§ 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen



Das Testat liefert der Anbieter. Die Aufgabenliste darunter liefert er gleich mit – an Sie.

Wissen

Alle Beiträge der Serie im Überblick:

› **Microsoft 365 im Krankenhaus**

Beratung

Cloud-Nachweise, Konzept, Tenant-Prüfung:

› **Microsoft 365 Beratung für Krankenhäuser**

Schulung

Für IT, ISB, Datenschutz und QM:

› **Microsoft 365 Schulung für Krankenhäuser**

Es gibt im Krankenhaus zwei Sorten von Papier: das, was im Zertifizierungsaudit auf den Tisch muss, und das, was erst dann auftaucht, wenn etwas schiefgegangen ist. Das C5-Testat Ihres Cloud-Anbieters gehört seit dem Sommer 2025 eindeutig zur ersten Sorte. Trotzdem liegt es in vielen Häusern bestenfalls als PDF im Downloadordner der IT-Leitung, ungelesen, irgendwo zwischen dem Lizenzvertrag und dem Wartungsvertrag für die Rohrpost.

Dabei ist die Rechtslage überraschend klar formuliert. **§ 393 SGB V** erlaubt Krankenhäusern die Verarbeitung von Sozial- und Gesundheitsdaten in Cloud-Diensten – aber nur unter Bedingungen. Eine davon heißt: aktuelles C5-Testat, seit 1. Juli 2025 vom Typ 2. Eine andere, gern überlesene, heißt: Das Krankenhaus setzt die Kriterien um, die der Prüfbericht ihm als Kunden zuweist. Und genau dort wird aus einem Nachweis des Anbieters eine Aufgabe für Ihr Haus.

Dieser Beitrag erklärt, was § 393 SGB V verlangt, wie Sie ein C5-Testat lesen, wie Sie für Microsoft 365 selbst prüfen, was abgedeckt ist – und warum die Frage „Haben wir Gesundheitsdaten in Microsoft 365?“ ehrlicher beantwortet werden sollte als im letzten Datenschutzgespräch. Er gehört zur Serie Microsoft 365 im Krankenhaus und richtet sich an IT-Leitung, Geschäftsführung, Informationssicherheit, Datenschutz, QM und die Interessenvertretung gleichermaßen.

Fakten auf einen Blick

- **Rechtsgrundlage:** § 393 SGB V, Cloud-Einsatz im Gesundheitswesen, in Kraft seit 1. Juli 2024.
- **Wer:** Leistungserbringer nach dem Vierten Kapitel SGB V – also auch zugelassene Krankenhäuser –, Kranken- und Pflegekassen und deren Auftragsverarbeiter.
- **Was:** Verarbeitung von Sozial- und Gesundheitsdaten mittels Cloud-Computing-Diensten.
- **Nachweis:** aktuelles C5-Testat des BSI, seit 1. Juli 2025 Typ 2 – oder ein gleichwertiger Nachweis nach der C5-Gleichwertigkeitsverordnung.
- **Und:** Umsetzung der im Prüfbericht ausgewiesenen Kundenkriterien durch das Krankenhaus selbst.

Was § 393 SGB V eigentlich verlangt

Bevor wir über Microsoft reden, lohnt ein Blick in den Gesetzestext selbst. Er ist im amtlichen Gesetzesportal des Bundes frei abrufbar und ist mit acht Absätzen erfreulich kurz – kürzer jedenfalls als die durchschnittliche Verfahrensanweisung zur Händedesinfektion. Wir fassen ihn hier inhaltlich zusammen; den genauen Wortlaut sollten Sie vor jeder Entscheidung selbst nachlesen, denn das SGB V wird gern und oft geändert.

Anwendungsbereich: Sozial- und Gesundheitsdaten im Cloud-Dienst

Absatz 1 erlaubt Leistungserbringern nach dem Vierten Kapitel des SGB V, Kranken- und Pflegekassen sowie deren Auftragsverarbeitern, Sozial- und Gesundheitsdaten mittels Cloud-Computing-Diensten zu verarbeiten – sofern die Voraussetzungen der folgenden Absätze erfüllt sind. Zugelassene Krankenhäuser sind Leistungserbringer im Sinne dieses Kapitels. Arztpraxen und Kassen fallen ebenfalls darunter, sind aber nicht Thema dieses Beitrags.

Der Knackpunkt steckt in zwei Begriffen. **Gesundheitsdaten** sind nicht nur Befunde und Diagnosen, sondern alles, was Rückschlüsse auf den Gesundheitszustand einer Person zulässt – die Belegungsliste einer Station inklusive. Und **Cloud-Computing-Dienst** ist alles, was Sie als Dienst aus einem Rechenzentrum eines Anbieters beziehen. Exchange Online, SharePoint Online, OneDrive und Teams fallen erkennbar in diese Kategorie.

Ort der Verarbeitung und Niederlassung

Absatz 2 regelt das Wo: Die Verarbeitung muss im Inland, in einem Mitgliedstaat der EU, in einem nach § 35 Absatz 7 SGB I gleichgestellten Staat – also EWR und Schweiz – oder in einem Drittstaat mit Angemessenheitsbeschluss nach Artikel 45 DSGVO stattfinden. Zusätzlich verlangt das Gesetz, dass die verarbeitende Stelle über eine Niederlassung im Inland verfügt.

Für die Praxis heißt das: Sie brauchen eine belastbare Aussage, wo Ihre Daten liegen und wo sie verarbeitet werden – inklusive Support- und Wartungszugriffen. Die Antwort „Irgendwo in Europa, glaube ich“ hält erfahrungsgemäß genau bis zur ersten Rückfrage der Aufsichtsbehörde.

