An das
Bundeskanzleramt
Büro für strategische Netz- und
Informationssystemsicherheit
Ballhausplatz 2
1010 Wien
Per Email an:
nis@bka.gv.at
cc: begutachtungsverfahren@parlament.gv.at

Landeskliniken-Holding
IHRE GESUNDHEIT. UNSER ZIEL.

Kennzeichen:
Beilagen:
Bearbeiter: Mag. Tina Wozniak
Durchwahl:11334

Datum: 31.10.2018

Betrifft: BKA-180.310/0234-I/6/2018, Stellungnahme zum Entwurf des NIS-G

Sehr geehrte Damen und Herren!

Die NÖ Landeskliniken-Holding darf zum gegenständlichen Begutachtungsentwurf Stellung nehmen wie folgt:

Mit dem gegenständlichen Begutachtungsentwurf soll 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-RILI) auf nationaler Ebene umgesetzt werden.
Der nationale Gesetzgeber trifft in einigen Punkten jedoch strengere Regelungen als in der NIS-RILI vorgesehen. Dadurch sind nicht unbeachtliche Mehrkosten zu erwarten, welche sich insb. in Anbetracht des Umstandes, dass viele Faktoren erst in den aufgrund des NIS-G zu erlassenden Verordnungen geregelt werden sollen, nicht abschließend beurteilen lassen.

So kann der Bundeskanzler mit dem Bundesminister für Inneres insb. Kriterien für die Parameter eines Sicherheitsvorfalls iSd § 3 Z 6 lit a bis d sowie gemäß § 4 Abs 1 Z 7 Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste, die jedenfalls zur Gewährleistung der Anforderungen nach § 15 Abs 1 geeignet sind, durch Verordnung festlegen. Insb. unter Berücksichtigung der Erläuterungen zu § 3 Z 6, wonach ein Sicherheitsvorfall auch dann vorliegen kann, wenn er zwar nicht zu einem vollständigen Ausfall eines betriebenen Dienstes, aber zu einer Einschränkung der Verfügbarkeit dieses Dienstes geführt hat, sollten - zumindest in den Erläuterungen - ergänzende Klarstellungen erfolgen.

NÖ Landeskliniken-Holding
Stattersdorfer Hauptstraße 6/C • 3100 St.Pölten
Tel.: +43 (0)2742 9009 • Fax: +43 (0)2742 9009-499 • office@holding.lknoe.at • www.lknoe.at
DVR Nr.: 2112072 • UID Nr.: ATU 619 43 838

Landeskliniken-Holding
IHRE GESUNDHEIT. UNSER ZIEL.

Die Parameter zur Beurteilung des Vorliegens eines Sicherheitsvorfalls sowie der geforderten Sicherheitsanforderungen sollten vom Gesetzgeber unter Berücksichtigung der sektorenspezifischen Faktoren sowie im Sinne eines risikobasierten Ansatzes zudem genau definiert werden. Aus Sicht der NÖ Landeskliniken-Holding muss vor Erlassung der zuvor genannten Verordnungen jedenfalls ein offizielles Begutachtungsverfahren unter Darlegung der aus diesen Verordnungsentwürfen ableitbaren Kosten eingeleitet werden.

Zu § 9:

