Stellungnahme des AOK-Bundesverbandes zur Verbändebeteiligung des BMI

zum Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

AOK-Bundesverband
Rosenthaler Str. 31
10178 Berlin
Tel: 030 34646-2299
info@bv.aok.de

AOK-Bundesverband
Die Gesundheitskasse.

Der AOK-Bundesverband ist registrierter Interessenvertreter i. S. d. Lobbyregistergesetzes

Inhaltsverzeichnis

I. Zusammenfassung ... 3

II. Stellungnahme zu einzelnen Regelungen ... 5

Artikel 1 Änderung des BSI-Gesetz – BSIG ... 5

§ 2 BSIG Begriffsbestimmungen ... 5

§ 30 BSIG Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen ... 7

§ 31 BSIG Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen ... 8

§ 32 BSIG Meldepflichten ... 9

§ 35 BSIG Unterrichtungspflichten ... 10

§ 56 BSIG Ermächtigung zum Erlass von Rechtsverordnungen ... 11

Artikel 8 Änderung BSI-KritisV ... 12

§ 7 BSI-KritisV und neu § 8 BSI-KritisV ... 12

III. Zusätzlicher Änderungsbedarf aus Sicht des AOK-Bundesverbandes ... 13

I. Zusammenfassung

Die Anpassung der deutschen Cybersicherheitsgesetzgebung an die europäische NIS2-Richtlinie wird durch den AOK-Bundesverband grundsätzlich begrüßt und als notwendiger Schritt betrachtet. Die Stärkung der Resilienz gegenüber Cyberbedrohungen ist von entscheidender Bedeutung für die Sicherheit des Landes und seiner kritischen Infrastrukturen.

Der vorliegende Referentenentwurf des NIS2-Umsetzungsgesetzes weist in seiner aktuellen Form allerdings konzeptionelle Mängel auf. Diese führen zu einer Doppelregulierung, erhöhter Bürokratie und gefährden die effiziente und sichere Erbringung von Versorgungsdienstleistungen. Für gesetzliche Kranken- und Pflegekassen, die den Schwellenwert gemäß BSI-Kritis-Verordnung überschreiten, besteht durch die Vorgaben im SGB (§ 217f Abs. 4c, 4d SGB V, § 392 SGB V, § 103a SGB XI) bereits eine Doppelregulierung. Zusätzlich zur Nachweisführung gegenüber dem BSI nach BSIG besteht gemäß § 217f Abs. 4d SGB V eine jährliche Berichtspflicht an das Bundesministerium für Gesundheit über den GKV-Spitzenverband.

Im Sinne des im Koalitionsvertrag verankerten Ziels, Bürokratie zu reduzieren, sollte diese Doppelregulierung abgeschafft und die damit verbundenen Nachweis- und Berichtspflichten reduziert sowie vereinheitlicht werden. Statt einer dringend notwendigen gesetzliche Harmonisierung schafft der Entwurf jedoch eine Parallelstruktur zu bestehenden Regelwerken.

Zudem fehlt es dem Entwurf an einer klaren Abgrenzung oder einer sinnvollen Integration bestehender Pflichten. Es ist zu prüfen, ob die Umsetzung der Anforderungen aus unterschiedlichen Standards widerspruchsfrei möglich ist. Die Breite der geforderten Standards bei Ausschreibungen und Vorhaben lässt befürchten, dass es zu einer erheblichen Markteinengung bis hin zur völligen Lähmung kommen könnte. Es sind Konstellationen denkbar, in denen unterschiedliche Standards parallel Anwendung finden müssten.

Um das Potenzial des NIS2UmsuCG vollständig zu nutzen und eine substanzielle Stärkung der Cybersicherheit zu gewährleisten, ohne unverhältnismäßige Belastungen zu verursachen, ist eine Nachjustierung des Referentenentwurfs daher erforderlich. Die folgenden Aspekte sind dabei von herausgehobener Relevanz:

- Eine konsequente Harmonisierung bestehender Gesetze, wobei nationale Umsetzungsspielräume konsequent genutzt werden sollten, um eine Doppelregulierung zu vermeiden und effiziente Meldewege zu etablieren.
- Definitionen und Prozessen präzise, objektiv und praxistauglich bei deren Einführung gestalten, damit sie die operativen Realitäten der betroffenen Akteure widerspiegeln.