C5-Testat und Kundenkriterien

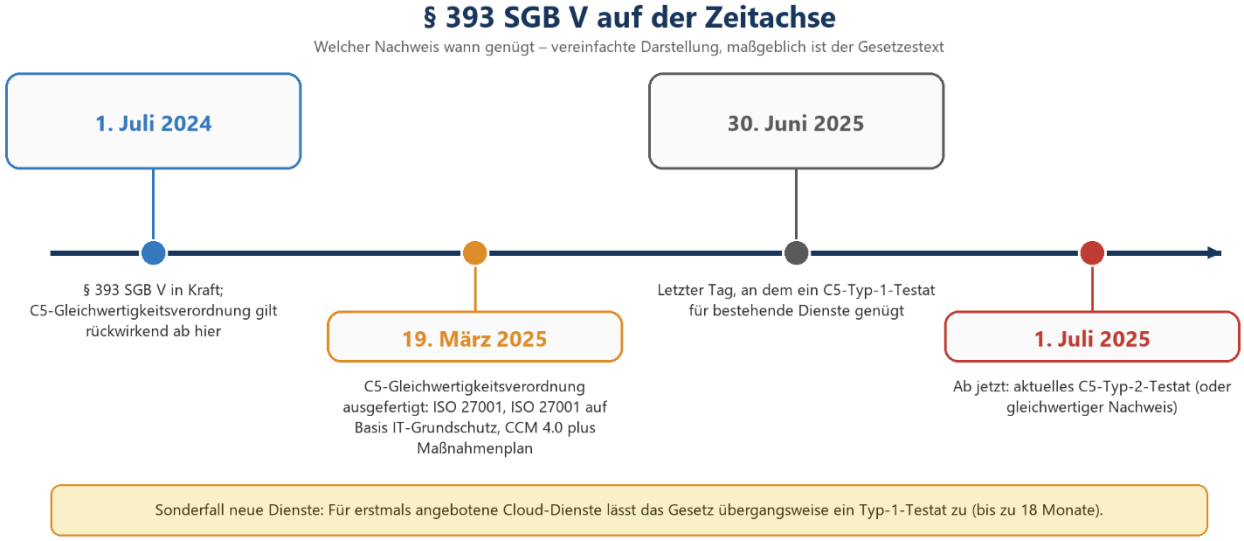
Absatz 3 nennt drei Bedingungen, die zusätzlich erfüllt sein müssen:

- Es sind **nach dem Stand der Technik angemessene technische und organisatorische Maßnahmen** zur Informationssicherheit getroffen.
- Für den Cloud-Dienst liegt ein **aktuelles C5-Testat** vor.
- Die im Prüfbericht ausgewiesenen **Kriterien für Kunden** – im C5 die korrespondierenden Kundenkriterien – sind umgesetzt.

Was „angemessen“ heißt, beantwortet Absatz 5 für Krankenhäuser mit einem Verweis auf § 391 SGB V: Wer die IT-Sicherheitsanforderungen für Krankenhäuser erfüllt, erfüllt insoweit auch diese Bedingung. Für Betreiber kritischer Anlagen gelten die Pflichten des BSI-Gesetzes. Wie § 391 SGB V, das BSIG nach dem NIS2-Umsetzungsgesetz und der branchenspezifische Sicherheitsstandard der DKG zusammenspielen, ist ein eigenes Thema; hier genügt: Ohne funktionierendes Informationssicherheitsmanagement im Haus ist § 393 SGB V nicht erfüllbar.

Typ 1, Typ 2 und der 1. Juli 2025

Absatz 4 regelt den Übergang. Bis zum 30. Juni 2025 genügte ein C5-Testat vom Typ 1, seit dem 1. Juli 2025 muss es ein Testat vom Typ 2 sein. Für Cloud-Dienste, die neu angeboten werden, lässt das Gesetz übergangsweise für bis zu 18 Monate ein Typ-1-Testat zu. Die Übergangsfrist für bestehende Dienste ist damit seit über einem Jahr abgelaufen – wer heute noch mit einem Typ-1-Bericht argumentiert, sollte sich zumindest einen guten Grund zurechtlegen.



Skizze 1: Die wichtigsten Daten rund um § 393 SGB V und die C5-Gleichwertigkeitsverordnung.

Gleichwertigkeit: die C5-Gleichwertigkeitsverordnung

Absatz 4 erlaubt neben dem C5-Testat auch gleichwertige Testate oder Zertifikate und ermächtigt das Bundesministerium für Gesundheit, im Einvernehmen mit dem BSI per Rechtsverordnung festzulegen, welche das sind. Das ist mit der **C5-Gleichwertigkeitsverordnung (C5GleichwV)** geschehen, ausgefertigt am 19. März 2025 und rückwirkend zum 1. Juli 2024 in Kraft. Als gleichwertig gelten danach Testierungen oder Zertifizierungen nach:

- ISO/IEC 27001 in der jeweils gültigen Fassung,
- ISO 27001 auf der Basis von IT-Grundschutz des BSI,
- Cloud Controls Matrix (CCM) in Version 4.0 in der jeweils gültigen Fassung.

Allein reicht das Zertifikat aber nicht. Der Anbieter braucht zusätzlich einen Maßnahmenplan, der die C5-Basiskriterien benennt, die der alternative Standard nicht abdeckt, die Maßnahmen zur Schließung dieser Lücken dokumentiert, eine Meilensteinplanung von höchstens zwölf Monaten enthält und belegt, dass ein C5-Typ-1-Testat binnen 18 und ein Typ-2-Testat binnen 24 Monaten angestrebt wird. Maßnahmenplan und Zertifikat muss der Anbieter dem Krankenhaus und den Aufsichtsbehörden auf Verlangen unverzüglich vorlegen.

