C5-Äquivalenzverordnung

Januar 2025

Stellungnahme zum Referentenentwurf einer C5-Äquivalenzverordnung

Mit dem Digital-Gesetz hat das BMG die Nutzung für Cloud-Computing im Gesundheitswesen erleichtert und Vorgaben für die Verarbeitung von Gesundheits- und Sozialdaten in der Cloud formuliert.

In diesem Zusammenhang besteht grundsätzlich seit Juli 2024 für alle Anbieter von Software as a Service (SaaS) im Gesundheitswesen, Leistungserbringende sowie Kranken- und Pflegekassen die Verpflichtung eines aktuellem C5-Testats der datenverarbeitenden Stelle. Dies stellt derzeit ein C5-Typ-1-testat da, ab Juli 2025 ist ein C5-Typ-2-Testat erforderlich. § 393 Absatz 4 Satz 3 SGB V sieht alternative Nachweismöglichkeiten des Sicherheitsniveaus der Cloud-Systeme vor, die in der vorliegenden Rechtsverordnung konkretisiert werden.

Zusammenfassung

Mit Blick auf die gesetzliche Grundlage, sieht der Bitkom eine pauschale und alternativlose Verpflichtung eines C5-Testats für alle Anbieter von Cloud-Anwendungen im Gesundheitswesen als nicht angemessen. **Deswegen sollte in der Rechtsverordnung klargestellt werden, ob und für welche Anwendungsfälle sich eine C5-Testierungspflicht ergibt.**

Dennoch begrüßen wir das Ziel dieser Rechtsverordnung, Cloud-Computing rechtssicher im Gesundheitswesen einsetzen zu können. Die vorgeschlagenen Anforderungen an cloudbasierte Systeme scheinen grundsätzlich zielführend. Durch eine unklare Abgrenzung der Begrifflichkeiten Cloud-Systeme, Cloud-Technik, Anbieter, Hersteller, etc. bleibt der Anwendungsbereich dieser Verordnung unklar. Der propagierte Anwendungsbereich von § 393 sowie dieser Verordnung würde zu einer Doppelzertifizierung führen. Hier fehlt eine Klarstellung, dass Cloud-Services, die

bereits ein C5-Testat mit sich bringen, nicht erneut von den Unternehmen zertifiziert werden müssen.

Die Rechtsverordnung zielt darauf ab, den betroffenen Unternehmen einen Handlungsspielraum zu ermöglichen, um die gesetzlichen Anforderungen an Cloud Computing (vgl. § 393 SGB V) zu erfüllen und ihre Systeme einem Migrationsprozess bis zur Erreichung des geforderten Schutzniveaus zu unterziehen.

Dafür sieht das BMG eine Frist von 18 Monaten vor, um ein C5 Typ 1 Testat zu erlangen. Diese Übergangsfrist kann jedoch durch die gesetzliche Vorgabe im § 393 nicht ausgeschöpft werden und verkürzt sich somit auf wenige Monate (je nach Inkrafttreten der Verordnung). Es fehlt jegliche Aussage zu den ab dem 1.Juli 2025 relevanten Äquivalenzstandards, da ab diesem Zeitpunkt C5-Typ2-Testate notwendig sind, die Äquivalenzverordnung jedoch nur Aussagen zu C5-Typ1-Testaten macht.

Um die Angebotsvielfalt des Marktes zu erhalten, muss diese Rechtsverordnung auf die C5-Typ 2-Testate ausgeweitet werden und mit einer entsprechenden Frist ergänzt werden.

Konkrete Anmerkungen und Änderungsvorschläge

Entwurf	**Änderungsvorschlag**	**Begründung**
Zu § 1 Nachweise, die geeignet sind, die Einhaltung eines Sicherheitsniveaus zu dokumentieren, das mit einer Typ1-Testierung nach dem C5-Kriterienkatalog vergleichbar ist	**Zu § 1 Nachweise, die geeignet sind, die Einhaltung eines Sicherheitsniveaus zu dokumentieren, das mit einer Typ1-/ Typ2-Testierung nach dem C5-Kriterienkatalog vergleichbar ist**	Eine **Ausweitung der Regelungen auf ein C5-Typ-2-Testat** würde eine Rechtssicherheit über den 1.7.2025 hinaus ermöglichen.
(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	(1) Eine Testierung oder Zertifizierung eines Cloud-Computing-Dienstes nach einem nachfolgend aufgezählten Standard gilt als Nachweis der Einhaltung eines zu einem Typ1-/ Typ2-Testat nach dem Kriterienkatalog C5 des Bundesamtes für Sicherheit in der Informationstechnik gleichwertigen Sicherheitsniveaus im Sinne des	s.o.

