Amt der Wiener Landesregierung

Magistratsdirektion der Stadt Wien
Geschäftsbereich Recht
Rathaus, Stiege 8, 2. Stock, Tür 428
1082 Wien
Tel.: +43 1 4000 82345
Fax: +43 1 4000 99 82310
E-Mail: post@md-r.wien.gv.at
www.wien.at

Bundeskanzleramt

MDR - 802800-2018-12
Entwurf eines Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz - NISG);
Begutachtung
Stellungnahme

Wien, 24. Oktober 2018

zu BKA-180.310/0234-I/6/2018

Zu dem mit Schreiben vom 19. September 2018 übermittelten Entwurf eines Bundesgesetzes zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) wird wie folgt Stellung genommen:

In grundsätzlicher Hinsicht:

Der Entwurf dient der Umsetzung 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 (NIS-RL). Die Umsetzung erfolgt in der Weise, dass für alle Belange der Sicherheit von Netz- und Informationssystemen sowohl privater Anbieter wesentlicher Dienste als auch für die Erbringung wesentlicher Dienste durch die Länder und Gemeinden ausschließlich der Bund, und zwar zentral der Bundeskanzler und der Bundesminister für Inneres zuständig gemacht werden soll. Diese Behörden sollen also auch in jenen Bereichen zuständig gemacht werden, in denen die Gesetzgebung bzw. die Vollziehung gemäß Art. 12 bzw. Art. 15 Abs. 1 B-VG den Ländern zusteht. Nach den Ausführungen in den Erläuterungen betrifft dies die Kompetenzen der Länder zur Vollziehung der Straßenpolizei (Art. 11 Abs. 1 Z 4 B-VG), der Binnenschifffahrt hinsichtlich Schifffahrtsanlagen bzw. der Strom- und Schifffahrtspolizei auf Binnengewässern (Art. 11 Abs. 1 Z 6 B-VG), ferner die Kompetenz der Länder zur Regelung des Gesundheitswesens, soweit es sich um Krankenanstalten handelt (Heil- und Pflegeanstalten Art. 12 Abs. 1 Z 1 B-VG), des Rettungswesens

(Art. 15 Abs. 1 B-VG) und des Elektrizitätswesens, soweit es nicht unter Art. 10 B-VG fällt (Art. 12 Abs. 1 Z 5 B-VG). Aus § 14 Abs. 2 des Entwurfes, der festlegt, ab wann ein Dienst wesentlich ist, ergibt sich, dass darunter auch die Länder und Gemeinden als Anbieter öffentlicher Gesundheitsdienstleistungen, der öffentlichen Versorgung mit Wasser, Energie und lebenswichtigen Gütern (etwa Gas und Fernwärme, aber auch Müllabfuhr) fallen, sofern deren Verfügbarkeit zu einem überwiegenden Teil von Netz- und Informationssystemen abhängig ist.

Dazu ist festzustellen, dass die Aufzählung der betroffenen Landesmaterien in den Erläuterungen nicht vollständig ist. Wie der kompetenzrechtlichen Beurteilung des BKA vom 26. September 2017, Zl. BKA-602.808/0003-V/5/2017, über die Umsetzung der NIS-RL entnommen werden kann, sind weitere Landeskompetenzen betroffen wie etwa die vom Kompetenztatbestand „Heil- und Pflegeanstalten“ mitumfassten nichtöffentlichen Krankenanstalten, insbesondere die selbständigen Ambulatorien und die von kasseneigenen Einrichtungen selbst angebotenen Leistungen wie etwa jene der KFA. Aber auch eine nachvollziehbare Darstellung der vom Entwurf betroffenen Leistungen der Gemeinden im Wege der Privatwirtschaftsverwaltung wie etwa jene der Trink- und Nutzwasserversorgung oder der aus hygienischer Sicht und zur Vermeidung von Seuchen lebenswichtigen Müllentsorgung durch gemeindeeigene Einrichtungen fehlt in den Erläuterungen zur Gänze. Der Entwurf ist daher von wesentlich weiterer Tragweite als darin ausgeführt. Dies ist insbesondere für die Interpretation der Kompetenzdeckungsklausel, die den Bund ja auch zur Erlassung künftiger Regelungen auf den vom Entwurf erfassten Gebieten ermächtigt, von wesentlicher Bedeutung.