Der Bundesminister für Inneres soll ermächtigt werden technische Einrichtungen zu betreiben, die Unregelmäßigkeiten oder Störungen von Netz- und Informationssystemen frühzeitig erkennen. Betreiber wesentlicher Dienste können an den vom Bundesminister für Inneres betriebenen technischen Einrichtungen teilnehmen und festlegen, welche Daten übermittelt werden. Der Gesetzesentwurf sieht eine Kostenersatzpflicht der Betreiber von wesentlichen Diensten vor und lässt dabei im Unklaren, wie hoch ein etwaiger Kostenersatz ausfallen wird und auch in welcher Art und Weise ein Zugriff des Bundesministers für Inneres auf Netzwerke von Betreibern wesentlicher Dienste erfolgen soll. Ein Zugriff nach § 9 Abs 2 sollte sich ausschließlich auf Sensorsysteme außerhalb der Netz- und Informationssysteme des Betreibers wesentlicher Dienste beschränken. Zudem muss klargestellt werden, dass ausschließlich jene Daten ermittelt werden dürfen, die der Bundesminister für Inneres zur Erfüllung seiner gesetzlich übertragenen Aufgaben tatsächlich benötigt. Diese sind im Gesetzesentwurf auch entsprechend zu spezifizieren. Zumindest der Großteil an Kosten für den Einsatz von technischen Einrichtungen zur Vorbeugung von Sicherheitsvorfällen bzw. zur Feststellung von Anomalien, sind aus Sicht der NÖ Landeskliniken-Holding jedenfalls vom Bund zu tragen (ErwG 31 zur NIS-RILI).

Zu § 10 und § 11:

Der Bundeskanzler, der Bundesminister für Inneres und der Bundesminister für Landesverteidigung sollen als gemeinsame Verantwortliche iSd Art 4 Z 7 iVm Art 26 DSGVO für die Datenverarbeitung zum Zweck der Bewertung von Risiken für Netz- und Informationssysteme sowie zur Erstellung des Lagebildes gelten und dabei sehr weitreichende, jedoch nicht näher begründete, Ermächtigungen zur Datenverarbeitung erhalten.

NÖ Landeskliniken-Holding
Stattersdorfer Hauptstraße 6/C • 3100 St.Pölten
Tel.: +43 (0)2742 9009 • Fax: +43 (0)2742 9009-499 • office@holding.lknoe.at • www.lknoe.at
DVR Nr.: 2112072 • UID Nr.: ATU 619 43 838

Landeskliniken-Holding
IHRE GESUNDHEIT. UNSER ZIEL.

Die in gegenständlichem Begutachtungsentwurf getroffene Festlegung legt dabei die jeweiligen Zuständigkeiten der gemeinsamen Verantwortlichen im Hinblick auf die zu verarbeitenden Datenkategorien nicht ausreichend transparent dar. Die pauschale Ermächtigung zur Datenverarbeitung scheint zu weitreichend. Der Zugriff auf Informationen wie Ergebnisse von Einschauen, vorhandene Sicherheitsvorkehrungen und diesbezügliche Unterlagen eines Betreibers sollte im Rahmen des § 11 Abs 1 nur, sofern dies zur Aufgabenerfüllung nach § 4 und 5 des gegenständlichen Gesetzesentwurfes tatsächlich erforderlich ist, erfolgen dürfen.

Die Befugnis zur Auskunftseinholung bzw. die damit korrespondierende Verpflichtung von Betreibern wesentlicher Dienste (unverzüglich) Auskünfte zu erteilen (§ 10 Abs 3), sollte auf konkrete und vom Gesetzgeber zu definierende Anlassfälle beschränkt werden (z.B. Meldung von erheblichen Sicherheitsvorfällen) und insb. im Hinblick auf die betroffenen (zu übermittelnden) Datenkategorien jedenfalls spezifiziert werden.

Eine Determinierung des Begriffs „unverzügliche Auskunft“ nach § 10 Abs 3 bzw der „unverzüglichen Meldepflicht“ nach § 16 Abs 1 sollte getroffen werden und angemessene Fristen, jeweils unter Berücksichtigung des Regelbetriebes bzw der vorhandenen personellen Ressourcen des jeweiligen Sektors, vorgesehen werden.

