Referentenentwurf

Bundesministerium für Gesundheit

C5-Äquivalenz-Verordnung

A. Problem und Ziel

Die digitale Transformation des Gesundheitswesens und der Pflege hat ein herausragendes Potential für eine effizientere, qualitativ hochwertige und patientenzentrierte gesundheitliche und pflegerische Versorgung. Eine Grundvoraussetzung für die vertrauensvolle Nutzung digitaler Anwendungen stellt hierbei die Gewährleistung der Cybersicherheit dar.

Da sich nicht zuletzt aufgrund des Angriffskrieges Russlands gegen die Ukraine die abstrakten Cybersicherheitsrisiken erhöht haben, wurden mit dem Digital-Gesetz für die Einrichtungen im Gesundheitswesen die Anforderungen zur Steigerung der Resilienz der eingesetzten informationstechnischen Systeme verbessert.

Insbesondere der Einsatz cloudbasierter Informationssysteme bietet auch im Gesundheitswesen erhebliche Vorteile. Sofern damit personenbezogene Gesundheits- / oder Sozialdaten verarbeitet werden sollen, besteht ein gesonderter Schutzbedarf. Mit dem durch das Digital-Gesetz neu eingeführten § 393 des Fünften Buches Sozialgesetzbuch (SGB V) wurde daher der durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte „Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)“ als verpflichtend einzuhaltender Sicherheitsmaßstab für das Gesundheitswesen festgelegt.

Durch die Testierung eines Cloud-Computing-Dienstes nach dem C5-Standard wird sichergestellt, dass bei der Verarbeitung besonders schützenswerter Daten mithilfe von cloudbasierten Informationssystemen definierte Mindestanforderungen erfüllt werden.

Nach § 393 Absatz 4 Satz 3 SGB V darf eine Verarbeitung von personenbezogenen Gesundheits-/oder Sozialdaten auch ohne ein C5-Testat erfolgen, soweit für die im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die Cloud-Technik anstelle eines aktuellen C5-Testats ein Testat oder Zertifikat nach einem Standard vorliegt, dessen Befolgung ein im Vergleich zum C5-Standard vergleichbares oder höheres Sicherheitsniveau sicherstellt.

B. Lösung

Mit dieser Rechtsverordnung nimmt das Bundesministerium für Gesundheit im Einvernehmen mit dem BSI die Ermächtigung zum Erlass einer klarstellenden Rechtsverordnung nach § 393 Absatz 4 Satz 3 SGB V in Anspruch.

Indem für eine Übergangszeit der Nachweis der Einhaltung eines zum C5-Kriterienkatalog äquivalenten Sicherheitsniveaus durch alternative Zertifikate und Testate erbracht werden kann, wird den Herstellern und Anbietern von cloud-basierten informationstechnischen Systemen eine stufenweise Migration der internen Sicherheitskontrollen auf den C5-Standard ermöglicht. Zugleich werden die Anforderung an die Nachweiserbringung eines gleichwertigen Sicherheitsniveaus auch für die Fallgruppen beschrieben, in denen einzelne Basiskriterien des C5-Kriterienkatalogs nicht per se durch alternative Standards adressiert werden. Dies schafft zugleich Rechtssicherheit über die individuelle Beurteilung, welche Nachweise

zur Dokumentation der Einhaltung eines vergleichbaren oder höheren Sicherheitsniveaus im Vergleich zu einer C5-Typ1-Testierung geeignet sind.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

a) Bund

Keine.

b) Länder

Keine.

c) Sozialversicherung

Keine.

E. Erfüllungsaufwand

Keiner.

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Durch die Inanspruchnahme der Rechtsverordnungskompetenz entstehen keine zusätzlichen Kosten, da die Regelungen keine ergänzenden Pflichten darstellen, sondern zeitlich befristet aufwandsmindernd alternative Zertifikate und Testate gegenüber einem C5-Typ1-Testat als Nachweismöglichkeit festlegt. Der Handlungsspielraum der Unternehmen wird durch die Rechtsverordnung erweitert, nicht verengt.

Der geringfügige, jedoch nicht quantifizierbare Erfüllungsaufwand für die Wirtschaft im Rahmen der Durchführung einer Testierung nach dem eigentlichen C5-Kriterienkatalog wurde bereits im Rahmen des Digital-Gesetzes erfasst.

