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 und der Bundesminister für Inneres die operativen Aufgaben wahrnehmen.

Um ein hohes Sicherheitsniveau von Netz- und Informationssystemen zu erreichen, werden in diesem Bundesgesetz Maßnahmen vorgesehen. Neben den Verpflichtungen, die Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie 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.

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 von Verpflichtungen für die ermittelten Betreiber wesentlicher Dienste, die digitalen Diensteanbieter sowie Einrichtungen des Bundes. Diese haben einerseits angemessene Sicherheitsvorkehrungen für ihre Netz- und Informationssysteme vorzusehen und anderseits Sicherheitsvorfälle an die zuständigen Stellen zu melden;
- die Überprüfung geeigneter Sicherheitsvorkehrungen und der Einhaltung der Meldepflicht;
- die Einrichtung von Computer-Notfallteams und Festlegung der Aufgaben, die diesen zukommen sollen;
- die Regelung von Strukturen und Aufgaben 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. Die Kompetenzdeckungsklausel umfasst im Sinne der jüngeren Staatspraxis auch die Änderung von Vorschriften, wie sie in diesem Bundesgesetz enthalten sind. Nicht erfasst von der Kompetenzdeckungsklausel ist der Bereich der Hoheitsverwaltung der Länder und Gemeinden, doch können die Länder auf freiwilliger Basis nach § 22 Abs. 5 die Pflichten gemäß § 22 Abs. 1 und 2 auch in Hinblick auf wichtige Dienste für anwendbar erklären.

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 § 2 wird der sachliche Anwendungsbereich des NISG festgelegt. Umfasst sind Betreiber wesentlicher Dienste (§ 3 Z 10) aus den in Z 1 bis 7 genannten Sektoren, Anbieter digitaler Dienste (§ 3 Z 13), Einrichtungen der öffentlichen Verwaltung (§ 3 Z 19). Diese Betreiber, Anbieter und Einrichtungen sind von hoher Bedeutung für das Funktionieren des Gemeinwesens, weil durch einen Sicherheitsvorfall (§ 3 Z 6) insbesondere Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit oder der Funktionsfähigkeit von staatlichen Einrichtungen sowie die Aufrechterhaltung kritischer gesellschaftlicher bzw. wirtschaftlicher Tätigkeiten beeinträchtigt würden.

Die in Z 1 bis 7 genannten Sektoren werden in der Verordnung, die gemäß § 4 Abs. 2 Z 2 zu erlassen ist, noch weiter konkretisiert, insbesondere werden in dieser Verordnung auch die betroffenen Teilsektoren, Bereiche 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. Ein Bereich kann im Teilsektor Elektrizität beispielsweise die Stromübertragung sein. Der Betrieb von Rechenzentren fällt unter keinen der genannten Sektoren, ist aber im Rahmen einer Dienstleisterstellung für die Betreiber wesentlicher Dienste sowie die Einrichtungen des Bundes von den Verpflichtungen (zB sind angemessene und geeignete Sicherheitsvorkehrungen zu ergreifen) grundsätzlich mitumfasst.

Die 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 18 aufgelistet sind. Darüber hinaus besteht für die Länder die Möglichkeit, den Anwendungsbereich auf die Ämter der Landesregierungen und sonstige Organisationseinheiten der Länder mittels Landesgesetz in den Anwendungsbereich aufzunehmen. Mit der Aufnahme dieser Einrichtungen der öffentlichen Verwaltung (§ 3 Z 19) 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 neben Betreibern wesentlicher Dienste und Anbietern digitaler Dienste auch Einrichtungen der öffentlichen Verwaltung, gleichermaßen das Funktionieren des Gemeinwesens gewährleisten und für die Daseinsvorsorge daher von hoher Bedeutung sind.

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 beispielsweise räumlich verteilte, digitale Verarbeitungsvorrichtungen 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, Sicherheitsvorfälle abzuwehren, sondern auch die Fähigkeit, Sicherheitsvorfällen präventiv vorzubeugen, eine bereits entstandene Störung zu erkennen, zu beseitigen und möglichst rasch den Normalbetrieb wiederherzustellen. 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.

Auf Basis sowie unter Einbindung bereits bestehender, operativer Strukturen werden Koordinierungsstrukturen geschaffen (§ 7). Diese Koordinierungsstrukturen bestehen aus einem sogenannten „Inneren Kreis“ und einem „Äußeren Kreis“. Der Innere Kreis der Operativen Koordinierungsstruktur (IKDOK) (Z 4) ist eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen. Für den äußeren Kreis wird eine neue Struktur zur Koordination auf der operativen Ebene (OpKoord) (Z 5) geschaffen. In Rahmen der Koordinierungsstrukturen 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 Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes von erheblicher Auswirkung geführt hat. Eine solche Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen kann beispielsweise neben Cyberangriffen oder Einwirkungen Dritter auch durch physische Ereignisse wie etwa Naturereignisse, aber auch durch Ereignisse wie z. B. Stromausfälle oder das Verhalten eigener Mitarbeiter verursacht werden. Der Dienst ist ein wesentlicher Dienst gemäß § 3 Z 9, ein digitaler Dienst gemäß § 3 Z 12 oder ein wichtiger Dienst, den eine Einrichtung des Bundes erbringt. Damit ein Sicherheitsvorfall im Sinne dieser Definition vorliegt, muss der Dienst unverfügbar (Ausfall) oder in qualitativer Hinsicht eingeschränkt verfügbar sein (Einschränkung). Bei der Beurteilung, ob eine Störung erhebliche Auswirkungen hat und somit einen Sicherheitsvorfall darstellt, 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 (§ 4 Abs. 2 Z 1) können die Parameter für beide Fälle konkretisiert werden.

Ein Vorfall (Z 7) stellt alle Ereignisse dar, die tatsächlich nachteilige Auswirkungen auf die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen haben. Dabei werden aber die Erheblichkeitsschwellen eines Sicherheitsvorfalls nicht erreicht.

Im Rahmen des gegenständlichen Gesetzes stellt ein Risiko (Z 8) eine potentielle Gefahrensituation dar, die durch Umstände oder Ereignisse ausgelöst wird, die nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssysteme haben können. Risiken können beispielsweise Schwachstellen in Netz- und Informationssystemen sein.

Ein wesentlicher Dienst (Z 9) wird in einem der in § 2 genannten Sektoren erbracht. Er zeichnet sich durch eine wesentliche Bedeutung für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie aus. Seine Verfügbarkeit muss abhängig von Netz- und Informationssystemen sein, was dann der Fall ist, wenn bei seiner Bereitstellung bzw. Erbringung Netz- und Informationssysteme eingesetzt werden. Zu den verwendeten Begrifflichkeiten ist auf ErläutRV 99 BlgNR 25. GP 13 f (zu § 22 Abs. 1 Z 6 SPG) hinzuweisen.

Betreiber wesentlicher Dienste (Z 8) sind private oder öffentliche Einrichtungen mit Niederlassung in Österreich, die einen wesentlichen Dienst in einem der in § 2 genannten Sektoren erbringen. Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus.

Qualifizierte Stellen (Z 11) sind Einrichtungen mit Niederlassung in Österreich, die zur Überprüfung der Sicherheitsvorkehrungen von Betreibern wesentlicher Dienste geeignet sind. Die Eignung wird vom Bundesminister für Inneres per Bescheid gemäß § 18 Abs. 1 festgestellt.

Digitale Dienste (Z 12) 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 13) sind juristische Personen oder eingetragene Personengesellschaften, die einen solchen digitalen Dienst in Österreich anbieten und eine Hauptniederlassung in Österreich haben oder einen Vertreter (Z 14) in Österreich namhaft gemacht haben. Eine Hauptniederlassung ist im Allgemeinen der Ort, an dem der Anbieter seinen Hauptsitz hat. 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). Für die Feststellung der Eigenschaft als Anbieter digitaler Dienste sind die Mitarbeiterzahlen und finanziellen Schwellenwerte nach Art. 2 Abs. 2 und 3 des Anhangs der Empfehlung 2003/361/EG, ABl. Nr. L 124 vom 20.05.2003 S. 36, bei jener juristischen Person oder eingetragenen Personengesellschaft, die den digitalen Dienst anbietet, maßgeblich. Anbieter digitaler Dienste ohne Hauptniederlassung in der Europäischen Union sind verpflichtet, einen Vertreter 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 15) 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 16) 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 17) 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 18). Der zuständige Bundesminister kann weitere Dienststellen des Bundes durch Verordnung bestimmen. Einrichtungen der öffentlichen Verwaltung umfassen neben Einrichtungen des Bundes auch Einrichtungen der Länder, und zwar die Ämter der Landesregierungen, ebenso mitsamt all ihren Organisationseinheiten und der damit verbundenen technischen Infrastruktur, sowie gegebenenfalls weitere Dienststellen der Länder und Gemeinden (Z 19 iVm § 22 Abs. 5). Die Einrichtungen der öffentlichen Verwaltung sind für die Funktionsfähigkeit des (Rechts-)Staates und daher für das Gemeinwesen und die Daseinsvorsorge der Bevölkerung von hoher Bedeutung.