Der Bundesminister für Inneres soll gemäß § 11 Abs 3 des gegenständlichen Entwurfs zudem eine Doppelfunktion (einerseits als gemeinsamer Verantwortlicher im Sinne des Art 26 DSGVO, andererseits als Auftragsverarbeiter im Sinne des Art 28 DSGVO) wahrnehmen. Der Gesetzesentwurf lässt im Dunkeln, in Hinblick auf welche Datenkategorien/Verarbeitungszwecke die jeweilige datenschutzrechtliche Rolle übernommen wird, zumal ein gemeinsam Verantwortlicher iSd Art 26 DSGVO zeitgleich nicht auch Auftragsverarbeiter iSd Art 4 Z 8 DSGVO sein kann.
Ferner soll eine Klarstellung der datenschutzrechtlichen Rollen der anderen Beteiligten insb. NIS-Büros, Computer-Notfallteams (vgl. § 12 Abs 7) erfolgen.

NÖ Landeskliniken-Holding
Stattersdorfer Hauptstraße 6/C • 3100 St.Pölten
Tel.: +43 (0)2742 9009 • Fax: +43 (0)2742 9009-499 • office@holding.lknoe.at • www.lknoe.at
DVR Nr.: 2112072 • UID Nr.: ATU 619 43 838

Landeskliniken-Holding
IHRE GESUNDHEIT. UNSER ZIEL.

Die weitreichende Übermittlungsbefugnis von Daten durch die NIS-Büros oder den Bundesminister für Landesverteidigung an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspolizei, ua. an Gerichte, Staatsanwaltschaften, Datenschutzbehörde sowie an sonstige in- und ausländische Behörden oder Stellen, soweit dies zur Aufgabenerfüllung erforderlich ist, scheint sehr überschießend.

Datenübermittlungen bzw. Konsultationen von anderen Behörden sollten lediglich im konkreten Anlassfall, welcher vom Gesetzgeber definiert werden sollte (z.B. erheblicher Sicherheitsvorfall unter Angabe der konkreten Parameter für dessen Beurteilung) und nur dann erfolgen, wenn es zur Erfüllung der übertragenen Aufgaben tatsächlich unbedingt erforderlich ist.

Konsultationen mit anderen Behörden sollten zudem nur dann personenbezogen bzw auf den einzelnen Betreiber wesentlicher Dienste rückverfolgbar erfolgen, sofern die Zweckerfüllung nicht auch mit anonymisierten bzw pseudonymisierten Daten erreicht werden kann, zumal die NIS-RILI an mehreren Stellen den Schutz der Vertraulichkeit der Meldungen sowie der Identität der Betreiber wesentlicher Dienste oder der Anbieter digitaler Dienste vorsieht (siehe z.B. ErwG 33 und 41).

Wenn der Verdacht besteht, dass ein Sicherheitsvorfall im Zusammenhang mit schweren kriminellen Handlungen steht, so sollten die nationalen Behörden die Betreiber wesentlicher Dienste dazu anhalten, diese Sicherheitsvorfälle den entsprechenden Strafverfolgungsbehörden zu melden. Die Letztentscheidung muss jedoch dem Betreiber wesentlicher Dienste selbst überlassen bleiben. Dies gilt insb. auch im Zusammenhang mit etwaigen Meldungen nach Art 33 DSGVO an die Datenschutzbehörde, zumal selbst das Vorliegen eines Sicherheitsvorfalles nach § 3 Z 6 des gegenständlichen Gesetzesentwurfes nicht zwingend gleichzusetzen ist mit dem Vorliegen eines „data breaches“ und der damit zusammenhängenden „data breach notification“ nach Art 33 DSGVO.

NÖ Landeskliniken-Holding
Stattersdorfer Hauptstraße 6/C • 3100 St.Pölten
Tel.: +43 (0)2742 9009 • Fax: +43 (0)2742 9009-499 • office@holding.lknoe.at • www.lknoe.at
DVR Nr.: 2112072 • UID Nr.: ATU 619 43 838

Landeskliniken-Holding
IHRE GESUNDHEIT. UNSER ZIEL.

Zu § 12:

Die Kosten für die Einrichtung bzw Aufrechterhaltung der Betriebskontinuität eines etwaigen sektorenspezifischen Computer-Notfallteams sind aus Sicht der NÖ Landeskliniken-Holding vom Bund zu tragen.

