 4 zu verweisen.

Zu § 12 (Aufgaben der Computer-Notfallteams):

Um die Prävention, Erkennung, Reaktion und Folgenminderung bei NIS-Vorfällen und -Risiken gewährleisten zu können, ist es wichtig, über gut funktionierende Computer-Notfallteams oder CSIRT – Computer Security Incident Response Teams (auch: CERT – Computer Emergency Response Teams) – zu verfügen, die die grundlegenden Anforderungen im Hinblick auf die Gewährleistung wirksamer und kompatibler Fähigkeiten zur Bewältigung von Risiken und Sicherheitsvorfällen und einer effizienten Zusammenarbeit auf Unionsebene erfüllen. Wegen der Bedeutung der internationalen Zusammenarbeit im Bereich NIS beteiligen sich die Computer-Notfallteams zusätzlich zum durch die NIS-RL geschaffenen CSIRT-Netzwerks auch an nationalen sowie anderen internationalen Kooperationsnetzen. In Umsetzung von Art. 9 und des Anhangs I der NIS-RL werden daher in den §§ 12 und 13 die Aufgaben und Anforderungen für Computer-Notfallteams geregelt.

Zur Unterstützung der Betreiber wesentlicher Dienste können sektorenspezifische Computer-Notfallteams eingerichtet werden (Abs. 1). Diese verfügen über das notwendige Fachwissen aus dem jeweiligen Sektor und können den Betreibern wesentlicher Dienste die bestmögliche technische Unterstützung im Rahmen der Bewältigung von Risiken und Sicherheitsvorfällen bieten. Pro Sektor kann es jedenfalls nur ein sektorenspezifisches Notfallteam geben. Gibt es (noch) kein sektorenspezifisches Computer-Notfallteam für einen bestimmten Sektor, fallen die Aufgaben (Abs. 2) dem nationalen Computer-Notfallteam zu. Das nationale Computer-Notfallteam ist daher grundsätzlich für alle Betreiber wesentlicher Dienste und Anbieter digitaler Dienste zuständig und hat die Aufgaben, die einem Computer-Notfallteam nach diesem Bundesgesetz zukommen, sektorenübergreifend zu erfüllen.

Zu den Hauptaufgaben der Computer-Notfallteams zählt die Entgegennahme von Meldungen über Sicherheitsvorfälle oder sonstige Störungen bei Betreibern wesentlicher Dienste oder Anbietern digitaler Dienste (Abs. 2 Z 1) und deren Weiterleitung an den Bundesminister für Inneres (Abs. 2 Z 2). Die Computer-Notfallteams sind damit die Erstanlaufstelle für alle in den Anwendungsbereich dieses Bundesgesetzes fallenden Einrichtungen, die von einem Sicherheitsvorfall betroffen sind. Die Zuständigkeit zur Entgegennahme von Meldungen erstreckt sich auf Sicherheitsvorfälle, die eine Meldepflicht für Betreiber wesentlicher Dienste (§ 16) und Anbieter digitaler Dienste (§ 18 Abs. 2) auslösen, sowie auf Störungen, die freiwillig gemeldet werden (§ 20).

Zusätzlich nehmen Computer Notfallteams noch weitere technische Aufgaben wahr (Abs. 2 Z 3 bis 5). Dazu gehören etwa eine laufende Analyse und Beobachtung von Risiken und Sicherheitsvorfällen im Bereich der IT und die Ausgabe von Warnungen oder Alarmmeldungen, wenn Informationen über Risiken oder Sicherheitsvorfälle bekannt werden. Die Informationen zu Risiken und Sicherheitsvorfällen können etwa von Dritten (anderen Computer-Notfallteams, Herstellern, Sicherheitsforschern, Dienstleistern, Non-Profit-Organisationen etc.) stammen oder sie können von den Computer-Notfallteams selbst, etwa durch aktive Informationseinholung (auf Schwachstellen oder Fehlkonfigurationen) ermittelt werden.

Falls erforderlich können auch allgemeine Handlungsempfehlungen an die betroffenen Einrichtungen ausgegeben werden. Kommt es bei einem Betreiber wesentlicher Dienste oder einem Anbieter digitaler Dienste zu einem Sicherheitsvorfall, so werden sie von einem Computer-Notfallteam bei der ersten allgemeinen technischen Reaktion auf diesen Vorfall unterstützt. In der Regel handelt es sich dabei um konkrete Handlungsanweisungen und Informationen, um den aktuellen Sicherheitsvorfall abzuwehren und die negativen Auswirkungen dadurch möglichst gering zu halten. Nur in Ausnahmefällen können Computer-Notfallteams auch vor Ort eine technische Unterstützung leisten, worauf die betroffene Einrichtung jedoch keinen Rechtsanspruch hat.

Darüber hinaus beteiligen sich alle Computer-Notfallteams am europäischen CSIRT-Netzwerk, nehmen an der OpKoord teil und leisten damit einen wesentlichen Beitrag für die Erstellung eines gesamtheitlichen Lagebildes für Österreich (Z 6).

Abs. 3 ermöglicht es Betreibern wesentlicher Dienste, sektorenspezifische Computer-Notfallteams damit zu beauftragen, die Analyse und Bewertung von Unregelmäßigkeiten, die durch eine bei diesem Betreiber wesentlicher Dienste eingerichteten technischen Einrichtung gemäß § 9 Abs. 1 erkannt wurden,

vorzunehmen. Anbieter digitaler Dienste können das nationale Computer-Notfallteam (§ 12 Abs. 3 letzter Satz), Einrichtungen des Bundes das GovCERT (§ 12 Abs. 4 zweiter Satz) damit beauftragen.

