Niedersächsisches Ministerium
für Inneres und Sport

Nds. Ministerium für Inneres und Sport, Postfach 2 21, 30002 Hannover

HK2 Rechtsanwälte
Herrn Rechtsanwalt Bartels
Hausvogteiplatz 11A
10117 Berlin

ausschließlich per E-Mail: bartels@hk2.eu

Bearbeitet von: [redacted]

Ihr Zeichen, Ihre Nachricht vom	Mein Zeichen (Bei Antwort angeben)	Durchwahl Nr. (05 11) 1·20-	Hannover,
20.12.2023	[redacted]	[redacted]	03.01.2024

Umsetzung der NIS-2-Richtlinie/ Fragen zum Gesetzgebungsstand
Ihr Schreiben vom 20.12.2023

Sehr geehrter Herr Rechtsanwalt Bartels,

vielen Dank für Ihr Schreiben vom 20.12.2023, auf das ich wie folgt antworten möchte.

Frage 1: Bestehen bereits Landesgesetze, welche den europäischen Umsetzungsvorgaben der NIS-2-Richtlinie genügen? Bejahendenfalls: in welchem Gesetz bzw. welchen Gesetzen sind diese zu finden?

Die Umsetzung der NIS-2-Richtlinie obliegt aufgrund der Gesetzgebungskompetenzordnung des Grundgesetzes im Wesentlichen dem Bund. Der Entwurf eines NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) befindet sich nach hiesiger Kenntnis weiterhin in der Ressortabstimmung auf Bundesebene. Die Länder wurden bislang nicht formal nach § 47 der Gemeinsamen Geschäftsordnung der Bundesministerien beteiligt, hatten jedoch Gelegenheit, zu dem Diskussionspapier des Bundesministeriums des Innern und für Heimat vom 27.09.2023 Stellung zu nehmen.

Dienstgebäude/
Paketanschrift
Lavesallee 6
30169 Hannover

Telefon
0511 120-0
Telefax
0511 120-6550

E-Mail
poststelle@mi.niedersachsen.de

Bankverbindung
IBAN: DE43 2505 0000 0106 0353 55
BIC: NOLA DE 2H

Bezüglich einiger Vorgaben der NIS-2-Richtlinie verfügt der Bund über keine Gesetzgebungskompetenz. Daher sind die Länder gefordert, Regelungen zu treffen, um eine vollständige Umsetzung durch die Bundesrepublik Deutschland zu gewährleisten. Dies gilt insbesondere mit Blick auf Art. 2 Abs. 2 Buchst. f) Ziffer ii), Art. 2 Abs. 5, Art. 7 Abs. 1, Art. 8 Abs. 1 und Art. 10 Abs. 1 der NIS-2-Richtlinie.

Nach Art. 41 Abs. 1 der NIS-2-Richtlinie müssen die Mitgliedstaaten die erforderlichen Vorschriften zur Umsetzung der Richtlinie bis zum 17.10.2024 erlassen. Gemäß Art. 288 Abs. 3 AEUV sind die Mitgliedstaaten bei der Umsetzung von Richtlinien in der Wahl der Form und Mittel grundsätzlich frei. Die Art und Weise der Umsetzung hängt insbesondere von den konkreten Vorgaben der jeweiligen Richtlinie ab. Die Wahl des Regulierungstyps muss geeignet sein, das von der Richtlinie verfolgte Ziel verbindlich zu erreichen. Dabei muss die Umsetzung Mindeststandards an Bestimmtheit und Publizität genügen.

Mit dem Niedersächsischen Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) verfügt Niedersachsen bereits seit 2019 über einen modernen Rechtsrahmen. Behörden, die das Landesdatennetz betreiben oder an das Landesdatennetz angeschlossen sind, sind zu einem umfassenden Informationssicherheitsmanagement verpflichtet. Zudem wurde mit dem NDIG die Zentralstelle für Informationssicherheit eingeführt.