Die Kooperationsgruppe (Z 20) und das CSIRTs-Netzwerk (Z 21) 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 CSIRTs-Netzwerk für operative Themen zuständig.

Führt ein Sicherheitsvorfall oder führen mehrere Sicherheitsvorfälle 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 22). In einem solchen Fall tritt das Cyberkrisenmanagement (Z 23) 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, des Bundesministeriums für Europa, Integration und Äußeres etwa im Bereich der Cyberdiplomatie oder des Bundesministeriums für Landesverteidigung für die internationale militärische Zusammenarbeit in Angelegenheiten der Sicherheit von Netz- und Informationssystemen.

Die Strategie und der jährliche Bericht zur Sicherheit von Netz- und Informationssystemen (Abs. 1 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 CSIRTs-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 die Sicherheit von Netz- und Informationssystemen (Abs. 2 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 (Abs. 1 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 Störung eines betriebenen wesentlichen Dienstes erhebliche Auswirkungen hat 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 mit Verordnung, im Einvernehmen mit dem Bundesminister für Inneres, Kriterien für diese Parameter festlegen (Abs. 2 Z 1).

Betrifft ein Sicherheitsvorfall mehrere vom Anwendungsbereich dieses Bundesgesetzes umfasste Sektoren, so obliegt es dem Bundeskanzler, die Öffentlichkeit über diesen Vorfall nach Maßgabe des § 10 Abs. 1 zu informieren (Abs. 1 Z 5), wobei eine Anhörung des Betreibers wesentlicher Dienste und eine Interessenabwägung voranzugehen hat (§ 10 Abs. 1). Davon unberührt bleibt die Pflicht gemäß Art. 34 DSGVO, betroffene Personen im Falle der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen.

Dem Bundeskanzler kommt gemäß § 16 Abs. 1 die Aufgabe zu, die vom Anwendungsbereich dieses Bundesgesetzes umfassten Betreiber wesentlicher Dienste zu ermitteln (Abs. 1 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 § 17 Abs. 1 geeignet sind, fest (Abs. 2 Z 3). 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 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 (Abs. 1 Z 7). Dies ist insbesondere dann notwendig, wenn es erforderlich erscheint, die getroffenen Sicherheitsmaßnahmen für diese Netz- und Informationssysteme vor Ort zu überprüfen.

Der Bundeskanzler betreibt das bei ihm eingerichtete GovCERT (Abs. 1 Z 4). Ferner stellt er im Einvernehmen mit dem Bundesminister für Inneres die Eignung von Computer-Notfallteams gemäß § 15 Abs. 3 fest (Abs. 1 Z 8) und veröffentlicht und aktualisiert eine Liste der Computer-Notfallteams nach § 15 Abs. 1 in geeigneter Form, was zB auf einer Website sein kann (Abs. 1 Z 9).

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 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 für operative Zwecke 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 CSIRTs-Netzwerk) geschaffen und betrieben (Abs. 1 Z 1; vgl. auch § 6).

Die Koordinierungsstrukturen OpKoord (§ 3 Z 5 sowie § 7 Abs. 2) und IKDOK (§ 3 Z 4 sowie § 7 Abs. 1) werden vom Bundesminister für Inneres organisatorisch geleitet (Abs. 1 Z 2), wobei dieser gemäß § 7 Abs. 3 ermächtigt ist, das Zusammenwirken der Koordinierungsstrukturen (zB die Einberufung von Sitzungen, die Zusammensetzung, die Entscheidungsfindung) im Rahmen einer Geschäftsordnung näher zu regeln.

Neben der zentralen Anlaufstelle (SPOC) fungiert der Bundesminister für Inneres auch als Meldesammelstelle aller Computer-Notfallteams (§ 14). Dabei werden die von den Computer-Notfallteams eingehenden Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle, die von der Finanzmarktaufsichtsbehörde (FMA) eingehenden Meldungen über schwerwiegende Betriebs- oder Sicherheitsvorfälle (§ 20 Abs. 2) sowie die Meldungen an die Regulierungsbehörde (RTR) gemäß § 16a Abs. 5a TKG 2003 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 (Abs. 1 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. Das sind beispielsweise entsprechende Warnungen oder Handlungsempfehlungen, die im Vorhinein weitergeben werden können, um das Ziel des Gesetzes, ein möglichst hohes Niveau an Netz- und Informationssystemsicherheit, zu erreichen (Abs. 1 Z 4).

Der Bundesminister für Inneres ist gemäß §§ 17 und 21 ermächtigt, die Sicherheitsvorkehrungen, die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste zu treffen haben, zu überprüfen. Auch wird vom Bundesminister für Inneres evaluiert, ob den Meldepflichten gemäß §§ 19 und 21 nachgekommen wird (Abs. 1 Z 5). Die Feststellung und Überprüfung der qualifizierten Stellen obliegt ebenfalls dem Bundesminister für Inneres (Abs. 1 Z 6). In diesem Zusammenhang legt er durch Verordnung im Einvernehmen mit dem Bundeskanzler Erfordernisse und Kriterien sowie das Verfahren zu Feststellung qualifizierter Stellen fest.

Gegebenenfalls kann die Öffentlichkeit über einzelne Sicherheitsvorfälle nach Anhörung des von einem Sicherheitsvorfall betroffenen Betreibers wesentlicher Dienste oder Anbieter digitaler Dienste vom Bundesminister für Inneres unterrichtet werden (Abs. 1 Z 7; § 10 Abs. 1). Dabei ist eine Interessenabwägung vorzunehmen. Davon unberührt bleibt die Pflicht gemäß Art. 34 DSGVO, betroffene Personen im Falle der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen.

Im Fall einer Cyberkrise kommt dem Bundesminister für Inneres darüber hinaus die operative Leitung und Koordination des Cyberkrisenmanagements zu (Abs. 1 Z 8 sowie 6. Abschnitt).

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 Bundeskanzlers im Rahmen seiner Aufgaben oder die direkte Kommunikation der Computer-Notfallteams im Rahmen des CSIRTs-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 an die Mitglieder des IKDOK und Computer-Notfallteams (§ 14) weiterzuleiten, soweit dies zur Erfüllung einer gesetzlich übertragenen Aufgabe des jeweiligen Mitglieds des IKDOK oder Computer-Notfallteams erforderlich ist. Der Empfänger übernimmt infolge die weitere Behandlung. Betrifft ein 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).

Zu § 7 (Koordinierungsstrukturen):

Auf Basis sowie unter Einbindung bestehender operativer Strukturen wird eine neue Struktur zur Koordination auf der operativen Ebene geschaffen. Diese Koordinierungsstruktur besteht aus einem sogenannten „Inneren Kreis“ und einem „Äußeren Kreis“.