Für die Einrichtungen des Bundes erfüllt das GovCERT die Aufgaben eines Computer-Notfallteams. Das beim Bundeskanzler eingerichtete GovCERT (Abs. 4) ist daher das sektorenspezifische Computer-Notfallteam für die öffentliche Verwaltung. Der Bundeskanzler und der Bundesminister für Inneres, denen nach diesem Bundesgesetz besondere Aufgaben zukommen, sind von der Zuständigkeit des GovCERT nicht erfasst, insbesondere in Hinblick auf die Entgegennahme von Meldungen. Zusätzlich zu den Aufgaben eines Computer-Notfallteams kann das GovCERT technische Einrichtungen betreiben, die Muster von Angriffen auf Netz- und Informationssysteme erkennen lassen (sog. „Honeypots“ und „Sinkholes“).

Computer-Notfallteams sind zur Beteiligung am europäischen CSIRT-Netzwerk berechtigt und können sich zB auf E-Mail-Verteilerlisten eintragen lassen oder in grenzüberschreitenden Arbeitsgruppen mitwirken (Abs. 2 Z 6 zweiter Fall). Die Teilnahme an den Sitzungen des CSIRT-Netzwerks ist jedoch nur Vertretern des nationalen Computer-Notfallteams und des GovCERT vorbehalten (Abs. 5). Damit wird der Vorgabe der NIS-RL Rechnung getragen, der zufolge nur eine beschränkte Anzahl von Personen pro Mitgliedstaat an Sitzungen des CSIRT-Netzwerks teilnehmen kann.

Computer-Notfallteams sind in Österreich wesentliche Ansprechpartner im Bereich der IT-Sicherheit und betreuen im Rahmen ihrer Tätigkeit nicht nur Betreiber wesentlicher Dienste und Anbieter digitaler Dienste. Insbesondere das nationale Computer-Notfallteam soll daher im Rahmen der ihm zur Verfügung stehenden Ressourcen beispielsweise auch Warnungen, Alerts und Tipps für KMU (kleine und mittlere Unternehmen) oder auch für eine breitere Öffentlichkeit, die auch Privatpersonen umfasst, herausgeben können (Abs. 6).

Zur Erfüllung ihrer Aufgaben sollen Computer-Notfallteams personenbezogene Daten verarbeiten dürfen. Dabei sind insbesondere jene personenbezogenen Daten betroffen, die auch von den NIS-Büros im Rahmen der gemeinsamen Datenverarbeitung gemäß § 11 Abs. 1 verarbeitet werden dürfen (vgl. auch die Aufzählung der Datenarten in den Erläuterungen zu § 11). Es wird daher eine ausdrückliche gesetzliche Grundlage geschaffen, die Computer-Notfallteams dazu ermächtigt, personenbezogene Daten zu verarbeiten, sofern dies zur Erfüllung ihrer Aufgaben gemäß Abs. 2 notwendig ist (Abs. 7). Damit ist auch eine gegenseitige Übermittlung der Daten zwischen den Computer-Notfallteams zulässig. Dies umfasst alle personenbezogenen Daten von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste, sonstigen Einrichtungen und Personen, die im Zusammenhang mit einem Sicherheitsvorfall oder einer sonstigen Störung stehen oder die bei der Beobachtung und Analyse von Risiken und Bedrohungen zu verarbeiten sind, und für die Computer-Notfallteams gemäß Abs. 1, 3, 4 und 6 die Aufgaben gemäß Abs. 2 wahrnehmen. Die Absätze 3, 4 und 6 sind daher ebenso von der Datenverarbeitungsermächtigung erfasst, da sie jeweils an die Erfüllung der Aufgaben gemäß Abs. 2 anknüpfen.

Im Kontext dieser Bestimmung ist auf ErwGr 49 der DSGVO hinzuweisen. In diesem ErwGr wird ausgeführt, dass die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams – CERT, bzw. Computer Security Incident Response Teams – CSIRT), 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 solches 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.

Zu § 13 (Anforderungen und Eignung eines Computer-Notfallteams):

Computer-Notfallteams erfüllen zentrale Aufgaben im Bereich der NIS, insbesondere sind sie für die Entgegennahme von Meldungen sowie die Überwachung und Analyse von Bedrohungslagen zuständig. Es ist daher erforderlich, dass Computer-Notfallteams gewisse Anforderungen erfüllen müssen (Abs. 1). Diese Anforderungen entsprechen zu einem großen Teil den Anforderungen an CSIRT, die in Anhang I Z 1 NIS-RL vorgegeben werden. Dies betrifft etwa die sicheren Räumlichkeiten (Z 1), wobei man sich hier auch vor allem an den datenschutzrechtlichen Vorgaben aus der DSGVO orientiert, und die

Betriebskontinuität, die sowohl im personellen, technischen als auch im infrastrukturellen Bereich sichergestellt sein muss (Z 2). Die NIS-RL verlangt in diesem Zusammenhang eine ständige Bereitschaft, worunter wohl zumindest eine rund um die Uhr vorhandene Rufbereitschaft zu verstehen ist. Handelt es sich bei einem Computer-Notfallteam um ein sektorenspezifisches Computer-Notfallteam, so muss der Nachweis erbracht werden, dass zumindest ein Teil der in diesem Sektor gemäß § 14 ermittelten Betreiber dieses Computer-Notfallteam unterstützt (Z 3). Sofern in einem Sektor daher mehr als ein Betreiber wesentlicher Dienste ermittelt wurde, ist die Unterstützung von zumindest zwei Betreibern wesentlicher Dienste aus diesem Sektor nachzuweisen. Im Einzelfall ist zu beurteilen, ob die Unterstützung aus einem Sektor (bezogen auf die Anzahl der in diesem Sektor ermittelten Betreiber) ausreichend ist. Darüber hinaus ist sicherzustellen, dass die bei einem Computer-Notfallteam angestellten Personen über die notwendige fachliche Eignung verfügen und sich vor Beginn ihrer Tätigkeit einer Sicherheitsüberprüfung nach den Bestimmungen des Sicherheitspolizeigesetzes unterzogen haben (Z 4).

