Eine Cloud ist eine Cloud.
Oder etwa doch nicht?

Erarbeitet von:

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Version 1.1

Autor: Dr. Bernd Schütze
Leiter GMDS AG „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Änderungshistorie

Version	Stand der Bearbeitung	Änderung
1.0	30. Juni 2024	Initiale Erstellung
1.1	Juli 2024	• Kleinere Fehler beseitigt • Kapitel 5.2.1.1 mit Adressaten von § 393 SGB V eingefügt, da Nachfragen zur Zugehörigkeit beim Begriff „Leistungserbringer“ erfolgten • Anhang 1 mit einer beispielhaften Nennung von Leistungserbringer im Kontext von Heil- und Hilfsmitteln eingefügt

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

- Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
- Im folgenden Text werden, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
- Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Dieses Werk ist unter einer Creative Commons-Lizenz (4.0 Deutschland Lizenzvertrag) lizenziert. D. h. Sie dürfen:

- Teilen: Das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten
- Bearbeiten: Das Material remixen, verändern und darauf aufbauen

und zwar für beliebige Zwecke, sogar kommerziell. Der Lizenzgeber kann diese Freiheiten nicht widerrufen, solange Sie sich an die Lizenzbedingungen halten.

Die Nutzung ist unter den folgenden Bedingungen möglich:

- Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
- Weitergabe unter gleichen Bedingungen: Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.
- Keine weiteren Einschränkungen: Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Im Weiteren gilt:

- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.
- Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

https://creativecommons.org/licenses/by-sa/4.0/deed.de

bzw. für den vollständigen Lizenztext

https://creativecommons.org/licenses/by-sa/4.0/legalcode

Inhaltsverzeichnis

1 Einführung ins Thema

Unter Cloud-Computing wurde, nicht nur in Deutschland, über Jahre hinweg eine Form der Bereitstellung von gemeinsam nutzbaren und flexibel skalierbaren IT-Leistungen durch nicht fest zugeordnete IT-Ressourcen verstanden. Im Rahmen von Outsourcing-Projekten wurden Cloud-Dienstleistungen eingekauft, um z. B. eine Anwendung in einem externen Rechenzentrum bei einem Dienstleister zu betreiben und sich keine Gedanken um CPU, Arbeitsspeicher oder Speicherkapazität zu machen: Bei Bedarf musste nichts angeschafft, sondern nur beim Dienstleister nachbestellt werden.

Seit Dezember 2022 wird der Begriff aus rechtlicher Sicht „Cloud-Computing-Dienst“ europäisch definiert. Damit ist rechtlich festgelegt, was ein Cloud-Computing-Dienst ist und was nicht – was letztlich u. a. auch Auswirkungen auf die Vertragsgestaltung hat: Wird ein Cloud-Computing-Dienst angeboten, so müssen die Vorgaben der Definition erfüllt sein.

Zugleich bestehen rechtliche Anforderungen, sowohl an Cloud-Anbieter als auch an Cloud-Nutzer, insbesondere im Bereich der IT-Sicherheit. Es wird daher vermutlich Unternehmen geben, die in der Vergangenheit einen Cloud-Dienst einkauften und seitdem nutzen. Diese sollten prüfen, ob die gesetzliche Begriffsbestimmung des „Cloud-Computing“ mit dem eingekauften Dienst übereinstimmt. Wenn nicht, sollten die betreffenden Unternehmen überlegen, ob man aufgrund der gesetzlichen Begriffsbestimmung die Namenskonventionen zum eingekauften Dienst zusammen mit dem Anbieter anpasst; explizit einen Cloud-Dienst einzukaufen und zu nutzen, dann aber gesetzliche Anforderungen, wie sie beispielsweise in § 393 SGB V zu finden sind, mit dem Hinweis „ist kein Cloud-Dienst“ nicht umzusetzen, könnte bei Prüfungen durch Behörden rechtliche Herausforderungen bringen.

Anbieter von entsprechenden Diensten sollten ebenfalls prüfen, ob die von ihnen angebotenen Dienste der europäischen Cloud-Definition entsprechen. Ist dies so, müssen alle gesetzlichen Anforderungen an einen Cloud-Computing-Dienst erfüllt werden. Insbesondere sollten entsprechende Anbieter die Aktivitäten der EU-Kommission hinsichtlich Umsetzung der Vorgaben der NIS-2-Richtlinie verfolgen; es könnten ihnen daraus ab Oktober 2024 neue rechtliche Anforderungen bezüglich zu ergreifender Maßnahmen erwachsen – inkl. Nachweisplicht.

Wird hingegen die Begriffsbestimmung des Cloud-Computings nicht erfüllt, sollte ein Dienst auch nicht mit diesem Label vertrieben werden. Aus Marketing-Gründen Kunden einen Cloud-Dienst zu verkaufen, jedoch die Vorgaben bzgl. Cloud-Computing nicht zu erfüllen (insbesondere Anforderungen hinsichtlich IT-Sicherheit aus diversen EU-Gesetzen), wird rechtliche Herausforderungen beinhalten, wie z. B., dass Kunden falsche Informationen und Zusicherungen über den verkauften Dienst bereitgestellt werden.

2 Definition der Cloud: Europäisch geregelt

Am 27. Dezember 202252 wurde die NIS-2-RL[1] im Amtsblatt der EU veröffentlicht, welche bis zum 14. Oktober 2024 durch das nationale Recht umgesetzt werden muss. Im Mai stellte das Bundesministerium des Innern und für Heimat den Referentenentwurf[2] für ein Umsetzungsgesetz der NIS-2-RL vor. Die NIS-2-RL enthält eine Definition des Cloud-Computings, sodass seit Oktober 2022 eine europäische Begriffsbestimmung existiert. Diese Definition wurde nahezu wortgleich vom deutschen Referentenentwurf übernommen und wurde ebenso im Digital-Gesetz[3] des Bundesministeriums für Gesundheit in das SGB V eingeführt:

Art. 6 Nr. 30 NIS-2-RL	§ 2 Abs. 1 Nr. 34 RefE NIS-2-Umsetzungsgesetz	§ 384 Nr. 5 SGB V
„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.	„Cloud-Computing-Dienst“ ein digitaler Dienst, der auf Abruf die Verwaltung eines skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen sowie den umfassenden Fernzugang zu diesem Pool ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind.	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.

Wie der Europäische Gerichtshof (EuGH) schon mehrfach urteilte, ist europäisches Recht vorrangig anzuwenden.[4] Bei Richtlinien haben nationale Gesetzgeber zwar einen gewissen Spielraum, müssen jedoch zwingend beachten, dass die Rechtswirkungen der nationalen Gesetze denen der Richtlinie entsprechen, d. h. die seitens des europäischen Gesetzgebers beabsichtigte Auswirkungen müssen im nationalen Gesetz abgebildet sein – ansonsten müssen nationale Gerichte die europäischen Vorgaben der jeweiligen Richtlinie bei der Urteilsfindung statt der nationalen Regelungen heranziehen.

2.1 Was versteht der europäische Gesetzgeber unter „Cloud-Computing“?

Aufgrund der Vorrangigkeit des europäischen Rechts müssen die nationalen Umsetzungen in § 2 Abs. 1 Nr. 34 RefE NIS-2-Umsetzungsgesetz und § 384 Nr. 5 SGB V den europäischen Vorgaben entsprechen. Um zu verstehen, wie Cloud-Computing definiert wird, muss man daher die europäischen Vorgaben betrachten, d. h. die Begriffsbestimmung in Art. 6 Nr. 30 NIS-2 Richtlinie auslegen.

[1] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-RL). Online, zitiert am 2024-06-26; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555

[2] BMI: Entwurf eines Gesetzes zur Umsetzung der NIS-2-RL und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. Online, zitiert am 2024-06-26; verfügbar unter https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html

[3] BMG: Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG). Online, zitiert am 2024-06-26; verfügbar unter https://www.bundesgesundheitsministerium.de/ministerium/gesetze-und-verordnungen/guv-20-lp/digig

[4] Art. 288 Abs. 2 AEUV. Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union ist zu finden unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012E/TXT (zuletzt abgerufen 2024-06-26)

Der EuGH[5] führt hierzu aus: „Bei der Prüfung dieser Bestimmungen sind nicht nur ihr Wortlaut, sondern auch ihr Zusammenhang und die Ziele zu berücksichtigen, die mit der Regelung, zu der sie gehören, verfolgt werden“. Wie der EuGH darstellt, sind somit insbesondere die Ziele des jeweiligen Rechtsaktes zu berücksichtigen. Allerdings wird die Möglichkeit der Auslegung durch den Wortlaut des Gesetzestextes beschränkt; keine Auslegung kann die Bedeutung des Wortlauts einer Regelung ändern, wenn der Wortlaut eindeutig ist. Die Erwägungsgründe eines europäischen Rechtsaktes sind hinsichtlich der Interpretation bei einem nicht eindeutig interpretierbaren Wortlaut vorrangig zu berücksichtigen, sind sie doch Bestandteil der jeweiligen europäischer Rechtsakte[6]. Der EuGH weist darauf hin, dass „Begründungserwägungen eines Gemeinschaftsrechtsakts rechtlich nicht verbindlich sind und weder herangezogen werden können, um von den Bestimmungen des betreffenden Rechtsaktes abzuweichen, noch, um diese Bestimmungen in einem Sinne auszulegen, der ihrem Wortlaut offensichtlich widerspricht“[7].

Die Begriffsbestimmung für Cloud-Computing beinhaltet sechs „Muss“- und ein „Kann“-Kriterium:

„Cloud-Computing-Dienst“

- einen digitalen Dienst, („muss“)
- der auf Abruf die Verwaltung („muss“)
- und den umfassenden Fernzugang („muss“)
- zu einem skalierbaren („muss“)
- und elastischen Pool („muss“)
- gemeinsam nutzbarer Rechenressourcen ermöglicht, („muss“)
- auch wenn diese Ressourcen auf mehrere Standorte verteilt sind („kann“).

Die Muss-Kriterien sind alle durch „und“ verknüpft, d. h. jede dieser Bedingungen muss erfüllt sein, damit es sich um einen Cloud-Computing-Dienst handelt. Die letzte Bedingung kann erfüllt sein, muss es aber nicht.

Nachfolgend werden die Bedingungen näher betrachtet, damit eine Einschätzung vorgenommen werden kann, ob es sich bei einem Dienst um Cloud-Computing handelt oder nicht.

2.2 Muss-Kriterium: Digitaler Dienst

Art. 6 Nr. 23 NIS-2-RL definiert einen „digitaler Dienst“ als einen Dienst im Sinne des Art. 1 Abs. 1 lit. b Richtlinie (EU) 2015/1535. In Art. 1 Abs. 1 lit. b Richtlinie (EU) 2015/1535[8] findet sich:

[5] EuGH, Urt. v. 25. Oktober 2011, Az. C-509/09, C-161/10, Rn. 54. Online, zitiert am 2023-11-01; verfügbar unter https://dejure.org/2011,48 bzw. Volltext des Urteils unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62009CJ0509

[6] Siehe auch „Gemeinsamer Leitfaden des Europäischen Parlaments, des Rates und der Kommission für Personen, die an der Abfassung von Rechtstexten der Europäischen Union mitwirken“, Abschnitt 10.5: „Die Erwägungsgründe müssen in möglichst knapper Form die Gründe für die wesentlichen Vorschriften des verfügenden Teils des Rechtsakts angeben.“ Online, zitiert am 2023-11-01; verfügbar unter https://op.europa.eu/de/publication-detail/-/publication/3879747d-7a3c-411b-a3a0-55c14e2ba732/language-de

[7] EuGH, Urt. v. 19. Juni 2014, Az. C-345/13, Rn. 31. Online, zitiert am 2023-11-01; verfügbar unter https://dejure.org/2014,13697 bzw. Volltext des Urteils unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62013CJ0345

[8] Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft. Online, zitiert am 2024-06-26; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32015L1535

„Dienst“ eine Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.

Im Sinne dieser Definition bezeichnet der Ausdruck

i) „im Fernabsatz erbrachte Dienstleistung“ eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird;

ii) „elektronisch erbrachte Dienstleistung“ 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;

iii) „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“ eine Dienstleistung die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird.

Eine Beispielliste der nicht unter diese Definition fallenden Dienste findet sich in Anhang I.

Ein digitaler Dienst ist also jede elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.

Keinen elektronischen Dienst stellt die Bereitstellung von Hardware dar (siehe Anhang I Nr. 2 RL (EU) 2015/1535). Als elektronische Dienste seien beispielhaft die Bereitstellung von virtuellen Maschinen zur Installation von Software (egal ob mit oder ohne Betriebssystem) oder auch die Bereitstellung von Software genannt.

2.3 Muss-Kriterium: Verwaltung auf Abruf

In ErwGr. 33 NIS-2-RL findet sich folgende Erläuterung zur Anforderung „Verwaltung auf Abruf“:

„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.“

Die Verwaltung auf Abruf bedingt also, dass sich Cloud-Nutzer (= Kunden) ohne Interaktion mit dem Cloud-Anbieter Rechenkapazitäten zuweisen können. Dabei ist es egal, ab die vom Kunden selbst zugeteilten Rechenkapazitäten vom Cloud-Anbieter berechnet werden oder nicht.

Es kommt lediglich darauf an, dass sich Cloud-Nutzer Rechenkapazitäten *selbst* zuteilen können. Müssen Cloud-Kunden beim Cloud-Anbieter Rechenkapazitäten beantragen und die Entscheidung, ob diese zugeteilt werden oder nicht, liegt beim Cloud-Anbieter, so ist dieses Kriterium nicht erfüllt.

2.4 Muss-Kriterium: Umfassender Fernzugang

In ErwGr. 33 NIS-2-RL findet sich folgende Erläuterung zur Anforderung „umfassender Fernzugriff“:

„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.“

Jeder über ein Netzwerk, insbesondere auch unter Nutzung des Internets, bereitgestellte Dienst erfüllt diese Anforderung.

2.5 Muss-Kriterium: Skalierbarer Pool

In ErwGr. 33 NIS-2-RL findet sich folgende Erläuterung zur Anforderung „Skalierbarkeit“:

> „Der Begriff „skalierbar“ bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können.“

Immer, wenn ein Cloud-Anbieter flexibel auf Auslastungen eines Dienstes reagieren kann, ist diese Bedingung erfüllt. Ob dabei auf Rechenressourcen unterschiedlicher Standorte von Rechenzentren zugegriffen wird, spiel hierbei keine Rolle. „Unabhängig vom geografischen Standort“ erlaubt es, alles in einem Rechenzentrum zu organisieren oder auch unterschiedliche Rechenzentren zur Lastverteilung zu nutzen.