Davon Bürokratiekosten aus Informationspflichten

Keine.

E.3 Erfüllungsaufwand der Verwaltung

Für den Bund und die Länder entsteht kein Erfüllungsaufwand. Erfüllungsaufwände für die Verwaltung wurden bereits im Rahmen des Digital-Gesetzes erfasst. Durch die

Inanspruchnahme der Rechtsverordnungskompetenz entstehen keine darüberhinausgehenden Aufwände.

F. Weitere Kosten

Keine.

Referentenentwurf des Bundesministeriums für Gesundheit

C5-Äquivalenzverordnung

([…]V)

Vom ...

Auf Grund des § 393 Absatz 4 Satz 3 des Fünften Buches Sozialgesetzbuch, der durch Artikel 2 Nummer 6 des Gesetzes vom 22. März 2024 (BGBl. I Nr. 101) eingefügt wurde, verordnet das Bundesministerium für Gesundheit im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik:

§ 1

Nachweise, die geeignet sind, die Einhaltung eines Sicherheitsniveaus zu dokumentieren, das mit einer Typ1-Testierung nach dem C5-Kriterienkatalog vergleichbar ist

(1) Eine Testierung oder Zertifizierung eines Cloud-Computing-Dienstes nach einem nachfolgend aufgezählten Standard gilt als Nachweis der Einhaltung eines zu einem Typ1-Testat nach dem Kriterienkatalog C5 des Bundesamtes für Sicherheit in der Informationstechnik gleichwertigen Sicherheitsniveaus im Sinne des § 393 Absatz 4 Satz 3 des Fünften Buches Sozialgesetzbuch, sofern die ergänzenden Voraussetzungen der Absätze 2 bis 3 erfüllt sind:

1. DIN EN ISO/IEC 27001:2022

2. ISO 27001 auf der Basis von IT-Grundschutz durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)

3. Cloud Controls Matrix Version 4.0

(2) Ergänzend zu dem bestehenden Testat oder Zertifikat muss für einen Cloud-Computing-Dienst ein Maßnahmenplan vorliegen, der mindestens folgendes enthält:

1. eine Dokumentation, die sich an den einzelnen Basiskriterien des C5-Kriterienkatalogs ausrichtet und diejenigen Basiskriterien hervorhebt, die materiell nicht durch das bestehende Testat oder Zertifikat zugrundeliegenden Standard abgedeckt werden,

2. eine Dokumentation der individuellen technischen und organisatorischen Vorkehrungen, die ergriffen werden, um die unter Nummer 1 gekennzeichneten materiellen Lücken zwischen den Anforderungen des C5-Kriterienkatalogs und den Anforderungen des alternativen Standards zu beheben,

3. eine Meilensteinplanung, aus der hervorgeht, bis wann die einzelnen Vorkehrungen nach Nummer 2 derart umgesetzt sein sollen, dass die unter Nummer 1 gekennzeichneten materiellen Lücken zu den Anforderungen der Basiskriterien des C5-Kriterienkatalogs behoben sind; hierbei darf ein Zeitraum von zwölf Monaten ab der Erstellung der Meilensteinplanung nicht überschritten werden und

4. eine Dokumentation von Maßnahmen zur Erlangung eines C5-Typ-1-Testats für den Cloud-Computing-Dienst innerhalb von 18 Monaten ab Erstellung der

Meilensteinplanung; hierunter fallen auch vertragliche Vereinbarungen mit einem Auditor zur Durchführung eines C5-Typ-1-Audits oder die Aufnahme von Vertragsverhandlungen hierzu.

(3) Der Maßnahmenplan nach Absatz 2 und das Testat oder Zertifikat sind dem Leistungserbringer nach dem Vierten Kapitel des Fünften Buches Sozialgesetzbuch, der einen Cloud-Computing-Dienst beauftragt, sowie dessen zuständiger Aufsichtsbehörde zur Einsichtnahme vorzuhalten.