Der Innere Kreis der operativen Koordinierungsstruktur (IKDOK) (§ 3 Z 4) setzt sich aus Vertretern jener Behörden, denen nach den Bestimmungen der §§ 4 und 5 Aufgaben zugewiesen werden sowie des

Bundesministeriums für Landesverteidigung und des Bundesministeriums für Europa, Integration und Äußeres (BMEIA) zusammen. Teilnehmende Vertreter sind vor Beginn der Teilnahme einer Sicherheitsüberprüfung für den Zugang zu geheimer Information zu unterziehen sind (§ 3 Z 4). 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. Aus diesem Grund soll das BMEIA auch berechtigt sein, Daten nach Maßgabe von § 9 Abs. 1 und 2 zu verarbeiten. Ferner ist dem BMEIA auch die IKDOK-Plattform bereitzustellen. Die Teilnahme des Bundesministeriums für Landesverteidigung ist im Hinblick auf den Umstand, dass bei der gesamtstaatlich zu beurteilenden NIS der Bundesminister für Landesverteidigung einer der vorrangigen Akteure ist und das Bundesheer die Cyberverteidigung als Teilbereich der militärischen Landesverteidigung wahrnimmt, erforderlich. Die Cyberverteidigung umfasst dabei sämtliche vom Bundesheer im Rahmen der militärischen Landesverteidigung gemäß Art. 79 Abs. 1 B-VG zu setzenden Maßnahmen zur Bewältigung von Sicherheitsvorfällen, die einen Angriff auf die Souveränität der Republik Österreich darstellen. Vor diesem Hintergrund soll er auch berechtigt sein, personenbezogene Daten zum Zweck der Analyse und Bewältigung von Risiken, Vorfällen und Sicherheitsvorfällen nach Maßgabe von § 9 Abs. 3 verarbeiten zu können und neben der IKDOK-Plattform auch am NIS-Meldeanalysesystem teilnehmen zu können. 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 § 13 Abs. 1 beim Bundesminister für Inneres betriebenen IKT-Lösungen 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 § 13 Abs. 2 beim Bundesminister für Inneres sowie gemäß § 14 Abs. 4 beim Bundeskanzler (GovCERT) betriebenen oder von diesen genutzten IKT-Lösungen zur Erkennung von Mustern von Angriffen auf Netz- und Informationssysteme (insbesondere „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 (§ 25) durch Erstellung von anlassbezogenen Lagebildern und technische Expertise zu unterstützen (§ 25 Abs. 3).

Der äußere Kreis namens OpKoord (§ 3 Z 5) dient zur Erörterung eines gesamtheitlichen Lagebilds unter Einbeziehung der Computer-Notfallteams. Bei Bedarf können auch Vertreter anderer Ressorts und anderer Einrichtungen des Bundes sowie Vertreter von Einrichtungen der Länder eingebunden werden, wenn deren gesetzliche Wirkungsbereiche betroffen sind, sowie Vertreter aus Wirtschaft (insbesondere Betreiber wesentlicher Dienste und Anbieter digitaler Dienste) 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 (Datenverarbeitung):

Im 3. Abschnitt (§ 9 bis § 13) werden datenschutzrechtliche Bestimmungen zur Verarbeitung von personenbezogenen Daten im Sinne des Art. 4 Z 2 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) und § 36 Datenschutzgesetz (DSG) geregelt. Bundeskanzler, Bundesminister für Inneres, Bundesminister für Landesverteidigung und Bundesminister für Europa, Integration und Äußeres, aber auch die Computer-Notfallteams sollen gemäß § 9 Abs. 1 explizit ermächtigt sein, zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen bei der Wahrnehmung ihrer Aufgaben nach diesem Bundesgesetz und zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit die erforderlichen personenbezogenen Daten zu verarbeiten. Beim Verarbeiten von personenbezogenen Daten sind jedenfalls die Grundsätze für die Verarbeitung personenbezogener Daten, wie insbesondere der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO), der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) und der Verhältnismäßigkeitsgrundsatz (§ 1 Abs. 2 DSG) zu beachten. Abs. 1 ermächtigt die oben genannten Verantwortlichen zudem, die Daten einander sowie den Mitgliedern der OpKoord übermitteln zu dürfen. Da die oben genannten Verantwortlichen ständig in der OpKoord vertreten sind, werden damit Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen des Bundes und der öffentlichen Verwaltung gemeint, die an der OpKoord anlassbezogen (also im Falle der Betroffenheit ihres Wirkungsbereiches von einem Risiko, Vorfall oder Sicherheitsvorfall) teilnehmen.

Insbesondere unter Berücksichtigung der Prinzipien der Zweckbindung und der Verhältnismäßigkeit verfolgt § 9 den Ansatz, dass sich der Kreis der zur Verarbeitung Berechtigten mit der zunehmenden Datenmenge und dem zunehmenden Detaillierungsgrad der Daten reduziert, bzw. umso weniger zur Verarbeitung berechtigt sind, je größer die Menge und je höher der Detaillierungsgrad der Daten ist.

Bei den oben genannten personenbezogenen Daten handelt es sich zum einen um Daten von Teilnehmern und ihren Organisationseinheiten (Abs. 2 Z 1) zu organisatorischen Zwecken (zB E-Mail-Adressen), andererseits um Daten von Personen, die in Zusammenhang mit Risiken, Vorfällen und Sicherheitsvorfällen stehen (Abs. 2 Z 2). Letztere Daten werden zur Erörterung und Aktualisierung des Lagebildes, zur Erörterung von Erkenntnissen, die aus IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen (§ 13 Abs. 1 und 2) gewonnen wurden, und zur Unterstützung des Koordinationsausschusses verarbeitet. Dabei kann es sich zB um Daten handeln, die zur Beschreibung von Ursachen und Entwicklungstendenzen diverser Cyberangriffsszenarien erforderlich sind. Des Weiteren dürfen Daten von Personen, die an einem Geschäftsfall mitwirken oder davon betroffen sind, verarbeitet werden (Abs. 2 Z 2). Hierbei sind Daten, die beispielsweise bei der Verwendung des ELAK anfallen, gemeint.

In Abs. 3 werden der Bundeskanzler, der Bundesminister für Inneres und der Bundesminister für Landesverteidigung als jene Behörden, die Informationen im Zusammenhang mit Risiken, Vorfällen und Sicherheitsvorfällen auf einer technischeren Ebene zum Zwecke der Bewältigung analysieren können sollen, ermächtigt, über zusätzlich zu den bisher genannten Datenkategorien weitere personenbezogene Daten zu verarbeiten und einander zu übermitteln. Konkret sind Kontakt- und Identitätsdaten sowie technische Daten des Einmelders und der Kontaktperson hiervon erfasst. Darunter fallen insbesondere

jene personenbezogenen Daten, die für die Entgegennahme von Meldungen über Risiken, Vorfälle und Sicherheitsvorfälle relevant sind, wie Daten des Einmelders, der Kontaktperson (Abs. 3 Z 1). Das sind insbesondere Namen, Anschriften, Telefonnummern und E-Mail-Adressen. Überdies sollen Kontakt- und Identitätsdaten sowie technische Daten von Personen, die mit einer Meldung zu einem Risiko, Vorfall oder Sicherheitsvorfall in Zusammenhang stehen, verarbeitet und einander übermittelt werden dürfen (Abs. 3 Z 2). Dazu zählen insbesondere Daten über Opfer und Angreifer, wie zB die IP-Adresse eines Angreifers oder die technischen Daten eines gehackten Servers, aber auch sonstige, den Sachverhalt spezifizierende technische Daten. So sind weitere Beispiele für Daten dieser Kategorie, deren Analyse erforderlich ist, um Risiken, Vorfälle und Sicherheitsvorfälle zu bewältigen, Daten, welche die Identifikation einer Einrichtung ermöglichen, von der eine Gefahr oder sogar ein Angriff ausgeht. 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.

In Abs. 4 werden Datenkategorien bestimmt, die über die in Abs. 2 und 3 genannten hinausgehen und die der Bundeskanzler und der Bundesminister für Inneres zur Erfüllung ihrer Aufgaben nach §§ 4 und 5 verarbeiten und einander übermitteln dürfen. Es handelt sich dabei um Daten, die für den unmittelbaren Vollzug des Bundesgesetzes erforderlich sind und deren Verarbeitung daher nur für den Bundeskanzler und den Bundesminister für Inneres erforderlich ist. So hat der Bundeskanzler insbesondere jene personenbezogenen Daten zu verarbeiten, die für die Ermittlung der Betreiber wesentlicher Dienste erforderlich sind. Solche Daten können Name, Firmenname oder Adresse der jeweils betroffenen Einrichtung sein, die einen wesentlichen Dienst betreibt. Darüber hinaus werden auch jene personenbezogenen Daten verarbeitet, die im Zuge der Bekanntgabe einer Kontaktstelle im Sinne des § 16 Abs. 3 übermittelt werden. Dabei handelt es sich zB um Name, E-Mail-Adresse und Telefonnummer der als Kontaktstelle bzw. Kontaktperson benannten Personen. Überdies ist es erforderlich, die Erreichbarkeitsdaten der zuständigen Behörden anderer Mitgliedstaaten im Sinne des Art. 8 Abs. 1 NIS-RL sowie Verteilerlisten von EU-weiten, internationalen und nationalen Gremien für die Sicherheit von Netz- und Informationssystemen verarbeitet werden dürfen.