Die Beteiligung der Betroffenen sorgt für Feedback und Praxistauglichkeit. Dies sollte durch die Einbeziehung der Wirtschaft und Branchenverbände bei Verordnungsermächtigungen sowie bei der Ausgestaltung von Detailregelungen, wo Spielräume vorhanden sind, erfolgen.

II. Stellungnahme zu einzelnen Regelungen

Artikel 1 Änderung des BSI-Gesetzes – BSIG

§ 2 BSIG Begriffsbestimmungen

A Beabsichtigte Neuregelung

In § 2 des Entwurfs des NIS2UmsuCG werden eine Reihe von Begriffen definiert, die für die Anwendung des Gesetzes von zentraler Bedeutung sind. Dazu gehören u. a. *Beinahevorfall*, *erhebliche Cyberbedrohung* und *erheblicher Sicherheitsvorfall*.

B Stellungnahme

Die Qualifizierung dieser Begriffe erfolgt maßgeblich durch Begriffe wie *beinahe* oder *erheblich*, ohne dass diese näher konkretisiert oder objektive Kriterien für ihre Bewertung festgelegt werden.

Die unpräzise Formulierung birgt dementsprechend zu hohe Risiken bei der einheitlichen und rechtssicheren Auslegung des Gesetzes. Zudem wird auf nachfolgende (zum Teil noch fehlende) Rechtsverordnungen verwiesen.

- Rechtsunsicherheit: Die unspezifischen Definitionen können zu Unsicherheiten bei der Auslegung und Umsetzung der Meldepflichten und der zu ergreifenden Sicherheitsmaßnahmen führen. Gesetzliche Krankenkassen sind wesentliche Einrichtungen im Gesundheitssektor und unterliegen bereits einer Vielzahl spezifischer regulatorischer Anforderungen. Um konsistent und gesetzeskonform agieren zu können, ist hier eine klare und eindeutige Definition unerlässlich.
- Inkonsistenz: Ohne eindeutige, sachliche Maßstäbe besteht das Risiko einer inkonsistenten Umsetzung durch die einzelnen Vertreter der gesetzlichen Krankenkassen sowie einer uneinheitlichen Interpretation durch die Aufsichtsbehörden. Dadurch werden Vergleichbarkeit, Koordination und die Einhaltung eines einheitlichen Sicherheitsniveaus erschwert.
- Herausforderung: In der Praxis erfordert die Entscheidung, ob es sich um einen meldepflichtigen erheblichen Sicherheitsvorfall oder einen Beinahevorfall handelt, eine schnelle und eindeutige Einschätzung. Unklare Definitionen können dazu führen, dass das BSI sowie die meldenden Stellen überlastet werden, da es zu unnötigen oder falschen Meldungen kommt. Ebenso kann es passieren, dass relevante Vorfälle nicht oder verspätet gemeldet werden, was die gesamtstaatliche Lageübersicht beeinträchtigt.

C Änderungsvorschlag

Es wird dringend empfohlen, den Einsatz bzw. die Notwendigkeit der Begriffe aus § 2 zu überprüfen. Es erscheint fraglich, welchen Mehrwert die Definition eines Beinahevorfalls in diesem Kontext hat. Andere Begriffe wie *erhebliche Cyberbedrohung*

und *erheblicher Sicherheitsvorfall* sowie alle ähnlichen unbestimmten Rechtsbegriffe sollten präzisiert und mit objektiven, nachvollziehbaren Kriterien unterlegt werden.

- Vorschlag: Damit es nicht zu unterschiedlichen Auslegungen kommt, sollte man die Erheblichkeit an konkrete, messbare Kriterien binden. Dazu gehören insbesondere folgende Punkte:
    - Anzahl der betroffenen Personen, Systeme oder Datenbestände: Festlegung von Schwellenwerten (z. B. „mehr als X Versicherte betroffen", „Ausfall von mehr als Y % der IT-Systeme").
    - Dauer der Dienstunterbrechung: Angabe von Mindestdauern für die Erheblichkeit (z. B. „Dienstausfall von über X Stunden")
    - Finanzieller Schaden: Festlegung von monetären Schwellenwerten (z. B. „geschätzter finanzieller Schaden über X Euro" oder Y % vom jährlichen Umsatz).