Tipp: Gleichwertig heißt nicht bequem

Die Gleichwertigkeit ist vor allem für kleinere Anbieter gedacht, die ein C5-Testat erst aufbauen. Wenn ein Anbieter Ihnen „nur“ ein ISO-27001-Zertifikat vorlegt, fragen Sie konsequent nach dem Maßnahmenplan und dessen Meilensteinen. Fehlt der, fehlt der Nachweis. Das betrifft übrigens nicht nur Microsoft 365, sondern auch die vielen kleinen Cloud-Dienste rund um Dienstplan, Patientenportal oder Terminvergabe.

Was § 393 SGB V nicht regelt

Absatz 8 stellt klar, dass das SGB X und das Bundesdatenschutzgesetz unberührt bleiben. Daneben gelten die DSGVO, das Landesrecht – Landeskrankenhausgesetze und Landesdatenschutzgesetze, die sich von Bundesland zu Bundesland teils erheblich unterscheiden, etwa bei der Frage, ob und unter welchen Bedingungen Patientendaten außerhalb des Krankenhauses verarbeitet werden dürfen – sowie die strafrechtliche Schweigepflicht. Für kirchliche Häuser kommt das kirchliche Datenschutzrecht hinzu. § 393 SGB V ist also eine notwendige, keine hinreichende Bedingung. Ein C5-Testat beantwortet die Frage nach der Informationssicherheit beim Anbieter, nicht die Frage, ob die Verarbeitung insgesamt zulässig ist.

Ein Detail am Rande: Absatz 7 sieht vor, dass das Kompetenzzentrum für Interoperabilität im Gesundheitswesen testierte Cloud-Systeme auf Antrag veröffentlicht. Ein Eintrag dort ist ein Hinweis, aber kein Ersatz für Ihre eigene Prüfung des Berichts.

Die Anforderungen in einer Tabelle

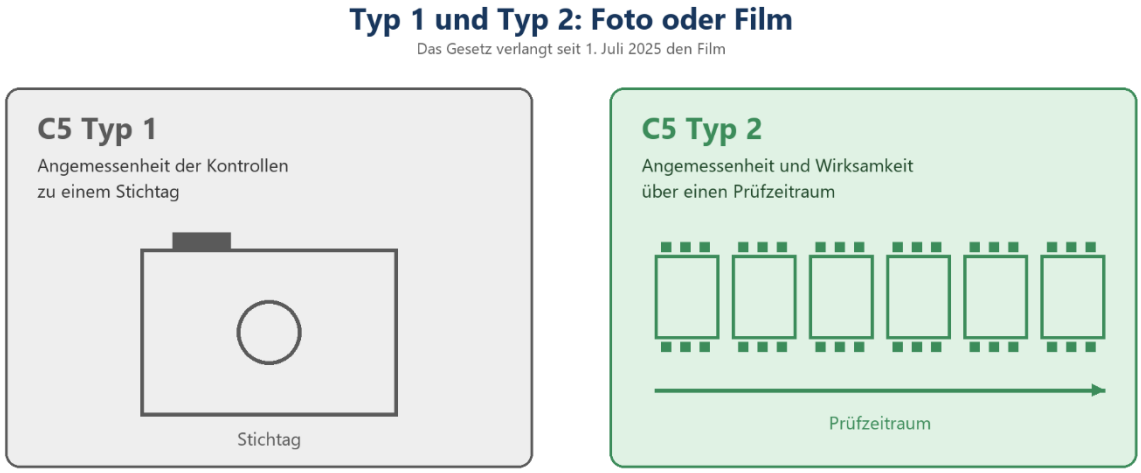
Anforderung	Was sie bedeutet	Wer liefert den Nachweis
Verarbeitungsort (Abs. 2)	Inland, EU, EWR, Schweiz oder Drittstaat mit Angemessenheitsbeschluss	Anbieter (Vertragsunterlagen, Datenresidenz-Zusagen, Umfeldparameter im Testat); Krankenhaus prüft und dokumentiert
Niederlassung im Inland (Abs. 2)	Die verarbeitende Stelle hat eine Niederlassung in Deutschland	Anbieter; Krankenhaus hält den Beleg in der Vertragsakte
Angemessene TOM (Abs. 3, 5)	Informationssicherheit nach Stand der Technik; für Krankenhäuser über § 391 SGB V bzw. BSIG	Krankenhaus (ISMS, B3S-Umsetzung, Prüfnachweise) – nicht der Anbieter
Aktuelles C5-Testat (Abs. 3, 4)	Seit 1. Juli 2025 Typ 2; Geltungsbereich muss den genutzten Dienst umfassen	Anbieter (Prüfbericht eines Wirtschaftsprüfers); Krankenhaus prüft Typ, Zeitraum und Geltungsbereich
Gleichwertiger Nachweis (Abs. 4, C5GleichwV)	ISO 27001, ISO 27001 auf Basis IT-Grundschutz oder CCM 4.0 plus Maßnahmenplan	Anbieter; Vorlage auf Verlangen unverzüglich
Kundenkriterien (Abs. 3)	Die im Prüfbericht dem Kunden zugewiesenen Kriterien sind umgesetzt	Krankenhaus – vollständig und allein

C5 lesen lernen: Typ, Zeitraum, Geltungsbereich

Der Kriterienkatalog C5 – Cloud Computing Compliance Criteria Catalogue – stammt vom BSI und beschreibt Mindestanforderungen an sichere Cloud-Dienste. Ein unabhängiger Wirtschaftsprüfer prüft den Anbieter dagegen und erteilt ein Testat samt Prüfbericht. Das ist kein Siegel, das man an die Tür klebt, sondern ein Bericht mit mehreren hundert Seiten. Wer ihn zum ersten Mal öffnet, erlebt einen ähnlichen Moment wie beim ersten Blick in die Konfiguration eines gewachsenen KIS: Es ist alles da, man muss nur wissen, wo.