Zusätzlich zu den in Abs. 2, 3 und 4 genannten Datenkategorien darf der Bundesminister für Inneres zur Erfüllung seiner Aufgaben nach § 5 Z 4 bis 6 weitere Datenkategorien verarbeiten, deren Verarbeitung alleinig zur Aufgabenerfüllung des Bundesministers für Inneres erforderlich ist. Daten dieser Kategorien umfassen zB personenbezogene Daten, die im Zusammenhang mit aufgedeckten Sicherheitsmängel, Ergebnissen der Einschau in die Netz- und Informationssysteme und dazugehörige Unterlagen (zB Audit-Reports) sowie mögliche ausgesprochene Empfehlungen ermittelt werden, weiters bestimmte Daten von qualifizierten Stellen und deren Mitarbeitern.

Überdies ist der Bundesminister für Inneres nach Abs. 5 Z 3 ermächtigt, die Daten von Personen zu verarbeiten, die im Zuge des Betriebs bzw. der Nutzung von IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen (§ 13 Abs. 1 und 2) ermittelt werden. Der tatsächliche Umfang der Datenverarbeitung richtet sich dabei nach der Vereinbarung des Bundesministers für Inneres mit der betroffenen Einrichtung (siehe dazu unten bei § 13). Bei den Daten, die bei solchen IKT-Lösungen ermittelt werden, zählen insbesondere technische personenbezogene Daten, wie IP-Adressen der zugreifenden Systeme oder 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).

In Abs. 6 wird vorgesehen, dass jede Abfrage, Übermittlung und Änderung personenbezogener Daten zur besseren Nachvollziehbarkeit und Überprüfbarkeit revisionssicher zu protokollieren ist, wobei die Protokollierungsdauer drei Jahre betragen soll. Bei der Protokollierung der verarbeiteten Daten soll den gängigen IT-Anwendungen entsprechend dem Stand der Technik eine Zuordnung von Abfragen, Übermittlungen oder Änderungen zu den die Aktion setzenden Personen erfolgen.

Abs. 7 sieht vor, dass das Recht auf Löschung und auf Widerspruch gemäß DSGVO oder § 45 DSG insoweit beschränkt wird, als durch Gesetz oder Verordnung eine Aufbewahrungspflicht oder Archivierung vorgesehen ist oder der Löschung das öffentliche Interesse der Gewährleistung eines hohen Niveaus von Netz- und Informationssystemsicherheit entgegensteht und die betroffene Person nicht

Gründe nachweisen kann, die sich aus ihrer besonderen Situation ergeben und welche die Ziele der Beschränkung des Rechtes überwiegen. Der zuständige Datenschutzbeauftragte ist über die Vornahme und das Ergebnis einer solchen Abwägung in Kenntnis zu setzen.

Eine Beschränkung des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO oder § 45 DSG wird in Bezug auf integrierte Datenverarbeitungssysteme für die Dauer einer Überprüfung der von der betroffenen Person bestrittenen Richtigkeit ihrer personenbezogenen Daten sowie für den Zeitraum, in dem die betroffene Person ihr Recht auf Widerspruch geltend gemacht hat und noch nicht feststeht, ob die berechtigten Gründe des datenschutzrechtlich Verantwortlichen gegenüber denen der betroffenen Person überwiegen, wird in Abs. 8 normiert.

Abs. 9 bestimmt, dass die datenschutzrechtlichen Pflichten, wie sie sich aus der DSGVO und dem 3. Hauptstück DSG ergeben, also zB die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten und die Ergreifung von Maßnahmen zur Sicherheit der Verarbeitung, von jedem datenschutzrechtlichen Verantwortlichen hinsichtlich jener personenbezogenen Daten, die im Zusammenhang mit den von ihm geführten Verfahren oder den von ihm gesetzten Maßnahmen verarbeitet, übermittelt oder weiterverarbeitet werden, selbstständig wahrzunehmen sind.

Zu § 10 (Datenübermittlung):

In Abs. 1 wird in Umsetzung von Art. 14 Abs. 6 und Art. 16 Abs. 7 NIS-RL geregelt, dass die Öffentlichkeit in bestimmten Fällen von einem Sicherheitsvorfall unterrichtet werden kann. Dabei dürfen Daten nach § 9 Abs. 3 Z 2 übermittelt werden. Der Bundeskanzler kann die Öffentlichkeit über einen Sicherheitsvorfall bei Betreibern wesentlicher Dienste, der mehrere der in § 2 genannten Sektoren betrifft, unterrichten, wohingegen der Bundesminister für Inneres die Öffentlichkeit über einzelne Sicherheitsvorfälle oder über Sicherheitsvorfälle bei Anbietern digitaler Dienste unterrichtet. Von Anbietern digitaler Dienste kann der Bundesminister für Inneres verlangen, dass dieser die Unterrichtung der Öffentlichkeit selbst zu vornimmt. Vor Unterrichtung ist der betroffene Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste anzuhören und eine Interessenabwägung vorzunehmen. Bei der Interessenabwägung sind die insbesondere die Auswirkungen auf die datenschutzrechtlichen Betroffenen zu berücksichtigen. Die Unterrichtung der Öffentlichkeit muss für die Sensibilisierung dieser zur Verhütung oder zur Bewältigung von Sicherheitsvorfällen erforderlich sein. Eine Offenlegung des Sicherheitsvorfalls kann aber auch auf sonstige Weise im öffentlichen Interesse liegen. Von Abs. 1 unberührt bleibt die Pflicht des Verantwortlichen gemäß Art. 34 DSGVO, betroffene Personen im Falle der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen.

Nach Abs. 2 sind der Bundeskanzler, der Bundesminister für Inneres, der Bundesminister für Landesverteidigung und der Bundesminister für Europa, Integration und Äußeres berechtigt, Daten, die sie aufgrund der Wahrnehmung ihrer Aufgaben nach diesem Bundesgesetz ermittelt haben, an militärische Organe und Behörden für Zwecke der militärischen Landesverteidigung gemäß Art. 79 Abs. 1 B-VG, an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege sowie an inländische Behörden, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist, zu übermitteln. Der Bundesminister für Inneres kann darüber hinaus zur Vorbeugung von Sicherheitsvorfällen (§ 5 Abs. 1 Z 4) Daten von Personen, die mit Risiken, Vorfällen und Sicherheitsvorfällen in Zusammenhang stehen (§ 9 Abs. 2 Z 2 und Abs. 3 Z 2), an Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und an sonstige Einrichtungen übermitteln, wenn diese von einem Risiko, Vorfall oder Sicherheitsvorfall betroffen sind (Abs. 3). Zudem darf der Bundesminister für Inneres die von ihm gemäß § 9 Abs. 2 bis 5 verarbeiteten Daten an bestimmte ausländische Sicherheitsbehörden und Sicherheitsorganisationen (§ 2 Abs. 2 und 3 Polizeikooperationsgesetz) sowie Organe der Europäischen Union oder der Vereinten Nationen in Einklang mit den Bestimmungen über die internationale polizeiliche Amtshilfe übermitteln (Abs. 4).

In Umsetzung von Art. 14 Abs. 5 und Art. 16 Abs. 6 hat der Bundesminister für Inneres die zentralen Anlaufstellen der anderen Mitgliedstaaten zu unterrichten, wenn ein Sicherheitsvorfall einen grenzüberschreitenden Bezug hat (§§ 19 Abs. 5, 21 Abs. 3, 22 Abs. 4), etwa, weil der Betreiber wesentlicher Dienste seinen Dienst in mehreren EU-Mitgliedstaaten erbringt. Dabei hat der Bundesminister für Inneres eine Interessenabwägung vorzunehmen, die die wirtschaftlichen Interessen der betroffenen Einrichtung sowie die Vertraulichkeit der in der Meldung bereitgestellten Informationen berücksichtigt. Abs. 5 berechtigt den Bundesminister für Inneres, bei der Wahrnehmung dieser Aufgabe die erforderlichen personenbezogenen Daten an die zentralen Anlaufstellen in den von einem Sicherheitsvorfall betroffenen Mitgliedstaaten zu übermitteln.

Um sicherzustellen, dass die Computer-Notfallteams ihre Aufgaben gemäß § 14 Abs. 2 gegenüber den Betreibern wesentlicher Dienste und Anbietern digitaler Dienste wahrnehmen können, ist der

Bundeskanzler berechtigt, deren personenbezogenen Kontakt- und Identitätsdaten an die Computer-Notfallteams nach Maßgabe der Erforderlichkeit zu übermitteln.

Der Bundeskanzler darf auch die Identitätsnamen der Betreiber wesentlicher Dienste an die Länder und Aufsichtsbehörden des Sektors übermitteln.

