BVMed Bundesverband Medizintechnologie e.V.

Stellungnahme

Referentenentwurf zur C5-Äquivalenzverordnung

24. Januar 2025

Einordnung

Der Einsatz cloudbasierter Informationssysteme bietet im Gesundheitswesen erhebliche Vorteile. Zugleich besteht ein gesonderter Schutzbedarf, sofern personenbezogene Daten in den Cloud-Lösungen verarbeitet werden.

Mit dem durch das Digital-Gesetz neu eingeführten § 393 des Fünften Buches Sozialgesetzbuch (SGB V) wurde im Jahr 2024 diesbezüglich der „Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)“ als verpflichtend einzuhaltender Sicherheitsmaßstab für das Gesundheitswesen festgelegt. Darüber hinaus sind laut Gesetz weitere Testate oder Zertifikate möglich, deren *„Befolgung ein im Vergleich zum C5-Standard vergleichbares oder höheres Sicherheitsniveau sicherstellt“.*

Der vorliegende Entwurf einer Rechtsverordnung dient der Festlegung, welche Standards diese Anforderungen erfüllen.

1. Allgemeine Anmerkungen

Zunächst ist positiv festzustellen, dass das Bundesministerium für Gesundheit (BMG) international anerkannte Standards als Alternativen zum C5-Typ-1-Testat in Betracht zieht. Dies ermöglicht es vielen Unternehmen, bereits vorhandene Zertifizierungen zum Einsatz zu bringen.

Das BMG nimmt jedoch nicht die Gelegenheit wahr, auch Alternativen für das C5-Typ-2-Testat festzulegen, das ab dem 01.07.2025 verpflichtend vorzulegen ist. Im europäischen Ausland gibt es bereits einige aus unserer Sicht vergleichbare Zertifikate zur Sicherung von Daten in Clouds, die als dauerhaftes Äquivalent geeignet wären und es den Unternehmen wesentlich erleichtern würden, nicht mehrere Zertifikate parallel vorlegen zu müssen.

Darüber hinaus sehen wir folgende drei Punkte als kritisch an:

1.1 Keine ausreichende Berücksichtigung von C5-Äquivalenten

Die Verordnung sieht lediglich eine temporäre Ausnahme von maximal 18 Monaten von der Verpflichtung des Erlangens eines C5-Typ-1-Testats vor. Jedes Unternehmen, das Cloud-Computing-Dienste im Sinne von § 393 SGB V anbietet, muss somit ein C5-Typ-1-Testat oder Äquivalente vorweisen und einen Plan zum Erlangen des C5-Typ-2-Testates vorlegen. Diese Vorgehensweise bezüglich

alternativer Zertifikate ist dem Wortlaut des § 393 SGB V nicht zu entnehmen und stellt aus unserer Sicht eine erhebliche Einschränkung des Handlungsspielraumes von Unternehmen dar.

Andere europäische Länder haben schon vor einiger Zeit Sicherheitszertifikate für Clouds eingeführt, die viele europaweit tätige Unternehmen bereits vorhalten. In einem europäischen Binnenmarkt ist die Parallelität von verschiedenen nationalen Anforderungen ein hoher bürokratischer Aufwand und mit hohen Kosten verbunden. Jedes Zertifikat verlangt nicht nur Eigenleistung, sondern auch die Beauftragung von anerkannten Prüfstellen. Eine europaweite Vereinbarung über die gegenseitige Anerkennung von Zertifikaten wird seit einigen Jahren vorbereitet, ist aber noch nicht beschlossen.

Im Sinne europaweiter Regelungen fordern wir daher, vergleichbare Standards, die schon heute in Europa Anwendung finden, wie beispielsweise SecNumCloud, als dauerhafte Alternative zu benennen.

