Piltz Legal

Gutachten zu Fragen der Mitglieder des Bundesverband Gesundheits-IT – bvitg e.V.

Vorab zum Hintergrund des beauftragten Gutachtens:

Am 14. Dezember 2023 verabschiedete der Bundestag in 2. und 3. Lesung das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – „**DigiG**"), welches u.a. Änderungen des Fünften Buches Sozialgesetzbuch beinhaltet. Dabei sind die Regelungen hinsichtlich Cloud-Computing von besonderem Interesse.

§ 384 Ziffer 5 DigiG enthält die Definition von „Cloud-Computing-Dienst", § 384 Ziffer 6 DigiG legt fest, was unter einem „aktuellem C5-Testat" verstanden wird und § 393 DigiG enthält Anforderungen, welche bei der Verarbeitung von Sozial- und Gesundheitsdaten zu beachten sind.

Die Regelungen werfen diverse Fragen auf. Die in diesem Dokument enthaltenen Fragen sollen in einem Rechtsgutachten beantwortet sowie die Kernaussagen des Rechtsgutachtens in einer etwa zweistündigen Web-Konferenz den Mitgliedern kurz vorgestellt werden.

Dieses Gutachten wurde von der Kanzlei Piltz Rechtsanwälte PartGmbB (Südwestkorso 3, 12161 Berlin, nachfolgend auch „**wir**" oder „**uns**") erstellt und vom Bundesverband Gesundheits-IT – bvitg e.V. (im Folgenden auch „**bvitg**") beauftragt.

Stand: 2. Mai 2024

Piltz Legal

Inhalt

A. Übersicht zu Fragen und Antworten

Innerhalb dieses Gutachtens werden verschiedene Fragen zu den gesetzlichen Neuerungen im Bereich der Cloud-Computing-Dienste beantwortet. In den nachfolgenden Abschnitten werden die Fragen aufgelistet, die Antworten in Kurzform zusammengefasst und sodann ausführlicher beantwortet. In der nachfolgenden Tabelle finden Sie eine Übersicht zu den Fragen, den Antworten in Kurzform und Verweise auf die Seiten dieses Gutachtens, auf denen Sie die ausführlichen Antworten nachlesen können.

Ziffer der Frage	Die Frage	Die Antwort in Kurzform	Seiten im Gutachten
1. 1) a)	Sind die Definitionen aus der DSGVO im Kontext der Regelungen § 393 SGB V anzuwenden?	Ja, die Definitionen aus der DSGVO sind im Kontext der Regelungen des § 393 SGB V anzuwenden.	**Ab Seite *11***
1. 1) b)	Werden genetische Daten von der Erlaubnisnorm ebenfalls erfasst, d.h. zählen genetische Daten zu Gesundheitsdaten?	Ja, genetische Daten sind zum Teil erfasst. Genetische Daten sind manchmal aber nicht immer Gesundheitsdaten und können auch Sozialdaten sein und dann der Vorschrift unterfallen.	**Ab Seite *12***
1. 1) c)	Oder sind genetische Daten von § 393 SGB V nicht erfasst, d.h. die Regelungen von § 393 SGB V gelten nicht für genetische Daten?	Die Regelungen aus § 393 Abs. 1 SGB V gelten dann nicht, wenn die genetischen Daten weder Gesundheitsdaten sind noch von einer in § 35 SGB I genannten Stelle im Hinblick auf Aufgaben nach dem SGB I verarbeitet werden und deswegen auch keine Sozialdaten sind.	**Ab Seite *14***
1. 2) a)	Dürfen Beschäftigtendaten im Cloud-Kontext verarbeitet werden, da durch die in § 393 Abs. 1 SGB V enthaltene Erlaubnis der Verarbeitung von Sozial- und Gesundheitsdaten implizit auch die Erlaubnis zur Verarbeitung von Beschäftigtendaten (z.B. zur Zugriffsverwaltung) enthalten ist?	Nein, § 393 Abs. 1 SGB V enthält nicht implizit auch eine Erlaubnis zur Verarbeitung von Beschäftigtendaten. Trotzdem ist der auf Basis von § 393 Abs. 1 SGB V legitimierte Einsatz eines Cloud-Computing-Dienstes ein Stück weit ein Indiz für die Legitimität der Verarbeitung der erforderlichen Beschäftigtendaten. Die Zulässigkeit der Datenverarbeitung ist im Einzelfall jedoch anhand der Vorgaben aus der DSGVO und dem BDSG zu bestimmen.	**Ab Seite *15***
1. 2) b)	Dürfen aus demselben Grund (implizite Erlaubnis durch die Regelung in § 393 SGB V) biometrische Daten verarbeitet werden?	Nein. Wenn biometrische Daten als Gesundheits- oder Sozialdaten verarbeitet werden, dann ist deren Verarbeitung auf Basis von § 393 Abs. 1 SGB V ggf. legitimierbar. In anderen Fällen muss die Zulässigkeit der Verarbeitung von biometrischen Daten anhand einer anderen Rechtsgrundlage geprüft werden.	**Ab Seite *15***
1. 2) c)	Oder dürfen Beschäftigtendaten und biometrische Daten nur verarbeitet werden, wenn ein anderer Erlaubnistatbestand als § 393 SGB V die Verarbeitung dieser Daten erlaubt?	Wenn Beschäftigtendaten oder biometrische Daten entweder Gesundheits- oder Sozialdaten sind, dann ist § 393 SGB V anwendbar. In allen anderen Fällen ist die Rechtmäßigkeit der Datenverarbeitungen anhand der Vorgaben aus der DSGVO und dem BDSG zu bestimmen.	**Ab Seite *15***

2. 1)	Stand heute ist unklar, welche Begriffsbestimmung im deutschen NIS2-Umsetzungsgesetz seitens des deutschen Gesetzgebers gewählt wird. Da die Begriffsbestimmung in § 384 Ziffer 5 SGB V dem Wortlaut der Definition in Art. 6 Ziff. 30 NIS2-RL entspricht: Kann die Definition angewendet werden, auch wenn im deutschen NIS2-Umsetzungsgesetz eine andere Definition verwendet wird?	Ja, die Definition aus Art. 6 Nr. 30 NIS2-RL kann angewendet werden. Es ist wegen der gleichzeitigen Relevanz des Begriffs für das BSI-Gesetz („BSIG") theoretisch nur möglich, dass der deutsche Gesetzgeber die Definition noch weiter fasst oder lediglich sprachlich anders formuliert, wobei der Anwendungsbereich jedoch mindestens genauso groß sein muss, wie derjenige der Definition aus der Richtlinie. In den aktuell vorliegenden Entwürfen für das NIS2-Umsetzungsgesetz ist aber eine Intention zur Verwendung eines anderen Begriffs nicht erkennbar.	**Ab Seite *16***
2. 2) a)	Welche Gegebenheiten müssen erfüllt sein, damit die Definition eines Cloud-Computing-Dienst im Sinne des § 384 Ziffer 5 SGB V (im Folgenden nur als „Definition" bezeichnet) erfüllt ist?	Es muss ein digitaler Dienst[1] vorliegen, der durch Abruf die Verwaltung[2] und einen umfassenden Fernzugang[3] zu einem skalierbaren[4] und elastischen[5] Pool gemeinsam nutzbarer[6] Rechenressourcen[7] ermöglicht.	**Ab Seite *19***
2. 2) b)	Stellt jede über einen Fernzugang (= Internetnutzung) erreichbare Ressource (KIS, PVS, TI WANDA Dienst …) einen Cloud-Computing Dienst im Sinne der Definition dar?	Nein, nicht jede über einen Fernzugang erreichbare Ressource ist auch ein Cloud-Computing Dienst im Sinne der Definition, weil neben dem Vorhandensein eines umfassenden Fernzugangs auch andere Merkmale der Begriffsdefinition erfüllt sein müssen. Bspw. wenn der Fernzugang zu einer anderen Ressource als einer Rechenressource bereitgestellt wird, dann liegt kein Cloud-Computing-Dienst vor. Es kommt zusätzlich vor	**Ab Seite *20***

[1] Art. 1 Abs. 1 lit. b Richtlinie (EU) 2015/1535: Gemäß dieser Vorschrift geht es dann um einen digitalen Dienst, wenn eine Dienstleistung der Informationsgesellschaft vorliegt. Das meint jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.

[2] ErwGr. 33 Satz 6 zur NIS2-RL: „*Dass sich der Cloud-Computing-Nutzer selbst ohne Interaktion mit dem Anbieter von Cloud-Computing-Diensten Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann, könnte als Verwaltung auf Abruf beschrieben werden.*"

[3] ErwGr. 33 Satz 7 zur NIS2-RL: „*Der Begriff „umfassender Fernzugang" wird verwendet, um zu beschreiben, dass die Cloud-Kapazitäten über das Netz bereitgestellt und über Mechanismen zugänglich gemacht werden, die den Einsatz heterogener Thin- oder Thick-Client-Plattformen (einschließlich Mobiltelefonen, Tablets, Laptops und Arbeitsplatzrechnern) fördern.*"

[4] ErwGr. 33 Satz 8 zur NIS2-RL: „*Der Begriff „skalierbar" bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können.*"

[5] ErwGr. 33 Satz 9 zur NIS2-RL: „*Der Begriff „elastischer Pool" wird verwendet, um Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die Menge der verfügbaren Ressourcen je nach Arbeitsaufkommen rasch erhöht oder reduziert werden kann.*"

[6] ErwGr. 33 Satz 10 zur NIS2-RL: „*Der Begriff „gemeinsam nutzbar" wird verwendet, um Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird.*"

[7] ErwGr. 33 Satz 2 bis 4 zur NIS2-RL: „*Zu Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Betriebssysteme, Software, Speicher, Anwendungen und Dienste. Zu den Dienstmodellen des Cloud-Computing gehören unter anderem IaaS (Infrastructure as a Service, PaaS (Platform as a Service), SaaS (Software as a Service) und NaaS (Network as a Service). Die Bereitstellungsmodelle für Cloud-Computing sollten die private, die gemeinschaftliche, die öffentliche und die hybride Cloud umfassen.*"

		allem darauf an, ob der Dienst auf Abruf die Verwaltung ermöglicht, der Pool skalierbar und elastisch ist und der Dienst eine gemeinsame Nutzung von Rechenressourcen ermöglicht.	
2. 2) c)	Stellt die für den Fernzugang verwendete Cloud-Technologie ebenfalls einen Cloud-Computing Dienst im Sinne der Definition dar?	Es kommt darauf an, ob so eine Technologie auch alle Merkmale der Begriffsdefinition erfüllt. Ist dies der Fall, dann ja. Ist dies nicht der Fall, dann nein. Nur weil für den Fernzugang an sich eine Cloud-Technologie verwendet wird, scheidet das Vorliegen eines Cloud-Computing-Dienstes noch nicht kategorisch aus. Es kommt vor allem darauf an, ob der Dienst auf Abruf die Verwaltung ermöglicht, der Pool skalierbar und elastisch ist und der Dienst eine gemeinsame Nutzung von Rechenressourcen ermöglicht.	**Ab Seite *21***
2. 2) d)	Wenn skalierbare Ressourcen wie Arbeitsspeicher, Datenspeicher oder CPU im Rechenzentrum nach Bedarf gebucht werden können, stellen dann die unter der vorhergehenden Frage beschriebene Dienste einen Cloud-Computing Dienst im Sinne der Definition dar?	Es kommt darauf an, ob auch das Definitionsmerkmal „die gemeinsame Nutzung ermöglicht“ erfüllt ist. Ist dies der Fall, dann ja. Ist dies nicht der Fall, dann nein.	**Ab Seite *21***
2. 2) e)	Stellt ein sog. Housing im Rechenzentrum einen Cloud-Computing Dienst im Sinne der Definition nach?	Nein, weil beim in der ausführlichen Antwort näher beschriebenen Housing die Dienstleistung nicht elektronisch erbracht wird und somit kein elektronischer Dienst vorliegt, ist das Housing auch keine Form von Cloud-Computing-Dienst. Der Fall ist dann anders zu beurteilen, wenn das Housing in Form der Bereitstellung virtueller Maschinen erfolgt und deswegen ein digitaler Dienst vorliegt. In so einem Fall erfolgt das virtuelle Housing auch in Form eines Cloud-Computing-Dienstes, sofern alle anderen Definitionsmerkmale erfüllt sind.	**Ab Seite *22***
2. 2) f)	Stellt eine in einer Cloud-Umgebung gehostete Anwendung, z.B. eine Software zur klinischen Entscheidungshilfe oder auch ein PVS/KIS, einen Cloud-Computing-Dienst im Sinne der Definition dar?	Ja, sofern für den Dienst die Verarbeitung hinsichtlich der Nutzer separat erfolgt. „Separat“ verlangt eine Form von Mandantentrennung. Es sprechen mehrere Argumente dafür, dass der „Cloud-Nutzer“ in diesem Sinne ein Unternehmen und keine Einzelperson ist.	**Ab Seite *23***

2. 2) g) i) und ii)	i) Fällt eine von einem Hoster bereitgestellte Vmware-vSphere-Umgebung unter die Definition eines Cloud-Computing-Dienstes? ii) D.h., sind diese Hoster Cloud-Anbieter, wenn sie über das Internet erreichbare vSphere-Umgebungen anbieten?	Wenn ein Anbieter die Infrastruktur inkl. Server und das Betriebssystem bereitstellt, dann ist der bereitgestellte Dienst nicht allein deswegen kein Cloud-Computing-Dienst, weil lediglich die Infrastruktur inkl. Server und das Betriebssystem bereitgestellt werden. Denn hier geht es um Rechenressourcen, die im Rahmen der Begriffsdefinition für einen Cloud-Computing-Dienst vorliegen müssen. Ein Hoster ist dann ein Anbieter eines Cloud-Computing-Dienstes, wenn er den Cloud-Dienst unter seinem eigenen Namen oder unter seiner eigenen Marke vermarktet oder unter fremder Marke vertreibt oder vertreiben lässt. Im Kontext des § 393 SGB V ist jedoch zu beachten, dass diese Vorschrift nicht nur für Anbieter eines Cloud-Computing-Dienstes gilt, sondern für Leistungserbringer und Kranken- und Pflegekassen und deren Auftragsverarbeiter.	**Ab Seite *25***
2. 2) h) i) und ii)	i): Stellt diese Bereitstellung von medizinischen Katalogdaten ohne Personenbezug einen Cloud-Computing-Dienst im Sinne der Definition dar? ii): Wenn die in der Cloud bereitgestellten nicht personenbezogenen Katalogdaten ohne lokale Zwischenspeicherung direkt in der lokal laufenden Applikation verwendet werden: stellt diese direkte Nutzung von medizinischen Katalogdaten ohne Personenbezug einen Cloud-Computing-Dienst im Sinne der Definition dar?	Für das Vorliegen eines Cloud-Computing-Dienstes kommt es nicht darauf an, ob die mit so einem Dienst verarbeiteten Daten einen Personenbezug haben oder nicht. Die beschriebene Bereitstellung von medizinischen Katalogdaten ohne Personenbezug erfolgt dann als Cloud-Computing-Dienst, wenn alle Definitionsmerkmale erfüllt sind. Dabei kommt es nicht auf den Personenbezug der Daten an. Es kommt für das Vorliegen der Begriffsmerkmale auch nicht darauf an, ob in einer Cloud gespeicherte Informationen nur ohne Zwischenspeicherung in einer lokal verwendeten Applikation genutzt werden.	**Ab Seite *26***
2. 2) h) iii)	Wenn eine der beiden oder auch beide Fragen mit „ja“ beantwortet werden, sind dann die Regelungen von § 393 SGB V anzuwenden, auch wenn kein Personenbezug existiert?	Nein, weil die Regelungen aus § 393 SGB V alle nur für die Verarbeitung von Sozial- und Gesundheitsdaten gelten und diese Datenarten immer personenbezogen sind.	**Ab Seite *27***
2. 2) h) iv)	Stellt eine über einen Fernzugang erreichbare Ressource, welche Metainformationen zu lokal	Für das Vorliegen eines Cloud-Computing-Dienstes kommt es nicht darauf an, ob Metainformationen zu lokal	**Ab Seite *27***

	verwendeten Applikationen verarbeitet und auf Basis dieser Informationen Dateien zum Download bereitstellt (Applikationsdaten, Kataloge etc.), einen Cloud-Dienst im Sinne der Definition dar?	verwendeten Applikationen verarbeitet werden. Der in der Frage geschilderte Dienst kann grundsätzlich alle Definitionsmerkmale eines Cloud-Computing-Dienstes erfüllen.	
2. 2) i)	Bei Online-Terminvereinbarungen zwischen Patienten und Leistungserbringern werden Gesundheitsdaten verarbeitet. Wenn bei dieser Onlineterminvereinbarung eine Speicherung dieser Daten nur temporär und verschlüsselt in der Cloud erfolgt, ist dann für diesen Dienst ein BSI-C5-Testat notwendig?	Der Umstand, dass die verarbeiteten Daten verschlüsselt sind und nur temporär gespeichert werden, ist für das Vorliegen eines Cloud-Computing-Dienstes nicht relevant. Die Dauer der Datenverarbeitung ist für das Vorliegen einer Verarbeitung personenbezogener Daten nicht relevant und daher auch nicht für die Anwendbarkeit des § 393 SGB V maßgeblich. Dasselbe gilt auch für eine Verschlüsselung in dem in der Frage beschriebenen Fall. Das Testat kann auch für längere Zeit als „aktuell“ gelten, solange es noch nicht abgelaufen ist und die faktischen, attestierten Gegebenheiten weiterhin mit der Wirklichkeit übereinstimmen und § 393 Abs. 4 SGB V zu dem relevanten Zeitpunkt nicht einen anderen Typ von Testat (bspw. Typ2) verlangt.	**Ab Seite *28***
2. 3) a)	Ist es richtig, dass ein Rechenzentrumsdienst kein Cloud-Computing-Dienst im Sinne des § 384 Ziffer 5 SGB V sein kann, auch wenn der Rechenzentrumsdienst in einem von einem Dienstleister bereitgestellten externen Rechenzentrum betrieben wird?	Nein, es ist nicht richtig, dass ein Rechenzentrumsdienst – der in einem von einem Dienstleister bereitgestellten externen Rechenzentrum betrieben wird – kein Cloud-Computing-Dienst im Sinne des § 384 Nr. 5 SGB V sein kann. Ausweislich ErwGr. 35 Satz 1 zur NIS2-RL ist ein Rechenzentrumsdienst manchmal aber nicht immer auch ein Cloud-Computing-Dienst.	**Ab Seite *30***
2. 3) b)	Wenn die Antwort auf Frage a) ja lautet: Anhand welcher Kriterien kann zwischen „Cloud-Computing-Dienst“ und „Rechenzentrumsdienst“ differenziert werden?	Die Antwort lautete zwar „nein“, aber wir möchten trotzdem kurz auf die Abgrenzung beider Arten von Diensten eingehen. Ein Rechenzentrumsdienst wäre dann kein Cloud-Computing-Dienst, wenn der Rechenzentrumsdienst: • nicht elektronisch erbracht wird und deswegen kein „digitaler Dienst“ ist oder • keinen umfassenden Fernzugang ermöglicht oder • nicht in Bezug auf Rechenressourcen erbracht wird oder • der Pool nicht skalierbar ist oder • der Pool nicht elastisch ist oder	**Ab Seite *30***

		• nicht gemeinsam nutzbar ist.	
3. 1) a)	Können amerikanische Hyperscaler (Microsoft, AWS, Google etc.) auch genutzt werden, wenn der Angemessenheitsbeschluss der EU-Kommission vom EuGH annulliert wird, sofern ausschließlich Rechenzentren in Europa zur Verarbeitung genutzt werden, der Hyperscaler über eine Niederlassung im Inland verfügt, jedoch im Rahmen der Fernwartung des Cloud-Systems ein Fernzugriff aus den USA aufgrund der Notwendigkeit der Hinzuziehung eines entsprechenden spezialisierten Technikers nicht 100%ig sicher ausgeschlossen werden kann?	Die in der Frage explizit genannten Umstände führen nicht dazu, dass durch einen tatsächlich auch erfolgenden Fernzugriff auf Gesundheits- oder Sozialdaten keine Datenübermittlung in die USA erfolgen würde und die Vorgaben aus § 393 Abs. 2 SGB V erfüllt wären. Weil § 393 Abs. 2 Nr. 3 SGB V nur dann eine Datenübermittlung in ein Drittland ermöglicht, wenn für dieses Land ein Angemessenheitsbeschluss vorhanden ist, würde ein fehlender Angemessenheitsbeschluss weitreichende Konsequenzen haben und die Zusammenarbeit mit US-amerikanischen Hyperscalern schwer denkbar erscheinen lassen.	**Ab Seite *32***
3. 1) b) i) und ii)	i): Ist es richtig, dass BCRs nicht ausreichend sind, um eine Verarbeitung in einem Drittland zu ermöglichen, wenn gleichzeitig kein Angemessenheitsbeschluss für das Drittland existiert? ii): D.h., ist eine Drittlandverarbeitung möglich, wenn ein Angemessenheitsbeschluss für das betreffende Drittland existiert?	i): Ja, es ist richtig, dass BCRs nicht ausreichend sind, um eine Verarbeitung in einem Drittland zu ermöglichen, wenn gleichzeitig kein Angemessenheitsbeschluss für das Drittland existiert und § 393 SGB V anwendbar ist. ii): Ja, eine Verarbeitung im Drittland ist im Anwendungsbereich des § 393 SGB V nur möglich, wenn ein Angemessenheitsbeschluss für das betreffende Drittland existiert.	**Ab Seite *35***
3. 2) a) und b)	a) Sind die Begriffe „internationale Organisation“ und „Hauptniederlassung“ auch im Hinblick auf § 393 SGB V so anzuwenden, wie sie in der DSGVO stehen? b) Wenn nein, wie sind die Begriffe im Kontext des § 393 SGB V anzuwenden?	a): Im Grundsatz, ja. Der Begriff „Hauptniederlassung“ spielt allerdings im Kontext des § 393 SGB V keine große Rolle. Der Niederlassungsbegriff aus der DSGVO sollte bei § 393 SGB V aber genauso angewendet werden. Der Begriff „internationale Organisation“ wird nicht in § 393 SGB V erwähnt, kann aber im Kontext des § 393 Abs. 2 SGB V relevant sein, insbesondere wenn es für eine internationale Organisation einen Angemessenheitsbeschluss gibt. b): Da die Frage a) mit „ja“ beantwortet wurde, erübrigt sich die Frage b).	**Ab Seite *36* und *38***
3. 2) c)	Gelten die Vorgaben auch für Cloud-Dienstleistungen, die von internationalen Organisationen angeboten werden?	Die Vorgaben aus § 393 Abs. 2 SGB V gelten auch, wenn eine Datenübermittlung an eine internationale Organisation erfolgt. Im Falle eines	**Ab Seite *38***

		Angemessenheitsbeschlusses für eine internationale Organisation kann der deutsche Gesetzgeber aber nicht die Möglichkeit ausschließen, die Datenübermittlungen auf Basis eines Angemessenheitsbeschlusses vorzunehmen. In dem Fall sind die Vorgaben aus § 393 Abs. 2 Nr. 3 SGB V erfüllt. Bei einem fehlenden Angemessenheitsbeschluss für eine internationale Organisation sind die Vorgaben aus § 393 Abs. 2 Nr. 3 SGB V hingegen nicht erfüllt.	
4. 1)	Ist es richtig, dass durch die „und"-Verknüpfung § 393 Abs. 3 SGB V alle in den Nr. 1 bis 3 gestellten Anforderungen gemeinsam erfüllt werden müssen?	Ja, alle der Voraussetzungen aus den drei Ziffern des § 393 Abs. 3 SGB V müssen zusammen erfüllt werden, weil Nr. 2 und Nr. 3 mit einem „Und" verknüpft sind und Nr. 1 entsprechend der Gesetzesbegründung auch immer erfüllt sein muss und es keine Anhaltspunkte für eine Intention zur Regulierung von alternativen Optionen gibt.	**Ab Seite *39***
4. 2) a)	Im Datenschutzrecht ist die „datenverarbeitende Stelle" der Verantwortliche, der Cloud-Dienstleistung erbringende Anbieter/Dienstleister wäre als Auftragsverarbeiter hingegen keine datenverarbeitende Stelle. Ist es richtig, dass Leistungserbringer oder Krankenkassen als datenverarbeitende Stelle mit der Pflicht zur Erbringung eines C5-Testates anzusehen sind?	Der Begriff „datenverarbeitende" Stelle war früher gebräuchlich, wird heute aber in Datenschutzgesetzen nicht mehr wirklich verwendet. Es ist nicht vollkommen klar, ob der Gesetzgeber nur Leistungserbringer und Kranken- und Pflegekassen als datenverarbeitende Stelle ansieht oder auch deren Auftragsverarbeiter. Die besseren Argumente sprechen aber dafür, dass die datenverarbeitende Stelle nur den Verantwortlichen meint.	**Ab Seite *39***
4. 2) b)	Trifft die Pflicht, ein C5-Zertifikat für den eingesetzten Cloud-Computing-Dienst vorweisen zu können, die datenverarbeitende Stelle, muss dann ein BSI C5-Testat für jeden einzelnen Cloud-Computing-Dienst vorliegen? Oder kann für mehrere verschiedene Cloud-Computing-Dienste ein einziges BSI-C5 Testat den gesetzlichen Anforderungen genügen?	Das hängt von dem Umfang des Testats ab. Wenn es für mehrere Dienste gilt, dann kann auch der Nachweis für mehrere Dienste durch so ein einzelnes Testat erbracht werden. Wenn es aber nur für einen von mehreren Diensten gilt, dann muss für die übrigen Dienste auch der Nachweis des Vorliegens eines Testats durch andere Testate erbracht werden.	**Ab Seite *42***
4. 2) c)	Muss sowohl die datenverarbeitende Stelle als auch der Cloud-Computing-Dienst nach BSI C5 testiert worden sein?	Nein, nur der Cloud-Computing-Dienst muss nach BSI-C5 testiert worden sein und die datenverarbeitende Stelle muss die Vorgaben aus § 393 Abs. 3 Nr. 3 SGB V selbst erfüllen, ohne dabei testiert zu werden. Es ist nach dem Willen des deutschen Gesetzgebers aber auch möglich, dass sich eine Einrichtung den konkreten Einsatz bei ihr	**Ab Seite *42***

		nach BSI-C5 testieren lässt, wenn bspw. der Hersteller des Dienstes noch kein Testat vorlegen kann.	
5. 1) a)	Fällt BSI C5 unter die Definition „nationales Schema für die Cybersicherheitszertifizierung“ gemäß Art. 2 Ziff. 10 Verordnung (EU) 2019/881?	Ja, das BSI-C5-Testat ist ein „nationales Schema für die Cybersicherheitszertifizierung“ gemäß Art. 2 Nr. 10 Verordnung (EU) 2019/881.	**Ab Seite *43***
5. 1) b)	Ist es richtig, dass mit einem im Amtsblatt der EU veröffentlichtem Cloud-Schema entsprechend europäischen Recht, u.a. durch Art. 57 Abs. 1 Verordnung (EU) 2019/881, das BSI C5 unwirksam wird?	Ja, es ist richtig, dass das BSI-C5-Testat in Zukunft einmal unwirksam wird. Gleichzeitig bedeutet dies noch nicht automatisch, dass das Testat im Rahmen des § 393 SGB V dann auch keine Rolle mehr spielt.	**Ab Seite *44***
5. 1) c)	Wenn das BSI-Schema unwirksam wird, ist es dann richtig, dass aufgrund der in § 393 SGB V verankerten nationalen Pflicht an Stelle des BSI C5-Testates eine Zertifizierung nach ENISA-Vorgaben erforderlich sein wird?	Nein, es wird nicht zwangsläufig eine Zertifizierung nach ENISA-Vorgaben notwendig sein, sondern ebenso ein C5-Testat ausreichen. Etwas anderes gilt nur bei einer – aus unserer Sicht unwahrscheinlichen – Anpassung des § 393 SGB V. Weitere Zertifizierungen nach anderen Vorgaben werden aber künftig ebenso neben dem C5-Testat akzeptiert.	**Ab Seite *45***

B. In diesem Gutachten zu beantwortende Fragen und dazugehörige Antworten

Wir wurden damit beauftragt, die im Folgenden aufgelisteten Fragen im Rahmen dieses Gutachtens zu bewerten. Es wird zunächst immer die gestellte Frage aufgeführt und sodann beantwortet.