§ 2

Inkrafttreten

Diese Verordnung tritt mit Wirkung vom 1. Juli 2024 in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

§ 393 des Fünften Buches Sozialgesetzbuch (SGB V) setzt im Grundsatz den durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelten „Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)“ als verpflichtend einzuhaltenden Sicherheitsmaßstab für die Verarbeitung personenbezogener Gesundheits- / oder Sozialdaten durch cloudbasierte Informationssysteme im Gesundheitswesen fest.

Abweichend hiervon darf nach § 393 Absatz 4 Satz 3 SGB V eine Verarbeitung von personenbezogenen Gesundheits-/oder Sozialdaten übergangsweise auch ohne ein C5-Testat erfolgen, soweit für die im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die Cloud-Technik anstelle eines aktuellen C5-Testats ein Testat oder Zertifikat nach einem Standard vorliegt, dessen Befolgung ein im Vergleich zum C5-Standard vergleichbares oder höheres Sicherheitsniveau sicherstellt.

Mit dieser Rechtsverordnung nimmt das Bundesministerium für Gesundheit im Einvernehmen mit dem BSI die Ermächtigung zum Erlass einer klarstellenden Rechtsverordnung nach § 393 Absatz 4 Satz 3 SGB V in Anspruch und legt fest, welche Standards in Kombination mit ergänzenden Maßnahmen die Einhaltung eines vergleichbaren Sicherheitsniveaus sicherstellen.

Für eine Übergangszeit soll so Unternehmen eine Nachweismöglichkeit anhand alternativer Zertifizierungs- oder Testierungsschemata ermöglicht werden; letztlich soll jedoch auf Sicht eine Testierung nach dem C5-Kriterienkatalog eine maßgebliche Voraussetzung für eine cloudbasierte Verarbeitung von personenbezogenen Gesundheits-/oder Sozialdaten im Gesundheitswesen darstellen.

II. Wesentlicher Inhalt des Entwurfs

Eine Testierung oder Zertifizierung eines Cloud-Computing-Dienstes nach einem durch diesen Verordnungsentwurf festgelegten Standard gilt als Nachweis der Einhaltung eines zu einem Typ1-Testat nach dem Kriterienkatalog C5 des Bundesamtes für Sicherheit in der Informationstechnik gleichwertigen Sicherheitsniveaus, sofern die ebenfalls benannten ergänzenden Voraussetzungen eingehalten werden.

Für eine Übergangszeit wird so der Handlungsspielraum von Unternehmen erhöht, bis zu dem der Testierungsprozess nach dem C5-Kriterienkatalog durchlaufen werden konnte.

III. Alternativen

Keine.

IV. Regelungskompetenz

Die Ermächtigung zum Erlass dieser Rechtverordnung folgt aus § 393 Absatz 4 Satz 3 des Fünften Buches Sozialgesetzbuch.

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und mit völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar.

VI. Regelungsfolgen

1. Rechts- und Verwaltungsvereinfachung

Entfällt.

2. Nachhaltigkeitsaspekte

Der Verordnungsentwurf folgt entsprechend der Fassung vom 07. Oktober 2021 den Leitgedanken der Bundesregierung zur Berücksichtigung der Nachhaltigkeit, indem zur Stärkung von Lebensqualität und Gesundheit der Bürgerinnen und Bürger sowie zu sozialem Zusammenhalt und gleichberechtigter Teilhabe an der wirtschaftlichen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie beigetragen wird.

Mit dem Verordnungsentwurf werden weitere notwendigen Maßnahmen zur Sicherheit der Digitalisierung des Gesundheitswesens fortgeführt. Eine Verbesserung der Cybersicherheit dient dem Schutz der Verfügbarkeit informationstechnischer Systeme, die für die Gesundheitsversorgung unerlässlich sind. Die Verfügbarkeit und Sicherheit digital-gestützter Behandlungsmöglichkeiten dient der weiteren qualitativen Verbesserung und Sicherstellung der medizinischen und pflegerischen Versorgung der Menschen.

Der Verordnungsentwurf wurde unter Berücksichtigung der Prinzipien der nachhaltigen Entwicklung im Hinblick auf die Nachhaltigkeit geprüft. Hinsichtlich seiner Wirkungen entspricht er insbesondere den Zielen 3 (Gesundheit und Wohlergehen) und 9 (Industrie, Innovation und Infrastruktur) der Deutschen Nachhaltigkeitsstrategie, indem ein gesundes Leben für alle Menschen jeden Alters gewährleistet und ihr Wohlergehen sowie Innovationen gefördert werden. Damit wird die Umsetzung der Deutschen Nachhaltigkeitsstrategie weiter unterstützt.