Bzgl. Auslastungen ist es egal, ob zeitliche Effekte eine Rolle spielen (z. B. erhöhte Nutzung von Cloud-Ressourcen zwischen 8 und 19 Uhr) oder nicht. Die dem Kunden zugesicherte Leistung muss erbracht werden.

2.6 Muss-Kriterium: Elastischer Pool

In ErwGr. 33 NIS-2-RL findet sich folgende Erläuterung zur Anforderung „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.“

Die Anforderung eines „elastischen Pools“ ergänzt die Anforderung „skalierbarer Pool“. Während die Anforderung „skalierbarer Pool“ verlangt, dass Cloud-Anbieter Nachfrageschwankungen ausgleichen können, verlangt die Anforderung eines elastischen Pools, dass Cloud-Anbieter auf Nachfragen von Cloud-Kunden diesen Rechenressourcen zur Verfügung stellen können.

2.7 Muss-Kriterium: Gemeinsam nutzbar

In ErwGr. 33 NIS-2-RL findet sich folgende Erläuterung zur Anforderung „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.

Ein Anbieter stellt Rechenressourcen einer Vielzahl von Kunden zur Verfügung. Die Anforderung „Verarbeitung für jeden Nutzer separat“ wird in der Regel durch eine Mandantentrennung umgesetzt, durch welche die Daten der verschiedenen Nutzer und damit auch die Zugriffsmöglichkeiten voneinander getrennt werden.

2.8 Kann-Kriterium: Auf mehrere Standorte verteilt

Der Wortlaut „[…] auch wenn diese Ressourcen auf mehrere Standorte verteilt sind […]“ in der Begriffsbestimmung in Art. 6 Nr. 30 NIS-2-RL weist auf die Optionalität hin: „auch“ bedeutet, dass die Bedingung bei einem Cloud-Computing-Dienst nicht erfüllt sein muss, jedoch erfüllt sein darf.

In ErwGr. 33 NIS-2-RL findet sich folgende Erläuterung zur Anforderung „gemeinsam nutzbar“:

> „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.“

„Verteil“ ist also erfüllt, wenn Rechenressourcen von vernetzten Geräten genutzt werden. Dies können vernetzte Rechenzentren sein, aber auch vernetzte Computer (z. B. in einem Cluster verbundene Computer) in einem einzigen Rechenzentrum.

2.9 Prüfung, ob Cloud-Computing vorliegt oder nicht

Zusammenfassend eine Kurzfassung, welche Bedingungen erfüllt sein müssen, damit ein Dienst einen Cloud-Computing-Dienst darstellt:

- **Digitaler Dienst**:
  Wird i. d. R. gegeben sein, wenn mehr als Hardware von einem Anbieter bereitgestellt wird.
- **Verwaltung auf Abruf**:
  Cloud-Nutzer kann sich selbst ohne Interaktion mit dem Anbieter von Cloud-Computing-Diensten Rechenkapazitäten zuweisen.
- **Umfassender Fernzugang**:
  Cloud-Kapazitäten werden über das Netz bereitgestellt und über Mechanismen zugänglich gemacht.
- **Skalierbarer Pool**:
  Rechenressourcen werden unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt, damit Nachfrageschwankungen bewältigt werden können.
- **Elastischer Pool**:
  Rechenressourcen werden entsprechend der Nachfrage bereitgestellt und freigegeben, damit die Menge der verfügbaren Ressourcen je nach Arbeitsaufkommen rasch erhöht oder reduziert werden kann.
- **Gemeinsam nutzbar**:
  Rechenressourcen werden einer Vielzahl von Nutzern bereitgestellt, wobei die Nutzer über einen gemeinsamen Zugang auf den Dienst zugreifen, die Verarbeitung für jeden Nutzer jedoch separat erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird.

Zusätzlich **kann** folgendes Kriterium erfüllt sein:

- **Verteilt**:
  Rechenressourcen befinden sich auf verschiedenen vernetzten Computern oder Geräten.

3 Arten von Cloud-Computing-Diensten

Cloud-Computing-Dienste ermöglichen entsprechend der Definition in Art. 6 Nr. 30 NIS-2-RL den Zugang zu gemeinsam nutzbarer Rechenressourcen. Gemäß ErwGr. 33 NIS-2-RL zählen zu Rechenressourcen „Ressourcen wie Netze, Server oder sonstige Infrastruktur, Betriebssysteme, Software, Speicher, Anwendungen und Dienste“.

Zu den Dienstmodellen des Cloud-Computings gehören entsprechend ErwGr. 33 NIS-2-RL u. a.

- IaaS (Infrastructure as a Service,
- PaaS (Platform as a Service),
- SaaS (Software as a Service) und
- NaaS (Network as a Service).

Dies ist keine abschließende Aufzählung. ISO/IEC 22123-1[9] kennt z. B. ergänzend zu der Aufzählung in ErwGr. 33 NIS-2-RL noch die folgenden Cloud-Dienstmodelle:

- CaaS (Communications as a Service),
- CompaaS (Compute as a Service),
- DSaaS (Data storage as a Service).

Die Bereitstellungsmodelle für Cloud-Computing sollten die private („private cloud“), die gemeinschaftliche („community cloud“), die öffentliche „public cloud“) und die hybride Cloud („hybrid cloud“) umfassen. Die Cloud-Computing-Dienst- und Bereitstellungsmodelle haben dieselbe Bedeutung wie die in der Norm ISO/IEC 17788:2014[10] definierten Dienst- und Bereitstellungsmodelle.

Dem europäischen Gesetzgeber war offensichtlich nicht bekannt, dass die (relativ alte) ISO/IEC 17788:2014 von den Normungsgremien zurückgezogen wurde.[11] Ersetzt wurde die ISO/IEC 17788:2014 durch die ISO/IEC 22123:2023, die aus drei Teilen besteht:

- ISO/IEC 22123-1:2023 - Cloud computing - Part 1: Vocabulary
- ISO/IEC 22123-2:2023 - Cloud computing - Part 2: Concepts
- SO/IEC 22123-3:2023 - Cloud computing - Part 3: Reference architecture

Die Begriffsdefinitionen wie „hybrid cloud“ finden sich jetzt in Teil 1, Teil 2 spezifiziert Konzepte, die im Bereich des Cloud Computings verwendet werden. Während sich die Begriffsbestimmungen in Teil 1 befinden, beschreibt Teil 2 – unter Nutzung der Begriffsbestimmungen die grundlegenden Konzepte des Cloud Computings. So werden in Teil 2 die Hauptmerkmale des Cloud Computings beschrieben wie beispielsweise:

- Umfassender Netzwerkzugang,
- Messbarer Dienst,
- Mehrmandantenfähigkeit,
- Selbstverwaltung auf Abruf oder
- Schnelle Elastizität und Skalierbarkeit.

Die ISO/IEC 22123-2:2023 kann ergänzend zu ErwGr. 33 NIS-2-RL genutzt werden, um die in der Begriffsbestimmung „Cloud-Computing-Dienst enthaltenen Anforderungen besser zu verstehen.

[9] ISO/IEC 22123-1:2023-02 „Cloud Computing - Teil 1: Terminologie“. Online, zitiert am 2023-11-01; verfügbar unter https://www.iso.org/standard/82758.html

[10] DIN ISO/IEC 17788:2016-04 „Cloud Computing - Übersicht und Vokabular“. “. Online, zitiert am 2023-11-01; verfügbar unter https://www.dinmedia.de/de/norm/din-iso-iec-17788/247977149

[11] ISO/IEC 17788:2014 „Cloud computing — Overview and vocabulary“. Online, zitiert am 2023-11-01; verfügbar unter https://www.iso.org/standard/60544.html

3.1 Definition Dienstmodelle

Die Definitionen der Dienstmodelle lauten entsprechend ISO/IEC 22123-1:2023:

Dienstmodelle	Englisch	Deutsch[12]
CaaS	cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration	Cloud-Service-Kategorie, bei der dem Kunden des Cloud-Services Echtzeit-Interaktion und -Zusammenarbeit angeboten wird
CompaaS	cloud service category in which the capabilities provided to the cloud service customer are the provision and use of processing resources needed to deploy and run software	Cloud-Service-Kategorie, bei der die dem Cloud-Service-Kunden zur Verfügung gestellten Möglichkeiten in der Bereitstellung und Nutzung von Verarbeitungsressourcen bestehen, die für die Bereitstellung und Ausführung von Software erforderlich sind
DSaaS	cloud service category in which the capability provided to the cloud service customer is the provision and use of data storage and related capabilities	Cloud-Service-Kategorie, bei der die für den Cloud-Service-Kunden erbrachte Leistung in der Bereitstellung und Nutzung von Datenspeicherung und damit verbundenen Leistungen besteht
IaaS	cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type	Cloud-Service-Kategorie, bei der die dem Cloud-Service-Kunden bereitgestellte Form der Cloud-Funktionalität eine Infrastruktur-Funktionalität ist
NaaS	cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities	Cloud-Service-Kategorie, bei der die dem Cloud-Service-Kunden zur Verfügung gestellte Leistung die Transportkonnektivität und die damit verbundenen Netzkapazitäten ist
PaaS	cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type	Cloud-Service-Kategorie, bei der die dem Cloud-Service-Kunden bereitgestellte Cloud-Funktionalität eine Plattformfunktion darstellt
SaaS	cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type	Cloud-Service-Kategorie, bei der die dem Cloud-Service-Kunden bereitgestellte Cloud-Leistung in der Bereitstellung von Software-Funktionalität besteht

[12] Eigene, d. h. nicht offizielle Übersetzung

3.2 Definition Bereitstellungsmodelle

Die Definitionen der Bereitstellungsmodelle lauten entsprechend ISO/IEC 22123-1:2023:

Bereitstellungsmodell	Englisch	Deutsch[12]
community cloud	cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection	Cloud-Bereitstellungsmodell, bei dem Cloud-Dienste ausschließlich einer bestimmten Gruppe von Kunden zur Verfügung gestellt und von ihnen gemeinsam genutzt werden, wobei diese Kunden gemeinsame Anforderungen haben und in einer bestimmten Beziehung zueinanderstehen, und bei dem die Ressourcen von mindestens einem Mitglied dieser Gruppe kontrolliert werden
hybrid cloud	cloud deployment model that uses a private cloud and a public cloud	Cloud-Bereitstellungsmodell, welches eine private Cloud und eine öffentliche Cloud umfasst
private cloud	cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer	Cloud-Bereitstellungsmodell, bei dem Cloud-Dienste ausschließlich von einem einzigen Cloud-Service-Kunden genutzt werden und die Ressourcen von diesem Cloud-Service-Kunden kontrolliert werden
public cloud	cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider	Cloud-Bereitstellungsmodell, bei dem die Cloud-Dienste potenziell jedem Cloud-Service-Kunden zur Verfügung stehen und die Ressourcen vom Cloud-Service-Anbieter kontrolliert werden

ISO/IEC 22123-1:2023 kennt ergänzend noch ein weiteres Bereitstellungsmodell: multi-cloud (oder auch multicloud), deren Definition lautet:

	cloud deployment model in which a cloud service customer uses public cloud services provided by two or more cloud service providers	Cloud-Bereitstellungsmodell, bei dem ein Cloud-Service-Kunde öffentliche Cloud-Dienste nutzt, die von zwei oder mehr Cloud-Service-Anbietern bereitgestellt werden

4 Cloud vs. Rechenzentrum

Art. 6 Nr. 31 NIS-2-RL definiert einen Rechenzentrumsdienst als 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“.

Ein Rechenzentrumsdienst stellt also letztlich die Ressourcen wie Hardware, Netzwerkanbindung usw. zur Verfügung, die für die Installation und Nutzung von Softwareprodukten erforderlich sind. Es handelt sich also um einen Infrastrukturdienst.

In ErwGr. 35 NIS-2-RL wird dazu ausgeführt, dass von Anbietern von Rechenzentrumsdiensten angebotenen Diensten möglicherweise nicht immer in Form eines Cloud-Computing-Diensts erbracht werden und dementsprechend Rechenzentren möglicherweise nicht immer Teil einer Cloud-Computing-Infrastruktur sind.

Fazit: Nicht jeder Rechenzentrumsdienst ist ein Cloud-Computing-Dienst, aber Rechenzentrumsdienste können Cloud-Computing-Dienste sein. Ob es sich bei einem Rechenzentrumsdienst um einen Cloud-Computing-Dienst handelt oder nicht, wird allein durch die Definition des Cloud-Computing-Dienstes in Art. 6 Nr. 30 NIS-2-RL bestimmt: Werden die Bedingungen der Definition erfüllt, so handelt es sich bei dem Rechenzentrumsdienst um einen Cloud-Computing-Dienst, sonst nicht.

5 Rechtliche Anforderung bei Cloud-Computing

5.1 Anforderungen an Cloud-Anbieter

5.1.1 Anforderungen aus der NIS-2-Richtlinie

5.1.1.1 Cloud-Anbieter: Wesentliche oder wichtige Einrichtung

Die NIS-2-RL unterscheidet „wesentliche“ und „wichtige“ Einrichtungen. Wesentliche Einrichtungen werden in Art. 3 Abs. 1 NIS-2-RL bestimmt, wichtige Einrichtungen in Art. 3 Abs. 2 NIS-2-RL. Beide Regelungen verweisen u. a. auf Anhang I der NIS-2-RL.

Anbieter von Cloud-Computing-Diensten sowie Anbieter von Rechenzentrumsdiensten gelten entsprechend Anhang I NIS-2-RL als Dienste mit „hoher Kritikalität“ im Sektor „Digitale Infrastruktur“.

- Entsprechend Art. 3 Abs. 1 NIS-2-RL gelten sie als wesentliche Einrichtungen, wenn sie als mittlere Unternehmen gelten oder die Schwellenwerte[13] für mittlere Unternehmen sogar überschreiten; d. h. die Regelung adressiert mittlere sowie große Unternehmen.
- Kleine Unternehmen sowie Kleinstunternehmen gelten gemäß Art. 3 Abs. 2 NIS-2-RL hingegen als wichtige Einrichtungen.

Entsprechend der Einstufung resultieren Anforderung an die zu gewährleistende IT-Sicherheit (siehe insbesondere Art. 21 NIS-2-RL).

5.1.1.2 Gewährleistung IT-Sicherheit

Art. 21 Abs. 2 NIS-2-RL verlangt von wesentlichen und wichtigen Einrichtungen, dass diese „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen“ ergreifen, welche sicherstellen, dass die Risiken für die Sicherheit der Netz- und Informationssysteme beherrscht werden und dass die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste verhindert oder möglichst geringgehalten werden.