§ 30 BSIG Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

A Beabsichtigte Neuregelung

Gemäß § 30 des Entwurfs des NIS2UmsuCG sind die zentralen technischen und organisatorischen Maßnahmen zum Risikomanagement der Cybersicherheit für besonders wichtige und wichtige Einrichtungen festgelegt. Dies bildet den Kern der präventiven Pflichten, die aus der NIS2-Richtlinie in nationales Recht überführt werden.

In Absatz 2 ist ein Maßnahmenkatalog definiert. Die darin aufgeführten Maßnahmen müssen den Stand der Technik einhalten, einschlägige europäische und internationale Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz basieren.

B Stellungnahme

Die aufgeführten Maßnahmen erweisen sich als teilweise widersprüchlich, sodass eine Anpassung erforderlich ist. Gemäß § 30 Abs. 2 Nr. 5 werden das Management und die Offenlegung von Schwachstellen gefordert. Aus den vorliegenden Informationen lässt sich nicht ableiten, welche Schwachstellen von wem offengelegt werden.

C Änderungsvorschlag

a.) In § 30 Abs. 2 Nr. 5: Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, ~~einschließlich Management und Offenlegung von Schwachstellen~~

b.) In § 30 Abs. 2 Nr. 5: Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen *(+ zusätzlich einer Klarstellung, wer Schwachstellen offenlegen muss)*

§ 31 BSIG Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

A Beabsichtigte Neuregelung

§ 31 des Entwurfs des NIS2UmsuCG legt für Betreiber kritischer Anlagen zusätzliche und spezifisch erhöhte Anforderungen an die Risikomanagementmaßnahmen fest, die über die allgemeinen Pflichten aus § 30 hinausgehen.

Gemäß Absatz 2 sind Betreiber kritischer Anlagen dazu verpflichtet, für die maßgeblichen IT-Systeme, Komponenten und Prozesse ihrer kritischen Anlagen Systeme zur Angriffserkennung einzusetzen.

B Stellungnahme

Hier erfolgt eine unscharfe Verwendung von unterschiedlichen Begriffen. Gemäß dem Wortlaut in § 31 Abs. 2 sind die Systeme zur Angriffserkennung einzusetzen. Zwischen den Begriffen Angriff und Bedrohung existiert in der IT-/Informationssicherheit ein begründeter Unterschied bzw. Zusammenhang.

Ein Angriff im Sinne der Cybersicherheit beschreibt eine konkrete und aktive Handlung, die darauf abzielt, die Schutzziele von Prozessen, Daten oder Systemen zu beeinträchtigen. Es handelt sich um die Durchführung einer potenziell schädigenden Aktion.

Im Gegensatz dazu stellt eine Bedrohung eine potenzielle Ursache für einen unerwünschten Vorfall dar. Diese kann in der Folge dazu führen, dass Prozessen, Daten oder Systemen Schaden zugefügt wird. Sie ist eine Gegebenheit oder Möglichkeit, die eine Schwachstelle ausnutzen könnte, aber selbst noch keine aktive Handlung.

C Änderungsvorschlag

[…] Sie sollten dazu in der Lage sein, fortwährend ~~Bedrohungen~~ *sicherheitsrelevante Ereignisse* zu identifizieren und *Angriffe* zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. […]

§ 32 BSIG Meldepflichten

A Beabsichtigte Neuregelung

§ 32 des Entwurfs regelt das Verfahren zur Meldung von erheblichen Sicherheitsvorfällen an eine zentrale Meldestelle. In der Regel umfasst dies eine initiale Meldung innerhalb einer kurzen Frist (z. B. 24 Stunden), eine aktualisierte Meldung mit weiteren Details (z. B. innerhalb von 72 Stunden) sowie einen abschließenden Bericht nach Behebung des Vorfalls (z. B. innerhalb eines Monats).

