E-Mail an:

→ CIO Bund /Staatssekretär Dr. Markus Richter
StR@bmi.bund.de

→ Bitkom Herrn Marc Danneberg
M.Danneberg@bitkom.org

Düsseldorf, 4. September 2023

Sehr geehrte Damen und Herren,

am 11. Februar 2022 nahm der IT-Planungsrat mit Beschluss 2022/01[1] die EVB-IT Cloud zur Kenntnis und empfahl seinen Mitgliedern die Nutzung der EVB-IT Cloud. Das Bundesministerium des Inneren und für Heimat (BMI) veröffentlichte am 02. März 2022 die vertraglichen Grundlagen für die Vergabe von Cloud-Leistungen durch die öffentliche Verwaltung. 18 Monate nach ihrer Veröffentlichung sollen die EVB-IT Cloud einer erneuten Prüfung unterzogen und ggf. angepasst werden.[2]

Die „ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen“ (EVB-IT) sind von der öffentlichen Hand mit Vertretern aus der Wirtschaft abgestimmte Vertragsbedingungen. Als sorgfältig ausgearbeitete Verträge zwischen Auftraggebern und Auftragnehmern werden die EVB-IT gerne auch in der Privatwirtschaft angewendet. Die Cloud-Nutzung spielt in der Gesundheitsversorgung eine zunehmende Rolle, weswegen sich eine Arbeitsgruppe bestehend aus Mitgliedern der drei Verbände

- Bundesverband der Krankenhaus IT - Leiterinnen/Leiter e.V. (KH-IT)
- Bundesverband Gesundheits-IT – bvitg e. V.
  Projektgruppe PG Cloud in der Praxis
- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)
  Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

bildete, um eine Praxishilfe mit Anwendungshinweisen zu den EVB-IT Cloud in der Gesundheitsversorgung zu erstellen.

Im Rahmen der Erarbeitung der Praxishilfe fielen dabei verschiedene Aspekte auf, die im Rahmen einer Evaluierung und ggf. Anpassung Ihrerseits vielleicht berücksichtigt werden könnten. Wir gruppierten unsere Rückmeldungen entsprechend den Vertragsbestandteilen, d. h. die Rückmeldungen sind nach Vertrag, Kriterienkatalog, Cloud-AGB sowie die Einbeziehung auftragnehmerseitiger AGB sortiert.

Unsere Vorschläge zur Anpassung der Vertragsbestandteile der EVB-IT Cloud im Einzelnen:

1. **EVB-IT Cloud Vertrag**
   - Kap. 2, „Überblick über die vereinbarten Leistungen“: Software as a Service* (SaaS*), Platform as a Service* (PaaS*) ist nur gemeinsam auswählbar, jedoch nicht einzeln. Denkbar sind jedoch auch Konstellationen, dass ein Auftraggeber SaaS auf eine von ihm bereits genutzte PaaS ausschreibt. Daher ist es wünschenswert, dass hier sowohl SaaS als auch PaaS einzeln auswählbar sind.
   - Kap. 4.2, „Zahlung der Vergütung“: Hier existiert ein Rechtschreibfehler, genauer ein fehlendes Komma: „[…] eine fällige Vergütung nicht 30 Tage, sondern Tage nach Zugang […]“
   - Kap. 7, „Beauftragte und Ansprechpartner“: Cloud-Verträge werden in der Regel langfristig geschlossen. Während dieser Laufphasen ändern sich Ansprechpartner.

[1] IT-Planunsrat: EVB-IT Cloud. Online, abrufbar unter https://www.it-planungsrat.de/beschluss/beschluss-2022-01

[2] CIO Bund: Meldung „Mustervertrag zur Beschaffung von Cloudleistungen steht zur Verfügung“ vom 1. März 2022. Online, abrufbar unter https://www.cio.bund.de/SharedDocs/kurzmeldungen/Webs/CIO/DE/startseite/mustervertrag-zur-beschaffung-von-cloudleistungen.html