I. Fragen zur Möglichkeit, Daten in der Cloud zu verarbeiten

Die im Folgenden Abschnitt beantworteten Fragen betreffen jeweils direkt oder indirekt Aspekte der Rechtmäßigkeit der Datenverarbeitung in der Cloud.

1. Fragen und Antworten zu Fragen unter 1.)

1.1. Die Fragen

§ 393 Abs. 1 SGB V erlaubt die Cloud-Verarbeitung von Sozial- und Gesundheitsdaten, wobei „Sozialdaten“ mit Verweis auf § 67 Absatz 2 des Zehnten Buches definiert wird. Der Begriff „Gesundheitsdaten“ wird in Art. 4 Ziff. 15 DSGVO definiert. Der Begriff "genetische Daten" wird in Art. 4 Ziff. 13 DSGVO definiert, jedoch von § 393 SGV nicht benutzt.

> 1. 1) a) Sind die Definitionen aus der DSGVO im Kontext der Regelungen § 393 SGB V anzuwenden?
>
> 1. 1) b) Werden genetische Daten von der Erlaubnisnorm ebenfalls erfasst, d.h. zählen genetische Daten zu Gesundheitsdaten?
>
> 1. 1) c) Oder sind genetische Daten von § 393 SGB V nicht erfasst, d.h. die Regelungen von § 393 SGB V gelten nicht für genetische Daten?

1.2. Die Antworten

Im Folgenden beantworten wir die Fragen zu 1.1 a) bis 1.1 c) getrennt. Zusammengefasst lauten die Antworten auf folgende Fragen wie folgt:

- *1. 1) a)*: Ja, die Definitionen aus der DSGVO sind im Kontext der Regelungen des § 393 SGB V anzuwenden.
- *1. 1) b)*: Ja, genetische Daten sind zum Teil erfasst. Genetische Daten sind manchmal aber nicht immer Gesundheitsdaten und können auch Sozialdaten sein. Die Verarbeitung von genetischen Daten unterfällt dann dem § 393 Abs. 1 SGB V, wenn die genetischen Daten auch gleichzeitig Gesundheitsdaten sind oder von einer in § 35 SGB I genannten Stelle im Hinblick auf Aufgaben nach dem SGB I verarbeitet werden.
- *1. 1) c)*: Die Regelungen aus § 393 Abs. 1 SGB V gelten dann nicht, wenn die genetischen Daten weder Gesundheitsdaten sind noch von einer in § 35 SGB I genannten Stelle im Hinblick auf Aufgaben nach dem SGB I verarbeitet werden und deswegen auch keine Sozialdaten sind.

1.2.1. Antwort zu 1. 1) a)

Es ist fraglich, ob die Definitionen aus der DSGVO im Kontext der Regelungen des § 393 SGB V anzuwenden sind. Gemäß § 393 Abs. 1 SGB V in der durch das DigiG abgeänderten Fassung gilt Folgendes:

> *„Leistungserbringer im Sinne des Vierten Kapitels und Kranken- und Pflegekassen sowie ihre jeweiligen Auftragsdatenverarbeiter dürfen Sozialdaten und Gesundheitsdaten auch im Wege des Cloud-Computing-Dienstes verarbeiten, sofern die Voraussetzungen der Absätze 2 bis 4 erfüllt sind.“*

In der finalen Version des DigiG ist – anders als in der Vorbemerkung zur Frage angegeben – kein Verweis mehr auf die Definition für Sozialdaten aus § 67 Abs. 2 SGB X enthalten. Es gilt aber weiterhin gemäß § 393 Abs. 8 SGB V, dass die Vorschriften aus dem SGB X und dem BDSG unberührt bleiben. Dass der deutsche Gesetzgeber in § 393 Abs. 8 SGB V geregelt hat, dass die Vorschriften des BDSG unberührt bleiben, ist ein Indiz für die Relevanz der gängigen datenschutzrechtlichen Definitionen im Kontext des neuen § 393 SGB V. Denn lediglich im BDSG und bspw. auch SGB kann der deutsche Gesetzgeber zur DSGVO ergänzende oder auch ein Stück weit abweichende Regelungen treffen. Weil aber eine Änderung der DSGVO als eine europäische Verordnung ohnehin nicht möglich war, hat der deutsche Gesetzgeber wahrscheinlich nur einen Verweis auf das BDSG aufgenommen und nicht auch geregelt, dass die DSGVO unberührt bleibt. Diese Annahme wird auch dadurch gestützt, dass sich der § 393 Abs. 8 SGB V in seiner

finalen Fassung nicht vom Entwurf der Bundesregierung unterscheidet[8] und in der Gesetzesbegründung aber ausdrücklich darauf verwiesen wird, dass auch die Vorgaben aus der DSGVO unberührt bleiben: „*Diese Regelung lässt die Regelungen zum geltenden Datenschutzrecht gemäß dem Zehnten Buch (insb. § 80 SGB X), dem Bundesdatenschutzgesetz und der europäischen Datenschutzgrundverordnung unberührt*."[9]

Gemäß der Regelung aus § 35 Abs. 2 SGB I gilt, dass in den Sozialgesetzbüchern die Verarbeitung personenbezogener Daten abschließend geregelt wird, sofern nicht die DSGVO unmittelbar anwendbar ist. Mit anderen Worten ausgedrückt können SGB-Bestimmungen also nur dann abschließend sein, wenn die DSGVO nicht sowieso unmittelbar gilt. Nur in solchen Fällen ist es denkbar, dass im SGB die Vorgaben für die Verarbeitung abschließend sind.[10] Gemäß § 393 Abs. 8 SGB V bleibt das BDSG unberührt. Das sollte im Ergebnis bedeuten, dass die Regelungen aus dem BDSG weiterhin genauso gelten wie vor der Einführung des § 393 SGB V.

Dass die Begriffsbestimmungen der DSGVO maßgeblich sind, ist auch bereits deswegen stimmig, weil in § 393 SGB V u.a. eine Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten geregelt ist und im Rahmen dessen schließlich das Begriffsverständnis für „Gesundheitsdaten" aus der DSGVO angewendet werden muss. Was speziell den Begriff „Gesundheitsdaten" betrifft, so muss die Definition aus der DSGVO auch im Kontext des § 393 SGB V von vornherein maßgeblich sein, wenn der deutsche Gesetzgeber den Begriff „Gesundheitsdaten" nicht abweichend in einem anderen Gesetz definiert hat. Soweit ersichtlich ist keine abweichende nationale Definition vorhanden.

In § 67 SGB X definiert der deutsche Gesetzgeber „*ergänzend zu Artikel 4*" DSGVO einige Begriffe, wie u.a. Sozialdaten. Hier wird ein weiteres Mal deutlich, dass die Begriffsdefinitionen aus Art. 4 DSGVO auch im Kontext des Sozialrechts relevant sind und andere Definitionen mit Datenschutzbezug in deutschen Gesetzen nur ergänzend hinzutreten. In der deutschen Rechtsprechung wird von Gerichten im Anwendungsbereich des SGB auf die Definition für Gesundheitsdaten aus Art. 4 Nr. 15 DSGVO verwiesen.[11] Auch der Umstand, dass die DSGVO u.a. in Art. 9 Abs. 2 lit. h DSGVO Regelungen für den „*Gesundheits- oder Sozialbereich*" und in lit. b derselben Vorschrift zum „*Recht der sozialen Sicherheit und des Sozialschutzes*" enthält, spricht dafür, dass die Definitionen der Verordnung im Rahmen des § 393 SGB V gelten, weil die DSGVO im Allgemeinen die Verarbeitungen in solchen Bereichen regelt.

Auch der Begriff „Auftragsdatenverarbeiter" ist im Einklang mit den DSGVO-Vorgaben zu verstehen, obwohl in der DSGVO die Formulierung „Auftragsverarbeiter" verwendet wird. Das wird auch daran deutlich, dass in der Gesetzesbegründung in dem Begriffskontext explizit auf Art. 28 DSGVO verwiesen wird.[12]

Insgesamt ist also festzustellen, dass die Definitionen aus der DSGVO auch im Anwendungsbereich des § 393 SGB V relevant sind.

1.2.2. Antwort zu 1. 1) b)

Es ist fraglich, ob genetische Daten von der Erlaubnisnorm in § 393 Abs. 1 SGB V ebenfalls erfasst sind. Insbesondere ist zu klären, ob genetische Daten zu Gesundheitsdaten zählen.

Genetische Daten würden grundsätzlich dann auch im Rahmen des § 393 Abs. 1 SGB V erfasst sein, wenn sie ebenfalls Gesundheitsdaten oder Sozialdaten wären.

Gemäß Art. 4 Nr. 13 DSGVO werden genetische Daten wie folgt definiert: „*personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie* ***oder die Gesundheit*** *dieser natürlichen Person liefern und insbesondere aus*

---

[8] Vgl. die aktuell geltende Version des § 393 SGB V und die Vorschrift im Entwurf der Bundesregierung (Drucksache 20/9048), der unter folgender URL abrufbar ist: https://dserver.bundestag.de/btd/20/090/2009048.pdf (letzter Abruf am 22.4.2024).

[9] BT, Drucksache 20/9048, S. 151 zu Abs. 8.

[10] *Krahmer/Strothmann*, in: Krahmer, Sozialdatenschutzrecht, § 35 SGB I Rn. 20: „*§ 35 Abs. 2 Satz 1 SGB X stellt zudem fest, dass die „abschließende" Datenschutzwirkung des Sozialgesetzbuches nur insoweit gilt, als die grundsätzlich vorrangig geltende DS-GVO keine unmittelbare Anwendung findet*."

[11] Siehe etwa BSG, Urt. v. 8.10.2019 - B 1 A 3/19 R, Rn. 32; BSG, Urt. v. 20.1.2021 – B 1 KR 7/20 R, Rn. 66.

[12] BT, Drucksache 20/9048, S. 150 zu Abs. 1.

der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden." Aus dieser Definition geht hervor, dass in einigen Fällen genetische Daten Gesundheitsdaten sein können während in anderen Fällen genetische Daten keine Gesundheitsdaten sind. Bspw. wären genetische Daten dann keine Gesundheitsdaten, wenn es um Informationen über die Physiologie ohne Gesundheitsbezug ginge. In dem Zusammenhang sei auch auf die Kommentierung von *Petri*[13] verwiesen, der zutreffend folgende Feststellungen trifft:

> *„Werden aus genetischen Daten Angaben abgeleitet, die Aussagen über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person treffen, dann handelt es sich – zumindest auch – um Gesundheitsdaten iSd Art. 4 Nr. 15. Die einer solchen Analyse zugrunde liegenden genetischen Codes sind hingegen genetische Daten iSv Art. 4 Nr. 13."*

Dass genetische Daten auch Gesundheitsdaten sein können, wird im Wortlaut beider Definitionen und an deren jeweiligen Reichweite erkennbar. Für das Vorliegen von Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO ist es nur notwendig, dass aus personenbezogenen Daten „*Informationen über […] [den] Gesundheitszustand* ***hervorgehen***". Auch in ErwGr. 35 Satz 1 zur DSGVO heißt es außerdem wie folgt: „*Zu den personenbezogenen Gesundheitsdaten sollten* ***alle Daten*** *zählen, […] aus denen* ***Informationen*** *über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person* ***hervorgehen***." Im Einklang mit der EuGH-Rechtsprechung meint „*hervorgehen*", dass auch solche Verarbeitungen von der Vorschrift erfasst sind, die nicht in Bezug auf dem Wesen nach sensiblen Informationen erfolgen. Die Anwendbarkeit erstreckt sich „*auch auf [Verarbeitungen von] Daten, aus denen sich mittels eines Denkvorgangs der Ableitung oder des Abgleichs indirekt sensible Informationen ergeben*".[14] Das Vorliegen von genetischen Daten i.S.v. Art. 4 Nr. 13 DSGVO verlangt, dass "*personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften" […]* ***eindeutige Informationen*** *über die […]* ***Gesundheit*** *[…]* ***liefern***." Der Anwendungsbereich von Art. 4 Nr. 15 DSGVO ist also naturgemäß weiter als der Anwendungsbereich von Art. 4 Nr. 13 DSGVO. Während es bei den Gesundheitsdaten nur darauf ankommt, dass in irgendeiner Form auch Informationen über die Gesundheit aus personenbezogenen Daten „hervorgehen", verlangt Art. 4 Nr. 13 DSGVO, dass genetische Daten eine „eindeutige Information" über die Gesundheit liefern. Sofern also genetische Daten eine eindeutige Information über die Gesundheit liefern, müssen diese auch gleichzeitig vom vergleichsweisen weiten Anwendungsbereich für Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO erfasst sein.[15] Dabei ist es unschädlich, dass genetische Daten schon vor den Gesundheitsdaten in Art. 4 definiert werden und die Definition zu Gesundheitsdaten nicht explizit auf jene für genetische Daten Bezug nimmt. Eine solche Bezugnahme ist grundsätzlich nicht erforderlich und u.a. in dem Fall nicht notwendig, weil der Wortlaut hinreichend klar genug die Überschneidungen erkennen lässt.

Sofern die verarbeiteten genetischen Daten auch Gesundheitsdaten sind, ist § 393 Abs. 1 SGB V anwendbar. Wenn genetische Daten ohne Gesundheitsbezug verarbeitet werden, dann ist dies keine Verarbeitung von Gesundheitsdaten i.S.v. § 393 Abs. 1 SGB V. Es ist jedoch auch denkbar, dass die Verarbeitung von genetischen Daten als eine Verarbeitung von Sozialdaten i.S.v. § 393 Abs. 1 SGB V erfolgt. Die Verarbeitung von genetischen Daten in Form von Sozialdaten unterfällt dann ebenfalls dem § 393 Abs. 1 SGB V.

Gemäß § 67 Abs. 2 SGB X sind Sozialdaten personenbezogene Daten, „*die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden*." Sozialdaten werden demzufolge dann verarbeitet, wenn die folgenden zwei Voraussetzungen erfüllt sind: (i) es geht um personenbezogene Daten und (ii) die Daten werden von einer in § 35 SGB I genannten Stelle im Hinblick auf Aufgaben nach dem SGB I verarbeitet. Genetische Daten sind immer personenbezogene Daten, weswegen die Voraussetzung (i) stets erfüllt ist. Genetische Daten sind dann auch Sozialdaten, wenn sie von einer in § 35 SGB I genannten Stelle im Hinblick auf Aufgaben nach dem

---

[13] *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 Nr. 13 DSGVO Rn. 13.
[14] Siehe exemplarisch EuGH, Urt. v. 1.8.2022, C-184/20, ECLI:EU:C:2022:601 Rn. 123.
[15] Zur Weite der beiden Anwendungsbereiche im Vergleich und deren Überschneidungen siehe auch *Strassemeyer/Quiel*, in: Freund/Schmidt/Heep/Roschek, Praxis-Kommentar DSGVO, Art. 4 DSGVO Rn. 291; mit demselben Ergebnis auch *Schreiber*, in: Plath, DSGVO/BDSG/TTDSG, Art. 4 DSGVO Rn. 56.

SGB I verarbeitet werden. Es kommt also für das Vorliegen von genetischen Daten als Sozialdaten auf die Art der verarbeitenden Stelle und die Zwecke der Verarbeitung an. Somit fallen genetische Daten – unabhängig vom Vorliegen von Gesundheitsdaten – auch dann in den Anwendungsbereich des § 393 Abs. 1 SGB V, wenn sie von einer entsprechenden Stelle für die entsprechenden Zwecke verarbeitet werden.[16]

Zusammengefasst lautet die Antwort auf die Frage also, dass genetische Daten dann dem Anwendungsbereich des § 393 Abs. 1 SGB V unterfallen, wenn sie entweder unter den Begriff Gesundheitsdaten zu subsumieren sind oder von einer in § 35 SGB I genannten Stelle im Hinblick auf Aufgaben nach dem SGB I verarbeitet werden.

1.2.3 Antwort zu 1. 1) c)

Es ist fraglich ob, genetische Daten von § 393 SGB V nicht erfasst sind, d.h. die Regelungen von § 393 SGB V nicht für genetische Daten gelten würde.

Wie den Ausführungen zu Frage b) entnommen werden kann, sind genetische Daten dann nicht von § 393 Abs. 1 SGB V erfasst, wenn die genetischen Daten

- keine Gesundheitsdaten sind und
- nicht von einer in § 35 SGB I genannten Stelle im Hinblick auf Aufgaben nach dem SGB I verarbeitet werden.

2. Fragen und Antworten zu Fragen unter 2.)

2.1. Die Fragen

§ 393 Abs. 1 SGB V enthält keine Regelung zu Beschäftigtendaten und ebenfalls nicht zu biometrischen Daten im Sinne von Art. 4 Ziff. 14 DSGVO. Biometrische Daten werden sehr häufig zur Authentifizierung von Personen benutzt, auch bei Cloud-Dienstleistungen wird der Zugriff häufig über biometrische Identifikationsmechanismen abgesichert.

> 1. 2) a) Dürfen Beschäftigtendaten im Cloud-Kontext verarbeitet werden, da durch die in § 393 Abs. 1 SGB V enthaltene Erlaubnis der Verarbeitung von Sozial- und Gesundheitsdaten implizit auch die Erlaubnis zur Verarbeitung von Beschäftigtendaten (z.B. zur Zugriffsverwaltung) enthalten ist?
>
> 1. 2) b) Dürfen aus demselben Grund (implizite Erlaubnis durch die Regelung in § 393 SGB V) biometrische Daten verarbeitet werden?
>
> 1. 2 c) Oder dürfen Beschäftigtendaten und biometrische Daten nur verarbeitet werden, wenn ein anderer Erlaubnistatbestand als § 393 SGB V die Verarbeitung dieser Daten erlaubt?

2.2. Die Antworten

Im Folgenden beantworten wir die Fragen zu 1. 2) a) bis 1. 2) c) getrennt. Zusammengefasst lauten die Antworten auf folgende Fragen wie folgt:

- *1. 2) a)*: Nein, § 393 Abs. 1 SGB V enthält nicht implizit auch eine Erlaubnis zur Verarbeitung von Beschäftigtendaten. Trotzdem ist der auf Basis von § 393 Abs. 1 SGB V legitimierte Einsatz eines Cloud-Computing-Dienstes ein Stück weit ein Indiz für die Legitimität der Verarbeitung der erforderlichen Beschäftigtendaten. Die Zulässigkeit der Datenverarbeitung ist im Einzelfall jedoch anhand der Vorgaben aus der DSGVO und dem BDSG zu bestimmen.
- *1. 2) b)*: Nein. Wenn biometrische Daten als Gesundheits- oder Sozialdaten verarbeitet werden, dann ist deren Verarbeitung auf Basis von § 393 Abs. 1 SGB V ggf. legitimierbar. In anderen Fällen muss die Zulässigkeit der Verarbeitung von biometrischen Daten anhand einer anderen Rechtsgrundlage geprüft werden.

[16] Mit Blick auf den weiten Anwendungsbereich von „Sozialdaten“ und der Möglichkeit, dass fast jedes personenbezogene Datum auch ein Sozialdatum sein kann, *Kipker/Pollmann*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 26 Rn. 20.

- *1. 2) c)*: Wenn Beschäftigtendaten oder biometrische Daten entweder Gesundheits- oder Sozialdaten sind, dann ist § 393 SGB V anwendbar. In allen anderen Fällen ist die Rechtmäßigkeit der Datenverarbeitungen anhand der Vorgaben aus der DSGVO und dem BDSG zu bestimmen.

2.2.1. Antwort zu 1. 2) a)

Es ist fraglich, ob Beschäftigtendaten im Cloud-Kontext verarbeitet werden dürfen, da durch die in § 393 Abs. 1 SGB V enthaltene Erlaubnis der Verarbeitung von Sozial- und Gesundheitsdaten implizit auch die Erlaubnis zur Verarbeitung von Beschäftigtendaten (z.B. zur Zugriffsverwaltung) enthalten sein könnte.

Der Gesetzesbegründung ist zu entnehmen, dass § 393 Abs. 1 SGB V „*als expliziter Erlaubnistatbestand der Nutzung des Cloud-Computings für die aufgezählten Fälle bei der Verarbeitung von Sozial- und Gesundheitsdaten unter Festlegung bestimmter Mindeststandards*“ gilt.[17] Der Erlaubnistatbestand bezieht sich somit ausschließlich auf die Verarbeitung von Gesundheitsdaten und Sozialdaten bei der Verwendung von Cloud-Computing-Diensten. In diesen Tatbestand eine Erlaubnis für die Verarbeitung von Beschäftigtendaten implizit hineinzulesen, ohne dabei auf eine Verarbeitung von Gesundheits- oder Sozialdaten abzustellen, erscheint angesichts der Gesetzesbegründung und dem Wortlaut der Vorschrift nicht überzeugend.

Wenn die Verarbeitung von Beschäftigtendaten nicht als eine Verarbeitung von Gesundheitsdaten oder Sozialdaten erfolgt, dann ist in § 393 Abs. 1 SGB V hierfür keine Rechtsgrundlage vorgesehen. Gleichzeitig kann ein auf Basis von § 393 Abs. 1 SGB V legitimierter Einsatz eines Cloud-Computing-Dienstes ein Indiz dafür sein, dass die Verarbeitung von notwendigen Beschäftigtendaten auch legitim sein sollte. Hierbei ist die Rechtsgrundlage jedoch in Art. 6 Abs. 1 DSGVO / Art. 9 Abs. 2 DSGVO und ggf. § 26 BDSG enthalten und nicht automatisch schon implizit von § 393 Abs. 1 SGB V abgedeckt. Es ist im Einzelfall anhand der Bestimmungen aus der DSGVO und dem BDSG zu prüfen, ob es für die Verarbeitungen von Beschäftigtendaten eine Rechtsgrundlage gibt.

