
Deutsche Industrie- und Handelskammer

Stellungnahme

Referentenentwurf der C5-Äquivalenz-Verordnung

Wir bedanken uns bei dem Bundesministerium für Gesundheit für die Gelegenheit zur Stellungnahme zu dem o. g. Entwurf.

Grundlage dieser Stellungnahme sind die der DIHK bis zur Abgabe der Stellungnahme zugegangenen Äußerungen der IHKs sowie die wirtschaftspolitischen Positionen der DIHK. Sollten der DIHK noch weitere in dieser Stellungnahme noch nicht berücksichtigte relevante Äußerungen zugehen, wird die DIHK diese Stellungnahme entsprechend ergänzen.

A. Das Wichtigste in Kürze

Der im „Gesetz zur Beschleunigung der Digitalisierung im Gesundheitswesen“ (Digital-Gesetz) eingeführte §393 SGB V („Cloudeinsatz im Gesundheitswesen“) legt den vom Bundesamt für Sicherheit und Informationsstandard (BSI) entwickelten Kriterienkatalog C5 als verpflichtend einzuhaltenden IT-Sicherheitsstandard an Cloud-Computing-Dienste für die Verarbeitung von Sozial- und Gesundheitsdaten fest. Hierunter fallen z. B. Cloud-Anbieter, deren Kunden (u.a. Einrichtungen und Leistungserbringer des ambulanten und stationären Sektors oder Kranken- und Pflegekassen) bzw. Dienstleister, die im Auftrag Sozial- und Gesundheitsdaten prozessieren, sind.

Nach § 393 Abs. 4 Satz 3 SGB V kann eine Datenverarbeitung auch ohne C5-Testat erfolgen, sofern ein Zertifikat oder Testat vorliegt, dessen Standard ein gleichwertiges oder höheres Sicherheitsniveau als der C5-Standard sicherstellt.

Die DIHK begrüßt grundsätzlich das Ziel des Verordnungsentwurfes, klarzustellen, welche Anforderungen Hersteller und Anbieter von Cloud-Computing-Diensten im Gesundheitswesen erfüllen müssen, damit gewährleistet ist, dass die Verarbeitung personenbezogener Gesundheits- und Sozialdaten in einer Cloud dem Standard des C5-Kriterienkataloges entspricht oder ein höheres Sicherheitsniveau sicherstellt. Dies schafft für die Betriebe Transparenz und Planungssicherheit.

Positiv bewerten wir zudem, dass das Digital-Gesetz die Auslagerung der Datenverarbeitung in Clouds ermöglicht und damit eine erste regulatorische Grundlage für die Förderung digitaler Lösungen zur Vereinfachung des Behandlungsalltags mit einer hohen Datensicherheit im Gesundheitswesen geschaffen hat. Vor dem Hintergrund des demographischen Wandels und der Sicherstellung eines leistungsfähigen Gesundheitssystems, sind Vorhaben, die die Digitalisierung im Gesundheitswesen fördern, um u.a. sektorenübergreifende Datenaustausche zur Realisierung von Effizienzreserven zu vereinfachen, auch für die Wirtschaft von hoher Bedeutung. Denn sie bergen Potenziale zur Kostensenkung und Stabilisierung der Ausgaben im Gesundheitswesen und damit letztlich auch der Sozialversicherungsbeiträge.

Doch Paragraph 393 Abs. 4 Satz 3 SGB V, der durch den Entwurf der vorliegenden C5-Äquivalenz-Verordnung konkretisiert werden soll, wird sowohl Hersteller bzw. Anbieter von Cloud-Computing-Diensten sowie Leistungserbringer im Gesundheitswesen hinsichtlich des ihnen entstehenden Erfüllungsaufwandes perspektivisch vor Herausforderungen stellen.

B. Bewertung im Einzelnen

Testierung eines Cloud-Computing-Dienstes

Die C5-Äquivalenzverordnung soll rückwirkend zum 01.07.2024 in Kraft treten und sieht eine mögliche Verlängerung der Umsetzungsfrist für die C5-Typ-1 Attestierung (Angemessenheits- und Wirksamkeitsprüfung) unter Berücksichtigung eines gleichwertigen, in der Verordnung genannten, Standards vor. Hierzu wird eine Gap-Analyse mit einem Wirtschaftsprüfer vorgeschlagen. Die Abarbeitung der identifizierten Lücken in Bezug auf den BSI-C5-Standard kann dann im Anschluss innerhalb von 18 Monaten nach einem Meilensteinplan erfolgen. Ab dem 1.07.2025 müssen Anbieter zudem das erweiterte C5-Typ-2-Testat (Angemessenheits- und Wirksamkeitsprüfung) nachweisen. Diese Testierungen sind für Hersteller und Anbieter mit hohen Prüfkosten verbunden, insbesondere da diese Prüfung jedes Jahr neu durchgeführt werden sollte.

Die DIHK unterstützt grundsätzlich diese Maßnahmen zur Datensicherheit und sieht den zeitlichen Rahmen und Aufwand zur Umstellung auf das C5-Typ-1-Testat im Prinzip als ausreichend an. Allerdings verfügen nicht alle Cloud-Anbieter über die finanziellen Mittel, um jährlich ein gültiges C5-Testat zu erwerben, was in Folge den Wettbewerb zwischen den Anbietern einschränken kann, was wiederum ein reduziertes Cloud-Angebot für Leistungserbringer im Gesundheitswesen ergibt. Bereits heute zeichnet sich ein deutlicher Trend zum Cloud-Computing ab, der zu einer steigenden Nachfrage, wie etwa über die elektronische Patientenakte, führen wird. Die DIHK schlägt deshalb vor, die Prüfungsanforderungen der Testierungen so zu gestalten, dass der Aufwand der jährlichen Nachweiserbringung für die Anbieter möglichst bürokratiarm und ressourcenschonend ausfällt.