Auch das gemäß § 12 Abs. 4 beim Bundeskanzler eingerichtete GovCERT hat die Anforderungen, die gemäß Abs. 1 Z 1, 2 und 4 an ein Computer-Notfallteam gestellt werden, zu erfüllen. Aufgrund seiner besonderen Stellung, Zuständigkeit und gesetzlichen Einrichtung ist kein Nachweis im Sinne des Abs. 1 Z 3 erforderlich (Abs. 2).

Die Eignung eines Computer-Notfallteams ist vom Bundeskanzler im Einvernehmen mit dem Bundesminister für Inneres festzustellen (Abs. 3). Da es sich bei den Aufgaben „Entgegennahme und Weiterleitung von Meldungen“ um hoheitliche Aufgaben handelt, sind die Computer-Notfallteams, sofern es sich dabei um private Einrichtungen handelt, für diese Tätigkeiten als Beliehene anzusehen. Computer-Notfallteams 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. Sollte sich an den Umständen, die zur Erlassung dieses Bescheids geführt haben, etwas ändern, so hat das betroffene Computer-Notfallteam dies unverzüglich dem Bundeskanzler anzuzeigen. Dieser hat die geänderten Umstände zu prüfen und kann die Ermächtigung ganz oder teilweise widerrufen.

Zu § 14 (Ermittlung der Betreiber wesentlicher Dienste):

In Umsetzung von Art. 5 und 6 NIS-RL sind die Einrichtungen zu ermitteln, welche die durch die Definition des Begriffs „Betreiber wesentlicher Dienste“ in der NIS-RL festgelegten Kriterien erfüllen. Damit ein unionsweit einheitlicher Ansatz gewährleistet ist, ist der Begriff „Betreiber wesentlicher Dienste“ in allen Mitgliedstaaten richtlinienkonform auszulegen.

Es ist Aufgabe des Bundeskanzlers, jene Einrichtungen zu ermitteln, die einen wesentlichen Dienst (Abs. 2) in einem der in § 2 Abs. 1 genannten Sektoren erbringen (Abs. 1). Diese Sektoren orientieren sich am Anhang II der NIS-RL. Im Ermittlungsprozess sollen auch der Bundesminister für Inneres und die für den jeweiligen Sektor zuständigen Bundesminister befasst werden. Dies umfasst insbesondere die Teilnahme an Abstimmungssitzungen mit Vertretern der betroffenen Sektoren und den zuständigen Interessenvertretungen.

Bei der Bewertung, ob einem Dienst eine wesentliche Bedeutung für die in Abs. 2 erster Satz genannten Rechtsgüter zukommt, sind die in der NIS-RL vorgegebenen sektorenübergreifenden Faktoren, mit denen bestimmt wird, ob eine erhebliche Störung einen potenziellen Sicherheitsvorfall bewirken würde und diesem daher eine wesentliche Bedeutung zukommt, zu berücksichtigen. Zu den verwendeten Begrifflichkeiten in Abs. 2 erster Satz siehe ErläutRV 99 BlgNR 25. GP 13 f (zu § 22 Abs. 1 Z 6 SPG). Sofern dies notwendig erscheint, können auch konkrete sektorenspezifische Faktoren berücksichtigt werden. Außerdem sollte die Erbringung des wesentlichen Dienstes zu einem überwiegenden Teil von Netz- und Informationssystemen abhängig sein, damit dieser in den Anwendungsbereich fällt.

Um eine funktionierende Kommunikation zwischen den zuständigen Behörden und den Computer-Notfallteams mit den ermittelten Betreibern wesentlicher Dienste sicherzustellen, haben die Betreiber wesentlicher Dienste gegenüber dem Bundeskanzler eine Kontaktstelle (zB Telefonnummer, E-Mail-Adresse) bekanntzugeben (Abs. 3). Die Betreiber wesentlicher Dienste haben sicherzustellen, dass sie jedenfalls in jenem Zeitraum, in dem sie ihre wesentlichen Dienste zur Verfügung stellen, über diese Kontaktstelle erreichbar sind.

Mit Verordnung werden die in § 2 Abs. 1 genannten Sektoren und die Faktoren gemäß Abs. 2, die zur Ermittlung der Betreiber wesentlicher Dienste herangezogen werden sollen, näher konkretisiert (Abs. 4). In dieser Verordnung werden insbesondere die betroffenen Teilsektoren und die Schwellenwerte bestimmt, die für die Beurteilung der Wesentlichkeit eines betriebenen Dienstes heranzuziehen sind. Außerdem können jene Vorschriften zu Sicherheitsvorkehrungen und zur Meldepflicht, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme gewährleisten, festgelegt werden.

Dies betrifft etwa bereits bestehende Regelungen in den Sektoren Bankwesen und Finanzmarktinfrastrukturen (§ 2 Abs. 1 Z 3 und 4).

Im Zusammenhang mit der Ermittlung von Betreibern wesentlicher Dienste kommen dem Bundeskanzler zentrale Aufgaben zu (Abs. 5 Z 1 bis 4).

Ein Betreiber wesentlicher Dienste ist erst vom Anwendungsbereich erfasst, wenn er durch den Bundeskanzler als solcher ermittelt wurde und ihm gegenüber über diesen Umstand ein Bescheid erlassen wurde (Z 1). Diesem Bescheid kommt daher für die Eigenschaft als Betreiber wesentlicher Dienste eine konstitutive Wirkung zu. Dabei ist gemäß Art. I Abs. 2 Z 1 EGVG auf das behördliche Verfahren das AVG anzuwenden. Fallen die Voraussetzungen weg, die für die Ermittlung eines Betreibers wesentlicher Dienste maßgeblich waren, so ist der Bescheid zu widerrufen, wenn dem Bundeskanzler diese Umstände bekannt werden.