2.2.2. Antwort zu 1. 2) b)

Es ist fraglich, ob § 393 Abs. 1 SGB V implizit eine Erlaubnis zur Verarbeitung von biometrischen Daten enthält. Biometrische Daten werden sehr häufig zur Authentifizierung von Personen benutzt, auch bei Cloud-Dienstleistungen wird der Zugriff häufig über biometrische Identifikationsmechanismen abgesichert.

Wie den Ausführungen unter der Frage a) zu entnehmen ist, enthält § 393 Abs. 1 SGB V keine pauschale implizite Erlaubnis zur Verarbeitung von Beschäftigtendaten. Dasselbe gilt mangels anderer Anhaltspunkte ebenso für die Verarbeitung biometrischer Daten. Entweder die Verarbeitung von biometrischen Daten erfolgt in Form einer Verarbeitung von Gesundheits- oder Sozialdaten nach § 393 Abs. 1 SGB V oder es muss eine andere Rechtsgrundlage für die Verarbeitung biometrischer Daten vorhanden sein. Im Gegensatz zu genetischen Daten werden biometrische Daten noch seltener gleichzeitig auch Gesundheitsdaten sein. Daher scheint es eher möglich, dass biometrische Daten in Form von Sozialdaten vorliegen. Biometrische Daten würden dann als Sozialdaten verarbeitet werden, wenn die Verarbeitung durch eine in § 35 SGB I genannten Stelle im Hinblick auf Aufgaben nach dem SGB I erfolgen würde. Ist dies nicht der Fall, muss die Zulässigkeit der Verarbeitung von biometrischen Daten auf eine andere Rechtsgrundlage gestützt werden. Im Regelfall sollte sich die Zulässigkeit der Verarbeitung von biometrischen Daten im Bereich des Cloud-Computings eher aus der DSGVO und ggf. zusätzlich dem BDSG ergeben.

2.2.3. Antwort zu 1. 2) c)

Es ist fraglich, ob Beschäftigtendaten und biometrische Daten nur verarbeitet werden dürfen, wenn ein anderer Erlaubnistatbestand als § 393 SGB V die Verarbeitung dieser Daten erlaubt.

Wie den Ausführungen bei den Antworten zu den Fragen a) und b) zu entnehmen ist, können Beschäftigtendaten und biometrische Daten ggf. auch in Form von Sozialdaten und ggf. auch als Gesundheitsdaten verarbeitet werden und diese Verarbeitung kann auf Basis von § 393 Abs. 1 SGB V

[17] BT, Drucksache 20/9048, S. 150 zu Abs. 1.

legitimiert sein. Ist dies nicht der Fall, so muss die Zulässigkeit der Datenverarbeitung anhand von anderen Erlaubnistatbeständen geprüft werden.

II. Fragen zur Cloud-Definition

Die im Folgenden Abschnitt beantworteten Fragen betreffen jeweils direkt oder indirekt Aspekte der Cloud-Definition.

1. Fragen und Antworten zu Fragen unter 2. (1) bis 2) f))

1.1. Die Fragen zu 2. 1)

Die europäische Definition eines Cloud-Computing-Dienstes findet sich in Art. 6 Ziff. 30 Richtlinie (EU) 2022/2555 („**NIS2-RL**“) wie folgt:

„[…]

30. „Cloud-Computing-Dienst“ einen 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;

[…]“

Stand heute ist unklar, welche Begriffsbestimmung im deutschen NIS2-Umsetzungsgesetz seitens des deutschen Gesetzgebers gewählt wird. Da die Begriffsbestimmung in § 384 Ziffer 5 SGB V dem Wortlaut der Definition in Art. 6 Ziff. 30 NIS2-RL entspricht: Kann die Definition angewendet werden, auch wenn im deutschen NIS2-Umsetzungsgesetz eine andere Definition verwendet wird?

1.2. Die Antworten zu 2. 1)

Die Antwort in Kürze: Ja, die Definition aus Art. 6 Nr. 30 NIS2-RL kann angewendet werden. Es ist wegen der gleichzeitigen Relevanz des Begriffs für das BSI-Gesetz („BSIG“) theoretisch nur möglich, dass der deutsche Gesetzgeber die Definition noch weiter fasst oder lediglich sprachlich anders formuliert, wobei der Anwendungsbereich jedoch mindestens genauso groß sein muss, wie derjenige der Definition aus der Richtlinie. In den aktuell vorliegenden Entwürfen für das NIS2-Umsetzungsgesetz ist aber eine Intention zur Verwendung eines anderen Begriffs nicht erkennbar.

Es ist fraglich, ob der Begriff „Cloud-Computing-Dienst“ i.S.v. § 393 SGB V im Einklang mit Art. 6 Nr. 30 NIS2-RL verstanden werden muss oder bei einer ggf. künftig noch erfolgenden abweichenden Definition im BSI-Gesetz nicht die Definition aus der Richtlinie, sondern jene aus dem BSI-Gesetz anzuwenden wäre. Anders gefragt soll hier beantwortet werden, ob die Definition aus der Richtlinie direkt angewendet werden kann, auch wenn künftig ggf. im deutschen NIS2-Umsetzungsgesetz eine andere Definition verwendet wird.

Vorab sei angemerkt, dass die Begriffsdefinition für § 393 SGB V eine andere Rolle spielt als im BSIG. Während im BSIG Vorgaben aus der NIS2-RL umgesetzt werden, wird in § 393 SGB V eine Erlaubnisnorm für Verarbeitungen personenbezogener Daten geschaffen. Weil der Gesetzgeber sowohl im SGB V als auch im BSIG eine übereinstimmende Definition verwenden möchte, ist die im BSIG erfolgende Umsetzung der Vorgaben aus der NIS2-RL ebenso für das Begriffsverständnis im Anwendungsbereich des SGB V relevant.

Die Gesetzesbegründung zu § 384 Nr. 5 SGB V enthält die folgende Aussage: „*Die Definition entspricht der Definition nach § 2 Nummer 2 BSIG-E nach dem Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG). Sobald das NIS2UmsuCG in Kraft getreten ist, wird die Definition durch einen Verweis auf das BSIG ersetzt*.“[18] Aus dieser Aussage wird nicht ganz deutlich, ob der deutsche Gesetzgeber damit andeutet, dass es künftig auch eine inhaltlich abweichende Definition im BSIG geben kann, oder ob im Nachgang lediglich ein Verweis auf die aktuell im Entwurf zum BSIG[19] auch schon genauso vorhandene und der NIS-Richtlinie entsprechenden Definition eingefügt werden soll. Es

[18] BT, Drucksache 20/9048, S. 135.

[19] Der Entwurf mit Stand vom 22.12.2023 steht unter der folgenden URL zum Download bereit: https://ag.kritis.info/wp-content/uploads/2024/03/CI1_17002_41_22-86-32-NIS2UmsuCG-2.-RefE-22-12-2023-09-58h.docx (letzter Abruf am 22.4.2024).

scheint zunächst einmal beides denkbar zu sein, wobei jedoch in jedem Fall davon auszugehen ist, dass die Definition im Kontext des § 393 SGB V genauso gelten soll wie auch im BSIG.

Wegen dieser Überlappungen stellt sich daher die Frage, welchen Umsetzungsspielraum der deutsche Gesetzgeber bei der Umsetzung der Vorgaben aus der NIS2-RL mit Blick auf den Begriff „Cloud-Computing-Dienst" hat. Der Adressat einer europäischen Richtlinie (wie der NIS2-RL) ist in erster Linie immer ein Mitgliedstaat.[20] Deutschland ist unter der NIS2-RL verpflichtet, die Ziele der Regelungen aus der Richtlinie in nationales Recht umzusetzen.[21] In dem Kontext ist es relevant, dass die Begriffsdefinition für § 393 SGB V auch genauso für die Umsetzung der Vorgaben aus der NIS2-RL im BSIG gelten soll, weil dann auch im SGB V indirekt die Ziele aus der NIS2-RL umgesetzt werden. Unter dem Ziel in diesem Sinne wird das vom europäischen Gesetzgeber intendierte Ergebnis verstanden.[22] In der Regel steht es den Mitgliedstaaten jedoch frei, die Form und Mittel der Umsetzung der Ziele der Richtlinienvorgaben zu wählen. In einigen Fällen besteht auch einmal aus faktischer Sicht betrachtet kein oder kaum Umsetzungsspielraum hinsichtlich des Inhaltes einer nationalen Umsetzungsnorm, weil eine Regelung aus einer Richtlinie bereits „unbedingt" ist. Eine Bestimmung gilt dann als „unbedingt", wenn sie weder mit einem Vorbehalt noch mit einer Bedingung versehen ist und ihrem Wesen nach keiner weiteren Maßnahme der Unionsorgane oder der Mitgliedstaaten bedarf.[23] In solchen Fällen besteht naturgemäß ein eingeschränkter Umsetzungsspielraum.

Übertragen auf die Vorgaben aus Art. 6 Nr. 30 NIS2-RL ist festzustellen, dass das Ziel dieser Begriffsbestimmung darin besteht, dass andere Vorgaben aus der Richtlinie, die für Cloud-Computing-Dienste Regelungen vorsehen, eben für solche Dienste auch im nationalen Recht gelten. Der deutsche Gesetzgeber wird bspw. in der neuen Version des BSIG die Vorgaben aus der Richtlinie in Bezug auf Regelungen für Cloud-Computing-Dienste dadurch umsetzen, dass die Vorgaben für solche Dienste aus der Richtlinie auch entsprechend im nationalen Recht geregelt werden und Cloud-Computing-Dienste im Einklang mit der Richtlinie definiert werden. Naturgemäß hat der deutsche Gesetzgeber bei der Umsetzung im BSIG eine eingeschränkte Wahl, weil er das eben benannte Ziel umsetzen muss. Das gilt indirekt genauso für die Definition im Anwendungsbereich des § 393 SGB V, weil hier genau dasselbe Begriffsverständnis gelten soll, wie es unter dem BSIG anzuwenden ist. Die Definition aus der Richtlinie scheint auch „unbedingt" zu sein, weil sie keine Vorbehalte regelt und auch nicht mit einer Bedingung versehen ist. Das spricht ebenfalls für einen geringen Umsetzungsspielraum bei der Einbettung der Begriffsdefinition in das nationale Recht.

Allerdings wäre es theoretisch im Einklang mit den europarechtlichen Vorgaben denkbar, dass der deutsche Gesetzgeber die Definition auf mehr Akteure ausweitet als dies in der Richtlinie vorgesehen ist. Eine solche Ausweitung könnte zu einer überschießenden Umsetzung führen, die grundsätzlich zulässig ist.[24] Es wäre jedoch nicht möglich, dass der deutsche Gesetzgeber die Definition enger fasst, als sie in Art. 6 Nr. 30 NIS2-RL geregelt wird, weil andernfalls die Ziele der Richtlinie – die der deutsche Gesetzgeber u.a. im BSIG umsetzt – nicht erreicht werden.[25] Hinsichtlich der Umsetzung von Definitionen soll aber nicht unerwähnt bleiben, dass ein nationaler Gesetzgeber grundsätzlich nicht verpflichtet ist, Definitionen aus einer Richtlinie wortwörtlich in sein nationales Recht zu übernehmen.[26] Eine Verpflichtung zur wortwörtlichen Übernahme besteht nur dann, wenn die Ziele der unionsrechtlichen Vorgaben anders nicht erreicht werden können.[27] Sprachliche Abweichungen wären grundsätzlich möglich, wobei inhaltlich weiterhin der Anwendungsbereich der nationalen Definition

[20] Siehe Art. 288 Abs. 3 AEUV: „*Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel*".
[21] Siehe dazu exemplarisch *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, Art. 288 AEUV Rn. 27 und 28.
[22] *Schroeder*, in: Streinz, EUV/AEUV, Art. 288 AEUV Rn. 61.
[23] *Schroeder*, in: Streinz, EUV/AEUV, Art. 288 AEUV Rn. 94.
[24] Siehe zur Zulässigkeit der überschießenden Umsetzung *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, Art. 288 AEUV Rn. 131.
[25] *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, Art. 288 AEUV Rn. 120: „*Eine Pflicht zur Umsetzung unter Übernahme des Wortlautes der Richtlinie besteht allerdings nicht; den Mitgliedstaaten bleibt die Wahl der Formulierung, solange sich nur die Rechtsgehalte der Richtlinie im nationalen Recht inhaltsgleich wiederfinden*".
[26] Zur Umsetzung von Definitionen EuGH, Urt. v. 19.12.2013, C-281/11, ECLI:EU:C:855 Rn. 59 ff. und die dort aufgeführte Rechtsprechung; siehe auch EuGH, Urt. v. 25.1.2018, C-314/16, ECLI:EU:C:2018:42 Rn. 35.
[27] Siehe hierzu explizit EuGH, Urt. v. 25.1.2018, C-314/16, ECLI:EU:C:2018:42 Rn. 36.

mindestens genauso weit sein muss, wie die Definition aus der Richtlinie. Es müssen alle in der Richtlinie definierten Fälle miterfasst werden. Sofern der deutsche Gesetzgeber keine überschießende Umsetzung vornehmen wird, gilt sowohl für das BSIG als auch für § 393 SGB V die Begriffsdefinition aus der NIS2-RL.

Insgesamt ist also festzustellen, dass die Definition für Cloud-Computing-Dienste aus der NIS2-RL auch im Rahmen des § 393 SGB V angewendet werden kann. Es ist lediglich denkbar, dass der deutsche Gesetzgeber sich dafür entscheidet, die Definition noch weiter zu fassen, als sie in der NIS2-RL angelegt ist. Für eine solche gesetzgeberische Absicht gibt es aktuell aber keine Anzeichen. Es ist wahrscheinlich, dass der deutsche Gesetzgeber im BSIG die gleiche Definition übernehmen wird, wie sie jetzt schon in § 384 Nr. 5 SGB V enthalten ist.

1.3. Die Fragen zu 2. 2) a) bis f)

Es gibt verschiedene Arten der Rechenzentrumsleistung für einen Leistungserbringer; z.B. Betrieb eines Praxisverwaltungssystems (PVS), Betrieb eines Krankenhausinformationssystems (KIS) oder auch Abruf von Daten wie z.B. radiologische Bilddaten oder Labordaten aus entsprechend über das Internet erreichbaren IT-Systemen, wobei der Abruf und die dazu gehörende Übertragung der Daten dem Stand der Technik entsprechend geschützt werden.

> 2. 2 a) Welche Gegebenheiten müssen erfüllt sein, damit die Definition eines Cloud-Computing-Dienst im Sinne des § 384 Ziffer 5 SGB V (im Folgenden nur als „Definition“ bezeichnet) erfüllt ist?
>
> 2. 2) b) Stellt jede über einen Fernzugang (= Internetnutzung) erreichbare Ressource (KIS, PVS, TI WANDA Dienst ...) einen Cloud-Computing Dienst im Sinne der Definition dar?
>
> 2. 2) c) Stellt die für den Fernzugang verwendete Cloud-Technologie ebenfalls einen Cloud-Computing Dienst im Sinne der Definition dar?
>
> 2. 2) d) Wenn skalierbare Ressourcen wie Arbeitsspeicher, Datenspeicher oder CPU im Rechenzentrum nach Bedarf gebucht werden können, stellen dann die unter der vorhergehenden Frage beschriebene Dienste einen Cloud-Computing Dienst im Sinne der Definition dar?
>
> 2. 2) e) Stellt ein sog. Housing im Rechenzentrum einen Cloud-Computing Dienst im Sinne der Definition nach?
>
> 2. 2) f) Stellt eine in einer Cloud-Umgebung gehostete Anwendung, z.B. eine Software zur klinischen Entscheidungshilfe oder auch ein PVS/KIS, einen Cloud-Computing-Dienst im Sinne der Definition dar?

1.4. Die Antworten zu 2. 2) a) bis f)

Im Folgenden beantworten wir die Fragen zu 2. 2) a) bis 2. 2) f) getrennt. Zusammengefasst lauten die Antworten auf folgende Fragen wie folgt:

- *2. 2) a)*: Es muss ein digitaler Dienst vorliegen, der durch Abruf die Verwaltung und einen umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht.
- *2. 2) b)*: Nein, nicht jede über einen Fernzugang erreichbare Ressource ist auch ein Cloud-Computing Dienst im Sinne der Definition, weil neben dem Vorhandensein eines umfassenden Fernzugangs auch andere Merkmale der Begriffsdefinition erfüllt sein müssen. Bspw. wenn der Fernzugang zu einer anderen Ressource als einer Rechenressource bereitgestellt wird, dann liegt kein Cloud-Computing-Dienst vor. Es kommt zusätzlich vor allem darauf an, ob der Dienst auf Abruf die Verwaltung ermöglicht, der Pool skalierbar und elastisch ist und der Dienst eine gemeinsame Nutzung von Rechenressourcen ermöglicht.
- *2. 2) c)*: Es kommt darauf an, ob so eine Technologie auch alle Merkmale der Begriffsdefinition erfüllt. Ist dies der Fall, dann ja. Ist dies nicht der Fall, dann nein. Nur weil für den Fernzugang an sich eine Cloud-Technologie verwendet wird, scheidet das Vorliegen eines Cloud-

Computing-Dienstes noch nicht kategorisch aus. Es kommt vor allem darauf an, ob der Dienst auf Abruf die Verwaltung ermöglicht, der Pool skalierbar und elastisch ist und der Dienst eine gemeinsame Nutzung von Rechenressourcen ermöglicht.

- *2. 2) d)*: Es kommt darauf an, ob auch das Definitionsmerkmal „die gemeinsame Nutzung ermöglicht" erfüllt ist. Ist dies der Fall, dann ja. Ist dies nicht der Fall, dann nein.
- *2. 2) e)*: Nein, weil beim in der ausführlichen Antwort näher beschriebenen Housing die Dienstleistung nicht elektronisch erbracht wird und somit kein elektronischer Dienst vorliegt, ist das Housing auch keine Form von Cloud-Computing-Dienst. Der Fall ist dann anders zu beurteilen, wenn das Housing in Form der Bereitstellung virtueller Maschinen erfolgt und deswegen ein digitaler Dienst vorliegt. In so einem Fall erfolgt das virtuelle Housing auch in Form eines Cloud-Computing-Dienstes, sofern alle anderen Definitionsmerkmale erfüllt sind.*2. 2) f)*: Ja, sofern für den Dienst die Verarbeitung hinsichtlich der Nutzer separat erfolgt. „Separat" verlangt eine Form von Mandantentrennung. Es sprechen mehrere Argumente dafür, dass der „Cloud-Nutzer" in diesem Sinne ein Unternehmen und keine Einzelperson ist.

1.4.1. Antwort zu 2. 2) a)

Es ist fraglich, welche Gegebenheiten erfüllt sein müssen, damit die Definition eines Cloud-Computing-Dienstes im Sinne des § 384 Nr. 5 SGB V erfüllt ist. Gemäß § 384 Nr. 5 SGB V und Art. 6 Nr. 30 NIS2-RL wird ein Cloud-Computing-Dienst wie folgt definiert: „*Cloud-Computing-Dienst [meint] einen 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*."

Aus der Definition ist erkennbar, dass ein Cloud-Computing-Dienst nur dann vorliegt, wenn die folgenden Voraussetzungen alle zusammen erfüllt sind:

- a) es geht um einen digitalen Dienst;
- b) durch Abruf wird die Verwaltung und der umfassende Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht.

Gemäß der Definition ist es wegen der Formulierung „*auch wenn*" irrelevant, ob die Ressourcen auf mehrere Standorte verteilt sind oder nicht. In ErwGr. 33 Satz 3 NIS2-RL wird erkennbar, dass Bereitstellungsmodelle für Cloud-Computing die private, die gemeinschaftliche, die öffentliche und die hybride Cloud umfassen.

Zum Kriterium a): Der Begriff digitaler Dienst ist im Einklang mit der Definition aus Art. 1 Abs. 1 lit. b Richtlinie (EU) 2015/1535 zu verstehen.[28] Gemäß dieser Vorschrift geht es dann um einen digitalen Dienst, wenn eine Dienstleistung der Informationsgesellschaft vorliegt. Das meint jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Digitale Dienste werden immer elektronisch erbracht.[29]

Zum Kriterium b): Innerhalb des Kriteriums b) gibt es verschiedene Begrifflichkeiten, deren Inhalt klärungsbedürftig ist. Hierzu zählen die folgenden Begriffe, die laut ErwGr. 33 zur NIS2-RL Folgendes umfassen oder meinen:

Begriff	Bedeutung entsprechend ErwGr. 33
Umfassender Fernzugang	Der Begriff „umfassender Fernzugang" wird verwendet, um zu beschreiben, dass die Cloud-Kapazitäten über das Netz bereitgestellt und über Mechanismen zugänglich gemacht werden, die den Einsatz heterogener Thin- oder Thick-Client-Plattformen (einschließlich Mobiltelefonen, Tablets, Laptops und Arbeitsplatzrechnern) fördern.
Skalierbar	Der Begriff „skalierbar" bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes

[28] Art. 6 Nr. 23 NIS2-RL: „*digitaler Dienst" einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates*".
[29] Zu diesem Kriterium und dessen Relevanz für die Abgrenzung zu einem Rechenzentrumsdienst siehe auch die Antwort zu 2. 3) b).

	flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können.
Elastischer Pool	Der Begriff „elastischer Pool“ wird verwendet, um Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die Menge der verfügbaren Ressourcen je nach Arbeitsaufkommen rasch erhöht oder reduziert werden kann.
Gemeinsam nutzbar	Der Begriff „gemeinsam nutzbar“ wird verwendet, um Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird.
Rechenressourcen	Zu Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Betriebssysteme, Software, Speicher, Anwendungen und Dienste. Zu den Dienstmodellen des Cloud-Computing gehören unter anderem IaaS (Infrastructure as a Service, PaaS (Platform as a Service), SaaS (Software as a Service) und NaaS (Network as a Service).
Verteilt	Der Begriff „verteilt“ wird verwendet, um Rechenressourcen zu beschreiben, die sich auf verschiedenen vernetzten Computern oder Geräten befinden und die untereinander durch Nachrichtenaustausch kommunizieren und koordinieren.
Verwaltung	Dass sich der Cloud-Computing-Nutzer selbst ohne Interaktion mit dem Anbieter von Cloud-Computing-Diensten Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann, könnte als Verwaltung auf Abruf beschrieben werden.

1.4.2. Antwort zu 2. 2) b)

Es ist fraglich, ob jede über einen Fernzugang (= Internetnutzung) erreichbare Ressource (KIS, PVS, TI WANDA Dienst…) ein Cloud-Computing Dienst im Sinne der Definition ist. Ausweislich § 384 Nr. 5 SGB V und Art. 6 Nr. 30 NIS2-RL meint ein Cloud-Computing-Dienst „*einen 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*.“

Weil ein Fernzugang über das Internet erfolgt, scheint das Merkmal „digitaler Dienst“ erfüllt zu sein. Es wird im Folgenden auch davon ausgegangen, dass das Kriterium „umfassender Fernzugang“ erfüllt ist. Die hier zu untersuchende Dienste-Art wäre dann kein Cloud-Computing-Dienst, wenn nicht alle anderen Merkmale der Begriffsdefinition ebenfalls erfüllt sind. Ausweislich der Frage wird darauf abgestellt, ob schon ein irgendwie gearteter Fernzugang immer dazu führt, dass auch ein Cloud-Computing-Dienst vorliegt. Das ist grundsätzlich zu verneinen, weil die Ressource auch immer eine Rechenressource sein muss und die übrigen Definitionsmerkmale ebenfalls erfüllt sein müssen.

ErwGr. 33 Satz 2 bis 4 zur NIS2-RL benennt folgende Beispiele für Rechenressourcen und deren Bereitstellungsmodelle: „*Zu Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Betriebssysteme, Software, Speicher, Anwendungen und Dienste. Zu den Dienstmodellen des Cloud-Computing gehören unter anderem IaaS (Infrastructure as a Service, PaaS (Platform as a Service), SaaS (Software as a Service) und NaaS (Network as a Service). Die Bereitstellungsmodelle für Cloud-Computing sollten die private, die gemeinschaftliche, die öffentliche und die hybride Cloud umfassen*.“ Wenn ein Fernzugang zu einer Ressource bereitgestellt wird, die keine Rechenressource in diesem Sinne ist, dann liegt auch kein Cloud-Computing-Dienst vor.

Außerdem ist denkbar, dass der Dienst andere Definitionsmerkmale nicht erfüllt. Wenn ein Dienst zwar einen Fernzugang zu einer Rechenressource ermöglicht, aber

- der Dienst nicht auf Abruf die Verwaltung eines skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen ermöglicht oder
- der Pool jedoch nicht skalierbar ist (die Ressource kann nicht unabhängig von ihrem geografischen Standort oder nicht flexibel zugeteilt werden) oder

- der Pool jedoch nicht elastisch ist (Rechenressourcen werden nicht entsprechend der Nachfrage bereitgestellt und freigegeben) oder
- nicht die gemeinsame Nutzung von Rechenressourcen ermöglicht (der Dienst wird nicht einer Vielzahl von Nutzern bereitgestellt oder es gibt keinen gemeinsamen Zugang für eine Vielzahl an Nutzern oder die Verarbeitung erfolgt nicht separat oder der Dienst wird nicht über dieselbe elektronische Ausrüstung erbracht),

dann ist die über den Fernzugang erreichbare Rechenressource kein Cloud-Computing Dienst im Sinne der Definition.