Neben der umfassenden Zentralisierung, die der Entwurf intendiert, ist zu bemerken, dass der Entwurf im Vergleich zu den Vorgaben der Richtlinie zum Teil erheblich von diesen abweicht und diese übererfüllt (sog. golden plating). Dabei wird eine grundsätzliche Tendenz feststellbar, die vor allem in rechtsstaatlicher Hinsicht, aber auch auf Grund der dadurch verursachten Kostenbelastung zu kritisieren ist: die Richtlinie verlangt in allen Zusammenhängen immer nur „verhältnismäßige“ technische und organisatorische Maßnahmen (siehe etwa die Art. 15 Abs. 1 und 16 Abs. 1 der Richtlinie) bzw. Maßnahmen, sofern solche „erforderlich“ sind (siehe etwa Art. 17 Abs. 1 der Richtlinie). Der Entwurf unterstellt hingegen die Erforderlichkeit und Verhältnismäßigkeit so weitgehender Maßnahmen wie einer unbeschränkten Einschaumöglichkeit in Netz- und Informationssysteme sowie in nicht näher genannte Unterlagen und die Verhängung von gravierenden Geldstrafen, schon bei Verstoß gegen einfache Meldepflichten, allein unter Berufung auf die abstrakt behauptete Beeinträchtigung der öffentlichen Sicherheit, dies ohne nähere Differenzierung. In all diesen Zusammenhängen wären aber, wie der Gleichheitsgrundsatz des Art. 7 B-VG sowie die zu Grunde liegende Richtlinie vorgibt, nur verhältnismäßige Maßnahmen zulässig und diese daher einfachgesetzlich mit am jeweils zu erwartenden Sicherheitsrisiko orientierten Parametern entsprechend abzubilden.

In grundsätzlicher Hinsicht ist weiters zu kritisieren, dass der Entwurf von den von den Gebietskörperschaften angebotenen wesentlichen Diensten nur jene des Bundes durch Sonderbestimmungen in § 19 privilegiert, jene der Länder und Gemeinden aber - trotz Entzug der diesbezüglichen Regelungskompetenzen der Länder durch die Kompetenzdeckungsklausel (!) - den allgemeinen Regelungen des Entwurfes unterstellt, wozu auch die Strafbestimmungen gehören. Dies ist für Wien weder aus Landes- noch aus Gemeindesicht akzeptabel.

Zu den Bestimmungen im Einzelnen:

Zu § 1:

Die in dieser Bestimmung enthaltene Kompetenzdeckungsklausel lautet: „Die Erlassung, Aufhebung sowie Vollziehung von Vorschriften, wie sie in diesem Bundesgesetz enthalten sind, sind auch in den Belangen Bundessache, hinsichtlich derer das Bundes-Verfassungsgesetz (B-VG), BGBl. Nr. 1/1930, etwas anderes bestimmt. Die in diesen Vorschriften geregelten Angelegenheiten können in unmittelbarer Bundesverwaltung besorgt werden.“ Das Wort „Erlassung“ erfasst, versteht man es nicht bloß als einmaligen Akt, auch die Änderung der einmal erlassenen Vorschriften, zumindest in dem durch die erstmalige Erlassung gesteckten thematischen Rahmen. In den Erläuterungen wäre daher klarzustellen, inwieweit Änderungen und insbesondere thematische Erweiterungen von dieser Klausel gedeckt sind.

Gemäß Erwägungsgrund 9 der NIS-RL gehen spezifische Sicherheits-Rechtsakte für einzelne Sektoren vor. In diesem Zusammenhang stellt sich die Frage, ob auch solche europäischen Rechtsakte auf Grundlage der Kompetenzdeckungsklausel vom Bund umgesetzt wurden bzw. werden oder ob sich in diesen Fällen die Zuständigkeit nach dem B-VG richtet.

Ferner wirft die Formulierung die Frage auf, ob diese Klausel - ausgehend von den Vorschriften über die Sicherheit in den Bundesministerien und Bundesämtern - nicht bereits schon jetzt den Bund auch zur Erlassung von Vorschriften über die Sicherheitsstrategie und die Sicherheitsvorkehrungen in den Ämtern der Länder und Gemeinden ermächtigen soll. Dies ist entschieden abzulehnen. Es wäre in den Erläuterungen entsprechend klarzustellen, dass sich der Entwurf darauf nicht bezieht.