Daher sollte im Vertrag eine Regelung aufgenommen werden, nach welcher der Auftragnehmer den Auftraggeber bei einem Wechsel des Ansprechpartners informiert. Dies in AGB zu verlagern, erscheint nicht sinnvoll, da einerseits die Regelung direkt zu diesem Kapitel gehört, andererseits Anforderungen aus einem Vertrag regelhaft gewissenhafter in den Workflow integriert werden als Anforderungen in einem sehr umfangreichen AGB-Text, wo Anforderungen durch die reine Textmenge teilweise eher „versteckt“ werden. Man sollte nicht davon ausgehen, dass jeder Cloud-Dienstleister eine umfangreiche Rechtsabteilung unterhalten kann, welcher die Anforderungen der AGB extrahiert.

- Kap. 8.1, „Besondere Anforderungen an Mitarbeiter des Auftragnehmers“: Im öffentlichen Bereich sind personenbezogene Daten häufig durch § 203 Abs. 2 StGB geschützt. § 203 Abs. 4 StGB verlangt hier ebenfalls eine Verpflichtung. Es sollte daher überlegt werden, ob dies an dieser Vertragsstelle durch einen entsprechenden Punkt analog zur Verpflichtung nach dem Verpflichtungsgesetz aufgenommen wird.
- In Ziffer 8.4 Unterauftragnehmer besteht die Option zur Abweichung von Ziffer 15.1 EVB-IT Cloud-AGB durch Auswahl von Ziffer 15.2 EVB-IT Cloud-AGB.
  Hier liegt ein redaktioneller Fehler vor, da Ziffer 15 EVB-IT Cloud-AGB eine Auswahl zwischen Ziff. 15.1 und 15.3 vorsieht. 15.1 EVB-IT Cloud-AGB verlangt die Benennung der Unterauftragnehmer, 15.3 die Genehmigung durch ausdrückliche Zustimmung des Auftraggebers.
  Der EVB-IT Cloudvertrag lässt aber nur die Wahl zwischen 15.1 und 15.2 EVB-IT Cloud-AGB. Korrekterweise müsste Ziffer 8.4 Cloudvertrag die Optionen 15.1 und 15.3 EVB-IT Cloud-AGB aufführen.
- In Ziffer 8.6 sollte überlegt werden, ob der Auftragnehmer neben dem Vorliegen einer Haftpflichtversicherung nicht auch das Vorliegen einer Cyberversicherung nachweisen sollte.
- Nirgendwo im EVB-IT Cloud wird die Unterstützung des Auftraggebers bei der Umsetzung der Anforderungen der „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“[3] des Bundesamts für Sicherheit in der Informationstechnik (BSI) (OH SzA) gefordert, welche Betreiber Kritischer Infrastrukturen adressiert und von diesen erfüllt werden müssen. Diverse Auftraggeber werden als Kritische Infrastruktur anzusehen sein, daher regen wir an, entweder
  - im Vertrag unter Ziffer 8.2 ein entsprechendes Ankreuzfeld zu ergänzen
  - oder (vielleicht besser zum Vertragsaufbau passend) ein entsprechendes Ankreuzfeld im Kriterienkatalog in Ziffer 18 einzufügen.

  Vorschlag für den Text
  - Vertrag, Ziffer 8.2:
    „☐ den Auftraggeber bei der Erfüllung der Anforderungen der „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ (SzA) des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu unterstützen und entsprechende Systeme für alle Aspekte der vertraglich vereinbarten Leistungen einzusetzen.“
  - Kriterienkatalog Ziffer 18
    „☐ Ergänzend zu Ziffer 1.2 EVB-IT Cloud-AGB ist der Einsatz von Systemen zur Angriffserkennung entsprechend den Vorgaben der „Orientierungshilfe

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI): Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung. Online, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html

zum Einsatz von Systemen zur Angriffserkennung“ (SzA) des Bundesamts für Sicherheit in der Informationstechnik (BSI) geschuldet. Weiterhin muss der Auftragnehmer den Auftraggeber bei der Erfüllung der Anforderungen der SzA zu unterstützen, sodass der Auftraggeber gegenüber dem BSI seinen Nachweispflichten genügen kann.“