1.4.3. Antwort zu 2. 2) c)

Es ist fraglich, ob eine für den Fernzugang verwendete Cloud-Technologie ebenfalls ein Cloud-Computing-Dienst im Sinne der Definition ist. Dies wäre dann der Fall, wenn eine für den Fernzugang verwendete Cloud-Technologie alle Merkmale der Begriffsdefinition erfüllt. Also die für den Fernzugang verwendete Cloud-Technologie ein digitaler Dienst ist, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht. Sind alle Merkmale erfüllt, dann ist auch die für einen Fernzugang verwendete Cloud-Technologie ein Cloud-Computing-Dienst. Im Umkehrschluss gilt auch, dass sobald ein Merkmal der Begriffsdefinition nicht erfüllt ist, die für einen Fernzugang verwendete Cloud-Technologie kein Cloud-Computing-Dienst ist.

Der Frage ist zu entnehmen, dass es hier um eine Cloud-Technologie geht, weswegen im Folgenden davon ausgegangen wird, dass das Merkmal „digitaler Dienst“ erfüllt ist. Weil die Technologie für einen Fernzugang verwendet wird, wird auch davon ausgegangen, dass das Kriterium „umfassender Fernzugang“ erfüllt ist. Die Aufzählung der Beispiele für Rechenressourcen in ErwGr. 33 Satz 2 NIS2-RL ist nicht abschließend, weil das Wort „wie“ verwendet wird. Es werden die folgenden Arten von Ressourcen explizit benannt: „*Netze*, *Server oder sonstige Infrastruktur*, *Betriebssysteme*, *Software*, *Speicher*, *Anwendungen und Dienste*“. Wenn eine für den Fernzugang verwendete Technologie einen Zugang zu einem Cloud-Computing-Dienst ermöglicht, dann ist es wahrscheinlich, dass auch ein Zugang zu Rechenressourcen vorliegt, weil der Begriff „Rechenressourcen“ alle möglichen Formen von elektronischen Ressourcen erfasst. Allerdings müssen auch in diesem Fall die übrigen Merkmale der Begriffsdefinition erfüllt sein, damit die für den Fernzugang verwendete Cloud-Technologie auch selbst ein Cloud-Computing-Dienst ist.

In der Frage wird ein Stück weit darauf abgestellt, ob schon deswegen kein Cloud-Computing-Dienst vorliegt, weil für den Fernzugang an sich eine Cloud-Technologie genutzt wird. Es gibt in der Begriffsdefinition keine Anhaltspunkte dafür, dass so eine Art von Dienst kategorisch kein Cloud-Computing-Dienst sein kann.

Eine für den Fernzugang verwendete Cloud-Technologie wäre dann kein Cloud-Computing-Dienst, wenn:

- der Dienst nicht auf Abruf die Verwaltung eines skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen ermöglicht oder
- der Pool nicht skalierbar ist (die Ressource kann nicht unabhängig von ihrem geografischen Standort oder nicht flexibel zugeteilt werden) oder
- der Pool nicht elastisch ist (Rechenressourcen werden nicht entsprechend der Nachfrage bereitgestellt und freigegeben) oder
- der Dienst nicht die gemeinsame Nutzung von Rechenressourcen ermöglicht (der Dienst wird nicht einer Vielzahl von Nutzern bereitgestellt oder es gibt keinen gemeinsamen Zugang für eine Vielzahl an Nutzern oder die Verarbeitung erfolgt nicht separat oder der Dienst wird nicht über dieselbe elektronische Ausrüstung erbracht).

1.4.4. Antwort zu 2. 2) d)

Es ist fraglich, ob die folgenden Dienste als Cloud-Computing-Dienst gelten, wenn skalierbare Ressourcen wie Arbeitsspeicher, Datenspeicher oder CPU im Rechenzentrum nach Bedarf gebucht werden können:

- a) jede über einen Fernzugang erreichbare Ressource;
- b) die für den Fernzugang verwendete Cloud-Technologie.

Die in der Frage benannten Ressourcen gelten als Rechenressourcen im Sinne der Begriffsdefinition (zur in dem Zusammenhang indirekt relevanten Abgrenzung von Cloud-Computing-Diensten und Rechenzentrumsdiensten siehe auch die Antwort zu 2. 3) b)). Dieses Merkmal ist demzufolge erfüllt. Aus der Frage geht auch hervor, dass das Merkmal „skalierbar" erfüllt ist. Weil nach Bedarf gebucht werden kann, ist auch das Kriterium „elastisch" erfüllt. Da nach Bedarf gebucht werden kann, scheint auch eine Verwaltung auf Abruf vorzuliegen. Sowohl bei a) als auch bei b) liegt jeweils ein Fernzugang vor, weswegen das Kriterium „umfassender Fernzugang" erfüllt sein sollte. Es gibt keine Anhaltspunkte dafür, dass es nicht um einen digitalen Dienst geht.

Damit in den unter a) und b) benannten Fällen auch ein Cloud-Computing-Dienst i.S.d. Definition vorliegt, müsste zudem das folgende Merkmal erfüllt sein, damit alle Merkmale vollständig vorliegen: „*die gemeinsame Nutzung von Rechenressourcen ermöglicht*".

Der relevante Dienst ermöglicht dann keine „gemeinsame Nutzung", wenn er nicht einer Vielzahl von Nutzern bereitgestellt wird oder es keinen gemeinsamen Zugang für eine Vielzahl an Nutzern gibt oder die Verarbeitung nicht separat erfolgt oder der Dienst nicht über dieselbe elektronische Ausrüstung erbracht wird. In solchen Fällen sind die unter a) und b) benannten Dienste keine Cloud-Computing-Dienste i.S.d. Begriffsdefinition.

1.4.5. Antwort zu 2. 2) e)

Es ist fraglich, ob ein Housing im Rechenzentrum als ein Cloud-Computing-Dienst im Sinne der Definition erfolgt. Im Folgenden wird davon ausgegangen, dass „Housing" eine Dienstleistung meint, die darin besteht, dass ein Dritter beim Housing-Anbieter physisch seine Server und ggf. Hardware stellen darf und der Housing-Anbieter die Stromzufuhr, Kühlung, den Brandschutz und ähnliche Aspekte sicherstellt. Außerdem sorgt der Housing-Anbieter auch für die Anbindung an das Internet. Bei dieser Dienstleistung greift der Housing-Anbieter nicht auf den Server und die darauf gespeicherten Daten zu. Damit ein Housing-Anbieter einen Cloud-Computing-Dienst bereitstellen würde, müssten alle Merkmale der Begriffsdefinition erfüllt sein.

Beim Housing müsste es also auch um einen digitalen Dienst gehen, weil jeder Cloud-Computing-Dienst auch ein „digitaler Dienst" ist.[30] Gemäß Art. 1 Abs. 1 lit. b Richtlinie (EU) 2015/1535 liegt nur dann ein digitaler Dienst vor, wenn die mit dem Dienst erbrachte Dienstleistung auch elektronisch erbracht wird. Eine Dienstleistung wird gemäß Art. 1 Abs. 1 lit. b ii) Richtlinie (EU) 2015/ 1535 dann elektronisch erbracht, wenn sie „*mittels Geräte für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird*".

Weil die Dienstleistung beim Housing eher mit einem Mietrecht vergleichbar ist,[31] es vordergründig um die Bereitstellung eines sicheren Standortes für Server geht und die eigentliche Leistung nicht mit elektronischen Mitteln erbracht wird, ist das Housing keine Form von Cloud-Computing-Dienst.

Der Fall wäre nur dann anders zu beurteilen, wenn nicht die im ersten Absatz der Antwort hier beschriebene Form von Housing relevant wäre. Es wäre nämlich auch denkbar, dass ein Housing in virtueller Form vorgenommen wird, indem virtuelle Maschinen bereitgestellt werden. In diesen Fällen erfolgt das Housing auch in Form der Bereitstellung eines digitalen Dienstes und ist dann auch ein Cloud-Computing-Dienst, wenn die weiteren Definitionsmerkmale erfüllt sind.

[30] Vgl. § 384 Nr. 5 SGB V und Art. 6 Nr. 30 NIS2-RL; siehe dazu auch *Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, § 2 BSIG Rn. 32.
[31] Siehe dazu exemplarisch *Auer-Reinsdorff*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 21 Rn. 41.

1.4.6. Antwort zu 2. 2) f)

Es ist fraglich, ob eine in einer Cloud-Umgebung gehostete Anwendung, z.B. eine Software zur klinischen Entscheidungshilfe oder auch ein PVS/KIS, ein Cloud-Computing-Dienst im Sinne der Definition ist. Dies wäre dann der Fall, wenn alle Definitionsmerkmale zusammen erfüllt sind.

Die Frage zielt auch ein Stück weit darauf ab, ob eine gehostete Anwendung als eine Rechenressource im Sinne der Begriffsdefinition gilt. Weil in ErwGr. 33 Satz 2 zur NIS2-RL auch Software, Anwendungen und Dienste als Beispiele für Rechenressourcen genannt werden, steht die Einstufung einer in einer Cloud-Umgebung gehosteten Anwendung als Cloud-Computing-Dienst nicht bereits der Umstand entgegen, dass die Ressource an sich in einer Cloud-Umgebung gehostet wird. Es wird im Folgenden davon ausgegangen, dass auch das Merkmal „digitaler Dienst" erfüllt ist, weil es um eine in einer Cloud-Umgebung gehosteten Anwendung geht. Weil über das Internet auf die Anwendung in der Cloud zugegriffen werden würde, wird auch vom Vorliegen des Kriteriums „umfassender Fernzugang" ausgegangen. Da in der Cloud-Umgebung gehostete Anwendungen typischerweise unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden können, wird auch angenommen, dass das Merkmal „skalierbar" erfüllt ist. Eine in einer Cloud-Umgebung gehostete Anwendung sollte in der Regel auch entsprechend der Nachfrage bereitgestellt und freigegeben werden können und es liegt somit auch das Kriterium „elastisch" vor.

Neben diesen erfüllten Merkmalen müsste der Dienst aber auch die gemeinsame Nutzung ermöglichen. Dies ist dann der Fall, wenn die Rechenressourcen einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird. Demzufolge wäre eine in der Cloud-Umgebung gehostete Anwendung dann kein Cloud-Computing-Dienst, wenn:

- 1) der Dienst nicht einer Vielzahl von Nutzern bereitgestellt wird oder
- 2) es keinen gemeinsamen Zugang für eine Vielzahl an Nutzern gibt oder
- 3) die Verarbeitung nicht separat erfolgt oder
- 4) der Dienst nicht über dieselbe elektronische Ausrüstung erbracht wird.

Hinsichtlich des im letzten Bulletpoint genannten Kriteriums 4) ist allerdings davon auszugehen, dass eine in einer Cloud-Umgebung gehostete Anwendung auch in der Regel über dieselbe elektronische Ausrüstung erbracht wird. Der bvitg hat uns außerdem mitgeteilt, dass wir auch vom Vorliegen der Kriterien 1) und 2) der Bulletpoints ausgehen und auf das Kriterium 3) weiter eingehen sollen.

Kriterium 3 verlangt, dass eine Verarbeitung „für jeden Nutzer separat erfolgt". Was hierrunter zu verstehen ist, wird weder in der Richtlinie noch in dazugehörigen ErwGr. oder im SGB näher bestimmt. Es dürfte hinsichtlich des Merkmals „separat" wohl darauf ankommen, dass eine Form von Mandantentrennung erfolgt und so für jeden Nutzer die Verarbeitung auch separat erfolgen kann. Würde hingegen keine Mandantentrennung vorgenommen werden, dann erfolgt die Verarbeitung auch nicht mehr für mehrere Nutzer, aber doch gleichzeitig separat. Es muss irgendwie möglich sein, die Verarbeitung für mehrere Nutzer zu separieren, obwohl es einen gemeinsamen Zugang gibt. In dem Kontext stellt sich auch die Frage, ob ein „Nutzer" in diesem Sinne eine Einzelperson oder ein Unternehmen ist. In der NIS2-RL wird dies nicht explizit geregelt, aber in ErwGr. 35 zur NIS2-RL wird der Begriff „Cloud-Computing-Nutzer" so verwendet, dass der Nutzer die Person ist, welche *„selbst ohne Interaktion mit dem Anbieter von Cloud-Computing-Diensten Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann"*. Es scheint also darauf anzukommen, dass es zwischen dem Nutzer und dem Anbieter ein Vertragsverhältnis gibt, auf dessen Basis Rechenkapazitäten zugewiesen werden. Außerdem sollte auch wesentlich sein, dass der Nutzer derjenige ist, der beim Anbieter ohne Interaktion Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann. In der Regel sollte das Vertragsverhältnis mit einem Unternehmen und nicht einer Einzelperson vorliegen. Ebenso sollte in der Regel auch die Zuweisung der Rechenkapazitäten eher durch ein Unternehmen oder zumindest in dessen Namen erfolgen. Das spricht dafür, dass der Nutzer eines Cloud-Computing-Dienstes, für den die Verarbeitungen separat erfolgen müssen, in der Regel ein Unternehmen ist. Es soll aber nicht unerwähnt bleiben, dass „Nutzer" in der NIS2-RL auch in anderen Kontexten und nicht nur in Bezug auf Cloud-Computing-Nutzer verwendet wird und an anderen Stellen mit Nutzer auch Einzelpersonen gemeint sein können.

2. Fragen und Antworten zu Fragen unter 2. (2) g) bis i))

2.1. Die Fragen zu 2. 2) g) bis i)

2. 2) g) VMware vSphere wurde ursprünglich entwickelt, damit in Rechenzentren virtualisierte IT-Ressourcen bereitgestellt werden können und somit nicht für jede neue Applikation ein eigener, physischer Server existieren muss. Wenn Krankenhäuser keine Kapazität in ihrem eigenen Rechenzentrum haben, werden Dienstleister („Hoster“) beauftragt. Viele von diesen Dienstleistern setzen vSphere ein, um Workloads verschiedener Kunden zu virtualisieren.

i) Fällt eine von einem Hoster bereitgestellte Vmware-vSphere-Umgebung unter die Definition eines Cloud-Computing-Dienstes?

ii) D.h., sind diese Hoster Cloud-Anbieter, wenn sie über das Internet erreichbare vSphere-Umgebungen anbieten?

2. 2) h) Nicht personenbezogene Katalogdaten wie beispielsweise Arzneimittel, Diagnosen oder auch Prozeduren werden teilweise in einer Cloud gepflegt. In der Gesundheitsversorgung eingesetzte Systeme rufen diese Daten ab und aktualisieren dadurch die lokal gespeicherten Daten. Nur mit den lokal gespeicherten Daten wird im Rahmen der Patientenbehandlung gearbeitet, z.B. ein Rezept ausgestellt.

i) Stellt diese Bereitstellung von medizinischen Katalogdaten ohne Personenbezug einen Cloud-Computing-Dienst im Sinne der Definition dar?

ii) Wenn die in der Cloud bereitgestellten nicht personenbezogenen Katalogdaten ohne lokale Zwischenspeicherung direkt in der lokal laufenden Applikation verwendet werden: stellt diese direkte Nutzung von medizinischen Katalogdaten ohne Personenbezug einen Cloud-Computing-Dienst im Sinne der Definition dar?

iii) Wenn eine der beiden oder auch beide Fragen mit „ja“ beantwortet werden, sind dann die Regelungen von § 393 SGB V anzuwenden, auch wenn kein Personenbezug existiert?

iv) Stellt eine über einen Fernzugang erreichbare Ressource, welche Metainformationen zu lokal verwendeten Applikationen verarbeitet und auf Basis dieser Informationen Dateien zum Download bereitstellt (Applikationsdaten, Kataloge etc.), einen Cloud-Dienst im Sinne der Definition dar?

2. 2) i) Bei Online-Terminvereinbarungen zwischen Patienten und Leistungserbringern werden Gesundheitsdaten verarbeitet. Wenn bei dieser Onlineterminvereinbarung eine Speicherung dieser Daten nur temporär und verschlüsselt in der Cloud erfolgt, ist dann für diesen Dienst ein BSI-C5-Testat notwendig?

2.2. Die Antworten zu 2 (2. 2) g) bis i))

Im Folgenden beantworten wir die Fragen zu 2. 2) g) bis 2. 2) i) getrennt. Zusammengefasst lauten die Antworten auf folgende Fragen wie folgt:

- *2. 2) g) i) und ii)*: Wenn ein Anbieter die Infrastruktur inkl. Server und das Betriebssystem bereitstellt, dann ist der bereitgestellte Dienst nicht allein deswegen kein Cloud-Computing-Dienst, weil lediglich die Infrastruktur inkl. Server und das Betriebssystem bereitgestellt werden. Denn hier geht es um Rechenressourcen, die im Rahmen der Begriffsdefinition für einen Cloud-Computing-Dienst vorliegen müssen. Ein Hoster ist dann ein Anbieter eines Cloud-Computing-Dienstes, wenn er den Cloud-Dienst unter seinem eigenen Namen oder unter seiner eigenen Marke vermarktet oder unter fremder Marke vertreibt oder vertreiben lässt. Im Kontext des § 393 SGB V ist jedoch zu beachten, dass diese Vorschrift nicht nur für Anbieter eines Cloud-Computing-Dienstes gilt, sondern für Leistungserbringer und Kranken- und Pflegekassen und deren Auftragsverarbeiter.
- *2. 2) h) i und ii)*: Für das Vorliegen eines Cloud-Computing-Dienstes kommt es nicht darauf an, ob die mit so einem Dienst verarbeiteten Daten einen Personenbezug haben oder nicht. Die

beschriebene Bereitstellung von medizinischen Katalogdaten ohne Personenbezug erfolgt dann als Cloud-Computing-Dienst, wenn alle Definitionsmerkmale erfüllt sind. Dabei kommt es nicht auf den Personenbezug der Daten an. Liegt ein Cloud-Computing-Dienst vor, aber es werden mit diesem Dienst keine personenbezogenen Daten verarbeitet, dann ist § 393 SGB V nicht anwendbar. Es kommt für das Vorliegen der Begriffsmerkmale auch nicht darauf an, ob in einer Cloud gespeicherte Informationen nur ohne Zwischenspeicherung in einer lokal verwendeten Applikation genutzt werden.

- *2. 2) h) iii)*: Nein, weil die Regelungen aus § 393 SGB V alle nur für die Verarbeitung von Sozial- und Gesundheitsdaten gelten und diese Datenarten immer personenbezogen sind.
- *2. 2) h) iv)*: Für das Vorliegen eines Cloud-Computing-Dienstes kommt es nicht darauf an, ob Metainformationen zu lokal verwendeten Applikationen verarbeitet werden. Der in der Frage geschilderte Dienst kann grundsätzlich alle Definitionsmerkmale eines Cloud-Computing-Dienstes erfüllen.
- *2. 2) i)*: Der Umstand, dass die verarbeiteten Daten verschlüsselt sind und nur temporär gespeichert werden, ist für das Vorliegen eines Cloud-Computing-Dienstes nicht relevant. Die Dauer der Datenverarbeitung ist für das Vorliegen einer Verarbeitung personenbezogener Daten nicht relevant und daher auch nicht für die Anwendbarkeit des § 393 SGB V maßgeblich. Dasselbe gilt auch für eine Verschlüsselung in dem in der Frage beschriebenen Fall. Das Testat kann auch für längere Zeit als „aktuell" gelten, solange es noch nicht abgelaufen ist und die faktischen, attestierten Gegebenheiten weiterhin mit der Wirklichkeit übereinstimmen und § 393 Abs. 4 SGB V zu dem relevanten Zeitpunkt nicht einen anderen Typ von Testat (bspw. Typ2) verlangt.

2.3. Antwort zu 2. 2) g) i) und ii)

Es ist fraglich, ob eine von einem Hoster bereitgestellte VMware-vSphere-Umgebung unter die Definition eines Cloud-Computing-Dienstes fällt (Frage i)) und ob Hoster Cloud-Anbieter sind, wenn sie über das Internet erreichbare vSphere-Umgebungen anbieten (Frage ii)). Auf unsere Rückfragen hin hat der bvitg mitgeteilt, dass es im Rahmen der Frage i) vor allem darum geht zu klären, ob auch dann ein Cloud-Computing-Dienst vorliegt, wenn durch die Bereitstellung der VMware-vSphere-Umgebung nur Infrastruktur inkl. Server und Betriebssystem bereitgestellt werden. Bei der Frage ii) soll das Dreiecksverhältnis zwischen Hoster, VMware-Anbieter und Cloud-Anbieter beachtet werden.

In Bezug auf Frage i) ist festzustellen, dass ErwGr. 33 zur NIS2-RL beispielhaft die folgenden Rechenressourcen benennt: „*Ressourcen wie Netze*, *Server oder sonstige Infrastruktur*, *Betriebssysteme*, *Software*, *Speicher*, *Anwendungen und Dienste*". Wenn ein Anbieter demzufolge die Infrastruktur inkl. Server und Betriebssystem bereitstellt, dann ist der bereitgestellte Dienst nicht allein deswegen kein Cloud-Computing-Dienst, weil lediglich die Infrastruktur inkl. Server und Betriebssystem bereitgestellt werden. Denn hier geht es um Rechenressourcen, die im Rahmen der Begriffsdefinition für einen Cloud-Computing-Dienst vorliegen müssen. In dem eben schon erwähnten ErwGr. 33 wird hinsichtlich der Bereitstellungsmodelle auch auf Dienste der Art Infrastructure as a Service verwiesen. Der in Frage i) angesprochene Dienst wäre wohl hierunter zu subsumieren.

Mit Blick auf die Frage ii) ist relevant, dass in § 384 SGB V durch die Gesetzesänderung Folgendes mit aufgenommen wurde: „*Im Sinne dieses Kapitels bezeichnet der Ausdruck (…) 4.: Anbieter eine natürliche oder juristische Person, die ein informationstechnisches System* ***unter ihrem eigenen Namen oder unter ihrer eigenen Marke vermarktet oder*** *unter* ***fremder Marke vertreibt oder vertreiben lässt***". Der Anbieter eines Cloud-Computing-Dienstes muss einerseits die eben zitierte Definition erfüllen und andererseits muss auch der von ihm angebotene Dienst die Merkmale eines Cloud-Computing-Dienstes erfüllen. Somit ist ein Hoster dann ein Anbieter eines Cloud-Computing-Dienstes, wenn er den Cloud-Dienst unter seinem eigenen Namen oder unter seiner eigenen Marke vermarktet oder unter fremder Marke vertreibt oder vertreiben lässt. Im Kontext des § 393 SGB V ist jedoch zu beachten, dass diese Vorschrift nicht nur für Anbieter eines Cloud-Computing-Dienstes gilt, sondern für die Verarbeitung personenbezogener Daten im Wege eines Cloud-Computing-Dienstes und für Leistungserbringer, Kranken- und Pflegekassen sowie deren Auftragsverarbeiter.

2.3.1. Antwort zu 2. 2) h) i) und ii)

Nicht personenbezogene Katalogdaten wie beispielsweise Arzneimittel, Diagnosen oder auch Prozeduren werden teilweise in einer Cloud gepflegt. In der Gesundheitsversorgung eingesetzte Systeme rufen diese Daten ab und aktualisieren dadurch die lokal gespeicherten Daten. Nur mit den lokal gespeicherten Daten wird im Rahmen der Patientenbehandlung gearbeitet, z.B. ein Rezept ausgestellt.

Es ist fraglich, ob diese Bereitstellung von medizinischen Katalogdaten ohne Personenbezug in Form eines Cloud-Computing-Dienstes erfolgt (Frage i). Außerdem ist fraglich, ob in einem Fall, indem die in der Cloud bereitgestellten nicht personenbezogenen Katalogdaten ohne lokale Zwischenspeicherung direkt in der lokal laufenden Applikation verwendet werden, diese direkte Nutzung von medizinischen Katalogdaten ohne Personenbezug eine Nutzung eines Cloud-Computing-Dienstes ist (Frage ii).

Beide Fragen zielen darauf ab, zu hinterfragen, ob es für das Vorliegen eines Cloud-Computing-Dienstes darauf ankommt, ob mit so einem Dienst personenbezogene Daten verarbeitet werden. Ausweislich der Begriffsdefinition aus § 384 Nr. 5 SGB V und Art. 6 Nr. 30 NIS2-RL kommt es jedenfalls nicht explizit darauf an, ob der digitale Dienst für die Verarbeitung personenbezogener Daten verwendet wird. Aus den bereits in diesem Gutachten mehrfach angesprochenen Merkmalen der Begriffsdefinition geht auch nicht indirekt hervor, dass nur dann ein Cloud-Computing-Dienst vorliegen kann, wenn mit so einem Dienst personenbezogene Daten verarbeitet werden. Weil die NIS2-RL auch nicht auf Basis der Kompetenznorm für Verarbeitungen personenbezogener Daten aus Art. 16 Abs. 2 AEUV, sondern der allgemeinen Binnenmarktkompetenz aus Art. 114 AEUV erlassen wurde, lässt sich auch nicht argumentieren, dass der Anwendungsbereich der Richtlinie oder speziell der Begriffsdefinition auf Situationen begrenzt ist, in denen personenbezogene Daten verarbeitet werden. Es gibt auch sonst keine Anhaltspunkte dafür, dass die Begriffsdefinition für Cloud-Computing-Dienste in irgendeiner Weise verlangt, dass mit dem relevanten Dienst immer auch personenbezogene Daten verarbeitet werden.