Hierzu verlangt Art. 21 Abs. 3 NIS-2-RL, dass diese Maßnahmen zumindest Folgendes umfassen:

lit. a): **Konzepte** in Bezug auf die **Risikoanalyse und Sicherheit** für **Informationssysteme**;
lit. b): **Bewältigung von Sicherheitsvorfällen**;
lit. c): **Aufrechterhaltung des Betriebs**, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
lit. d): **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
lit. e): **Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen**, einschließlich Management und Offenlegung von Schwachstellen;
lit. f): **Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen** im Bereich der Cybersicherheit;
lit. g): **grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen** im Bereich der Cybersicherheit;
lit. h): **Konzepte und Verfahren für den Einsatz von Kryptografie** und gegebenenfalls Verschlüsselung;

[13] Die Schwellwerte richten sich nach Art. 2 des Anhangs der Empfehlung 2003/361/EG. Mittlere Unternehmen sind Unternehmen mit 50 bis 250 beschäftigten Personen, die einen Jahresumsatz von höchstens 50 Mio. Euro erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. Euro beläuft. Online, zitiert am 2024-06-26; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32003H0361

lit. i): Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

lit. j): **Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung**, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Der RefE des NIS2-Umsetzungsgesetzes enthält die wortgleichen Anforderungen in § 30 Abs. 2 BSIG-E (Art. 1 RefE).

5.1.1.3 Ermächtigung EU-Kommission zur Festlegung von TOM

Entsprechend Art. 21 Abs. 5 NIS-2-RL **muss** die EU-Kommission bis zum 17. Oktober 2024 Durchführungsrechtsakte zur Festlegung der technischen und methodischen Anforderungen veröffentlichen, die auch Cloud-Computing-Dienstleister sowie Anbieter von Rechenzentrumsdiensten adressieren. Diese von der EU-Kommission festgelegten Anforderungen sind zwingend umzusetzen.

5.1.1.4 Meldepflicht bei Sicherheitsvorfällen

Entsprechend Art. 23 Abs. 1 müssen wesentliche und wichtige Einrichtungen unverzüglich die zuständige Stelle über jeden Sicherheitsvorfall unterrichten, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat, also einen erheblichen Sicherheitsvorfall darstellt. Entsprechend Art. 6 Nr. 6 ist ein Sicherheitsvorfall „ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt“. Gemäß Art. 21 Abs. 3 NIS-2-RL gilt ein Sicherheitsvorfall als erheblich, wenn

a) er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;
b) er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Ebenfalls bis zum 17. Oktober 2024 muss die EU-Kommission Durchführungsrechtsakte erlassen, in denen näher bestimmt wird, in welchen Fällen ein Sicherheitsvorfall als erheblich und somit als meldepflichtig anzusehen (Art. 23 Abs. 11 NIS-2-RL). Auch diese Rechtsakte adressieren u. a. Cloud-Computing-Dienstleister sowie Anbieter von Rechenzentrumsdiensten.

Diese europäischen Vorgaben werden durch § 30 Abs. 2 BSI-Gesetz (Art. 1 RefE) umgesetzt. Die verpflichtenden Meldungen müssen an eine vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle übermittelt werden (§ 32 Abs. 1 BSIG-E). Die Meldung muss „unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung“ erfolgen („Erstmeldung“). Spätestens einen Monat nach Übermittlung der Erstmeldung des Sicherheitsvorfalls muss eine Abschlussmeldung erfolgen, die Folgendes enthält:

a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;
b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;
c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;
d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls;

Diese Regelungen im RefE entsprechen den Vorgaben in Art. 23 Abs. 4 NIS-2-RL.

5.1.2 Anforderungen aus dem Data Act

Die Datenverordnung[14] („Data Act“) wurde am 10. Dezember 2023 im europäischen Amtsblatt veröffentlicht und die darin enthaltenen Regelungen entfalten ab dem 12. September 2025 ihre Wirkung. Die Verordnung gilt für (Art. 1 Abs. 3 Datenverordnung):

- Hersteller vernetzter Produkte, die in der Union in Verkehr gebracht werden, und Anbieter verbundener Dienste, unabhängig vom Ort der Niederlassung dieser Hersteller oder Anbieter;
- Anbieter von Datenverarbeitungsdiensten, unabhängig vom Ort ihrer Niederlassung, die Kunden in der Union solche Dienste anbieten;
- u. a.

Entsprechend Art. 2 Nr. 8 Datenverordnung ist ein Datenverarbeitungsdienst wie folgt definiert:

> Ein Datenverarbeitungsdienst ist „eine digitale Dienstleistung, die einem Kunden bereitgestellt wird und einen flächendeckenden und auf Abruf verfügbaren Netzzugang zu einem **gemeinsam genutzten Pool** konfigurierbarer**, skalierbarer und elastischer Rechenressourcen** zentralisierter, verteilter oder hochgradig verteilter Art ermöglicht, die mit minimalem Verwaltungsaufwand oder minimaler Interaktion des Diensteanbieters rasch bereitgestellt und freigegeben werden können“

Betrachtet man die Begriffsbestimmung eines Cloud-Computing-Dienstes in Art. 4 Nr. 19 NIS-2-RL (siehe Kapitel 2)

> „Cloud-Computing-Dienst“ einen digitalen Dienst, der den Zugang zu **einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen** ermöglicht,

so ist offensichtlich, dass ein Cloud-Computing-Dienst einen Datenverarbeitungsdienst darstellt.

5.1.2.1 Wechsel zwischen Diensteanbieter

Kapitel VI Datenverordnung enthält Vorgaben für den Wechsel eines Kunden zwischen Datenverarbeitungsdiensten. Das erklärte Ziel Art. 23–31 Datenverordnung ist, sowohl Barrieren beim Wechsel von sog. Datenverarbeitungsdiensten abzubauen als auch ein sog. Vendor Lock-in von Kunden zu verhindern.

Der in den Regelungen enthaltenen Begriffe „ursprünglicher Anbieter“ (source provider) und „übernehmender Anbieter“ (destination provider) sind in der Datenverordnung zwar nicht definiert, findet sich jedoch in den Erwägungsgründen wieder, sodass die Bedeutung der Begriffe im Kontext der Erwägungsgründe bestimmbar ist. Im Kontext des Dienstleisterwechsels gilt daher:

- Ursprüngliche Anbieter ist der Alt-Anbieter, mit dem der Kunde bislang ein bestehendes Vertragsverhältnis hatte.
- Übernehmender Anbieter ist der Neu-Anbieter, zu dem der Kunde wechseln möchte.

5.1.2.2 Vertragsklauseln für den Anbieterwechsel

Art. 25 Datenverordnung enthält Vorgaben für Vertragsklauseln für den Wechsel. Gemäß Art. 25 Abs. 1 Datenverordnung müssen „die Rechte des Kunden und die Pflichten des Anbieters von Datenverarbeitungsdiensten in Bezug auf den Wechsel zwischen Anbietern“ eindeutig in einem schriftlichen Vertrag festgelegt sein. Art. 25 Abs. 2, 3 Datenverordnung enthält Mindestanforderungen an diesen Vertrag, u. a. muss ein Anbieter von Datenverarbeitungsdiensten

[14] Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung). Online, zitiert am 2024-06-26; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1710657540953&uri=CELEX%3A32023R2854

- dem Kunden und von ihm autorisierten Dritten beim Vollzug des Wechsels angemessene Unterstützung leisten,
- mit der gebotenen Sorgfalt handeln, um die Kontinuität des Geschäftsbetriebs aufrechtzuerhalten und die Erbringung der vertragsmäßigen Funktionen oder Dienste fortzusetzen,
- während der Wechsel vollzogen wird, für ein hohes Maß an Sicherheit sorgen.

Die Vorgabe für die maximale Kündigungsfrist für die Einleitung des Wechsels darf dabei zwei Monate nicht überschreiten. Weiterhin ist eine „erschöpfende Auflistung aller Kategorien von Daten und digitalen Vermögenswerten, die während des Wechselvollzugs übertragen werden können, einschließlich mindestens aller exportierbaren Daten“ verpflichtender Bestandteil des Vertrages. Eine weitere Vertragsklausel muss garantieren, dass alle exportierbaren Daten und digitalen Vermögenswerte, die direkt vom Kunden generiert werden oder sich direkt auf den Kunden beziehen, vollständig gelöscht werden, sofern der Wechsel erfolgreich vollzogen ist.

Der Wechsel kann dabei zu einem anderen Anbieter von Datenverarbeitungsdiensten erfolgen oder auch einen Wechsel zu einer IKT-Infrastruktur in eigenen Räumlichkeiten beinhalten.

5.1.2.3 Technische Vorgaben für den Wechsel

Art. 30 Abs. 2 Datenverordnung verlangt von einem Anbieter von Datenverarbeitungsdiensten, dass dieser allen ihren Kunden und den betreffenden übernehmenden Anbietern von Datenverarbeitungsdiensten unentgeltlich offene Schnittstellen bereitstellen muss; eine Ausnahme besteht entsprechend Art. 30 Abs. 1 Datenverordnung für reine Infrastrukturanbieter.

Dabei müssen Anbieter von Datenverarbeitungsdiensten gemäß Art. 30 Abs. 3 Datenverordnung die Kompatibilität mit gemeinsamen Spezifikationen auf der Grundlage offener Interoperabilitätsspezifikationen oder harmonisierter Interoperabilitätsnormen gewährleisten.

Nach Art. 31 Datenverordnung gibt es aber Ausnahmen von diesen Regelungen:

Abs. 1: Individuallösungen, „bei denen die meisten zentralen Funktionen auf die spezifischen Bedürfnisse eines einzelnen Kunden zugeschnitten wurden“, fallen nicht unter Regelungen Kap. VI Datenverordnung.
Abs. 2: Teststellungen fallen ebenfalls nicht unter Regelungen Kap. VI Datenverordnung.

5.1.2.4 Kosten für den Kunden: Wechselentgelte

Entsprechend Art. 29 Abs. 1 Datenverordnung darf ein Wechsel des Anbieters und die Bereitstellung/Übertragung der Daten ab dem 12. Januar 2027 nichts kosten. Gemäß Art. 29 Abs. 2 Datenverordnung dürfen Anbieter von Datenverarbeitungsdiensten vom 11. Januar 2024 bis zum 12. Januar 2027 jedoch bei den Kunden für den Vollzug des Wechsels ermäßigte Wechselentgelte erheben, wobei die Wechselentgelte entsprechend Art. 29 Abs. 3 Datenverordnung die Kosten, die dem Anbieter von Datenverarbeitungsdiensten im unmittelbaren Zusammenhang mit dem betreffenden Wechsel entstehen, nicht übersteigen dürfen.

5.1.2.5 Mustervertragsklauseln

Entsprechend Art. 41 Datenverordnung muss die Kommission vor dem 12. September 2025 unverbindliche Mustervertragsklauseln für den Datenzugang und die Datennutzung erstellen. Diese Mustervertragsklauseln müssen u. a. Bedingungen für eine angemessene Gegenleistung und den Schutz von Geschäftsgeheimnissen sowie nicht verbindliche Standardvertragsklauseln für Verträge über Cloud-Computing beinhalten.

5.1.3 Ausblick: Der kommende Cyber Resilience Act

Der Cyber Resilience Act[15] ist noch nicht verabschiedet, der offizielle Status[16] lautet aktuell „Awaiting Council's 1st reading position“. Der Text, den das EU-Parlament annahm, ist öffentlich verfügbar.[17]

5.1.3.1 Anwendungsbereich

Die Verordnung gilt gemäß Art. 2 Abs. 1 Verordnungsvorschlag für „auf dem Markt bereitgestellte Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt“. Art. 2 Abs. 2-4 Verordnungsvorschlag enthält eine abschließende Aufzählung, wofür die Verordnung nicht gelten soll, da diese Produkte durch andere Normen reguliert werden:

- Verordnung (EU) 2017/745 (Medizinprodukte),
- Verordnung (EU) 2017/746 (In-vitro-Diagnostika),
- Verordnung (EU) 2019/2144 (Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern usw.),
- Verordnung (EU) 2018/1139 (Zivilluftfahrt),
- Richtlinie 2014/90/EU (Schiffsausrüstung).

Art. 3 Verordnungsvorschlag enthält die Begriffsbestimmung eines „Produkt mit digitalen Elementen“:

> „ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden“.

Art. 3 Verordnungsvorschlag enthält ergänzend Begriffsbestimmungen zu „Software“, „Hardware“, „Komponente“ und „elektronisches Informationssystem“, sodass vermutlich jede Software im Kontext der Gesundheitsversorgung, welches kein Medizinprodukt ist, von der Norm vollständig erfasst wird. Insbesondere werden voraussichtlich auch Cloud-Computing-Dienste von der Verordnung erfasst.

5.1.3.2 Anforderungen

Entsprechend Art. 6 Verordnungsvorschlag müssen alle Produkte den grundlegenden Anforderungen in Anhang I Teil I und II genügen. Art. 7 Verordnungsvorschlag adressiert „wichtige Produkte“. Dies sind Produkte, die Kernfunktionen einer in Anhang III aufgeführten Produktkategorie aufweisen, z. B.

- Identitätsmanagementsysteme sowie Software und Hardware für die Verwaltung des privilegierten Zugangs, einschließlich Lesegeräte für die Authentifizierung und Zugangskontrolle, auch biometrische Lesegeräte,
- eigenständige und eingebettete Browser oder auch
- am Körper tragbare Produkte, die zum Zwecke der Gesundheitsüberwachung (z. B. Tracking) bestimmt sind, die kein Medizinprodukt sind.

---

[15] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020. Online, zitiert am 2024-06-26; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A52022PC0454

[16] Der Status des Rechtsaktes kann unter „Legislative Observatory“ des EU Parlaments abgerufen werden. Link zum Cyber Resilience Act (zuletzt abgerufen 2024-06-26): https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0272(COD)&l=en

[17] Legislative Entschließung des Europäischen Parlaments vom 12. März 2024 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)). Online, zitiert am 2024-06-26; verfügbar unter https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_DE.html

Nahezu alle Informationssysteme wie auch Cloud-Computing-Dienste enthalten Identitätsmanagementsysteme: Anwender müssen sich anmelden, um auf Funktionen der Software sowie auf gespeicherte Daten zugreifen zu dürfen.

Art. 8 Verordnungsvorschlag enthält Vorgaben für „kritische Produkte“, die im Anhang IV beschrieben sind; die EU-Kommission darf die Liste aber ändern. Aktuell gehören u. a. dazu:

- Hardwaregeräte mit Sicherheitsboxen; dies eröffnet die Frage, ob der TI-Konnektor dazugehört und die sicherheitstechnischen Vorgaben darauf anzuwenden sind.
- Chipkarten oder ähnliche Geräte, einschließlich Sicherheitselemente, was sicherlich auf Patientenausweis, HPC usw. zutreffen wird.