Zu § 2:

Nach § 2 Abs. 1 Z 1 des vorliegenden Gesetzesentwurfes unterliegt in Umsetzung der NIS-RL auch der Energiesektor diesem Gesetz. Im Elektrizitäts- und Erdgassektor existieren unterschiedliche Marktakteure, die zum Teil auch wesentliche Dienste zu erbringen haben. Die betroffenen Unternehmen sollten im Gesetz abschließend aufgezählt werden. Nach der Richtlinie wären nur die Verteilernetzbetreiber, Übertragungsnetzbetreiber und die Stromversorger einzubeziehen. Dies sind die Hauptakteure, die nach den beiden Richtlinien zur Liberalisierung des Elektrizitäts- und Erdgassektors in jedem Mitgliedstaat vorzusehen waren. Aufzunehmen wäre jedenfalls auch der Bilanzgruppenkoordinator (BKO), der seit rund fünf Jahren die Plattform für den standardisierten Lieferantenwechsel betreibt. Die weiteren Marktakteure, die im Elektrizitäts- und Erdgassektor überdies einzubeziehen wären, sollten ebenso im Gesetz (allenfalls unter Einbeziehung der Regulierungsbehörde - E-Control) festgelegt werden.

Die Betreiber öffentlicher oder privater Tarifkalkulatoren wären als Betreiber von Online-Suchmaschinen ebenfalls einzubeziehen. Diese sind als Betreiber digitaler Dienste anzusehen.

Als Einrichtung des Bundes sollte jedenfalls die Regulierungsbehörde (E-Control) in das NIS-Gesetz ausdrücklich aufgenommen werden.

Die Betreiber wesentlicher Dienste bedienen sich im Energiebereich kritischer ICT-Infrastrukturen. Es handelt sich dabei beispielhaft um IDS/IPS-Anlagen, Firewalls, kryptographische Systeme. Entsprechend dem so genannten „Need-to-know-Prinzip“ (siehe in ISO/IEC 27036-3 - 6.3.5) muss zwecks Risikominimierung der Kreis der Wissenden möglichst gering gehalten werden. Die EU hat jedoch die Schaffung eines „EU-weiten Zertifizierungssystems für Cybersicherheit“ angekündigt (vgl. die Schlussfolgerungen des Rates vom 19./20. Oktober 2017, EUCO 14/17 S 6). Durch die damit verbundene Einschränkung berechtigter Systemhersteller (und die Reduktion der in Frage kommenden Systeme) sind die in Zukunft verwendbaren Systemtypen für eine breite Anwendergruppe zugänglich. Die Verarbeitung (Weitergabe, Entgegennahme und Auswertung) von Sicherheitsinformationen ist daher besonders risikobehaftet. Alle mit der Verarbeitung von Sicherheitsinformationen befassten Einrichtungen müssen daher unbedingt angemessene Sicherheitsvorkehrungen treffen. Die gesetzlichen Rahmenbedingungen müssen dementsprechend ausgestaltet sein.

Weiters ist anzumerken, dass der Begriff „Betreiber“ vor dem Hintergrund der österreichischen Gesundheitslandschaft im Zuge der Richtlinienumsetzung nicht ausreichend spezifiziert wurde. Es ist unklar, ob damit zum Beispiel der Wiener Krankenanstaltenverbund als Zusammenschluss von Gesundheitseinrichtungen oder die einzelnen Krankenanstalten oder sonstigen Einrichtungen (Pflegewohnhäuser, sonstige Serviceeinheiten wie Wäscherei) gemeint sind. Fraglich ist, ob das aus dem gemäß § 14 Abs. 5 Z 1 zu erlassenden Bescheid hervorzugehen hat oder ob dies Gegenstand einer allenfalls gemäß § 14 Abs. 4 des Entwurfes zu erlassenden Verordnung sein soll. Eine legistische Klarstellung wäre erforderlich.

Zu § 3:

Z 1 lit. b definiert als „Netz- und Informationssystem“ unter anderem „eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen.“ Damit fällt auch jede Vorrichtung, die mit dem Internet verbunden ist, sei es ein Computer oder ein Mobiltelefon, ebenfalls unter die Begriffsbestimmung. Die Erläuterungen beziehen sich aber auf „digitale Hochgeschwindigkeitsverarbeitungsvorrichtungen“, ohne dass dieser Begriff näher definiert oder im Gesetzestext genannt wird.