Typ 1 und Typ 2

Der Unterschied ist schnell erklärt und folgenreich. Ein Testat vom Typ 1 bestätigt, dass die Kontrollen des Anbieters zu einem Stichtag angemessen ausgestaltet sind. Ein Testat vom Typ 2 bestätigt darüber hinaus, dass sie über einen Prüfzeitraum hinweg wirksam gearbeitet haben. Das eine ist das Foto vom aufgeräumten Lager am Tag der Begehung, das andere die Inventurliste des ganzen Jahres.



Skizze 2: Typ 1 prüft die Ausgestaltung zu einem Stichtag, Typ 2 die Wirksamkeit über einen Zeitraum.

Merkmal	C5 Typ 1	C5 Typ 2
Prüfgegenstand	Angemessenheit der Kontrollen (Design)	Angemessenheit und Wirksamkeit der Kontrollen
Bezugspunkt	Stichtag	Prüfzeitraum
Genügt nach § 393 SGB V	bis 30. Juni 2025; für neue Dienste übergangsweise bis zu 18 Monate	seit 1. Juli 2025 Regelfall
Aussagekraft für das Krankenhaus	Der Anbieter hat sich etwas vorgenommen	Der Anbieter hat es auch durchgehalten

Die Bestandteile eines Prüfberichts

Für Ihre Prüfung sind vier Teile des Berichts entscheidend:

- **Systembeschreibung:** Welche Dienste, Komponenten und Standorte geprüft wurden. Hier entscheidet sich der Geltungsbereich.

- **Umfeldparameter:** Angaben zu Gerichtsstand, Verarbeitungsorten, Erbringung des Dienstes und Offenlegungspflichten gegenüber Behörden. Das ist Ihr Material für Absatz 2.
- **Kriterien und Prüfergebnisse:** Je Kriterium die Kontrolle des Anbieters, die Prüfhandlung und das Ergebnis – inklusive Abweichungen.
- **Korrespondierende Kundenkriterien:** Was der Anbieter ausdrücklich vom Kunden erwartet, damit die eigenen Kontrollen wirken. Das ist Ihre Aufgabenliste.

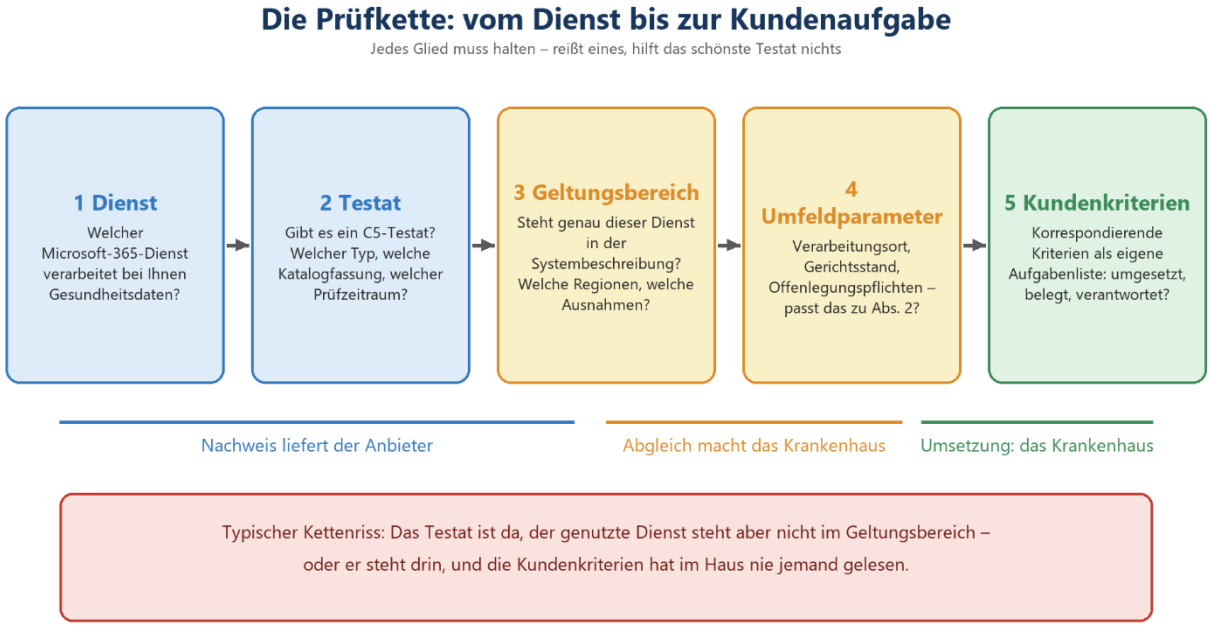
Achten Sie außerdem darauf, nach welcher Fassung des Katalogs geprüft wurde. Das BSI hat den C5 überarbeitet; welche Fassung für welchen Prüfzeitraum gilt, regelt das BSI auf seinen Seiten. Für Sie zählt: Die Fassung steht im Bericht, und ein Bericht, dessen Prüfzeitraum lange zurückliegt, ist kein „aktuelles“ Testat im Sinne des Gesetzes mehr. Wann genau die Grenze erreicht ist, ist eine Bewertungsfrage, die Sie mit Ihrem Datenschutz und im Zweifel juristisch klären sollten.

Warnung: Abweichungen nicht überblättern

Ein Testat kann Einschränkungen und Abweichungen enthalten. Wenn der Prüfer bei einem Kriterium Abweichungen festgestellt hat, gehört das in Ihre Risikobewertung – auch wenn das Gesamturteil positiv ausfällt. „Testat liegt vor“ ist ein Status, keine Inhaltsangabe.

Microsoft 365 prüfen: der Prüfauftrag in fünf Schritten

Jetzt zur Frage, die in jedem Lenkungsausschuss zuerst gestellt wird: „Ist Microsoft 365 C5-testiert?“ Die ehrliche Antwort lautet: Die Frage ist falsch gestellt. Microsoft 365 ist kein einzelner Dienst, sondern ein Bündel aus Dutzenden Diensten, Funktionen und Zusatzmodulen, die sich laufend ändern. Ob *der Dienst, den Sie nutzen,* im Geltungsbereich *des aktuellen Berichts* in *der geforderten Form* steht, können nur Sie anhand des Berichts beantworten. Wir machen dazu bewusst keine Aussage – nicht aus Vorsicht, sondern weil jede pauschale Aussage beim nächsten Berichtszyklus falsch sein kann.