Da sich die konkreten Umsetzungsverpflichtungen der Länder ausschließlich auf die unmittelbaren Landesverwaltungen auswirken werden und sich keine Individualansprüche aus der Umsetzung ergeben werden, wird in Niedersachsen eine Umsetzung durch einen gemeinsamen Runderlass der Staatskanzlei und aller Ministerien avisiert. Verwaltungsvorschriften sind abstrakt-generelle Regelungen innerhalb der Verwaltungsorganisation und ohne unmittelbare Außenwirkung, welche von übergeordneten Verwaltungsinstanzen an nachgeordnete Behörden bzw. Bedienstete ergehen und dazu dienen, Organisation und Handeln der Verwaltung (vorliegend insbesondere Norminterpretation und -konkretisierung) zu bestimmen. Der Entwurf dieses Runderlasses befindet sich noch in der internen Abstimmung.

Frage 2: Bestehen verneinendenfalls Pläne zur Einführung oder Überarbeitung entsprechender IT-Sicherheitsvorschriften, um den Umsetzungsvorgaben zu genügen? Soweit vorhanden: welcher Zeitplan unterliegt der Planung? Bitte übersenden/ verlinken Sie bestehende Gesetzesentwürfe.

Es wird auf die Beantwortung der Frage 1 verwiesen. Eine Anpassung des NDIG ist derzeit nicht vorgesehen. Der Runderlass muss spätestens am 17.10.2024 in Kraft getreten sein. Hieran orientiert sich der Zeitplan.

Frage 3: Bestehen bereits Vorschriften bzw. sind solche geplant, welche die Umsetzungsvorgaben der NIS-2-Richtlinie auf Einrichtungen der kommunalen Verwaltung sowie Bildungseinrichtungen erstrecken, wie es Art. 2 Abs. 5 lit. a und b der NIS-2-Richtlinie optional vorsieht? Welche Vorschriften sind das bejahendenfalls? Warum werden diese Bereiche ggf. nicht reguliert?

Der IT-Planungsrat Bund/ Länder hat in seiner 42. Sitzung am 03.11.2023 folgenden Beschluss gefasst (2023/39):
„Er nimmt den Sachstandsbericht der AG Informationssicherheit zur Kenntnis und bittet die Länder und den Bund, von der Option, den Anwendungsbereich der NIS-2-Richtlinie auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen zu erstrecken, keinen Gebrauch zu machen."

Die Cyberbedrohungslage ist auch für Kommunen auf einem anhaltend hohen Niveau. Dies zeigen die bereits erfolgreichen Cyberangriffe auf kommunale Einrichtungen. Die betroffenen Kommunen waren zum Teil über Monate nicht vollständig arbeitsfähig. Der IT-Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik 2023 hebt hervor, dass im aktuellen Berichtszeitraum monatlich durchschnittlich zwei Kommunalverwaltungen oder kommunale Betriebe als Opfer von Ransomware-Angriffen bekannt wurden.[1]

Die NIS-2-Richtlinie adressiert jedoch ganz vorrangig Unternehmen. Ziel der Richtlinie ist die Harmonisierung des Binnenmarktes.[2] Dies wird auch dadurch deutlich, dass Einrichtungen der öffentlichen Verwaltung nur sehr fragmentiert in den Anwendungsbereich einbezogen werden. So

---

[1] Die Lage der IT-Sicherheit in Deutschland 2023, *BSI*, Seite 68.
[2] Richtlinie (EU) 2022/2555, u. a. Erwägungsgrund 3

werden ausschließlich die obersten Bundesbehörden sowie Landesbehörden nach risikobasierter Bewertung von Art. 2 Abs. 2 Buchst. f) NIS-2-Richtlinie erfasst.