Die von der Verordnung adressierten Produkte müssen u. a. umsetzen:

- Eine Bewertung der Cybersicherheitsrisiken (Art. 13 Abs. 3 Verordnungsvorschlag);
    - (Art. 31, Anhang VII Verordnungsvorschlag);
- Software-Stücklisten („Software Bill of Materials”, SBOM) müssen vorhanden und auf dem aktuellen Stand sein;
- Meldepflicht bzgl. aktiv ausgenutzter Schwachstelle(n) (Art. 14 Verordnungsvorschlag); dabei können auch freiwillige Meldungen bzgl. „enthaltene Schwachstelle sowie Cyberbedrohungen, die sich auf das Risikoprofil eines Produkts mit digitalen Elementen auswirken könnten“ von anderen Personen als Hersteller erfolgen (Art. 15 Verordnungsvorschlag), d. h. Kunden dürfen ohne Rücksprache mit dem Hersteller Schwachstellen und Cyberbedrohungen an die nationale Stelle oder auch direkt an ENISA melden;
- CE-Kennzeichnung darf nur nach Konformitätsbewertung erfolgen (Art. 29 ff Verordnungsvorschlag).

Die EU-Kommission soll Leitlinien veröffentlichen, um Wirtschaftsakteure bei der Anwendung der Verordnung zu unterstützen (Art. 26), besonderer Schwerpunkt ist dabei die Erleichterung der Anwendung der Verordnung für KMUs.

Weiterhin soll die EU-Kommission eine oder mehrere europäische Normungsorganisationen auffordern, harmonisierte Normen für die in Anhang I der Verordnung aufgeführten grundlegenden Anforderungen auszuarbeiten.

5.1.3.3 Cloud-Computing

Cloud-Computing wird in den Regelungen des Cyber Resilience Act selbst nicht erwähnt, jedoch wird im ErwGr. 12 Cyber Resilience Act auf Cloud Computing eingegangen. Darin heißt es:

> „Cloud-Lösungen gelten nur dann als Datenfernverarbeitungslösungen im Sinne dieser Verordnung, wenn sie der in dieser Verordnung festgelegten Begriffsbestimmung entsprechen.
>
> So fallen beispielsweise vom Hersteller von intelligenten Haushaltsgeräten angebotene Cloud-Funktionen, die es den Nutzern ermöglichen, das Gerät aus der Ferne zu steuern, in den Anwendungsbereich dieser Verordnung.
>
> Dagegen fallen Websites, die die Funktionalität eines Produkts mit digitalen Elementen nicht unterstützen, oder Cloud-Dienste, die außerhalb der Verantwortung eines Herstellers eines Produkts mit digitalen Elementen entworfen und entwickelt wurden, nicht in den Anwendungsbereich dieser Verordnung.“

Ein Erwägungsgrund kann keine Regelung einer Verordnung oder Richtlinie ändern, sondern dient nur der Interpretation der jeweiligen korrespondierenden Regelung. Dementsprechend gilt: Treffen die Vorgaben der jeweiligen Regelung zu, ist die Regelung anzuwenden.

Der Erwägungsgrund betrachtet zunächst „Datenfernverarbeitungslösungen“, die in Art. 3 Nr. 2 Cyber Resilience Act definiert sind. Demnach ist eine Datenfernverarbeitung eine

> „entfernt stattfindende Datenverarbeitung, für die eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte.“

Nutzt eine Software eine externe Cloud-Infrastruktur, die „außerhalb der Verantwortung“ des Software-Herstellers agiert, so wird diese Cloud-Infrastruktur entsprechend ErwGr. 12 Cyber Resilience Act nicht unter den Anwendungsbereich des Cyber Resilience Act fallen.

5.2 Anforderungen an Cloud-Nutzer

5.2.1 Cloud-Nutzer im Gesundheitswesen: § 393 SGB V

Mit dem Digital-Gesetz[18] des BMG wurde § 393 SGB V „Cloud-Einsatz im Gesundheitswesen“ eingeführt, der ab 1. Juli 2024 gilt. § 393 SGB V enthält Anforderungen, die alle gesetzlichen Pflege- und Krankenkassen sowie alle Leistungserbringer (also Arztpraxen, Krankenhäuser, Apotheken, häusliche Pflege usw.) bei Nutzung von Cloud-Computing Diensten erbringen müssen.

Cloud-Computing i. S. d § 393 SGB V bedingt fast immer eine Form des Outsourcings. Obwohl § 393 Abs. 1 SGB V eine Erlaubnisnorm darstellt, muss bei der Anwendung der Regelung zunächst beurteilt werden, ob vorrangiges Landesrecht zu beachten ist.

Insbesondere im Bereich des Krankenhausrechts, der Gesetzgebung für den Rettungsdienst wie auch des Heilberuferechts liegen gerade die organisatorischen Gesetzgebungskompetenzen, zu denen auch das Outsourcing zählt, bei den jeweiligen Bundesländern.[19]

Im Falle von vorrangig geltendem Landesrecht muss zunächst geprüft werden, ob das jeweilige Landesrecht ein Outsourcing erlaubt und, sofern dies im Landesrecht gestattet ist, die entsprechend Landesrecht einzuhaltenden Bedingungen auch ein Outsourcing in die avisierte Cloud gestattet. Nur wenn diese Bedingungen erfüllt sind, gelten ergänzend die Regelungen des § 393 SGB V.

5.2.1.1 Normadressaten des § 393 SGB V

§ 393 Abs. 1 SGB V adressiert Leistungserbringer sowie (gesetzliche) Kranken- und Pflegekassen.

Dabei besteht ein Unterschied zwischen den Normadressaten: Mit Kranken- und Pflegekassen wird direkt der rechtsfähige Träger angesprochen, mit Leistungserbringer hingegen die Funktion, die eine natürliche oder juristische Person ausübt. Ein Krankenhaus oder andere entsprechend adressierte

[18] BMG: Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG). Online, zitiert am 2024-06-26; verfügbar unter https://www.bundesgesundheitsministerium.de/ministerium/gesetze-und-verordnungen/guv-20-lp/digig

[19] Siehe z. B.

- Wissenschaftliche Dienste Deutscher Bundestag. (2019) Gesetzgebungskompetenzen im Bereich des Krankenhausrechts. Online, zitiert am 2024-03-21; verfügbar unter https://www.bundestag.de/resource/blob/648488/7920b181e85756ccdedff0334a18145b/WD-3-094-19-pdf-data.pdf
- Wissenschaftliche Dienste Deutscher Bundestag. (2022) Verfassungsrechtlicher Rahmen für die Regelung der stationären medizinischen Versorgung. Online, zitiert am 2024-03-21; verfügbar unter https://www.bundestag.de/resource/blob/899852/e48e78cfe536ee972862bab82b8618e9/WD-3-054-22-pdf-data.pdf
- Wissenschaftliche Dienste Deutscher Bundestag. (2019) Zur Frage der Gesetzgebungskompetenz des Bundes für den Öffentlichen Gesundheitsdienst. Online, zitiert am 2024-03-21; verfügbar unter https://www.bundestag.de/resource/blob/657236/c82ba2db1cd763e2f46439828d73c4e0/WD-9-043-19-pdf-data.pdf

Personen agiert als Leistungserbringer nur dann, wenn es eine entsprechende im SGB enthaltene Aufgabe wahrnimmt, d. h. i. d. R. alles im Kontext der Patientenbehandlung. Juristische Personen wie ein Krankenhaus haben häufig noch andere Aufgaben, z. B. agieren sie auch als Arbeitgeber. Im Kontext dieser nicht vom SGB adressierten Aufgaben sind diese Personen keine Leistungserbringer.

Beispiel:

a) Bei der Verarbeitung von Patientendaten zur Gesundheitsversorgung agiert ein Krankenhaus als Leistungserbringer. Bei der Verarbeitung von Beschäftigtendaten werden u. a. zwar auch Gesundheitsdaten (z. B. bei einer Krankmeldung) verarbeitet, jedoch im Kontext eines Arbeitgebers, nicht jedoch als Leistungserbringer.
b) Eine Krankenkasse verarbeitet Daten von versicherten Personen als Krankenkasse. Aber auch die Daten von beschäftigten Personen werden von der seitens der Norm adressierten Krankenkasse verarbeitet, daher fallen auch die Gesundheitsdaten von Beschäftigten unter den Vorgaben des § 393 SGB V.

Leistungserbringer werden vom § 393 SGB V adressiert, Arbeitgeber hingegen nicht. Bei der Anwendung des § 393 SGB V muss daher bei Leistungserbringer darauf geachtet werden, ob die jeweilige juristische oder natürliche Person Gesundheitsdaten auch als Leistungserbringer in einer Cloud verarbeiten will. Bei der Verarbeitung von Patientendaten wird man immer als Leistungserbringer anzusehen sein, bei der Verarbeitung von Beschäftigtendaten ist dies ggf. anders zu bewerten.

Im Nachfolgenden werden diese Begriffe „Krankenkasse“, „Pflegekasse“ und „Leistungserbringer“ näher betrachtet.

5.2.1.1.1 Krankenkassen

Entsprechend § 4 Abs. 2 SGB V gliedert sich die (gesetzliche) Krankenversicherung in folgende Kassenarten:

- Allgemeine Ortskrankenkassen,
- Betriebskrankenkassen,
- Innungskrankenkassen,
- Sozialversicherung für Landwirtschaft, Forsten und Gartenbau als Träger der Krankenversicherung der Landwirte,
- Deutsche Rentenversicherung Knappschaft-Bahn-See als Träger der Krankenversicherung (Deutsche Rentenversicherung Knappschaft-Bahn-See),
- Ersatzkassen.

Die von § 393 SGB V adressierten Krankenkassen sind daher die in § 4 Abs. 2 SGB V Krankenversicherungen,

5.2.1.1.2 Pflegekassen

Entsprechend § 46 Abs. 1 SGB XI sind die Pflegekassen die Träger der sozialen Pflegeversicherung. Jede der in § 4 Abs. 2 SGB V genannten Krankenkasse muss eine Pflegekasse einrichten (§ 46 Abs. 1 S. 2 SGB XI). Dabei sind die Pflegekassen rechtsfähige Körperschaften des öffentlichen Rechts mit Selbstverwaltung (§ 46 Abs. 2 SGB XI). D. h., Pflegekassen agieren unabhängig von den Krankenkassen, auch wenn Organe der Pflegekassen immer auch zugleich Organe der Krankenkassen, bei denen sie errichtet sind, darstellen.

Die Selbstständigkeit der Pflegekassen wird insbesondere dadurch deutlich, dass sie:[20]

[20] Siehe auch Baier G.: § 46 SGB XI, Rn. 4. In: Krauskopf (Hrsg.) Soziale Krankenversicherung, Pflegeversicherung. Verlag C. H. Beck, 121. Auflage. 2024. ISBN 978-3-406-45832-3

- rechtsfähig und damit selbst Träger von Rechten und Pflichten sind (Abs 2 S 1),
- nach außen unter eigenem Namen und in eigener Verantwortung auftreten,
- eine eigene Satzung haben (§ 47),
- eine gesonderte Haushaltsführung, Rechnungslegung und Rechnungsprüfung haben und damit gegenüber den Krankenkassen finanziell selbstständig und unabhängig sind,
- eigene Geschäftsübersichten und Statistiken erstellen und vorlegen,
- Sozialdaten grundsätzlich getrennt von den Daten der Krankenkasse verarbeiten.

Die Verbände der Pflegekassen werden auf Landesebene von den Landesverbänden der Pflegekassen wahrgenommen (§ 52 Abs. 1 SGB XI); diese Aufgaben nehmen die Landesverbände der entsprechenden Krankenkassen wahr.

Auf Bundesebene nimmt der Spitzenverband Bund der Krankenkassen die Aufgaben des Spitzenverbandes Bund der Pflegekassen wahr (§ 53 SGB XI).

Die von § 393 SGB V adressierten Pflegekassen sind daher die von den Krankenkassen eingerichteten Pflegekassen.

5.2.1.1.3 Leistungserbringer

In den Sozialgesetzbüchern existiert leider keine Begriffsbestimmung des Begriffs „Leistungserbringer“. Allgemein wird unter „Leistungserbringer“ alle diejenigen Gruppierungen zu verstehen sein, die Leistungen für die Versicherten der Krankenkassen erbringen.

Leistungserbringer werden im SGB V insbesondere in nachfolgenden Regelungen angesprochen:
- §§ 72ff. SGB V (Vertragsärzte)
- §§ 107ff. SGB V (Krankenhäuser)
- §§ 124ff. SGB V (Heilmittelerbringer)
- §§ 126 ff. SGB V (Hilfsmittelerbringer)
- §§ 129ff. SGB V (Apotheken und pharmazeutische Unternehmer)
- §§ 132ff. SGB V (sonstige Leistungserbringer).

Die meisten verstehen unter „Leistungserbringer“ Ärzte, sei es im niedergelassenen oder stationären Umfeld. Leistungserbringer werden im Sozialgesetzbuch überwiegend über ihre Beziehung zu den Pflege- und Krankenkassen definiert. Entsprechend den Vorgaben gehören aber viel mehr Personengruppen zu den Leistungserbringern. Nach dem Vierten Kapitel des SGB V zur Versorgung berechtigt sind:[21]
- Viertes Kapitel Zweiter Abschnitt Siebter Titel: §§. 95 SGB V, dies sind
    - Zugelassene Ärzte, Zahnärzte, Psychotherapeuten
    - Medizinische Versorgungszentren sowie
    - Ermächtigte Ärzte, Zahnärzte, Psychotherapeuten und Einrichtungen;
- Viertes Kapitel Dritter Abschnitt; §§ 107 ff. SGB V, dies sind
    - Krankenhäuser,
    - Vorsorge- und Rehaeinrichtungen,
    - Einrichtungen des Müttergenesungswerks oder gleichartige Einrichtungen;
- Viertes Kapitel Fünfter Abschnitt: §§ 124 ff. SGB V, d. h.
    - Leistungserbringer von Heilmitteln (siehe Anhang 1.1);
- Viertes Kapitel Sechster Abschnitt: §§ 126 SGB ff. V, d. h.
    - Leistungserbringer von Hilfsmitteln (siehe Anhang 1.2);

[21] Baumann C, Matthäus D.: § 140a SGB Vm Rn, 83. In: Schlegel/Voelzke (Hrsg.) juris PraxisKommentar SGB V. Juris, 8. Auflage 2022. ISBN 978-3-86330-257-3

- Viertes Kapitel Siebter Abschnitt: §§ 129 ff. SGB V
    - Apotheken,
    - Krankenhausapotheken,
    - Pharmazeutische Unternehmer[22];
- Viertes Kapitel Achter Abschnitt: §§ 132 ff. SGB V
    - Sonstige Leistungserbringer, d. h. Erbringer von
        - Haushaltshilfe,
        - häuslicher Krankenpflege,
        - Soziotherapie,
        - sozialmedizinischen Nachsorgemaßnahmen,
        - spezialisierter ambulanter Palliativversorgung,
        - Schutzimpfungen,
        - Krankentransportleistungen und
        - Hebammenhilfe.