B Stellungnahme

Gemäß § 32 wird das vorgegebene Meldeverfahren der NIS2-Richtlinie definiert. Es besteht demnach kein Änderungsbedarf im vorliegenden Kontext. Die unklaren Begriffsbestimmungen in § 2 zur Definition eines erheblichen Sicherheitsvorfalls werfen jedoch weiterhin Fragen auf. Eine präzisere Definition ist unerlässlich, um eine einheitliche Auslegung und Anwendung der Meldepflichten in der Praxis zu gewährleisten und unnötige Meldungen ebenso wie das Übersehen relevanter Vorfälle zu vermeiden.

C Änderungsvorschlag

Kein wesentlicher Änderungsbedarf.

§ 35 BSIG Unterrichtungspflichten

A Beabsichtigte Neuregelung

§ 35 des Entwurfs regelt die Pflicht wichtiger und besonders wichtiger Einrichtungen, die Nutzer ihrer Dienste oder die Öffentlichkeit sowohl über erhebliche Sicherheitsvorfälle als auch erhebliche Cyberbedrohungen zu unterrichten. Dies umfasst verschiedene Informationen über die Beeinträchtigung und mögliche Auswirkungen, die getroffenen oder beabsichtigten Gegenmaßnahmen sowie gegebenenfalls Empfehlungen für die betroffenen Personen. Die Unterrichtungspflichten gelten dabei unverzüglich und sind an den Interessen von Sender und Empfänger auszurichten.

B Stellungnahme

Die in § 35 vorgesehenen Unterrichtungspflichten sind für die gesetzlichen Krankenkassen von immenser Bedeutung. In ihrer aktuellen Form bergen sie jedoch erhebliche Herausforderungen:

- Kommunikationsaufwand: Für die Bereitstellung von Informationen zu einer erheblichen Cyberbedrohung wurden keine Angaben zum Kommunikationsmedium gemacht. Adressaten der Meldungen sind die Diensteempfänger der gesetzlichen Krankenkassen. Hier besteht eine sehr große Heterogenität. Zusätzlich muss eine Abwägung der Interessen von Sender und Empfänger durchgeführt werden. Die logistische und finanzielle Herausforderung, diese große Anzahl von Personen angemessen, sicher und verständlich zu informieren (z. B. per Post oder über sichere digitale Kanäle), ist enorm. Dabei muss die Art der Kommunikation dem sensiblen Charakter Rechnung tragen.

C Änderungsvorschlag

Für die Sicherstellung von effizienten und praktikablen Unterrichtungspflichten nach § 35 werden folgende Änderungen und Klarstellungen vorgeschlagen:

- Streichung § 35 Absatz 2, Unterrichtungspflicht bei Cyberbedrohungen: Die Pflicht zur Unterrichtung der Diensteempfänger bei erheblichen Cyberbedrohungen sollte aus dem Gesetz gestrichen werden. In der Regel sollten Informationen über Bedrohungen an klar definierte, objektive Schwellenwerte und Kriterien gekoppelt sein, die über die Erheblichkeit einer Cyberbedrohung hinausgehen und konkrete Risiken für die Betroffenen abbilden. Da diese Kriterien einem ständigen Wandel unterliegen, ist eine Umsetzung kaum möglich. Gleichzeitig steigt der Kommunikationsumfang mit den Versicherten und die Gefahr der Überbeanspruchung.

§ 56 BSIG Ermächtigung zum Erlass von Rechtsverordnungen

A Beabsichtigte Neuregelung

Gemäß § 56 ist das Bundesministerium des Innern (BMI) dazu ermächtigt, durch verschiedene Rechtsverordnungen zahlreiche detaillierte Regelungen zum NIS2UmsuCG zu erlassen. Dies umfasst unter anderem:

- Absatz 1: […]
- Absatz 2: […]
- Absatz 3: […]
- Absatz 4: Festlegung, welche Anlagen als kritische Anlagen im Sinne des Gesetzes gelten, basierend auf Sektoren sowie branchenspezifischen Schwellenwerten
- Absatz 5: […]
- Absatz 6: […]

B Stellungnahme

Die Ermächtigungen des BMI zum Erlass von Rechtsverordnungen gemäß § 56 sind in ihrer aktuellen Ausgestaltung zu weitreichend, intransparent und bergen erhebliche praktische Risiken für die Empfänger bzw. regulierten Einrichtungen. Dies bereitet insbesondere den gesetzlichen Krankenkassen als besonders wichtigen Einrichtungen im Gesundheitssektor größte Sorgen.