Skizze 3: Die Prüfkette vom genutzten Dienst über Testat, Geltungsbereich und Umfeldparameter bis zu den Kundenkriterien.

Schritt 1: Dienste inventarisieren

Bevor Sie einen Bericht öffnen, brauchen Sie eine Liste: Welche Microsoft-Dienste nutzt Ihr Haus tatsächlich, und in welchen davon landen – geplant oder ungeplant – Gesundheitsdaten? Exchange Online, SharePoint Online, OneDrive, Teams mit Chat, Besprechungen und Aufzeichnungen, Forms, Planner, Power-Plattform, Copilot, Zusatzdienste von Drittanbietern im Teams-Store. Die Liste ist in der Regel länger als erwartet, besonders in einem Klinikverbund, in dem jeder Standort seine eigene Vorgeschichte mitbringt.

Schritt 2: Bericht im Service Trust Portal beschaffen

Microsoft stellt Prüfberichte im Service Trust Portal bereit. Die Anmeldung erfolgt mit einem Konto Ihres Tenants. Einen Überblick, wie Microsoft selbst das C5-Angebot beschreibt, gibt die Seite Cloud Computing Compliance Criteria Catalog (C5) auf Microsoft Learn. Laden Sie den Bericht herunter, der zu Ihrem Dienst passt, und legen Sie ihn mit Abrufdatum in der Vertragsakte ab. Prüfen Sie zusätzlich, ob es neben dem C5-Bericht weitere Berichte gibt, die für Ihre Dienste relevant sind, und welcher Bericht welche Dienstfamilie abdeckt.

Schritt 3: Typ, Fassung und Prüfzeitraum prüfen

Steht auf dem Bericht Typ 2? Nach welcher Fassung des C5 wurde geprüft? Welcher Prüfzeitraum ist angegeben, und wann wurde der Bericht erteilt? Notieren Sie diese drei Angaben in Ihrem Verzeichnis der Cloud-Dienste. Und setzen Sie sich eine Wiedervorlage: Berichte werden periodisch erneuert, und der nächste ist nicht automatisch identisch mit dem letzten.

Schritt 4: Geltungsbereich und Umfeldparameter abgleichen

Jetzt kommt die eigentliche Arbeit: Gleichen Sie Ihre Dienstliste aus Schritt 1 mit der Systembeschreibung ab. Steht jeder Dienst, in dem Gesundheitsdaten verarbeitet werden, ausdrücklich im Geltungsbereich? Gibt es Einschränkungen nach Region, Rechenzentrum oder Funktion? Passen die Umfeldparameter zu Absatz 2? Für jeden Dienst ohne Treffer gibt es genau zwei saubere Optionen: Gesundheitsdaten dort nicht verarbeiten oder einen anderen, gleichwertigen Nachweis finden.

Schritt 5: Kundenkriterien als eigene Aufgabenliste anlegen

Ziehen Sie die korrespondierenden Kundenkriterien aus dem Bericht heraus und machen Sie daraus eine Aufgabenliste mit Zuständigkeit, Umsetzungsstand und Nachweis. Das ist der Schritt, der in den meisten Häusern fehlt – und der Schritt, den § 393 Absatz 3 ausdrücklich verlangt. Dazu gleich mehr.

Tipp: Compliance Manager als Werkzeug, nicht als Ersatz

Laut Microsoft-Dokumentation bietet der Compliance Manager in Microsoft Purview eine Bewertungsvorlage für C5 an. Das kann helfen, Maßnahmen zu strukturieren und Nachweise zu sammeln. Ihre eigene Prüfung des Berichts und Ihre Bewertung ersetzt es nicht. Wie Purview in der Klinik sonst sinnvoll eingesetzt wird, beschreibt der Kompetenzbereich Microsoft Purview.

Wichtig: Wer prüft, dokumentiert

Halten Sie Ihr Prüfergebnis schriftlich fest: welcher Bericht, abgerufen wann, geprüft von wem, mit welchem Ergebnis je Dienst. Im QM-Handbuch oder im ISMS als Verfahrensanweisung „Prüfung von Cloud-Nachweisen“ abgelegt, ist das genau die Art Dokument, nach der im

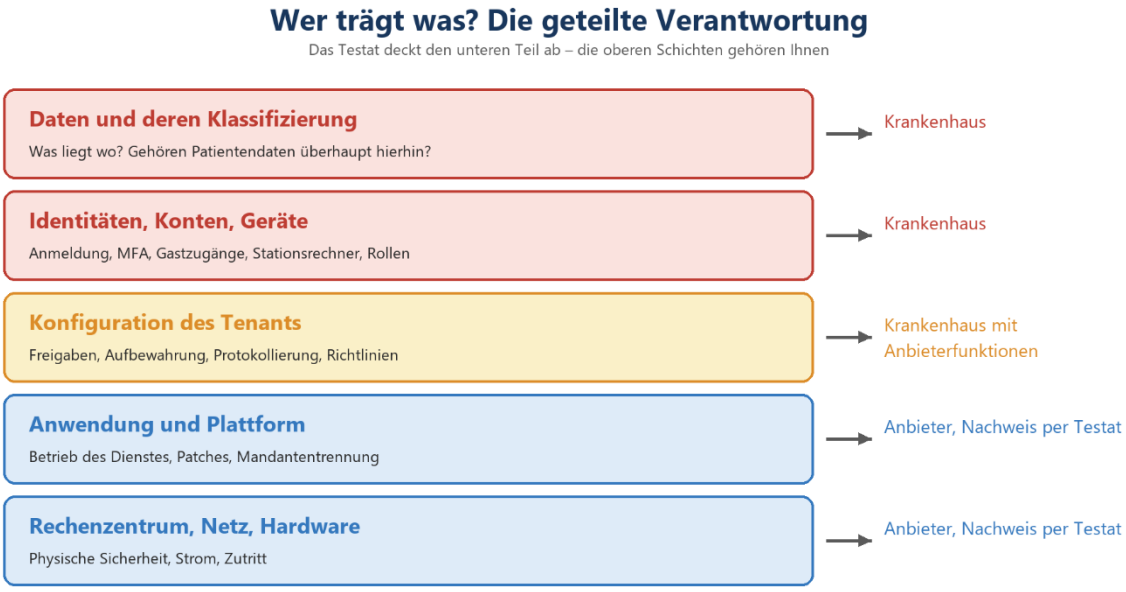
nächsten Audit gefragt wird.