Leistungserbringer i. S. d. § 393 SGB V sind daher diese zur Versorgung gesetzlich versicherter Menschen berechtigte Einrichtungen bzw. Personengruppen.

5.2.1.2 Datenarten

Leistungserbringer sowie (gesetzliche) Kranken- und Pflegekassen sowie ihre jeweiligen Auftragsdatenverarbeiter dürfen Sozialdaten und Gesundheitsdaten unter Nutzung eines Cloud-Computing-Dienstes verarbeiten. Andere Daten wie Beschäftigtendaten oder genetische Daten werden von der Regelung jedoch nicht umfasst.

Insbesondere die fehlende Einbeziehung von Beschäftigtendaten ist ein Hindernis: Damit Gesundheits- und Sozialdaten in der Cloud verarbeitet werden dürfen, ist zwingen eine Authentifizierung der zugreifenden Personen sowie deren Befugnis für die Verarbeitung zu prüfen. D. H. bei Cloud-Computing im Kontext des § 393 SGB V müssen immer auch Beschäftigtendaten verarbeitet werden. Die Erlaubnistatbestände zur Verarbeitung der Beschäftigtendaten richtet sich daher nach dem allgemeinen Datenschutzrecht, d. h. nach den Vorgaben der DS-GVO, ergänzend die Vorgaben der deutschen Gesetzgebung.

Nachfolgend werden in Kürze die Begriffe betrachtet.

5.2.1.2.1 Gesundheitsdaten

Der Begriff „Gesundheitsdaten“ wird in Art. 4 Nr. 15 DS-GVO europaweit legal definiert. Gesundheitsdaten sind „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.

Gesundheitsdaten gehören zu den in Art. 9 Abs. 1 DS-GVO genannten „besonderen Kategorien personenbezogener Daten“, deren Verarbeitung grundsätzlich verboten ist, ausgenommen ein in

[22] Pharmazeutische Unternehmen sind Leistungserbringer im Sinne des SGB V, weil der 7. Abschnitt des Vierten Kapitels ihre Beziehungen zu den Apotheken regelt. So z. B. zu finden in:

- Sodan H. „Handbuch des Krankenversicherungsrechts“: § 13 Leistungserbringung durch Dritte als Folge des Sachleistungsprinzips, Rn. 37, 38. Verlag C. H. Beck, 3. Auflage 2018. ISBN 978-3-406-71288-3
- Zuck R.: § 36 Pharmazeutische Unternehmen, Rn. 2. In: Quaas/Zuck Clemens (Hrsg.) Medizinrecht. Verlag C. H. Beck, 4. Auflage 2018. ISBN 978-3-406-70773-5
- Krauskopf „Soziale Krankenversicherung, Pflegeversicherung“: § 128 SGB V, Rn. 26, 27. Verlag C. H. Beck, 121. Auflage 2024. ISBN 978-3-406-45832-3

Art. 9 Abs. 2 genannter Ausnahmetatbestand erlaubt die Verarbeitung.[23] Entsprechend der Rechtsprechung des EuGH ist die Zuordnung eines Datums als „sensibles Datum" i. S. d. Art. 9 Abs, 1 DS-GVO weit zu verstehen[24]. Auch wenn ein Datum aufgrund der eigenen Bedeutung nach an sich kein sensibles Datum darstellt, ist entsprechend dem Urteil des EuGH zu prüfen, ob „mittels gedanklicher Kombination oder Ableitung" auf diese in Art. 9 Abs. 1 DS-GVO genannten Datenkategorien geschlossen werden kann. Werden in Art. 9 Abs. 1 DS-GVO genannte Datenkategorien mit anderen Daten verknüpft/in Beziehung gebracht, so gilt das Verarbeitungsverbot entsprechend der Rechtsprechung des EuGH für die Gesamtheit dieser Daten.[25]

Aufgrund dieser Vorgaben des EuGH ist der Begriff „Gesundheitsdatum" weit auszulegen. Insbesondere müssen auch indirekt mögliche Aussagen geprüft werden.

> Beispiel: Eine Person besucht eine Arztpraxis. Die Standortdaten, also Straße, Postleitzahl und Ort, der Arztpraxis stellen eigentlich keine sensiblen Daten i. S. v. Art. 9 Abs. 1 DS-GVO dar. Da aber bekannt ist, dass eine Arztpraxis aufgesucht wird und dies i. d. R. für eine medizinische Betreuung erfolgt, ist diese Information damit als sensibles Datum aufzufassen.

5.2.1.2.2 Genetische Daten

Der Begriff „genetische Daten" wird in Art. 4 Nr. 13 DS-GVO europaweit legal definiert. Genetische Daten sind „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 der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden".

Genetische Daten selbst stellen keine Gesundheitsdaten dar, da diese Daten selbst keine direkt verfügbaren Informationen über die Gesundheit einer natürlichen Person beinhalten. Allerdings können genetische Daten Informationen „liefern", welche sich auf die Gesundheit einer natürlichen Person beziehen. Die gelieferten Informationen, die selbst wiederum keine genetischen Daten darstellen, können Gesundheitsdaten i. S. d. Art. 4 Nr. 13 DS-GVO sein.

5.2.1.2.3 Biometrische Daten

Der Begriff „biometrische Daten" wird in Art. 4 Nr. 14 DS-GVO europaweit legal definiert. Biometrische Daten sind „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten".

Biometrische Daten werden häufig als Faktor bei der Identifizierung einer Person genutzt. Beispiele hierfür sind Gesichtserkennung oder Fingerabdruckprüfung. Biometrische Daten gehören zu den in Art. 9 Abs. 1 DS-GVO genannten „besonderer Kategorien personenbezogener Daten", Daten mit besonders hohem Schutzniveau. Der EuGH urteilte hierzu:[26]

> „Art. 9 Abs. 1 DS-GVO verbietet eine Verarbeitung grundsätzlich, versehen mit einer Liste von Ausnahmen des Verbots in Art. 9 Abs. 2 DS-GVO.

[23] EuGH Urt. v. 2023-01-26, Rechtssache C-205/21. Rn. 63. Online, zitiert am 2024-06-26; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0205

[24] EuGH, Urt. v. 2022-08-01, Rechtssache C-92/09, C-93/09, Rn. 119, 120, 125. Online, zitiert am 2024-01-15; verfügbar unter https://dejure.org/2010,236 bzw. Volltext abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1698904362512&uri=CELEX%3A62020CJ0184

[25] EuGH Urt. v. 2023-07-04, Rechtssache C-252/21. Rn. 73. Online, zitiert am 2024-06-26; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252

[26] EuGH Urt. v. 2023-01-26, Rechtssache C-205/21. Rn. 63, 66. Online, zitiert am 2024-06-26; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0205

> Nationale Recht, welches eine Verarbeitung biometrischer und genetischer Daten erlaubt, darf hinsichtlich der für diese Erlaubnis geltenden Voraussetzungen keine Unklarheit enthalten. Die betroffenen Personen und die zuständigen Gerichte müssen nämlich in der Lage sein, insbesondere die Voraussetzungen, unter denen diese Verarbeitung erfolgen kann, sowie die Zwecke, denen sie rechtmäßig dienen kann, genau bestimmen zu können."

Die Verarbeitung biometrischer Daten erfordert daher einen ausdrücklichen gesetzlichen Erlaubnistatbestand, welcher bzgl. der Verarbeitung biometrischer Daten keine Unklarheiten aufweisen darf.

5.2.1.2.4 Sozialdaten

Sozialdaten sind nicht durch europäisches Recht, sondern durch deutsches Recht definiert. Die Begriffsbestimmung findet sich in § 67 Abs. 2 SGB X:

> „Sozialdaten sind personenbezogene Daten (Artikel 4 Nummer 1 der Verordnung (EU) 2016/679), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden. Betriebs- und Geschäftsgeheimnisse sind alle betriebs- oder geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben."

Der Begriff Sozialdaten kann somit alle Formen personenbezogener Daten einbeziehen, einschließlich pseudonymer Daten (Art. 4 Nr. 5 DS-GVO), genetischer Daten (Art. 4 Nr. 13 DS-GVO), biometrischer Daten (Art. 4 Nr. 14 DS-GVO) und Gesundheitsdaten (Art. 4 Nr. 15 DS-GVO).

Damit ein personenbezogenes Datum als Sozialdatum gilt, muss eine einzige Bedingung erfüllt werden: Die Verarbeitung muss von einer in § 35 SGB I genannten Stelle „im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch" durchgeführt werden.

§ 35 SGB I benennt ausschließlich „Leistungsträger". Die zum Sozialdatenschutz verpflichteten Leistungsträger ergeben sich aus § 12 i. V. m. §§ 18-29, d. h. es handelt sich ausschließlich die in den §§ 18-29 SGB I genannten Körperschaften, Anstalten und Behörden. Dies sind:

- Ämter und die Landesämter für Ausbildungsförderung (§ 18 SGB I);
- Agenturen für Arbeit und die sonstigen Dienststellen der Bundesagentur für Arbeit (§§ 19, 19a, 19b SGB I);
- Gesetzliche Krankenversicherung, d. h. Orts-, Betriebs- und Innungskrankenkassen, die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau als landwirtschaftliche Krankenkasse, die Deutsche Rentenversicherung Knappschaft-Bahn-See und die Ersatzkassen (§ 21, 21b SGB I);
- Pflegekassen (§ 21a SGB I);
- Gesetzliche Unfallversicherung, d. h. die gewerblichen Berufsgenossenschaften, die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau als landwirtschaftliche Berufsgenossenschaft, die Gemeindeunfallversicherungsverbände, die Feuerwehr-Unfallkassen, die Unfallkassen der Länder und Gemeinden, die gemeinsamen Unfallkassen für den Landes- und kommunalen Bereich und die Unfallversicherung Bund und Bahn (§ 22 SGB I);
- Gesetzliche Rentenversicherung (§ 23 SGB I);
- Die nach Bundesrecht oder Landesrecht bestimmten Träger der sozialen Entschädigung (§ 24 SGB I);
- Die nach § 7 des Bundeskindergeldgesetzes bestimmten Stellen sowie die für Bundeselterngeld- und Elternzeitgesetzes bestimmten Stellen (§ 25 SGB I);
- Die durch Landesrecht bestimmten für das Wohngeld zuständigen Behörden (§ 26 SGB I);

- Die für die Leistungen der Kinder- und Jugendhilfe zuständigen Kreise und die kreisfreien Städte, nach Maßgabe des Landesrechts auch kreisangehörige Gemeinden (§ 27 SGB I);
- Die für die Leistungen der Sozialhilfe zuständigen reise und kreisfreien Städte, die überörtlichen Träger der Sozialhilfe und für besondere Aufgaben die Gesundheitsämter (§ 28 SGB I);
- Die durch Landesrecht bestimmten für die Leistungen der Eingliederungshilfe zuständigen Behörden (§ 28a SGB I);
- Die für die Leistungen zur Rehabilitation und Teilhabe behinderter Menschen zuständigen und in den §§ 19 bis 24, 27 und 28 g genannten Leistungsträger und die Integrationsämter (§ 29 SGB I).

Entsprechend § 35 Abs. 2 SGB I regeln die Vorschriften des 2. Kapitels SGB X und der übrigen Bücher des Sozialgesetzbuches die Verarbeitung von Sozialdaten abschließend, soweit nicht die DS-GVO unmittelbar gilt. Daher können die in § 35 SGB I genannten Stellen auch mit Einwilligung personenbezogene Daten nur verarbeiten, wenn ihnen dies aufgrund einer (ausdrücklichen) Regelung des Sozialgesetzbuches erlaubt ist.

Leistungserbringer wie Krankenhäuser niedergelassene Arztpraxen, Apotheken, häuslicher Pflegedienst usw. verarbeiten daher **nie** Sozialdaten, da sie zu keiner der in § 35 SGB I genannten Stellen gehören. Erhält ein Leistungserbringer Daten von einem Leistungsträger, so sind die Daten nach Erhalt keine Sozialdaten mehr: Ab Erhalt der Daten verarbeitet ein Leistungserbringer die Daten und entsprechend der gesetzlichen Begriffsbestimmung können die Daten nicht mehr als Sozialdaten gelten, sobald sie unter der Verfügungsgewalt eines Leistungserbringers stehen und somit von diesem und nicht von einem Leistungsträger verarbeitet werden.

5.2.1.3 Ort der Verarbeitung

Diese Anforderungen beinhalten u. a. Vorgaben für die Auswahl des Cloud-Dienstleisters. So darf die Verarbeitung im Wege des Cloud-Computing-Dienstes darf nur im Inland, in einem Mitgliedstaat der Europäischen Union erfolgen. In einem Drittstaat wie den USA oder Japan hingegen nur, wenn für dieses Drittland ein Angemessenheitsbeschluss der EU-Kommission vorliegt.[27]

Speziell beim Angemessenheitsbeschluss der USA ist zu beachten, dass kein Angemessenheitsbeschluss für die USA selbst vorliegt, sondern nur für zertifizierte Unternehmen.[28] Beim Angemessenheitsbeschluss für die USA (EU-US Data Privacy Framework) werden zwei Arten der Selbst-Zertifizierung unterschieden: „Non-HR-Data“ und „HR-Data“. Zum Stand dieser Ausarbeitung existierten bei den nachfolgend genannten amerikanischen Cloud-Anbietern folgende Zertifizierungen:

Cloud-Anbieter	Non-HR-Data	HR Data
Amazon.com, Inc.	Ja	Nein
Apple Inc.	Nein	Nein
Broadcom Inc. (VMWare)	Nein	Nein
Cisco Systems, Inc.	Nein	Nein
Dell Technologies Inc.	Nein	Nein
Dropbox Inc.	Nein	Nein
Google LLC	Ja	Ja

[27] Eine Liste der Angemessenheitsbeschlüsse der EU-Kommission findet man unter https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=de (letzter Abruf der Webseite 2024-06-26)

[28] Siehe Data Privacy Framework List. Online, zitiert am 2024-06-26; verfügbar unter https://www.dataprivacyframework.gov/list

Cloud-Anbieter	Non-HR-Data	HR Data
International Business Machines Corporation (IBM)	Ja	Nein
Microsoft Corporation	Ja	Ja
Oracle America Inc.	Ja	Nein
Oracle (Cerner Corporation)	Ja	Ja
Rackspace Inc.	Nein	Nein
Salesforce	Ja	Ja
ServiceNow, Inc.	Ja	Ja
Snowflake Inc.	Ja	Nein
Workday, Inc.	Ja	Ja

Werden beim Cloud-Einsatz Beschäftigtendaten durch ein amerikanisches Unternehmen verarbeitet (z. B. durch personifizierte Anmeldung an den Cloud-Dienst), so muss nach Ansicht der EU-Kommission[29], des Europäischen Datenschutzausschusses wie auch der deutschen Datenschutz-Konferenz[30] eine „HR-Data"-Zertifizierung vorliegen; die amerikanische Regierung wiederum geht davon aus, dass eine „HR-Data"-Zertifizierung nur erforderlich ist, wenn Daten amerikanischer Unternehmen von europäischen Unternehmen (im Falle der Cloud also von den Cloud-Kunden) verarbeitet werden.[31]

Diese unterschiedliche Sichtweise auf das EU-U.S. Data Privacy Framework führt dazu, dass diverse amerikanische Unternehmen keine Zertifizierung „HR-Data" aufweisen und daher entsprechend den europäischen Vorgaben auch keine Daten von in Europa beschäftigten Personen verarbeiten dürfen.[32] Für die Verarbeitung aller anderen Daten die „Non-HR-Data"-Zertifizierung.