Die NIS-RL sieht einen Konsultationsprozess unter Einbeziehung der betreffenden Mitgliedstaaten im Falle von Einrichtungen, die in mehr als einem Mitgliedstaat Dienste erbringen, sowie Unterstützung der Kooperationsgruppe im Rahmen des Verfahrens der Ermittlung vor (Z 2). Für den Fall, dass ein Betreiber wesentlicher Dienste seine Dienste in zwei oder mehreren Mitgliedstaaten anbietet, sieht die NIS-RL in ErwGr 24 vor, dass die betroffenen Mitgliedstaaten zur Ermittlung des Betreibers untereinander bilaterale oder multilaterale Beratungen aufnehmen sollten. Dieser Konsultationsprozess soll den Mitgliedstaaten dabei helfen, die Kritikalität des Betreibers im Hinblick auf grenzüberschreitende Auswirkungen zu beurteilen, und ermöglicht es jedem beteiligten Mitgliedstaat, sich zu den Risiken zu äußern, die seiner Ansicht nach mit den von dem Betreiber angebotenen Diensten verbunden sind. Hierbei sollten die betroffenen Mitgliedstaaten den Ansichten der jeweils anderen Mitgliedstaaten Rechnung tragen. Die betroffenen Mitgliedstaaten können diesbezüglich die Unterstützung der Kooperationsgruppe anfordern.

Damit dafür gesorgt ist, dass etwaige Marktveränderungen genau berücksichtigt werden, soll eine Liste der ermittelten Dienste erstellt werden, welche regelmäßig überprüft und bei Bedarf aktualisiert werden muss (Z 3).

Ferner ist der Kommission diese Liste regelmäßig, zumindest aber alle zwei Jahre, zu übermitteln, um dieser eine Überprüfung der ordnungsgemäßen Anwendung der NIS-RL gemäß Art. 23 NIS-RL zu ermöglichen (Z 4).

Zu § 15 (Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste):

In Umsetzung des Art. 14 Abs. 1 NIS-RL wird den Betreibern wesentlicher Dienste vorgeschrieben, geeignete, dem Stand der Technik entsprechende, Sicherheitsvorkehrungen zu treffen. Diese können sowohl technischer als auch organisatorischer Art sein und sollen in Hinblick auf die betriebenen wesentlichen Dienste dazu dienen, die Netz- und Informationssystemsicherheit (NIS) zu gewährleisten (Abs. 1). Netz- und Informationssysteme müssen die Fähigkeit besitzen, Sicherheitsvorfällen (§ 3 Z 6) vorzubeugen, diese abzuwehren und zu beseitigen. Sicherheitsvorkehrungen, die jedenfalls zur Gewährleistung der Anforderungen nach Abs. 1 geeignet sind, können zu einem späteren Zeitpunkt durch Verordnung des Bundeskanzlers, im Einvernehmen mit dem Bundesminister für Inneres, festgelegt werden. Dabei werden die Arbeiten zu diesem Thema auf europäischer Ebene (zB im Rahmen der Kooperationsgruppe und mit Unterstützung der ENISA) und bereits bestehende und etablierte internationale Standards, die für den Bereich NIS einschlägig sind, berücksichtigt (Abs. 6).

Darüber hinaus können Betreiber wesentlicher Dienste gemeinsam mit ihren Sektorenverbänden eigene Sicherheitsvorkehrungen vorschlagen, mit denen die Anforderungen des Abs. 1 gewährleistet werden können (Abs. 2), und anschließend beantragen, dass die Eignung dieser Sicherheitsvorkehrungen festgestellt wird. Diese Möglichkeit besteht auch für einzelne Teilsektoren. Es ist Aufgabe des Bundesministers für Inneres, über einen solchen Antrag bescheidmäßig zu entscheiden.

Die NIS-RL sieht vor, dass die Einhaltung der Sicherheitsvorkehrungen periodisch zu überprüfen ist. Dafür haben die Betreiber dem Bundesminister für Inneres die Erfüllung der Anforderungen mindestens alle drei Jahre in geeigneter Weise nachzuweisen (Abs. 3). Hiefür ist es ausreichend, wenn eine Aufstellung der vorhandenen Sicherheitsvorkehrungen sowie ein Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen erbracht werden. Dieser Nachweis kann erst ein Jahr nach Zustellung des Bescheids, mit dem ein Betreiber wesentlicher Dienste ermittelt wurde, verlangt werden. Nach Ablauf dieser Ein-Jahres-Frist kann eine Überprüfung jederzeit erfolgen. Die Erfordernisse, die eine solche qualifizierte Stelle erfüllen muss, werden gesondert in der gemäß Abs. 4 zu erlassenden Verordnung festgelegt. Der Bundesminister für Inneres hat die Befugnis, Einschau in die notwendigen Unterlagen und bei Bedarf auch in die betroffenen Netz- und Informationssysteme der Betreiber wesentlicher Dienste zu nehmen.

Wird festgestellt, dass die Anforderungen gemäß Abs. 1 nicht erfüllt werden, so kann der Bundesminister für Inneres Handlungsempfehlungen aussprechen und einen Nachweis für deren Befolgung verlangen. Dafür ist eine angemessene Frist zu setzen. Wird diesen Empfehlungen nicht innerhalb dieser Frist vom Betreiber wesentlicher Dienste nachgekommen, so ist deren Befolgung bescheidmäßig und unter Androhung einer Sanktion anzuordnen.