2. EVB-IT Cloud Kriterienkatalog für Cloudleistungen

- Zu Kap. 1 „Kriterien“, Ziff. 18: Je nach Leistung ist eine verschlüsselte Speicherung, auch sensibler Daten wie z. B. Sozialdaten oder Gesundheitsdaten, nicht immer wünschenswert oder umsetzbar. Der C5-Kriterienkatalog fordert an verschiedenen Stellen jedoch eine Verschlüsselung, z.B.
  - CRY-01
  - CRY-03

  Es wäre wünschenswert, wenn der Auftraggeber unter Ziffer 18 die Verschlüsselung auch abwählbar gestalten kann, z. B. weil bereits verschlüsselte Daten als Backup in einer Cloud als Sicherheitskopie gespeichert werden sollen.

3. EVB-IT Cloud AGB

- In Ziffer 1.2 wird die Erfüllung der vertraglich vereinbarten Leistungen unter Einhaltung des bei Vertragsschluss jeweils aktuellen Cloud Computing Compliance Criteria Catalogue - C5 (Basiskriterien) gefordert, wobei in Ziffer 1.2 ausschließlich der Nachweis durch ein Testat eines Wirtschaftsprüfers möglich ist.

  In Ziffer 6.2.1 wird gefordert, dass das von Auftragnehmer eingesetzte Informationssicherheits-Managementsystem nicht nur den Anforderungen der ISO/IEC 27001 genügen muss, sondern sich das Sicherheitskonzept an EN ISO/IEC 27017 und, sofern personenbezogene Daten verarbeitet werden, auch an EN ISO/IEC 27018 ausrichten muss. Das BSI stellt eine Kreuzreferenztabelle zur Verfügung[4], mittels welcher die Anforderungen des BSI C5 Katalogs auf die ISO 27001 gemappt werden. Ergänzend wird weitere Kreuzreferenztabelle bereit gestellt[5], worin u. a. auch die EN ISO/IEC 27017 und 27018 berücksichtigt werden.

  Die seitens BSI adressierten datenschutzrechtlichen Anforderungen wie beispielsweise Aufgaben/-Mandantentrennung (OIS-04) werden von der EN ISO/IEC 27701 adressiert. Erfolgt eine ISO 27001-Zertifizierung unter Berücksichtigung der cloud-spezifischen ISO-Normen sowie der EN ISO/IEC 27701, so wird allen Anforderungen des BSI genügt.

  Es sollte geprüft werden, ob der Nachweis der Erfüllung der Anforderungen des C5-Kriterienkatalogs statt durch ein Testat eines Wirtschaftsprüfers, der ggf. nicht einmal über Fachkenntnisse in Bezug auf IT-Sicherheit verfügt und letztlich nur eine Prüfung vorgelegter Dokumente vornimmt, auch durch eine 27001-Zertifizierung nachgewiesen werden kann, wenn diese Zertifizierung die weiteren Normen (EN ISO/IEC 27017 und EN ISO/IEC 27701 sowie – falls zutreffend - EN ISO/IEC 27018) einbezieht und somit die durch einen unabhängigen und fachkundigen Prüfer alle adressierten Punkte während der Zertifizierung geprüft und die Erfüllung im Rahmen der Zertifizierung bestätigt wurde.
- Gemäß Ziffer 2.1.1 darf der Auftraggeber ohne vorherige Zustimmung des Auftragnehmers keine Penetrationstests in der jeweiligen Cloudinfrastruktur

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kreuzreferenztabelle C5_ISO IEC 27001 2022. Online, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2022_Referenztabelle_ISO27001.html