Die Kundenkriterien landen beim Krankenhaus

Der Kernsatz dieses Beitrags

Das Testat des Anbieters ersetzt nicht Ihre eigenen Pflichten. Es belegt, dass der Anbieter seinen Teil erfüllt – unter der Voraussetzung, dass Sie Ihren Teil erfüllen. Die korrespondierenden Kundenkriterien landen beim Krankenhaus, und § 393 SGB V macht ihre Umsetzung zur gesetzlichen Bedingung.

Cloud-Sicherheit ist eine geteilte Verantwortung. Der Anbieter verantwortet Rechenzentrum, Hardware, Plattform und Betrieb des Dienstes. Sie verantworten, wer sich anmelden darf, was geteilt wird, welche Daten überhaupt hineingehören und wie die Konfiguration des Tenants aussieht. Kein Testat der Welt prüft, ob Ihr Gastzugang aus einem Projekt von vor vier Jahren noch Zugriff auf das Laufwerk der Pflegedirektion hat.



Skizze 4: Geteilte Verantwortung – was das Testat abdeckt und was beim Krankenhaus bleibt.

Typische Themenfelder der Kundenkriterien

Welche Kundenkriterien genau gelten, steht in Ihrem Bericht und nur dort. Erfahrungsgemäß drehen sie sich aber um wiederkehrende Themenfelder. Die folgende Tabelle ist eine Orientierung für die Aufgabenverteilung im Haus, keine Wiedergabe eines konkreten Berichts:

Themenfeld	Was typischerweise erwartet wird	Wer im Haus	Beispiel in Microsoft 365
Identitäten und Zugriff	Benutzerkonten verwalten, starke Authentifizierung, Berechtigungen regelmäßig	IT-Leitung, Administration	Entra ID: MFA, bedingter Zugriff, Zugriffsüberprüfungen (Microsoft Entra ID)

Themenfeld	Was typischerweise erwartet wird	Wer im Haus	Beispiel in Microsoft 365
	überprüfen		
Konfiguration und Härtung	Sicherheitsrelevante Einstellungen des Mandanten bewusst setzen und dokumentieren	Administration, ISB	Freigabe- und Gastrichtlinien, Sicherheitsstandards (Microsoft 365 Security)
Protokollierung und Überwachung	Protokolle aktivieren, auswerten und Vorfälle melden	ISB, IT-Betrieb	Überwachungsprotokoll, Warnungen, Meldeweg im Notfallhandbuch
Daten und Klassifizierung	Wissen, welche Daten wo liegen; Schutzbedarf festlegen	Datenschutz, Fachbereiche, QMB	Vertraulichkeitsbezeichnungen, DLP-Richtlinien in Purview
Endgeräte	Sichere Geräte und Clients beim Kunden	IT-Betrieb, Medizintechnik bei Schnittstellen	Geräteverwaltung, Stationsrechner, gemeinsam genutzte Geräte
Organisation und Schulung	Rollen, Prozesse, Sensibilisierung der Mitarbeiterinnen und Mitarbeiter	Geschäftsführung, ISB, Personalabteilung	Schulungskonzept (Microsoft 365 Schulung für Krankenhäuser)

Aus Kriterien wird eine Aufgabenliste

Bewährt hat sich ein schlichtes Vorgehen: Jedes Kundenkriterium wird eine Zeile in einer Liste mit den Spalten Kriterium, Bedeutung für unser Haus, zuständige Rolle, Umsetzungsstand, Nachweis und nächste Überprüfung. Die Liste gehört ins ISMS, nicht in den Kopf der einen Administratorin oder des einen Administrators, die oder der sich zufällig auskennt. Wenn ein neuer Bericht erscheint, wird die Liste abgeglichen – neue Kriterien kommen hinzu, geänderte werden neu bewertet.

