EVB-IT Cloud: Kommentierung aus Sicht der Gesundheitsversorgung

Eine Zusammenarbeit von

Bundesverband der Krankenhaus IT-Leiterinnen/Leiter KH-IT

Bundesverband Gesundheits-IT – bvitg e. V.
Projektgruppe Cloud in der Praxis

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

Version 1.0

Stand der Bearbeitung: 23. Oktober 2023

Autoren (alphabetisch)

Philipp Barschkies	3M Medica, Zweigniederlassung der 3M Deutschland GmbH
Thomas Liebscher	Philips GmbH
Christian Meier	Universitätsklinikum und Medizinische Fakultät Tübingen, Stabsstelle des Vorstands | Informationssicherheit KV16
Nicole Schneidewind	Deutsche Telekom Healthcare and Security Solutions GmbH
Thorsten Schütz	Klinikum Itzehoe, Leiter IT und Betriebsorganisation
Dr. Bernd Schütze	Deutsche Telekom Healthcare and Security Solutions GmbH

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:

Inhaltsverzeichnis

Vorwort 1

EVB-IT: Eine kurze Einführung 2

EVB-IT: Vertragsübergreifende Regelungen 3

Änderungen der EVB-IT: Individuelle Anpassungen 4

Cloud Computing ist Outsourcing 4

Cloud Computing Verträge: SaaS als Mietvertrag 5

Cloud und Datenschutz: Orientierungshilfe des Bayerische Landesbeauftragte für den Datenschutz 6

Amerikanische Cloud-Anbieter und Vergabeverfahren 7

EVB-IT Cloud: Reihenfolge der Vertragsbestandteile 8

Vertrag über Cloudleistungen 9

Vorbemerkung 9

Allgemeines 9

Abschnitt „1 Gegenstand und Bestandteile des Vertrages“ 10

Zu Ziffer 1.2.1 10

Zu Ziffer 1.2.4 11

Abschnitt „2 Überblick über die vereinbarten Leistungen“ 13

Abschnitt „3 Gegenstand der Leistungen“ 14

Zu Ziffer 3.1 14

Zu Ziffer 3.2 14

Zu Ziffer 3.3 14

Zu Ziffer 3.4 15

Abschnitt „4 Fälligkeit und Zahlung der Vergütung“ 16

Zu Ziffer 4.3 16

Zu Ziffer 4.4 16

Abschnitt „6 Abweichende Haftungsregelungen“ 17

Abschnitt „7 Beauftragte und Ansprechpartner“ 18

Zu Ziffer 7.1 18

Zu Ziffer 7.2 18

Abschnitt „8 Weitere Regelungen“ 19

Zu Ziffer 8.1 19

Zu Ziffer 8.3 19

Zu Ziffer 8.4 19

Zu Ziffer 8.6 20

Kriterienkatalog für Cloudleistungen 21

Abschnitt „1 Kriterien“ 21

Zu Ziffer 1 21

Zu Ziffer 2 22

Zu Ziffer 3 23

Zu Ziffer 4 26

Zu Ziffer 5 26
Zu Ziffer 6 27
Zu Ziffer 7 27
Zu Ziffer 8 27
Zu Ziffer 9 27
Zu Ziffer 10 28
Zu Ziffer 12 29
Zu Ziffer 13 29
Zu Ziffer 15 30
Zu Ziffer 16 31
Zu Ziffer 17 32
Zu Ziffer 18 33
Zu Ziffer 19 34
Zu Ziffer 22 35

Anlage zur Einbeziehung von auftragnehmerseitigen AGB 37

Einleitung 37

Abschnitt „I Anhang zum EVB-IT Cloudvertrag“ 38

Abschnitt „II Anhang zum Kriterienkatalog“ 39

Ergänzende Vertragsbedingungen für Cloudleistungen – EVB-IT Cloud-AGB 40

Abschnitt „1 Gegenstand des Vertrages“ 40
Zu Ziffer 1.2 40
Zu Ziffer 1.3 41
Zu Ziffer 1.4 41

Abschnitt „2 Art und Umfang der Leistungen“ 43
Zu Ziffer 2.1.1 43

Abschnitt „3 Nutzungsverbote“ 44
Zu Ziffer 3.2 44

Abschnitt „4 Leistungsort“ 45
Zu Ziffer 4 45

Abschnitt „5 Zugriff/Speicherplatz“ 46
Zu Ziffer 5.3 46

Abschnitt „6 Datenschutz, IT-Sicherheit und Vertraulichkeit“ 47
Zu Ziffer 6.1.1 47
Zu Ziffer 6.1.2 47
Zu Ziffer 6.2.1 48
Zu Ziffer 6.3.1, 6.3.2 49
Zu Ziffer 6.4.2 50

Abschnitt „7 Datensicherungsservice / Backup / Herausgabe- und Löschungsanspruch“ 51
Zu Ziffer 7.3 51

Abschnitt „8 Verfügbarkeit“ 52
Zu Ziffer 8.2 52
Zu Ziffer 8.3 52

Abschnitt „9 Reportingpflichten“ 54
Zu Ziffer 9.1 54

Abschnitt „10 Störungsklassifizierung“ 55

Abschnitt „11 Störungsbeseitigung“ 56

Abschnitt „12 Änderung der Leistung nach Vertragsschluss durch den Auftragnehmer“ 57

Abschnitt „13 Pflichten und Leistungen im Zusammenhang mit dem Vertragsende“ 58

Zu Ziffer 13.2.2 58

Zu Ziffer 13.3.1 58

Abschnitt „15 Unterauftragnehmer“ 59

Zu Ziffer 15.1 59

Zu Ziffer 15.3 59

Abschnitt „17 Mitwirkung des Auftraggebers“ 61

Zu Ziffer 17.2 61

Zu Ziffer 17.3 67

Zu Ziffer 17.9 68

Abschnitt „18 Rechte des Auftraggebers bei Mängeln der Leistungen“ 69

Abschnitt „19 Haftungsbeschränkung“ 70

Zu Ziffer 19.1 70

Zu Ziffer 19.2 70

Abschnitt „20 Laufzeit und Kündigung“ 71

Zu Ziffer 20.2 71

Abschnitt „21 Haftpflichtversicherung“ 73

Abschnitt „23 Textform“ 74

Abschnitt „24 Anwendbares Recht, Gerichtsstand“ 74

Zu Ziffer 24.1 74

Abschnitt „Begriffsbestimmungen“ 75

Zu Verfügbarkeitsklassen 75

Abkürzungen 76

Vorwort

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 diese am 02. März 2022 Vorgaben für die Vergabe von Cloud-Leistungen durch die öffentliche Verwaltung und seitdem stehen diese der Allgemeinheit zur Verfügung.

Derartige „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.

18 Monate nach ihrer Veröffentlichung sollen die EVB-IT Cloud einer erneuten Prüfung unterzogen und ggf. angepasst werden[2], d. h., ab September 2023 soll geprüft werden, ob Anpassungen vorgenommen werden und falls dies der Fall ist, dürfte im Frühjahr 2024 mit der Veröffentlichung einer angepassten Version zu rechnen sein.

Daher ist bei der Nutzung dieser Kommentierung der EVB-IT Cloud darauf zu achten, ob die genutzten EVB-IT Cloud mit dem kommentierten Wortlaut übereinstimmen. Um diese Prüfung zu erleichtern, wird – wo relevant – der Wortlaut des Vertragstextes vor der Kommentierung wiederholt (erkennbar an einer Linie auf dem Seitenrand).

[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

EVB-IT: Eine kurze Einführung

Die öffentliche Hand muss bei ihren Beschaffungen den Vorgaben der Bundeshaushaltsordnung[3] genügen, insbesondere § 55 „Öffentliche Ausschreibung“. § 33 HGrG[4] i.V.m. § 55 Abs. 2 BHO enthalten den Grundsatz, dass öffentliche Auftraggeber beim Abschluss von Verträgen nach einheitlichen Richtlinien zu verfahren haben. In den „Allgemeine Verwaltungsvorschriften zur Bundeshaushaltsordnung“[5] zu § 55 BHO wird festgelegt, was unter dem Begriff der „einheitlichen Richtlinien“ zu verstehen ist. In den VV-BHO zu § 55 ist dabei auch festgelegt, dass die „ergänzenden Vertragsbedingungen für die Beschaffung von Informationstechnik[6]“ (EVB-IT) bei Ausschreibungen zu berücksichtigen sind.

Die EVB-IT werden von einer Arbeitsgruppe unter der Federführung des Bundesministeriums des Innern und für Heimat (BMI) erarbeitet und bei Bedarf an geänderte technische und rechtliche Anforderungen angepasst. Die EVB-IT werden mit den Interessenverbänden der IT-Wirtschaft (gegenwärtig dem Bitkom) verhandelt und einvernehmlich veröffentlicht. Dabei bleibt jedoch die finale Entscheidung, wie der Staat als Einkäufer die EVB-IT ausgestaltet, in der Hand des Staates.

Der IT-Planungsrat, ein 17-köpfiges Gremium bestehend aus Vertretern der Bundesregierung und der Regierungen der Länder, nimmt i. d. R. die von der Gruppe erarbeiteten Pläne an, d. h. es wird ein förmlicher Beschluss gefasst. Bzgl. der EVB-IT Cloud stammt der Beschluss vom 11. Februar 2022.[7] Verbunden mit dem Beschluss ist regelhaft die Empfehlung, dass die EVB-IT seitens der Mitglieder (also Bund und Länder) angewendet werden soll. Im Falle der EVB-IT Cloud muss der Vertrag daher bei der Ausschreibung bzw. Anschaffung von (Public) Cloud Dienstleistungen durch die öffentliche Hand berücksichtigt werden.

Die vom IT-Planungsrat per Beschluss angenommenen EVB-IT sind abrufbar unter https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/it-beschaffung/evb-it-und-bvb/evb-it/evb-it-node.html. Die EVB-IT werden zwischen Basis- und Systemverträgen unterschieden. Derzeit existieren 7 Basisverträge und 4 Systemverträge:

- Basisverträge
  - EVB-IT Cloud
  - EVB-IT Dienstleistung
  - EVB-IT Instandhaltung
  - EVB-IT Kauf
  - EVB-IT Pflege S
  - EVB-IT Überlassung Typ A
  - EVB-IT Überlassung Typ B
- Systemverträge
  - EVB-IT Erstellung
  - EVB-IT Service

[3] Bundeshaushaltsordnung (BHO). Online, zitiert am 2023-08-11; verfügbar unter https://www.gesetze-im-internet.de/bho/

[4] Gesetz über die Grundsätze des Haushaltsrechts des Bundes und der Länder (HGrG). Online, zitiert am 2023-08-11; verfügbar unter https://www.gesetze-im-internet.de/hgrg/

[5] Allgemeine Verwaltungsvorschriften zur Bundeshaushaltsordnung(VV-BHO). Online, zitiert am 2023-08-11; verfügbar unter https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_14032001_DokNr20110981762.htm

[6] Anlage zum BMF-Rundschreiben vom 20. Dezember 2013, Abschnitt 3.1.1. Online, zitiert am 2023-08-11; verfügbar unter https://www.verwaltungsvorschriften-im-internet.de/pdf/BMF-IIA3-20181002-H-05-01-2-KF-007-R011a.pdf

[7] IT-Planungsrat: EVB-IT Cloud. Online, zitiert am 2023-08-11; verfügbar unter https://www.it-planungsrat.de/beschluss/beschluss-2022-01

- EVB-IT System
- EVB-IT Systemlieferung.

Jeder EVB-IT besteht aus verschiedenen Teilen: dem Vertragsformular, dazugehörigen AGB sowie einem oder mehreren Mustern (z. B. für Mängelmeldungen oder einem Leistungsnachweis). Zu einigen EVB-IT existieren zusätzlich noch Nutzerhinweise sowie Anwendungsbeispiele.