Während § 393 Abs. 1 SGB V als Rechtsgrundlage für die Verarbeitung von Sozial- und Gesundheitsdaten – und damit nur für personenbezogene Daten[32] (siehe auch die Antwort zu 2. 2) h) iii)) – gilt, ist es für das Vorliegen eines Cloud-Computing-Dienstes jedoch nicht erforderlich, dass mit so einem Dienst personenbezogene Daten verarbeitet werden. Liegt ein Cloud-Computing-Dienst vor, aber es werden mit diesem Dienst keine personenbezogenen Daten verarbeitet, dann ist § 393 SGB V nicht anwendbar. Dabei ist jedoch zu beachten, dass der deutsche Gesetzgeber plant auf die Definition im noch zu verabschiedenden BSIG n.F. zu verweisen[33] und somit sowohl für die Rechtsgrundlage in § 393 Abs. 1 SGB V als auch Pflichten aus dem BSIG dasselbe Begriffsverständnis gelten wird.

Somit ist die Frage i) dahingehend zu beantworten, dass es für das Vorliegen eines Cloud-Computing-Dienstes nicht darauf ankommt, ob die mit so einem Dienst verarbeiteten Daten einen Personenbezug haben. Der beschriebene Dienst müsste aber auch fernab dessen alle Definitionsmerkmale des Begriffs „Cloud-Computing-Dienst“ erfüllen.

Im Rahmen der Frage ii) soll außerdem geprüft werden, ob die Verwendung der in der Cloud bereitgestellten Katalogdaten ohne lokale Zwischenspeicherung direkt in der lokal laufenden Applikation gegen das Vorliegen eines Cloud-Computing-Dienstes sprechen. Demzufolge soll hier hinterfragt werden, ob eine nicht erfolgende lokale Zwischenspeicherung und die erfolgende direkte Nutzung in der lokal laufenden Applikation entscheidend dafür sind, dass kein Cloud-Computing-Dienst vorliegt. Diese Umstände könnten nur dann entscheidend sein, wenn sie auch wesentlich für das Vorliegen eines Begriffsmerkmals der Definition für Cloud-Computing-Dienste sind. Es ist jedoch nicht ersichtlich, dass eine nicht erfolgende lokale Zwischenspeicherung wesentlich in diesem Sinne ist. Man könnte eventuell darüber nachdenken, ob auch eine Rechenressource vorliegt, weil es in der Frage vor allem um den Zugang zu Informationen geht. Wenn jedoch eine Art von Dienst für diesen Vorgang verwendet wird, dann kann dieser Dienst wiederum schon als eine Rechenressource anzusehen sein. Insgesamt sind wir der Auffassung, dass eine ausbleibende lokale Speicherung und Nutzung von in der Cloud hinterlegten

[32] Gesundheitsdaten sind immer personenbezogene Daten und auch Sozialdaten sind ausweislich § 67 Abs. 2 SGB X immer personenbezogene Daten.
[33] BT, Drucksache 20/9048, S. 135 in Bezug auf § 384 Nr. 5 SGB V.

Informationen in einer lokalen Applikation für sich genommen nicht dazu führen, dass kein Cloud-Computing-Dienst vorliegt.

2.3.2. Antwort zu 2. 2) h) iii)

Es ist fraglich, ob die Regelungen aus § 393 SGB V auch anzuwenden sind, wenn keine Verarbeitung personenbezogener Daten erfolgt. Es wäre einerseits theoretisch denkbar, dass der gesamte § 393 SGB V nur für die Verarbeitung personenbezogener Daten gilt, oder dass andererseits einige Vorgaben aus der Vorschrift nur für personenbezogene Daten gelten, während andere Vorgaben sowohl für personenbezogene als auch nicht personenbezogene Daten gelten.

Während Abs. 1 der Norm die Rechtsgrundlage für die Verarbeitung personenbezogener Daten allgemein ausgestaltet, werden in den Abs. 2 bis 4 die einzelnen zu Abs. 1 dazugehörigen Zulässigkeitsvoraussetzungen geregelt. Die Abs. 5 bis 7 nehmen Bezug auf die Anforderungen aus Abs. 3. Sie sind also zusammen mit den Zulässigkeitsvoraussetzungen zu lesen. § 393 Abs. 8 SGB V regelt lediglich, dass die Vorschriften aus dem SGB X und dem BDSG unberührt bleiben. Es ist also in der Gesamtschau der Norm ausgeschlossen, dass einige ihrer Bestandteile nur für personenbezogene Daten gelten, während andere Bestandteile gleichermaßen für personenbezogene und nicht personenbezogene Daten gelten. Der § 393 Abs. 1 SGB V dient ausweislich der Gesetzesbegründung *„als expliziter Erlaubnistatbestand der Nutzung des Cloud-Computings für die aufgezählten Fälle bei der Verarbeitung von Sozial- und Gesundheitsdaten“*.[34] § 393 Abs. 1 SGB V gilt für die Verarbeitung von „Sozial- und Gesundheitsdaten“. Sozial- und Gesundheitsdaten sind immer personenbezogen. Somit ist der Anwendungsbereich von vornherein auf die Verarbeitung personenbezogener Daten beschränkt.

Es ist daher ausgeschlossen, dass der § 393 SGB V auch dann anzuwenden ist, wenn keine Verarbeitung personenbezogener Daten erfolgt. Demzufolge gelten die Vorgaben aus § 393 SGB V nicht, wenn keine personenbezogenen Daten verarbeitet werden. Das steht einer Einstufung dieser Art von Diensten als Cloud-Computing-Dienste jedoch nicht entgegen (siehe die Antwort zu 2. 2) h) i) und ii)).

2.3.3. Antwort zu 2. 2) h) iv)

Es ist fraglich, ob eine über einen Fernzugang erreichbare Ressource, welche Metainformationen zu lokal verwendeten Applikationen verarbeitet und auf Basis dieser Informationen Dateien zum Download bereitstellt (Applikationsdaten, Kataloge etc.), ein Cloud-Computing-Dienst ist. Vorab sei anzumerken, dass im Einklang mit den Antworten zu den Fragen h) i) bis iii) irrelevant ist, ob die Metainformationen personenbezogene Daten sind oder nicht.

Damit eine über einen Fernzugang erreichbare Ressource, welche Metainformationen zu lokal verwendeten Applikationen verarbeitet und auf Basis dieser Informationen Dateien zum Download bereitstellt (Applikationsdaten, Kataloge etc.), ein Cloud-Computing-Dienst ist, müssten alle Merkmale der Begriffsdefinition erfüllt sein. Der Frage ist zu entnehmen, dass es um eine per Fernzugang erreichbare Ressource geht, weswegen vom Vorliegen eines umfassenden Fernzugangs und eines digitalen Dienstes ausgegangen wird. Der Frage ist nicht zu entnehmen, dass die Ressource nicht unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden kann. Demzufolge wird auch davon ausgegangen, dass das Merkmal „skalierbar“ erfüllt ist. Weil es keine Anhaltspunkte dafür gibt, dass die Ressourcen nicht entsprechend der Nachfrage bereitgestellt und freigegeben werden, wird auch vom Vorliegen des Merkmals „elastisch“ ausgegangen. Damit die Ressource als „gemeinsam nutzbar“ gilt, muss diese einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird. Der Frage ist nicht zu entnehmen, ob dies der Fall ist oder nicht.

Damit ein Cloud-Computing-Dienst vorliegt, müsste es bei der Ressource auch um eine Rechenressource gehen. Ausweislich ErwGr. 33 zur NIS2-RL zählen hierzu *„Ressourcen wie Netze, Server oder sonstige Infrastruktur, Betriebssysteme, Software, Speicher, Anwendungen und Dienste. Zu den Dienstmodellen des Cloud-Computing gehören unter anderem IaaS (Infrastructure as a Service, PaaS (Platform as a Service), SaaS (Software as a Service) und NaaS (Network as a Service).“* Der Frage ist zu entnehmen, dass

[34] BT, Drucksache 20/9048, S. 150 in Bezug auf § 393 Abs. 1 SGB V.

Metainformationen zu lokal verwendeten Applikationen verarbeitet werden und auf Basis dieser Informationen Dateien zum Download bereitgestellt werden. Somit könnte die Ressource darin gesehen werden, dass ein Speicher für die abgerufenen Informationen bereitgestellt wird oder der für den Abruf verwendete Dienst für sich genommen als eine „Anwendung" oder ein „Dienst" i.S.v. ErwGr. 33 zur NIS2-RL einzustufen ist.

Zusammenfassend ist mit Blick auf die Frage iv) festzustellen, dass es für das Vorliegen eines Cloud-Computing-Dienstes nicht darauf ankommt, ob Metainformationen zu lokal verwendeten Applikationen verarbeitet werden. Die Untersuchung der Definitionsmerkmale hat ergeben, dass in dem in der Frage geschilderten Fall ein Cloud-Computing-Dienst vorliegen könnte.

2.3.4. Antwort zu 2. 2) i)

Bei Online-Terminvereinbarungen zwischen Patienten und Leistungserbringern werden Gesundheitsdaten verarbeitet. Es soll davon ausgegangen werden, dass bei dieser Onlineterminvereinbarung eine Speicherung von Gesundheitsdaten nur temporär und verschlüsselt in der Cloud erfolgt. Es ist fraglich, ob in dem Fall für diesen Dienst ein BSI-C5-Testat notwendig ist. Unsere Rückfrage zu der hier zu klärenden Frage hat ergeben, dass wir prüfen sollen, ob auch bei einer nur temporären Speicherung und Verschlüsselung der Daten ein Cloud-Computing-Dienst vorliegt und ob ein „aktuelles" C5-Testat vorhanden sein muss.

Es wäre dann ein BSI-C5-Testat notwendig, wenn im Rahmen der geschilderten Online-Terminvereinbarungen ein Cloud-Computing-Dienst für die Verarbeitung von Gesundheits- oder Sozialdaten eingesetzt werden würde. Die Frage zielt darauf ab, ob eine lediglich temporäre Speicherung und eine Verschlüsselung dafür relevant sind, ob die Vorgaben aus § 393 SGB V beachtet werden müssen oder nicht. Wie bereits in diesem Gutachten ausgeführt, gelten die Vorgaben aus § 393 SGB V nur für die Verarbeitung personenbezogener Daten, obwohl es für das Vorliegen eines Cloud-Computing-Dienstes nicht erforderlich ist, dass mit so einem Dienst personenbezogene Daten verarbeitet werden. Eine Unanwendbarkeit des § 393 SGB V könnte also theoretisch daraus folgen, dass keine personenbezogenen Daten mit einem Cloud-Computing-Dienst verarbeitet werden. In dem Fall wäre dann auch die Pflicht zum Nachweis eines BSI-C5-Testats nicht mehr anwendbar.

Die Dauer der Speicherung ist für das Vorliegen einer Verarbeitung personenbezogener Daten irrelevant.[35] Denn in der DSGVO ist nirgendwo vorgesehen, dass ein nur besonders kurz erfolgender Vorgang, der ansonsten aber als Verarbeitung nach Art. 4 Nr. 2 DSGVO anzusehen ist, wegen seiner kurzen Dauer nicht mehr als Verarbeitung personenbezogener Daten gilt. Weil die DSGVO das Kriterium der Dauer für das Vorliegen einer Verarbeitung nicht erwähnt und Art. 4 Nr. 2 DSGVO für den gesamten Anwendungsbereich der Verordnung und deren Schutzumfang maßgeblich ist, ist das Ausscheiden des Vorliegens einer Verarbeitung wegen der kurzen Dauer eines Vorgangs im Einklang mit den Maßstäben aus der EuGH-Rechtsprechung nicht möglich.[36] Ein Abstellen auf die Dauer des Vorgangs, ohne dass hierfür Vorgaben in der DSGVO enthalten sind, stünde im Sinne der EuGH-Rechtsprechung dem Ziel der DSGVO entgegen, ein hohes Niveau des Schutzes (…) bei der Verarbeitung personenbezogener Daten zu gewährleisten. Somit kann eine temporäre Speicherung nicht schon dazu führen, dass keine Verarbeitung personenbezogener Daten erfolgt und deswegen die Vorgaben aus § 393 SGB V nicht anwendbar sind.

---

[35] Siehe zur Irrelevanz der Dauer der Datenspeicherung *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 4 DSGVO Rn. 11; siehe auch *Schwenke*, NJW 2018, 823 (824): „*Das gilt auch bei Löschung innerhalb weniger Millisekunden, da die DS-GVO keine Ausnahmeregeln für Zwischenverarbeitung entsprechend § 44 a UrhG enthält und auch bei schneller Verarbeitung Daten missbraucht werden können*".

[36] Siehe in dem Zusammenhang EuGH, Urt. v. 7.3.2024, C-740/22, ECLI:EU:C:2024:216 Rn. 31: „*Diese Auslegung des Begriffs „Verarbeitung" wird durch das Ziel der DSGVO bestätigt, die (…) ein hohes Niveau des Schutzes (…) bei der Verarbeitung personenbezogener Daten zu gewährleisten*" und den hier übertragbaren Gedanken in EuGH, Urt. v. 26.10.2023, C-307/22, ECLI:EU:C:2023:811 Rn. 51: „*Angesichts der Bedeutung, die die DSGVO dem (…) Recht auf Auskunft über die personenbezogenen Daten (…) zur Erreichung solcher Ziele beimisst, darf die Ausübung dieses Rechts folglich nicht von Bedingungen abhängig gemacht werden, die der Unionsgesetzgeber nicht ausdrücklich festgelegt hat*."

In einigen Fällen wird vertreten, dass eine verschlüsselte Speicherung keine Verarbeitung personenbezogener Daten sei, [37] während andere Stimmen den Entfall des Personenbezugs durch Verschlüsselung pauschal[38] ablehnen. Im Einklang mit der EuGH-Entscheidung in der Rechtssache Scania CV AB muss jedoch davon ausgegangen werden, dass auch die verschlüsselten Daten weiterhin als personenbezogene Daten für den Anbieter des Cloud-Speicherplatzes gelten würden, solange der die Daten in der Cloud speichernde Akteur einen Personenbezug herstellen kann.[39] Weil Leistungserbringer, Kranken- und Pflegekassen in der Regel genau wissen werden, auf wen sich die verschlüsselt in der Cloud gespeicherten Daten beziehen, bleibt der Personenbezug demzufolge auch für den Anbieter des Speicherplatzes (den Auftragsverarbeiter) bestehen. Demzufolge ist insgesamt ausgeschlossen, dass wegen einer nur temporär und nur verschlüsselt erfolgenden Speicherung keine Verarbeitung personenbezogener Daten vorliegt und deswegen auch § 393 SGB V nicht anwendbar sein würde.

Es wäre demzufolge lediglich denkbar, dass der in Frage i) beschriebene Dienst wegen anderen Gründen als der Dauer der Speicherung und der Verschlüsselung nicht in Form eines Cloud-Computing-Dienstes bereitgestellt wird und deswegen die Vorgaben zum BSI-C5-Testat in § 393 SGB V nicht anwendbar sind.

Für einen Cloud-Computing-Dienst ist in der Regel auch gemäß § 393 Abs. 3 Nr. 2 SGB V ein aktuelles BSI-C5-Testat notwendig. Unsere Rückfrage beim bvitg hat ergeben, dass man sich im Zusammenhang mit dem Merkmal „aktuell“ die Frage stellt, wann ein Testat als aktuell gilt und wann nicht mehr. Wir wurden in dem Kontext darauf hingewiesen, dass ein C5-Testat eines Wirtschaftsprüfers im Gegensatz zu Zertifikaten von Zertifizierungsstellen nie die Gültigkeit verliert. In der Gesetzesbegründung ist nicht ersichtlich, wann ein C5-Testat nach Willen des deutschen Gesetzgebers als „aktuell“ gilt und wann nicht. In § 393 Abs. 4 SGB V wird aber deutlich, dass in Zukunft andere Testate als das BSI-C5-Testat Typ1 als „aktuell“ gelten. Außerdem wird in § 384 Nr. 6 SGB V „aktuelles C5-Testat“ wie folgt definiert: „*das positive Prüfergebnis über einen sicheren Cloud-Computing-Dienst anhand des Kriterienkatalogs C5 (Cloud Computing Compliance Criteria Catalogue) des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils gültigen Fassung*.“ Hinsichtlich der Aktualität wird nur auf die jeweils gültige Fassung verwiesen.

Der Sinn und Zweck der Aufnahme der Anforderung, dass ein aktuelles Testat vorliegen muss, spricht dafür, dass das Testat nicht bereits abgelaufen sein darf, sofern es denn ein Ablaufdatum geben sollte. Außerdem ist ein Testat nur dann aktuell, wenn es auch die faktischen Gegebenheiten des Cloud-Computing-Dienstes hinreichend abdeckt. Dies wäre bspw. dann nicht der Fall, wenn das Testat für einen Dienst erteilt wurde, der aber mittlerweile ganz anders eingesetzt wird oder funktioniert, sodass das Testat den faktisch eingesetzten Dienst nicht in seiner aktuellen Form abdeckt. Solange die attestierten Aspekte weiterhin der Wirklichkeit entsprechen, solange sollte das Testat auch erst einmal grundsätzlich als „aktuell“ gelten können. Es ist jedoch zu beachten, dass ab 1.7.2025 nur noch ein C5-Typ2-Testat als „aktuelles“ Testat gilt.

3. Fragen und Antworten zu Fragen unter 2. 3)

In Art. 6 Ziff. 31 NIS2-RL wird ergänzend zum „Cloud-Computing-Dienst“ in Ziffer 30 der Terminus „Rechenzentrumsdienst“ legal definiert.

> a) Ist es richtig, dass ein Rechenzentrumsdienst kein Cloud-Computing-Dienst im Sinne des § 384 Ziffer 5 SGB V sein kann, auch wenn der Rechenzentrumsdienst in einem von einem Dienstleister bereitgestellten externen Rechenzentrum betrieben wird?

---

[37] Siehe etwa *Schultze-Melling*, in: Taeger/Gabel, DSGVO - BDSG – TTDSG, Art. 32 Rn. 16.

[38] Siehe etwa *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 32 DSGVO Rn. 33: „*Sowohl Pseudonymisierung als auch eine (grundsätzlich reversible) Verschlüsselung ändern nichts an der Einstufung der Daten als personenbezogen*“; *Klabunde*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 4 DSGVO Rn. 19: „*Selbstverständlich beeinflusst auch eine Verschlüsselung von Daten deren Personenbezug in keiner Weise*“; *Borges*, in: Borges/Hilber, BeckOK IT-Recht, Art. 32 DSGVO Rn. 11: „*Der Personenbezug bleibt hier (…) allerdings vollständig erhalten*“; etwas zurückhaltender *Martini*, in: Paal/Pauly, DS-GVO BDSG, Art. 32 DSGVO Rn. 34: „*der Personenbezug [bleibt] bei der Verschlüsselung grds. vollständig erhalten*“.

[39] EuGH, Urt. v. 9.11.2023, C-319/22, ECLI:EU:C:2023:837 Rn. 49: „*für diese Wirtschaftsakteure sowie mittelbar für die Fahrzeughersteller, die die FIN bereitstellen, ein personenbezogenes Datum im Sinne von Art. 4 Nr. 1 DSGVO dar, selbst wenn die FIN für sich genommen für die Fahrzeughersteller kein persönliches Datum darstellt*“.

b) Wenn ja: Anhand welcher Kriterien kann zwischen „Cloud-Computing-Dienst“ und „Rechenzentrumsdienst“ differenziert werden?

3.1. Antwort zu 2. 3) a)

Die Antwort in Kürze: Nein, es ist nicht richtig, dass ein Rechenzentrumsdienst – der in einem von einem Dienstleister bereitgestellten externen Rechenzentrum betrieben wird – kein Cloud-Computing-Dienst im Sinne des § 384 Nr. 5 SGB V sein kann. Ausweislich ErwGr. 35 Satz 1 zur NIS2-RL ist ein Rechenzentrumsdienst manchmal aber nicht immer auch ein Cloud-Computing-Dienst.

Es ist fraglich, ob ein Rechenzentrumsdienst kein Cloud-Computing-Dienst im Sinne des § 384 Nr. 5 SGB V sein kann, auch wenn der Rechenzentrumsdienst in einem von einem Dienstleister bereitgestellten externen Rechenzentrum betrieben wird (Frage a)).

Gemäß Art. 6 Nr. 31 NIS2-RL meint ein Rechenzentrumsdienst „*einen Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden*.“

In der Frage wird bereits richtigerweise angedeutet, dass das Vorliegen eines Rechenzentrumsdienstes verlangt, dass es nicht um „*interne Rechenzentren geht, die sich im Besitz der betreffenden Einrichtung befinden und von der betreffenden Einrichtung für eigene Zwecke betrieben werden*“. Demzufolge muss ein Rechenzentrumsdienst immer in einem externen Rechenzentrum erbracht werden. Das ergibt sich auch aus ErwGr. 35 Satz 4 zur NIS2-RL. In ErwGr. 35 Satz 1 zur NIS2-RL heißt es außerdem wie folgt: „*Dienste, die von Anbietern von Rechenzentrumsdiensten angeboten werden, werden möglicherweise* ***nicht immer in Form eines Cloud-Computing-Diensts*** *erbracht. Dementsprechend sind Rechenzentren möglicherweise* ***nicht immer*** *Teil einer Cloud-Computing-Infrastruktur*“. Anhand der eben zitierten Passage wird deutlich, dass in einigen Fällen Rechenzentrumsdienste auch Cloud-Computing-Dienste sind, während aber in anderen Fällen Rechenzentrumsdienste keine Cloud-Computing-Dienste sind. Demzufolge lautet die Antwort auf die Frage a), dass es nicht richtig ist, dass ein Rechenzentrumsdienst kein Cloud-Computing-Dienst im Sinne des § 384 Nr. 5 SGB V sein kann.

3.2. Antwort zu 2. 3) b)

Die Frage b) wird eigentlich nur gestellt, wenn die Antwort auf Frage a) „ja“ lautet. Die Antwort auf Frage a) ist jedoch „nein“, weil auch ein Rechenzentrumsdienst ein Cloud-Computing-Dienst sein kann. Dennoch wollen wir im Folgenden kurz darstellen, wie Rechenzentrumsdienste von Cloud-Computing-Diensten abzugrenzen sind.

Im Allgemeinen liegt dann zwar ein Rechenzentrumsdienst aber kein Cloud-Computing-Dienst vor, wenn der Dienst alle Merkmale der Definition aus Art. 6 Nr. 31 NIS2-RL erfüllt, gleichzeitig jedoch nicht alle Merkmale aus Art. 6 Nr. 30 NIS2-RL vorliegen. In den folgenden Fällen geht es zwar um einen Rechenzentrumsdienst, aber dieser Dienst ist dann kein Cloud-Computing-Dienst, wenn einer der folgenden Aussagen auf so einen Rechenzentrumsdienst zutrifft:

- der Rechenzentrumsdienst ist kein digitaler Dienst, weil die relevante Dienstleistung nicht elektronisch[40], sondern in anderer Form erbracht wird;
- der Rechenzentrumsdienst ermöglicht keinen umfassenden Fernzugang, weil der Dienst nicht über das Netz bereitgestellt wird oder nicht über Mechanismen zugänglich gemacht wird, die den Einsatz heterogener Thin- oder Thick-Client-Plattformen (einschließlich Mobiltelefonen, Tablets, Laptops und Arbeitsplatzrechnern) fördern;
- der Rechenzentrumsdienst wird nicht in Bezug auf Rechenressourcen erbracht, weil ein Zugang zu anderen Arten von Ressourcen bereitgestellt wird (bspw. nur Serverunterbringung);

[40] In den folgenden Fällen wir eine Dienstleistung elektronisch erbracht: eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird (Art. 1 Abs. 1 lit. b ii) Richtlinie (EU) 2015/1535).

- der Rechenzentrumsdienst ist nicht skalierbar, weil die Rechenressourcen nicht unabhängig von ihrem geografischen Standort vom Anbieter des Dienstes flexibel zugeteilt werden können;
- der Rechenzentrumsdienst ist nicht elastisch, weil die Rechenressource nicht entsprechend der Nachfrage bereitgestellt und freigegeben wird und somit die Menge der verfügbaren Ressourcen nicht rasch erhöht oder reduziert werden kann;
- der Rechenzentrumsdienst ist nicht gemeinsam nutzbar, weil
    - er nicht einer Vielzahl von Nutzern bereitgestellt wird oder
    - weil es keinen gemeinsamen Zugang auf den Dienst für die Vielzahl an Nutzer gibt, sondern die Nutzer einen getrennten Zugang haben oder
    - die Verarbeitung für jeden Nutzer nicht separat, sondern zusammen für alle Nutzer erfolgt oder
    - der Dienst nicht für alle Nutzer über dieselbe elektronische Ausrüstung erbracht wird, sondern bei unterschiedlichen Nutzern mit unterschiedlicher elektronischer Ausrüstung erbracht wird.