Z 1 lit. c definiert auch die „digitalen Daten, die von den - in lit. a und b genannten - Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden“, als „Netz- und Informationssystem“. Damit fallen jedoch alle Daten, die in der Cloud gespeichert werden oder über Netze übertragen werden, unter die Legaldefinition.

In beiden Fällen wären entsprechende Konkretisierungen erforderlich.

Z 10 definiert als „Anbieter digitaler Dienste“ eine juristische Person
a) mit Hauptniederlassung in Österreich oder
b) ohne Hauptniederlassung in der Europäischen Union, die einen Vertreter (Z 11) namhaft gemacht hat, ...“ Es stellt sich die Frage, ob die Einschränkung „ohne Hauptniederlassung in der Europäischen Union“ in lit. b angesichts der Legaldefinition in Z 11 erforder-

lich ist, weil Vertreter nach Z 11 ohnedies nur benannt werden können, um im Auftrag eines nicht in der Europäischen Union niedergelassenen Anbieters digitaler Dienste zu handeln.

Im vorliegenden Gesetzentwurf findet sich mehrfach die Wortfolge „natürliche oder juristische Person“ (z. B. in § 3 Z 11). Aus rechtlicher Sicht wäre dies durch die Formulierung „natürliche oder juristische Person oder eingetragene Personengesellschaft“ zu ersetzen.

Die Wortfolge „gemeinsam nutzbarer Rechenressourcen“ in § 3 Z 14 ist ohne die Ausführungen in den Erläuterungen nicht verständlich. Der Begriff „gemeinsam“ ist irreführend und unterstellt das Zusammenwirken mehrerer Nutzer. Folgende Formulierung wird daher vorgeschlagen: „Cloud-Computing-Dienst“ ist „ein digitaler Dienst, der den Zugang zu einem skalierbaren und elastischen Pool nutzbarer Rechenressourcen für eine Vielzahl von Nutzern ermöglicht“.

Zu § 6:

Gemäß dem Entwurf dient die Zentrale Anlaufstelle auch als Verbindungsstelle zur Kooperationsgruppe. Die Kooperationsgruppe dient laut § 3 Z 16 der strategischen Zusammenarbeit, die entsprechend der österreichischen Vertretung in diesem Gremium dem Bundeskanzleramt zukommt (vgl. § 4 und dessen Z 2). Es stellt sich in diesem Zusammenhang die Frage, warum die „Gewährleistung der grenzüberschreitenden Zusammenarbeit .... mit der Kooperationsgruppe“ durch das Innenministerium, das nach der Intention des Gesetzesentwurfs für operative Angelegenheiten zuständig sein soll, erfolgen soll. Sollte hingegen gemeint sein, dass die Zentrale Anlaufstelle der Kooperationsgruppe zum „Zwecke der wirksamen Information“ zusammenfassende Berichte über die durch die operative Tätigkeit gemachten Erfahrungen zusammenstellen soll, wäre dies klarer auszudrücken.

Zu § 9:

Gemäß § 9 Abs. 1 ist die Teilnahme für Betreiber wesentlicher Dienste an „technischen Einrichtungen“ des Innenministeriums, die Unregelmäßigkeiten oder Störungen von Netz- und Informationssystemen frühzeitig erkennen, freiwillig. Dies wird durch die Formulierung „können an den vom Bundesminister für Inneres betriebenen technischen Einrichtungen teilnehmen“ ausgedrückt. Sie können dabei „festlegen, welche Daten an den Bundesminister für Inneres übermittelt werden.“ In den Erläuterungen wird diese Freiwilligkeit auch betont, wobei sich dort die Ergänzung findet: „..., wohingegen ein gänzlicher Ausschluss der Datenübermittlung nicht möglich ist.“ Dies ist allerdings ein offensichtlicher Widerspruch. Möglicherweise ist damit gemeint, dass im Fall einer freiwilligen Teilnahme an den technischen Einrichtungen des Innenministeriums jedenfalls ein Minimum an Datenübermittlung erforderlich ist. Es wird ersucht, dies im Gesetz durch Präzisierung der Datenarten klarzustellen.

Gemäß § 9 Abs. 2 ist der Bundesminister für Inneres zur Erfüllung der Aufgabe gemäß § 5 Z 4 ermächtigt, technische Einrichtungen nicht nur (Erg.: selbst) zu betreiben, sondern auch zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen. Die Nutzung technischer Einrichtungen von Betreibern wesentlicher Dienste oder Anbietern digitaler Dienste stellt einen Eingriff in das Eigentumsrecht und in berechtigte Geheimhaltungsinteressen dar und ist in dieser Form nicht zulässig.