Zu § 11 (NIS-Meldeanalysesystem):

In § 11 wird die Einrichtung des „NIS-Meldeanalysesystems“ vorgesehen. Bei diesem System handelt es sich um IKT-Lösungen und IT-Verfahren, in welchen Inhalte von Meldungen über Risiken, Vorfälle und Sicherheitsvorfälle sowie Erkenntnissen, die aus dem Betrieb von IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen gemäß (§ 13 Abs. 1 und 2) gewonnen wurden, verarbeitet werden. Hinsichtlich der im Rahmen des NIS-Meldeanalysesystems verarbeiteten Daten kann diesbezüglich auf § 9 Abs. 2 Z 2 und Abs. 3 Z 1 und 2 verwiesen werden. Der Zweck des Betriebs des NIS-Meldeanalysesystems liegt in der Bewertung von Risiken, Vorfällen und Sicherheitsvorfällen für Netz- und Informationssysteme und der Unterstützung der Erstellung eines Lagebilds mittels strategischer oder operativer Analyse. Die 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.

Das NIS-Meldeanalysesystem soll vom Bundesminister für Inneres technisch betrieben und dem Bundeskanzler und dem Bundesminister für Landesverteidigung bereitgestellt werden. Es handelt sich dabei um ein Dateisystem (Art. 4 Z 6 DSGVO), für welches der Bundesminister für Inneres, der Bundeskanzler und der Bundesminister für Landesverteidigung gemeinsam datenschutzrechtliche Verantwortliche gemäß Art. 4 Z 7 in Verbindung mit Art. 26 DSGVO bzw. § 36 DSG (Abs. 2). Da Art. 26 DSGVO eine Öffnungsklausel enthält, sollen nähere Regelungen zur Aufteilung der Pflichten als gemeinsam datenschutzrechtliche Verantwortliche durch eine Verordnung des Bundeskanzlers, die er im Einvernehmen mit dem Bundesminister für Inneres und dem Bundesminister für Landesverteidigung zu erlassen hat, erfolgen (Abs. 3).

Zu § 12 (IKDOK-Plattform):

In § 12 wird die Möglichkeit vorgesehen, dass der Bundesminister für Inneres eine IKT-Lösung betreiben kann, die der Organisation des IKDOK und der Wahrnehmung der Aufgaben gemäß § 7 Abs. 1 dient. Im Falle des Betriebs einer solchen IKT-Lösung ist diese den im IKDOK vertretenen Ressorts bereitzustellen (Abs. 1). Der Bundesminister für Inneres, der Bundeskanzler, der Bundesminister für Landesverteidigung und der Bundesminister für Europa, Integration und Äußeres sind im Falle des Betriebs gemeinsam datenschutzrechtliche Verantwortliche gemäß Art. 4 Z 7 in Verbindung mit Art. 26 DSGVO bzw. § 47 DSG. Hinsichtlich der in der IKDOK-Plattform verarbeiteten Datenkategorien kann auf § 9 Abs. 2 Z 1 bis 3 verwiesen werden. Die sich aus der DSGVO ergebenden Pflichten sind grundsätzlich vom Bundesminister für Inneres wahrzunehmen (Abs. 2). Hinsichtlich der Betroffenenrechte gemäß den Bestimmungen des Kapitels 3 DSGVO oder §§ 42 bis 45 DSG regelt Abs. 3 abweichend von Abs. 2, dass jeder der gemeinsam datenschutzrechtlichen Verantwortlichen bezüglich der von ihm erhobenen und verarbeiteten Daten die Pflichten in Zusammenhang mit den Rechten betroffener Personen selbstständig wahrzunehmen hat. Jedenfalls haben die gemeinsam datenschutzrechtlichen Verantwortlichen einander unverzüglich mitzuteilen, wenn eine betroffene Person ihre Rechte geltend macht.

Zu § 13 (Betrieb von IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen):

Durch Abs. 1 und 2 wird vorgesehen, dass der Bundesminister für Inneres bestimmte IKT-Lösungen betreiben oder nutzen darf. Unter einer IKT-Lösung wird hierbei allgemein die Gesamtheit aller informationstechnologischen Maßnahmen und technischen Mittel, die erforderlich sind, um Nutzern Funktionen und Informationen automationsunterstützt zur Verfügung zu stellen, verstanden.

Gemäß Abs. 1 ist 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, als Ergänzung der vorhandenen proaktiven Sicherheitsmaßnahmen IKT-Lösungen 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 Frühwarnsystem wird der Betrieb der eingesetzten technischen Einrichtungen durch den Bundesminister für Inneres für den zivilen Bereich durchgeführt.

Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie Einrichtungen des Bundes und der Länder sollen freiwillig am Betrieb teilnehmen können, wobei insbesondere die Teilnahme mittels Vertrag geregelt wird. Gegenstand eines solchen Vertrages können beispielsweise Teilnahmemodalitäten, Austauschmodalitäten von Erkenntnissen, die Örtlichkeit der Anbringung der technischen Einrichtung, technische Spezifikationen (wie etwa Schnittstellen), Regelungen zur Informations- und Datensicherheit oder nähere Bestimmungen zur Datenverarbeitung sein. Dem Teilnehmer soll hierbei die Möglichkeit gegeben werden, zu bestimmen, 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 IKT-Lösungen sowie deren jährliche Wartungs- bzw. Instandhaltungskosten zu berücksichtigen.

Der Betrieb der IKT-Lösungen durch den Bundesminister für Inneres umfasst neben deren Instandhaltung (das heißt Installation, Sicherstellung der Funktionalität, Wartung etc.) und Management auch die Führung einer „Threat Intelligence“ (TI), die als zentrale Datenbank Informationen zu aktuellen Bedrohungen aufbereitet und die IKT-Lösungen mit jenen Erkennungsmustern (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 IKT-Lösungen 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 IKT-Lösungen möglich, Unregelmäßigkeiten zu erkennen (IOC-basiertes Frühwarnsystem). Ob es sich bei einer Unregelmäßigkeit auch tatsächlich um eine Störung handelt, die eine Alarmierung und entsprechende Behandlung nach sich zieht, kann erst nach eingehender Analyse und Bewertung entschieden werden, wofür primär der jeweilige Teilnehmer bzw. dessen „Security Operation Center“ (SOC, eine IT-Sicherheitsabteilung, die durch den Teilnehmer selbst oder einen externen Dienstleister bereitgestellt wird) zuständig ist. Zudem bietet § 14 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 und der Länder das GovCERT (§ 14 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, IKT-Lösungen, wie zB „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. IKT-Lösungen wie zB „Sinkholes“ können dadurch genutzt werden, indem der Bundesminister für Inneres solche nicht unbedingt von sich aus physisch betreibt, sondern auch nur auf den Datenverkehr von bei Dritten installierten Sinkholes nach deren auf freiwilliger Basis erteilten Einwilligung Zugriff bekommt.

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 (§ 9 Abs. 5).

Neben dem Bundesminister für Inneres kommt gemäß § 13 Abs. 2 zweiter Satz auch dem GovCERT innerhalb seines Zuständigkeitsbereichs die Befugnis zu, solche IKT-Lösungen zu betreiben oder zu nutzen, um zu wichtigen Informationen der aktuellen Gefährdungslage zu gelangen.

Zu § 14 (Aufgaben und Zweck der Computer-Notfallteams):

Um die Prävention, Erkennung, Reaktion und Folgenminderung bei Risiken, Vorfällen und Sicherheitsvorfällen gewährleisten zu können, ist es wichtig, über gut funktionierende Computer-Notfallteams bzw. CSIRTs – Computer Security Incident Response Teams (auch: CERTs – Computer Emergency Response Teams) – zu verfügen, die die grundlegenden Anforderungen im Hinblick auf die Gewährleistung wirksamer und kompatibler Fähigkeiten zur Bewältigung von Risiken, Vorfällen 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 CSIRTs-Netzwerk auch an nationalen sowie anderen internationalen Kooperationsnetzen. In Umsetzung von Art. 9 und des Anhangs I der NIS-RL werden daher in den §§ 14 und 15 die Aufgaben und Anforderungen für Computer-Notfallteams geregelt.

Zur Unterstützung der Betreiber wesentlicher Dienste können sektorenspezifische Computer-Notfallteams eingerichtet werden (Abs. 3). 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 Vorfällen und Sicherheitsvorfällen bieten. Pro Sektor kann es jedenfalls nur ein sektorenspezifisches Computer-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. Sollte auch kein nationales Computer-Notfallteam eingerichtet sein (weil beispielsweise dessen Eignung und

Ermächtigung zu widerrufen war), so übernimmt das GovCERT dessen Aufgaben in Bezug auf das Meldewesen.