III. Fragen zum Ort der Cloud-Verarbeitung

Die im Folgenden Abschnitt beantworteten Fragen betreffen den Ort der Cloud-Verarbeitung.

1. Fragen und Antworten zu Fragen unter 3. 1)

1.1. Die Fragen zu 3. 1)

§ 393 Abs. 2 SGB V legt den Ort der Verarbeitung auf die EU oder Drittländer mit Angemessenheitsbeschluss fest.

> a) Können amerikanische Hyperscaler (Microsoft, AWS, Google etc.) auch genutzt werden, wenn der Angemessenheitsbeschluss der EU-Kommission vom EuGH annulliert wird, sofern ausschließlich Rechenzentren in Europa zur Verarbeitung genutzt werden, der Hyperscaler über eine Niederlassung im Inland verfügt, jedoch im Rahmen der Fernwartung des Cloud-Systems ein Fernzugriff aus den USA aufgrund der Notwendigkeit der Hinzuziehung eines entsprechenden spezialisierten Technikers nicht 100%ig sicher ausgeschlossen werden kann?
>
> b) Verarbeitungen innerhalb von Unternehmens-Gruppen basieren häufig auf verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules, BCRs). Im Rahmen von Cloud-Diensten werden mitunter auch Beschäftigte aus einem Drittland für einzelne Supportleistungen, insbesondere bei Fehlerbeseitigungen, eingesetzt werden müssen.
>
> > i) Ist es richtig, dass BCRs nicht ausreichend sind, um eine Verarbeitung in einem Drittland zu ermöglichen, wenn gleichzeitig kein Angemessenheitsbeschluss für das Drittland existiert?
> >
> > ii.) D.h., ist eine Drittlandverarbeitung möglich, wenn ein Angemessenheitsbeschluss für das betreffende Drittland existiert?

1.2. Die Antworten zu den Fragen unter 3. 1)

Im Folgenden werden die Antworten zu den Fragen a) und b) getrennt erteilt. Zusammengefasst lauten die Antworten auf folgende Fragen wie folgt:

- *a)*: Die in der Frage explizit genannten Umstände führen nicht dazu, dass durch einen tatsächlich auch erfolgenden Fernzugriff auf Gesundheits- oder Sozialdaten keine Datenübermittlung in die USA erfolgen würde und die Vorgaben aus § 393 Abs. 2 SGB V erfüllt wären. Weil § 393 Abs. 2 Nr. 3 SGB V nur dann eine Datenübermittlung in ein Drittland ermöglicht, wenn für dieses Land ein Angemessenheitsbeschluss vorhanden ist, würde ein fehlender Angemessenheitsbeschluss weitreichende Konsequenzen haben und die Zusammenarbeit mit US-amerikanischen Hyperscalern schwer denkbar erscheinen lassen.
- *b) i)*: Ja, es ist richtig, dass BCRs nicht ausreichend sind, um eine Verarbeitung in einem Drittland zu ermöglichen, wenn gleichzeitig kein Angemessenheitsbeschluss für das Drittland existiert und § 393 SGB V anwendbar ist.

- *b) ii)*: Ja, eine Verarbeitung im Drittland ist im Anwendungsbereich des § 393 SGB V nur möglich, wenn ein Angemessenheitsbeschluss für das betreffende Drittland existiert.

1.2.1. Antwort auf Frage a)

Es ist fraglich, ob amerikanische Hyperscaler (Microsoft, AWS, Google etc.) auch genutzt werden können, wenn der Angemessenheitsbeschluss der Europäischen Kommission vom EuGH annulliert wird, sofern ausschließlich Rechenzentren in Europa zur Verarbeitung genutzt werden, der Hyperscaler über eine Niederlassung im Inland verfügt, jedoch im Rahmen der Fernwartung des Cloud-Systems ein Fernzugriff aus den USA aufgrund der Notwendigkeit der Hinzuziehung eines entsprechenden spezialisierten Technikers nicht 100%ig sicher ausgeschlossen werden kann.

Der Frage ist zu entnehmen, dass davon ausgegangen werden soll, dass für die Datenverarbeitungen ausschließlich Rechenzentren in Europa genutzt werden, es aber im Rahmen der Fernwartung zu Fernzugriffen aus den USA kommen kann. Für die Beantwortung der Frage wird davon ausgegangen, dass der Fernzugriff auch hinsichtlich Gesundheits- und Sozialdaten nicht 100%ig sicher ausgeschlossen werden kann. Zudem wird davon ausgegangen, dass die Rechenzentren sich nicht nur in Europa befinden, sondern in einem Mitgliedstaat der EU oder des EWR.

Gemäß § 393 Abs. 2 SGB V gilt Folgendes: Die Verarbeitung von Sozial- und Gesundheitsdaten im Wege des Cloud-Computing-Dienstes darf nur

- 1. im Inland; oder
- 2. in einem Mitgliedstaat der Europäischen Union; oder
- 3. in einem diesem nach § 35 Absatz 7 des Ersten Buches gleichgestellten Staat oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat erfolgen

und sofern die datenverarbeitende Stelle über eine Niederlassung im Inland verfügt.

Die Vorgaben aus § 393 Abs. 2 SGB V sind aber nur dann anwendbar, wenn mit einem Cloud-Computing-Dienst auch Gesundheits- und Sozialdaten durch Leistungserbringer, Kranken- oder Pflegekassen oder deren Auftragsverarbeiter verarbeitet werden. Die zuvor hier zitierten Vorgaben entsprechen im Wesentlichen auch jenen, die in § 80 Abs. 2 SGB X geregelt sind. Hinzukommend regelt § 393 Abs. 2 SGB V noch die Notwendigkeit einer Niederlassung im Inland. Demzufolge gelten im Anwendungsbereich des § 393 SGB V auch immer die Voraussetzungen aus § 80 Abs. 2 SGB X. Ausweislich der Frage soll davon ausgegangen werden, dass die Hyperscaler über eine Niederlassung im Inland verfügen, weswegen dieses Kriterium nicht mehr im weiteren Verlauf geprüft wird (zur Frage, wer mit „datenverarbeitende Stelle“ gemeint ist und eine Niederlassung im Inland haben muss, siehe die Antwort auf die Frage 4. 2) a)). Vorab sei auch angemerkt, dass die Einschränkungen in § 393 Abs. 2 SGB V und § 80 Abs. 2 SGB X auf Art. 49 Abs. 5 DSGVO basieren, wonach Datenübermittlungen in Drittländer u.a. durch mitgliedstaatliches Recht Beschränkungen unterliegen können.[41]

Im Rahmen des § 393 Abs. 2 SGB V kommt es – genauso wie bei § 80 Abs. 2 SGB X – auf den Ort der Datenverarbeitung an und nicht lediglich auf das Land, indem ein Auftragsverarbeiter seinen Sitz hat.[42] Der Frage ist zu entnehmen, dass diese für den Fall beantwortet werden soll, dass für die USA kein Angemessenheitsbeschluss mehr besteht, aber Zugriffe aus den USA im Rahmen der Fernwartung nicht ausgeschlossen sind. Die USA sind kein gleichgestellter Staat i.S.v. § 393 Abs. 2 SGB V und gelten auch nicht als „Inland“ oder als „Mitgliedstaat der EU“. Daher bliebe es nur theoretisch möglich, dass die Verarbeitung auch bei einem solchen US-Fernzugriff im Inland oder in einem Mitgliedstaat der EU i.S.v. § 393 Abs. 2 Nr. 1 oder 2 SGB V erfolgt und deswegen die Voraussetzungen aus § 393 Abs. 2 SGB V erfüllt sind, obwohl es einen Fernzugriff aus den USA geben kann. Denn sobald eine Verarbeitung auch in einem Drittland ohne Angemessenheitsbeschluss erfolgen würde, wären die Voraussetzungen aus §

[41] Siehe zu Art. 49 Abs. 5 DSGVO als Öffnungsklausel und Grundlage des § 80 Abs. 2 SGB X *Rombach*, in: Hauck/Noftz, SGB X, § 80 SBG X Rn. 17; *Palsherm*, in: Schlegel/Voelzke, juris PraxisKommentar SGB X, § 80 SGB X Rn. 40.

[42] *Palsherm*, in: Schlegel/Voelzke, juris PraxisKommentar SGB X, § 80 SGB X Rn. 40; *Strothmann/Ahrend*, in: Krahmer, Sozialdatenschutzrecht, § 80 SGB X Rn. 33.

393 Abs. 2 SGB V nicht mehr erfüllt.[43] Weil der Frage zu entnehmen ist, dass die Datenverarbeitungen in Rechenzentren innerhalb der EU erfolgen, ist davon auszugehen, dass keine Verarbeitung im Inland i.S.v. § 393 Abs. 2 Nr. 1 vorliegt. Hierfür wäre es nämlich erforderlich, dass die Daten nicht außerhalb von Deutschland übermittelt werden. Es wäre also nur theoretisch denkbar, dass die Verarbeitung auch bei einem Fernzugriff in der EU erfolgt, weil in der EU die Rechenzentren betrieben werden.

Eine Verarbeitung erfolgt dann in einem Mitgliedstaat der EU i.S.v. § 393 Abs. 2 Nr. 2 SGB V, wenn keine Datenübermittlung außerhalb der EU erfolgt. Die bloße Tatsache, dass ein Auftragsverarbeiter eine US-amerikanische Muttergesellschaft hat, führt nicht bereits zu einer Verarbeitung der Daten in den USA.[44] Es wäre aber denkbar, dass durch den Fernzugriff aus den USA eine Verarbeitung in den USA stattfindet. In dem Fall wären die Vorgaben aus § 393 Abs. 2 Nr. 2 SGB V nicht erfüllt.

Der Begriff „Datenübermittlungen in Drittländer" sollte im Kontext des § 393 Abs. 2 SGB V (dort „Verarbeitung in einem Drittstaat") genauso verstanden werden, wie in Kapitel V DSGVO, weil die Vorschrift aus dem SGB V ausweislich der Gesetzesbegründung datenschutzrechtlicher Natur ist.[45] Das folgt auch aus der Gesetzesbegründung zu § 80 Abs. 2 SGB X, wonach durch die speziellen Vorgaben für den Ort der Datenverarbeitung *„gewährleistet [wird], dass Sozialdaten nicht in unsichere Drittstaaten übermittelt werden*."[46] Das gilt gleichermaßen für die Vorgaben aus § 393 Abs. 2 SGB V, weil diese in Anlehnung an § 80 Abs. 2 SGB X erlassen wurden und alle Voraussetzungen aus § 80 Abs. 2 SGB X auch Bestandteil von § 393 Abs. 2 SGB V sind.[47] Eine Auslegung im Einklang mit der DSGVO ist auch deswegen notwendig, weil die Vorgaben – wie bereits erwähnt – auf Basis der Öffnungsklausel aus Art. 49 Abs. 5 DSGVO erlassen wurden und Beschränkung der Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer darauf basierend vorsehen.[48] Ohne eine solche Beschränkungsbefugnis wäre es nicht ohne weiteres möglich, dass der deutsche Gesetzgeber die Anwendbarkeit der meisten Erlaubnistatbestände für Drittlandsübermittlungen aus Kapitel V DSGVO ausschließt. Deswegen muss das Begriffsverständnis für Datenübermittlungen in Drittländer zwangsläufig im SGB V dem entsprechen, wie es auch in der DSGVO vorgesehen ist.

In der DSGVO wird allerdings nicht definiert, wann eine Übermittlung personenbezogener Daten in Drittländer erfolgt. Der Begriff „Datenübermittlung in Drittländer" sollte entsprechend der Formulierung „jedwede Übermittlung" in Art. 44 Satz 1 DSGVO und entsprechend des Schutzwecks[49] der Vorschrift grundsätzlich weit verstanden werden. Das Ziel der Bestimmungen aus Kapitel V DSGVO besteht darin, das in der EU garantierte Schutzniveau auch dann zu gewährleisten, wenn Daten in ein Drittland übermittelt oder in einem solchen Land verarbeitet werden.[50] Wie bereits erwähnt, besteht der Schutzzweck der Vorschriften aus § 393 Abs. 2 SGB V und § 80 Abs. 2 SGB X jeweils darin, dass Sozial- und Gesundheitsdaten nicht in unsichere Drittländer übertragen werden. Als „unsicher" in diesem Sinne gelten ausweislich § 393 Abs. 2 Nr. 3 SGB V und § 80 Abs. 2 SGB X alle Drittländer ohne Angemessenheitsbeschluss.

Es ist im Einklang mit den vorstehenden Ausführungen für die Klärung der gestellten Frage zu prüfen, ob auch ein Fernzugriff aus den USA auf in der EU gespeicherte Daten eine Datenübermittlung im Sinne von Art. 44 DSGVO wäre. Der EDSA geht davon aus, dass bei einem Fernzugriff aus einem Drittland auf

---

[43] Siehe in dem Zusammenhang auch BKartA, Beschl. v. 13.2.2023 – VK 2 - 114/22, Rn. 119; *Strothmann/Ahrend*, in: Krahmer, Sozialdatenschutzrecht, § 80 SGB X Rn. 33: *„Nicht möglich ist die Beauftragung eines Auftragsverarbeiters in einem Drittstaat, für den kein Angemessenheitsbeschluss vorliegt*."; siehe auch zur Rechtslage vor dem Angemessenheitsbeschluss für die USA *Herbst*, in: Rolfs/Körner/Krasney/Mutschler, beck-online.GROSSKOMMENTAR, § 80 SGB X Rn. 56: *„Eine Datenübermittlung an die USA ist daher nur nach den Maßgaben des Abs. 3 möglich.*"

[44] BKartA, Beschl. v. 13.2.2023 – VK 2 - 114/22, Rn. 119.

[45] BT, Drucksache 20/9048, S. 150 in Bezug auf § 393 Abs. 2 SGB V.

[46] BT, Drucksache 18/12611, S. 115 in Bezug auf § 80 Abs. 2 SGB X.

[47] BT, Drucksache 20/9048, S. 150 in Bezug auf § 393 Abs. 2 SGB V.

[48] BT, Drucksache 18/12611, S. 115 in Bezug auf § 80 Abs. 2 SGB X.

[49] Zur Notwendigkeit einer weiten Auslegung wegen des Schutzzwecks siehe *Schröder*, in: Kühling/Buchner, DS-GVO BDSG, Art. 44 DSGVO Rn. 16.

[50] EuGH, Urt. v. 16.7.2020, C-311/18, ECLI:EU:C:2020:559 Rn. 91; vgl. auch ErwGr. 6 zur DSGVO.

in der EU gespeicherte Daten eine Datenübermittlung in Drittländer erfolgt.[51] Auch der LfDI Baden-Württemberg geht in einer neueren Handreichung davon aus, dass so ein tatsächlich erfolgender Zugriff, der über eine rein theoretische Zugriffsmöglichkeit hinausgeht, eine Datenübermittlung in Drittländer ist.[52] Bei einem Fernzugriff aus einem Drittland werden zwar ggf. keine Daten in dem Drittland gespeichert, sondern es wird nur vom Drittland heraus darauf zugegriffen. Allerdings scheint mit Blick auf den Schutzzweck der Vorgaben aus Kapitel V DSGVO und § 393 Abs. 2 SGB V eine solche Auslegung eher fernliegend, nach der diese Form des Zugriffs keine Übermittlung in ein Drittland sein würde.[53] Denn die Anwendbarkeit der Vorschriften aus Kapitel V DSGVO und § 393 Abs. 2 Nr. 3 SGB V könnte dann einfach dadurch umgangen werden, dass Daten nicht mehr in Drittländer gesendet werden, sondern nur noch aus einem Drittland heraus auf Daten zugegriffen wird.[54] Es ist jedoch nicht ersichtlich, warum ein solcher Zugriff aus einem Drittland heraus nicht mehr dem Schutz aus § 393 Abs. 2 SGB V und Kapitel V DSGVO unterliegen sollte.

Innerhalb der Frage wird auch angedeutet, dass ein Fernzugriff nicht zwangsläufig auch den Zugriff auf personenbezogene Daten erfordert, sondern ein solcher Zugriff nur nicht 100%ig ausgeschlossen werden kann. In § 80 Abs. 5 SGB X hat der deutsche Gesetzgeber für solche Fälle Ausnahmen für die Pflichten des § 80 Abs. 3 SGB X geregelt, wobei sich diese Pflichten von vornherein nicht auf Datenübermittlungen beziehen. In dem Kontext stellt sich die Frage, ob in den Fällen des § 80 Abs. 5 SGB X eventuell die Vorgaben aus § 393 Abs. 2 SGB V nicht gelten. In dem Zusammenhang ist es wichtig zu beachten, dass im Anwendungsbereich des § 80 SGB X aber auch in solchen Fällen weiterhin die Vorgaben für den Ort der Verarbeitung aus § 80 Abs. 2 SGB X gelten. Demzufolge erscheint es fernliegend – ohne eine entsprechend explizite Regelung in § 393 Abs. 2 SGB V – davon auszugehen, dass in Fällen des § 80 Abs. 5 SGB X quasi automatisch die Vorgaben aus § 393 Abs. 2 SGB V nicht gelten. Dennoch soll nicht unerwähnt bleiben, dass eine bloße Zugriffsmöglichkeit ohne tatsächlich erfolgenden Zugriff auf personenbezogene Daten – und damit ohne eine Verarbeitung i.S.v. Art. 4 Nr. 2 DSGVO, die für die Anwendbarkeit der Vorgaben der DSGVO aber immer vorliegen muss – noch keine Datenübermittlung in ein Drittland ist.[55] Erfolgt aber ein laut der Frage nicht 100%ig ausschließbarer Zugriff auf personenbezogene Daten auch tatsächlich, dann sind die Vorgaben aus § 393 Abs. 2 SGB V zu beachten.

Zusammenfassend ist die Frage also so zu beantworten, dass auch ein Fernzugriff auf personenbezogene Daten eine Übermittlung in ein Drittland wäre und somit nach Maßgabe von § 393 Abs. 2 DSGVO für ein solches Drittland ein Angemessenheitsbeschluss vorliegen müsste. In der Frage wird explizit auf die Nutzung von amerikanischen Hyperscalern eingegangen. Die Zusammenarbeit mit diesen Unternehmen ist im Einklang mit § 393 Abs. 2 SGB V dann möglich, wenn der Fernzugriff nicht aus den USA heraus, sondern aus einem Mitgliedstaat der EU oder einem Staat mit Angemessenheitsbeschluss heraus stattfindet oder nicht Sozial- oder Gesundheitsdaten betrifft.

Der deutsche Gesetzgeber hat zwar mit der Aufnahme des § 393 SGB V beabsichtigt, einen *„sicheren Einsatz dieser modernen, grundsätzlich weit verbreiteten Technik im Gesundheitswesen zu ermöglichen“*.[56] Allerdings würde dieses Ziel im Falle der Ungültigkeit eines Angemessenheitsbeschlusses für die USA schon bereits faktisch nicht mehr erfüllt werden können. Hyperscaler bieten die mit Abstand am

---

[51] EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Rn. 13, abrufbar unter folgender URL: https://www.edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf (letzter Abruf am 22.4.2024).

[52] LfDI Baden-Württemberg, Drittstaatentransfer unter der Datenschutz-Grundverordnung (DS-GVO), Eine Handreichung zu Kapitel V der DS-GVO, S. 5, abrufbar unter folgender URL: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/Drittstaatentransfer-_online.pdf (letzter Abruf am 22.4.2024).

[53] Im Ergebnis so auch *Strothmann/Ahrend*, in: Krahmer, Sozialdatenschutzrecht, § 80 SGB X Rn. 33.

[54] Zur Relevanz der Verhinderung von Umgehungsmechanismen siehe EuGH, Urt. v. 7.3.2024, C-740/22, ECLI:EU:C:2024:216 Rn. 31.

[55] So auch BKartA, Beschl. v. 13.2.2023 – VK 2 - 114/22, Rn. 119; ebenso wohl auch LfDI Baden-Württemberg, Drittstaatentransfer unter der Datenschutz-Grundverordnung (DS-GVO), Eine Handreichung zu Kapitel V der DS-GVO, S. 5.

[56] Siehe die Gesetzesbegründung zu § 393 SGB V unter BT, Drucksache 20/9048, S. 150.

weitesten verbreiteten Dienste an und sind aktuell darauf angewiesen, dass auch Datenübermittlungen in die USA legitimiert werden können. Das ist aber im Anwendungsbereich des § 393 SGB V nicht möglich, sobald es keinen Angemessenheitsbeschluss mehr gibt. In der Konsequenz ist in dem Fall dann auch die Nutzung der am weitesten verbreiteten Cloud-Computing-Dienste nicht mehr möglich. In der Literatur wurde im Kontext des § 80 Abs. 2 SGB X bereits darauf hingewiesen, welche weitreichenden Folgen sich daraus ergeben können, dass im SGB-Kontext Datenübermittlungen außerhalb der EU und des EWR mitunter nur erfolgen können, wenn ein Angemessenheitsbeschluss vorhanden ist.[57]

1.2.2. Antwort auf Fragen 3. 1) b) i) und ii)

Verarbeitungen innerhalb von Unternehmens-Gruppen basieren häufig auf verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules, BCRs). Im Rahmen von Cloud-Diensten werden mitunter auch Beschäftigte aus einem Drittland für einzelne Supportleistungen, insbesondere bei Fehlerbeseitigungen, eingesetzt werden müssen. Es ist fraglich, ob es richtig ist, dass BCRs nicht ausreichend sind, um eine Verarbeitung in einem Drittland zu ermöglichen, wenn gleichzeitig kein Angemessenheitsbeschluss für das Drittland existiert (Frage i)). Außerdem ist fraglich, ob eine Verarbeitung im Drittland nur dann möglich ist, wenn ein Angemessenheitsbeschluss für das betreffende Drittland existiert (Frage ii)). Unsere Rückfragen haben ergeben, dass die BCRs des Anbieters eines Cloud-Computing-Dienstes und dessen Mitarbeiter sowie die BCRs von Unterauftragsverarbeitern und deren Mitarbeiter gemeint sind.

In § 393 Abs. 2 SGB V wird nicht auf die Möglichkeit eingegangen, dass Datenübermittlungen in ein Drittland auf Basis von BCRs erfolgen können. Die Vorschrift kennt nur die Möglichkeit, dass für ein Drittland ein Angemessenheitsbeschluss vorhanden ist und deswegen eine Verarbeitung im Drittland entsprechend den Vorgaben aus § 393 Abs. 2 Nr. 3 SGB V möglich ist. Sobald eine Verarbeitung auch in einem Drittland ohne Angemessenheitsbeschluss erfolgen würde, wären die Voraussetzungen aus § 393 Abs. 2 SGB V nicht mehr erfüllt.[58] Wäre bspw. für „Drittland A“ ein Angemessenheitsbeschluss vorhanden aber für „Drittland B“ nicht und die Daten würden auf Basis von BCRs aus Land A nach Land B übertragen werden sollen, dann könnte die Übermittlung in Land B nicht im Einklang mit § 393 Abs. 2 Nr. 3 SGB V erfolgen. Im Kontext des § 393 SGB V sind Möglichkeiten für eine zulässige Datenübermittlung in Drittländer stark begrenzt.

Es stellt sich in dem Zusammenhang die Frage, ob der deutsche Gesetzgeber einschränkend regeln darf, dass Übermittlungen von Gesundheits- und Sozialdaten in Drittländer bei Nutzung von Cloud-Computing-Diensten nicht auch auf Basis von Art. 46 Abs. 2 lit. b DSGVO erfolgen dürfen, wenn der Anwendungsbereich des § 393 SGB V eröffnet ist. Schließlich wäre es auf Basis von Art. 46 Abs. 2 lit. c DSGVO für sich genommen grundsätzlich denkbar, dass eine Datenübermittlung in ein Drittland auch auf Basis von BCRs legitimiert werden kann. In der deutschen Kommentarliteratur besteht Einigkeit darüber, dass die Mitgliedstaaten auf Basis von Art. 49 Abs. 5 DSGVO die Zulässigkeit der Übermittlung bestimmter Datenkategorien in Drittländer beschränken können und dies auch die Befugnis zur Regelung der Unanwendbarkeit von BCRs umfasst.[59] Angesichts dessen scheint es naheliegend, dass der deutsche Gesetzgeber für die Datenkategorien „Gesundheits- und Sozialdaten“ im Kontext der Nutzung von Cloud-Computing-Diensten regeln darf, dass ein Angemessenheitsbeschluss vorhanden sein muss, wenn Übermittlungen von Gesundheits- oder Sozialdaten in Drittländer erfolgen sollen. Demzufolge ist auch

---

[57] Siehe etwa *Strothmann/Ahrend*, in: Krahmer, Sozialdatenschutzrecht, § 80 SGB X Rn. 33.

