§ 103a

IT-Sicherheit der Pflegekassen

(1) Pflegekassen sind verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der jeweiligen Pflegekasse und die Sicherheit der verarbeiteten Versicherteninformationen maßgeblich sind.

(2) Organisatorische und technische Vorkehrungen nach Absatz 1 sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der Arbeitsprozesse der Pflegekasse oder der Sicherheit der verarbeiteten Versicherteninformationen steht.

(3) Die Pflegekassen erfüllen die Verpflichtungen nach Absatz 1, insbesondere indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Pflegekassen in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.

(4) [1] Die Pflegekassen sind verpflichtet, repräsentiert durch ihre Verbände und den Spitzenverband der Pflegekassen, in einem gemeinsam bestehenden oder zu schaffenden Branchenarbeitskreis an der Entwicklung des branchenspezifischen Sicherheitsstandards für die informationstechnische Sicherheit der Pflegekasse im Sinne des Absatzes 3 mitzuwirken. [2] Die Pflegekassen, repräsentiert durch ihre Verbände und den Spitzenverband der Pflegekassen, haben darauf hinzuwirken, dass der branchenspezifische Sicherheitsstandard auch Vorgaben enthält zu

1. **geeigneten Maßnahmen zur Erhöhung der Cybersecurity-Awareness,**
2. **dem Einsatz von Systemen zur Angriffserkennung, die geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten, wobei diese dazu in der Lage sein sollten, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen (Maßnahmen zur Aufrechterhaltung der Betriebskontinuität),**
3. **an IT-Dienstleister zu stellende Sicherheitsanforderungen gemäß Absatz 6, sofern diese Leistungen für die Pflegekassen zur Wahrnehmung ihrer gesetzlichen Aufgaben erbringen.**

(5) Die Verpflichtung nach Absatz 1 gilt für alle Pflegekassen, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene organisatorische und technische Vorkehrungen zu treffen haben.

(6) Sofern eine Pflegekasse im Rahmen ihrer Aufgabenerfüllung IT-Dienstleistungen eines Dritten in Anspruch nimmt und eine Störung der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse des Dritten zu einer Beeinträchtigung der Funktionsfähigkeit der jeweiligen Pflegekasse oder der Sicherheit der verarbeiteten Versicherteninformationen führen kann, so muss die Pflegekasse durch geeignete vertragliche Vereinbarungen sicherstellen, dass die Einhaltung des branchenspezifischen Sicherheitsstandards im Sinne des Absatzes 3 durch den Dritten gewährleistet wird.

(7) [1] Der Spitzenverband der Pflegekassen legt bis einschließlich 30. Juni 2024 den branchenspezifischen Sicherheitsstandard im Sinne des Absatzes 3 in der jeweils aktuellen Fassung als Richtlinie zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse der Pflegekassen für diese verbindlich fest. [2] Die Richtlinie ist jährlich an die jeweils aktuelle Fassung des branchenspezifischen Sicherheitsstandards anzupassen.

(8) [1] Der Spitzenverband der Pflegekassen berichtet dem Bundesministerium für Gesundheit und den anderen zuständigen Aufsichtsbehörden der Pflegekassen erstmals bis zum 31. De-

zember 2024 und danach jährlich über den aktuellen Stand der Umsetzung der Vorgaben der Richtlinie im Sinne des Absatzes 7. [2] Dabei ist für jede Pflegekasse gesondert darzustellen, ob die Vorgaben der Richtlinie im Sinne des Absatzes 7 umgesetzt und welche Maßnahmen hierzu im Einzelnen ergriffen wurden.

Begründung zum Digital-Gesetz zum Einfügen von § 103a:

Die fortschreitende Digitalisierung eröffnet neue Potenziale und Synergien entlang der medizinischen Versorgungsprozesse im Gesundheitswesen und der Pflege. Gleichzeitig wächst jedoch auch das Bedrohungspotenzial durch zunehmend zielgerichtete, technologisch ausgereiftere und komplexere Angriffe. Solche Cyberangriffe richten sich nicht mehr nur gegen die unmittelbaren Leistungserbringer, sondern auch zunehmend gegen Kranken- und Pflegekassen und deren IT-Dienstleister. Aufgrund der zentralen Stellung der gesetzlichen Kranken- und Pflegekassen im Rahmen der sachlichen und finanziellen Leistungsgewährung und aufgrund der hohen Schutzbedürftigkeit der in diesem Zusammenhang vorgehaltenen und verarbeiteten Daten, besteht für die bei den Pflegekassen eingesetzten informationstechnischen Systeme ein besonders hohes Schadenspotential. Sofern sich die Pflegekassen im Rahmen ihrer Aufgabenwahrnehmung IT-Dienstleistern bedienen, besteht für die dortigen IT-Systeme ein gleichsam hohes Schadenspotential. Die bestehenden Regelungen zur verbindlichen Umsetzung risikominimierender IT-Schutzmaßnahmen im Bereich der vertragsärztlichen und vertragszahnärztlichen Versorgung gemäß § 390 SGB V und zur Stärkung der IT-Sicherheit in den Krankenhäusern gemäß § 391 SGB V sowie der IT-Sicherheit der gesetzlichen Krankenkassen gemäß § 392 SGB V sind daher um Regelungen zur Stärkung der IT-Sicherheit der Pflegekassen und deren IT-Dienstleister zu ergänzen.