Durch Verordnung werden die verpflichtenden Erfordernisse einer qualifizierten Stelle vom Bundesminister für Inneres im Einvernehmen mit dem Bundeskanzler festgelegt (Abs. 4). Unternehmen, die als qualifizierte Stelle fungieren möchten, können einen Antrag an den Bundesminister für Inneres stellen, der daraufhin über das Vorliegen einer qualifizierten Stelle im jeweiligen Fall mit Bescheid entscheidet. Darüber hinaus kann der Bundesminister für Inneres besondere Kriterien festlegen, deren Erfüllung ein Unternehmen ohne vorherige Bescheiderlassung jedenfalls dazu berechtigt, als qualifizierte Stelle aufzutreten.

Um zu gewährleisten, dass die (durch die Verordnung festgelegten) Erfordernisse an und die Kriterien für qualifizierte Stellen von diesen auch entsprechend erfüllt und eingehalten werden, kann der Bundesminister für Inneres zu Überprüfungszwecken jederzeit Einschau in deren Netz- und Informationssysteme und diesbezüglichen Unterlagen nehmen (Abs. 5). Werden die durch die Verordnung festgelegten Kriterien seitens des Unternehmens nicht mehr erfüllt, ist dieses nicht mehr berechtigt, als qualifizierte Stelle aufzutreten. Dasselbe gilt für den Fall, dass die durch Verordnung festgelegten Erfordernisse nicht mehr gegeben sind, wobei in diesem Fall der Status „qualifizierte Stelle“ durch den Bundesminister für Inneres bescheidmäßig zu entziehen ist (Abs. 4).

Zu § 16 (Meldepflicht für Betreiber wesentlicher Dienste):

Die Tragweite, Häufigkeit und Auswirkungen von Sicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Diese Systeme können auch zu einem Angriffsziel vorsätzlich schädigender Handlungen werden, die auf die Störung oder den Ausfall des Betriebs der Systeme gerichtet sind. Solche Sicherheitsvorfälle können die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, beträchtliche finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Gesellschaft und Wirtschaft großen Schaden zufügen.

In Umsetzung des Art. 14 Abs. 3 NIS-RL wird daher in Abs. 1 vorgesehen, dass Betreiber wesentlicher Dienste Sicherheitsvorfälle (§ 3 Z 6) unverzüglich zu melden haben. Die Meldung, aus der sich das Vorliegen eines (meldepflichtigen) Sicherheitsvorfalls eindeutig ergeben muss, erfolgt an das jeweils zuständige Computer-Notfallteam. Dieses ist das sektorenspezifische Computer-Notfallteam, sofern ein solches vorhanden ist und der betroffene Betreiber wesentlicher Dienste dieses unterstützt, andernfalls das nationale Computer-Notfallteam (Abs. 2). Das Computer-Notfallteam, das eine solche Meldung erhält, hat diese unverzüglich an den Bundesminister für Inneres weiterzuleiten. Die eingehenden Meldungen werden vom Bundesminister für Inneres bei der Erstellung des Lagebilds berücksichtigt und sind somit Teil der im IKDOK auszutauschenden Informationen.

Die Meldungen, die ein Betreiber wesentlicher Dienste abgibt, haben alle notwendigen Angaben und Informationen zum Sicherheitsvorfall zu enthalten, die es braucht, um die Lage der betroffenen Einrichtung, Erheblichkeit des Sicherheitsvorfalls generell und allfällige Auswirkungen auf andere Sektoren oder die Öffentlichkeit bewerten zu können, da sich daran weitere Rechtsfolgen und Informationsverpflichtungen knüpfen können (Abs. 3). Dies umfasst insbesondere die technischen Rahmenbedingungen, die vermutete oder tatsächliche Ursache, die konkret betroffenen Netz- und Informationssysteme sowie allgemeine Informationen zum betroffenen Betreiber wesentlicher Dienste. Angaben über später bekanntgewordene Umstände sind ohne unangemessene weitere Verzögerung mitzuteilen. Durch diese Regelung wird zum Ausdruck gebracht, dass einer möglichst frühzeitigen Meldung Vorrang gegenüber einer vollständigen Meldung eingeräumt wird. Die Pflicht, später bekanntgewordene Angaben zu melden, soll die Bewältigung eines Sicherheitsvorfalls nicht beeinträchtigen. Zur Erfüllung der Meldepflicht ist es jedoch jedenfalls erforderlich, sämtliche Umstände bekannt zu geben, die zum Zeitpunkt der Meldung bekannt sind. In Abstimmung mit dem anderen NIS-Büro und den Computer-Notfallteams kann der Bundesminister für Inneres einen sicheren Kommunikationskanal und geläufige elektronische Formate, die bei einer Meldung zu verwenden sind, festlegen.

Hat ein Sicherheitsvorfall bei einem Anbieter digitaler Dienste erhebliche Auswirkungen auf die Bereitstellung des Dienstes, den ein Betreiber wesentlicher Dienste erbringt, weil dieser sich des Anbieters digitaler Dienste als Dienstleister bedient, so trifft den Betreiber wesentlicher Dienste eine Meldepflicht gemäß Abs. 1 (Abs. 4). Eine allfällige gesonderte Meldepflicht, die den eigentlich von dem Sicherheitsvorfall betroffenen Anbieter digitaler Dienste trifft, ist davon unbeschadet.

Hat ein Sicherheitsvorfall einen grenzüberschreitenden Bezug, etwa weil der Betreiber wesentlicher Dienste seinen Dienst in mehreren EU-Mitgliedstaaten erbringt, so sind die zentralen Anlaufstellen in den anderen Ländern im Wege der zentralen Anlaufstelle (SPOC) über diesen Sicherheitsvorfall zu informieren (Abs. 5).