Die EVB-IT stellen die Einkaufs-AGB (Allgemeine Geschäftsbedingungen) von Bund und Ländern bei der Beschaffung von Informationstechnik dar. Für EVB-IT gelten daher selbstverständlich die gleichen gesetzlichen Anforderungen wie für andere AGB auch.[8]

Die EVB-IT lassen der öffentlichen Hand in Ausschreibungsverfahren dabei Spielräume für Ergänzungen. Dies ist auch beim EVB-IT Cloud der Fall.

Bei den EVB-IT handelt es sich zwar um die Einkaufsbedingungen der öffentlichen Hand, sie werden allerdings in der Praxis auch von außerhalb der öffentlichen Hand, d. h. seitens der Privatwirtschaft, verwendet, insbesondere auch von Einrichtungen der Gesundheitsversorgung wie beispielsweise Krankenhäusern, da die EVB-IT als Vertragsmuster für Software-Verträge ein hohes Niveau abbilden. Allerdings bedarf es einer guten Einarbeitung in die jeweiligen EVB-IT-Verträge und dies gilt in gleicher Weise auch für den EVB-IT-Cloud-Vertrag.

EVB-IT: Vertragsübergreifende Regelungen

Die EVB-IT folgen dem Konzept eines einheitlichen Aufbaus, berücksichtigen aber auch, Klauseln, die sich für unterschiedliche EVB-IT Vertragstypen (z. B. „Standardsoftware“) eignen, auch gleichlautend bzw. nahezu gleichlautend in den jeweiligen EVB-IT zu verwenden.

Sämtliche Vertragsmuster zwingen die vertragsschließenden Parteien, Basisinformationen wie Kontaktdaten Auftraggeber und Auftragnehmer, Vertragsnummer/-kennung usw. anzugeben, wodurch eine eindeutige Identifizierbarkeit sowohl der beteiligten Vertragsparteien als auch des einzelnen Vertrages gewährleistet wird.

Ebenso enthält jeder EVB-IT einen Punkt „Vertragsgegenstand“, wo der Leistungsgegenstand kurz beschrieben werden muss, sowie Regelungen hinsichtlich der Vergütung. Die Art der Vergütung ist dabei auf den jeweiligen EVB-IT angepasst. So ist bei Hardware-Käufen die Vergütung regelhaft nach der Lieferung der Hardware fällig, bei Verträgen mit Dauerschuldcharakter, wie z. B. Software-Leasing-Verträge, sind hingegen unterschiedliche Regelungen vorgesehen, je nachdem, ob die Vergütung nach dem jeweiligen erbrachten Aufwand oder durch eine pauschale Vergütung vertraglich vereinbart wird.

EVB-IT versuchen, eine weitgehend einheitliche Terminologie durch Definitionen zu schaffen. Auf diese jeweiligen Definitionen ist dann im Text selbst durch Sternchenhinweise (*) verwiesen. So auch in den EVB-IT Cloud, wo im Vertrag selbst auf die Definitionen in den EVB-IT Cloud-AGB verwiesen wird. Die Definitionen in den EVB-IT versuchen, die gängige Rechtsprechung zu berücksichtigen, was mehr oder weniger gut gelingt.

> Beispiel: Die Definition des Begriffs „Standardsoftware“ berücksichtigt die Rechtsprechung des BGH von 1989[9], wonach z. B. ein Benutzerhandbuch zwingend erforderlich ist, die Rechtsprechung des BGH aus dem Jahr 1999[10], wonach zwischen der

[8] BGH, Urt. v. 1997-03-04 Az. – X ZR 141/95: Urteil zu BVB-Überlassung, Vorgänger der EVB-IT; Urteil ist 1:1 auf EVB-IT übertragbar. Online, zitiert am 2023-08-11; verfügbar unter https://dejure.org/1997,1406

[9] BGH, Urt. v. 1989-07-05 Az. VIII ZR 334/8, Leitsatz. Online, zitiert am 2023-08-11; verfügbar unter https://dejure.org/1989,81

[10] BGH, Urt. v. 1999-12-22 Az. VIII ZR 299/98, Rn. 10 und 11. Online, zitiert am 2023-08-11; verfügbar unter https://dejure.org/1999,244

Bedienungsanleitung/dem Handbuch einerseits und der Online-Hilfe unterschieden werden muss, wird in den EVB-IT nicht berücksichtigt.

Mit Einführung der EVB-IT System differenzieren die EVB-IT nicht mehr nach einem Haftungsgrund wie beispielsweise Verzug, Sachmangel, Schutzrechtsverletzung oder sonstigen Rechtsverletzungen, sondern seitdem sehen die EVB-IT eine Haftungsregelung für alle Haftungstatbestände (also auch Tatbestände wie beispielsweise deliktische Ansprüche) vor. Die Haftung wird i. d. R. auf den Auftragswert beschränkt, ausgenommen, der Auftragswert beträgt weniger als 25.000 Euro; in diesen Fällen sehen die EVB-IT eine Haftung von 50.000 Euro vor.

Änderungen der EVB-IT: Individuelle Anpassungen

Den EVB-IT wird über das Haushaltsrecht der öffentlichen Hand der Charakter einer verbindlichen Dienstanweisung beigemessen. Daher sind Abweichungen nur dort möglich, wo die EVB-IT selbst für den Auftraggeber Regelungsspielräume eröffnen.[11]

Werden EVB-IT Verträge hingegen bei Verträgen zwischen Privaten angewendet, ist grundsätzlich auch eine Modifizierung möglich. Hierbei ist aber dem Umstand von „Treu und Glauben“ zu folgen: Da die EVB-IT Verträge und deren Inhalte gut bekannt sind, muss auf Änderungen ausdrücklich und gut sichtbar hingewiesen werden. In Ausschreibungen erwiesen sich hier Mapping-Tabellen in der Form

Vertragsort	Regelung EVB-IT	Eigene Regelung
Vertrag, Ziffer 1.3	xxx	yyy
AGB, Ziffer 3.4	…	…
Kriterienkatalog, Abschnitt I, Nr. 3	…	
…	…	…

als hilfreich. Zu beachten ist natürlich, dass die Anpassungen nicht anderen Vertragsbestandteilen widersprechen dürfen. Beispielsweise kann nicht in den EVB-IT Cloud AGB Ziffer 1.2 gelöscht werden, d. h. auf die Umsetzung des BSI C5 Katalogs verzichtet werden, ohne auch a) in anderer Form die angemessene IT-Sicherheit zu gewährleisten und b) alle anderen verweise auf den BSI C5 Katalog ebenfalls anzupassen. Sollte eine Anpassung eines der EVB-IT-Vertragsmuster bei Verträgen zwischen Privaten gewünscht sein, empfiehlt sich die Hinzuziehung einer auf IT-Recht spezialisierten Kanzlei – idealerweise mit entsprechender Expertise bzgl. öffentlicher Ausschreibungen und den darin eingesetzten, jetzt anzupassenden EVB-IT Vertragsmustern.

Cloud Computing ist Outsourcing

Wird Cloud Computing durch einen externen Anbieter betrieben, handelt es sich regelmäßig um eine Form des Outsourcings. Sowohl im Sozialgesetzbuch wie auch in verschiedenen für Krankenhäuser geltenden Landesgesetzen finden sich Vorgaben, wann überhaupt Outsourcing betrieben werden darf.

Beispiel § 80 Abs. 3 SGB 10:

„Die Erteilung eines Auftrags zur Verarbeitung von Sozialdaten durch nicht-öffentliche Stellen ist nur zulässig, wenn

1. beim Verantwortlichen sonst Störungen im Betriebsablauf auftreten können oder
2. die übertragenen Arbeiten beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden können.

[11] Müglich A.: Teil 191 Vertragsbedingungen der öffentlichen Hand EVB-IT, Rn. 72. In: Taeger/Pohle, Computerrechts-Handbuch. C. H. Beck Verlag, 37. Auflage. 2021. ISBN 978-3-406-31830-6

Entsprechend Formulierungen finden sich auch in einigen Landeskrankenhausgesetzen. D. h. für *jede* Form des Outsourcings muss in diesen Fällen eine dieser Bedingungen erfüllt werden. Um im Beispiel zu bleiben:

a) Störungen im Betriebsablauf
   Es muss also dargestellt werden, welche Störungen ohne Outsourcing/Auftragsverarbeitungen auftreten würden, die mit Outsourcing (aus welchen Gründen?) vermieden werden können. Wird eine Abwicklung der Leistungen zu Lasten des Leistungsempfängers (verzögerte Behandlung mit daraus resultierender Gefährdung der Gesundheit Bei Leistungserbringern bzw. Verzögerungen von Leistungsbewilligungen durch eine Krankenversicherung gegenüber der versicherten Person) ohne Auftragsverarbeitung verzögert, kann dies z. B. eine Störung im Betriebsablauf darstellen.
b) **Erheblich** kostengünstiger
   Es reicht nicht, dass Aufträge vom Dienstleister kostengünstiger erledigt werden, sondern es muss **erheblich** kostengünstiger erfolgen. „Erheblich" ist gesetzlich nicht definiert, daher wird man eine Einzelfallprüfung durchführen müssen. I. d. R. wird eine Vergleichsberechnung hinsichtlich der zu erwartenden Kosten erforderlich sein.
   Bei Beurteilung ist grundsätzlich zu beachten:
   a. Der Gesetzeszweck muss beachtet werden. Durch die Aufnahme entsprechender Bedingungen will der jeweilige Gesetzgeber eine Begrenzung der Datenverarbeitung durch externe Stellen erzielen.
   b. Der Schutzbedarf von Gesundheits- und Sozialdaten ist sehr hoch.
   c. Es muss sich eine **Ersparnis** ergeben, die bei **objektiver Betrachtung** die **eigene Datenverarbeitung** schlichtweg **unwirtschaftlich und unverhältnismäßig erscheinen lässt**.[12]

Verantwortlich für die Einhaltung entsprechender für den Auftraggeber geltenden Vorgaben ist stets der Auftraggeber selbst, die Verantwortung zur Einhaltung kann der Auftraggeber auch nicht vertraglich weitergeben. Eine Regelung wie „der Auftragnehmer ist dafür verantwortlich, die übertragenen Aufgaben erheblich günstiger durchzuführen" wäre nicht wirksam; es ist Sache des Auftraggebers, Preise zu vergleichen und zu bewerten. Gleiches gilt für alle anderen Vorbedingungen, die für ein Outsourcing im jeweils für den Auftraggeber geltenden Rahmenwerk zu finden sind. Der Auftraggeber muss durch vertragliche/organisatorische Regelungen und ggf. auch technische Maßnahmen die Erfüllung der gesetzlichen Forderungen gewährleisten.

Selbstverständlich sind Regelungen wie „Verarbeitung nur im Geltungsbereich des Grundgesetzes" oder „es dürfen nur Beschäftigte eingesetzt werden, die unter dem Geltungsbereich des § 203 StGB fallen und entsprechend verpflichtet wurden" zulässig, da in diesen Fällen der Auftraggeber seine gesetzliche Verantwortung wahrnimmt, aber nicht weitergibt.

Cloud Computing Verträge: SaaS als Mietvertrag

In seiner „ASP-Entscheidung"[13] unterwarf der BGH Cloud Computing Verträge im weitesten Sinne grundsätzlich dem Mietvertragsrecht, insbesondere die im Bereich der Gesundheitsversorgung besonders im Fokus stehenden SaaS-Angebote. Dementsprechend sind die Regelungen für Mietverträge auch für Cloud-Dienstleistungen anzuwenden. Auch der EVB-IT Cloud-Vertrag ist somit aus rechtlicher Sicht im Wesentlichen als ein Mietvertrag anzusehen.

