Stellungnahme
der Bundesärztekammer

zum Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)

Berlin, 04.07.2025

Korrespondenzadresse:

Bundesärztekammer
Herbert-Lewin-Platz 1
10623 Berlin

1. Grundlegende Bewertung des Gesetzesentwurfs

Das Regelungsvorhaben ist aus Sicht der Bundesärztekammer sinnvoll und mit Blick auf das laufende Vertragsverletzungsverfahren der EU-Kommission gegen die Bundesrepublik Deutschland überfällig. Anforderungen an die Cybersicherheit sind nicht nur für das Vertrauensverhältnis von Patientinnen und Patienten zu den Tätigen in den Gesundheitseinrichtungen von Bedeutung, sondern auch für das Gemeinwesen mit Blick auf eine hinreichende Krisenresilienz und den Erhalt der Funktionsfähigkeit der Gesundheitsversorgung. Daher sollten angemessene technische und organisatorische Maßnahmen – auch unabhängig von den allgemeinen Pflichten zur Datensicherheit aus dem Datenschutzrecht – von den Gesundheitseinrichtungen getroffen werden.

Mit Blick auf den Anwendungsbereich des geplanten BSIG-E ist aber eine Doppelregulierung für Arztpraxen und MVZ hinsichtlich verschiedener Verpflichtungen im Kontext der IT-Sicherheit zu erwarten, weil diese dann sowohl die Anforderungen nach BSIG als auch nach der IT-Sicherheitsrichtlinie der KBV gem. § 390 SGB V zu erfüllen hätten. Das löst zusätzliche Prüf- und Dokumentationspflichten aus.

Nicht zuletzt im Interesse eines Bürokratieabbaus wird daher eine Ausnahmeregelung für § 390 SGB V in Artikel 21 des vorliegenden Referentenentwurfs vorgeschlagen, wie sie für Krankenhäuser bereits in § 391 Abs. 5 SGB V existiert.

2. Stellungnahme im Einzelnen

Anwendungsbereich des BSIG

§ 28 BSIG-E

A) Beabsichtigte Neuregelung

§ 28 BSIG-E regelt den Anwendungsbereich des BSIG für Einrichtungen, die bestimmte Anforderungen der IT-Sicherheit zu erfüllen haben (§§ 30 ff. BSIG-E). Der Anwendungsbereich des BSIG-E umfasst neben den bestehenden Betreibern kritischer Anlagen (KRITIS) künftig auch die sog. besonders wichtigen sowie die wichtigen Einrichtungen. „Besonders wichtige Einrichtungen“ im Sektor Gesundheit sind Unternehmen ab 250 Mitarbeitern oder Unternehmen über 50 Mio. EUR Umsatz und Bilanz über 43 Mio. EUR. „Wichtige Einrichtungen“ im Sektor Gesundheit sind Unternehmen ab 50 Mitarbeitern oder Unternehmen über 10 Mio. EUR Umsatz und Bilanz über 10 Mio. EUR. Im Sektor Gesundheit sind neben EU-Referenzlaboratorien, die Medizinforschung im Bereich von Arzneimitteln sowie Hersteller von Pharmazeutika und von Medizinprodukten vor allem Gesundheitsdienstleister i.S.d. Art. 3 lit. g RL 2011/24/EU erfasst. Gesundheitsdienstleister ist jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt (Art. 3 lit. g RL 2011/24/EU).

B) Stellungnahme der Bundesärztekammer

Mit der Erweiterung des Anwendungsbereichs des BSIG sind – je nach Größe des Unternehmens – neben größeren Unternehmen im Gesundheitswesen auch mittlere Unternehmen, wie MVZ oder Arztpraxen als Gesundheitsdienstleister i.S.d. Art. 3 lit. g RL 2011/24/EU erfasst. Unternehmen, die diese Werte nicht erreichen, unterfallen dem BSIG-E nicht. Mit Blick auf die Empfehlung der EU-Kommission 2003/361/EG betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, auf die auch der BSIG-E referenziert, dürften kleine Unternehmen und Kleinstunternehmen im Gesundheitswesen nicht dem Anwendungsbereich des BSIG-E unterfallen.

Schätzungen zufolge unterfallen ca. 1.000 zusätzliche Einrichtungen aus dem Gesundheitswesen dem erweiterten Anwendungsbereich des BSIG-E, davon 800 MVZ und 200 Berufsausübungsgemeinschaften. Damit sind nicht mehr nur Krankenhäuser einer bestimmten Größenordnung als kritische Anlagen vom BSIG-E erfasst. Sofern größere Arztpraxen oder MVZ künftig den Anforderungen des BSIG unterfallen, müssen sie neben den neuen Anforderungen nach BSIG-E zugleich weiterhin die Anforderungen der IT-Sicherheitsrichtlinie der KBV gem. § 390 SGB V erfüllen. Die Folge der Doppelregulierung wäre ein zusätzlicher Prüfungs- und ein doppelter Dokumentationsaufwand.

Im Interesse einer Bürokratieentlastung sollte eine solche Doppelregulierung unterbleiben.

C) Änderungsvorschlag der Bundesärztekammer

In Artikel 21 des Entwurfs sollte eine Änderung von § 390 SGB V aufgenommen werden. § 390 Absatz 6 Satz 2 SGB V sollte dabei wie folgt geändert werden:

„(6) Die Richtlinie ist nicht anzuwenden für an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmende Leistungserbringer, die als besonders wichtige Einrichtungen und wichtige Einrichtungen im Sinne des § 28 BSIG ohnehin organisatorische und technische Vorkehrungen nach dem BSIG zu treffen haben, und für die vertragsärztliche und vertragszahnärztliche Versorgung im Krankenhaus, soweit dort bereits angemessene Vorkehrungen nach § 391 getroffen werden.“

Begründung:

Da Regelungen im SGB V infolge des BSIG-E ohnehin redaktionell anzupassen sind (s. Art. 21 des vorliegenden Entwurfs), wäre eine sinnvolle Regelung im SGB V möglich, indem dort nach dem Vorbild von § 391 Abs. 5 SGB V eine Ausnahmeregelung aufgenommen wird. Es wäre ein Ausnahmetatbestand in § 390 SGB V zu verankern, wonach die IT-Sicherheitsrichtlinie der KBV für an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer nicht verpflichtend ist, soweit die Praxis oder MVZ ohnehin bereits Anforderungen nach dem BSIG erfüllen muss.