In bestimmten Fällen kann es erforderlich sein, dass die Öffentlichkeit über einen Sicherheitsvorfall informiert wird (Abs. 6). Dies ist insbesondere dann der Fall, wenn es einer Sensibilisierung der Öffentlichkeit zur Verhütung künftiger Sicherheitsvorfälle, die eventuell mit noch gravierenderen Auswirkungen als der aktuelle Sicherheitsvorfall verbunden sind, dienen kann. Außerdem ist die Öffentlichkeit zu informieren, wenn dies notwendig erscheint, um die Auswirkungen des Sicherheitsvorfalls zu bewältigen oder um einer größeren Verunsicherung in der Bevölkerung entgegenzuwirken. Der Betreiber wesentlicher Dienste kann dazu aufgefordert werden, selbst die Öffentlichkeit zu informieren. Zuständig für diese Öffentlichkeitsarbeit ist der Bundeskanzler, sofern ein Sicherheitsvorfall mehr als einen Sektor betrifft. In allen anderen Fällen ist der Bundesminister für Inneres im Rahmen seines gesetzlichen Wirkungsbereichs zuständig.

Mit Verordnung können nähere Kriterien zu den Parametern des § 3 Z 6 lit. a bis dfestgelegt werden (Abs. 7).

Zu § 17 (Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste)

Art. 1 Abs. 7 der NIS-RL enthält eine Lex-specialis-Bestimmung, wonach die Bestimmungen über die Sicherheitsanforderungen oder Meldepflichten für Anbieter digitaler Dienste oder Betreiber wesentlicher Dienste nach der NIS-RL keine Anwendung finden, wenn sektorenspezifische Rechtsvorschriften der Europäischen Union für Sicherheitsanforderungen oder Meldepflichten gelten, die in ihrer Wirkung den in der NIS-RL enthaltenen Pflichten mindestens gleichwertig sind. In diesem Fall sind die einschlägigen Bestimmungen jenes sektorenspezifischen Unionsrechtsakts, wie zB der Richtlinie (EU) 2015/2366 („Zweite Zahlungsdiensterichtlinie“), anzuwenden. Art. 1 Abs. 7 der NIS-RL ist von den Mitgliedstaaten bei der Umsetzung zu berücksichtigen (vgl. auch ErwGr 9 NIS-RL). Dies geschieht durch § 18. Trotz Anwendbarkeit von Lex-specialis-Bestimmungen wird eine Einrichtung als Betreiber wesentlicher Dienste gemäß § 14 ermittelt, um solchen Einrichtungen insbesondere die Einrichtung eines sektorenspezifischen Computer-Notfallteams (§ 12 Abs. 1 zweiter Satz) sowie die Teilnahme an einer technischen Einrichtung nach § 9 Abs. 1 zu ermöglichen. Die Verpflichtung zur Nennung einer Kontaktstelle (§ 14 Abs. 3) bleibt von § 18 unberührt.

Obwohl Betreiber wesentlicher Dienste, für die Lex-specialis-Bestimmungen im Sinne des Abs. 1 zur Meldepflicht anwendbar sind, Sicherheitsvorfälle nicht gemäß § 16 zu melden haben, soll ein gesamtstaatliches und vollständiges Lagebild erstellt werden. Um dies zu gewährleisten, sieht Abs. 2 vor, dass die Finanzmarktaufsichtsbehörde (FMA) Meldungen, die im Falle eines schwerwiegenden Betriebs- oder Sicherheitsvorfalls von einem Zahlungsdienstleister an die FMA gemäß § 86 Abs. 1 Zahlungsdienstegesetz 2018 (ZaDiG 2018), BGBl. I Nr. 17/2018, unverzüglich mitzuteilen sind, an den Bundesminister für Inneres unverzüglich weiterzuleiten hat. Dadurch soll sichergestellt werden, dass das gesamtheitliche Lagebild, welches in der OpKoord (§ 3 Z 5) erörtert werden soll, auch Informationen über schwerwiegende Betriebs- oder Sicherheitsvorfälle bei Betreibern wesentlicher Dienste aus dem Sektor Bankwesen enthält.

Zu § 18 (Sicherheitsvorkehrungen und Meldepflicht für Anbieter digitaler Dienste):

Viele Unternehmen verlassen sich bei der Bereitstellung ihrer eigenen Dienste auf Anbieter digitaler Dienste im Sinne dieses Bundesgesetzes. Da manche digitale Dienste für ihre Nutzer, darunter auch Betreiber wesentlicher Dienste, eine wichtige Ressource darstellen können, und da derartigen Nutzern nicht immer Alternativen zur Verfügung stehen, sollen die in diesem Bundesgesetz vorgeschriebenen Verpflichtungen auch für die Anbieter derartiger Dienste gelten. Die Sicherheit, Kontinuität und Verlässlichkeit dieser digitalen Dienste sind für das reibungslose Funktionieren vieler Unternehmen von wesentlicher Bedeutung. Eine Störung eines digitalen Dienstes könnte die Bereitstellung anderer, von ihnen abhängiger Dienste verhindern und somit wesentliche wirtschaftliche und gesellschaftliche Tätigkeiten beeinträchtigen.

Angesichts der Bedeutung ihrer Dienste für die Tätigkeit anderer Unternehmen sollten Anbieter digitaler Dienste ein Sicherheitsniveau gewährleisten, das der Höhe des Risikos für die Sicherheit der von ihnen gebotenen Dienste angemessen ist (Abs. 1). Die von ihnen zu treffenden Sicherheitsvorkehrungen können sowohl technischer als auch organisatorischer Art sein und sollen in Hinblick auf die betriebenen digitalen Dienste dazu dienen, die Netz- und Informationssystemsicherheit (NIS) zu gewährleisten. In der Praxis wird das Risiko für die Betreiber wesentlicher Dienste, die oft für die Aufrechterhaltung kritischer gesellschaftlicher und wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung sind, höher sein als das Risiko für die Anbieter digitaler Dienste. Der Entfall der Nachweispflicht (vgl. § 15 Abs. 3) sowie der

Verzicht auf eine Verordnungsermächtigung zur Festlegung der Sicherheitsvorkehrungen (vgl. § 15 Abs. 6), wie dies bei Betreibern wesentlicher Dienste vorgesehen ist, begründen sich unmittelbar aus der NIS-RL (vgl. Art. 16 Abs. 10 NIS-RL) und somit dem Umstand, dass es in deren Verantwortungsbereich zu belassen ist, welche Maßnahmen sie ergreifen, die sie für die Bewältigung der Risiken für die Sicherheit ihrer Netze und Informationssysteme für angemessen halten. Aufgrund des grenzüberschreitenden Charakters ihrer Tätigkeiten unterliegen die Anbieter digitaler Dienste einem auf europäischer Ebene stärker harmonisiertem Konzept. Durchführungsrechtsakte der Europäischen Kommission erleichtern die Spezifikation und Umsetzung derartiger Maßnahmen.