[12] * So z.B. Herbst S.: § 80 Rn. 64. In: Hrsg: Rolfs (geschf.) / Körner / Krasney / Mutschler: Kasseler Kommentar SGB X., Stand 2023-0215

[13] BGH, Urt. v. 2006-11-15 Az. XII ZR 120/04. Online, zitiert am 2023-08-28; verfügbar unter https://dejure.org/2006,247, Volltext unter https://openjur.de/u/79503.html

Ergänzend zum deutschen Recht muss beachtet werden, dass die Richtlinie (EU) 2019/770[14] (häufig als „Digitale-Inhalte-Richtlinie“ bezeichnet) entsprechend ErwGr. 19, 41, 51 und 57 ausdrücklich Cloud-Dienste adressiert. In dieser Richtlinie werden Themen wie beispielsweise Anforderungen an die Vertragsmäßigkeit, Gewährleistungspflichten oder auch die Haftung des die Dienstleistung anbietenden Unternehmens geregelt. Wie bei Richtlinien üblich bestehen für den nationalen Gesetzgeber Anpassungsmöglichkeiten, z. B. richten sich die Gewährleistung oder auch die Verjährungsfristen grundsätzlich nach nationalem Recht. Weiterhin enthält die Richtlinie (EU) 2019/770 diverse Öffnungsklauseln für den nationalen Gesetzgeber, u. a. betrifft dies das Zustandekommen, die Gültigkeit, die Nichtigkeit oder die Wirkungen von Verträgen. Dabei muss der nationale Gesetzgeber eine unionskonforme Umsetzung gewährleisten.

Die nationale Umsetzung gestaltete das Bundesministerium der Justiz und für Verbraucherschutz, der Bundestag stimmte am 24. Juni 2021 dem Gesetzesentwurf „zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags“ zu.[15] Das Gesetz wurde am 30. Juni 2021 im Bundesgesetzblatt veröffentlicht[16] und trat am 1. Januar 2022 in Kraft. Mit dem Gesetz erfolgten die sich aus der Richtlinie (EU) 2019/770 ergebenden notwendigen Anpassungen im BGB. Allerdings adressiert Richtlinie (EU) 2019/770 Verbraucherverträge. Der Anwendungsbereich der Richtlinie hätte eine Erstreckung auf B2B-Verträge durch den jeweiligen nationalen Gesetzgeber nicht ausgeschlossen, jedoch wurde vom deutschen Gesetzgeber diese Möglichkeit nicht genutzt. Daher werden von diesen Umsetzungs-Regelungen nur B2C-Verträge erfasst, nicht hingegen B2B-Verträge.

Im Rahmen der EVB-IT Cloud handelt es sich regelhaft um B2B-Verträge, weswegen die Richtlinie (EU) 2019/770 in diesem Kontext regelhaft nicht anwendbar sein wird.

Cloud und Datenschutz: Orientierungshilfe des Bayerische Landesbeauftragte für den Datenschutz

Im April 2023 veröffentlichte der Bayerische Landesbeauftragte für den Datenschutz die Orientierungshilfe „Datenschutz als Kriterium im Vergabeverfahren“[17], in welcher die Situation der Cloud-Verarbeitung an verschiedenen Stellen betrachtet wird und sogar ein eigenes Kapitel („VII. Besondere Problemstellung: Beschaffung von Cloud-Services“) erhielt.

Im angesprochenen Kapitel VII wird einerseits die aktuelle Rechtslage mit Stand April 2023 betrachtet (inkl. des damals nur als Ankündigung vorliegenden Angemessenheitsbeschluss der Europäischen Kommission), als auch diverse Einzelaspekte besprochen.

Der Bayerische Landesbeauftragte für den Datenschutz weist im Rahmen der rechtlichen Betrachtung (Rn. 85-87) darauf hin, dass bei Konstellationen, bei denen „die Daten zwar in der EU beziehungsweise dem EWR verarbeitet werden, Anbieter der betreffenden Cloud allerdings eine Tochter eines US-amerikanischen Unternehmens ist“, „mit Blick auf den CLOUD Act sowie FISA 702 die abstrakte Gefahr einer nach EU-Recht unzulässigen Übermittlung von personenbezogenen Daten in einen Drittstaat“

[14] Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. Online, zitiert am 2023-08-28; verfügbar unter https://eur-lex.europa.eu/eli/dir/2019/770/oj

[15] Deutscher Bundestag: Verkauf von Sachen mit digitalen Elementen. Online, zitiert am 2023-08-28; verfügbar unter https://www.bundestag.de/dokumente/textarchiv/2021/kw18-pa-recht-digitale-inhalte-837652

[16] Bundesgesetzblatt Teil 1, Ausgabe Nr. 37 vom 30.06.2021: "Gesetz zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags". Online, zitiert am 2023-08-28; verfügbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s2133.pdf

[17] Der Bayerische Landesbeauftragte für den Datenschutz: Orientierungshilfe „Datenschutz als Kriterium im Vergabeverfahren“. Online, zitiert am 2023-08-18; verfügbar unter https://www.datenschutz-bayern.de/datenschutzreform2018/ bzw. Direktlink zur pdf-Datei https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Vergabe.pdf

besteht und in diesen Fällen an die nach Art. 28 Abs. 1 DS-GVO erforderliche Prüfung der Zuverlässigkeit des Auftragsverarbeiters (und deren Dokumentation) in diesem Fall besonders hohe Anforderungen zu stellen sind. Dementsprechend müssen die (dokumentierten und prüfbaren) technische und organisatorische Maßnahmen ein dem Schutzniveau der Daten entsprechendes Datenschutzniveau; im Kontext von Gesundheitsdaten ist dementsprechend ein sehr hohes Schutzniveau zu gewährleisten.

Amerikanische Cloud-Anbieter und Vergabeverfahren

Die Vergabekammer des Bundes urteilte aus Sicht des deutschen Vergaberechts am 13.02.2023[18] darüber, ob ein in Deutschland registriertes Unternehmen mit amerikanischer Muttergesellschaft aufgrund der datenschutzrechtlichen Bestimmungen der Vergabeunterlagen als Bieter aus einem Vergabeverfahren auszuschließen sei.

Gegenstand der Ausschreibung war eine Rahmenvereinbarung mehrerer gesetzlicher Krankenkassen für technische Anwendungen in Bezug auf die elektronische Patientenakte (ePA). Im Streitverfahren ging es darum, dass ein deutsches Tochterunternehmen einer US-amerikanischen Muttergesellschaft den Zuschlag bekommen sollte. Das Tochterunternehmen sicherte im Rahmen der Ausschreibung zu, dass alle Daten auf Servern im Inland verarbeitet werden und erklärte, dass das Tochterunternehmen Weisungen der Muttergesellschaft in Bezug auf die Herausgabe von Daten nicht befolgen würde.

Ein Mitwettbewerber klagte gegen diesen Zuschlag, da der Mitwettberber darin einen Verstoß gegen § 80 Abs. 2 SGB X sah.

Die Vergabekammer Bund bewertete den Nachprüfungsantrag als unbegründet, da keinerlei vergaberechtliche Verstöße festzustellen seien.

Bzgl. der datenschutzrechtlichen Argumentation beim Antrag führte die Vergabekammer Bund aus, dass allein durch das Vorhandensein einer amerikanischen Muttergesellschaft kein Verstoß gegen § 80 Abs. 2 SGB X vorläge:

> „Denn die Auftragsdatenverarbeitung erfolgt nach dem Angebot der Bg ausschließlich in Deutschland. Ob ein Angemessenheitsbeschluss für die USA vorliegt, ist daher irrelevant, denn es greift in Bezug auf das Angebotskonzept der Bg mit ihrer Nachunternehmerin bereits die 1. Alternative von § 80 Abs. 2 SGB X, die Verarbeitung im Inland. Eines Angemessenheitsbeschlusses für die USA bedürfte es nur, wenn eine Datenverarbeitung in den USA stattfände, was aufgrund der alleinigen Verarbeitung im Inland gerade nicht der Fall ist.
>
> Auf das Leistungsversprechen der Bg dürfen die Ag vertrauen (so grundlegend bereits OLG Düsseldorf, Beschluss vom 17.02.2016 - Verg 37/14 zu Eigenerklärungen, ferner z. B. Beschluss vom 26. August 2018 – Verg 23/18 zum Vertrauen des Auftraggebers auf die Einhaltung vertraglicher Zusagen durch den Bieter als späteren Auftragnehmer; konkret in Bezug auf Datenschutzzusagen einer europäischen Tochtergesellschaft eines US-amerikanischen Mutterkonzerns OLG Karlsruhe, Beschluss vom 7. September 2022 – 15 Verg 8/22), denn es gibt keinen Anlass, anzunehmen, die Nachunternehmerin könnte nicht in der Lage sein, ihre Zusagen einzuhalten […]“

Die Vergabekammer Bund argumentiere weiter:

> „Eine Art von eigenmächtigem, zwangsweisen Datenzugriff amerikanischer Behörden ist – ungeachtet dessen, wie wahrscheinlich ein solches Ansinnen in der Praxis überhaupt sein kann

[18] VK Bund, Beschluss 2023-02-13 Az. VK 2-114/22. Online, zitiert am 2023-10-08; verfügbar unter https://dejure.org/2023,2700 bzw. Volltext unter https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Vergaberecht/2023/VK2-114-22.html

- mangels US-amerikanischer Staatsgewalt in Deutschland nicht realisierbar. Ebenso wenig kann die Unterauftragnehmerin der Bg über ihre Muttergesellschaft gezwungen werden, Daten an diese herauszugeben. Denn in der Übermittlung an die in den USA ansässige amerikanische Muttergesellschaft der Unterauftragnehmerin läge nicht nur eine im Verhältnis zu den Ag weisungs- und damit vertragswidrige Datenherausgabe, sondern daneben ein Verstoß gegen § 80 Abs. 2 SGB X. Eine Datenübermittlung an die amerikanische Muttergesellschaft wäre nach dieser Vorschrift rechtswidrig […]“

Weiterhin urteilte die Vergabekammer Bund, dass das Vergaberecht den Ausschluss des Angebots selbst nicht gebietet und einen Ausschluss auch gar nicht zulässt.

EVB-IT Cloud: Reihenfolge der Vertragsbestandteile

Im EVB-IT Cloud werden unter Ziffer 1.2 die Vertragsbestandteile benannt und auch die Reihenfolge, in welcher die Dokumente anzuwenden sind, angegeben. Demnach gilt die Reihenfolge:

1) EVB-IT Cloud Vertrag
2) Leistungsbeschreibung (sofern separat vorhanden)
3) EVB-IT Cloud Kriterienkatalog für Cloudleistungen
4) EVB-IT Cloud Anlage zur Einbeziehung von auftragnehmerseitigen AGB
5) Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitungsvertrag, AVV)
6) EVB-IT Cloud AGB
7) Allgemeine Vertragsbedingungen für die Ausführung von Leistungen (VOL/B)
8) Auftragnehmerseitige AGB (wenn seitens Auftraggeber zugelassen)

Über die Anlage zur Einbeziehung von auftragnehmerseitigen AGB können **einzelne** Regelungen von auftragnehmerseitigen AGB auch vorrangig anwendbar sein. In diesem Fall gilt die Reihenfolge:

1) EVB-IT Cloud Vertrag
2) Leistungsbeschreibung (sofern separat vorhanden)
3) EVB-IT Cloud Kriterienkatalog für Cloudleistungen
4) EVB-IT Cloud Anlage zur Einbeziehung von auftragnehmerseitigen AGB
5) Einzelne, von Auftraggeber ausgewählte Regelungen der auftragnehmerseitigen AGB
6) Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitungsvertrag, AVV)
7) EVB-IT Cloud AGB
8) Allgemeine Vertragsbedingungen für die Ausführung von Leistungen (VOL/B)
9) Auftragnehmerseitige AGB (wenn seitens Auftraggeber zugelassen)

Vertrag über Cloudleistungen

Vorbemerkung

In den meisten Fällen wird Cloud Computing im Gesundheitswesen vermutlich eingesetzt, um damit eine Software wie ein Informations-System zu betreiben. Im Gesundheitswesen wird klassisch Software gekauft und dabei Pflege und Wartung als Zusatzleistung eingekauft. Cloud Computing ist im Regelfall ein Mietvertrag, d. h. keine Beschaffung im eigenen Sinne. Beim Einsatz vom EVB-IT Cloud sollte daher unbedingt beachtet werden:

1) Es handelt sich um einen Cloud-Vertrag. Software steht hier nicht im Fokus.
2) Viele Aspekte, die man in einem Software-Kaufvertrag regeln würde, finden sich daher im EVB-IT Cloud entweder gar nicht wieder oder sind nur rudimentär angesprochen.
3) Ggf. sollte daher überlegt werden, ob man ergänzend einen Vertrag zur Software-Miete nutzen will. Es gibt zwei EVB-IT Verträge, die Softwareüberlassung adressieren:
    a. EVB-IT Überlassung Typ A (Überlassung und Nutzung von Standardsoftware auf Dauer)
    b. EVB-IT Überlassung Typ B (zeitlich befristete Überlassung und Nutzung von Software)

    Ergänzend findet sich noch der EVB-IT Pflege S (Wartungsvertrag für Standardsoftware).