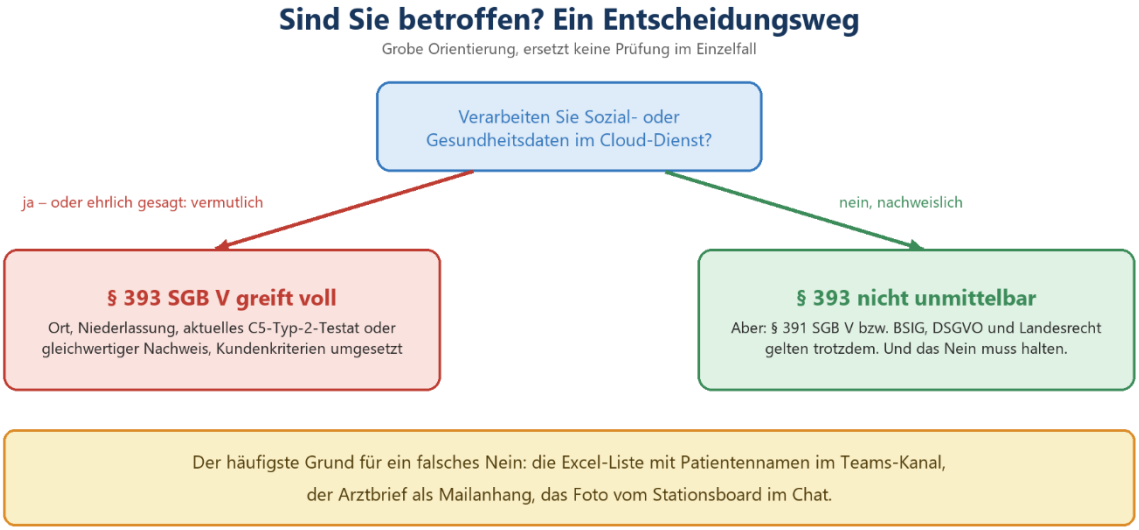
Für die Geschäftsführung ist die Liste übrigens das wertvollste Dokument der ganzen Übung: Sie zeigt auf einer Seite, was das Haus selbst leisten muss, damit die Cloud-Nutzung rechtlich trägt. Das ist eine andere Diskussion als „Microsoft ist doch zertifiziert“ – und eine deutlich ehrlichere.

Tipp: Kerberos, PKI und Konten nicht vergessen

Viele Kundenkriterien zu Identitäten wirken nur, wenn das lokale Active Directory sauber ist – denn von dort werden die Konten in aller Regel synchronisiert. Alte Vertrauensstellungen, NTLM-Altlasten und verwaiste Dienstkonten im Klinikverbund untergraben jede noch so gute Cloud-Konfiguration. Aus der langjährigen Begleitung eines Krankenhausverbunds mit mehreren Standorten wissen wir: Dieser Teil dauert länger als die Cloud-Einstellungen, lohnt sich aber am meisten.

Wer ist wie betroffen: Gesundheitsdaten in Microsoft 365 oder nicht

Die Grundhaltung dieser Serie ist klar: Patientendaten gehören ins KIS und seine Subsysteme – LIS, RIS, PACS und die übrigen Klinikanwendungen. Microsoft 365 ist das Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit. Wie diese Grenze im Alltag gezogen wird, beschreibt der Beitrag Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt. Für § 393 SGB V ist diese Grenze entscheidend, denn sie bestimmt, wie stark Sie betroffen sind.



Skizze 5: Grober Entscheidungsweg zur Betroffenheit nach § 393 SGB V.

Drei typische Ausgangslagen

Ausgangslage	Bedeutung für § 393 SGB V	Was zu tun ist
Microsoft 365 nur für Verwaltung, QM und Gremien – nachweislich ohne Gesundheitsdaten	Nicht unmittelbar betroffen, solange die Abgrenzung hält	Abgrenzung dokumentieren, technisch absichern (Klassifizierung, DLP), Mitarbeiterinnen und Mitarbeiter schulen, regelmäßig prüfen
Gesundheitsdaten werden bewusst und geregelt verarbeitet, etwa in einem klar umrissenen Anwendungsfall	Voll betroffen	Prüfkette vollständig durchlaufen, Kundenkriterien umsetzen, Rechtsgrundlagen nach Landesrecht und Schweigepflicht klären
Offiziell keine Gesundheitsdaten – faktisch doch (Listen, Mailanhänge, Fotos im Chat)	Betroffen, aber ohne Nachweis: die ungünstigste Lage	Bestandsaufnahme, Bereinigung, klare Regeln, technische Leitplanken – und ehrliche Kommunikation an die Geschäftsführung

Die Realität mit der Excel-Liste

Machen wir uns nichts vor: In vielen Häusern gibt es sie, die Excel-Liste mit Patientennamen, Zimmernummern und Bemerkungen, die irgendwann jemand in einen Teams-Kanal gelegt hat, damit die Übergabe schneller geht. Das ist nicht böse Absicht, sondern Pragmatismus im Schichtdienst, wenn das KIS an einer Stelle umständlich ist. Es ist aber auch nicht der Normalfall, den man in ein Konzept schreibt – und es ist genau die Stelle, an der aus „Wir verarbeiten keine Gesundheitsdaten in der Cloud“ ein Satz mit sehr kurzer Haltbarkeit wird.

Warnung: Das falsche Nein ist teurer als das ehrliche Ja

Wer im Verzeichnis der Verarbeitungstätigkeiten „keine Gesundheitsdaten in Microsoft 365“ einträgt, ohne das zu prüfen, hat im Ernstfall weder die Abgrenzung noch die Nachweise nach § 393 SGB V. Besser: Bestandsaufnahme mit den Werkzeugen, die der Tenant ohnehin bietet, dann entscheiden, was ins KIS zurückgehört und was bleiben darf – mit sauberer Rechtsgrundlage.

Auch das „Nein“ braucht übrigens einen Nachweis. Wenn Sie sich auf den Standpunkt stellen, dass § 393 SGB V Sie mangels Gesundheitsdaten nicht betrifft, müssen Sie das im Zweifel belegen können: mit einer dokumentierten Regelung, technischen Leitplanken wie Vertraulichkeitsbezeichnungen und Richtlinien zur Verhinderung von Datenverlust und mit Stichproben. Warum Krankenhäuser in dieser Frage anders ticken als eine Stadtverwaltung oder ein Mittelständler, erläutert Microsoft 365 im Krankenhaus: Warum die Klinik anders tickt als Verwaltung und Mittelstand.

Trägerschaft, Landesrecht und Interessenvertretung

§ 393 SGB V gilt für alle zugelassenen Krankenhäuser, unabhängig vom Träger. Was daneben gilt, unterscheidet sich: Öffentliche und kommunale Häuser unterliegen dem jeweiligen Landesdatenschutzgesetz und dem Landeskrankenhausgesetz ihres Bundeslandes, kirchliche Häuser zusätzlich dem kirchlichen Datenschutzrecht, private Träger der DSGVO und dem BDSG. Einige Landeskrankenhausgesetze enthalten eigene, teils strengere Vorgaben zur Verarbeitung von Patientendaten durch Dritte, andere verweisen weitgehend auf das allgemeine Datenschutzrecht. Kein Bundesland ist hier der Maßstab für alle anderen – prüfen Sie Ihr eigenes.