Zu den Hauptaufgaben der Computer-Notfallteams zählt die Entgegennahme von Meldungen über Risiken, Vorfälle und Sicherheitsvorfälle 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 (§ 19) und Anbieter digitaler Dienste (§ 21 Abs. 2) auslösen, sowie Risiken und Vorfälle, die freiwillig gemeldet werden (§ 23).

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, Vorfällen und Sicherheitsvorfällen im Bereich der IT und die Ausgabe von Warnungen oder Alarmmeldungen, wenn Informationen über Risiken, Vorfälle oder Sicherheitsvorfälle bekannt werden. Die Informationen zu Risiken, Vorfällen 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 etwa 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 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 CSIRTs-Netzwerk und nehmen an der OpKoord teil (Abs. 2 Z 6).

Abs. 3 ermöglicht es Betreibern wesentlicher Dienste zudem, sektorenspezifische Computer-Notfallteams damit zu beauftragen, die Analyse und Bewertung von Unregelmäßigkeiten, die durch eine bei diesem Betreiber wesentlicher Dienste eingerichteten IKT-Lösung gemäß § 13 Abs. 1 erkannt wurden, vorzunehmen. Anbieter digitaler Dienste können das nationale Computer-Notfallteam, Einrichtungen der öffentlichen Verwaltung das GovCERT damit beauftragen.

Für die Einrichtungen der öffentlichen Verwaltung 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, welche neben der Bundes- und der Landesebene auch die kommunale bzw. Gemeindeebene einschließt. Zusätzlich zu den Aufgaben eines Computer-Notfallteams kann das GovCERT IKT-Lösungen betreiben, die Muster von Angriffen auf Netz- und Informationssysteme erkennen lassen (zB „Honeypots“ und „Sinkholes“).

Computer-Notfallteams sind zur Beteiligung am europäischen CSIRTs-Netzwerk berechtigt und können sich zB auf E-Mail-Verteilerlisten eintragen lassen oder in grenzüberschreitenden Arbeitsgruppen mitwirken (Abs. 2 Z 6 zweiter Fall).

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).

Entsprechend den anderen datenschutzrechtlichen Bestimmungen werden in Abs. 7 und 8 auch für Computer-Notfallteams explizite datenschutzrechtliche Grundlagen geschaffen. Im diesem Kontext dieser Bestimmungen ist auch 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 § 15 (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 CSIRTs, 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 § 16 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). Zudem haben Computer-Notfallteams in Wahrnehmung ihrer Aufgaben gemäß § 14 Abs. 2 Z 1 und 2 sichere Kommunikationskanäle, die sie vorab mit dem Bundesminister für Inneres abgestimmt haben, zu verwenden.

Auch das gemäß § 14 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 iVm § 4 Abs. 1 Z 8). 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.

Die Kontakt-und Identitätsdaten der Computer-Notfallteams sind vom Bundeskanzler in geeigneter Form (zB auf einer Website) zu veröffentlichen (siehe auch § 4 Abs. 1 Z 9).

Zu § 16 (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 in einem der in § 2 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.

Zu den in § 2 genannten Sektoren kann der Bundeskanzler mittels Verordnung nähere Regelungen treffen (Abs. 2 iVm § 4 Abs. 2 Z 2) (siehe auch oben bei § 2). In dieser Verordnung werden insbesondere die Teilsektoren, Bereiche und die darin erbrachten wesentlichen Dienste genannt. Bei der Bewertung, ob einem Dienst eine wesentliche Bedeutung für die in § 3 Z 9 genannten Rechtsgüter zukommt, sind die in der NIS-RL vorgegebenen sektorenübergreifenden Faktoren, mit denen bestimmt wird, ob eine Störung einen potenziellen Sicherheitsvorfall bewirken würde und diesem daher eine wesentliche Bedeutung zukommt, zu berücksichtigen. Es können zudem konkrete sektorenspezifische Faktoren berücksichtigt werden. Beispielsweise könnten bei Energieversorgern die Menge oder der Anteil der landesweit produzierten Energie gehören, beim Luftverkehr, einschließlich Flughäfen und Luftfahrtunternehmen, Schienenverkehr und bei Seehäfen der Anteil des landesweiten Verkehrsvolumens und die Anzahl der Passagiere oder der Frachtdienste pro Jahr, bei Bank- oder Finanzmarktinfrastrukturen deren Systemrelevanz aufgrund der Bilanzsumme, bei der Wassergewinnung, -aufbereitung und -versorgung die Wassermenge, die Anzahl und die Arten der belieferten Verbraucher, einschließlich beispielsweise Krankenhäuser, öffentliche Dienstleister oder Einzelpersonen, herangezogen werden (vgl. ErwGr 28 NIS-RL). Demgemäß können die sektorenübergreifenden und sektorenspezifischen Faktoren durch Schwellenwert ausgedrückt werden.

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 genannten Sektoren und die Faktoren gemäß Abs. 2, die zur Ermittlung der Betreiber wesentlicher Dienste herangezogen werden sollen, näher konkretisiert.

Im Zusammenhang mit der Ermittlung von Betreibern wesentlicher Dienste kommen dem Bundeskanzler zentrale Aufgaben zu (Abs. 4 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 nachträglich weg, die für die Ermittlung eines Betreibers wesentlicher Dienste maßgeblich waren, oder stellt sich heraus, dass sie von vornherein nicht vorgelegen sind, so ist der Bescheid (ebenfalls mit 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 und die von dieser erarbeiteten Leitlinien über den Konsultationsprozess heranziehen.

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 § 17 (Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste):

In Umsetzung des Art. 14 Abs. 1 NIS-RL wird den Betreibern wesentlicher Dienste vorgeschrieben, Sicherheitsvorkehrungen technischer und organisatorischer Art zu treffen. Diese sollen in Hinblick auf

die betriebenen wesentlichen Dienste dazu dienen, die Netz- und Informationssystemsicherheit (NIS) zu gewährleisten (Abs. 1). Betreiber wesentlicher Dienste haben demnach die Fähigkeit zu besitzen, Sicherheitsvorfällen (§ 3 Z 6) vorzubeugen, diese zu erkennen, abzuwehren und zu beseitigen.

Sicherheitsvorkehrungen nach Abs. 1 haben geeignet und verhältnismäßig zu sein, den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein. Dadurch soll insbesondere der im Bereich der Netz- und Informationssicherheit praktizierte „risikobasierte Ansatz“ abgebildet werden. Jene Sicherheitsvorkehrungen, die jedenfalls zur Gewährleistung der Anforderungen nach Abs. 1 geeignet sind, können 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 (§ 4 Abs. 2 Z 2).

Betreiber wesentlicher Dienste können gemeinsam mit ihren Sektorenverbänden eigene Sicherheitsvorkehrungen vorschlagen, mit denen die Anforderungen des Abs. 1 gewährleistet werden (Abs. 2) und anschließend beantragen, dass die Eignung dieser Sicherheitsvorkehrungen festgestellt wird. Diese Möglichkeit besteht auch für einzelne Teilsektoren und Bereiche. 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 wird die Aufstellung der vorhandenen Sicherheitsvorkehrungen mittels eines Nachweises von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen einschließlich aufgedeckter Sicherheitsmängel dem Bundesminister für Inneres übermittelt.

Der Bundesminister für Inneres hat die Befugnis, Einschau in die notwendigen Unterlagen zu nehmen. Diese Unterlagen können auch allenfalls bereits vorhandene Nachweise über die Aufstellung der vorhandenen Sicherheitsvorkehrungen darstellen. Bei Bedarf kann der Bundesminister für Inneres auch in jene Netz- und Informationssysteme, die für die Bereitstellung des wesentlichen Dienstes genutzt werden, Einschau nehmen und zu diesem Zweck – nach Verständigung – die Örtlichkeiten, in denen diese Netz- und Informationssysteme gelegen sind, betreten. Die Ausübung dieser Kontrollbefugnisse hat im Einklang mit den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit zu erfolgen. Rechte der betroffenen Einrichtung, wie zB Geschäfts- und Betriebsgeheimnisse, und Rechte Dritter, wie zB Datenschutzrechte, sowie auch der Betrieb, also etwa der Betriebsablauf und Sicherheitsregeln (wie zB Safetyanforderungen), sind möglichst zu schonen bzw. zu beachten.

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.