- Gesetzgebungskompetenzen / fehlende Beteiligung: § 56 ermächtigt das BMI, zentrale Definitionen (z. B. erheblich in Abs. 5), Anwendungsbereiche (z. B. kritische Anlagen in Abs. 4) sowie konkrete Implementierungspflichten (z. B. zertifizierungspflichtige Produkte in Abs. 3) durch Rechtsverordnung festzulegen. Dies sind typischerweise Themen, die im Gesetz selbst oder zumindest in einer zustimmungspflichtigen Rechtsverordnung geregelt sein sollten. Die jetzige Regelung schafft jedoch eine unkontrollierbare Verordnungshoheit, die zu Überraschungen und unvorhersehbaren Belastungen für die Betroffenen führen kann. Eine weitergehende Regelung durch Rechtsverordnungen wird abgelehnt. Gemäß der Gesetzesbegründung, orientiert sich § 2 Nr. 24 an der Begriffsbestimmung aus § 1 Abs. 1 Nr. 3 BSI-KritisV. Die Schwellenwerte für die betroffenen Sektoren werden in der BSI-KritisV sowie den Anhängen 1-8 dargelegt.

C Änderungsvorschlag

Einführung in § 56 Abs. 4 […] *nach Anhörung von Vertretern der Wissenschaft, der betroffenen Unternehmen und der betroffenen Wirtschaftsverbände* […]

Artikel 8 Änderung BSI-KritisV

§ 7 BSI-KritisV und neu § 8 BSI-KritisV

A Beabsichtigte Neuregelung

Artikel 8 des NIS2UmsuCG passt die bestehende BSI-Kritisverordnung an die NIS2-Richtlinie an. Es werden einzelne Sektoren weiter aufgetrennt.

B Stellungnahme

Der Referentenentwurf sieht eine Auftrennung des bisherigen Sektors "Finanz- und Versicherungswesen" in die Sektoren "Finanzwesen" und "Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende" vor. Bei der Auftrennung sind einige Fehler unterlaufen.

C Änderungsvorschlag

- Art. 8 Nr. 3c: Der aktuelle Entwurf sieht vor, dass unter § 7 Abs. 1 Nr. 5 BSI-KritisV die Formulierung „Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende" als kritische Dienstleistung des Sektors „Finanzwesen" erhalten bleibt. Sie sollte jedoch analog zu § 7 Abs. 6 BSI-KritisV in den neu aufgenommenen § 8 „Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende" überführt werden.
- Art. 8 Nr. 5: Die durch Art. 8 Nr. 9c gestrichenen Inhalte zur Definition der Schwellenwerte sollten dem neu aufgenommenen § 8 „Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende" hinzugefügt werden, da es ansonsten für diesen Sektor keine Schwellenwertdefinition gibt.

III. Zusätzlicher Änderungsbedarf aus Sicht des AOK-Bundesverbandes

Gesetzesharmonisierung von BSIG und SGB V

Sachstand

Die Implementierung des NIS2UmsuCG resultiert in der Schaffung eines umfassenden, sektorübergreifenden Rechtsrahmens für Cybersicherheit. Das Ziel besteht darin, das Schutzniveau wichtiger und besonders wichtiger Einrichtungen zu erhöhen und eine einheitliche Basis zu schaffen. Gemäß der Regelung im § 59 BSIG wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zuständige Behörde für die wichtigen und besonders wichtigen Einrichtungen im Anwendungsbereich des Gesetzes benannt. Dies impliziert eine zentrale Rolle des BSI bei der Überwachung und Durchsetzung von Anforderungen und Regulierungen in der Cybersicherheit. Gemäß den Vorgaben im Sozialgesetzbuch (SGB), konkret in § 217f Abs. 4c, 4d SGB V, § 392 SGB V, § 393 SGB V und § 103a SGB XI, bestehen für gesetzliche Krankenkassen bereits umfangreiche Pflichten im Bereich der Cybersicherheit.