Ob jemand ergänzend zu einer „Non-HR-Data"-Zertifizierung" zur Verarbeitung von Beschäftigtendaten andere Garantien entsprechend der DS-GVO nutzen kann, ist rechtlich mindestens zweifelhaft. In Art. 46 Abs. 1 DS-GVO heißt es:

> „**Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt**, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, […]"

[29] Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA. Anhang I, III. Zusatzgrundsätze, Nr. 6 „Selbstzertifizierung", lit. c. Online, zitiert am 2024-06-26; verfügbar unter https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj?locale=de

[30] Datenschutzkonferenz (DSK): Anwendungshinweis vom 4. September 2023 „Übermittlung personenbezogener Daten aus Europa an die USA", S. 12 Kap. 1.2 „Welche Übermittlungen sind erfasst?" Online, zitiert am 2024-06-26; verfügbar unter https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

[31] U.S. Department of Commerce: FAQs – Privacy Policy, Q7: Are there different requirements under the DPF Principles for non-human resources and human resources privacy policies? Online, zitiert am 2024-06-26; verfügbar unter https://www.dataprivacyframework.gov/program-articles/FAQs%20%E2%80%93%20Privacy-Policy-(6%E2%80%9310)

[32] Sie auch Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg „Tätigkeitsbericht 2023", S. 103, Spalte 2: „Obwohl der Begriff „Beschäftigtendaten" durchaus nahelegt, dass darunter zumindest auch die Daten der Beschäftigten des jeweiligen Datenexporteurs – und gegebenenfalls auch anderer Stellen in der EU – fallen, sind damit nach dem Verständnis der US-Seite nur die Daten der Beschäftigten des jeweiligen Datenimporteurs in den USA gemeint." Online, zitiert am 2024-06-26; verfügbar unter https://www.baden-wuerttemberg.datenschutz.de/taetigkeitsbericht-2023-zukunft-mit-datenschutz-gestalten/ bzw. pdf-Download unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/TB_39_DS_barrierefrei.pdf

Jedoch liegt ein Angemessenheitsbeschluss vor, der für die eigentliche Verarbeitung gilt. Jedoch erstreckt sich der Angemessenheitsbeschluss nicht auf die für die Verarbeitung benötigten Beschäftigtendaten und für eine Verarbeitung zwei Garantien einzusetzen, wovon eine der Angemessenheitsbeschluss ist, dürfte von der Regelung in Art. 46 Abs. 1 DS-GVO vermutlich so nicht vorgesehen sein. Entsprechend der bisherigen Rechtsprechungspraxis des EuGH ist zu vermuten, dass der EuGH eine entsprechende Praxis ablehnt.

Und insbesondere in Fällen, wo im deutschen Recht ausdrücklich ein Angemessenheitsbeschluss gefordert ist (§ 80 SGB X, § 393 SGB V) ist dies auf jeden Fall keine Lösung.

5.2.1.4 TOM entsprechend „Stand der Technik“

Leistungserbringer sowie Kranken- und Pflegekassen müssen nach dem Stand der Technik angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit umgesetzt haben.

Der „Stand der Technik“ wird im § 393 Abs. 5,6 SGB V definiert:

- Für Betreiber einer kritischen Infrastruktur gelten die Anforderungen gemäß BSI-Gesetz.
- Vertragsärztliche und vertragszahnärztliche Versorgung:
  Die in der -vertragsärztlichen und vertragszahnärztlichen Versorgung tätigen Arztpraxen müssen die Richtlinie der Kassenärztlichen Bundesvereinigungen einhalten. Die ergriffenen technischen und organisatorischen Maßnahmen müssen auch beim Einsatz von Cloud-Computing-Diensten die IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung gewährleisten.
- Krankenhäuser:
  Krankenhäuser müssen die Vorgaben von § 391 SGB V auch bei Nutzung von Cloud Computing-Diensten einhalten, d. h. insbesondere müssen die Anforderungen hinsichtlich der angemessenen technischen und organisatorischen Maßnahmen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit die Cloud Computing-Dienste berücksichtigen und eine entsprechende IT-Sicherheit gewährleistet werden.
- Gesetzliche Krankenkassen bzw. B3S[33]-GKV/PV
  Krankenkassen müssen die Vorgaben des § 392 SGB V auch beim Einsatz von Cloud-Computing-Diensten gewährleisten. D. h. die angemessenen technischen und organisatorischen Maßnahmen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit müssen die Cloud-Computing-Dienste einbeziehen.
- Alle anderen:
  Alle anderen Leistungserbringer wie z. B. Apotheken oder Anbieter von häuslicher Pflege müssen zu § 391 SGB V gleichwertige Anforderungen erfüllen.

5.2.1.5 BSI C5-Testat erforderlich

Gesetzliche Kranken- und Pflegekassen sowie Leistungserbringer dürfen nur Cloud-Computing-Dienste einsetzen, bei denen ein „aktuelles“ C5-Testat[34] entsprechend der Vorgaben des BSI vorliegt.

[33] B3S = Branchenspezifischen Sicherheitsstandard. Liste der verfügbaren Standards siehe BSI: Übersicht der Branchenspezifischen Sicherheitsstandards (B3S). Online, zitiert am 2024-06-26; verfügbar unter https://www.bsi.bund.de/dok/b3s-uebersicht

[34] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kriterienkatalog Cloud Computing C5. Online, zitiert am 2024-06-26; verfügbar unter https://www.bsi.bund.de/dok/7685384

5.2.1.5.1 Vorgaben IDW

Das Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW) aktualisierte die Hinweise für Wirtschaftsprüfer bzgl. Cloud („Prüfung von Cloud-Diensten“, IDW PH 9.860.3[35]) im November 2021 aufgrund der Aktualisierung des C5-Kataloges durch das BSI.

IDW PH 9.860.3 Anlage 1 („Ziele und Basiskriterien oder Zusatzkriterien des BSI C5:2020 bzw. Anforderungen für die Prüfung von Cloud-Diensten sowie beispielhafte Prüfungshandlungen“) enthält Vorgaben, wie ein Wirtschaftsprüfer einen Cloud-Anbieter hinsichtlich der Einhaltung der C5-Kriterien prüfen soll.

5.2.1.5.2 Art des Testats

Entsprechend § 393 Abs. 4 SGB V reicht bis zum 30. Juni 2025 in C5-Typ1-Testat., ab dem 1. Juli 2025 gilt als aktuelles C5-Testat im Sinne des § 393 Abs. 3 Nr. 2 SGB V nur noch ein C5-Typ2-Testat.

Typ1 und Typ2 stellen entsprechend der Darstellung des BSI unterschiedliche Berichtweisen dar:[36]

- „Berichterstattungen vom Typ 1: Der Auditor gibt ein Prüfungsurteil darüber ab, ob die Kontrollen zum Zeitpunkt der Prüfung angemessen ausgestaltet und eingerichtet sind, um die Kriterien des C5 mit hinreichender Sicherheit zu erfüllen (englisch: „suitability of the design“).“
- „Berichterstattungen vom Typ 2: Neben der Aussage zur Angemessenheit, umfasst das Prüfungsurteil eine Aussage über die Wirksamkeit der Kontrollen in einem Prüfungszeitraum (englisch: „operating effectiveness“).“

D. h. ein Typ1-Testat beinhaltet nicht einmal die Ergebnisse einer Prüfung der Wirksamkeit der getroffenen Maßnahmen. Das BSI schreibt hierzu:[36]

> „Insbesondere bei der Nachweiserbringung werden die Unterschiede deutlich: Bei einer Prüfung für Typ 1 werden nur exemplarische Nachweise über die Einrichtung der Kontrollen erbracht. Beim Typ 2 hingegen wird die wirksame Anwendung bzw. Durchführung der Kontrollen über den gesamten Prüfungszeitraum, der typischerweise 6 oder 12 Monate beträgt, nachgewiesen. […]
>
> Nach Auffassung des BSI ist eine Wirksamkeitsprüfung (Typ 2) erforderlich, um eine angemessene Aussagekraft zu erzielen.“

Art. 28 Abs. 1 DS-GVO verlangt, dass ein Verantwortliche nur mit Auftragsverarbeitern zusammenarbeitet, die hinreichend Garantien bieten; ein Typ1-Testat bietet keinerlei Garantien, genügt daher nicht den Anforderungen von Art. 28 Abs. 1 DS-GVO. Der Verantwortliche muss den Nachweis, dass er einen Auftragsverarbeiter auswählte, welcher geeignete technische und organisatorische Maßnahmen zur Einhaltung der DS-GVO gewährleistet, unabhängig vom Vorliegen eines Typ1-Testates führen müssen.

5.2.1.5.3 Aktuelles Testat

Ein Testat entspricht in diesem Fall einem Bestätigungsvermerk § 322 HGB, d. h. es wird bestätigt, dass zu dem im Testat angegebenen Datum die im Testat bescheinigten Vorgaben erfüllt wurden. Ein Testat

---

[35] IDW Prüfungshinweis: Die Prüfung von Cloud-Diensten (IDW PH 9.860.3). Online, zitiert am 2024-06-26; verfügbar unter

- Presseerklärung IDW: https://www.idw.de/idw/idw-aktuell/idw-ph-9-860-3-fuer-pruefungen-von-cloud-diensten
- Katalog bei Beck: https://beck-online.beck.de/Bcid/Y-400-W-IDWPS-GL-ph-9-860-3

[36] Bundesamt für Sicherheit in der Informationstechnik (BSI): C5 - Informationen für Prüfer, Abschnitt „Zugrundeliegende Prüfungsmethodik“. Online, zitiert am 2024-06-26; verfügbar unter https://www.bsi.bund.de/dok/13447954

erlaubt keine Aussagen, ob die Vorgaben zu einem späteren Datum noch erfüllt sind. Weiterhin besitzt ein Testat eines Wirtschaftsprüfers im Gegensatz zu einem Zertifikat kein Ablaufdatum. Das „aktuelle“ Testat ist also das letzte Testat, welches den Eigenschaften des testierten Gegenstandes/Dienstes entspricht – egal ob es vor 2 Monaten oder 10 Jahren ausgestellt wurde.

5.2.1.5.4 C5-Anforderungen an den Cloud-Kunden

Entsprechend BSI C5 Kriterienkatalog (Kapitel 2.1) sollen Cloud-Anbieter Kunden bei der Identifizierung dieser korrespondierenden Kriterien für Kunden unterstützen, indem diese Kriterien bei der Erstellung der Systembeschreibung identifiziert und benannt werden. Für Prüfer fordert der BSI C5 Kriterienkatalog (Kapitel 2.1), dass diese die Angemessenheit der Angaben zu den korrespondierenden Kontrollen zu beurteilen.

Entsprechend § 393 Abs. 3 Nr. 3 SGB V muss vom Cloud-Kunden nachgewiesen werden, dass die „im Prüfbericht des Testats enthaltenen, korrespondierenden Kriterien für Kunden umgesetzt sind“. Daher müssen Kunden bei Vorlage eines Testas prüfen, welche der korrespondierenden Kriterien von ihnen umzusetzen sind. Findet man im Testat keine entsprechenden Angaben, sollte man den Cloud-Anbieter ansprechen und eine schriftliche (Nachweispflicht) Darstellung verlangen, welche korrespondierende Kontrollen auf Seiten der Kunden beim entsprechenden Cloud-Computing-Dienst seitens des Cloud-Anbieters vorausgesetzt werden.

Korrespondierenden Kriterien für Kunden werden im BSI C5 Kriterienkatalog Stand 2020 an folgenden Stellen benannt:

1) OIS-03 Schnittstellen und Abhängigkeiten:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass Richtlinien und Vorgaben zur Einhaltung vertraglich festgehaltener Vereinbarungen mit dem Cloud-Anbieter bezüglich Verantwortlichkeiten, Mitwirkungspflichten sowie Schnittstellen zum Melden von Sicherheitsvorfällen angemessen definiert, dokumentiert und eingerichtet sind.
2) AM-06 Klassifizierung und Kennzeichnung von Assets:
    - Cloud-Kunden können durch geeignete Kontrollen sicherstellen, dass der Schutzbedarf der Informationen, die mit dem Cloud-Dienst verarbeitet oder gespeichert werden dürfen, angemessen ermittelt wird.
    - Cloud-Kunden können zudem durch geeignete Kontrollen sicherstellen, dass die mit dem Cloud-Dienst verarbeiteten oder gespeicherten Informationen gemäß ihrem Schutzbedarf vor Manipulieren, Kopieren, Modifizieren, Umleiten oder Löschen geschützt sind.
3) OPS-02 Kapazitätsmanagement – Überwachung:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die mit dem Cloud-Anbieter vertraglich getroffenen Vereinbarungen zum Bereitstellen von Ressourcen bzw. der zu erbringenden Leistungen überwacht werden können. Im Falle von Abweichungen stellen geeignete Kontrollen eine Information des Cloud-Anbieters sicher, sodass der Cloud-Anbieter geeignete Maßnahmen einleiten kann.
4) OPS-03 Kapazitätsmanagement – Steuerung von Ressourcen:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie die Systemressourcen in ihrem Verantwortungsbereich steuern und überwachen.
5) OPS-05 Schutz vor Schadprogrammen – Umsetzung:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass jene Ebenen des Cloud-Dienstes, die unter ihrer Verantwortung stehen, mit Sicherheitsprodukten zur Erkennung und Beseitigung von Schadprogrammen versehen sind.
6) OPS-06 Vorgaben zur Datensicherung und Wiederherstellung – Konzept:

- Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die vertraglichen Vereinbarungen, welche mit dem Cloud-Anbieter bezüglich Umfang, Häufigkeit und Dauer der Aufbewahrung der Daten getroffen werden, den geschäftlichen Anforderungen entsprechen. Die geschäftlichen Anforderungen werden im Rahmen der Business Impact Analyse erhoben (vgl. BCM-02).