Zu § 18 (Qualifizierte Stellen):

Durch Verordnung werden die Erfordernisse, die eine qualifizierte Stelle (§ 3 Z 11) zu erfüllen hat, vom Bundesminister für Inneres im Einvernehmen mit dem Bundeskanzler festgelegt (§ 5 Abs. 2 Z 1). Darüber hinaus können im Rahmen der Verordnung besondere Kriterien, deren Erfüllung eine Einrichtung ohne vorherige Bescheiderlassung jedenfalls dazu berechtigt, als qualifizierte Stelle aufzutreten, sowie das Verfahren zur Feststellung der Eignung geregelt werden.

Einrichtungen, 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 (Abs. 1).

Um zu gewährleisten, dass die 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. 3). An dieser Stelle ist auf die Einschaumodalitäten bei Betreibern wesentlicher Dienste entsprechend zu verweisen (§ 17 Abs. 4).

Werden die durch die Verordnung festgelegten Erfordernisse oder Kriterien von der jeweiligen qualifizierten Stelle nicht mehr erfüllt, weist der Bundesminister für Inneres die qualifizierte Stelle unter Setzung einer angemessenen Frist an, die Erfordernisse oder Kriterien wieder zu erfüllen. Tritt dies nicht ein, wird der Bescheid, der nach Abs. 1 ergangen ist bzw. der Status „qualifizierte Stelle“, vom Bundesminister für Inneres widerrufen

Zu § 19 (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, die den wesentlichen Dienst betreffen, 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, falls ein solches vorhanden ist und der betroffene Betreiber wesentlicher Dienste dieses unterstützt, andernfalls das nationale Computer-Notfallteam, sofern ein solches eingerichtet ist, ansonsten das GovCERT (Abs. 2). Das jeweilige Computer-Notfallteam, das eine solche Meldung erhält, hat diese unverzüglich an den Bundesminister für Inneres weiterzuleiten. Die eingehenden Meldungen werden vom Bundesminister für Inneres insbesondere 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 relevanten Angaben und Informationen zum Sicherheitsvorfall zu enthalten, die notwendig sind, um die Lage der betroffenen Einrichtung, die 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 in Form von Nachmeldungen mitzuteilen, wobei schlussendlich eine Abschlussmeldung erfolgen soll. 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.

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 unberührt.

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).

Durch Verordnung können nähere Kriterien zu den Parametern des § 3 Z 6 lit. a bis d („Meldeschwellwerte“) festgelegt werden (§ 4 Abs. 2 Z 1).

Zu § 20 (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. Solche Vorschriften zu Sicherheitsvorkehrungen und zur Meldepflicht, die zumindest ein gleichwertiges Sicherheitsniveau für Netz- und Informationssysteme gewährleisten, werden in einer Verordnung durch den Bundeskanzler im Einvernehmen mit dem Bundesminister für Inneres festgelegt. 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 § 20. Trotz Anwendbarkeit von Lex-specialis-Bestimmungen wird eine Einrichtung als Betreiber wesentlicher Dienste gemäß § 16 ermittelt, um solchen Einrichtungen insbesondere die Einrichtung eines sektorenspezifischen Computer-Notfallteams sowie die Teilnahme an einer IKT-Lösung nach § 13 Abs. 1 zu ermöglichen. Die Verpflichtung zur Nennung einer Kontaktstelle (§ 16 Abs. 3) bleibt von § 20

unberührt. Die Meldepflichten nach diesem Bundesgesetz bleiben aufrecht, wenn sich bestehende Vorschriften nicht auf die Sicherheit der Netz- und Informationssysteme oder die Meldung von Sicherheitsvorfällen beziehen oder deren Anforderungen in ihrer Wirkung den in der NIS-RL enthaltenen Pflichten nicht mindestens gleichwertig sind, wie zB Meldungen an die Datenschutzbehörde nach Art. 33 DSGVO im Falle einer Verletzung des Schutzes personenbezogener Daten.

Obwohl Betreiber wesentlicher Dienste, für die Lex-specialis-Bestimmungen im Sinne des Abs. 1 zur Meldepflicht anwendbar sind, Sicherheitsvorfälle nicht gemäß § 19 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 erörtert werden soll, auch Informationen über schwerwiegende Betriebs- oder Sicherheitsvorfälle bei Betreibern wesentlicher Dienste aus dem Sektor Bankwesen enthält.

Zu § 21 (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 mit vernünftigem Aufwand feststellbaren 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 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. § 17 Abs. 3) sowie der Verzicht auf eine Verordnungsermächtigung zur Festlegung der Sicherheitsvorkehrungen (vgl. § 4 Abs. 2 Z 3), wie dies bei Betreibern wesentlicher Dienste vorgesehen ist, begründen sich unmittelbar aus der NIS-RL (vgl. Art. 16 Abs. 10 und Art. 17 Abs. 1 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 grundsätzlich 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) nachweisliche

Umstände zur Kenntnis gelangen, dass ein Anbieter digitaler Dienste die Anforderungen dieses Bundesgesetzes nicht erfüllt, vor allem dann, wenn sich ein Sicherheitsvorfall ereignet hat (Abs. 4).

Zu § 22 (Sicherheitsvorkehrungen und Meldepflicht für Einrichtungen der öffentlichen Verwaltung):

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 der öffentlichen Verwaltung (§ 3 Z 19) 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 und eines Landes ein Sicherheitsvorfall (§ 3 Z 6) vor, so ist dieser grundsätzlich an das dafür zuständige GovCERT zu melden (Abs. 2). Risiken und Vorfälle 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, die im IKDOK vertreten 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 oder eines Landes einen grenzüberschreitenden Bezug, so sind die zentralen Anlaufstellen in den anderen Mitgliedstaaten im Wege der zentralen Anlaufstelle (SPOC) über diesen Sicherheitsvorfall zu informieren (Abs. 4).

Zu § 23 (Freiwillige Meldungen):

Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung sollen die Möglichkeit haben, an das zuständige Computer-Notfallteam Risiken und Vorfälle melden zu können. Einrichtungen, die nicht als Betreiber wesentlicher Dienste, Anbieter digitaler Dienste oder Einrichtungen der öffentlichen Verwaltung in den Geltungsbereich dieses Gesetzes fallen, können ebenso mit Risiken und Vorfällen, aber auch mit Sicherheitsvorfällen konfrontiert sein. Die freiwillige Meldung solcher Risiken, Vorfällen und Sicherheitsvorfällen sollte im öffentlichen Interesse auf freiwilliger Basis möglich sein, da sie für ein gesamtstaatliches und vollständiges Lagebild essentiell ist. Art. 20 NIS-RL sieht die Möglichkeit der freiwilligen Meldungen explizit vor.

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. Auch können Informationen, die auf die Identität des Meldenden schließen lassen, 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.

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

Sie soll jedoch nicht dazu führen, dass der meldenden Einrichtung Pflichten auferlegt werden, die nicht für sie gegolten hätten, wenn sie nicht freiwillig gemeldet hätte. Für freiwillige Meldungen ist grundsätzlich der gleiche sichere Kommunikationskanal wie für verpflichtende Meldungen zu verwenden.

Zu § 24 (Cyberkrise):

Der Bundesminister für Inneres stellt fest, ob bei einer vorhandenen schweren Anomalie im Cyberraum die Voraussetzungen einer Cyberkrise (§ 3 Z 22) vorliegen und ruft diese gegebenenfalls aus. Bei seiner Entscheidungsfindung wird er durch den Koordinationsausschuss beratend unterstützt (§ 25).

Zu § 25 (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 (§ 24) 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 § 26 (Verwaltungsstrafbestimmungen):

Für Verstöße gegen die Verpflichtungen, die sich aus diesem Bundesgesetz ergeben, sind Verwaltungsstrafen von der zuständigen Bezirksverwaltungsbehörde zu verhängen (Abs. 2). 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 Meldepflichten 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 Geldstrafen gegen juristische Personen oder gegen eingetragene Personengesellschaften verhängt werden können (Abs. 4 und 5). Die Verhängung von Geldstrafen gegen juristische Personen oder gegen eingetragene Personengesellschaften orientiert sich an § 99d des Bankwesengesetzes (BWG), BGBl. Nr. 532/1993.

Unter Berücksichtigung des Doppelstrafverbots und in Orientierung an § 30 Abs. 3 DSG kann von der Bestrafung eines Verantwortlichen gemäß § 9 VStG abgesehen werden, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird (Abs. 6).

Zu §§ 27 bis 31 (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 Dieses Bundesgesetz soll mit Ablauf des Tages der Kundmachung in Kraft treten.