Der Beschluss des IT-Planungsrates Bund/ Länder ist rechtlich und fachlich nicht zu beanstanden. Niedersachsen wird von der fakultativen Einbeziehung der Kommunalverwaltungsebene sowie der Hochschulen daher dem Beschluss folgend keinen Gebrauch machen.

Der Betrieb der IT sowie die IT-Sicherheit sind Teil der Organisationshoheit der Kommunen und damit Ausprägung des kommunalen Selbstverwaltungsrechts, vgl. Art. 57 Abs. 1 Niedersächsische Verfassung. Ein Eingriff auf Grundlage einer „kann"-Regelung i. S. d. Art. 2 Abs. 5 NIS-2-Richtlinie wäre daher verfassungsrechtlich nicht unbedenklich. Zudem besteht bereits eine Vielzahl an rechtlich bindenden Vorgaben, aus denen auch die Kommunen verpflichtet sind, eine angemessene Informationssicherheit sicherzustellen. Neben speziellen Anforderungen aus Nutzungsbedingungen und vertraglichen Beziehungen zu Dritten ist jede Behörde insbesondere auf Grundlage datenschutzrechtlicher Anforderungen zum Schutz personenbezogener Daten nach Art. 24 und 25 DSGVO i. V. m. Art. 32 DSGVO verpflichtet, eben solche Maßnahmen zu ergreifen. Der Niedersächsische Landesrechnungshof sieht eine Verpflichtung ebenso aus Art. 20 Abs. 3 GG.[3]

Die beschlossene und empfohlene Nicht-Einbeziehung der Kommunalverwaltungsebene bezieht sich zudem lediglich auf Einrichtungen der öffentlichen Verwaltung, also Einrichtungen, die nicht am Markt teilnehmen. Sowohl kommunale Unternehmen als auch kommunale Eigenbetriebe werden in den Anwendungsbereich der Richtlinie fallen, sofern sie in einem der Sektoren des Anhangs I und II der NIS-2-Richtlinie tätig sind (u. a. Energie, Verkehr, Gesundheitswesen, Trinkwasser, Abwasser und Abfallwirtschaft) und die sog. Size-Cap-Rule erfüllen (mind. 50 Beschäftigte und/ oder mind. 10 Mio. Euro Jahresumsatz). Ein wesentlicher Teil der kritischen Aufgaben der Daseinsvorsorge einer Kommune wird dadurch von Cybersicherheitsmindestanforderungen betroffen sein. Diese Einrichtungen werden über Bundesrecht reguliert. Dies entspricht der derzeitigen Rechtslage, sofern Kommunen Kritische Infrastrukturen betreiben.

Niedersachsen setzt in bewährter Art auf eine kooperative Zusammenarbeit mit den Kommunen. Dies gilt beispielsweise mit Blick auf die seit Juni 2022 angebotenen kostenfreien Cybersicherheitsanalysen, mit deren Hilfe ermittelt werden kann, ob die bereits getroffenen Schutzmaßnahmen eine ausreichende Widerstandsfähigkeit gegen Cyber-Angriffe gewährleisten. Das Angebot wird auch im Jahr 2024 fortgesetzt.

---

[3] *Niedersächsischer Landesrechnungshof*, Kommunalbericht 2023, Kapitel 3.9, S. 67.

Nähere Informationen finden Sie unter:
https://www.mi.niedersachsen.de/startseite/themen/it_bevollmachtigter_der_landesregierung/cybersicherheit/cybersicherheit-150587.html

Die Ausführungen gelten in entsprechender Anwendung auch für die Hochschulen.

Gesetzliche Vorgaben können dabei helfen, die Informationssicherheit in den Kommunen und bei den Hochschulen zu erhöhen. Hierfür ist die NIS-2-Richtlinie jedoch nicht das richtige Instrumentarium.

Sollten Sie Rückfragen zu der Beantwortung Ihrer Fragen haben, stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen
Im Auftrage

[redacted] Digital unterschrieben
Datum: 2024.01.03
11:42:47 +01'00'