Zu § 14:

Bei der Ermittlung von Betreibern wesentlicher Dienste sollte berücksichtigt werden, dass es möglich ist, dass Einrichtungen in den in § 2 Abs 1 genannten Sektoren sowohl wesentliche als auch nicht wesentliche Dienste erbringen können. Betreiber wesentlicher Dienste sollten den spezifischen Sicherheitsanforderungen nur in Bezug auf die als wesentlich geltenden Dienste unterworfen werden (ErwG 22 NIS-RILI).

Im Bereich der öffentlichen Gesundheitsversorgung bzw. der Krankenanstalten sollte daher ausschließlich die Notfallversorgung vom Begriff des „wesentlichen Dienstes“ umfasst werden.

Durch die vorgesehene Einrichtung einer Kontaktstelle (§ 14 Abs 3 des gegenständlichen Begutachtungsentwurfes), welche jedenfalls in jenem Zeitraum erreichbar sein muss, in dem der wesentliche Dienst zur Verfügung gestellt wird, trifft der nationale Gesetzgeber strengere Anforderungen als in der NIS-RILI vorgesehen.

Sollte aus Sicht des Gesetzgebers (im Bereich der Krankenanstalten) damit die Bereitstellung einer 24/7 Kontaktstelle als erforderlich erachtet werden, wird dies erhebliche personelle und finanzielle Ressourcen erfordern.

Zu § 15:

Die mit den erst durch Verordnung zu spezifizierenden Sicherheitsanforderungen verbundenen Mehrkosten sowie die Kosten, die aufgrund der regelmäßigen Nachweispflicht (z.B. durch Zertifizierungen) entstehen, können aufgrund fehlender Konkretisierungen in gegenständlichem Begutachtungsentwurf nicht abschließend beurteilt werden. Es ist jedoch ein beträchtlicher finanzieller Aufwand zu erwarten.

Die Einschau in Netz- und Informationssysteme und diesbezügliche Unterlagen zur Kontrolle der Einhaltung der Sicherheitsanforderungen sollte nach entsprechender Ankündigung durch den Bundesminister für Inneres und ohne Einschränkung des Betriebsablaufes erfolgen.

NÖ Landeskliniken-Holding
Stattersdorfer Hauptstraße 6/C • 3100 St.Pölten
Tel.: +43 (0)2742 9009 • Fax: +43 (0)2742 9009-499 • office@holding.lknoe.at • www.lknoe.at
DVR Nr.: 2112072 • UID Nr.: ATU 619 43 838

Landeskliniken-Holding
IHRE GESUNDHEIT. UNSER ZIEL.

Da sich Betreiber wesentlicher Dienste zur Erfüllung ihre Pflichten zur Sicherstellung der Netz- und Informationssicherheit oftmals auch (technischer) Dienstleister bedienen, sollte das Gesetz im Hinblick auf die Einhaltung der Sicherheitsanforderungen auch Dienstleister umfassen.
Die Dienstleister sollte eine Mitwirkungs- bzw Unterstützungspflicht bei der Überprüfung der vorgeschriebenen Sicherheitsmaßnahmen nach § 15 Abs 1 des gegenständlichen Entwurfes treffen und das Auditrecht des Bundesministers sich auch auf diese erstrecken.

Eine Ausfertigung dieser Stellungnahme wird unter einem auch dem Präsidium des Nationalrates übermittelt.

Mit der Bitte um Berücksichtigung der obenstehenden Anregungen, verbleibe ich

mit freundlichen Grüßen,

M a g . E r i k a M e i n o l f e . h .
Abteilungsleiterin Recht und Personal

NÖ Landeskliniken-Holding
Stattersdorfer Hauptstraße 6/C • 3100 St.Pölten
Tel.: +43 (0)2742 9009 • Fax: +43 (0)2742 9009-499 • office@holding.lknoe.at • www.lknoe.at
DVR Nr.: 2112072 • UID Nr.: ATU 619 43 838