Bei der Nutzung des EVB-IT Cloud-Vertrages ist also zu beachten, dass im Wesentlichen „nur“ Cloud-Beschaffung im Fokus des Vertragswerks geregelt ist. Dies aber dafür gut. Will man ergänzend noch andere Aspekte geregelt haben und findet diese im EVB-IT Cloud Vertrag nicht oder nicht ausreichend berücksichtigt, so muss man ggf. ergänzende Verträge abschließen.

Allgemeines

Die Grundregeln für die Leistungserbringung sind in den Allgemeinen Geschäftsbedingungen enthalten und bilden somit das Herzstück des EVB-IT Cloudvertrages. Diese Regeln repräsentieren die Mindestanforderungen, die sämtliche Cloud-Anbieter erfüllen müssen, wodurch in Ausschreibungen die vergaberechtlich vorgeschriebene Vergleichbarkeit der Angebote gewährleistet wird.

Der Kriterienkatalog erlaubt Einschränkungen wie auch Ergänzungen bzgl. der vertraglich vereinbarten Leistungen. Datensicherung beispielsweise ist kein Cloud-Thema, wird entsprechend seitens der EVB-IT Cloud-Vertrages auch nicht geregelt und kann nur über den Kriterienkatalog als ergänzende Leistung vereinbart werden.

Je nach getroffener Auswahl kann dementsprechend der Bieterkreis erweitert oder eingeschränkt werden. Z. B., weil einzelne Anbieter keine Backup-Lösung im Angebot beinhalten oder in ihrem Angebot auf eine Verarbeitung in Drittstaaten ohne seitens EU-Kommission anerkanntes Datenschutz-Niveau angewiesen sind. Daher kann es von Vorteil sein, im Vorfeld eine Marktanalyse durchzuführen und zu evaluieren, welchen Rahmenbedingungen die wichtigsten potenziellen Bieter unterliegen und zu prüfen, ob man diesen Rahmenbedingungen aufgrund geltender rechtlicher Verpflichtungen oder auch anderer Vorgaben entgegenkommen kann. Ist dies nicht möglich, muss der Auftraggeber damit rechnen, dass relevante potenzielle Bieter sich nicht an der Ausschreibung beteiligen können.

Weiterhin ist eine vorhergehende Marktanalyse hilfreich, um die Anzahl von Bieternachfragen im Ausscheidungsprozess vorab zu reduzieren, da vorab wichtige Fragen bereits geklärt wurden.

Abschnitt „1 Gegenstand und Bestandteile des Vertrages“

Zu Ziffer 1.2.1

1.2.1 dieser Vertragstext mit den folgenden Anlagen:

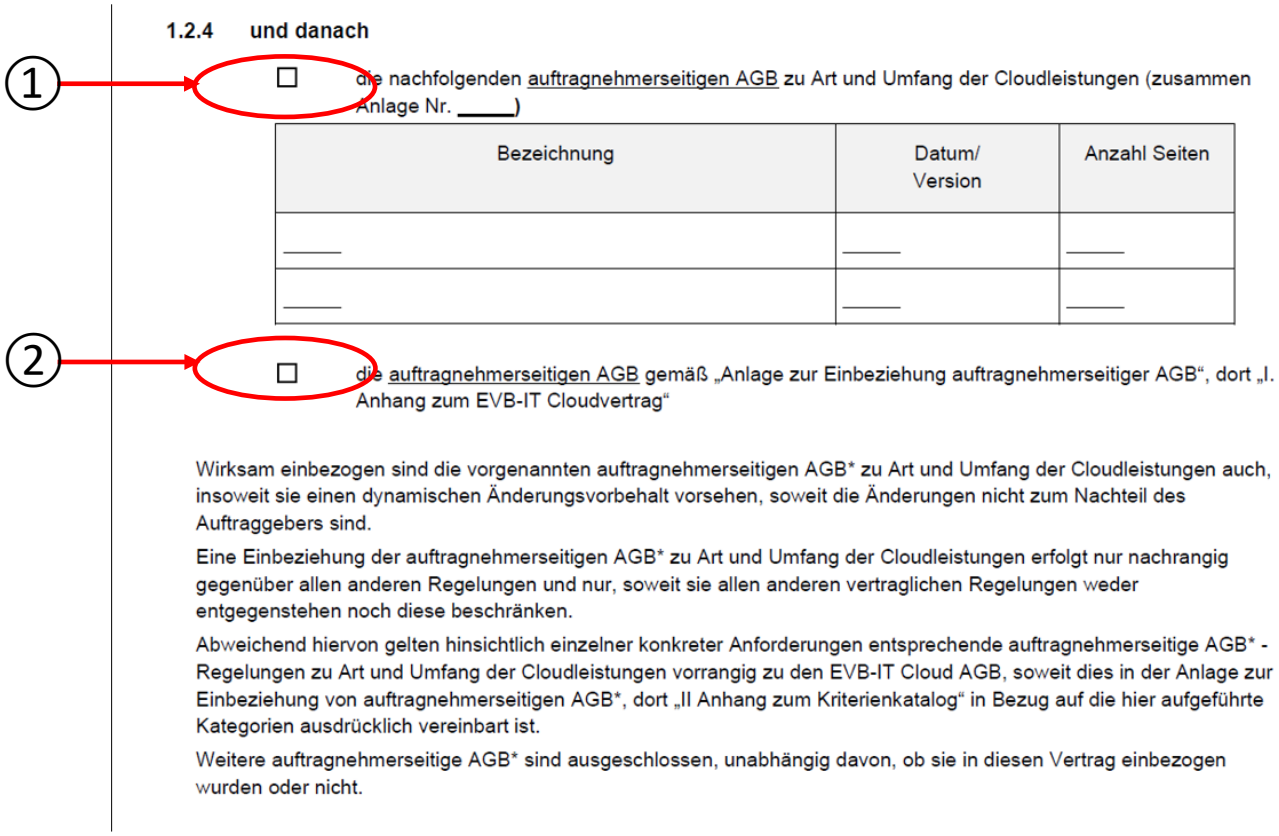
Anlagen zum EVB-IT Cloudvertrag (Achtung: Die auftragnehmerseitigen AGB sind nicht hier, sondern in Nummer 1.2.4 anzugeben)			
Anlage Nr.	Bezeichnung	Datum/ Version	Anzahl Seiten
1	2	3	4
1	_____	_____	_____
2	_____	_____	_____
3	Kriterienkatalog für Cloudleistungen (ggf. mehrere Kriterienkataloge, dann Anlage Nr. 3a, 3b etc.), inklusive Anlage zur Einbeziehung von auftragnehmerseitigen AGB mit Anhang I und II ▫	_____	_____
4	Vereinbarung zur Auftragsverarbeitung (AVV) inklusive der technischen und organisatorischen Maßnahmen (TOM)	_____	_____

☐ Es gelten die Anlagen in folgender Rangfolge _____.

Verträge zur Auftragsverarbeitung gelten entsprechend Ziffer 1.2.1 nachrangig gegenüber dem Vertrag über Cloudleistungen sowie gegenüber dem Kriterienkatalog für Cloudleistungen. Sowohl der Vertrag über Cloudleistungen als auch der Kriterienkatalog für Cloudleistungen enthalten Vorgaben hinsichtlich datenschutzrechtlicher Themen, z. B. die Einbeziehung von Unterauftragnehmern.

Viele Verträge zur Verarbeitung im Auftrag enthalten eine Regelung, dass die in einem Vertrag zur Verarbeitung im Auftrag enthaltenen Regelungen vorrangig gegenüber denen in einem Hauptvertrag anzuwenden sind. In diesen Fällen muss der Auftraggeber seinen Vertrag zur Verarbeitung im Auftrag anpassen, dass speziell bei Anwendung des Vertrags über Cloudleistungen dieser vor den Regelungen im Vertrag über Auftragsverarbeitung anwendbar ist.

Zu Ziffer 1.2.4



1.2.4 und danach

① ☐ die nachfolgenden auftragnehmerseitigen AGB zu Art und Umfang der Cloudleistungen (zusammen Anlage Nr. _____)

Bezeichnung	Datum/ Version	Anzahl Seiten
_____	_____	_____
_____	_____	_____

② ☐ die auftragnehmerseitigen AGB gemäß „Anlage zur Einbeziehung auftragnehmerseitiger AGB", dort „I. Anhang zum EVB-IT Cloudvertrag"

Wirksam einbezogen sind die vorgenannten auftragnehmerseitigen AGB* zu Art und Umfang der Cloudleistungen auch, insoweit sie einen dynamischen Änderungsvorbehalt vorsehen, soweit die Änderungen nicht zum Nachteil des Auftraggebers sind.

Eine Einbeziehung der auftragnehmerseitigen AGB* zu Art und Umfang der Cloudleistungen erfolgt nur nachrangig gegenüber allen anderen Regelungen und nur, soweit sie allen anderen vertraglichen Regelungen weder entgegenstehen noch diese beschränken.

Abweichend hiervon gelten hinsichtlich einzelner konkreter Anforderungen entsprechende auftragnehmerseitige AGB* - Regelungen zu Art und Umfang der Cloudleistungen vorrangig zu den EVB-IT Cloud AGB, soweit dies in der Anlage zur Einbeziehung von auftragnehmerseitigen AGB*, dort „II Anhang zum Kriterienkatalog" in Bezug auf die hier aufgeführte Kategorien ausdrücklich vereinbart ist.

Weitere auftragnehmerseitige AGB* sind ausgeschlossen, unabhängig davon, ob sie in diesen Vertrag einbezogen wurden oder nicht.

Hier wird die Einbeziehung auftragnehmerseitige AGB geregelt. Nur der Auftraggeber hat das Recht, hier ein Kreuz zu setzen und somit die Einbeziehung auftragnehmerseitige AGB zu erlauben.

Wird ein Kreuz im ersten Ankreuzfeld (mit „①" gekennzeichnet) gesetzt, sind auftragnehmerseitige AGB nur nachrangig anwendbar, d. h. auftragnehmerseitige AGB sind nur anwendbar, wenn diese auftragnehmerseitigen AGB nicht Regelungen durch Vertrag über Cloud-Dienstleistungen sowie den dazugehörigen in den Ziffern 1.2.1., 1.2.2 und 1.2.3 beschriebenen Anlagen widersprechen.