Und weil die Kundenkriterien regelmäßig Protokollierung und Überwachung betreffen, sitzen Betriebsrat, Personalrat oder Mitarbeitervertretung schneller mit am Tisch, als die IT es plant. Das ist kein Hindernis, sondern eine gute Gelegenheit, die Regeln einmal sauber festzuhalten.

Hinweis: Keine Rechtsberatung

Dieser Beitrag beschreibt die Rechtslage und ein praktisches Vorgehen nach bestem Wissen zum Stand Oktober 2026. Er ist keine Rechtsberatung. Ob und wie Ihr Krankenhaus Gesundheitsdaten in einem Cloud-Dienst verarbeiten darf, hängt von Trägerschaft, Bundesland, kirchlichem Recht, Verträgen und dem konkreten Anwendungsfall ab. Bewerten Sie das gemeinsam mit Ihrem Datenschutzbeauftragten und lassen Sie es im Zweifel juristisch prüfen.

Häufige Fragen (FAQ)

Ist Microsoft 365 C5-testiert?

Diese Frage beantworten wir bewusst nicht pauschal. Microsoft veröffentlicht Prüfberichte im Service Trust Portal. Ob der Dienst, den Sie nutzen, im Geltungsbereich des aktuellen Berichts steht und welcher Testattyp vorliegt, prüfen Sie anhand des Berichts selbst – und zwar bei jedem neuen Berichtszyklus erneut.

Reicht es, das Testat in der Vertragsakte abzulegen?

Nein. § 393 SGB V verlangt zusätzlich, dass das Krankenhaus die im Prüfbericht ausgewiesenen Kundenkriterien umsetzt und angemessene eigene Sicherheitsmaßnahmen trifft. Das Testat ist Voraussetzung, nicht Erledigung.

Was ist der Unterschied zwischen C5 Typ 1 und Typ 2?

Typ 1 bestätigt die angemessene Ausgestaltung der Kontrollen zu einem Stichtag, Typ 2 zusätzlich deren Wirksamkeit über einen Prüfzeitraum. Seit 1. Juli 2025 verlangt § 393 SGB V für bestehende Dienste Typ 2.

Gilt ein ISO-27001-Zertifikat als gleichwertig?

Nach der C5-Gleichwertigkeitsverordnung ja – aber nur zusammen mit einem Maßnahmenplan, der die Lücken zum C5 benennt, ihre Schließung binnen zwölf Monaten plant und den Weg zum C5-Testat belegt. Ohne diesen Plan ist das Zertifikat allein kein ausreichender Nachweis.

Wir verarbeiten keine Patientendaten in Microsoft 365. Betrifft uns § 393 SGB V trotzdem?

Unmittelbar nicht, solange das stimmt. Sie sollten die Abgrenzung aber dokumentieren und technisch absichern. Die IT-Sicherheitspflichten nach § 391 SGB V beziehungsweise dem BSIG, die DSGVO und das Landesrecht gelten ohnehin.

Wer im Krankenhaus ist für die Prüfung zuständig?

Das legt Ihre Organisation fest. Bewährt hat sich: IT-Leitung beschafft und prüft den Bericht technisch, Informationssicherheit bewertet Abweichungen und führt die Liste der Kundenkriterien, der Datenschutz prüft Verarbeitungsort und Rechtsgrundlage, die Geschäftsführung trägt die Entscheidung.

Wie oft muss die Prüfung wiederholt werden?

Immer dann, wenn ein neuer Bericht erscheint, wenn Sie neue Dienste einführen oder wenn sich die Nutzung ändert – etwa durch Copilot oder neue Teams-Anwendungen. Eine feste Wiedervorlage im ISMS verhindert, dass das Testat still veraltet.

Ersetzt das C5-Testat die Auftragsverarbeitungsvereinbarung?

Nein. Testat und Vertrag beantworten unterschiedliche Fragen. Die datenschutzrechtliche Ausgestaltung der Auftragsverarbeitung, die Schweigepflicht und landesrechtliche Vorgaben bleiben eigene Prüfpunkte.

Fazit: Das Testat ist der Anfang der Prüfung, nicht ihr Ende

§ 393 SGB V ist eine der klarer formulierten Vorschriften im Gesundheitswesen: Ort, Niederlassung, angemessene Sicherheit, aktuelles C5-Testat vom Typ 2 oder ein gleichwertiger

Nachweis, umgesetzte Kundenkriterien. Der Anbieter liefert das Testat. Den Abgleich mit Ihren Diensten und die Umsetzung der Kundenkriterien liefert Ihr Haus – und niemand sonst.

Für Microsoft 365 bedeutet das einen wiederkehrenden Prüfauftrag statt einer einmaligen Ja-Nein-Antwort: Dienste inventarisieren, Bericht im Service Trust Portal beschaffen, Typ und Zeitraum prüfen, Geltungsbereich abgleichen, Kundenkriterien als Aufgabenliste führen. Und vorher die ehrliche Frage beantworten, ob Gesundheitsdaten überhaupt dorthin gehören. Wenn Sie diese Prüfung strukturiert aufsetzen möchten oder einen zweiten Blick auf Ihren Tenant brauchen, unterstützt Sie die Microsoft 365 Beratung für Krankenhäuser. Der Galgenhumor darf bleiben – die Excel-Liste mit Patientennamen im Teams-Kanal nicht.

Weiterlesen

› Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt

› NIS2 technisch umsetzen mit Microsoft 365

› Microsoft 365 Beratung für Krankenhäuser