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kruzreferenztabelle. Online, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020_Referenztabelle.xlsx?__blob=publicationFile&v=4

durchführen oder autorisieren. Jedoch können entsprechende Penetrationstests für den Nachweis einer sicheren Verarbeitung erforderlich sein.
Insbesondere für Einrichtungen, die als kritische Infrastruktur angesehen werden müssen, können Penetrationstests, welche das gesamte System umfassen (getrennte Testung der Systeme von Auftraggeber und Auftragnehmer können nicht das Zusammenspiel der Systeme erfassen), rechtlich erforderlich sein.
Daher sollte überlegt werden, ob in dieser Ziffer dem Auftraggeber nicht zugesichert wird, dass Auftragnehmer entsprechende Penetrationstests unter Beachtung der Sicherheitsbelange und der Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie der weiteren Kunden des Auftragnehmers zulassen und unterstützen.
Wir möchten darauf hinweisen, dass die Anforderungen des BSI an kritische Infrastrukturen bzgl. umfassender Penetrationstests überdacht und die Verwendung von Penetrationstests, die bereits von IaaS-, SaaS- und PaaS-Anbietern durchgeführt wurden, als ausreichend angesehen werden sollen.

- In Ziffer 4 ist für „die Speicherung und sonstige Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer“ der Leistungsort standardmäßig auf die EU, den EWR sowie „sofern ein Angemessenheitsbeschluss gem. Art. 45 DSGVO besteht“ auch auf die Schweiz begrenzt.
  Hier wäre aufgrund des Brexits eine Ausweitung für das Vereinigte Königreich wünschenswert, welches ebenfalls über einen Angemessenheitsbeschluss verfügt, aber weder in der EU noch im EWR ein Mitglied ist.
  Die Regelungen analog zur Schweiz wären aus unserer Sicht eine sinnvolle Ergänzung, da aufgrund der früheren Zugehörigkeit des Vereinigten Königreichs zur EU viele bilaterale Geschäftsbeziehungen bestehen. Und aktuell kann im Kriterienkatalog in Ziffer 3 nur allen Ländern mit Angemessenheitsbeschluss seitens des Auftraggebers zugestimmt werden, was ggf. seitens des Auftraggebers nicht gewünscht ist.
- Entsprechend Ziffer 5.3 muss der Auftragnehmer Zugriff auf die Daten des Auftraggebers durch unberechtigte Stellen und Personen mit angemessenen Maßnahmen verhindern. Jedoch wird vertraglich nicht geregelt, ob der Zugriff aus Sicht des Auftraggebers oder Auftragnehmers als „unberechtigt“ beurteilt werden muss.
  Unterliegt der Auftragnehmer ausländischem Recht, so kann aus Sicht des Auftragnehmers ein Zugriff durch Behörden dieses anderen Landes als „berechtigt“ anzusehen sein, aus Sicht in Deutschland tätigen Auftraggebers wäre der Zugriff nach deutschem Recht als „unberechtigt“ zu bewerten.
  Es sollte daher geprüft werden, ob an dieser Stelle nicht dargestellt wird, dass die Prüfung bzgl. berechtigten Zugriff ausschließlich aus Sicht des Auftraggebers zu beurteilen ist.
- Mit Ziffer 6.1.1 wird nicht die Einhaltung von europäischem und deutschem Recht vereinbart, sondern die Einhaltung der „Leistung jeweils auf sie anwendbaren Bestimmungen über den Datenschutz“. Die vertraglichen Regelungen sind seitens Auftragnehmer an Unterauftragnehmer im jeweils für die Unterauftragnehmer entsprechend ihrer Leistungserbringung erforderlichen Umfang weiterzugeben. Somit gilt für einen Unterauftragnehmer in den USA oder Indien nur das in den USA bzw. Indien geltende Recht, nicht aber europäisches oder deutsches Datenschutzrecht. Hier sollte geprüft werden, ob nicht grundsätzlich die Einhaltung von europäischem und ergänzend dem deutschem Datenschutzrecht seitens Auftraggeber und Auftragnehmer gefordert wird.
  Da entsprechend § 1.2.1 des Cloud-Vertrages ein Vertrag zur Auftragsverarbeitung nachrangig gegenüber dem Kriterienkatalog für Cloudleistungen inklusive Anlage zur

Einbeziehung von auftragnehmerseitigen AGB mit Anhang I und II gilt, über den Kriterienkatalog wiederum Drittstaaten außerhalb EU/EWR zugelassen werden können, ist rechtlich nicht unstrittig, ob mittels eines Vertrages zur Auftragsverarbeitung in diesen Fällen für (Unter-)Auftragnehmer die Einhaltung von europäischem und deutschem Datenschutzrecht wirksam vereinbart werden kann.