Wird ein Kreuz im zweiten Ankreuzfeld (mit „②" gekennzeichnet) gesetzt, erfolgt die Regelung durch die „Anlage zur Einbeziehung auftragnehmerseitiger AGB". Diese Anlage soll kontrolliert und vergaberechtskonform die Öffnung der EVB-IT Cloud für auftragnehmerseitige AGB ermöglichen, wobei insbesondere die Vergleichbarkeit der Angebote auch durch Zulassung von punktuell vorrangig anwendbaren auftragnehmerseitige AGB erhalten bleiben soll.[19] In der Anlage gibt es zwei Möglichkeiten zur Einbindung von auftragnehmerseitigen AGB:

1. I. Anhang zum EVB-IT Cloudvertrag
   In diesem Abschnitt angegebene auftragnehmerseitige AGB gelten ebenfalls nur nachrangig; dass oben gesagte zur nachrangigen Anwendbarkeit gilt entsprechend.
2. II. Anhang zum Kriterienkatalog
   In diesem Abschnitt angegebene auftragnehmerseitige AGB können **punktuell**, d. h. für einzelne Klauseln der auftraggeberseitigen AGB geltend, **vorrangig** vor den Regelungen im Vertrag über Cloud-Dienstleistungen sowie den dazugehörigen in den Ziffern 1.2.1., 1.2.2 und 1.2.3 beschriebenen Anlagen gelten. Es muss **seitens Auftraggeber** festgelegt werden, in welchen Bereichen eine vorrangige Anwendbarkeit von auftragnehmerseitigen AGB ermöglicht wird. Seitens des Anhangs zum Kriterienkatalog sind nur Klauseln mit Bezug

[19] Siehe Seite 2, Tabellenpunkt „4" in „EVB-IT Cloud: Hinweise zur Nutzung – Kurzfassung"

- zum Leistungsort,
- dem Übergabepunkt,
- den Nutzern,
- der Lizenzmetrik,
- den Endgeräten,
- der Datensicherung,
- Gutschriften,
- der Protokollierung und
- dem Reporting

vorgesehen, eine pauschale Zulassung auftragnehmerseitiger AGB ist nicht möglich.

In den Nutzungshinweisen[19] wird dargestellt, dass der Auftraggeber im Vorfeld (z. B. in Form einer Markterkundung) die Punkte identifizieren soll, in denen für den Auftraggeber eine Geltung von auftragnehmerseitigen AGB in Betracht kommt und diese Punkte sollen dann zum Gegenstand des Verfahrens gemacht werden, z. B. in Form von Bewertungskriterien in einer Leistungsbewertungsmatrix, mittels derer die Vergleichbarkeit der Angebote für eine Angebotsbewertung hergestellt wird.

Abschnitt „2 Überblick über die vereinbarten Leistungen“

Abschnitt 2 bietet einen Überblick der vertraglich zu vereinbarenden Leistungen. Hierbei kann der Auftraggeber das gewünschten Cloud-Model, also IaaS, SaaS oder PaaS auswählen, sowie zusätzliche Leistungen zu Beginn und nach Ende der eigentlichen Cloudmiete wählen.

Nicht immer wird sowohl Software as a Service (SaaS) als auch Platform as a Service (PaaS) ausgeschrieben, es sind auch Konstellationen denkbar, wo der Auftraggeber die Plattform selbst zur Verfügung stellt (z. B., weil die Plattform bereits bei einem anderen Cloud-Anbieter eingekauft wurde, oder der Auftraggeber nur eine PaaS-Leistung einkaufen will, weil der Auftraggeber die Software selbst betreibt. Im Vertrag ist beides nur gemeinsam auswählbar, es wird daher dazu geraten, entweder das nicht gewünschte durchzustreichen oder den Vertrag dahingehend zu ändern, dass beide Möglichkeiten separat auswählbar sind.

Die unterschiedlichen Clouddienste und Modelle unterscheiden sich maßgeblich der organisatorischen bzw. technischen Kontrollmöglichkeiten des Cloudnutzers:

- Im SaaS-Modell gibt der Nutzer im Wesentlichen die gesamte Kontrolle an den Cloudanbieter ab.
- Im PaaS-Modell behält der Nutzer lediglich die Kontrolle über seine Anwendungen, die auf der Plattform ausgeführt werden.
- Im IaaS-Modell hat der Nutzer die volle Kontrolle über das IT-System ab dem Betriebssystem (wobei die Kontrolle für die physische Umgebung immer beim Anbieter liegt), da alles innerhalb seines Verantwortungsbereichs betrieben wird.

Zudem definiert der EVB-IT-Cloudvertrag die einzelnen Leistungen in den AGB auf den Seiten 18 ff. unter Begriffsbestimmungen.

- Managed Cloud Services (MCS): Managed Cloud Services sind Leistungen, die über die typischen Leistungspflichten des Auftragnehmers hinausgehen, z. B. die Benutzerverwaltung, ggf. die Verwaltung verschiedener Cloud-Angebote bzw. Optionen, Kapazitätsmanagement, Beratung bei Upgrade- und Lizenzfragen etc. - jeweils ausgerichtet am individuellen Bedarf des Auftraggebers.

Der Kriterienkatalog listet in Nr. 2 bereits eine Auswahl gängiger MCS-Leistungen, die jedoch auch über eine Anlage erweitert werden können. Auch Aktivitäten, die im Standardfall als Mitwirkungsobliegenheiten des Auftraggebers, wie in Ziff. 17 AGB geregelt sind, können mit Hilfe von Nr. 2 des Kriterienkatalogs als MCS-Leistungen an den Auftragnehmer delegiert werden.[20]

Darüber hinaus können anderweitige gewünschte Leistungen, die keiner Dienstleistung in der Cloud entsprechen, als sonstige Leitungen vereinbart werden. Denkbar wären beispielsweise Schulungen oder Anwendertrainings sowie Projektmanagement rund um die Implementierung eines neuen Systems.

[20] Bitkom e. V.: Frequently Asked Questions zu den EVB-IT Cloud, S. 6. Online, zitiert am 2023-08-11; verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Frequently-Asked-Questions-zu-den-EVB-IT-Cloud

Abschnitt „3 Gegenstand der Leistungen“

In Abschnitt 3 werden die Details des Leistungsgegenstandes festgelegt.

Zu Ziffer 3.1

3.1 Leistungen gemäß Ziffer 1.1 EVB-IT Cloud-AGB

Lfd. Nr.	Produkt/Leistung: (Produkt- und Leistungsbeschreibung und/oder Verweis auf Kriterienkatalog(e) für Cloudleistung in Anlage Nr. 3)	Menge	MVD[1]	Beginn[2]	Ende/Termin[3]	Abweichende Kündigungsfrist in Monaten[4]	Automatische Verlängerung um Anzahl Monate[5]	Monatlicher Preis oder, abweichendes Preismodell gemäß Anlage[6]
1	2		3	4	5	6	7	8
_____	_____	_____	_____	_____	_____	_____	_____	_____

Der in Ziff. 3.1 aufgeführte Termin- und Leistungsplan bietet die Möglichkeit die Produkt- und Leistungsbeschreibung, die Mengenangaben, Laufzeiten und Preise in übersichtlicher und transparenter Weise im Detail festzuhalten.

Zu Ziffer 3.2

Ziff. 3.2 ermöglicht die Vereinbarung von einmaligen Leistungen, zu Beginn des Leistungszeitraumes und nach Ende dessen. Hierbei sind insbesondere Leistungen zum Setup der Software (Herbeiführung der Betriebsbereitschaft also dem Zeitpunkt, an dem die Leistung störungsfrei funktioniert) denkbar, wie auch Migrationsunterstützungen nach Ende der Laufzeit. Die Cloud-Portabilität, also die Fähigkeit, eine Anwendung (oder auch Daten) von einem Cloud-Dienstanbieter zu einem anderen zu verschieben, ohne sie neu schreiben oder umstrukturieren zu müssen, sollte unbedingt an dieser Stelle berücksichtigt werden. Diese Leistungen können entweder über eine Anlage näher definiert, oder gar in einen separaten Dienstleistungsvertrag verlagert werden. Zudem kann die dafür zu entrichtende Vergütung mittels Pauschale oder aufwandsbezogen vereinbart werden.

Zu Ziffer 3.3

3.3 Leistungen auf Abruf

Die Leistungen gemäß Nummer _____ (hier Nummer 3.1 lfd. Nr. X oder Nummer 3.2.2 eintragen) werden auf Abruf erbracht.

☐ Der Mindestvorlauf für den Abruf beträgt _____ (Stunden/Tage).

☐ Die geschätzte Abnahme beträgt _____ (Menge) pro _____ (z.B. Vertragsmonat/Vertragsquartal/Vertragsjahr/Vertragslaufzeit); die Höchstmenge bzw. der Höchstwert beträgt _____ (Menge/Euro).

☐ Die vereinbarte Mindestabnahme beträgt _____ (Menge) pro _____ (z.B. Vertragsmonat, Vertragsquartal, Vertragsjahr, Vertragslaufzeit).

Der Auftraggeber ist nicht zum Abruf verpflichtet. Dies gilt nicht für die hier ggf. vereinbarte Mindestabnahme.

Ziff. 3.3 versetzt den Auftraggeber in die Lage, Leistungen auf Abruf für die Zukunft zu vereinbaren und Konditionen für den Bedarfsfall festzulegen. Er ist jedoch nicht zum Abruf der Leistungen verpflichtet, sofern keine Mindestabnahme unter dieser Ziffer vereinbart wurde.

Zu Ziffer 3.4

3.4 Ticketsystem

☐ Für die Meldung, Klassifizierung und Bestätigung von Störungen*, sonstigen Meldungen und Anfragen sowie die Beobachtung und Überwachung des Bearbeitungsfortschritts verwenden die Parteien das Ticketsystem

_____

☐ des Auftragnehmers,

☐ des Auftraggebers,

welches

☐ unter der Web-Adresse _____ erreichbar ist.

☐ wie folgt zur Verfügung gestellt wird _____.

Ziff. 3.4 bietet die Möglichkeit, die Einbindung eines automatisierten Ticketsystems für den Supportfall zu regeln. Hier kann sowohl das Ticketsystem des Auftragnehmers als auch des Auftraggebers ausgewählt werden und per jeweiliger Web-Adresse hinterlegt werden.

Abschnitt „4 Fälligkeit und Zahlung der Vergütung“

Ziff. 4 fasst die vertraglichen Zahlungsmodalitäten zusammen und regelt die Fälligkeit der Zahlungen, die Rechnungsstellung sowie die Preisanpassungen, die entweder abweichend der oder sich beziehend auf den Standardregelungen zur Vergütung aus Ziff. 16 der EVB-IT Cloud AGB vereinbart werden sollen.

Zu Ziffer 4.3

4.3 Rechnungsadresse

☐ Die Rechnung ist nach den Vorgaben der E-Rechnungsverordnung elektronisch einzureichen.

In der Rechnung bzw. zur Rechnungserstellung ist die Leitweg-ID _____ anzugeben. Zudem müssen bei der Rechnung alle Pflichtfelder sowie die Zusatzfelder

_____

_____

gefüllt sein.

Eine Rechnung, die entgegen vorstehender Regelung nicht elektronisch gestellt wird, begründet keinen Verzug nach § 286 Abs. 3 BGB.

☐ Die Rechnungsanschrift ergibt sich aus Anlage Nr. _____.

Unter Ziff. 4.3 wird ausdrücklich auch die Nutzung der elektronischen Rechnungsstellung nach den Vorgaben der E-Rechnungsverordnung ermöglicht. D. h., bei der elektronischen Rechnungsstellung muss den Anforderungen der „Verordnung über die elektronische Rechnungsstellung im öffentlichen Auftragswesen des Bundes“[21] genügt werden. Somit muss entweder der Datenaustauschstandard XRechnung verwendet werden, oder ein anderer Datenaustauschstandard, welcher den Anforderungen der europäischen Norm für die elektronische Rechnungsstellung entspricht.

Zu Ziffer 4.4

4.4 Preisanpassung

☐ Es wird eine Preisanpassung vereinbart:

- ☐ gemäß Ziffer 16.5 EVB-IT-Cloud-AGB:
  - ☐ für den monatlichen Pauschalfestpreis gemäß Nummer 3.1.
  - ☐ für die folgenden weiteren Vergütungen: _____.
- ☐ gemäß Anlage Nr. _____.

