# CLOUD-DIENSTE FÜR GESUNDHEIT: ZVEI FORDERT PRAGMATISCHEN ANSATZ FÜR C5-ÄQUIVALENZ-VERORDNUNG

Cloudbasierte Informationssysteme sind im Bereich Gesundheit inzwischen weit verbreitet, denn sie bieten erhebliche Vorteile. Werden damit personenbezogen Gesundheitsdaten verarbeitet, besteht besonderer Schutzbedarf. Der dafür verpflichtende BSI-Kriterienkatalog C5 soll nun durch eine C5-Äquivalenz-Verordnung ergänzt werden.

zvei
electrifying ideas

**ZVEI e. V.**
**Verband der Elektro- und Digitalindustrie**
Lyoner Straße 9, 60528 Frankfurt am Main
Tel.: +49-(0)69-6302-206
Fax: +49-(0)69-6302-390
E-Mail: medtech@zvei.org
www.zvei.org/gesundheit

Der ZVEI sieht die Gefahr einer zusätzlichen Belastung der Anbieter ohne Mehrwert für die Sicherheit, anstatt die Verordnung zu einer bürokratischen Entlastung des Systems zu nutzen.

Aber von vorn: Cloudbasierte Informationssysteme können zum Beispiel zum Einsatz kommen, um die Funktion von Systemen zu ermöglichen oder zu unterstützen, die selbst keine Cloud-Dienste sind. Gerade international tätige Anbieter verfügen deshalb bereits über Systeme, die ein hohes Niveau an Cybersicherheit bieten und nach internationalen Standards zertifiziert sind.

In Deutschland wurde mit dem Digital-Gesetz der Paragraf 393 SGB V neu eingeführt. Er legt fest, dass der durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte „Kriterienkatalog C5“ (Cloud Computing Compliance Criteria Catalogue) als Sicherheitsmaßstab für die Cybersicherheit von cloudbasierten Diensten im deutschen Gesundheitssystem verpflichtend eingehalten werden muss. Insbesondere, wenn es um die Verarbeitung von personenbezogenen Daten geht.

Nach Paragraf 393 Absatz 4 Satz 3 SGB V darf eine Verarbeitung von personenbezogenen Gesundheitsdaten auch ohne ein C5-Testat erfolgen, wenn für die im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die Cloud-Technik ein Testat oder Zertifikat nach einem Standard vorliegt, dessen Befolgung ein im Vergleich zum C5-Standard vergleichbares oder höheres Sicherheitsniveau sicherstellt. Welche Standards das sind, legt das Bundesministerium für Gesundheit (BMG) durch Rechtsverordnungen fest.

Diese Regelung stellt für Anbieter, die bereits über ein entsprechend äquivalentes Zertifikat verfügen, zunächst eine wertvolle Entlastung dar. Das Bundesministerium für Gesundheit listet in seinem Referentenentwurf der C5-Äquivalenz-Verordnung von Dezember 2024 drei Normen und Standards auf, die als äquivalent mit einem C5-Typ-1-Testat des BSI gelten. Die Äquivalenz ist allerdings an eine Reihe von ergänzenden Voraussetzungen gebunden:

Die Anbieter müssen nach dem Entwurf der Verordnung eine umfangreiche Dokumentation vorlegen, mit der detailliert belegt werden muss, wo das bestehende Zertifikat von den C5-Kriterien abweicht. Zusätzlich muss ein Zeitplan vorgelegt werden, wie und bis wann diese Abweichungen beseitigt werden. Abschließend wird gefordert, dass der Anbieter innerhalb von 18 Monaten ein C5-Typ-1-Testat erlangen soll. Außerdem legt der Entwurf der Verordnung lediglich eine Äquivalenz mit dem Typ 1-Testat des BSI fest. C5-Typ-1-Testate müssen aber nach Paragraf 393 Absatz 4 SGB V bereits ab dem 1. Juli 2025 durch ein C5-Typ-2-Testat ersetzt werden.

Die Anbieter von Cloud-Diensten würden also nur sehr kurz von der Äquivalenz der vorhandenen Cybersicherheitssysteme profitieren. Eine dauerhafte Äquivalenz von Zertifikaten nach internationalen Normen mit hohem Sicherheitsniveau ist so nicht gegeben. Der ZVEI fordert daher, dass die C5-Äquivalenz-Verordnung eine pragmatische Lösung für eine dauerhafte Äquivalenz bietet, um auch wirklich eine Entlastung bei Anbietern zu bewirken.

**Hans-Peter Bursig**
ZVEI-Bereichsleiter Gesundheit