3. Haushaltsausgaben ohne Erfüllungsaufwand

a) Bund

Keine.

b) Länder

Keine.

c) Sozialversicherung

Keine.

4. Erfüllungsaufwand

Keiner.

Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

Erfüllungsaufwand für die Wirtschaft

Durch die Inanspruchnahme der Rechtsverordnungskompetenz entstehen keine zusätzlichen Kosten, da die Regelungen keine ergänzenden Pflichten darstellen, sondern zeitlich befristet aufwandsmindernd alternative Zertifikate und Testate gegenüber einem C5-Typ1-Testat als Nachweismöglichkeit festlegt. Der Handlungsspielraum der Unternehmen wird durch die Rechtsverordnung erweitert, nicht verengt.

Der geringfügige, jedoch nicht quantifizierbare Erfüllungsaufwand für die Wirtschaft im Rahmen der Durchführung einer Testierung nach dem eigentlichen C5-Kriterienkatalog wurde bereits im Rahmen des Digital-Gesetzes erfasst.

Davon Bürokratiekosten aus Informationspflichten

Keine.

Erfüllungsaufwand der Verwaltung

Für den Bund und die Länder entsteht kein Erfüllungsaufwand. Erfüllungsaufwände für die Verwaltung wurden bereits im Rahmen des Digital-Gesetzes erfasst. Durch die Inanspruchnahme der Rechtsverordnungskompetenz entstehen keine darüberhinausgehenden Aufwände.

Durch die Inanspruchnahme der Rechtsverordnungskompetenz entstehen keine zusätzlichen Kosten, da die Regelungen keine ergänzenden Pflichten darstellen, sondern zeitlich befristet aufwandsmindernd alternative Zertifikate und Testate gegenüber einem C5-Typ1-Testat als Nachweismöglichkeit festlegt. Der Handlungsspielraum der Unternehmen wird durch die Rechtsverordnung erweitert, nicht verengt.

Der geringfügige, jedoch nicht quantifizierbare Erfüllungsaufwand für die Wirtschaft im Rahmen der Durchführung einer Testierung nach dem eigentlichen C5-Kriterienkatalog wurde bereits im Rahmen des Digital-Gesetzes erfasst.

5. Weitere Kosten

Keine.

6. Weitere Regelungsfolgen

Auswirkungen von gleichstellungspolitischer Bedeutung sind nicht zu erwarten. Die in dem Regelungsentwurf vorgesehenen Maßnahmen leisten vor dem Hintergrund der zunehmenden Alterung und Multimorbidität der Gesellschaft mit der Sicherstellung der Verfügbarkeit, Integrität und Vertraulichkeit informationstechnischer Systeme zum sektorenübergreifenden Datenaustauschs einen Beitrag, die Leistungsfähigkeit des Gesundheitssystems auch in Zukunft sicherzustellen und die Versorgungsqualität zu erhöhen.

VII. Befristung; Evaluierung

§ 1 Absatz 2 Nummer 4 des Entwurfs enthält eine materielle Befristung auf Tatbestandsebene. Diese unterstreicht das grundsätzliche Anliegen des Verordnungsgebers, den in § 393 Absatz 3 und 4 SGB V enthaltenen Grundsatz einer Testierung eines Cloud-Computing-Dienstes nach dem C5-Kriterienkatalog zu erwirken.

B. Besonderer Teil

Zu § 1 (Nachweise, die geeignet sind, die Einhaltung eines Sicherheitsniveaus zu dokumentieren, das mit einer Typ1-Testierung nach dem C5-Kriterienkatalog vergleichbar ist)

Zu Absatz 1

Absatz 1 legt fest, welche Standards in Kombination mit ergänzenden Maßnahmen die Einhaltung eines zum C5-Kriterienkatalog vergleichbaren Sicherheitsniveaus sicherstellen.