Eine Preisanpassung während der Vertragslaufzeit muss ausdrücklich in Ziff. 4.4 aktiviert also durch explizite Vereinbarung beschlossen werden. Ziff. 16.5 der Cloud AGB regelt hierzu, dass eine Preiserhöhung frühestens nach Ablauf des ersten Jahres mit zusätzlicher drei-monatiger Ankündigung möglich ist und maximal 3 % der zum Zeitpunkt der Ankündigung der Erhöhung geltenden Vergütung betragen. Weitere Erhöhungen können wiederum frühestens 12 Monate nach Wirksamwerden der vorherigen Erhöhung angekündigt werden. Es kann somit gemessen am Tage des Leistungsbeginns, im Maximalfall nach 12 Monaten eine Erhöhung angekündigt und nach 15 Monaten umgesetzt werden, nach 27 Monaten Laufzeit erneut angekündigt und nach 30 Monaten erfolgen, wiederum nach 42 angekündigt und 45 Monaten erfolgen, usw. Alternativ dazu können in Ziff. 4.4 abweichende Regelungen getroffen werden.

[21] Verordnung über die elektronische Rechnungsstellung im öffentlichen Auftragswesen des Bundes (E-Rechnungsverordnung - ERechV). Online, abrufbar unter https://www.gesetze-im-internet.de/erechv/index.html

Abschnitt „6 Abweichende Haftungsregelungen“

Die Regelungen zur Haftungsbeschränkung sind im Allgemeinen in Ziffer 19 der EVB-IT Cloud AGB geregelt. Ziff. 19.1 beschränkt die Haftung für leichte Fahrlässigkeit insgesamt auf den Auftragswert. Im ersten Vertragsjahr bemisst sich die Haftungssumme jedoch mindestens auf das Doppelte und maximal das Vierfache der Vergütung, die für das erste Vertragsjahr zu zahlen ist. Bei einem Auftragswert von unter 50.000, - Euro, ist dies die Mindesthaftungsobergrenze, bei Sachschäden eine Million Euro, sofern der Auftragswert geringer als eine Million Euro beträgt.

Ziff. 6 des EVB-IT Cloudvertrages ermöglicht alternativ eine Abweichung von Ziff. 19 Cloud AGB bei leicht fahrlässigen Pflichtverletzungen durch die Ergänzung einer separaten Anlage. Es gilt hierbei zu beachten, dass Haftungsbeschränkungen durch AGB strengen Anforderungen des Gesetzgebers, gemäß §§ 305 ff BGB und Rechtsprechung, unterliegen. Ein Haftungsausschluss für grobe Fahrlässigkeit, Vorsatz, sowie bei Schäden resultierend aus der Verletzung des Lebens, des Körpers oder der Gesundheit ist in der Regel unwirksam. Ziffer 19.2 Cloud AGB sieht eine Haftung für entgangene Gewinne standardmäßig nicht vor, welches in Ziff. 6 Cloudvertrag jedoch verschärft werden kann.

Abschnitt „7 Beauftragte und Ansprechpartner“

Wie auch bereits aus anderen EVB-IT-Vertragsmustern bekannt, bietet auch der EVB-IT Cloud die Möglichkeit, explizite Ansprechpartner zu benennen und somit klare Zuständigkeiten zu vereinbaren.

Zu Ziffer 7.1

> **7.1 Beauftragte des Auftragnehmers (Name, Mailadresse)**
>
> ☐ Informationssicherheit: _____,
>
> ☐ Datenschutz: _____,
>
> ☐ Geheimschutz: _____.

Es sollte sachgemäß sein, unter Ziff. 7.1 auch generische Funktionen und dazugehörige E-Mail-Adressen einzutragen, um einem personellen Wechsel vorzubeugen. Ein Funktionstitel gibt zudem darüber Aufschluss, ob es sich beim benannten Ansprechpartner über den legal definierten Beauftragten, wie bspw. dem Datenschutzbeauftragten, handelt, oder um einen fachlichen Ansprechpartner, der sich dem Sachverhalt innerhalb des Geschäftsbereichs annimmt, ggfs. aber keine definierten Befugnisse ausübt. Gerade in Konzernstrukturen ist es nicht unüblich, dass mehrere Personen verschiedene Aspekte der Rolle ausüben.

Allerdings muss vom Auftraggeber immer auch ein Name angegeben werden, der zumindest zum Zeitpunkt des Vertragsabschlusses der zentrale Ansprechpartner bzgl. der adressierten Fragestellung ist, also z. B. der Name des Datenschutzbeauftragten.

Zu Ziffer 7.2

> **7.2 Ansprechpartner für Fragen zum Vertrag (Name, Mailadresse)**
>
> beim Auftragnehmer _____
>
> beim Aufraggeber _____

Bzgl. Ziffer 7.2 ist die namentliche Benennung nützlich, um eine persönliche Kontaktaufnahme zu vereinfachen. Hier sollte überlegt werden, ob parallel zur Mailadresse auch entsprechende telefonische Kontaktmöglichkeiten angeben werden.

Abschnitt „8 Weitere Regelungen“

Zu Ziffer 8.1

8.1 Besondere Anforderungen an Mitarbeiter des Auftragnehmers

☐ Für die Aufgaben gemäß Anlage Nr. _____ ist nur Personal einzusetzen, welches bereit ist, sich aufgrund des Verpflichtungsgesetzes verpflichten zu lassen.

☐ Mindestanforderungen an das einzusetzende Personal des Auftragnehmers (z.B. Sicherheitsüberprüfung nach SÜG) ergeben sich aus Anlage Nr. _____.

Ziff. 8.1 ermöglicht die Ergänzung besonderer Anforderungen an Mitarbeiter des Auftragnehmers, wie beispielsweise eine Sicherheitsüberprüfung nach SÜG einzufordern. Diese Anforderungen sollten sich primär an den sektorspezifischen Vorgaben orientieren und ggfs. auch rechtliche Vorgaben aus dem Berufsrecht einbeziehen. Im Gesundheitsbereich wäre hierbei insbesondere eine Verpflichtung des Personals des Auftragnehmers und seiner Unterauftragnehmer auf die Vorschrift § 203 StGB empfehlenswert, sofern die zu verarbeitenden Daten der gesetzlichen Schweigepflicht unterliegen.

Zu Ziffer 8.3

8.3 Prüfrechte

☐ Ergänzend zu Ziffer 6.4 EVB-IT Cloud-AGB und unbeschadet der gesetzlichen Regelungen, sind nicht nur der Auftraggeber und vom Auftraggeber zur Berufsverschwiegenheit verpflichtete Prüfungsgesellschaften, sondern auch

- ☐ die Aufsichtsorgane des Auftraggebers
- ☐ das BSI
- ☐ folgende von ihm benannte Prüfer _____

zur Prüfung der Einhaltung der Maßnahmen berechtigt. Der Auftragnehmer gewährt die dafür notwendigen Zutritts-, Einsichts- und Auskunftsrechte und unterstützt im erforderlichen Ausmaß.

☐ Ergänzend zu bzw. abweichend von Ziffer 6.4 EVB-IT Cloud-AGB ergeben sich Regelungen zu Prüfrechten aus Anlage Nr. _____.

Die in Ziff. 8.3 auszuwählenden Prüfrechte, die über Ziff. 6.4 EVB-IT Cloud AGB hinausgehen, sollten unter Berücksichtigung der für den Auftraggeber anzuwendenden Rechtsvorschriften ausgewählt werden. Hierbei können sich bspw. für Betreiber kritischer Infrastruktur gemäß KRITIS-Verordnung auch Prüfrechte des BSI ergeben, die unter Umständen auch sich beim Auftraggeber im Einsatz befindende Cloudanwendungen von Dritten umfassen.

Zu Ziffer 8.4

8.4 Unterauftragnehmer

☐ In Bezug auf den Einsatz von Unterauftragnehmern gilt anstelle von Ziffer 15.1 EVB-IT Cloud-AGB die Ziffer 15.2 EVB-IT Cloud-AGB.

Ziffer 8.4 regelt den Einbezug von Unterauftragnehmern durch den Auftragnehmer, der abweichend von den allgemeinen Regeln aus Ziff. 15 EVB-IT Cloud-AGB vereinbart werden soll und bietet die Möglichkeit einer Verschärfung der Vorgaben. Ziff. 15.1 in Verbindung mit Ziff. 15.2 EVB-IT Cloud-AGB sieht eine Benennung der Unterauftragnehmer vor und verpflichtet den Auftragnehmer bei Änderungen zur Benachrichtigung des Auftraggebers, und Einräumung einer 30-tägigen Widerspruchsfrist. Kann keine Einigung erzielt werden, verbleibt dem Auftraggeber ein außerordentliches Kündigungsrecht. Im Gegenzug dazu, fordert Ziff. 15.3 EVB-IT Cloud-AGB die ausdrückliche Zustimmung des Auftraggebers zur E7inbindung jeglicher Unterauftragnehmer.

Vergleichbare Regelungen sind aus dem Datenschutzrecht (vgl. Art. 28 Abs. 2 DSGVO) bekannt und bieten dem Auftraggeber eine größtmögliche Kontrolle der einzubeziehenden Unterauftragnehmer, die ggfs. auch als Unterauftragsverarbeiter im datenschutzrechtlichen Sinne tätig werden. Allerdings ist im Cloudumfeld darauf hinzuweisen, dass insbesondere bei Nutzung der Cloudangebote der sogenannten international agierenden Hyperscaler eine Zustimmungspflicht für den Einsatz von Unterauftragnehmern praktisch nicht umzusetzen ist und über deren AGB ausgeschlossen wird.

Zu Ziffer 8.6

8.6 Haftpflichtversicherung

☐ Der Nachweis einer Haftpflichtversicherung gemäß Ziffer 21 EVB-IT Cloud-AGB wird vereinbart.

Ziff. 8.6 ermöglicht den Nachweis einer Haftpflichtversicherung gemäß Ziffer 21 EVB-IT Cloud-AGB, welche im Rahmen und Umfang den marktüblichen Industriehaftpflichtversicherungen aus einem EU-Mitgliedsstaat entspricht. Der Auftragnehmer ist dazu verpflichtet den Versicherungsschutz bis zur Verjährung sämtlicher Mängelansprüche aufrecht zu erhalten.

Kriterienkatalog für Cloudleistungen

Der Kriterienkatalog ist ein fakultativer Bestandteil der EVB-IT Cloudvertragsunterlagen. Es obliegt dem Auftraggeber diesen zuzulassen, ggfs. als Checkliste zu nutzen, oder gänzlich auf die Nutzung dieser Anlage zu verzichten. Wenn jedoch Teile der AGB des Auftragnehmers zugelassen werden, ist seine Anwendung ratsam.

Der Kriterienkatalog erlaubt es, spezifische Anforderungen für die Cloud-Anwendungen festzulegen, die von den Bestimmungen in den EVB-IT Cloud AGB abweichen oder diese übertreffen können. Außerdem ermöglicht der Kriterienkatalog, auf bestimmte Leistungs- und Regelungsbereiche, zusätzliche Anlagen seitens des Auftraggebers sowie spezifische Bestimmungen in den AGB des Auftragnehmers zu verweisen.

Abschnitt „1 Kriterien“

Zu Ziffer 1

1.	Art der Cloud	☐ Public Cloud (Ressourcen werden für eine Vielzahl nicht näher bestimmter Kunden bereitgestellt) ☐ Private Cloud bzw. sonstige Cloud gemäß Anlage Nr. _____ (z.B. Hybrid-Cloud, künftige Private Government Cloud für öffentliche Stellen)

Die Arbeitsgruppe „Cloud in der Praxis“ des bvitg definiert die beiden verfügbaren Arten der Cloud entsprechend der ISO/IEC 22123-1 (2023) wie folgt:

Public Cloud: durch die Allgemeinheit nutzbare Cloud-Infrastruktur, deren Service mit anderen geteilt genutzt (Multi-Mandanten) und bei der der Zugriff auf Daten und Ressourcen logisch separiert wird.

Private Cloud: für die ausschließliche Verwendung durch eine einzige Organisation mit unterschiedlichen Nutzern bereitgestellte Cloud-Infrastruktur.