1.2 Bürokratie beim Nachweis des Sicherheitsniveaus

Laut dem § 1 Absatz 2 der Verordnung müssen Unternehmen zahlreiche Schritte gehen:

- eine umfassende Dokumentation über die C5-Basiskriterien erstellen, welche materiell nicht mit der bestehenden Zertifizierung des Unternehmens abgedeckt werden;
- eine umfassende Dokumentation der technischen und organisatorischen Maßnahmen, mit denen die materiellen Lücken zum C5-Typ-2-Testat behoben werden;
- eine Meilensteinplanung, wie die Vorkehrungen umgesetzt werden, sowie
- eine Dokumentation der Maßnahmen zur Erlangung des C5-Typ-1-Testats.

De facto werden also die genannten bestehenden Zertifikate (DIN EN ISO/IES 27001:2022 etc.) nur in Kombination mit dem Weg hin zu einem C5-Typ-1-Zertifikat anerkannt. Das Erreichen des geforderten Schutzniveaus ist somit mit immensem bürokratischem Aufwand verbunden.

Vor dem Hintergrund von Bürokratieabbau fordern wir einen Verzicht auf dieses aufwendige Verfahren.

1.3 Fehlende Beachtung des europäischen Binnenmarktes

Medizintechnikunternehmen bieten ihre Lösungen europaweit an. Mit dem C5-Testat spricht sich Deutschland für ein Sicherheitsmaßstab aus, der momentan nur für Deutschland verpflichtend ist. Andere Länder fragen andere Zertifikate an. Das bedeutet, die Hersteller müssen verschiedenste Testate und Zertifikate für den europäischen Binnenmarkt vorhalten. Dies ist mit Mehraufwänden und höheren Kosten für die Hersteller verbunden.

Neben der Forderung, gleichwertige und vom Schutzniveau vergleichbare Alternativen aus anderen europäischen Ländern zu akzeptieren, regen wir an, schon jetzt in der Verordnung künftige, in Europa harmonisierte Zertifikate, wie den European Cybersecurity Certification Scheme for Cloud Services (EUCS), zu verankern. Hierzu gehört auch der Verweis, dass diese als vollwertige C5-

Äquivalente zu behandeln sind und in Zukunft vorrangig sein sollen bzw. C5-Testate ersetzen werden.

Auf Basis der allgemeinen Anmerkungen schlagen wir vor, den **§ 1 Nachweise, die geeignet sind, die Einhaltung eines Sicherheitsniveaus zu dokumentieren, das mit einer Typ1-Testierung nach dem C5-Kriterienkatalog vergleichbar ist** wie folgt neu zu benennen und umzuformulieren:

2. Formulierungsvorschläge

§ 1 Nachweise, die geeignet sind, die Einhaltung eines Sicherheitsniveaus zu dokumentieren

Absatz 1 neu:

(1) *Eine Testierung oder Zertifizierung eines Cloud-Computing-Dienstes nach einem nachfolgend aufgezählten Standard gilt als vollumfänglicher Nachweis der Einhaltung eines zu einem C5-Typ-2-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*:

1. *SecNumCloud*
2. *Esquema Nacional de Seguridad (ENS)*

Absatz 1 alt wird Absatz 2 neu:

(2) 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 3 bis 4* 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

Absatz 3 neu:

(3) Ergänzend zu dem bestehenden Testat oder Zertifikat gemäß Absatz 2 muss für einen Cloud-Computing-Dienst ein Dokument vorlegen, aus dem hervorgeht, bis wann die Erlangung eines C5-Typ-1-Testats oder eines äquivalenten Zertifikats nach Absatz 1 für den Cloud-Computing-Dienst innerhalb von 18 Monaten geplant ist. Hierunter fallen auch vertragliche Vereinbarungen mit einem Auditor zur Durchführung eines Audits oder die Aufnahme von Vertragsverhandlungen drunter.

Absatz 3 alt wird Absatz 4 neu:

(4) Die Dokumente nach Absatz 2, sowie das damit verbundene 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.

Absatz 5 neu:

(5) Diese Verordnung tritt außer Kraft, wenn eine europäische Richtlinie zur Cybersicherheit in Kraft tritt.

BVMed
Bundesverband Medizintechnologie e.V.
Georgenstraße 25, 10117 Berlin
+49 30 246 255 - 0
info@bvmed.de
www.bvmed.de