- Ziffer 6.1.4 verlangt, dass ein Datenschutzbeauftragter benannt wird, wenn dies gesetzlich gefordert wird. Damit ist diese Formulierung unnötig, denn gesetzliche Vorgaben sind natürlich für beide Vertragspartner immer bindend. Wir schlagen als Änderung vor:
  „Sofern der Auftragnehmer über einen Datenschutzbeauftragten verfügt, teilt der Auftragnehmer dem Auftraggeber auf Anfrage dessen Kontaktdaten mit."
- In Ziffer 6.2.2 wird vom „IT-Sicherheitsbeauftragten" gesprochen. Das BSI spricht in seinen aktuellen Veröffentlichungen vom „Informationssicherheitsbeauftragten", z. B. Lerneinheit 2.4, abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/ Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_2_Sicherheitsmanagement/Lektion_2_04/Lektion_2_04_node.html.
  - Wir schlagen daher eine Anpassung bei den EVB-IT Cloud hinsichtlich der vom BSI verwendeten Nomenklatur vor.
- Das in Ziffer 7.3 geforderte „marktübliches Austauschformat" wird ggf. nicht den aus der DS-GVO resultierenden gesetzlichen Anforderungen genügen, wenn ein Verantwortlicher entsprechend Art. 20 DS-GVO personenbezogene Daten auf Antrag einer betroffenen Person in einem „strukturierten, gängigen und maschinenlesbaren Format" bereitstellen oder übermitteln muss.
  Art. 2 Ziff. 13 Richtlinie (EU) 2019/1024[6] bezeichnet „maschinenlesbares Format" als Dateiformat, welches so strukturiert ist, dass Softwareanwendungen
  - konkrete Daten,
    - einschließlich einzelner Sachverhaltsdarstellungen und deren interner Struktur,
  - leicht identifizieren, erkennen und extrahieren können.

  Vielleicht ist es sinnvoll, in Ziffer 7.3 statt ein „marktübliches Austauschformat" die Definition von Art. 2 Ziff. 13 Richtlinie (EU) 2019/1024 zu referenzieren?
  Vorschlag für eine Formulierung:
  „[…] durch den Auftragnehmer aus der Cloudinfrastruktur in einem marktüblichen Austauschformat, welches der Definition in Definition von Art. 2 Ziff. 13 Richtlinie (EU) 2019/1024 genügen muss, exportiert werden können […]"

- In Ziffer 11 wird zwischen „Erledigungszeiten" und „Wiederherstellungszeiten" unterschieden, in beiden Fällen auf die Begriffsbestimmungen verwiesen. Jedoch existiert nur für den Begriff „Wiederherstellungszeit" eine Begriffsbestimmung.
  Vielleicht wurde der Begriff „Erledigungszeit" aus den EVB-IT Service übernommen. In den EVB-IT Service-AGB findet sich die Begriffsbestimmung:
  „Erledigungszeit
  Zeitraum, innerhalb dessen der Auftragnehmer die Serviceleistungen erfolgreich abzuschließen hat. Der Zeitraum beginnt mit dem Zugang der

[6] Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors. Online, abrufbar unter https://eur lex.europa.eu/legal content/DE/TXT/?uri=CELEX%3A32019L1024

entsprechenden Meldung oder dem Eintritt eines vereinbarten Ereignisses innerhalb der vereinbarten Servicezeiten* und läuft ausschließlich während der vereinbarten Servicezeiten*. Geht eine Meldung oder tritt ein vereinbartes Ereignis außerhalb der vereinbarten Servicezeiten* ein, beginnt die Erledigungszeit* mit Beginn der nächsten Servicezeit*."