Diese Unterscheidung ist von grundsätzlicher Bedeutung für die IT-Sicherheit, weil durch eine entsprechende Entscheidung immer auch Rahmenbedingungen entschieden werden. Beispielsweise wird das Angreifermodell durch die Entscheidung „Public Cloud“ oder „Private Cloud“ beeinflusst.

Auch die Möglichkeiten bzgl. Einsatz von SaaS-Angeboten werden durch eine entsprechende Auswahl beeinflusst, da nicht alle SaaS-Anbieter eine Private Cloud unterstützen. Einzelne SaaS-Anbieter legten sich zudem auf bestimmte Cloud-Infrastruktur-Provider fest, sodass Lösungen dieser SaaS-Anbieter auch nicht auf jeder Public Cloud betrieben werden können.

Im Vorfeld sollte seitens Auftraggeber hier die Angebote auf dem Markt evaluiert und die für ihn bestmögliche Option ausgewählt werden.

Zu Ziffer 2

2.	Managed Cloud Services (MCS)*	☐ Der Auftragnehmer erbringt folgende ergänzende Leistungen (Managed Cloud Services*): ☐ Zugangsverwaltung/Administration gemäß Anlage Nr. _____ ☐ ServiceDesk/Hotline gemäß Anlage Nr. _____ ☐ Kapazitätsmanagement gemäß Anlage Nr. _____ ☐ Automatisierung von Routineaufgaben gemäß Anlage Nr. _____ ☐ Incident- und Problemmanagement gemäß Anlage Nr. _____ ☐ Release- und Patchmanagement gemäß Anlage Nr. _____ ☐ Beratungsleistungen gemäß Anlage Nr. _____ ☐ _____ gemäß Anlage Nr. _____ ☐ Erbringung der Mitwirkungsleistungen die der Auftraggeber aus dem Vertrag/den Verträgen gemäß Anlage Nr. _____ schuldet.

In Ziff. 2.3 EVB-IT Cloud AGB wird definiert, dass MCS-Leistungen sowohl für IaaS, PaaS als auch SaaS wahlweise erbracht werden können.

Bei SaaS-Leistungen sind MCS-Leistungen wie Kapazitätsmanagement sowie Release- und Patchmanagement bei einigen SaaS-Anbietern untrennbarer Bestandteil von deren SaaS-Angebot. Der Auftraggeber kann bei diesen Anbietern diese Prozesse nicht beeinflussen. Ein vorhandenes oder fehlendes Kreuz bei diesen Leistungen kann daher zu Verhandlungsbedarf mit Anbietern führen. Auch Leistungen wie Service Desks/Hotline oder Incident- und Problemmanagement sind i. d. R. Bestandteil eines SaaS-SLA und werden dort in unterschiedlichen Stufen geregelt.

Der Auftraggeber hat unter Ziff. 2 des Weiteren die Möglichkeit, die in Ziff. 17 der Cloud-AGB festgelegten Mitwirkungsleistungen durch Aktivierung und Verweis auf eine zusätzliche Anlage, an den Auftragnehmer auszulagern. Der jeweilig vereinbarte Stand des C5-Kritierienkataloges enthält „Korrespondierende Kriterien für Kunden“, welche in Ziff. 17.2 der Cloud-AGB standardmäßig den Auftraggeber zur Erbringung entsprechender Leistungen verpflichten.

Zu Ziffer 3

3.	Leistungsort	Abweichend von Ziffer 4 EVB-IT Cloud-AGB erfolgt die Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer nicht beschränkt auf die EU und den EWR sowie, sofern ein Angemessenheitsbeschluss gem. Art. 45 DSGVO besteht, die Schweiz, sondern ☐ zusätzlich in Staaten mit Angemessenheitsbeschluss gem. Art. 45 DSGVO. ☐ ohne örtliche Beschränkung (sofern keine personenbezogenen Daten verarbeitet werden). ☐ ohne örtliche Beschränkung, sofern die Anforderungen aus Anlage Nr. _____ für die Verarbeitung personenbezogener Daten erfüllt sind. ☐ nur innerhalb der Bundesrepublik Deutschland ☐ nur in den folgenden vereinbarten Rechenzentren: _____ ☐ ausschließlich für Support- und Wartungszwecke ☐ auch in _____ ☐ auch außerhalb von EU und EWR, jedoch nicht in Staaten der Staatenliste im Sinne von § 13 Absatz 1 Nummer 17 SÜG und § 32 SÜG; wobei für personenbezogene Supportdaten die Regelungen zur Verarbeitung personenbezogener Daten vorrangig gelten. ☐ Abweichend von Ziffer 4 EVB-IT Cloud-AGB dürfen Metadaten im Sinne des Anforderungskataloges C 5 (in Version 2020: OPS 11) nur in der EU und im EWR verarbeitet werden. ☐ Gemäß Anlage zur Einbeziehung auftragnehmerseitiger AGB, dort Anhang II. zur Kategorie Leistungsort. ☐ _____

In Ziff. 4 EVB-IT Cloud AGB wird der Leistungsort auf die EU bzw. den EWR und die Schweiz eingeschränkt, d. h. die vertragliche vereinbarte Leistung darf nur aus diesen Ländern erbracht werden. Dabei ist zu beachten, dass eine Verarbeitung in Art. 4 Ziff. 2 DS-GVO sehr weitreichend definiert ist. Greift im Rahmen der Fernwartung ein Beschäftigter eines Auftragnehmers aus einem Land auf Daten eines Auftraggebers zu, so werden Daten im Land des zugreifenden Beschäftigten verarbeitet.

Somit ist auch eine Fernwartung nur aus der EU/EWR und der Schweiz zulässig. Gerade, wenn ein 24-Stunden-Support erforderlich ist, wird häufig ein Support „Follow-the-Sun“ angeboten, um so Nachtzuschläge zu vermeiden und den Support auch zu diesen Zeiten zu möglichst geringen Preisen anbieten zu können.

Weiterhin ist bei Cloud-Anbietern aus Drittländern wie den USA oder China der 3rd-Level-Support häufig nur aus dem jeweiligen Heimatland möglich, da hier die Software-Entwickler ansässig sind, die ggf. zur Beseitigung aufgetretener Störungen entsprechende Fehler-Dumps untersuchen müssen. Eine Einschränkung des Leistungsortes kann daher zu Verhandlungsbedarf der Bieter oder zu einer Einschränkung des Bieterkreises führen.

Kann und darf der Auftraggeber die Verarbeitung auch aus anderen Ländern zulassen, so kann es für den Auftraggeber von Vorteil sein, auch die Verarbeitung aus anderen Ländern zuzulassen. Dabei ist zu beachten, dass bei einer Verarbeitung in (oder aus einem) Drittland grundsätzlich eine Übermittlung stattfindet; Kap. V DS-GVO sieht nichts anderes vor. Diverse Landeskrankenhausgesetze enthalten Vorgaben für Übermittlungen von Patientendaten, sodass diese Regelungen bei der Prüfung der Zulässigkeit einzubeziehen sind.

Der Kriterienkatalog bietet hier verschiedene Möglichkeiten:

1) „zusätzlich in Staaten mit Angemessenheitsbeschluss gem. Art. 45 DSGVO“
    - Art. 45 DS-GVO eröffnet der Europäischen Kommission für ein Drittland, ein Gebiet in diesem Drittland oder ein oder mehrere spezifische Sektoren in diesem Drittland festzustellen, dass ein „angemessenes Schutzniveau“ vorliegt; es wird ein sog. „Angemessenheitsbeschluss“ gefasst.
    - Mit dieser Option wird die Möglichkeit zur Erbringung der Leistungen auf die in der Liste der Europäischen Kommission enthaltenen Länder erweitert. Die Liste ist veröffentlicht unter: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de
    - Wichtig: Da sich die Liste ändert, z. B., weil ein Drittland hinzukommt oder einem Drittland die Feststellung des Vorliegens eines angemessenen Schutzniveau entzogen wird, wie es bereits zweimal im Fall der USA durch den Europäischen Gerichtshof erfolgte, muss der Auftraggeber hier regelmäßig kontrollieren, ob Änderungen erfolgt sind und die Verarbeitung seiner Daten aus dem jeweiligen Drittland noch statthaft ist.
2) „ohne örtliche Beschränkung (sofern keine personenbezogenen Daten verarbeitet werden)“
    - Hier ist zu beachten, dass die Definition von „personenbezogenen Daten“ in Art. 4 Ziff. 1 DS-GVO sehr weitreichend ist. Die Daten müssen eine Person nicht namentlich identifizieren, sondern es muss sich lediglich feststellen lassen, dass es sich um eine Person handelt.
    - So gelten IP-Adressen, die sich in den meisten Protokollen befinden, i. d. R. bereits als personenbezogenes Datum.
    - Gerade im Gesundheitswesen wird es sich regelhaft um personenbezogene Daten handeln, weswegen eine sehr gründliche Prüfung ratsam ist, bevor diese Option genutzt wird.
3) „ohne örtliche Beschränkung, sofern die Anforderungen aus Anlage Nr. […] für die Verarbeitung personenbezogener Daten erfüllt sind“
    - Hier ist zu beachten, dass für die Verarbeitung personenbezogener Daten in einem Drittland immer die Vorgaben von Kap. V DS-GVO einzuhalten sind.
    - Weiterhin sind die in den Urteilen „Schrems I“ und „Schrems II“ getroffenen Auslegungen der DS-GVO durch den EuGH zu beachten und umzusetzen.
    - Entsprechende Vereinbarungen, die den oben angesprochenen Vorgaben genügen, finden sich bei Drittländern mit Angemessenheitsbeschluss der EU-Kommission in der Regel in den jeweiligen Verträgen zur Auftragsverarbeitung, bei Drittländern ohne Angemessenheitsbeschluss der EU-Kommission in den entsprechenden Standardvertragsklauseln der EU-Kommission und den darin beschriebenen zusätzlichen Maßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus.
4) „nur innerhalb der Bundesrepublik Deutschland“
    - Gesetzliche Regelungen können erfordern, dass die Erbringung der vertraglich vereinbarten Leistungen ausschließlich aus Deutschland heraus erfolgt.
    - Beispielsweise verlangt § 27b Abs. 2 ThürKHG, dass von der für den Verantwortlichen zuständigen Datenschutzkontrollbehörde veranlasste Kontrollen vom Auftragsverarbeiter jederzeit zu ermöglichen sind. Eine Verarbeitung im Ausland kann u. U. verhindern, dass eine „jederzeitige“ Kontrolle möglich ist.
5) „nur in den folgenden vereinbarten Rechenzentren“
    - Mit dieser Option werden die Rechenzentren benannt, in welcher die Leistungserbringung erfolgt.
    - Die Rechenzentren können dabei auch in unterschiedlichen Ländern stehen; es muss nur eine genaue Benennung des Rechenzentrums und des Ortes erfolgen.
    - Bzgl. der Verarbeitung personenbezogener Daten in einem Drittland sollten auch die in den anderen Punkten dieses Abschnitts dargestellten Hinweise hierzu beachtet

werden.