Zu § 10:

Gemäß Art. 6 Abs. 3 der Datenschutz-Grundverordnung (DSGVO) ist der Zweck der Verarbeitung in der Rechtsgrundlage festzulegen. Eine Festlegung des Zwecks nur in den Erläuterungen ist somit nicht ausreichend. Weiters wird auf die Möglichkeit zur Durchführung einer Datenschutz-Folgenabschätzung im Zusammenhang mit dem Erlass einer Rechtsgrundlage hingewiesen (Art. 35 Abs. 10 DSGVO).

Zu § 11:

§ 11 regelt die gemeinsame Verarbeitung personenbezogener Daten durch Bundeskanzler, Bundesminister für Inneres und Bundesminister für Landesverteidigung. Der Zusammenhang zu den „Erkenntnissen, die gemäß § 9 Abs. 1 und 2 gewonnen wurden“ (§ 11 Abs. 1 letzter Satz), ist nicht erkennbar, da laut Erläuterungen zu § 9 „eine Analyse von Daten innerhalb des Teilnehmernetzwerkes“ nicht erfolgt, Daten nicht entschlüsselt und die Klassifizierung von Daten gewahrt bleiben sollen. Ein Personenbezug könnte sich daher nur aus Daten ergeben, die vor dem Teilnehmernetzwerk zum Zweck des Datentransports entstehen, etwa Verkehrsdaten im Sinne von § 92 Abs. 3 Z 4 des Telekommunikationsgesetzes 2003 (TKG 2003). Eine Klarstellung, welche personenbezogenen Daten aus den Erkenntnissen gemäß § 9 Abs. 1 und 2 gewonnen werden, wäre erforderlich.

Die Rolle des Auftragsverarbeiters (§ 11 Abs. 3) kann der Bundesminister für Inneres nur gegenüber Bundeskanzler und Bundesminister für Landesverteidigung wahrnehmen, hinsichtlich der von ihm zur Verfügung gestellten Daten bleibt er Verantwortlicher im Sinne der Datenschutz-Grundverordnung.

§ 11 Abs. 4 würde die Möglichkeit der Umgehung strengerer Voraussetzungen schaffen, die das Sicherheitspolizeigesetz und die Strafprozessordnung für die zulässige Übermittlung vorsehen. Es wird ersucht, die Referenz auf die Bestimmungen des 4. Hauptstücks des Sicherheitspolizeigesetzes einzufügen, sodass der entsprechende Satzteil lautet: „Übermittlungen ..... sind zulässig an Sicherheitsbehörden zur Verarbeitung personenbezogener Daten im Rahmen der Sicherheitspolizei gemäß den Bestimmungen des 4. Hauptstücks des Sicherheitspolizeigesetz, BGBl. Nr. 566/1991 in der geltenden Fassung, ...“ Der Verweis auf die Strafrechtspflege hat zu entfallen, weil die entsprechenden Übermittlungsbestimmungen, wie sie beispielsweise durch die Strafprozessordnung geregelt werden, in die Kompetenz des Justizressorts fallen.

Zu § 12:

Für die Verarbeitung personenbezogener Daten durch Computer-Notfallteams gemäß § 12 Abs. 7 sollte eine maximale Aufbewahrungsdauer festgelegt werden, nach deren Ablauf die Daten zu löschen oder der Personenbezug durch Anonymisierung zu entfernen ist. Diese Forderung gilt selbstverständlich nicht für allgemeine Identifikations- und Erreichbarkeitsdaten im organisatorischen Netzwerk, die nicht in einem Zusammenhang mit einem bestimmten Sicherheitsvorfall stehen, sofern diese Daten aktuell gehalten sind.

Zur Beschreibung des zulässigen Zwecks der Verarbeitung ist der Verweis auf Erwägungsgrund 49 der Datenschutz-Grundverordnung in den Erläuterungen nicht ausreichend - der Zweck wäre direkt im Gesetzestext zu verankern.