Auch Anbieter digitaler Dienste unterliegen prinzipiell der Meldepflicht von Sicherheitsvorfällen, die bei ihnen auftreten (Abs. 2). Allerdings gilt dies nur dann, wenn sie Zugang zu Informationen haben, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls zu bewerten. Dabei handelt es sich insbesondere um Informationen über die Zahl der vom Sicherheitsvorfall betroffenen Nutzer, der Dauer des Sicherheitsvorfalls, die geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet, das Ausmaß der Unterbrechung der Bereitstellung des digitalen Dienstes und das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten. Das zuständige Computer-Notfallteam, an das die Meldung eines Anbieters digitaler Dienste zu erfolgen hat, ist das nationale Computer-Notfallteam.

Hat ein Sicherheitsvorfall einen grenzüberschreitenden Bezug, etwa weil der digitale Diensteanbieter seinen Dienst in mehreren EU-Mitgliedstaaten erbringt, so sind die zentralen Anlaufstellen in den anderen Ländern im Wege der zentralen Anlaufstelle (SPOC) über diesen Sicherheitsvorfall zu informieren (Abs. 3).

Anbieter digitaler Dienste unterliegen weniger strikten, reaktiven Aufsichtstätigkeiten, die durch die Art ihrer Dienste und Tätigkeiten gerechtfertigt sind. Der Bundesminister für Inneres wird daher nur dann tätig werden, wenn ihm (zB durch den Anbieter digitaler Dienste selbst, durch eine andere Behörde – auch der eines anderen EU-Mitgliedstaats – oder durch einen Nutzer des Dienstes) Nachweise dafür vorgelegt werden, dass ein Anbieter digitaler Dienste die Anforderungen dieses Bundesgesetzes nicht erfüllt, vor allem dann, wenn sich ein Sicherheitsvorfall ereignet hat (Abs. 4).

Zu § 19 (Sicherheitsvorkehrungen und Meldepflicht für Einrichtungen des Bundes):

Neben Betreibern wesentlicher Dienste und Anbietern digitaler Dienste kommt auch öffentlichen Stellen eine wesentliche Bedeutung bei der Aufrechterhaltung von zentralen gesellschaftlichen und staatlichen Funktionen zu. In dieser Bestimmung werden daher die Sicherheitsvorkehrungen (Abs. 1) und Meldepflichten (Abs. 2), die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste treffen, auch für die Einrichtungen des Bundes (§ 3 Z 15) vorgesehen. Allerdings liegt es in der Eigenverantwortung der jeweiligen Einrichtung, die Einhaltung der notwendigen und geeigneten Sicherheitsvorkehrungen zu gewährleisten, da eine regelmäßige oder auch eine anlassfallbezogene Überprüfung dieser Maßnahmen durch eine andere Stelle nicht vorgesehen ist.

Liegt bei einer Einrichtung des Bundes ein Sicherheitsvorfall (§ 3 Z 6) vor, so ist dieser grundsätzlich an das dafür zuständige GovCERT zu melden (Abs. 2). Störungen, die nicht die Erheblichkeit eines Sicherheitsvorfalls erreichen, können freiwillig an das GovCERT gemeldet werden (Abs. 3). Der Meldeprozess unterscheidet sich in weiterer Folge nicht von jenem, der für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste vorgesehen ist. Davon ausgenommen sind lediglich die Behörden, bei denen NIS-Büros eingerichtet sind und die ihrer Meldepflicht durch direkte Weitergabe der notwendigen Informationen im Rahmen des IKDOK nachkommen müssen. Freiwillige Meldungen werden ebenfalls im Rahmen des IKDOK weitergegeben.

Hat ein Sicherheitsvorfall bei einer Einrichtung des Bundes einen grenzüberschreitenden Bezug, so sind die zentralen Anlaufstellen in den anderen Ländern im Wege der zentralen Anlaufstelle (SPOC) über diesen Sicherheitsvorfall zu informieren (Abs. 4).

Zu § 20 (Freiwillige Meldungen):

Einrichtungen, die nicht in den Geltungsbereich dieses Gesetzes fallen, können mit Sicherheitsvorfällen konfrontiert sein, die sich in erheblichem Maße auf die von ihnen bereitgestellten Dienste auswirken. Sind diese Einrichtungen der Ansicht, dass es im öffentlichen Interesse liegt, den zuständigen Stellen das Auftreten derartiger Sicherheitsvorfälle zu melden, sollten sie dies auf freiwilliger Basis tun können. Art. 20 NIS-RL sieht diesen Fall der freiwilligen Meldungen explizit vor.

Gleiches gilt für Störungen, die nicht die Erheblichkeit eines Sicherheitsvorfalls (§ 3 Z 6) erreichen, aber bei einer Einrichtung, die vom Anwendungsbereich erfasst ist (zB bei einem Betreiber wesentlicher Dienste), auftreten. Auch solche Informationen sind von großem Interesse für ein gesamtstaatliches und vollständiges Lagebild und sollten daher an die zuständigen Stellen weitergegeben werden.