7) OPS-07 Datensicherung und Wiederherstellung – Überwachung:
   - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Datensicherung der in ihren Verantwortungsbereich fallenden Daten durch technische und organisatorische Maßnahmen überwacht wird.
8) OPS-10 Protokollierung und Überwachung – Konzept:
   - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass für jene Ebenen des Cloud-Dienstes, die unter ihrer Verantwortung stehen, eine angemessene Protokollierung und Überwachung von Ereignissen erfolgt, welche die Sicherheit und Verfügbarkeit des Cloud-Dienstes beeinträchtigen können (z. B. Administratoraktivitäten, Systemfehler, Authentifizierungsprüfungen, Datenlöschungen etc.).
9) OPS-15 Protokollierung und Überwachung – Zurechenbarkeit
   - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass eindeutige Benutzerkennungen vergeben werden, die im Falle eines Sicherheitsvorfalls eine entsprechende Analyse zulassen.
10) OPS-18 Umgang mit Schwachstellen, Störungen und Fehlern – Konzept:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie Systemkomponenten in ihrem Verantwortungsbereich regelmäßig auf Schwachstellen überprüfen und diese durch geeignete Maßnahmen adressieren.
11) OPS-21 Einbindung des Cloud-Kunden bei Störungen (Incidents)
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie Benachrichtigungen des Cloud-Anbieters bezüglich sie betreffender Störungen erhalten, und dass diese Benachrichtigungen zeitnah an die für die Bearbeitung verantwortliche Stelle des Cloud-Anbieters weitergeleitet werden, sodass eine angemessene Reaktion erfolgen kann.
12) OPS-22 Prüfung und Dokumentation offener Schwachstellen:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher jene Systemkomponenten, die unter ihrer Verantwortung stehen, regelmäßig auf Schwachstellen zu überprüfen und diese durch geeignete Maßnahmen zu adressieren.
13) OPS-23 Umgang mit Schwachstellen, Störungen und Fehlern – System-Härtung:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, jene Ebenen des Cloud-Dienstes, die unter ihrer Verantwortung stehen, gemäß allgemein etablierter und akzeptierter Industriestandards zu härten. Die angewendeten Härtungsmaßnahmen resultieren aus einer Risikobeurteilung der geplanten Nutzung des Cloud-Dienstes.
14) OPS-24 Separierung der Datenbestände in der Cloud-Infrastruktur:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die vom Cloud-Dienst bereitgestellten Funktionen zur Segregation gemeinsam genutzter virtueller und physischer Ressourcen so genutzt werden, dass Risiken mit Bezug zur Segregation entsprechend dem Schutzbedarf der Daten hinreichend adressiert sind.
15) CRY-02 Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung):
    - Cloud-Kunden stellen durch geeignete Kontrollen für jene Teile des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen, sicher, dass ihre Daten gemäß dem jeweiligen Schutzbedarf über verschlüsselte Verbindungen übertragen werden.
16) CRY-03 Verschlüsselung von sensiblen Daten bei der Speicherung:

- Cloud-Kunden stellen durch geeignete Kontrollen für jene Teile des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen (z. B. virtuelle Maschinen innerhalb einer IaaS-Lösung), sicher, dass ihre Daten bei der Speicherung gemäß dem jeweiligen Schutzbedarf verschlüsselt werden.

17) COS-01 Technische Schutzmaßnahmen:
    - Cloud-Kunden stellen durch geeignete Kontrollen für jene Teile des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen (z. B. virtuelle Maschinen innerhalb einer IaaS-Lösung), sicher, dass sie netzbasierte Angriffe auf Basis anomaler Eingangs- und Ausgangs-Traffic Muster (z. B. durch MAC-Spoofing und ARP-Poisoning-Angriffe) und/oder Distributed-Denial-of-Service (DDoS) Angriffe zeitnah erkennen und auf diese reagieren.
18) COS-03 Überwachung von Verbindungen im Netz des Cloud-Anbieters:
    - Cloud-Kunden stellen durch geeignete Kontrollen für die virtuellen Netze innerhalb des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen, sicher, dass diese gemäß ihren Netzsicherheitsanforderungen konzipiert, konfiguriert und dokumentiert sind (z. B. logische Segmentierung der Organisationseinheiten des Cloud-Kunden).
19) COS-04 Netzübergreifende Zugriffe:
    - Cloud-Kunden stellen durch geeignete Kontrollen für die Perimeter der virtuellen Netze innerhalb des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen, sicher, dass der Zugriff durch Sicherheitsgateways gemäß seines Schutzbedarfs kontrolliert wird.
20) COS-06 Segregation des Datenverkehrs in gemeinsam genutzten Netzumgebungen:
    - Cloud-Kunden stellen durch geeignete Kontrollen für den Datenverkehr und die virtuellen Netze innerhalb des Cloud-Dienstes, die in ihrem Verantwortungsbereich liegen, sicher, dass diese gemäß ihren Netzsicherheitsanforderungen konzipiert, konfiguriert und dokumentiert sind (z. B. logische Segmentierung der Organisationseinheiten der Cloud-Kunden).
21) COS-08 Richtlinien zur Datenübertragung:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die an den Cloud-Dienst übertragenen Daten gemäß ihrem Schutzbedarf vor Manipulieren, Kopieren, Modifizieren, Umleiten oder Löschen geschützt sind.
22) PI-01 Dokumentation und Sicherheit der Eingangs- und Ausgangs-Schnittstellen:
    - Der Kunde muss durch geeignete Kontrollen vor Beginn der Nutzung des Cloud-Dienstes und bei jeder Änderung der Schnittstellen sicherstellen, dass die bereitgestellten Schnittstellen (und deren Sicherheit) entsprechend seines Schutzbedarfs angemessen sind.
23) PI-02 Vertragliche Vereinbarungen zur Bereitstellung von Daten:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, die ihnen vertraglich zustehenden Daten beim Cloud-Anbieter am Vertragsende anzufragen oder über definierte Schnittstellen abzurufen (Art und Umfang der Daten entsprechen den vertraglichen Vereinbarungen, die vor Nutzung des Cloud-Dienstes festgelegt wurden) und für eine Aufbewahrung gemäß der für diese Daten geltenden gesetzlichen Anforderungen zu sorgen.
24) PI-03 Sichere Datenlöschung:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die rechtlichen und regulatorischen Rahmenbedingungen (z. B. gesetzliche Anforderungen an Aufbewahrung und Löschung) identifiziert sind und die Löschung ihrer Daten entsprechend initiiert wird.
25) DEV-06 Testen der Änderungen:

- Soweit Änderungen gemäß den vertraglichen Vereinbarungen vor der Bereitstellung in der Produktivumgebung durch die Cloud-Kunden zu testen sind, stellen diese durch geeignete Kontrollen sicher, dass die Tests angemessen durchgeführt werden, um Fehler zu identifizieren. Dies umfasst insbesondere die zeitgerechte Durchführung der Tests durch qualifiziertes Personal gemäß der vom Cloud-Anbieter vorgegebenen Rahmenbedingungen.

26) DEV-09 Freigaben zur Bereitstellung in der Produktionsumgebung:
    - Soweit Änderungen gemäß den vertraglichen Vereinbarungen vor der Bereitstellung in der Produktivumgebung durch die Cloud-Kunden freizugeben sind, stellen diese durch geeignete Kontrollen sicher, dass autorisiertes und qualifiziertes Personal die bereitgestellten Informationen entgegennimmt, die Auswirkungen im Rahmen des ISMS bewertet und gemäß der vom Cloud-Anbieter vorgegebenen Rahmenbedingungen über die Freigabe entscheidet.
27) SSO-04 Überwachung der Einhaltung der Anforderungen:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie sich über Subdienstleister ihres Cloud-Anbieters informieren (z. B. anhand der Angaben im C5-Prüfbericht) und anhand des Schutzbedarfs ihrer im Cloud-Dienst verarbeiteten und gespeicherten Daten entscheiden, ob weitergehende eigene Maßnahmen zur Überwachung und Überprüfung dieser Subdienstleister durchzuführen sind.
28) SIM-01 Richtlinie für den Umgang mit Sicherheitsvorfällen:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie Benachrichtigungen des Cloud-Anbieters bezüglich sie betreffender Sicherheitsvorfälle erhalten, und dass diese Benachrichtigungen zeitnah an die für die Bearbeitung verantwortliche Stelle weitergeleitet werden, sodass eine angemessene Reaktion erfolgen kann.
29) SIM-03 Dokumentation und Berichterstattung über Sicherheitsvorfälle:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie Benachrichtigungen des Cloud-Anbieters bezüglich sie betreffender Sicherheitsvorfälle sowie deren Lösung erhalten, und dass diese Benachrichtigungen zeitnah an die für die Bearbeitung verantwortliche Stelle weitergeleitet werden, sodass eine angemessene Reaktion erfolgen kann.

30) SIM-04 Verpflichtung der Nutzer zur Meldung von Sicherheitsvorfällen an eine zentrale Stelle:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass identifizierte Sicherheitsereignisse, deren Bearbeitung im Verantwortungsbereich des Cloud-Anbieters liegt, zeitnah an eine zuvor benannte zentrale Stelle gemeldet werden. Die Identifikation solche Sicherheitsereignisse wird durch geeignete Kontrollen unterstützt (vgl. korrespondierendes Kriterium zu OPS-10).
31) SIM-05 Auswertung und Lernprozess:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie die Erkenntnisse aus vergangenen Sicherheitsvorfällen, die Ihnen mitgeteilt wurden, und die daraus resultierenden Maßnahmen des Cloud-Anbieters in Ihr ISMS aufnehmen und bewerten, ob und wenn ja welche Maßnahmen sie auf ihrer Seite unterstützend ergreifen können.
32) BCM-02 Richtlinien und Verfahren zur Business Impact Analyse:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Szenarien für einen Ausfall des Cloud-Dienstes bzw. des Cloud-Anbieters im Rahmen ihrer Business Impact Analyse hinreichend berücksichtigt werden.
33) BCM-03 Planung der Betriebskontinuität:

- Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass bei der Planung der betrieblichen Kontinuität und des Geschäftsplans, die Ergebnisse der Business Impact Analyse hinreichend berücksichtigt werden, um für die Auswirkungen eines Ausfalls des Cloud-Dienstes bzw. des Cloud-Anbieters vorzusorgen.
- Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Verfügbarkeit des Cloud-Dienstes, seine Wiederherstellungszeit gemäß BCM-Plan sowie des Datenverlusts des Cloud-Dienstes mit ihren eigenen Verfügbarkeitsanforderungen und tolerierbarem Datenverlust im Einklang ist.

34) BCM-04 Verifizierung, Aktualisierung und Test der Betriebskontinuität:
- Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Maßnahmen zur Vorsorge der Auswirkungen eines Ausfalls des Cloud-Dienstes bzw. des Cloud-Anbieters regelmäßig überprüft, aktualisiert, getestet und geübt werden. Der Cloud-Anbieter wird gemäß den vertraglichen Vereinbarungen in die Tests und Übungen eingebunden.
- Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Ergebnisse der BCM-Tests und Übungen des Cloud-Anbieters in das eigene BCM einfließen und hinsichtlich der Sicherstellung der betrieblichen Kontinuität des Kunden umfassend gewürdigt werden.
- Bei Tests und Übungen, die den Kunden mit einbeziehen und daher eigene Maßnahmen auf Kundenseite bedingen, stellen Cloud-Kunden durch geeignete Kontrollen aus ihrem BCM sicher, dass die entsprechenden Maßnahmen zur Bewältigung gemäß Szenario geübt und getestet werden.

35) COM-02 Richtlinie für die Planung und Durchführung von Audits:
- Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass auf Störungen des Cloud-Dienstes durch solche Audits angemessen reagiert wird.
- Soweit vertraglich zugesicherte Informations- und Prüfrechte vorliegen, stellen Cloud-Kunden durch geeignete Kontrollen sicher, dass diese Rechte gemäß eigenen Anforderungen ausgestaltet und wahrgenommen werden.

36) INQ-01 Juristische Beurteilung von Ermittlungsanfragen:
- Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass Art und Umfang staatlicher Ermittlungsanfragen und der damit einhergehenden Offenlegung eigener Daten, im eigenen Risikomanagement behandelt wurde und die Nutzung des Cloud-Dienstes erst stattfindet, wenn dieses Risiko als tragbar erachtet wurde.

37) INQ-02 Information der Cloud-Kunden über Ermittlungsanfragen:
- Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass derartige Meldungen entgegengenommen und gemäß eigenen Vorgaben und Möglichkeiten rechtlich geprüft werden.

38) PSS-01 Leitlinien und Empfehlungen für Cloud-Kunden:
- Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass aus den Informationen des Cloud-Anbieters Richtlinien, Konzepte und Maßnahmen zur angemessen sicheren Konfiguration und Nutzung (gemäß eigener Risikobewertung) des Cloud-Dienstes abgeleitet und eingehalten werden. Änderungen in den Informationen werden zeitnah auf ihre Auswirkung in diesen Dokumenten hin bewertet und ggf. notwendige Änderungen umgesetzt.

39) PSS-03 Online-Register bekannter Schwachstellen:
- Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Informationen dieses Registers gemäß eigenen Anforderungen hinreichend schnell in das eigene Risikomanagement aufgenommen, bewertet und ggf. eigene Maßnahmen im eigenen Verantwortungsbereich ergriffen werden.

