Verordnung über gleichwertige Sicherheitsnachweise zum C5-Standard für Cloud-Computing-Dienste im Gesundheitswesen (C5-Gleichwertigkeitsverordnung - C5GleichwV)

C5GleichwV

Ausfertigungsdatum: 19.03.2025

Vollzitat:

"C5-Gleichwertigkeitsverordnung vom 19. März 2025 (BGBl. 2025 I Nr. 91)"

Fußnote

(+++ Textnachweis ab: 1.7.2024 +++)

Eingangsformel

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

§ 1 Nachweise für ein gleichwertiges Sicherheitsniveau zum C5-Kriterienkatalog

(1) Eine Testierung oder Zertifizierung eines Cloud-Computing-Dienstes nach einem nachfolgend aufgezählten Standard (alternativer Standard) gilt als Nachweis der Einhaltung eines zu einem Typ1- oder einem Typ2-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 zusätzlich die Voraussetzungen nach den Absätzen 2 und 3 erfüllt sind:

1. ISO/IEC 27001 in der jeweils gültigen Fassung,
2. ISO 27001 auf der Basis von IT-Grundschutz durch das Bundesamt für Sicherheit in der Informationstechnik und
3. Cloud Controls Matrix Version 4.0 in der jeweils gültigen Fassung.

(2) Zusätzlich zu dem bestehenden Testat oder Zertifikat aufgrund des alternativen Standards muss für einen Cloud-Computing-Dienst ein Maßnahmenplan vorliegen, der mindestens Folgendes enthält:

1. eine Dokumentation, die diejenigen Basiskriterien des C5-Kriterienkatalogs kennzeichnet, die materiell nicht durch den dem bestehenden Testat oder Zertifikat zugrundeliegenden alternativen Standard abgedeckt werden,
2. eine Dokumentation der individuellen technischen und organisatorischen Vorkehrungen, die ergriffen werden, um die nach Nummer 1 dokumentierten 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 nach Nummer 1 dokumentierten 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-Typ1-Testats für den Cloud-Computing-Dienst innerhalb von 18 Monaten ab der Erstellung der Meilensteinplanung nach Nummer 3 und von Maßnahmen zur Erlangung eines C5-Typ2-Testats für den Cloud-Computing-Dienst innerhalb von 24 Monaten ab Erstellung der Meilensteinplanung nach Nummer 3; hierunter fallen auch vertragliche Vereinbarungen mit einem Auditor zur Durchführung eines C5-Typ1- oder eines C5-Typ2-Audits oder die Aufnahme von Vertragsverhandlungen hierzu.

(3) Der Maßnahmenplan nach Absatz 2 und das bestehende Testat oder Zertifikat aufgrund des alternativen Standards sind den Leistungserbringern nach dem Vierten Kapitel des Fünften Buches Sozialgesetzbuch oder den Kranken- und Pflegekassen, die einen Cloud-Computing-Dienst beauftragen, sowie den jeweils zuständigen Aufsichtsbehörden auf deren Verlangen hin unverzüglich vorzulegen.

§ 2 Inkrafttreten

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