In den EVB-IT Cloud-AGB wird „Wiederherstellungszeit" definiert als:

„Zeitraum, innerhalb dessen der Auftragnehmer die Störungs- bzw. Mängelbehebungsarbeiten erfolgreich abzuschließen hat. Der Zeitraum beginnt mit dem Auftreten der Störung*, läuft jedoch nur in den vereinbarten Servicezeiten. Tritt die Störung* außerhalb dieser Zeiten ein, beginnt die Wiederherstellungszeit mit der nächsten Servicezeit."

Es spricht daher vieles dafür, dass beide Begriffen dieselbe Bedeutung haben, insbesondere, da im Kriterienkatalog für Cloudleistungen unter Ziffer 21 nur Wiederherstellungs-, aber keine Erledigungszeiten vereinbart werden können. Daher sollte hier eine einheitliche Begriffsverwendung erfolgen.

Falls dies nicht gewünscht ist, sollte zumindest „Erledigungszeit" ebenfalls unter „Begriffsbestimmungen" definiert und eine Möglichkeit zur Angabe vereinbarter Zeiten im Kriterienkatalog aufgenommen werden.

- In den „Begriffsbestimmungen" wird „Betriebsbereitschaft" als „die Leistung funktioniert störungsfrei" definiert.

  Solange die Leistung seitens Auftraggeber nicht abberufen wird, kann eine „Störungsfreiheit" nur angenommen, aber nicht als „sicher" bewertet werden.

  Vielleicht ist es sinnvoller, Betriebsbereitschaft wie folgt zu definieren:

  „Betriebsbereitschaft
  ein (Cloud-) Produkt, eine Dienstleistung, eine Umgebung oder eine Einrichtung befindet sich in einem Zustand, der es dem Auftragnehmer ermöglicht, die vertraglich vereinbarte Leistung im Rahmen der vereinbarten Zeitspanne zu nutzen."

- In den „Begriffsbestimmungen" sollte sich beim Begriff „Monitoring" die Erläuterung zum Sicherheitsmonitoring auch mindestens auf die Schutzziele beziehen.
  - Vorschlag:
    Sicherheits-Monitoring. Aktive Überwachung der Infrastruktur und der Services bzgl. auftretender Sicherheitsereignisse, welche mindestens die Schutzziele Vertraulichkeit und Verfügbarkeit verletzen. Ebenso die aktive Überwachung des Cloud-Dienstes auf Schwachstellen, die etwa aus einer Fehlkonfiguration oder der ausstehenden Einspielung von sicherheitsrelevanten Updates resultieren.

  Weiterhin werden nur Beispiele aufgezählt, aber entgegen der Überschrift „Begriffsbestimmungen" der Begriff nicht definiert. Vorschlag einer Definition des Begriffs „Monitoring":

  „Monitoring
  Überwachung, d. h. systematische Erfassung durch Messungen, Protokollierungen oder Beobachtungen eines Vorgangs oder Prozesses mittels technischer Hilfsmittel oder anderer Beobachtungssysteme sowie die Auswertung und Bewertung dieser erfassten Daten"

  Wenn nachfolgend die Beispiele angegeben werden, sollte der Begriff ausreichend klar bestimmt sein.

- Die Verfügbarkeit wird leider nicht definiert, man kann den Begriff nur indirekt durch die Nutzung in Ziffer 8 der AGB ableiten. Wir schlagen vor, auch „Verfügbarkeit“ in die Begriffsbestimmungen aufzunehmen. Als Definition bietet sich an

  „Verfügbarkeit
  die Eigenschaft, dass auf Verlangen eines Cloud-Dienst-Kunden ein vertraglich zugesicherter Cloud-Dienst im zuvor vereinbarten Umfang zugänglich und nutzbar ist.“
- In den „Begriffsbestimmungen“ sollte auch eine Definition des „IT-Sicherheitsbeauftragten“ (oder besser: „Informationssicherheitsbeauftragten“) enthalten sein, welche Vorgaben enthält, mit der man die in Ziffer 6.2.2 geforderte „erforderlichen Fachkunde“ bewerten kann.
- In den „Begriffsbestimmungen“ finden sich Definitionen, die von existierenden Definitionen in Normen/Standards mehr oder weniger abweichen. Wir schlagen hier eine Anpassung der Begriffsbestimmungen im EVB-IT Cloud vor, damit die Begriffsbestimmungen in den EVB-IT Cloud mit denen der Normung übereinstimmen. Insbesondere, da die EVB-IT Cloud selbst wiederum Verweise auf Normen wie beispielsweise ISO 27001 enthält. Insbesondere fallen die Unterschiede bei den drei Kernbegriffen aus dem Cloud-Umfeld auf:
  - Infrastruktur as a Service / IaaS