Zu § 14:

§ 14 Abs. 1 und 2 sieht vor, dass der Bundeskanzler die Betreiber wesentlicher Dienste für jeden in § 2 Abs. 1 genannten Sektor zu ermitteln hat. Die Strafbestimmungen in § 23 Abs. 1 erfassen unter anderem die Betreiber wesentlicher Dienste im Sinn des § 14 Abs. 2 (dazu gehören unter anderem auch die öffentlichen Versorger mit Wasser) und sehen bereits bei Verstößen gegen Informationspflichten Geldstrafen bis EUR 50.000,-- und im Wiederholungsfall bis EUR 100.000,-- vor. Diese Bestimmungen erscheinen nicht als verhältnismäßig: es wären die Gebietskörperschaften als Betreiber wesentlicher Dienste von den Strafbestimmungen auszunehmen (§ 23 Abs. 4 erfasst sogar die einzelnen Mitglieder eines Kollegialorgans einer Gebietskörperschaft). Hier bestehen auf Grund Art. 22 B-VG andere Mittel und Wege, die erforderlichen Informationen bzw. die Einhaltung von Vorgaben verlangen zu können. In diesem Zusammenhang ist anzumerken, dass der Bund für die von ihm betriebenen Dienste Sonderbestimmungen in § 19 vorsieht, diese sind freilich von der Strafbestimmung des § 23 Abs. 1 nicht erfasst. Das Bundeskanzleramt und das Bundesministerium für Inneres sind überdies von der Meldepflicht an das GovCERT befreit (siehe die Subsidiaritätsklausel in § 19 Abs. 2 erster Halbsatz). Diese Bestimmung bewirkt eine gravierende Ungleichbehandlung des Bundes einerseits und der Länder und Gemeinden andererseits.

Zur Liste der Betreiber wesentlicher Dienste gemäß § 14 Abs. 5 Z 3 lässt der Gesetzesentwurf offen, ob diese Liste publiziert wird bzw. wem diese zur Verfügung gestellt wird. Es gäbe durchaus Argumente, die Liste nicht zu veröffentlichen, um Angreifer der Netz- und Informationssicherheit nicht über potenzielle Ziele zu informieren. Andererseits wäre die Bekanntgabe der Liste an alle beteiligten Einrichtungen, die das vorliegende Gesetz vorsieht, inkl. der Computer-Notfallteams und der betroffenen Betreiber wesentlicher Dienste für die Zusammenarbeit nützlich. Um entsprechende Klarstellung wird ersucht.

Zu § 15:

§ 15 Abs. 1 sieht vor, dass die Betreiber wesentlicher Dienste geeignete, dem Stand der Technik entsprechende Sicherheitsvorkehrungen zu treffen haben. Diese Bestimmung ist ein Paradebeispiel für ein sog. golden plating: die Richtlinie sieht in Art. 16 Abs. 1 nur vor, dass die Mitgliedsstaaten sicherstellen, dass die Anbieter Maßnahmen treffen, die „unter Berücksichtigung des Standes der Technik ein Sicherheitsniveau gewährleisten, das dem bestehenden Risiko angemessen ist“. Diese Bestimmung bewirkt, dass die Anbieter wesentlicher Dienste (wozu auch die Länder und Gemeinden zählen) einer permanenten Nachrüstpflicht unterliegen, und zwar in allen Fällen, ungeachtet des Ausmaßes des dadurch verursachten Sicherheitsrisikos. Dies ist weder unionsrechtlich geschuldet noch sachlich und wäre daher, nicht zuletzt im Hinblick auf die daraus resultierende, rein durch den technischen Fortschritt enervierte budgetäre Belastung, durch sinnvolle, risikoorientierte Kriterien einzuschränken.

Die ersten beiden Sätze des § 15 Abs. 3 regeln die Zeit, innerhalb der die Betreiber wesentlicher Dienste die getroffenen Sicherheitsvorkehrungen nachzuweisen haben, und zwar mindestens alle drei Jahre, sofern jedoch ein Bescheid gemäß § 14 Abs. 5 Z 1 ergeht, jederzeit. Diese Differenzierung ist unionsrechtlich nicht vorgegeben; vor allem aber ist sie sachlich nicht nachvollziehbar: aus § 14 Abs. 1 ergibt sich, dass die Betreiber wesentlicher Dienste zu ermitteln sind. Daher ist davon auszugehen, dass der Erlassung

eines Bescheides nach § 14 Abs. 5 Z 1 konstitutionelle Wirkung zukommt. Anderenfalls hätte die Einräumung der Kompetenz zur Bescheiderlassung in dieser Bestimmung keinen Sinn. Die Nachweispflicht alle drei Jahre (ohne dass ein Bescheid erlassen wurde) hat daher, soweit ersichtlich, keinen Anwendungsbereich. Sollte die Zuerkennung der Betreibereigenschaft durch Bescheid hingegen keine konstitutionelle Wirkung haben, ist die Differenzierung zwischen der dreijährigen und der jederzeitigen Pflicht zur Erbringung des Nachweises der Erfüllung der Sicherheitsanforderungen nicht nachvollziehbar und daher unsachlich.

