BVMed Bundesverband Medizintechnologie e.V.

Infoblatt

C5-Testat / § 393 SGB V Cloud-Einsatz im Gesundheitswesen

Stand Januar 2026

Ziel des § 393 SGB V Cloud-Einsatz im Gesundheitswesen

Ziel des § 393 SGB V ist es, anhand von verbindlichen Mindeststandards zur Cybersicherheit den sicheren Einsatz von Cloud-Computing-Diensten durch Leistungsbringer im Gesundheitswesen und gesetzliche Kranken- und Pflegekassen zu ermöglichen. Systematisch stellt § 393 SGB V einen Erlaubnistatbestand dar, der die Nutzung von Cloud-Computing-Diensten durch die vorstehend genannten Akteure unter die Voraussetzung der Einhaltung bestimmter Cybersicherheitsanforderungen stellt.

Wann müssen Unternehmen der Medtech-Branche § 393 SGB V beachten?

§ 393 SGB V richtet sich an Leistungserbringer (z. B. DiGA-Anbieter, Vertragsärzte, Hebammen, Heil- und Hilfsmittelleistungserbringer, Pflegeberufe) und deren Auftragsverarbeiter, wenn sie personenbezogene Gesundheitsdaten von Patienten im Wege des Cloud-Computings verarbeiten.

§ 393 SGB V gilt *nicht* außerhalb der gesetzlichen Krankenversicherung wie beispielsweise für Leistungen, die gegenüber privaten Krankenversicherungen abgerechnet werden oder die direkt gegenüber Patienten ohne Einbindung einer GKV erbracht werden.

Wann liegt ein Cloud-Computing-Dienst vor?

§ 393 SGB V gilt nur, wenn die Software-Anwendung, mit der Gesundheitsdaten verarbeitet werden, als Cloud-Computing-Dienst zu qualifizieren ist. § 384 Nr. 5 SGB V definiert einen Cloud-Computing-Dienst als

> *„digitalen Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind“*

Die wesentlichen Merkmale können wie folgt näher beschrieben werden[1]:

> „Auf Abruf“: Der Cloud -Nutzer kann sich selbst ohne Interaktion mit dem Cloud-Anbieter Rechenkapazitäten wie bspw. Serverzeit oder Netzwerkspeicherplatz zuweisen.
> „Skalierbarer und elastischer Pool“: Rechenressourcen, die der Cloud-Anbieter flexibel entsprechend der Nachfrage bereitstellen kann.[2]
> „Gemeinsam nutzbar“: Rechenressourcen, die einer Vielzahl von Nutzern bereitgestellt werden, wobei die Verarbeitung für jeden Nutzer separat erfolgt.

Als Faustformel kann man festhalten, dass ein Cloud-Computing-Dienst vorliegt, wenn Unternehmen/Personen von einem Dritten eine Zugriffsmöglichkeit über Nutzerkonten auf Anwendungen und Daten per Fernzugriff erhalten. Das bedeutet:

> Die Plattformen der typischen Hyperscaler (z.B. AWS, Microsoft Azure, Google Cloud, Ionos, Stack IT) sind Cloud-Computing-Dienste.
> Anwendungen, die auf solchen Cloud-Infrastrukturen laufen („Software as a Service – SaaS“), sind ebenfalls (eigene) Cloud-Computing-Dienste.
Auch Cloud-Instanzen von Leistungserbringern/Unternehmen, die in eigenen oder fremden Rechenzentren laufen, können – auch nach der Gesetzesbegründung – unter die Definition der Cloud-Computing-Dienste fallen. Die Einordnung ist im Einzelfall auslegungsbedürftig und sollte dokumentiert sowie ggf. rechtlich geprüft werden.

Anwendungsbeispiele des § 393 SGB V

Cloud-basiertes PACS/Archivsystem für Bilddaten (Medizinprodukt)

Eine von Ärzten eingesetztes PACS zur Speicherung und Verarbeitung speichert die Daten auf einem Server in der Klinik und nutzt die Infrastruktur eines Hyperscalers zur Speicherung der Daten als Back-up. Für den Server in der Klinik sind die Anforderungen des § 393 SGB V nicht zu beachten, wohl aber für Back-up-Lösung in der Cloud und zwar (i) für die Plattform des Hyperscalers und (ii) die Anwendung, die auf der Plattform des Hyperscalers läuft.

On-Premises-Lösung/eigener Server

Der Betrieb eines eigenen Servers (etwa ein PACS-Server) oder einer Anwendung im lokalen Netzwerk des Krankenhauses oder der Praxis werden **in der Regel kein Cloud-Computing-Dienst** sein, daher ist § 393 SGB V nicht anwendbar. Für die Medizinprodukteanwendungen dezidierte Server, die beim Medizinprodukthersteller stehen, sind ebenfalls keine Cloud-Computing-Dienste, wenn es – wie in der Regel der Fall – sich nicht um Dienste handelt, bei denen Nutzer sich selbst „**auf Abruf**“ Rechenkapazitäten zuweisen können.