[58] Siehe in dem Zusammenhang auch BKartA, Beschl. v. 13.2.2023 – VK 2 - 114/22, Rn. 119; *Strothmann/Ahrend*, in: Krahmer, Sozialdatenschutzrecht, § 80 SGB X Rn. 33: *„Nicht möglich ist die Beauftragung eines Auftragsverarbeiters in einem Drittstaat, für den kein Angemessenheitsbeschluss vorliegt.“*; siehe auch zur Rechtslage vor dem Angemessenheitsbeschluss für die USA *Herbst*, in: Rolfs/Körner/Krasney/Mutschler, beck-online.GROSSKOMMENTAR, § 80 SGB X Rn. 56: *„Eine Datenübermittlung an die USA ist daher nur nach den Maßgaben des Abs. 3 möglich.“*

[59] Siehe etwa *Borges*, in: Borges/Hilber, BeckOK IT-Recht, Art. 49 DSGVO Rn. 35; *Zerdick*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 49 DSGVO Rn. 19; *Pauly*, in: Paal/Pauly, DS-GVO BDSG, Art. 49 DSGVO Rn. 34; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 49 DSGVO Rn. 60; *Gabel*, in: Taeger/Gabel, DSGVO - BDSG – TTDSG, Art. 49 DSGVO Rn. 30; *Klein/Pieper*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 49 DSGVO Rn. 31; *von dem Bussche/Raguse*, in: Plath, DSGVO/BDSG/TTDSG, Art. 49 DSGVO Rn. 40.

davon auszugehen, dass die bei Nutzung eines Cloud-Computing-Dienstes erfolgenden Datenübermittlungen in Drittländer nicht auf BCRs gestützt werden können.

Fernab dessen ist es aber möglich, dass bspw. Daten verarbeitet werden, die keine Gesundheits- und Sozialdaten sind, und hierbei auch eine Datenübermittlung in Drittländer erfolgt und diese Datenübermittlungen auf Basis von BCRs oder auch SCC gerechtfertigt werden können. In diesen Fällen findet dann aber der § 393 SGB V in Gänze keine Anwendung, soweit keine Verarbeitung von Gesundheits- und Sozialdaten im Wege eines Cloud-Computing-Dienstes erfolgt. Parallel sind aber ggf. die Vorgaben aus § 80 Abs. 2 SGB X zu beachten.

Die Fragen i) und ii) sind also so zu beantworten, dass BCRs Datenübermittlungen in Drittländer nicht im Anwendungsbereich des § 393 SGB V rechtfertigen können und für Datenverarbeitungen in Drittländer immer ein Angemessenheitsbeschluss vorhanden sein muss.

2. Fragen und Antworten zu Fragen unter 3. 2)

2.1. Die Fragen zu 3. 2)

Es wird in § 393 Abs. 2 SGB V nicht auf „internationale Organisation“ (Art. 4 Ziff. 26 DSGVO) oder „Hauptniederlassung“ (Art. 4 Ziff. 16 DSGVO) Bezug genommen.

> a) Sind die Begriffe „internationale Organisation“ und „Hauptniederlassung“ auch im Hinblick auf § 393 SGB V so anzuwenden, wie sie in der DSGVO stehen?
>
> b) Wenn nein, wie sind die Begriffe im Kontext des § 393 SGB V anzuwenden?
>
> c) Gelten die Vorgaben auch für Cloud-Dienstleistungen, die von internationalen Organisationen angeboten werden?

2.2. Die Antworten zu den Fragen unter 3. 2)

Im Folgenden werden die Antworten zu den Fragen a) bis c) getrennt erteilt. Zusammengefasst lauten die Antworten auf folgende Fragen wie folgt:

- *a)*: Im Grundsatz, ja. Der Begriff „Hauptniederlassung“ spielt allerdings im Kontext des § 393 SGB V keine große Rolle. Der Niederlassungsbegriff aus der DSGVO sollte bei § 393 SGB V aber genauso angewendet werden. Der Begriff „internationale Organisation“ wird nicht in § 393 SGB V erwähnt, kann aber im Kontext des § 393 Abs. 2 SGB V relevant sein, insbesondere wenn es für eine internationale Organisation einen Angemessenheitsbeschluss gibt.
- *b)*: Da die Frage a) mit „ja“ beantwortet wurde, erübrigt sich die Frage b).
- *c)*: Die Vorgaben aus § 393 Abs. 2 SGB V gelten auch, wenn eine Datenübermittlung an eine internationale Organisation erfolgt. Im Falle eines Angemessenheitsbeschlusses für eine internationale Organisation kann der deutsche Gesetzgeber aber nicht die Möglichkeit ausschließen, die Datenübermittlungen auf Basis eines Angemessenheitsbeschlusses vorzunehmen. In dem Fall sind die Vorgaben aus § 393 Abs. 2 Nr. 3 SGB V erfüllt. Bei einem fehlenden Angemessenheitsbeschluss für eine internationale Organisation sind die Vorgaben aus § 393 Abs. 2 Nr. 3 SGB V hingegen nicht erfüllt.

2.2.1. Antwort auf Frage a)

Es ist fraglich, ob die Begriffe „internationale Organisation“ und „Hauptniederlassung“ auch im Hinblick auf § 393 SGB V so anzuwenden sind, wie sie in der DSGVO stehen. In § 393 Abs. 2 Nr. 3 SGB V wird nicht der Begriff „Hauptniederlassung“, sondern nur der Begriff „Niederlassung“ verwendet. Hinsichtlich möglicher Angemessenheitsbeschlüsse verweist § 393 Abs. 2 Nr. 3 SGB V nur auf „in einem Drittstaat“ und nicht auf eine internationale Organisation.

Mit Blick auf den Begriff „Niederlassung“ ist zu erwähnen, dass die DSGVO sowohl eine „Niederlassung“[60] als auch eine „Hauptniederlassung“[61] kennt. Die beiden Begriffe werden in der DSGVO

[60] Vgl. etwa Art. 3 Abs. 1 DSGVO.
[61] Vgl. etwa Art. 4 Nr. 16 DSGVO.

nicht synonym verwendet.[62] Vielmehr ergibt sich u.a. aus der Definition in Art. 4 Nr. 16 DSGVO, dass es möglich ist, dass ein Unternehmen mehrere Niederlassungen hat, aber es stets nur eine Hauptniederlassung gibt. Weil § 393 Abs. 2 Nr. 3 SGB V nur den Begriff „Niederlassung" und nicht „Hauptniederlassung" verwendet, ist eine 1zu1 Anwendbarkeit der Begriffsdefinition für Hauptniederlassung im Kontext des § 393 Abs. 2 Nr. 3 SGB V fernliegend. Es ist aber stimmig, den Begriff „Niederlassung" in § 393 Abs. 2 Nr. 3 SGB V entsprechend seiner Bedeutung in der DSGVO auszulegen. Dies ist bereits deswegen erforderlich, weil die Beschränkung aus § 393 Abs. 2 SGB V auf Art. 49 Abs. 5 DSGVO basiert. „Niederlassung" ist in § 393 SGB V also genauso zu verstehen, wie auch unter der DSGVO.

Der Begriff „internationale Organisation" wird – anders als bspw. in § 80 Abs. 2 SGB X – nicht erwähnt. In § 393 Abs. 2 Nr. 3 SGB V wird die folgende Formulierung verwendet: „*sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat*." Demzufolge wird also nur auf einen Drittstaat und nicht auf eine internationale Organisation abgestellt, für die es aber eigentlich ebenfalls einen Angemessenheitsbeschluss geben kann. Fernab dessen gibt es keine Anzeichen für Gründe, die für eine abweichende Anwendung des Begriffs „internationale Organisation" im Kontext des § 393 SGB V sprechen.

Wie bereits in diesem Gutachten mehrfach erwähnt, basiert die Beschränkung für zulässige Datenübermittlungen von Gesundheits- und Sozialdaten in Drittländer auf der Öffnungsklausel des Art. 49 Abs. 5 DSGVO. Gemäß dem eindeutigen Wortlaut dieser Vorschrift dürfen die Mitgliedstaaten jedoch nur dann Beschränkungen vorsehen, wenn kein Angemessenheitsbeschluss vorliegt.[63] In der deutschen Kommentarliteratur herrscht Einigkeit darüber, dass ein nationaler Gesetzgeber nicht auf Basis von Art. 49 Abs. 5 DSGVO Beschränkungen vorsehen darf, wenn die Kommission einen Angemessenheitsbeschluss getroffen hat.[64] Dabei sollte unerheblich sein, ob so ein Angemessenheitsbeschluss für ein Land oder eine internationale Organisation erlassen wurde, weil dem Angemessenheitsbeschluss jeweils dieselbe Bedeutung zukommt.

Wenn es für eine internationale Organisation einen Angemessenheitsbeschluss gibt, dann sind die Vorgaben aus § 393 Abs. 2 Nr. 3 SGB V erfüllt. Der deutsche Gesetzgeber kann einen Angemessenheitsbeschluss für eine internationale Organisation nicht dadurch aushebeln, dass in § 393 Abs. 2 Nr. 3 SGB V immer für ein „Drittland" ein Angemessenheitsbeschluss verlangt wird und internationale Organisationen nicht erwähnt werden. Angemessenheitsbeschlüsse für internationale Organisationen müssen gleichwertig mit Angemessenheitsbeschlüssen für Drittländer sein. Denn im Falle eines Angemessenheitsbeschlusses kann der deutsche Gesetzgeber nicht regeln, dass eine Datenübermittlung an eine als von der Kommission angemessen befundene internationale Organisation nicht legitim ist. Hierfür hat der deutsche Gesetzgeber aus Art. 49 Abs. 5 DSGVO heraus keine Kompetenz. Er kann nur verlangen, dass es einen Angemessenheitsbeschluss geben muss und so indirekt die Anwendbarkeit der anderen Erlaubnistatbestände für Datenübermittlungen ausschließen.

Wenn für eine internationale Organisation allerdings kein Angemessenheitsbeschluss vorhanden ist, dann sind Datenübermittlungen an so eine im Drittland ansässige Organisation nicht im Einklang mit den Vorgaben aus § 393 Abs. 2 Nr. 3 SGB V möglich. Diese Vorschrift verlangt schließlich für jegliche Drittlandsübermittlungen, dass ein Angemessenheitsbeschluss vorhanden ist. Der Umstand, dass in § 393 Abs. 2 SGB V nicht auf eine internationale Organisation verwiesen wird, spricht nicht dafür, dass Übermittlungen an internationale Organisationen in Drittländer auch auf Basis von anderen Erlaubnistatbeständen aus Kapitel V DSGVO möglich sind. Weil § 393 Abs. 2 SGB V regelt, dass eine Datenverarbeitung „nur" unter Einhaltung der in der Vorschrift geregelten Voraussetzungen möglich ist,

---

[62] Siehe exemplarisch *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 3 DSGVO Rn. 21: „*Eine Definition der Niederlassung fehlt und kann auch Art. 4 Nr. 16 nicht entnommen werden*".

[63] „*Liegt kein Angemessenheitsbeschluss vor (…)*".

[64] Siehe etwa *Gabel*, in: Taeger/Gabel, DSGVO - BDSG – TTDSG, Art. 49 DSGVO Rn. 30: „*Eine Beschränkung ist überdies nicht möglich für Übermittlungen in Länder oder an internationale Organisationen, für die ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt*."; siehe auch *Zerdick*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 49 DSGVO Rn. 19; *Pauly*, in: Paal/Pauly, DS-GVO BDSG, Art. 49 DSGVO Rn. 34; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 49 DSGVO Rn. 60.

kann von der fehlenden Erwähnung internationaler Organisationen nicht darauf geschlossen werden, dass die Vorgaben des § 393 Abs. 2 SGB V ganz allgemein nicht für Übermittlungen an internationale Organisationen gelten.

2.2.2. Antwort auf Frage b)

Die Frage b) wäre nur zu beantworten, wenn die Antwort auf Frage a) „nein" gelautet hätte. Da dies nicht der Fall ist, wird die Frage b) nicht beantwortet.

2.2.3. Antwort auf Frage c)

Es ist fraglich, ob die Vorgaben auch für Cloud-Dienstleistungen gelten, die von internationalen Organisationen angeboten werden.

Wie den Ausführungen bei den Antworten zu Frage a) zu entnehmen ist, gilt § 393 Abs. 2 SGB V grundsätzlich auch dann, wenn eine Datenübermittlung an eine internationale Organisation erfolgt. Wenn allerdings für die internationale Organisation ein Angemessenheitsbeschluss vorhanden ist, dann sind die Vorgaben aus § 393 Abs. 2 Nr. 3 SGB V aber erfüllt. Das folgt daraus, dass der deutsche Gesetzgeber nur dann die Zulässigkeit von Datenübermittlungen nach Art. 49 Abs. 5 DSGVO beschränken kann, wenn kein Angemessenheitsbeschluss vorhanden ist. Wenn jedoch für eine internationale Organisation kein Angemessenheitsbeschluss erlassen wurde, dann können die Vorgaben aus § 393 Abs. 2 Nr. 3 SGB V nicht erfüllt werden.

IV. Fragen zum C5-Testat des BSI

Die im Folgenden Abschnitt beantworteten Fragen betreffen das C5-Testat des BSI.

1. Fragen unter 4.)

1) Ist es richtig, dass durch die „und"-Verknüpfung § 393 Abs. 3 SGB V alle in den Nr. 1 bis 3 gestellten Anforderungen gemeinsam erfüllt werden müssen?

2) § 393 Abs. 3 Nr. 2 SGB V verlangt ein „ein aktuelles C5-Testat der datenverarbeitenden Stelle".

> a) Im Datenschutzrecht ist die „datenverarbeitende Stelle" der Verantwortliche, der Cloud-Dienstleistung erbringende Anbieter/Dienstleister wäre als Auftragsverarbeiter hingegen keine datenverarbeitende Stelle. Ist es richtig, dass Leistungserbringer oder Krankenkassen als datenverarbeitende Stelle mit der Pflicht zur Erbringung eines C5-Testates anzusehen sind?
>
> b) Trifft die Pflicht, ein C5-Zertifikat für den eingesetzten Cloud-Computing-Dienst vorweisen zu können, die datenverarbeitende Stelle, muss dann ein BSI C5-Testat für jeden einzelnen Cloud-Computing-Dienst vorliegen? Oder kann für mehrere verschiedene Cloud-Computing-Dienste ein einziges BSI-C5 Testat den gesetzlichen Anforderungen genügen?
>
> c) Muss sowohl die datenverarbeitende Stelle als auch der Cloud-Computing-Dienst nach BSI C5 testiert worden sein?

2. Antworten zu den Fragen unter 4.)

Im Folgenden werden die Antworten zu den Fragen a) und c) getrennt erteilt. Zusammengefasst lauten die Antworten auf folgende Fragen wie folgt:

- *1*: Ja, alle der Voraussetzungen aus den drei Ziffern des § 393 Abs. 3 SGB V müssen zusammen erfüllt werden, weil Nr. 2 und Nr. 3 mit einem „Und" verknüpft sind und Nr. 1 entsprechend der Gesetzesbegründung auch immer erfüllt sein muss und es keine Anhaltspunkte für eine Intention zur Regulierung von alternativen Optionen gibt.
- *2 a)*: Der Begriff „datenverarbeitende" Stelle war früher gebräuchlich, wird heute aber in Datenschutzgesetzen nicht mehr wirklich verwendet. Es ist nicht vollkommen klar, ob der Gesetzgeber nur Leistungserbringer und Kranken- und Pflegekassen als datenverarbeitende Stelle ansieht oder auch deren Auftragsverarbeiter. Die besseren Argumente sprechen aber dafür, dass die datenverarbeitende Stelle nur den Verantwortlichen meint. Darum sollten Leistungserbringer und Kranken- und Pflegekassen das Vorliegen eines BSI-C5-Testats nachweisen können.

- *2 b)*: Das hängt von dem Umfang des Testats ab. Wenn es für mehrere Dienste gilt, dann kann auch der Nachweis für mehrere Dienste durch so ein einzelnes Testat erbracht werden. Wenn es aber nur für einen von mehreren Diensten gilt, dann muss für die übrigen Dienste auch der Nachweis des Vorliegens eines Testats durch andere Testate erbracht werden.
- *2 c)*: Nein, nur der Cloud-Computing-Dienst muss nach BSI-C5 testiert worden sein und die datenverarbeitende Stelle muss die Vorgaben aus § 393 Abs. 3 Nr. 3 SGB V selbst erfüllen, ohne dabei testiert zu werden. Es ist nach dem Willen des deutschen Gesetzgebers aber auch möglich, dass sich eine Einrichtung den konkreten Einsatz bei ihr nach BSI-C5 testieren lässt, wenn bspw. der Hersteller des Dienstes noch kein Testat vorlegen kann.

2.1. Antwort auf Frage 1)

Es ist fraglich, ob durch die „Und"-Verknüpfung in § 393 Abs. 3 SGB V alle in den Nr. 1 bis 3 gestellten Anforderungen gemeinsam erfüllt werden müssen.

Es ist nicht ersichtlich, dass der deutsche Gesetzgeber die Anforderungen in § 393 Abs. 3 Nr. 1 bis 3 SGB V alternativ und nicht kumulativ regeln wollte. Wie schon in der Frage erwähnt, ist die „Und"-Verknüpfung ein starkes Indiz dafür, dass zumindest die Anforderungen aus Nr. 2 und Nr. 3 gemeinsam erfüllt sein müssen. Dass nach Nr. 1 ein Komma gesetzt wurde und kein „oder" o.ä. steht, spricht ebenfalls dafür, dass die Voraussetzungen aller drei Ziffern zu erfüllen sind. Auch die Gesetzesbegründung zu § 393 Abs. 3 Nr. 1 SGB V spricht dafür, dass die Voraussetzungen aus allen drei Ziffern gemeinsam zu erfüllen sind. Dort hat der Gesetzgeber nämlich betont, dass „*die Datenverarbeitung […]* ***nur zulässig [ist],*** *soweit nach dem Stand der Technik angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit ergriffen worden sind*."[65] Weil Nr. 2 und Nr. 3 mit einem „und" verknüpft sind und Nr. 1 entsprechend der Formulierung in der Gesetzesbegründung auch immer erfüllt sein muss und es keine Anhaltspunkte für eine Intention zur Regulierung von alternativen Optionen gibt, müssen alle drei Voraussetzgen zusammen erfüllt sein.

2.2. Antwort auf Frage 2 a)

§ 393 Abs. 3 Nr. 2 SGB V verlangt ein „aktuelles C5-Testat der datenverarbeitenden Stelle". Im Datenschutzrecht ist die „datenverarbeitende Stelle" der Verantwortliche, der Cloud-Dienstleistung erbringende Anbieter/Dienstleister wäre als Auftragsverarbeiter hingegen keine datenverarbeitende Stelle. Es ist fraglich, ob es richtig ist, dass Leistungserbringer oder Krankenkassen als datenverarbeitende Stellen mit der Pflicht zur Erbringung eines C5-Testates anzusehen sind.

§ 393 Abs. 3 Nr. 2 SGB V verlangt, dass „*ein aktuelles C5-Testat der datenverarbeitenden Stelle im Hinblick auf die C5-Basiskriterien für die im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die eingesetzte Technik vorliegt*". Das C5-Testat muss für die „*im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die eingesetzte Technik*" gelten. Demzufolge wird nicht eine datenverarbeitende Stelle mit Blick auf die BSI-Kriterien zertifiziert, sondern die Cloud-Systeme und die eingesetzte Technik. Das deckt sich auch mit der Aussage in der Gesetzesbegründung, nach der „*über Nummer 2 […] im Weiteren eine unabhängige Prüfung und Testierung der eingesetzten* ***Cloud-Systeme*** *(Komponenten, Prozesse) und* ***Cloud-Technik*** *nach dem C5-Standard des BSI (…) vorausgesetzt [wird]*.[66] Es wird demzufolge nicht eine datenverarbeitende Stelle zertifiziert, die einen Cloud-Dienst nutzt, sondern die Cloud-Systeme und -Technik werden zertifiziert. Auch die Gesetzesbegründung zu § 393 Abs. 3 Nr. 3 SGB V verwendet die Formulierung „*testierten Systeme*",[67] was für eine Zertifizierung des Dienstes an sich spricht. Auch der Prüfbericht des Testats i.S.v. § 393 Abs. 3 Nr. 3 SGB V, wird für den Cloud-Computing-Dienst an sich und nicht für den einzelnen Kunden erstellt.

Den BSI-Kriterien ist zu entnehmen, dass diese vor allem für den Anbieter des Cloud-Computing-Dienstes gelten. Die Kriterien dienen ebenfalls dazu, um Cloud-Kunden gegenüber aufzuzeigen, an welchen Stellen Cloud-Kunden eigene Maßnahmen entwickeln müssen, um die Sicherheit des Cloud-

[65] BT, Drucksache 20/9048, S. 150 in Bezug auf § 393 Abs. 3 Nr. 1 SGB V.
[66] BT, Drucksache 20/9048, S. 150 in Bezug auf § 393 Abs. 3 Nr. 2 SGB V.
[67] BT, Drucksache 20/9048, S. 150 in Bezug auf § 393 Abs. 3 Nr. 3 SGB V.

Dienstes zu gewährleisten.[68] Genau diese an den Kunden gerichteten Maßnahmen werden in § 393 Abs. 3 Nr. 3 SGB V reguliert. Gemäß dieser Vorschrift, „*müssen die im Prüfbericht des Testats enthaltenen, korrespondierenden Kriterien für Kunden umgesetzt*“ sein. Während also § 393 Abs. 3 Nr. 2 SGB V eine Zertifizierung des Dienstes für sich verlangt, ist § 393 Abs. 3 Nr. 3 SGB V unmittelbar an den Kunden des Cloud-Anbieters adressiert. Unabhängig von der Frage, wer oder was in dem BSI-C5-Testat zertifiziert wird, stellt sich aber noch die Frage, wer die Zertifizierung nachweisen können muss.

Weil § 393 Abs. 3 Nr. 2 SGB V hier auf die datenverarbeitende Stelle abstellt, muss das BSI-C5-Testat zwar für den Cloud-Computing-Dienst vorliegen, aber die datenverarbeitende Stelle muss in der Lage sein nachzuweisen, dass es für den Dienst auch ein BSI-C5-Testat gibt. In dem Kontext ist fraglich, wer als „datenverarbeitende Stelle“ i.S.v. § 393 Abs. 3 Nr. 2 SGB V anzusehen ist. Dieser Begriff wird nicht im SGB V definiert und soweit ersichtlich auch nicht an anderer Stelle im selben Gesetz außer in § 393 Abs. 2 Nr. 3 SGB V verwendet. Gemäß § 393 Abs. 2 Nr. 3 SGB V ist es erforderlich, dass die datenverarbeitende Stelle eine Niederlassung im Inland hat. Dem Begriff „datenverarbeitende Stelle“ sollte in § 393 Abs. 2 Nr. 3 SGB V einerseits und in § 393 Abs. 3 Nr. 2 SGB V andererseits dieselbe Bedeutung zukommen. Die datenverarbeitende Stelle muss dann also das Vorliegen des BSI-C5-Testats nachweisen können und auch über eine Niederlassung im Inland verfügen.

Zur Klärung der Bedeutung des Begriffs „datenverarbeitende Stelle“ ist anzumerken, dass im Datenschutzrecht die „verantwortliche Stelle“ den Verantwortlichen meint, aber der Begriff „datenverarbeitende Stelle“ im Datenschutzrecht mittlerweile eher ungebräuchlich ist. Eine „datenverarbeitende Stelle“ verlangt dem Wortlaut nach nämlich nur eine Stelle, die Datenverarbeitungen vornimmt, ohne dabei auf einen Verantwortlichen oder Auftragsverarbeiter abzustellen. Allerdings wurde der Begriff früher in mittlerweile nicht mehr gültigen Datenschutzgesetzen der Bundesländer verwendet. Das hessische Datenschutzgesetz sah in seiner Fassung vom 20.5.2011 vor, dass die datenverarbeitende Stelle der Verantwortliche ist.[69] Genauso war es u.a. auch im Berliner Datenschutzgesetz in alter Fassung[70] und in den Gesetzen von Brandenburg[71] und Hamburg[72] geregelt. Während also vor Geltung der DSGVO der Begriff noch gebräuchlich war, so wird er aktuell aber nicht mehr verwendet. Es ist jedoch gut denkbar, dass der Autor des § 393 SGB V bei der Wortwahl „datenverarbeitende Stelle“ an das alte Begriffsverständnis anknüpfen wollte.

Im Referentenentwurf zu der § 393 SGB V entsprechenden Regelung war zuvor noch die folgende Formulierung vorgesehen: „*die **beauftragte, datenverarbeitende Stelle** über eine Niederlassung im Inland verfügt*“.[73] Bspw. der bitkom hatte im Rahmen seiner Stellungnahme zum Entwurf angemerkt, dass es

---

[68] Siehe hierzu die Aussage zu den Neuerungen, die aus der Überarbeitung des BSI-Standards resultieren: „*Aufnahme korrespondierender Kriterien für Cloud-Kunden, diese dienen dazu, aufzuzeigen, an welchen Stellen Cloud-Kunden eigene Maßnahmen entwickeln müssen, um die Sicherheit des Cloud-Dienstes zu gewährleisten*“, BSI, Cloud Computing Compliance Criteria Catalogue – C5:2020, S. 13, abrufbar unter folgender URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/C5_2020.pdf?__blob=publicationFile&v=3 (letzter Abruf am 22.4.2024).