40) PSS-04 Fehlerbehandlungs- und Protokollierungsmechanismen:
    - Sofern der Cloud-Dienst mit Fehlerbehandlungs- und Protokollierungsmechanismen ausgestattet ist, müssen Cloud-Kunden diese aktivieren und gemäß definierten Anforderungen konfigurieren. Hierzu hat der Cloud-Kunde das eigene Informationssicherheits-Management geeignet einzubinden.
41) PSS-05 Authentisierungsmechanismen:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die vom Cloud-Dienst angebotenen Authentisierungsmechanismen gemäß Vorgaben des Identitäts- und Berechtigungsmanagement des Kunden genutzt werden.
42) PSS-06 Session Management:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie die Schutzfunktionen des Session Managements des Cloud-Dienstes gemäß den Vorgaben aus ihrem eigenen ISMS nutzen. Außerdem legen sie die Zeitspanne, nach der eine Session ungültig wird, nach den Vorgaben aus ihrem eigenen ISMS fest.
43) PSS-07 Vertraulichkeit von Authentisierungsinformationen:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass gemäß eigener Bewertung hinreichend sichere Passwörter (vgl. IDM-09) verwendet werden und dass die mit der eigenen Wahl verbundenen Risiken eines unautorisierten Zugriffs getragen werden.
44) PSS-08 Rollen- und Rechtekonzept:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass:
        - die Vergabe von Berechtigungen an Benutzer in ihrem Verantwortungsbereich einer Autorisierung unterliegt.
        - die Angemessenheit der vergebenen Berechtigungen regelmäßig überprüft wird und Berechtigungen bei notwendigen Änderungen (zum Beispiel Mitarbeiter-Austritt) zeitgerecht angepasst oder entzogen werden.
45) PSS-11 Images für virtuelle Maschinen und Container:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass die Images von virtuellen Maschinen oder Containern, die sie mit dem Cloud-Dienst betreiben, den Vorgaben ihres Informationssicherheitsmanagements entsprechen und dass die Ergebnisse der Integritätsprüfung beim Start und zur Laufzeit entsprechend dieser Vorgaben verarbeitet werden.
46) PSS-12 Lokationen der Datenverarbeitung und -speicherung:
    - Cloud-Kunden stellen durch geeignete Kontrollen sicher, dass sie sich im Zuge der Dienstleister-Auswahl sowie beim Konfigurieren des Cloud-Dienstes über die Lokationen der Datenverarbeitung sowie -speicherung informieren und, wenn die Wahl zwischen verschiedenen Lokationen besteht, diejenigen auswählen, die den eigenen Anforderungen entsprechen.
    - Je nach Anwendungsbereich und insbesondere bei einer Nutzung angebotener Dienste des Cloud-Anbieters außerhalb ihres Landes, berücksichtigen Cloud-Kunden bei der Auswahl auch die für sie geltenden Gesetze (zum Beispiel bei der Verarbeitung personenbezogener Daten; Einhaltung der gesetzlichen Aufbewahrungspflichten für Geschäftsunterlagen etc.).

6 Empfehlungen

6.1 Anbieter von Diensten

Anbieter von entsprechenden Diensten sollten prüfen, ob der von ihnen angebotene Dienst ein Cloud-Computing-Dienst i. S. d. europäischen Cloud-Definition darstellt oder nicht.

Entspricht der Dienst nicht der Begriffsbestimmung und der Dienst wird als „Cloud-Computing-Dienst beworben, ohne dass den rechtlichen Anforderungen entsprochen wird, stellt dies regelhaft einen Verstoß gegen Treu und Glauben da. Kunden können den Dienst kündigen, bei Schadensvorfällen bei Kunden drohen dem Anbieter Haftungsprobleme aufgrund der Täuschung.

Entspricht der Dienst der Begriffsbestimmung, so müssen alle gesetzlichen Anforderungen an einen Cloud-Computing-Dienst erfüllt werden. Der entsprechende Anbieter sollte die nationalen Umsetzungen verfolgen, da z. B. zur Erfüllung von Meldepflichten die entsprechenden Stellen bekannt sein müssen.

Insbesondere sollten entsprechende Anbieter die Aktivitäten der EU-Kommission hinsichtlich Umsetzung der Vorgaben der NIS-2-Richtlinie verfolgen. Voraussichtlich werden ihnen aus den Vorgaben der EU-Kommission schon ab Oktober 2024 neue rechtliche Anforderungen bezüglich zu ergreifender Maßnahmen erwachsen.

Bei allem sollte man bedenken, dass natürlich die Nachweisplichten gelten und Verstöße u. a. auch durch Bußgeld sanktioniert werden können.

6.2 Cloud-Kunden

Unternehmen, die in der Vergangenheit einen Cloud-Dienst einkauften und seitdem nutzen, sollten prüfen, ob der eingekaufte Dienst der gesetzlichen Begriffsbestimmung des „Cloud-Computing“ entspricht. Ist dies nicht der Fall, sollten die betreffenden Unternehmen überlegen, ob man aufgrund der fehlenden Übereinstimmung mit der gesetzlichen Begriffsbestimmung die Namenskonventionen des eingekauften Dienstes zusammen mit dem Anbieter anpasst und „Cloud“ entfernt; sowohl für Anwender wie Hersteller resultieren schließlich Anforderungen bei einem Cloud-Computing-Dienst, die erfüllt werden müssen.

Bei neu eingekauften Diensten sollten insbesondere Kranken- und Pflegekassen sowie Leistungserbringer im Gesundheitswesen die verpflichtenden Vorgaben von § 393 SGB V beachten. Dazu gehört, dass sich ein Kunde von seinem Anbieter das C5-Testat nicht nur zeigen, sondern auch als Kopie aushändigen lässt; man muss schließlich bei einer Prüfung jederzeit das aktuelle Testat „vorliegen“ haben.

Ein C5-Typ1-Testat entspricht nicht den Anforderungen von Art. 28 Abs. 1 DS-GVO, daher muss sich ein Verantwortlicher auf anderem Weg von der Eignung des Anbieters überzeugen. Verpflichtender Bestanteil im BSI C5-Katalog (OIS-01) ist, dass ein Cloud-Anbieter ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 betreibt. Hier kann man sich das Prüfergebnis der letzten Zertifizierung vorzeigen lassen und prüfen, ob a) der Fokus des Zertifikats den eingekauften Dienst einschließt und b) keine Beanstandungen vorhanden sind, welche ein Sicherheitsrisiko für den verantwortlichen darstellen.

Weiterhin muss die Ortseinschränkung in § 393 Abs. 2 SGB V beachtet werden. BSI C5 verlangt (BC-01), dass Angaben zu Verarbeitungslokalisationen existieren, sodass die Einhaltung der gesetzlichen Vorgabe geprüft werden kann; vertragliche Zusicherungen sollten natürlich ebenfalls existieren.

7 Abkürzungen

Abs.	Absatz
Art.	Artikel
B3S	Branchenspezifischen Sicherheitsstandard
BDSG	Bundesdatenschutzgesetz
BMG	Bundesministerium für Gesundheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG-E	Entwurf des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG) (Art. 1 RefE NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)
BVerfG	Bundesverfassungsgericht
C5	Cloud Computing Compliance Criteria Catalogue
CaaS	Communications as a Service
CompaaS	Compute as a Service
DSaaS	Data storage as a Service
DS-GVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
DSK	Datenschutzkonferenz
EDPB	European Data Protection Board
EDSA	Europäischer Datenschutzausschuss
ENISA	Agentur der Europäischen Union für Cybersicherheit (European Union Agency for Cybersecurity)
ErwGr.	Erwägungsgrund/Erwägungsgründe
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GKV	Gesetzliche Krankenversicherung
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.
HR	Human Resources
Hs.	Halbsatz
IaaS	Infrastructure as a Service
i. d. R.	in der Regel
IDW	Institut der Wirtschaftsprüfer
i. S.	im Sinne
i. S. d.	Im Sinne des/der
i. S. d.	im Sinne der/des
i. V. m.	in Verbindung mit
i.S.v.	im Sinne von
IT	Informationstechnik, informationstechnisches…
Kap.	Kapitel
lit.	littera (lat. „Buchstabe“)
NaaS	Network as a Service
Nr.	Nummer
PaaS	Platform as a Service
PV	Pflegezusatzversicherung
RefE	Referentenentwurf
RL	Richtlinie
Rn.	Randnummer
S.	Satz

SaaS	Software as a Service
SGB	Sozialgesetzbuch
TOM	Technische und organisatorische Maßnahmen
Unterabs.	Unterabsatz
Urt.	Urteil
USA	Vereinigte Staaten von Amerika (engl. United States of America)
u. U.	unter Umständen
vgl.	vergleiche
VO	Verordnung
Ziff.	Ziffer

8 Literatur

8.1 Normen

- ISO/IEC 22123-1:2023-02 „Cloud Computing - Teil 1: Terminologie“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/82758.html
- ISO/IEC 22123-2:2023 „Cloud computingPart 2: Concepts“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/80351.html
- ISO/IEC 22123-3:2023 „Cloud computingPart 3: Reference architecture“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/82759.html
- ISO/IEC 27001:2022 „Information security management systems — Requirements“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/27001
- ISO/IEC 27002:2022 „Information security controls“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/75652.html
- ISO/IEC 27017:2015 „Code of practice for information security controls based on ISO/IEC 27002 for cloud services“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/43757.html
- ISO/IEC 27018:2019 „Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/76559.html
- ISO/IEC 27036-4:2016 „Information security for supplier relationships. Part 4: Guidelines for security of cloud services“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/search.html?PROD_isoorg_en%5Bquery%5D=27036
- ISO 27799:2016 „Information security management in health using ISO/IEC 27002“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/62777.html
- ISO/IEC TR 3445:2022 „Cloud computing — Audit of cloud services“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/79582.html
- ISO/TR 21332:2021 „Cloud computing considerations for the security and privacy of health information systems“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/70568.html
- ISO/TS 11633-1:2019 „Information security management for remote maintenance of medical devices and medical information systems. Part 1: Requirements and risk analysis“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/69336.html
- ISO/TR 11633-2:2021 „Information security management for remote maintenance of medical devices and medical information systems. Part 2: Implementation of an information security management system (ISMS)“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/78861.html
- ISO/TS 23535:2022 „Requirements for customer-oriented health cloud service agreements“. Online, zitiert am 2024-06-26; verfügbar unter https://www.iso.org/standard/75957.html

8.2 Zeitschriften

- Bomhard D. (2024) Auswirkungen des Data Act auf die Geschäftsmodelle von Cloud-Anbietern. Abbau von Wechselbarrieren. MMR: 109-112
- Falk M, Dolle W. (2024) Herausforderungen bei der effizienten Umsetzung von NIS-2. NIS-2 im Spannungsfeld fehlender nationaler Umsetzungsvorgaben und der Notwendigkeit für pragmatische Verbesserungen des Cyber-Risikos. WPg: 337-343
- Hartl K, Vogel P. (2024) Data Act und Legal Tech. LTZ: 104-110
- Heinzke, P. (2024) Data Act: Neue Regeln für Cloud-Service-Provider. Betriebs-Berater: 1291-1296
- Kraul T, Schmidt JP. (2023) Plattformregulierung 2.0 – Digital Services Act und Digital Markets Act als Herausforderung für die Compliance-Organisation. CCZ: 177-190
- Lagoni J. (2024) Cloud Switching gemäß Data Act: Die Abschaffung von Switching Charges. Was ist ein Wechselentgelt und welche Wechsel sind betroffen? CR: 91-95
- Piltz C, Zwerschke J. (2024) Cloud Switching nach dem Data Act aus der Beratungsperspektive. CR: 153-160
- Ruttloff M, Wagner E, Stilz M. (2024) Der Entwurf des Cyber Resilience Act (CRA) und seine Auswirkungen auf das Gewährleistungs- und Produkthaftungsrecht. BB: 1603-1612
- Schippel R. (2023) Der EU Data Act - die Zukunft von B2B-Datenlizenz und Data as a Service-Modellen. ITRB: 79-83
- Siglmüller J. (2023) Cyber Resilience Act und Digital Operational Resilience Act – Lässt sich IT-Sicherheit rechtlich erzwingen? ZfPC: 221-224

Anhang 1. Beispielhafte Nennung von Leistungserbringern

Anhang 1.1. Leistungserbringer von Heilmitteln

Heilmittel, die als Dienstleistung abgeben werden und nicht entsprechend § 34 SGB ausgeschlossen wurden (beispielsweise Arzneimittel zur Anwendung bei Erkältungskrankheiten und grippalen Infekten), dienen entsprechend § 124 SGB V insbesondere folgenden Leistungen:

- der Physiotherapie,
- der Stimm-, Sprech- und Sprachtherapie,
- der Ergotherapie,
- der Podologie oder
- der Ernährungstherapie.

Dies kann den ambulanten Sektor betreffen, aber auch stationäre Erbringer von entsprechenden Dienstleistungen werden von der Regelung erfasst (§ 124 Abs. 5 SGB V). Die Versorgung mit Heilmitteln darf entsprechend § 32 Abs. 1 SGB V auch telemedizinisch erbracht werden.

Erbringer von entsprechenden Dienstleistungen sind z. B.:

- Ergotherapeuten
- Ernährungstherapeuten wie beispielsweise Diätassistent(-in)
- Masseure, z. B. Masseur (-in) und medizinische Bademeister(-in)
- Physiotherapeuten
- Podologen wie beispielsweise
    - Medizinische(r) Fußpfleger(-in)
    - Podologe/-in
- Stimm-, Sprech-, Sprach- und Schlucktherapeuten, somit können beispielsweise folgende Berufsgruppen erfasst sein:
    - Akademische(r) Sprachtherapeut(-in)
    - Atem-, Sprech- und Stimmlehrer(-in)
    - Logopäde/-in
    - Medizinische(r) Sprachheilpädagoge(-in)
    - Staatlich anerkannter Sprachtherapeut(-in)

Anhang 1.2. Leistungserbringer von Hilfsmitteln

Dies umfasst alle Dienstleister, die als Vertragspartner mit Kranken- bzw. Pflegekassen (Pflegehilfsmittel nach § 40 SGB XI werden von den Pflegekassen finanziert) Hilfsmittel, die nicht entsprechend § 34 Abs. 4 SGB durch Rechtsverordnung des Bundesministeriums für Gesundheit von der gesetzlichen Leistung ausgeschlossen wurden, an gesetzlich Versicherte abgeben dürfen. Der Begriff „Hilfsmittel“ ist sehr weitgehend zu verstehen und umfasst beispielsweise:

- Gehhilfen,
- Hörhilfen,
- Inkontinenzhilfen,
- Kompressionsstrümpfe,
- Orthopädische Hilfsmittel,
- Mobilitätshilfen,
- Prothesen,
- Rollstühle,
- Schuheinlagen,

- Sehhilfen,
- Verbandmaterial.

Auch eine digitale Gesundheits- oder Pflegeanwendung (§ 33a SGB V bzw. § 40a SGB XI) stellt i. d. R. ein Hilfsmittel dar.

Im Hilfsmittelverzeichnis[37] der GKV werden alle zugelassenen Hilfsmittelarten aufgeführt. Dienstleister, die entsprechend Verträgen mit Krankenkassen zur Abgabe dieser Hilfsmittel berechtigt sind, fallen unter dem Begriff „Leistungserbringer“.

Leistungserbringer, die Hilfsmittel an Versicherte abgeben, sind beispielsweise:
- Apotheken,
- Augenoptiker(-in),
- Hörgeräteakustiker(-in),
- Orthopädietechniker(in),
- Orthopädieschuhmacher (-in),
- Sanitätshäuser.

[37] GKV-Spitzenverband: Hilfsmittelverzeichnis. Online, zitiert am 2024-07-14; verfügbar unter https://www.gkv-spitzenverband.de/krankenversicherung/hilfsmittel/hilfsmittelverzeichnis/hilfsmittelverzeichnis.jsp bzw. Online-Katalog unter https://hilfsmittel.gkv-spitzenverband.de/home