[1] Die Definition im § 384 Nr. 5 SGB V beruht auf der NIS-2-Richtlinie, die einzelnen Merkmale ("skalierbar", "auf Abruf" etc.) werden in Erwägungsgrund 33 der NIS-2-Richtline näher erläutert.
[2] Auto-Skalierbarkeit der Rechenressourcen nach NIST ist nach Auffassung des BSI dagegen kein erforderliches Kriterium, siehe BSI, Sektorspezifische Fragen und Antworten zu NIS-2, FAQ 5.

DiGA zur Behandlung von Schlafstörungen

Die DiGA speichert und bereitet Patientendaten in der Cloud auf. Der Anbieter der DiGA ist Leistungserbringer, der Cloud-Provider Auftragsverarbeiter.
Von beiden sind die Anforderungen des § 393 SGBV zu beachten.

CGM-System und Insulinpumpe

Ein Glukosesensor misst kontinuierlich den Gewebezucker; der mit dem Sensor verbundene Transmitter leitet die Messwerte an die Insulinpumpe. Dort werden die Werte mittels integrierten Algorithmus analysiert und die Insulinabgabe ausgelöst. Die dabei anfallenden Daten werden per Bluetooth an die auf dem Smartphone des Patienten installierte App übertragen und von dort in eine Cloud hochgeladen, aufbereitet und dem Patienten sowie über eine Plattform dem behandelnden medizinischen Fachpersonal zur Verfügung gestellt.

Die Cloud-Infrastruktur und die Plattform müssen die Anforderungen des § 393 SGB V beachten. Der Sensor und die Insulinpumpe sind dagegen keine Cloud-Computing-Dienste. Für Transmitter und die App verlangen Markteilnehmer in der Praxis (insb. Krankenkassen) teilweise C5-Typ2-Testate, weil sie untrennbar mit dem Cloud-Computing-Dienst verbunden sind.

Pflichten beim Einsatz eines Cloud-Computing-Dienstes nach § 393 SGB V

Ist § 393 SGB V anwendbar, sind folgende Pflichten einzuhalten:

> Der Cloud-Computing-Dienst muss ein C5-Typ2-Testat vorweisen (1.).
> Gesundheitsdaten dürfen nur in bestimmten Regionen verarbeitet werden (2.).
> Die „datenverarbeitende Stelle“ muss eine Niederlassung im Inland haben (3.).
> Es sind angemessene Sicherheitsmaßnahmen umzusetzen (4.).

1. C5-Typ2-Testat

Was ist ein C5-Typ2-Testat?

Der C5-Kriterienkatalog ist eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte Sammlung von Mindestanforderungen für sicheres Cloud Computing. Die Einhaltung weist ein Testat von Wirtschaftsprüfern nach. Erforderlich ist ein Typ2-Testat, das die Wirksamkeit der Kontrollen über einen längeren Zeitraum nachweist (typischerweise 6 oder 12 Monate).

Welche Alternativen gibt es zum C5-Typ2-Testat und wie lange können diese das Testat ersetzen?

Nach der C5-Gleichwertigkeitsverordnung stehen auch Alternativen zum C5-Typ2-Testat zur Verfügung: Eine ISO/IEC 27001 Zertifizierung in der jeweils gültigen Fassung (aktuell ISO/IEC 27001:2022), ISO 27001 auf der Basis von IT-Grundschutz durch das Bundesamt für Sicherheit in der Informationstechnik oder Cloud Controls Matrix Version 4.0 in der jeweils gültigen Fassung.

Diese Alternativen stehen aber nur vorübergehend zur Verfügung. Die Gleichwertigkeitsverordnung verlangt, die Lücken zum C5-Typ2-Testat zu dokumentieren (i), einen Plan zu erstellen, wie die Lücken innerhalb von 12 Monaten geschlossen werden (ii)und innerhalb von 24 Monaten das C5-Typ2-Testat erlangt werden soll (iii) (dazu gehört auch der Abschluss bzw. die Verhandlung von Verträgen mit Wirtschaftsprüfungsgesellschaften zur Testierung). Wer also ab dem 1. Juli 2025 einen Cloud-Computing-Dienst verwendet bzw. anbietet, muss zumindest sicherstellen, dass die Anforderungen der C5-Gleichwertigkeits-verordnung erfüllt sind und innerhalb von zwei Jahren das C5-Typ2-Testat vorliegt.

Was muss das C5-Typ2-Testat abdecken?