[69] Vgl. § 2 Abs. 3 des alten hessischen Datenschutzgesetzes („*Daten verarbeitende Stelle ist jede der in § 3 Abs. 1 genannten Stellen, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.*“), dessen Fassung unter folgender URL abrufbar ist: https://www.uni-giessen.de/de/fbz/fb06/psychologie/ethikkommission/downloads-intern/hessdatenschutzgesetz (letzter Abruf am 24.4.2024).

[70] § 4 Abs. 3 Nr. 1 des alten Berliner Datenschutzgesetzes („*datenverarbeitende Stelle jede Behörde oder sonstige öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt; nimmt diese unterschiedliche gesetzliche Aufgaben wahr, gilt diejenige Organisationseinheit als datenverarbeitende Stelle, der die Aufgabe zugewiesen ist*“), dessen Fassung unter folgender URL abrufbar ist: https://gesetze.berlin.de/bsbe/document/jlr-DSGBEV10P4 (letzter Abruf am 24.4.2024).

[71] § 3 Abs. 4 Nr. 1 des alten Brandenburgischen Datenschutzgesetzes („*datenverarbeitende Stelle jede öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten läßt*“), dessen Fassung unter folgender URL abrufbar ist: https://bravors.brandenburg.de/de/gesetze-213765#3 (letzter Abruf am 24.4.2024).

[72] § 4 Abs. 3 des alten Hamburgischen Datenschutzgesetzes („*Daten verarbeitende Stelle ist jede der in § 2 Absatz 1 Satz 1 genannten Stellen, die allein oder gemeinsam mit anderen Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt*“), dessen Fassung unter folgender URL abrufbar ist: https://www.umwelt-online.de/recht/allgemei/laender/hh/dsg01.htm (letzter Abruf am 24.4.2024).

[73] Referentenentwurf des Bundesministeriums für Gesundheit vom 13.7.2023, S. 56, abrufbar unter folgender URL: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/D/DigiG_RefE.pdf (letzter Abruf am 22.4.2024).

klärungsbedürftig sei, wer die datenverarbeitende Stelle ist.[74] In der endgültigen Fassung wird nur noch auf die datenverarbeitende Stelle abgestellt und „beauftragte" nicht mehr erwähnt. Der Entwurf der Bundesregierung verweist schon sowohl in Bezug auf § 393 Abs. 2 Nr. 2 SGB V als auch mit Blick auf den Abs. 3 Nr. 2 der Vorschrift nur auf „die datenverarbeitende Stelle". Hieraus kann man ableiten, dass der Gesetzgeber nicht mehr explizit auf den Hersteller des Dienstes / den Auftragsverarbeiter verweisen möchte. Es wäre dann einerseits denkbar, dass deswegen mit der „datenverarbeitenden Stelle" nur Leistungserbringer und Kranken- und Pflegekassen und nicht die beauftragten Stellen gemeint sind. Andererseits könnte man daraus auch ableiten, dass sowohl Leistungserbringer / Kranken- und Pflegekassen als auch deren Auftragsverarbeiter von dem Begriff erfasst sein sollen.

Weil der § 393 SGB V ausweislich seines Abs. 1 sowohl Leistungserbringer / Kranken- und Pflegekassen als auch deren Auftragsverarbeiter adressiert, könnte man hieraus potenziell schlussfolgern, dass alle diese Stellen auch datenverarbeitende Stellen sind. Schließlich gilt die Erlaubnisnorm sowohl für als Verantwortlicher agierende Leistungserbringer / Kranken- und Pflegekassen als auch für deren Auftragsverarbeiter. Weil allen diesen Einrichtungen auf Basis von § 393 SGB V die Verarbeitung von Gesundheits- und Sozialdaten ermöglicht wird, könnten auch alle diese Einrichtungen als datenverarbeitende Stelle anzusehen sein. Dem Wortlaut nach schein eine datenverarbeitende Stelle schließlich eine Stelle zu sein, die Datenverarbeitungen im Anwendungsbereich des § 393 SGB V vornimmt. Wie erwähnt, ist es aber auch gut denkbar, dass eigentlich das alte Begriffsverständnis auch im Kontext des neuen SGB V gelten soll und deswegen nur der Verantwortliche (Leistungserbringer, Kranken- und Pflegekassen) die datenverarbeitende Stelle ist.

In § 393 SGB V wird der Begriff „datenverarbeitende Stelle" immer in der Einzahl verwendet. Hätte der deutsche Gesetzgeber zum Ausdruck bringen wollen, dass sowohl die Auftragsverarbeiter als auch Verantwortlichen zu den datenverarbeitenden Stellen zählen, so hätte eine Verwendung des Begriffs in der Mehrzahl nahegelegen. Die Verwendung der Formulierung in der Einzahl ist zumindest ein Indiz dafür, dass der Gesetzgeber mit einer datenverarbeitenden Stelle wohl eher nur den Leistungserbringer oder die Kranken- oder Pflegekasse meint.

Würde auch ein Auftragsverarbeiter eine datenverarbeitende Stelle sein, dann hätte dies jedoch zur Folge, dass Anbieter von Cloud-Computing-Diensten auch immer einen Sitz in Deutschland haben müssten und nicht nur die Datenverarbeitungen im Inland, einem Mitgliedstaat der EU oder des EWR oder in einem Land mit Angemessenheitsbeschluss erfolgen müssten. Wäre die datenverarbeitende Stelle hingegen nur der Leistungserbringer oder die Kranken- oder Pflegekasse, dann müsste nur der diese Einrichtungen ihren Sitz im Inland haben. In dem Zusammenhang hatten u.a. der bvitg[75] und die Deutsche Krankenhausgesellschaft[76] im Rahmen ihrer Stellungnahmen zum Referentenentwurf angemerkt, dass bei einer Forderung nach einer Inlandsniederlassung des Cloud-Anbieters der Kreis der einsetzbaren Dienste verkleinert werden würde. Versteht man die Streichung von „beauftragte" als Reaktion auf die Hinweise in den Stellungnahmen, dann läge es nahe, dass die datenverarbeitende Stelle gerade nicht der Auftragsverarbeiter in Form des Herstellers des Cloud-Dienstes ist, sondern nur Leistungserbringer und Kranken- und Pflegekassen meinen kann.

Die vorstehenden Untersuchungen haben gezeigt, dass nicht eindeutig klar ist, wer genau die datenverarbeitende Stelle i.S.v. § 393 SGB V ist. Die besseren Argumente sprechen aber dafür, dass hiermit Leistungserbringer und Kranken- und Pflegekassen gemeint sind. Es wurde zumindest deutlich, dass Leistungserbringer und Kranken- und Pflegekassen mindestens vom Begriff mit gemeint zu sein

---

[74] Stellungnahme des bitkom, S. 30, abrufbar unter folgender URL: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_bitkom.pdf (letzter Abruf am 22.4.2024).

[75] Stellungnahme des bvitg, S. 32 und 33, abrufbar unter folgender URL: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_bvitg.pdf (letzter Abruf am 24.4.2024).

[76] Stellungnahme der Deutsche Krankenhausgesellschaft, S. 26, abrufbar unter folgender URL: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/Stellungnahmen_WP20/DigiG/stellungnahme_dkg.pdf (letzter Abruf am 24.4.2024).

scheinen. Daher ist es aus Sicht der Leistungserbringer und Kranken- und Pflegekassen notwendig, das Vorliegen eines BSI-C5-Testats auch nachweisen zu können.

2.3. Antwort auf Frage b)

Es ist fraglich, ob datenverarbeitende Stellen ein BSI-C5-Testat für jeden einzelnen Cloud-Computing-Dienst nachweisen müssen oder für mehrere verschiedene Cloud-Computing-Dienste ein einziges BSI-C5-Testat den gesetzlichen Anforderungen genügen kann. Wie bereits in der Antwort auf Frage a) dargelegt, wird das C5-Testat für den Cloud-Dienst erteilt, aber die datenverarbeitende Stelle muss das Vorliegen eines Testats für die Dienste nachweisen können. Demzufolge gilt ein C5-Testat in der Regel für bestimmte Cloud-Dienste und nicht für bestimmte datenverarbeitende Stellen.

Wenn ein Testat an sich für mehrere Dienste gilt, dann steht einem Nachweis mit einem einzelnen Zertifikat für mehrere Dienste nichts entgegen. Wenn aber das C5-Testat nur für einen von vielen von der datenverarbeitenden Stelle eingesetzten Dienst gilt, dann benötigt die datenverarbeitende Stelle für andere Dienste andere Testate.

2.4. Antwort auf Frage c)

Es ist fraglich, ob sowohl die datenverarbeitende Stelle als auch der Cloud-Computing-Dienst nach BSI-C5 testiert worden sein muss.

Wie den Antworten zu Frage a) zu entnehmen ist, wird das Testat für einen Dienst erstellt. Den Kunden des Cloud-Anbieters trifft aber die Pflicht aus § 393 Abs. 3 Nr. 3 SGB V. Hiernach muss der Kunde die im Testat angegebenen Konfigurationen etc. auch bei sich umsetzen. Der Kunde selbst muss aber nicht nach dem BSI-Standard testiert werden.

Es scheint nach Ansicht des deutschen Gesetzgebers aber möglich zu sein, dass ein Anbieter eines Cloud-Computing-Dienstes nicht über ein BSI-C5-Testat verfügt und die den Dienst einsetzende Einrichtung sich selbst den Einsatz bei Ihr nach BSI-C5 testieren lässt. Dies wird an folgender Passage aus der Gesetzesbegründung erkennbar: „*Im Rahmen des § 393 SGB V können für Unternehmen, die cloudbasierte informationstechnische Anwendungen einsetzen wollen, initial geringfügige Mehrkosten im unteren fünfstelligen Bereich für die Durchführung einer C5-Testierung entstehen, sofern der* ***konkrete Anbieter des Clouddienstes nicht bereits über ein C5-Testat verfügt***.“[77]

V. Fragen zu Auswirkungen europäischer Zertifizierungsvorgaben

Die im Folgenden Abschnitt beantworteten Fragen betreffen die Auswirkungen europäischer Zertifizierungsvorgaben.

1. Fragen unter 5.)

ENISA arbeitet seit 2020 an einer Cloud-Zertifizierung, die Vorgaben werden voraussichtlich 2024 veröffentlicht. Nach Art 57 Verordnung (EU) 2019/881 „*werden nationale Schemata für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und -Prozesse, die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, ab dem Zeit-punkt unwirksam, der in dem nach Artikel 49 Absatz 7 erlassenen Durchführungsrechtsakt festgelegt ist*“.

> a) Fällt BSI C5 unter die Definition „nationales Schema für die Cybersicherheitszertifizierung“ gemäß Art. 2 Ziff. 10 Verordnung (EU) 2019/881?
>
> b) Ist es richtig, dass mit einem im Amtsblatt der EU veröffentlichtem Cloud-Schema entsprechend europäischen Recht, u.a. durch Art. 57 Abs. 1 Verordnung (EU) 2019/881, das BSI C5 unwirksam wird?
>
> c) Wenn das BSI-Schema unwirksam wird, ist es dann richtig, dass aufgrund der in § 393 SGB V verankerten nationalen Pflicht an Stelle des BSI C5-Testates eine Zertifizierung nach ENISA-Vorgaben erforderlich sein wird?

[77] BT, Drucksache 20/9048, S. 88.

2. Antworten zu den Fragen unter 5.)

Im Folgenden werden die Antworten zu den Fragen a) und c) getrennt erteilt. Zusammengefasst lauten die Antworten auf folgende Fragen wie folgt:

- *a)*: Ja, das BSI-C5-Testat ist ein „nationales Schema für die Cybersicherheitszertifizierung" gemäß Art. 2 Nr. 10 Verordnung (EU) 2019/881.
- *b)*: Ja, es ist richtig, dass das BSI-C5-Testat in Zukunft einmal unwirksam wird. Gleichzeitig bedeutet dies noch nicht automatisch, dass das Testat im Rahmen des § 393 SGB V dann auch keine Rolle mehr spielt.
- *c)*: Nein, es wird nicht zwangsläufig eine Zertifizierung nach ENISA-Vorgaben notwendig sein, sondern ebenso ein C5-Testat ausreichen. Etwas anderes gilt nur bei einer – aus unserer Sicht unwahrscheinlichen – Anpassung des § 393 SGB V. Weitere Zertifizierungen nach anderen Vorgaben werden aber künftig ebenso neben dem C5-Testat akzeptiert.

2.1. Antwort auf Frage a)

Es ist fraglich, ob das BSI-C5-Testat ein „nationales Schema für die Cybersicherheitszertifizierung" gemäß Art. 2 Nr. 10 Verordnung (EU) 2019/881 („CSA") ist. Gemäß Art. 2 Nr. 10 CSA sind nationale Schema für Cybersicherheitszertifizierung wie folgt definiert: „*ein von einer nationalen Behörde ausgearbeitetes und erlassenes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die für die Zertifizierung oder Konformitätsbewertung von IKT-Produkten, -Diensten und -Prozessen gelten, die von diesem Schema erfasst werden*." Das BSI-C5-Testat wäre demzufolge dann ein nationales Schema für Cybersicherheitszertifizierung in diesem Sinne, wenn das Testat ein von einer nationalen Behörde ausgearbeitetes und erlassenes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren sein würde, die für die Zertifizierung oder Konformitätsbewertung von IKT-Produkten, -Diensten und -Prozessen gelten.

Der BSI Cloud Computing Compliance Criteria Catalogue ist ein Kriterienkatalog des Bundesamts für Informationssicherheit, der die Mindestanforderungen an die Informationssicherheit für Cloud-Dienste festlegt.[78] An dem notwendigen Erlass durch eine Behörde gibt es somit keine Zweifel. Des Weiteren enthält das BSI-C5 ein umfassendes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren. Die aktuelle Version (Katalog C5:2020) besteht aus 125 Kriterien, die in 17 Themengebiete untergliedert sind.[79] Die Inhalte aus dem C5-Kriterienkatalog wurden zudem in den Entwurf des Europäischen Zertifizierungsschemas übernommen.[80] In ihrem Entwurf für ein Europäisches Zertifizierungssystem für Cloud-Dienste („EUCS") benennt die ENISA das BSI-C5 explizit als nationales Schema für Cybersicherheitszertifizierung. Angesichts der Tatsache, dass die ENISA gemäß Art. 50 CSA auf ihrer Website nationale Cybersicherheitszertifizierungsschemata zu benennen hat – bspw. im Falle einer Ablösung durch ein entsprechendes europäisches Schema – spricht bereits diese Tatsache dafür, dass das BSI-C5 als nationales Schema für die Cybersicherheitszertifizierung qualifiziert werden kann.

Damit das BSI-C5-Testat auch alle Begriffsmerkmale der Definition aus Art. 2 Nr. 10 CSA erfüllt, müssen die Vorschriften, technischen Anforderungen, Normen und Verfahren außerdem für die Zertifizierung oder Konformitätsbewertung von „*IKT-Produkten, -Diensten und -Prozessen*" gelten. Cloud-Dienste oder

---

[78] Siehe hierzu das FAQ des BSI zum C5 unter dem Abschnitt „Inhaltliche Einordnung des C5", abrufbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Einfuehrung/Kunde/Kunde_node.html (letzter Abruf am 22.4.2024); siehe auch die Umsetzungshinweise zum Mindeststandard des BSI zur Nutzung externer Cloud-Dienste, Version 2.1 vom 15.12.2022, S. 12, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Umsetzungshinweise_Mindeststandards_Externe_Cloud-Dienste_Version_2_1.pdf?__blob=publicationFile&v=3 (letzter Abruf am 22.4.2024).

[79] Siehe hierzu das FAQ des BSI zum C5 unter dem Abschnitt „Inhaltliche Einordnung des C5", abrufbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Einfuehrung/Kunde/Kunde_node.html (letzter Abruf am 22.4.2024).

[80] Siehe die Pressemitteilung des BSI zum Thema „Sicheres Cloud Computing in der EU", abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210127_C5_Datenschutz.html (letzter Abruf am 22.4.2024).

-Systeme sind von der begrifflich weit gefassten Definition des „IKT-Dienstes“ in Art. 2 Nr. 13 CSA umfasst, da hierunter ein Dienst zu verstehen ist, „*der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht*“. Das trifft auf Cloud-Computing-Dienste zu. Zudem hat der Europäische Verordnungsgeber in Art. 6 Abs. 2 der Verordnung (EU, EURATOM) 2023/2841 Cloud-Computing-Umgebungen unter den Begriff „IKT-Umgebung“ gefasst. Insofern werden IKT-Produkte, -Dienste und -Prozesse vom BSI-C5 umfasst, da sich die Definitionen begrifflich sehr ähneln und ein Cloud-System sämtliche dieser technischen Komponenten abdecken dürfte.

Insgesamt ist also davon auszugehen, dass das BSI-C5-Testat ein „nationales Schema für die Cybersicherheitszertifizierung“ gemäß Art. 2 Nr. 10 CSA ist.

2.2. Antwort auf Frage b)

Es ist fraglich, ob es richtig ist, dass mit einem im Amtsblatt der EU veröffentlichtem Cloud-Schema entsprechend europäischen Recht, u.a. durch Art. 57 Abs. 1 CSA, das BSI-C5 unwirksam wird.

Gemäß Art. 57 Abs. 1 Satz 1 CSA werden nationale Schemata für die Cybersicherheitszertifizierung für IKT-Produkte, -Dienste und -Prozesse, die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam, der in dem nach Art. 49 Abs. 7 CSA erlassenen Durchführungsrechtsakt festgelegt ist. Insofern wäre das BSI-C5 als nationales Schema für die Cybersicherheitszertifizierung ab dem Zeitpunkt unwirksam, der in dem entsprechenden Durchführungsakt der Europäischen Kommission benannt wäre. Die ENISA hat in ihrem Entwurf eine Übergangsfrist von einem Jahr ab dem Erlass des Durchführungsakts vorgeschlagen.[81] Die Europäische Kommission kann auf Grundlage des von der ENISA ausgearbeiteten möglichen Schemas für die Cybersicherheitszertifizierung ein europäisches Schema für die Cybersicherheitszertifizierung festlegen. Am 31.1.2024 hat die Kommission die Durchführungsverordnung (EU) 2024/482 zum europäischen System für die Cybersicherheitszertifizierung erlassen. Derzeit arbeitet die ENISA einen Entwurf für ein europäisches Zertifizierungsschema für Cloud-Dienste aus.[82] In diesem Entwurf benennt die ENISA das BSI-C5 ausdrücklich als nationales Schema für die Cybersicherheitszertifizierung, das dieselben Kategorien von Diensten enthält, aber nicht alle Anforderungen des europäischen Schemas aufweist.[83] Jedoch kann das BSI-C5 für Zertifizierungen im Rahmen des EUCS verwendet werden, worüber die ENISA künftig in einem Leitfaden konkreter informieren wird.[84]

Gemäß Art. 57 Abs. 3 CSA bleiben vorhandene Zertifikate, die auf Basis eines nationalen Schemas für die Cybersicherheitszertifizierung ausgestellt wurden und unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, bis zum Ende ihrer Geltungsdauer gültig. Das bedeutet für die Praxis, dass auf Basis des BSI-C5 ab diesem Zeitpunkt keine erneuten Zertifizierungen stattfinden könnten, aber nichtsdestotrotz vorhandene Zertifikate ihre Gültigkeit bis zum Ende ihrer Geltungsdauer behalten würden.

Demzufolge verliert ein BSI-C5-Testat in Zukunft ggf. auch seine Gültigkeit, weil ein Cloud-Schema entsprechend europäischem Recht veröffentlicht wird und der Durchführungsakt der Kommission vorsieht, dass nach Ablauf einer Übergangsfrist das BSI-C5-Testat nicht mehr wirksam wäre. Hierbei ist jedoch zu beachten, dass daraus noch nicht automatisch folgt, dass das BSI-C5-Testat im Anwendungsbereich des § 393 SGB V keine Rolle mehr spielt (siehe hierzu auch die Antwort auf Frage c im nachfolgenden Abschnitt).

---

[81] Entwurf der ENISA für ein europäisches Zertifizierungsschema für Cloud-Dienste (EUCS), S. 57.
[82] Siehe hierzu die Website der ENISA zur Cybersicherheitszertifizierung, abrufbar unter: https://certification.enisa.europa.eu/ (letzter Abruf am 21.4.2024); siehe hierzu auch den Entwurf der ENISA für ein europäisches Zertifizierungsschema für Cloud-Dienste (EUCS), abrufbar unter folgender URL: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme (letzter Abruf am 21.4.2024).
[83] Entwurf der ENISA für ein europäisches Zertifizierungsschema für Cloud-Dienste (EUCS), S. 57.
[84] Entwurf der ENISA für ein europäisches Zertifizierungsschema für Cloud-Dienste (EUCS), S. 58.

2.3. Antwort auf Frage c)

Es ist fraglich, ob es richtig ist, dass bei Unwirksamkeit des BSI-Schemas aufgrund der in § 393 SGB V verankerten nationalen Pflicht an Stelle des BSI-C5-Testates eine Zertifizierung nach ENISA-Vorgaben erforderlich sein wird.

Bei der Beantwortung der Frage ist zu beachten, dass der deutsche Gesetzgeber in § 393 SGB V eine Erlaubnisnorm für die Verarbeitung personenbezogener Daten im Bereich des Cloud-Computings geregelt hat. Demzufolge werden in der Vorschrift selbst keine europäischen Vorgaben aus dem CSA umgesetzt, sondern der nationale Gesetzgeber regelt Voraussetzungen, bei deren Vorliegen eine Datenverarbeitung erlaubt ist. Bei der Festlegung dieser Voraussetzungen muss der deutsche Gesetzgeber sich nicht an die Vorgaben für nationale Schema halten. Er kann vielmehr – in den durch die DSGVO festgelegten Grenzen – relativ frei bestimmen, welche zusätzlichen Voraussetzungen erfüllt sein müssen, damit Verarbeitungen von Gesundheits- und Sozialdaten im Anwendungsbereich des § 393 SGB V erlaubt sind. Das BSI-C5 wird zwar als nationales Schema für die Cybersicherheitszertifizierung nicht mehr anwendbar sein. Allerdings stellt der Wortlaut in § 393 Abs. 3 Nr. 2 SGB V gerade nicht auf ein nationales Schema für die Cybersicherheitszertifizierung, sondern unmittelbar auf das BSI-C5 ab. Sofern der nationale Gesetzgeber diese Kriterien weiterhin als ausreichend ansieht und den Wortlaut der Vorschrift nicht anpasst, bleibt das BSI-C5 somit nach wie vor eine Option zur Erfüllung der Vorgaben aus § 393 Abs. 3 Nr. 2 SGB V. Wegen der bereits in § 393 Abs. 4 SGB V geregelten Fristen und Typen von Testaten ist es eher unwahrscheinlich, dass der Gesetzgeber in Zukunft das BSI-C5-Testat nicht mehr ausreichen lässt.

Gemäß § 393 Abs. 4 Satz 3 SGB V ist eine Verarbeitung auch dann zulässig, soweit anstelle eines aktuellen C5-Testates ein Testat oder Zertifikat nach einem anderen Standard vorliegt, der ein vergleichbares oder höheres Sicherheitsniveau sicherstellt. Das Bundesministerium für Gesundheit wird nach § 393 Abs. 4 Satz 4 SGB V mittels Rechtsverordnung festlegen, welche Standards diese Anforderungen erfüllen. In dem Kontext ist die folgende Passage aus der Gesetzesbegründung zu § 393 Abs. 4 SGB V relevant: „*Die Öffnung für gleichwertige Testate und Zertifikate ist aufgrund der schnellen Entwicklung in diesem Bereich geboten; es ist zu erwarten, dass die European Union Agency for Cybersecurity (ENISA) zeitnah eine gleichwertige Zertifizierung – Cloud Certification Schemes (EUCS) – bereitstellen wird, die* ***ebenso zugelassen*** *werden soll. Das Bundesministerium für Gesundheit wird hierbei ermächtigt, im Zuge einer Rechtsverordnung festzulegen, welche Zertifikate als gleichwertig bewertet werden, um eine IT-sichere Verarbeitung von Sozial- und Gesundheitsdaten zu gewährleisten und somit* ***ebenso zugelassen*** *werden* sollen.“[85]

Aus der Formulierung „ebenso zugelassen“ wird deutlich, dass das BSI-C5-Testat im Anwendungsbereich des § 393 SGB V nicht irrelevant wird, sondern eine Zertifizierung nach ENISA-Vorgaben nur ebenso eine Möglichkeit sein wird, um die Anforderungen aus § 393 Abs. 3 und 4 SGB V zu erfüllen. In dem Zusammenhang ist auch zu beachten, dass § 393 Abs. 4 SGB V ab dem 1.7.2025 grundsätzlich ein C5-Typ2-Testat verlangt.

[85] BT, Drucksache 20/9048, S. 151 in Bezug auf § 393 Abs. 4 SGB V.