Steiermärkische Krankenanstaltengesellschaft m.b.H.
Vorstand

KAGes

Bundeskanzleramt
BKA - I/6
Ballhausplatz 2
1010 Wien

KAGes-Management: Recht und Risikomanagement
Bearbeiter: HR Dr. Peter Schweppe/hol
Telefon: 0316/340-5111
Fax: 0316/340-5208
e-Mail: recht@kages.at
Geschäftszahl: RR-GE-33/18

Graz, am 30.10.2018

Per E-Mail:
nis@bka.gv.at
cc: begutachtungsverfahren@parlament.gv.at

Ihre GZ: BKA-180.310/0234-I/6/2018
Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen
Netz- und Informationssystemsicherheitsgesetz – NISG
Begutachtung

Sehr geehrte Damen und Herren!

In oben näher bezeichneter Angelegenheit dürfen wir zum gegenständlichen Gesetzesentwurf Stellung nehmen wie folgt:

Einleitend gilt es festzuhalten, dass es grundsätzlich begrüßenswert ist, dass die Thematik IT-Sicherheit ein entsprechender Stellenwert eingeräumt wird, wenngleich davon ausgegangen wird, dass der damit einhergehende Mehraufwand seitens des Bundes ersetzt wird (Verursacherprinzip).

Generell gilt es anzumerken, dass viele der angeführten Betreiber wesentlicher Dienste derzeit schon von sich aus eine Fülle von Maßnahmen zur Netzwerk- und Informationssicherheit getroffen haben. Auf diese Tatsache nimmt der gegenständliche Gesetzesentwurf kaum Bezug. Beispielsweise sei in diesem Zusammenhang die ISO-27001-Zertifizierung der KAGes für ihren IT-Kern-Bereich genannt. Daraus folgt, dass bereits schon jetzt ein entsprechender Prozess für den Fall von IT-Sicherheitsvorfällen vorliegt, der eine entsprechende Dokumentation und Bewertung sicherstellt. Ebenso definiert auch die DSG-VO Prozesse zur Meldung von IT-

Sicherheitsvorfällen („Data Breach Notification"). Diese bestehenden Strukturen, Vorgaben und Regelungen finden im Entwurf zu wenig Berücksichtigung und besteht dadurch insbesondere das Risiko, dass Parallelstrukturen geschaffen werden. So stellt etwa die definierte Anlaufstelle SPOC in vielen Fällen eine Parallelorganisation zur Datenschutzbehörde (DSB) dar.

In § 9 werden Gebühren genannt, die eingehoben werden, um Informationen zu bekommen, die Unregelmäßigkeiten oder Störungen betreffen. Dies entspricht einem zentralen CERT. In diesem Zusammenhang gilt es jedoch anzumerken bzw. zu hinterfragen, ob nicht auch dieses CERT Informationen von den Teilnehmern benötigt. Insofern erscheint die Einhebung von Gebühren sachlich nicht gerechtfertigt. Im Übrigen gilt es anzumerken, dass Sicherheitsvorfälle betreffend das Bankenwesen bzw. die Finanzmark-Infrastruktur für Einrichtungen des Gesundheitswesens von untergeordneter Relevanz sind. In Hinblick auf Rechtsträger öffentlicher Krankenanstalten wird analog zu § 64 KAKuG angeregt, diese von sämtlichen Gebühren zu befreien.

Unklar erscheint, was in § 10 Abs. 3 mit der Formulierung „unverzüglicher Auskunft" der Betreiber wesentlicher Dienste, sohin auch Krankenanstalten, gemeint ist, dies insbesondere hinsichtlich allenfalls einzurichtender Rund-um-die-Uhr-Bereitschaften und Wochenenddienste.

§ 12 definiert ein nationales Computer-Notfallteam; in diesem Zusammenhang wird angeregt, die Schnittstellen zwischen SPOC und DSB detailliert zu regeln.

Dieses zentrale Notfallteam dient auch gem. § 12 Abs. 2 Z 1 zur Entgegennahme von Meldungen von Betreibern wesentlicher Dienste, sohin auch Krankenanstaltenträgern. Ungeregelt bleibt, welche Meldepflichten bestehen und bis wann Meldungen zu tätigen sind. Zudem besteht Rechtsunsicherheit dahingehend, ob diese Regelung den Betrieb eines eigenen CERT impliziert.

Der Gesetzesentwurf definiert eine Reihe von Stellen und Zuständigkeiten. Es gilt zu überlegen, ob derartig komplexe Strukturen (SPOC, CIRST-Netzwerk, Computer-Notfallteam, NIS-Büros, GovCERT etc.) geeignet sind, auf Sicherheitsbedrohungen zeitgerecht zu reagieren, zumal gerade bei Cyberattacken in kürzester Zeit zu reagieren ist.

§ 14 Abs. 3 definiert eine Kontaktstelle, die in jenem Zeitraum erreichbar sein muss, in dem ein wesentlicher Dienst zur Verfügung gestellt wird. Im Falle eines Krankenanstaltenträgers bedeutet dies 24 Stunden, 7 Tage die Woche.

§ 15 regelt die Sicherheitsvorkehrungen der Betreiber und beschreibt Vorkehrungen nach dem Stand der Technik. In Absatz 2 soll der Bundesminister für Inneres auf Antrag feststellen, ob diese Maßnahmen geeignet sind. Diesbezüglich wird angeregt, dass bei Inhabern einer ISO-27001-Zertifizierung das Vorliegen von Vorkehrungen nach dem Stand der Technik gesetzlich vermutet wird.

§ 23 regelt Strafbestimmungen bei Verletzungen von Auskunfts- bzw. Meldepflichten. Diesbezüglich darf auf entsprechende Redundanzen betreffend Meldepflichten gem. der DSG-VO hingewiesen werden. Die Begrifflichkeit der „Unverzüglichkeit" ist als unbestimmter Rechtsbegriff determiniert, eine genauere zeitliche Definition erscheint gerade in Hinblick auf die verwaltungsstrafrechtlichen Konsequenzen angezeigt.

Abschließend darf noch darauf hingewiesen werden, dass der Gesetzesentwurf an mehreren Stellen Verordnungsermächtigungen enthält. Die beabsichtigten Inhalte der diesbezüglichen Verordnungen sind uns nicht bekannt, insofern wird im Falle der Erlassung derselben um Einbindung in die diesbezüglichen Begutachtungsverfahren ersucht.

Mit freundlichen Grüßen
Steiermärkische Krankenanstaltengesellschaft m.b.H.

Univ.Prof.Dr. KH. Tscheliessnigg
(Vorstandsvorsitzender)

Dipl.KHBW Ernst Fartek, MBA
(Vorstand für Finanzen und Technik)

Ergeht nachrichtlich an:

- Land Steiermark, z.Hd. Herrn Landesrat Mag. Christopher Drexler,
- Amt der Stmk. Landesregierung, Verfassungsdienst, z.Hd. Frau Mag. Ines Wünsch-Brandner,
- Amt der Stmk. Landesregierung, Fachabteilung 8A, Referat Sanitätsrecht, Legistik und Beteiligungsmanagement.