Zu Artikel 2 (§ 16a Abs. 5a TKG 2003):

Gemäß § 16a Abs. 5 TKG 2003 haben Betreiber öffentlicher Kommunikationsnetze oder -dienste der Regulierungsbehörde (RTR) Sicherheitsverletzungen oder einen Verlust der Integrität mitzuteilen, sofern dadurch beträchtliche Auswirkungen auf den Netzbetrieb oder die Dienstebereitstellung eingetreten sind. Der vorgesehene Abs. 5a bestimmt, dass die Regulierungsbehörde eine solche Mitteilung unverzüglich an den Bundesminister für Inneres weiterzuleiten hat. Dadurch soll sichergestellt werden, dass das gesamtheitliche Lagebild, welches im Rahmen der Koordinierungsstrukturen erörtert werden soll,

Informationen über Sicherheitsverletzungen oder den Verlust der Integrität bei Betreibern öffentlicher Kommunikationsnetze oder -dienste enthält.

Datenschutz-Folgenabschätzung

Systematische Beschreibung der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten öffentlichen Interessen

Der Bundeskanzler, der Bundesminister für Inneres, der Bundesminister für Landesverteidigung, der Bundesminister für Europa, Integration und Äußeres und die Computer-Notfallteams sind ermächtigt, personenbezogene Daten und personenbezogene Daten zu verarbeiten (§ 9 NISG) und einander zu übermitteln. Eine solche Verarbeitung oder Übermittlung muss entweder zwecks Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen und zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit oder zum Zwecke der Erfüllung der rechtlichen Verpflichtungen aufgrund des NISG bzw. aufgrund innerstaatlicher (§ 10 Abs. 2 NISG) oder internationaler Amtshilfe (§ 10 Abs. 3 und 4 NISG).

Die Kategorien von betroffenen Personen und umfassten Daten werden in § 9 NISG festgelegt und sind

- Organisatorische Daten (zB E-Mails) von Teilnehmern und ihren Organisationseinheiten im Zuge der Teilnahme an IKDOK und OpKoord,
- Lagebilddaten (zB Angriffsszenarien),
- Geschäftsfalldaten (zB ELAK-Daten),
- Daten von Einmelder und Kontaktperson (zB CISO eines angegriffenen Unternehmens),
- Vorfallbezogene Daten (zB Opfer [zB gehackter Server] und Angreifer [zB IP-Adresse des angreifenden Hackers]),
- Daten der Akteure des NISG (insb. Anbieter, Betreiber, Einrichtungen öffentlicher Verwaltung, Computer-Notfallteams),
- Kontaktdaten für EU-weite Gremien und
- Daten von qualifizierten Stellen, Personen wg. Überprüfung der Sicherheitsvorkehrungen, technische Rohdaten (zB aus Honeypot).

Es sind keine besonderen Kategorien betroffen.

Zur Analyse von Meldungen über Risiken, Vorfälle und Sicherheitsvorfälle sowie von Erkenntnissen, die gemäß § 13 Abs. 1 und 2 NISG gewonnen wurden, hat der Bundesminister für Inneres gemäß § 11 NISG IKT-Lösungen zu betreiben. Weiters ist er gemäß § 13 NISG ausdrücklich ermächtigt IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen zu betreiben.

Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

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

- der EU-rechtlichen Verpflichtung in Rahmen der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. Nr. L 194 vom 19.07.2016 S. 1,
- den auf der NIS-RL fußenden im NISG normierten Pflichten und
- erheblichem wichtigem öffentlichem Interesse an der Abwehr und schnellen Lösung von Cyberangriffen gegen „kritische Infrastruktur“ zur Gewährleistung eines hohen nationalen und internationalen Sicherheitsniveaus von Netz- und Informationssystemen

Im Zusammenhang mit der Verarbeitung, Übermittlung und Weiterverarbeitung personenbezogener Daten besonderer Kategorien darf insbesondere auf Art. 9 Abs. 2 lit. b, g, h und j DSGVO verwiesen werden. Bezüglich Art. 9 Abs. 2 lit. h DSGVO in Verbindung mit Art. 9 Abs. 3 DSGVO wird auf die Regelungen zur Amtsverschwiegenheit sowie auf anderweitige Verschwiegenheitspflichten verwiesen. Für die IKDOK-Teilnehmer wurde die Freigabe für Sicherheitsstufe „geheim“ normiert und für zusätzliche Teilnehmer an der OpKoord zur Klarstellung eine gesetzliche Verschwiegenheitspflicht auch im NISG vorgesehen.

Risiken

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

– „physische, materielle oder immaterielle Schäden“, „unbefugte Aufhebung der Pseudonymisierung“, „Rufschädigung“, „Identitätsdiebstahl oder -betrug“, „finanzielle Verluste“,

„Verlust der Vertraulichkeit bei Berufsgeheimnissen“ oder „erhebliche wirtschaftliche oder gesellschaftliche Nachteile“:

Diese Risiken beziehungsweise Nachteile sind nahezu ausgeschlossen, weil mit den Strafbestimmungen des vierten bis sechsten sowie zweiundzwanzigsten Abschnittes des Besonderen Teiles des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974, sowie den allenfalls anzuwendenden dienstrechtlichen Bestimmungen, wie beispielsweise dem Disziplinarrecht, wirksame Vorkehrungen gegen die unrechtmäßige Verarbeitung von Daten und somit das Entstehen von physischen, materiellen oder immateriellen Schäden bestehen. Wer die jeweiligen Daten missbraucht, geht angesichts der gerichtlichen Strafdrohung selbst ein sehr hohes Risiko ein.

Auf die Regelungen zur Amtsverschwiegenheit sowie auf anderweitige Verschwiegenheitspflichten darf verwiesen werden (vgl. Art. 20 B-VG, § 46 BDG 1979, …). Insbesondere ist aufgrund der durchgehenden Protokollierungspflicht (§ 9 Abs. 6) kein Missbrauch der Daten zu erwarten.

Aufgrund der Struktur des § 9 NISG ist gewährleistet, dass die Datenmenge und der Detailierungsgrad reziprok zur Anzahl der zur Verarbeitung befugten Stellen ist.

– „Verlust der Kontrolle über personenbezogene Daten“:

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

– „Diskriminierung“:

Dieses Risiko ist durch diverse Diskriminierungsverbote ausgeschlossen auch können freiwillige Meldungen anonym erfolgen (§ 23 Abs. 4 NISG).

– „Einschränkung der Rechte der betroffenen Personen“:

Die Rechte der betroffenen Personen werden in § 9 Abs. 7 und 8 NISG geregelt und gemessen am Zweck des NISG eingeschränkt, da nicht aufgrund der Ausübung des Betroffenenrechtes auf Löschung oder Widerspruch (z. B. der IP-Adresse eines Angreifers) die Möglichkeit der Analyse von Bedrohungsszenarien ausgeschlossen werden soll. Die Beschränkung der Rechte der betroffenen Person im notwendigen und verhältnismäßigen Ausmaß liegt im allgemeinen öffentlichen Interesse und stellt sicher, dass die Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen und zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit möglich ist.

Abhilfemaßnahmen

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

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

Grundsätzlich ist festzuhalten, dass nur ein sehr eingeschränkter Personenkreis, der vor Beginn der Tätigkeit einer Sicherheitsüberprüfung gemäß §§ 55 ff des Sicherheitspolizeigesetzes (SPG), BGBl. Nr. 566/1991, für den Zugang zu geheimer Information unterzogen wurde, Zugang zu den Daten hat.

– „schnellstmögliche Pseudonymisierung personenbezogener Daten“ (siehe auch Erwägungsgrund 28 DSGVO):

Soweit möglich wird im Lagebericht (§ 9 Abs. 2 Z 2 NISG) die Aufnahme von personenbezogenen Daten hintangehalten.

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

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

Außerdem wird durch das gemäß Art. 30 DSGVO zu führende Verzeichnis von Verarbeitungstätigkeiten, das der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist, dargestellt, welche Verarbeitungstätigkeiten jeweils vorgenommen werden und der jeweiligen Zuständigkeit unterliegen.

– „Datensicherheitsmaßnahmen“ (Erwägungsgrund 83 DSGVO):

Der Bundesminister für Inneres ist als Betreiber der IKT-Lösungen gemäß §§ 11 bis 13 NISG verpflichtet dem Stand der Technik entsprechende Maßnahmen gemäß Art. 32 DSGVO zu setzen.

Ergebnis

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