Zu Absatz 2

Absatz 2 setzt die Notwendigkeit fest, neben einer Zertifizierung oder Testierung nach einem Standard nach Absatz 1 Nummer 1 bis 3 einen Maßnahmenplan zu erstellen. Das Vorliegen des Maßnahmenplans ist notwendig, weil andernfalls aus fachlicher Sicher von keiner materiellen Vergleichbarkeit der Anforderungen der in Absatz 1 genannten Standards zu den Anforderungen des C5-Kriterienkatalogs ausgegangen werden kann.

Dementsprechend ist zwingender Bestandteil des Maßnahmenplans zunächst die Dokumentation einer Betrachtung derjenigen Basiskriterien des C5-Kriterienkatalogs, die nicht durch den jeweiligen Standard nach Absatz 1 abgedeckt sind (vgl. Absatz 2 Nummer 1).

Sodann sind diejenigen individuellen technischen und organisatorischen Vorkehrungen, die ergriffen werden, um die unter Nummer 1 gekennzeichneten materiellen Lücken zwischen den Anforderungen des C5-Kriterienkatalogs und den Anforderungen des alternativen Standards zu beheben, zu dokumentieren (vgl. Absatz 2 Nummer 2).

Auf Basis der in Nummer 1 und Nummer 2 getroffenen Erkenntnisse ist sodann eine Meilensteinplanung zu erstellen, aus der hervorgeht, bis wann die einzelnen Vorkehrungen nach Nummer 2 derart umgesetzt sein sollen, dass die unter Nummer 1 gekennzeichneten materiellen Lücken zu den Anforderungen der Basiskriterien des C5-Kriterienkatalogs behoben sind (Mitigation-Plan).

Da der durch die Rechtsverordnung skizzierte Mechanismus einen Übergangsweg hin zu einer Testierung nach dem C5-Kriterienkatalog darstellt, sind zudem als weiteres verbindliches Element des Maßnahmenplans nach Absatz 2 Nummer 4 alle Maßnahmen zu dokumentieren, die der schlussendlichen Erlangung einer C5-Testierung dienen. Teil hiervon können auch vertragliche Vereinbarungen mit Wirtschaftsprüfergesellschaften zur Durchführung einer Testierung nach dem C5-Kriterienkatalog sein. Auch die Dokumentation von Vertragsanbahnungen zum Abschluss einer entsprechenden Vereinbarung sind ausreichend. Die im Zusammenhang mit Absatz 2 Nummer 4 bestehende Frist von 18 Monaten gilt ab der erstmaligen Erstellung der Meilensteinplanung.

Erst ab der Erstellung der Meilensteinplanung mitsamt allen Pflichtinhalten nach Absatz 2 soll – gemeinsam mit der erfolgreichen Zertifizierung/Testierung nach einem Standard nach Absatz 1 – von einem einheitlichen gleichwertigen Nachweis zu einer Testierung nach dem C5-Kriterienkatalog ausgegangen werden.

Zu Absatz 3

Der Maßnahmenplan nach Absatz 2 und das Testat oder Zertifikat sind dem Leistungserbringer nach dem Vierten Kapitel des Fünften Buches Sozialgesetzbuch, der einen Cloud-Computing-Dienst beauftragt, sowie dessen zuständiger Aufsichtsbehörde zur Einsichtnahme vorzuhalten.

Zu § 2 (Inkrafttreten)

Das rückwirkende Inkrafttreten der Verordnung zum 1. Juli 2024 ist zulässig und auch zweckmäßig. Vorliegend handelt es sich um eine rückwirkende, privilegierende Regelung. Durch das rückwirkende Inkrafttreten werden nachträglich zum gleichen Zeitpunkt, zu dem nach § 393 Absatz 4 Satz 1 in Verbindung mit Absatz 3 Nummer 2 ein C5-Typ1-Testat vorliegen musste, weitere, alternative Zertifizierungen und Testierungen als gleichwertig anerkannt.

Ein rückwirkendes Inkrafttreten ist auch zweckmäßig, da die getroffenen Regelungen einen stufenweisen Übergang zu einem C5-Testat ermöglichen und zugleich die Rechtssicherheit für Unternehmen, die cloud-basierte Informationstechnische Systeme im Gesundheitswesen vertreiben, erhöhen.