Sicherheitsnachweis äquivalente Testate/Zertifikate

Die Verordnung in der vorliegenden Form soll es Herstellern erleichtern, für eine Übergangszeit auch ohne ein C5-Typ-1-Testat ihren Cloud-Computing-Dienst anbieten zu können, sofern sie einen gleichwertigen Nachweis vorlegen können. Die Verordnung sieht z.B. das von vielen Herstellern bereits erworbene Zertifikat DIN EN ISO/IEC 27001:2022 als gleichwertigen Nachweis an, das um einen Maßnahmenkatalog ergänzt werden muss, der die Differenz zum C5-Testat abbildet.

Gemäß Digital-Gesetz und §393 SGB V ist das C5-Typ-1-Testat aber in seiner Gültigkeit zeitlich begrenzt. Ab dem 01.07.2025 ist stattdessen eine C5-Typ-2-Attestierung aufgrund der höheren Aussagekraft und Verlässlichkeit nachzuweisen. Während das C5-Typ-1-Testat sicherstellt, dass die Anforderungen an die Basiskriterien erfüllt sind, umfasst das C5-Typ-2-Testat auch deren Wirksamkeit. Vor diesem Hintergrund schlägt die DIHK vor, den Verordnungsentwurf in §1, um das C5-Typ-2-Testat zu erweitern und ggf. allgemein von einem C5-Testat zu sprechen. Hierdurch wird klarer, wie mit der Nachweiserbringung zukünftig verfahren werden kann und gibt den Anbietern Sicherheit. Diese Regelung würde es den Anbietern ermöglichen, die volle Umsetzungsfrist in Anspruch zu nehmen und auch nach dem 01.07.2025 eine zeitlich begrenzte gültige Äquivalenz gegenüber einem Typ-2-Testat vorlegen zu können.

Tendenziell werden Betreiber im Gesundheitswesen keinen Cloud-Anbieter beauftragen, der eine alternative „Ersatzbescheinigung“ hat, die nur bis zum 30.06.2025 gültig ist. Eine alternative Lösung könnte hierfür sein, die im Verordnungsentwurf festgelegten C5-Äquivalenznachweise dauerhaft zuzulassen statt nur als Zwischenlösung.

Übergangszeit zum Nachweis eines äquivalenten Sicherheitsniveaus

Der Verordnungsentwurf sieht vor, für eine Übergangszeit den Nachweis der Einhaltung eines zum C5-Kriterienkatalog äquivalenten Sicherheitsniveaus durch alternative Zertifikate und Testate zu erbringen. Eine C5-Typ-2-Attestierung erfolgt üblicherweise nach einer C5-Typ-1-Attestierung. Als Zeitrahmen zur Prüfung der Wirksamkeit des C5-Typ-1-Testats haben Anbieter sechs Monate angenommen. Die DIHK schlägt deshalb vor, diese Übergangsfrist vom C5-Typ-1-Testat auf das C5-Typ-2-Testat in §1 (2) Abs. 4 des Verordnungsentwurfes zu berücksichtigen, sodass den Anbietern insgesamt 24 Monate ab Erstellung der Meilensteinplanung für die Umsetzung auf das abschließende C5 Typ-2-Testat möglich sind. Zusätzlich regen wir an, es den Anbietern und Herstellern unter Einbezug eines Wirtschaftsprüfers zu ermöglichen, direkt eine C5-Typ-2-Attestierung anzustreben.

C. Ergänzende Informationen

a. Ansprechpartner mit Kontaktdaten

Dr. Nadine Behncke
Referatsleiterin Gesundheitswirtschaft
DIHK - Deutsche Industrie- und Handelskammer
Breite Straße 29, 10178 Berlin
Telefon: 030/2 03 08 1116
behncke.nadine@dihk.de

b. Beschreibung DIHK

Wer wir sind:

Unter dem Dach der Deutschen Industrie- und Handelskammer (DIHK) sind die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich die DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein. Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zum Gesamtinteresse der gewerblichen Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Grundlage unserer Stellungnahmen sind die wirtschaftspolitischen/europapolitischen Positionen und beschlossenen Positionspapiere der DIHK unter Berücksichtigung der der DIHK bis zur Abgabe der Stellungnahme zugegangenen Äußerungen der IHKs und ihrer Mitgliedsunternehmen.

Darüber hinaus koordiniert die DIHK das Netzwerk der 150 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 93 Ländern.

D. Fußzeile

für Berlin:

DIHK | Deutsche Industrie- und Handelskammer
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin
Tel. 030-20308-0 | Internet: www.dihk.de

für Brüssel:

Vertretung der DIHK | Deutsche Industrie- und Handelskammer bei der EU
19 A-D, Avenue des Arts | B-1000 Bruxelles
Tel. +32 2 286-1611 | Fax +32 2 286-1605 | Internet: www.dihk.de

DIHK | Deutsche Industrie- und Handelskammer
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin
Tel. 030-20308-0 | Internet: www.dihk.de