Alle über die Cloud erbrachten Dienste müssen von einem C5-Typ2-Testat abgedeckt sein. Der Cloud-Anbieter, auf dessen Plattform die Gesundheitsdaten verarbeitet werden, muss also ein C5-Typ2-Testat vorweisen. Wenn auf der Cloud-Plattform zudem eine (SaaS-)Applikation des MedTech-Unternehmens läuft, dann muss auch diese ein C5-Typ2-Testat vorweisen.[3] Die Medizinprodukte (wie etwa eine Insulinpumpe) von denen Gesundheitsdaten direkt oder indirekt in die Cloud übertragen werden, müssen an sich kein C5-Typ2-Testat aufweisen, denn diese Geräte sind keine Cloud-Computing-Dienste im Sinne des § 384 Nr. 5 SGB V. Auch der maßgebliche C5-Kriterienkatalog des BSI[4] erfasst solche Geräte nicht. Bei der Kommunikation der Geräte mit dem Cloud-Computing-Dienst ist aber eine angemessene Transportverschlüsselung sicherzustellen.[5] Zudem müssen die im Bericht zum Testat enthaltenen Auflagen zur Konfiguration und zum Betrieb der testierten Systeme umgesetzt werden.[6]

2. In welchen Regionen dürfen die Gesundheitsdaten verarbeitet werden?

Gesundheitsdaten dürfen nur in Cloud-Instanzen in den folgenden Ländern gespeichert werden; ebenso ist der Zugriff auf Gesundheitsdaten nur aus diesen Ländern gestattet:

> Bundesrepublik Deutschland, Mitgliedstaaten der EU und des EWR[7]
> USA, Schweiz, Vereinigtes Königreich, Kanada, Israel Südkorea, Japan und die weiteren Staaten, für welche die EU Kommission einen Angemessenheitsbeschluss gem. Art. 45 DSGVO erlassen hat.[8]

[3] FAQ des BSI „Wie geht der Kriterienkatalog mit Unterauftragnehmern um? “
[4] § 384 Nr. 6 SGB V
[5] CRY-02 Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)
[6] § 393 Abs. 3 Nr. 3 SGB V
[7] Norwegen, Lichtenstein, Island
[8] Die weiteren Länder sind: Neuseeland, Andorra, Argentinien, Faröer Inseln, Guernsey, Isle of Man, Uruguay. Für die USA gilt der Angemessenheitsbeschluss nur für solche Unternehmen, die sich nach dem EU-US Data Privacy Framework zertifiziert haben. Die Liste der Unternehmen ist hier abrufbar. Die großen US-Hyperscaler sind – Stand 10.10.2025 – entsprechend zertifiziert.

Wichtig: Es reicht also nicht aus, dass bei einem Cloud-Anbieter eine der o.g. Regionen für die Speicherung ausgewählt wird. Auch die Zugriffe auf die Gesundheitsdaten dürfen nur aus den o.g. Ländern erfolgen. Zugriffe bspw. von Subunternehmern aus Indien, Malaysia oder China auf Gesundheitsdaten sind nicht erlaubt (auch nicht bei Verwendung von EU-Standardvertragsklauseln), wohl aber auf andere Daten (etwa den Namen eines Arztes). Das gilt auch, wenn Übermittlungen oder Zugriffe durch EU-Standardvertragsklauseln für Datentransfers in Drittländer abgesichert werden; bei § 393 SGB V ist der Transfer nur zulässig, wenn für das Land ein Angemessenheitsbeschluss vorliegt.

3. Bedarf es einer Niederlassung in der Bundesrepublik Deutschland?

Die „datenverarbeitende Stelle“ muss über eine Niederlassung im Inland verfügen. Mangels Klarstellung durch den Gesetzgeber ist derzeit unklar, wer alles „datenverarbeitende Stelle“ ist. Wahrscheinlich sind dies die Anbieter der eingesetzten Cloud-Computing-Dienste.[9]

Wichtig: Erforderlich ist also nicht, dass der Vertragspartner (etwa einer der großen US-Hyperscaler) des Medizinprodukteherstellers eine deutsche Gesellschaft ist, sondern dass es eine deutsche Konzerngesellschaft gibt, die als Niederlassung des Vertragspartners angesehen werden kann. Mögliches Beispiel: Vertragspartner ist Cloud-Anbieter Ireland, Niederlassung ist Cloud-Anbieter Deutschland GmbH.

4. Was gilt als angemessenes Sicherheitsniveau?

Es sind angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit zu ergreifen. In der Regel sind hierfür – etwa bei DiGA – die allgemein formulierten Anforderungen für Krankenhäuser nach § 391 Abs. 1, 2 SGB V maßgeblich, auf die § 393 Abs. 6 SGB V verweist.[10]

Kontakt
Natalie Gladkov
Referat Digitale Medizinprodukte
gladkov@bvmed.de

Dr. Katja Marx
Referat Recht
marx@bvmed.de

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

[9] Gemeint sein kann insbesondere *jedes* Unternehmen, das auf die Gesundheitsdaten in der Cloud zugreift oder (nur) die Anbieter der eingesetzten Cloud-Dienste. Für letzteres spricht, dass (nur) für diese die Pflicht gilt, das C5-Testat vorzuhalten (Abs. 3 Nr. 2 SGB V).

[10] § 391 Abs. 4 SGB V verweist zwar auf branchenspezifische Sicherheitsstandards – deren Umsetzung ist aber *nicht* verpflichtend.