Änderungsbedarf und Begründung

Die Abstimmung von Gesetzen aus verschiedenen Bereichen ist von essenzieller Bedeutung, um Überschneidungen und Doppelregulierungen zu vermeiden. Eine einheitliche Gesetzgebung gewährleistet Rechtssicherheit und optimiert die Effizienz der Umsetzung und Kontrolle. In Bezug auf die Cybersicherheit erweist sich diese Abstimmung als von eminenter Wichtigkeit. Gemäß der Neuregulierung von § 59 BSIG wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Sicherheit wichtiger und besonders wichtiger Einrichtungen in Deutschland zuständig sein. Die Bündelung der Fachlichkeit muss sich in den Gesetzgebungsvorhaben widerspiegeln. Es ist von hoher Relevanz, die Konsistenz der Anforderungen zu gewährleisten, den bürokratischen Aufwand zu minimieren und die Cybersicherheit in Deutschland auf einem hohen Niveau zu gewährleisten. Eine fehlende Harmonisierung würde ansonsten zu Unsicherheiten bei der Umsetzung führen.

- Gemäß § 370a SGB V ist die Kassenärztliche Bundesvereinigung dazu ermächtigt, eine vom BMG genehmigte Verfahrensordnung zur Nutzung ihrer Dienste zu erlassen. Wenn die Krankenkassen die entsprechenden Dienste nutzen möchten, benötigen sie eine ISO-27001-Zertifizierung. Hierbei ergibt sich eine Doppelregelung, da Krankenkassen durch die Anforderungen zu „Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen“ den Stand der Technik inklusive des Betriebes eines ISMS bereits umsetzen müssen.
- Gemäß § 392 SGB V sind Krankenkassen zur Einhaltung des Stands der Technik verpflichtet. Dies gilt jedoch nicht, wenn sie unter die Regelung zu Risikomanagementmaßnahmen besonders wichtiger oder wichtiger Einrichtungen fallen. Unberührt bleibt dennoch die Regelung des § 392 SGB V Absatz 6,

nach den Krankenkassen ihre IT-Dienstleister zur Umsetzung des branchenspezifischen Sicherheitsstandards (B3S) verpflichten müssen. Diese Regelung im SGB V ist jedoch nicht mehr notwendig, da die Sicherheit in der Lieferkette durch § 30 (2) Nr. 4 BSIG bereits berücksichtigt wird.

- § 393 SGB V regelt analog zu § 392 SGB V die Verarbeitung von „Sozial- und Gesundheitsdaten im Wege des Cloud-Computing". Demnach müssen Krankenkassen ihre Dienstleister zum C5-Testat Typ 2 verpflichten und die Anwendung des B3S gewährleisten. Diese Regelung ist jedoch nicht erforderlich, da Krankenkassen, die unter die Regelung zu § 30 BSIG „Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen" fallen, den Stand der Technik ohnehin für sich selbst und ihre Lieferkette sicherstellen müssen.

Änderungsvorschlag

- Es wird darum gebeten, die Regelungen zu harmonisieren und sicherzustellen, dass Krankenkassen, die unter die NIS2-Regelungen fallen, die Voraussetzungen zur Nutzung der Dienste der Kassenärztlichen Bundesvereinigung (KBV) erfüllen.
- Ferner wird angestrebt, die Regelungen zur Verarbeitung von Sozial- und Gesundheitsdaten im Cloud-Computing zu harmonisieren, um Rechtssicherheit für Krankenkassen zu schaffen. Dies kann durch die Umsetzung der Vorgaben aus NIS2 erreicht werden.
- § 392 Absatz 6 SGB V sowie die sich daraus ergebende Berichtspflicht gemäß § 271f (4d) SGB V sollten gestrichen werden, da es sich dabei um eine Doppelregulierung handelt.