Der Meldeweg unterscheidet sich grundsätzlich nicht von jenem für eine verpflichtende Meldung, das heißt auch freiwillige Meldungen ergehen direkt an das zuständige Computer-Notfallteam, welches diese Meldungen an den Bundesminister für Inneres 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 namentliche Nennung des (freiwilligen) Melders kann dabei auf dessen Verlangen entfallen. Die Bearbeitung von freiwilligen Meldungen sollte darüber hinaus zu keinem unverhältnismäßigen oder ungebührlichen Aufwand für die betreffende Stelle, an die gemeldet wird, führen und kann gegenüber einer verpflichtenden Meldung nachrangig bearbeitet werden.

Für freiwillige Meldungen ist grundsätzlich der gleiche sichere Kommunikationskanal wie für verpflichtende Meldungen zu verwenden.

Zu § 21 (Cyberkrise):

Der Bundesminister für Inneres stellt fest, ob bei einer vorhandenen schweren Anomalie im Cyberraum die Voraussetzungen einer Cyberkrise (§ 3 Z 18) vorliegen und ruft diese gegebenenfalls aus. Bei seiner Entscheidungsfindung wird er durch den Koordinationsausschuss beratend unterstützt (§ 22).

Zu § 22 (Koordinationsausschuss):

Der Koordinationsausschuss wird als interministerielles Gremium eingerichtet und besteht in seiner Stammbesetzung aus dem Generaldirektor für die öffentliche Sicherheit als Leiter, dem Chef des Generalstabs, dem Generalsekretär für auswärtige Angelegenheiten und dem Generalsekretär des Bundeskanzleramtes (Abs. 2 erster Satz). Zu seinen Aufgaben zählen die Beratung des Bundesministers für Inneres im Vorfeld einer möglichen Cyberkrise (§ 21) und hinsichtlich der operativen Maßnahmen zur Bewältigung der Cyberkrise auf strategischer Ebene sowie der Bundesregierung zur Koordination der Öffentlichkeitsarbeit im Zusammenhang mit einer Cyberkrise (Abs. 1).

Da der Koordinationsausschuss rechtlich betrachtet nicht direkt anordnungsbefugt ist, setzen sich seine Mitglieder primär aus Entscheidungsträgern der Bundesministerien zusammen, die die strategischen Entscheidungen bzw. abgestimmten Maßnahmen operativ umsetzen sollen. Zudem kann es erforderlich sein, den Ausschuss mit Vertretern von Bundes- oder Landesbehörden, Betreibern wesentlicher Dienste, Computer-Notfallteams sowie Einsatzorganisationen zu erweitern, um die Cyberkrise zu bewältigen (Abs. 2).

Der IKDOK (§ 7) soll den Koordinationsausschuss durch die Erstellung von anlassbezogenen Lagebildern und die technische Expertise seiner Mitglieder unterstützen (Abs. 3).

Zu § 23 (Verwaltungsstrafbestimmungen):

Für Verstöße gegen die Verpflichtungen, die sich aus diesem Bundesgesetz ergeben, sind Verwaltungsstrafen von der zuständigen Bezirksverwaltungsbehörde zu verhängen (Abs. 1). Nach dieser Bestimmung zu ahndende Verwaltungsübertretungen stellen insbesondere Verstöße gegen Mitwirkungspflichten im Rahmen der Überprüfung der von den Betreibern wesentlicher Dienste und Anbietern digitaler Dienste zu treffenden Sicherheitsvorkehrungen oder Missachtungen der Meldepflicht dar. Nachdem im österreichischen Recht Geldbußen gegen Behörden und öffentliche Stellen grundsätzlich nicht vorgesehen sind, ist ein Verstoß gegen die Verpflichtungen, die sich aus § 19 ergeben, nicht nach Abs. 1 zu ahnden.

Die örtliche Zuständigkeit richtet sich in der Regel nach der Hauptniederlassung der Einrichtung, die eine Verwaltungsübertretung gemäß Abs. 1 begangen hat (Abs. 2).

Werden verschiedene strafbare Handlungen durch eine Tat verwirklicht, dann sind diese mit dem Doppelbestrafungsverbot gemäß Art 4 7. ZPMRK nur dann vereinbar, wenn die strafbaren Handlungen nicht dieselben wesentlichen Elemente aufweisen (EGMR, Franz Fischer, 29.5.2001, 37.950/97). Dementsprechend liegt eine Verwaltungsübertretung gemäß Abs. 1 nur dann vor, wenn die Tat nicht den Tatbestand einer in die Zuständigkeit der ordentlichen Gerichte fallenden strafbaren Handlung bildet oder nicht nach anderen Verwaltungsstrafbestimmungen mit einer strengeren Strafe bedroht ist (Abs. 3).

Erforderlich erscheint eine Regelung, unter welchen Voraussetzungen Geldbußen gegen juristische Personen verhängt werden können (Abs. 4 und 5). Die Verhängung von Geldbußen gegen juristische Personen orientiert sich an § 99d des Bankwesengesetzes (BWG), BGBl. Nr. 532/1993.

Zu §§ 24 bis 28 (Schlussbestimmungen)

In den Schlussbestimmungen werden Regelungen in Hinblick auf die Verwendung personenbezogener Bezeichnungen, Verweisungen auf andere Bundesgesetze, europäische Vorgaben, die Vollziehung und das Inkrafttreten dieses Bundesgesetzes getroffen.

Mit diesem Bundesgesetz wird die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL) umgesetzt. Die Mitgliedstaaten haben diese gemäß Art. 25 Abs. 1 NIS-RL bis zum 9. Mai 2018 in nationales Recht umzusetzen. An diesem Tag soll daher auch dieses Bundesgesetz in Kraft treten, mit Ausnahme der Verwaltungsstrafbestimmungen (§ 23), welche mit Ablauf des Tages der Kundmachung dieses Bundesgesetzes in Kraft treten sollen.