Mit dem neuen § 103a werden auch solche Pflegekassen, die nicht Gegenstand der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Kritisverordnung – BSI-KritisV) sind, verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der jeweiligen Pflegekasse und die Sicherheit der verarbeiteten Versicherteninformationen maßgeblich sind.

Pflegekassen sollen hierzu den Branchenspezifischen Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer - „B3S-GKV/PV“- anwenden, der im Rahmen des Branchenarbeitskreises „Gesetzliche Kranken- und Pflegeversicherungen“ des Umsetzungsplans Kritis (UP KRITIS) entwickelt wurde und im Rahmen dieses Arbeitskreises aktiv weiterentwickelt wird. Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, ihren Verbänden und den zuständigen staatlichen Stellen, so auch für die Gesetzlichen Kranken- und Pflegeversicherungen. Die fachliche Eignung der aktuellen Version des B3S-GKV/PV wurde gemäß § 8a Absatz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt. Die Eignungsprüfung nach § 8a Absatz 2 BSIG findet seitens des BSI für jede neue Version des B3S gesondert statt.

Die Pflegekassen sind verpflichtet, an der inhaltlichen Weiterentwicklung des B3S-GKV/PV, vertreten durch ihre Verbände auf Bundesebene und den Spitzenverband der Pflegekassen, im Rahmen des Branchenarbeitskreises „Gesetzliche Kranken- und Pflegeversicherungen“ des Umsetzungsplans Kritis (UP KRITIS) mitzuwirken. Zu den insoweit adressierten Verbänden der Pflegekassen auf Bundesebene gehören unter anderem der AOK-Bundesverband, der BKK Dachverband, der IKK e.V., der SVLFG sowie der vdek. Entsprechend der grundlegenden Organisationsstruktur des UP KRITIS steht weiteren Akteuren die Mitgliedschaft in dem Branchenarbeitskreis auf freiwilliger Basis offen.

Im Rahmen der inhaltlichen Weiterentwicklung des bestehenden B3S-GKV/PV durch den Branchenarbeitskreis Gesetzliche Kranken- und Pflegeversicherungen des UP KRITIS sind die Pflegekassen, vertreten durch ihre Verbände auf Bundesebene und den Spitzenverband der Pflegekassen, dazu verpflichtet, auf die Aufnahme bestimmter Mindestinhalte hinzuwirken, wozu insbesondere Maßnahmen zur Aufrechterhaltung der Betriebskontinuität gehören, sowie an IT-Dienstleister zu stellende Mindestanforderungen bezüglich der Cybersicherheit deren informationstechnischer Systeme.

Sollten sich Pflegekassen im Rahmen der Wahrnehmung ihrer ihnen gesetzlich zugewiesenen Aufgaben Dritter bedienen, so sind sie verpflichtet, aufgrund des zuvor skizzierten Bedrohungspotentials auch für deren informationstechnischen Systeme vertragliche Vereinbarungen zu treffen, die eine verbindliche Umsetzung des B3S-GKV/PV auch durch diese Dienstleister sicherstellt.

Die Absätze 7 und 8 stellen klar, dass der Spitzenverband der Pflegekassen die jeweils aktuelle Fassung des B3S-GKV/PV für die Pflegekassen im Rahmen einer Richtlinie jährlich verbindlich festlegt. Zudem berichtet er dem Bundesministerium für Gesundheit und den jeweiligen Aufsichtsbehörden der einzelnen Pflegekassen über den Umsetzungsstand der Richtlinie, sodass erforderlichenfalls durch die zuständigen Behörden aufsichtsrechtliche Maßnahmen bei Verstößen gegen die Verpflichtung aus Absatz 1 ergriffen werden können.

Die bereits bestehende und vom BSI im Sinne des § 8a Absatz 2 BSIG bestätigte Version des B3S-GKV/PV wird durch den Spitzenverband der Pflegekassen erstmals zum 30. Juni 2024 im Wege einer Richtlinie für alle gesetzlichen Pflegekassen verbindlich festgelegt.
Die Richtlinie wird mindestens jährlich angepasst und hierbei inhaltlich überprüft: Sofern zwischenzeitlich eine neue inhaltliche Fassung des B3S-GKV/PV durch den BAK GKV/PV verabschiedet und das BSI bestätigt wurde, so setzt der Spitzenverband der Pflegekassen diese Aktualisierung im Wege des Erlasses einer entsprechend inhaltlich aktualisierten Richtlinie verbindlich für die Pflegekassen um.
Die Berichtspflichten des Spitzenverband der Pflegekassen gegenüber dem Bundesministerium für Gesundheit und den jeweiligen zuständigen Aufsichtsbehörden der jeweiligen Pflegekassen soll neben einer umfassenden Analyse der Umsetzung auch dazu dienen, den jeweils zuständigen Aufsichtsbehörden der Pflegekassen erforderlichenfalls die Ergreifung aufsichtsrechtlicher Mittel zu ermöglichen.
Um der strukturell vergleichbar gelagerten Gemengelage mit Blick auf die informationstechnischen Systeme der Krankenkassen und deren IT-Dienstleistern stringent zu begegnen, sieht dieses Gesetz mit der Einführung des neuen § 392 und der Ergänzung des § 217f Fünftes Buch Sozialgesetzbuch – der nahezu inhaltsgleichen Verpflichtungen an die Krankenkassen adressiert - eine ganzheitliche Strategie zur Risikominimierung vor.

Der 14. Ausschuss begründet die Änderungen wie folgt:

Es handelt sich um eine redaktionelle und eine rechtssystematische Folgeänderung, die sich aus der Rechtsprüfung ergeben.