§ 393 Absatz 4 Satz 3 des Fünften Buches Sozialgesetzbuch, sofern die ergänzenden Voraussetzungen der Absätze 2 bis 3 erfüllt sind:	§ 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	1. ~~DIN EN ISO/IEC 27001:2022~~ 1. ISO/IEC 27001:2022 oder DIN EN ISO/IEC 27001:2024 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 4.a SOC2 Typ 1 4.b SOC2 Typ 2 5. ISO 27017 6. ISO 2700 7. weitere vom Hersteller/ Anbieter eingeholte Nachweise der Gewährleistung der IT-Sicherheit	Es wird auf DIN EN ISO/IEC 27001:2022 referenziert, diese gibt es nicht. Entweder es wird auf die ISO/IEC 27001:2022 und ihre deutsche Äquivalenz verwiesen, oder auf die DIN EN ISO/IEC 27001:2024. Im nationalen sowie internationalen Umfeld kommen weitere Nachweise in Frage, weswegen diese Liste **regelmäßig ergänzt und nicht abschließend sein darf**. Mit Blick auf europäische Regelungen und insbesondere den EDHS müssen hier internationale Vorgaben berücksichtigt und gleichgesetzt werden. Auch sollte den Unternehmen die Möglichkeit gegeben werden individuelle Nachweise dem Stand der Technik entsprechend zu erbringen.
Ergänzend zu dem bestehenden Testat oder Zertifikat muss für einen Cloud-Computing-Dienst ein Maßnahmenplan vorliegen, der mindestens folgendes enthält: [...] 4. eine Dokumentation von Maßnahmen zur Erlangung eines C5-Typ-1-Testats für den	Ergänzend zu dem bestehenden Testat oder Zertifikat muss für einen Cloud-Computing-Dienst ein Maßnahmenplan vorliegen, der mindestens folgendes enthält: [...] 4. eine Dokumentation von Maßnahmen zur Erlangung eines C5-Typ-1-Testats für den	Um dem Aufwand einer Typ-2-Zertifizierung gerecht zu werden, erscheinen verschiedene Fristen gerechtfertigt.

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.	Cloud-Computing-Dienst innerhalb von 18 Monaten ab Erstellung der Meilensteinplanung oder eines C5-Typ-2-Testats für den Cloud-Computing-Dienst innerhalb von 24 Monaten ab Erstellung der Meilensteinplanung; hierunter fallen auch vertragliche Vereinbarungen mit einem Auditor zur Durchführung eines C5-Typ-1- oder Typ-2-Audits oder die Aufnahme von Vertragsverhandlungen hierzu.	

Weitere Anmerkungen und ergänzende Vorschläge

Gesundheitswirtschaft entlasten und Äquivalenztestierung zu C5 ermöglichen

Grundsätzlich wäre eine „echte“ Äquivalenzverordnung zur C5-Testierung mit diesem Entwurf begrüßenswert, denn sie gäbe insbesondere die Möglichkeit, die internationale Norm ISO 27001 mit ihr gleichzusetzen. Auch ist die Forderung nach zusätzlichen Maßnahmen nachvollziehbar. Allerdings hätte stattdessen auf die internationale Norm ISO 27017 und ISO 27018, die für Cloud Computing gilt, verwiesen werden können. Diese sind gemäß der Kreuzreferenztabelle des BSI insgesamt als vergleichbar anzusehen und erfüllen unserer Einschätzung nach ein sehr hohes Sicherheitsniveau für die Bereitstellung und den Betrieb von Cloud Services.

Kostenseitig könnte für die Anbieter – und damit letztlich auch für die Nutzer - eine deutliche Einsparung von personalaufwendigen Wirtschaftsprüfungsprozessen im höheren, mind. zweistelligen Millionen-Euro-Bereich jährlich mit sich bringen. Der enorme finanzielle und organisatorische Aufwand zur Erlangung eines C5-Testats insbesondere für kleinere Unternehmen und Startups, steht in keinem Verhältnis zum Nutzen. Sollte das BSI, als verantwortliche nationale Behörde, seine Sicherheitsanforderungen hinsichtlich einer C5-Erfüllung nicht in den internationalen Kriterienkatalogen wiederfinden, so hätte es sicherlich die Möglichkeit, sich in den internationalen Normungsprozess einzubringen.

Regelung zu Verfahren bei der Markteinführung von neuen Services

Ein weiterer Aspekt, welcher nach unserer Einschätzung eine gesteigerte Bedeutung aufweist, jedoch nicht durch den Entwurf der C5-Äquivalenzverodnung thematisiert wird, ist das grundlegende Verfahren bei der Markteinführung von neuen Services. Exemplarisch möchten wir hier einen fiktiven Service aufführen, welcher am

01.01.2026 in den Markt eingebracht wird. Entsprechend der Vorgaben des § 393, Abs. 4, S. 2 SGB V dürfte dieser Service nur beim Vorliegen eines gültigen C5 Typ 2 Testates bereitgestellt und genutzt werden. Aufgrund der Erfahrung bei den bisher erfolgten Testierungen ist dies unserer Einschätzung nach jedoch nicht möglich zum Marktstart die Wirksamkeit eines internen Kontrollsystems nachzuweisen. Ein neuer Service kann in jedem Fall bereits während der Entwicklungsphasen die Vorgaben des C5-Kriterienkataloges berücksichtigen. Ein hinreichender Nachweis der Wirksamkeit des eingeführten internen C5-Kontrollsystemes gegenüber einem Wirtschaftsprüfungsunternehmens kann jedoch erst frühestens nach einen Betriebszeitraum von mindestens vier Monaten möglich sein. Ebenso sollte der Geltungsbereich der Übergangsfristen entsprechend § 1 Abs. 2 Nr. 4 des Entwurfes der C5-Äquivalenz-Verordnung auch neue Services einschließen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartnerin

Dr. Ariane Schenk | Bereichsleiterin E-Health
T 030 27576-231 | a.schenk@bitkom.org

Verantwortliches Bitkom-Gremium

AK E-Health