Nach dem vierten Satz dieser Bestimmung kann der Bundesminister für Inneres zur Kontrolle der Einhaltung der Sicherheitsanforderungen Einschau in die Netz- und Informationssysteme und diesbezügliche Unterlagen nehmen. Eine Einschränkung auf welche Aspekte die Einschau zu beschränken ist, ist in der Bestimmung nicht enthalten. Dem Wortlaut nach ist dieses Einschaurecht daher nicht auf Aspekte der Netzsicherheit beschränkt, sondern umfasst auch die Einschau in die Inhalte der jeweiligen Datenbank. In einer Gesamtschau mit der datenschutzrechtlichen Ermächtigung des § 10 Abs. 1 des Entwurfes ergibt dies ein umfassendes, nicht näher determiniertes Einschaurecht in Daten und Unterlagen. Dies erscheint im Hinblick auf den Zweck der Einschau (Gewährleistung von dem Stand der Technik entsprechenden Sicherheitsvorkehrungen - siehe den Verweis auf Abs. 1) nicht gerechtfertigt und wäre durch gesetzlich festgelegte Grenzen einzuschränken.

§ 15 Abs. 4 lautet: „Der Bundesminister für Inneres sieht im Einvernehmen mit dem Bundeskanzler Erfordernisse, die eine qualifizierte Stelle erfüllen muss, durch Verordnung vor und entscheidet über das Vorliegen einer qualifizierten Stelle mittels Bescheid. Darüber hinaus kann er besondere Kriterien bestimmen, nach denen eine Stelle jedenfalls als qualifiziert gilt.“ Weder aus dieser noch einer vorangehenden oder nachfolgenden Bestimmung sind Kriterien zu entnehmen, an die die befugten Stellen bei der Verordnungserlassung, der Entscheidung mittels Bescheid und der Festlegung der ex lege-Qualifizierung gebunden sind. Diese Bestimmung enthält daher in dreifacher Hinsicht keine dem Art. 18 Abs. 1 B-VG entsprechenden Determinanten für den Vollzug. Dies ist verfassungswidrig.

Zu § 18:

§ 18 Abs. 4 ermächtigt den Bundesminister für Inneres von Anbietern digitaler Dienste im Rahmen ihrer Nachweispflicht über geeignete Sicherheitsvorkehrungen die Übermittlung einer „Aufstellung der vorhandenen Sicherheitsvorkehrungen“ zu verlangen. Auch hier könnten Geheimhaltungs- und Sicherheitsinteressen des Anbieters digitaler Dienste beeinträchtigt werden, sei es, dass die Unterlagen in unbefugte Hände geraten, sei es, dass die Herausgabe von Unterlagen deren Klassifizierung widersprechen oder die Geheimhaltungspflichten gegenüber Dritten verletzen würde. Als Alternative wird folgende Formulierung vorgeschlagen: „die getroffenen Sicherheitsvorkehrungen bekannt zu geben“, wobei diese nur genannt, aber nicht im Detail beschrieben werden müssen. Eine Einschau vor Ort - ohne Mitnahme von Unterlagen oder Kopien davon - stünde dem nicht entgegen.

Zu § 28:

§ 28 nennt für das Inkrafttreten ein in der Vergangenheit liegendes Datum. Es wird davon ausgegangen, dass ein rückwirkendes Inkrafttreten nicht beabsichtigt ist.

Für den Landesamtsdirektor:

OMR MMag. Michael Ramharter

Dr. Peter Krasa
Obersenatsrat

Ergeht an:

1. Präsidium des Nationalrates

2. alle Ämter der Landesregierungen

3. Verbindungsstelle der Bundesländer

4. MA 63
   (zu 823784-2018)
   mit dem Ersuchen um Weiterleitung an die einbezogenen Dienststellen