EVB-IT Cloud	ISO/IEC 22123-1 (2023): Cloud computing — Part 1: Vocabulary
Bei IaaS* werden IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze als Dienst angeboten. Ein Auftraggeber nutzt diese virtualisierten und in hohem Maß standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Auftraggeber z.B. Rechenleistung, Arbeitsspeicher und Datenspeicher nutzen und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.	cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type Note 1: The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer can also have limited ability to control certain networking components (e.g., host firewalls).

  - Plattform as a Service

EVB-IT Cloud	ISO/IEC 22123-1 (2023): Cloud computing — Part 1: Vocabulary
Ein PaaS-Provider stellt eine komplette Infrastruktur bereit und bietet dem Auftraggeber auf der Plattform standardisierte Schnittstellen an, die von Diensten des Auftraggebers genutzt werden. So kann die Plattform z. B. Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe, etc. als Service zur Verfügung stellen. Der Auftraggeber hat in der Regel keinen Zugriff auf die darunterliegenden Schichten (Betriebssystem, Hardware), er kann aber auf der Plattform eigene	cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type

Anwendungen laufen lassen, für deren Entwicklung der Auftragnehmer in der Regel eigene Werkzeuge anbietet.	

- Software as a Service

EVB-IT Cloud	ISO/IEC 22123-1 (2023): Cloud computing — Part 1: Vocabulary
Bezeichnet die Bereitstellung von Software bzw. Funktionen von Software in einer vom Auftragnehmer betriebenen Infrastruktur.	cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type

Die deutsche DIN SPEC 66286 (2014) „Management von Cloud Computing Lösungen in kleinen und mittleren Unternehmen (KMU)“ enthält ebenfalls Definitionen der drei Begriffe (IaaS Abschnitt 3.20.2.1, PaaS Abschnitt 3.20.2.2, SaaS Abschnitt 3.20.2.3 der Norm), die in etwa den Begriffen der ISO/IEC 22123-1 (2023) entsprechen.

- Im Kriterienkatalog befindet sich unter Ziffer 1 im Bereich „1. Kriterien“ die Auswahl zwischen Public und Private Cloud, jedoch wird beides nicht in den Begriffsbestimmungen der AGB definiert. Idealerweise würden hierzu die Definitionen aus bestehenden international anerkannten Normen wie z. B. der ISO ISO/IEC 22123-1 genutzt.

4. EVB-IT Cloud Anlage auftragnehmerseitige AGB

- Da diese Anlage in Anhang II zum Kriterienkatalog die Option bietet, einzelne Regelungen aus den AGB des Auftragnehmers vorrangig einzubeziehen, ist die Betitelung als „AGB“ irreführend.
  Denn im Gegensatz zu Anhang I ist bei Anhang II gerade keine komplette Einbeziehung eines standardisierten Regelwerkes möglich, sondern es können lediglich einzelne Klauseln der auftraggeberseitigen AGB vorrangig gelten.
  Daher ist die Bezeichnung ungünstig gewählt.

Wenn Sie die eine oder andere Anregung berücksichtigen könnten, würden Sie die Nutzbarkeit der schon heute aus unserer Sicht sehr guten EVB-IT Cloud noch einmal verbessern.

Für Rückfragen stehen wir sehr gerne zur Verfügung.

Für die kommentierende Arbeitsgruppe der drei beteiligten Verbände

Dr. Bernd Schütze
Leiter GMDS AG „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)
E-Mail: schuetze@medizin-informatik.org