6) „ausschließlich für Support- und Wartungszwecke auch in […], wobei für personenbezogene Supportdaten die Regelungen zur Verarbeitung personenbezogener Daten vorrangig gelten“
    - Hier ist zu beachten, dass die Regelungen im Vertrag zur Auftragsverarbeitung vorrangig anzuwenden sind, d. h. hier dürfen keine Orte angegeben werden, welche den Vorgaben im Vertrag zur Auftragsverarbeitung nicht entsprechen.
    - Da auch bei Support- und Wartungszwecken gerade im Gesundheitswesen auch personenbezogen Daten verarbeitet werden, sollten bei einer Verarbeitung in oder aus einem Drittland auch die in den anderen Punkten dieses Abschnitts dargestellten Hinweise hierzu beachtet werden.
    - Weiterhin muss beachtet werden, dass für die Verarbeitung personenbezogener Daten in einem Drittland immer die Vorgaben von Kap. V DS-GVO einzuhalten sind, in diesen Fällen also auch diesen Anforderungen genügt werden muss.
    - Aufgrund der Verteilung von Entwicklungszentren internationaler Anbieter von Cloud-Lösungen kann es sinnvoll sein, hier Länder außerhalb der EU und EWR zu akzeptieren, auch wenn für diese Länder kein Angemessenheitsbeschluss existiert, sofern dies aufgrund der für den Auftraggeber geltenden Rechtslage statthaft ist. Denn je nach Cloud-Anbieter kann es im Einzelfall erforderlich sein, dass ein Zugriff aus einem dieser Länder erforderlich ist, z. B. im Supportfall. Dies kann dann der Vermeidung von Folgekosten wie z. B. dem Einfliegen von Entwicklern dienen. Entsprechende Zugriffe müssen dann selbstverständlich technisch und organisatorisch entsprechend den aus den Urteilen des EuGH resultierenden Vorgaben eingeschränkt und abgesichert werden. Wenn bei Support- und Wartungszwecke kein Kreuz gesetzt wurde, kann es daher zu Verhandlungsbedarf bei internationalen Bietern kommen.

7) „ausschließlich für Support- und Wartungszwecke auch außerhalb von EU und EWR, jedoch nicht in Staaten der Staatenliste im Sinne von § 13 Abs. 1 Nr. 17 SÜG und § 32 SÜG, wobei für personenbezogene Supportdaten die Regelungen zur Verarbeitung personenbezogener Daten vorrangig gelten“
    - Siehe Punkt 6
    - SÜG = Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen; dieser Punkt wird daher in den meisten Fällen nur behördliche Einrichtungen betreffen
    - Die Regelung betrifft einerseits die Verarbeitung von
        - Wohnsitzen, Aufenthalten, Reisen, nahen Angehörigen und sonstigen Beziehungen in und zu Staaten von mit sicherheitsempfindlicher Tätigkeit befassten Personen (§ 13 Abs. 1 Nr. 17 SÜG)
        - Angaben zur Reisebeschränkung (§ 32 SÜG)

      Beide Punkte werden im Bereich der Gesundheitsversorgung eher selten eine Rolle spielen, kann aber in Einzelfällen auftreten.

8) „Abweichend von Ziff. 4 EVB-IT Cloud-AGB dürfen Metadaten im Sinne des Anforderungskataloges C5 (in Version 2020: OPS 11) nur in der EU und im EWR verarbeitet werden“
    - Metadaten, im BSI C5 OPS 11 auch „Nutzungsdaten genannt, stellen Protokolldaten dar, die zu Zwecken der Abrechnung, zum Beheben von Störungen und Fehlern sowie zum Bearbeiten von Sicherheitsvorfällen genutzt werden.
    - Zur Verbesserung des Cloud-Dienstes dürfen ausschließlich anonymisierte Metadaten genutzt werden, auch wenn dies keinen Zweck der Metadaten darstellt; BSI C5 OPS 11 sieht hier also eine Zweckänderung vor, stellt selbst aber natürlich keinen Erlaubnistatbestand zur Anonymisierung dar.
    - Diese Option kann sinnvoll sein, wenn nicht sicher ausgeschlossen werden kann, dass in den Metadaten auch personenbezogene Daten enthalten sind.

9) „Gemäß Anlage zur Einbeziehung auftragnehmerseitiger AGB, dort Anhang II. zur Kategorie

Leistungsort“

- Gerade Hyperscaler sehen in ihren auftragnehmerseitigen AGB häufig Orte zur Leistungserbringung vor. Anhang II zur Einbeziehung auftragnehmerseitiger AGB sieht unter Ziff. 3 die punktuelle vorrangige Einbeziehung entsprechender Angaben zum Leistungsort vor.
- Zu beachten ist hier, dass der Auftraggeber prüfen muss, ob diese in den auftragnehmerseitigen AGB enthaltenen Orte den rechtlichen Vorgaben, denen der Auftraggeber genügen muss, genügen.

Zu Ziffer 4

Das BSI veröffentlichte in seinen Cybersicherheitsempfehlungen „Kriterien für die Standortwahl von Rechenzentren“. In Kapitel 4 wird die Georedundanz darin als Redundanzgruppen definiert, „deren beteiligte Rechenzentren (RZ) räumlich so weit voneinander entfernt liegen, dass auch großflächige und überregionale Ereignisse mit hoher Wahrscheinlichkeit nicht mehrere der beteiligten RZ beeinträchtigen.“ [22] Das Kriterium für Georedundanz gebende Rechenzentren wird gemäß BSI mit einem Mindestabstand von ca. 200 km zwischen den Rechenzentren angegeben.

Zu Ziffer 5

5.	Übergabepunkt	Abweichend von Ziffer 5.1. der AGB ergibt sich der Übergabepunkt aus ☐ Anlage zur Einbeziehung auftragnehmerseitiger AGB, dort Anhang II. zur Kategorie Übergabepunkt. ☐ _____

EVB-IT Cloud AGB 5.1 regelt zwei Aspekte: „Der Zugriff auf die Leistung erfolgt über das öffentliche Internet mit einem marktüblichen Web-Browser ohne unangemessene oder marktunübliche Browser-Einstellungen und ohne spezielle Zugriffssoftware. Der Übergabepunkt ist das Gateway des Auftragnehmers in das Internet.“ Im Kriterienkatalog korrespondiert dies mit den Kriterien 5 Übergabepunkt. Dies führt in der Praxis häufig zu Verwirrung, in welchem Kriterium bspw. die Endnutzerplattformen (Browser, mobile Betriebssysteme) zu definieren sind oder wo bspw. ein anderer Übergabepunkt / Zugang zu definieren ist. [23]

Entsprechend Ziff. 5.1 der EVB-IT AGB ist der „Übergabepunkt“ das Gateway des Auftragnehmers in das Internet. D. h. der Zugriff auf die Leistung erfolgt über das Gateway des Auftragnehmers. Gemäß Ziffer 8.1 der EVB-IT Cloud AGB muss die Anbindung des Rechenzentrums des Auftragnehmers an den Übergabepunkt gewährleistet werden, nicht jedoch ein ortsunabhängiger Zugriff über beliebige Zugangswege. Dies kann aber trotzdem einen weltweiten Zugriff ermöglichen, setzt aber ggfs. voraus, dass z. B. über ein VPN dieser weltweite Zugriff trotzdem über den Übergabepunkt des Rechenzentrums des Auftraggebers erfolgt.

Der Kriterienkatalog sieht zwei Möglichkeiten zur Abweichung der Regelung vor:

1) Im Anhang II zur Einbeziehung auftragnehmerseitiger AGB können unter Ziff. 5 AGB des Auftragnehmers hinsichtlich des Übergabepunktes als vorrangig anwendbar ausgewählt werden, sodass der in den AGB des Auftragnehmers angegebene Übergabepunkt maßgeblich ist. Hier muss der Auftraggeber prüfen, ob dies für ihn rechtlich zulässig und auch praktikabel ist.
2) Weiterhin kann Freitext eingetragen und der Übergabepunkt so beliebig festgelegt werden.

[22] Bundesamt für Sicherheit in der Informationstechnik: Kriterien für die Standortwahl von Rechenzentren, Standort-Kriterien RZ, Oktober 2019, Version 2.0, S. 7.

[23] Ibid, S. 15.

Zu Ziffer 6

6.	Bereitstellungszeitpunkt	☐ ab Vertragsbeginn ☐ ab dem _____ ☐ innerhalb von _____ (z.B. 3 Tagen) nach Anforderung durch den Auftraggeber

Die EVB-IT Cloud AGB Ziff. 2.1.1 für SaaS/PaaS und Ziff. 2.2.1 für IaaS regeln die zum definierten Zeitpunkt zu erfolgende Bereitstellung der Anwendung und Zugänge (SaaS/PaaS) sowie der vereinbarten Cloudinfrastruktur in der vereinbarten Verfügbarkeit, Qualität und Sicherheit.

Auftraggeber müssen beachten, dass in der Regel der Zeitpunkt der Bereitstellung vor dem geplanten dem Zeitpunkt des Beginns der Nutzung liegen muss, da Cloud-Lösungen häufig nach Bereitstellung (des Auftraggebermandanten) erst noch eingerichtet und konfiguriert werden müssen.

Zu Ziffer 7

7.	Nutzer	☐ max. Anzahl gleichzeitiger Nutzer (concurrent user)*: _____ ☐ max. Anzahl benannter Nutzer (named user*): _____ ☐ Diese sind jederzeit austauschbar ☐ Dies sind nur aus wichtigen Grund jederzeit austauschbar, ohne wichtigen Grund alle _____ Tage. ☐ Gemäß Anlage zur Einbeziehung auftragnehmerseitiger AGB, dort Anhang II. zur Kategorie Nutzer. ☐ gemäß Anlage Nr. _____

SaaS-Lösungen werden häufig nach Anzahl von Nutzern - entweder gleichzeitige (aktive) Nutzer oder benannte (registrierte) Nutzer - lizenziert. Bei Verwendung von Lizenzierungsmodellen mit benannten Nutzern ist ein benannter Nutzer i. d. R. nicht jederzeit austauschbar, sondern wird z. B. monatsweise lizenziert. Ein Austausch ist dann erst nach der Mindestlizenzperiode möglich. Bei Verwendung des Lizenzierungsmodelles mit gleichzeitigen Nutzern spielt hingegen die Gesamtanzahl der benannten / registrierten, aber nicht aktiven Nutzer keine Rolle.

Zu Ziffer 8

8.	Nutzerkreis	☐ Keine Beschränkung ☐ _____ (z.B. Alle Mitarbeiter in der Finanzverwaltung) ☐ _____

Eine Eingrenzung des Nutzerkreises kann neben einer mittelbaren Begrenzung der Lizenzkosten (siehe Ziffer 7) auch sinnvoll sein, um im Betrieb die sich aus der EVB-IT Cloud AGB ergebenden Pflichten des Auftraggebers (u. a. eindeutige Benutzerkennungen für Zurechenbarkeit, Unterrichtung über Nutzungsvereinbarung, Verpflichtung der Nutzer zur Meldung von Sicherheitsvorfällen) abgrenzbar und beherrschbar zu machen.

Zu Ziffer 9

9.	Nutzungsort	☐ Abweichend von Ziffer 14.1 EVB-IT Cloud-AGB ist das Recht zur Nutzung der Leistung örtlich auf das Gebiet der Vertragsstaaten der EU und des EWR sowie der Schweiz beschränkt

Entsprechend Ziff. 14. EVB-IT Cloud AGB besteht das Nutzungsrecht weltweit bis auf diejenigen Länder, in denen der Auftragnehmer aufgrund staatlicher Rechtsakte wie beispielsweise

Exportbeschränkungen oder staatlicher Sanktionsvorgaben die jeweilige Leistung nicht allgemein anbietet und der Zugang zu den Leistungen bestimmungsgemäß nicht möglich ist.

Der Auftragnehmer muss dem Auftraggeber die Länder, in denen ein Zugriff nicht möglich ist, erst auf Aufforderung nennen.

Ziff. 9 im Kriterienkatalog bietet die Möglichkeit, den Nutzungsort auf die EU/EWR und die Schweiz zu beschränken. Dies ist sinnvoll, wenn Einschränkungen hinsichtlich der Verarbeitung personenbezogener Daten hinsichtlich des Verarbeitungsortes bestehen. Dies ist z. B. bei Sozialdaten der Fall, aber auch Landeskrankenhausgesetze enthalten Vorgaben, welche ggf. einen weltweiten Zugriff einschränken können. So enthalten diverse Krankenhausgesetze die Vorgabe, dass Patientendaten grundsätzlich im Krankenhaus verarbeitet werden müssen, wodurch Abweichungen begründet werden müssen. Ob ein Chefarzt, der einen Kongress besucht, zwingend vom Ort des Kongresses auf Patientendaten zugreifen muss oder die Entscheidung auch ein im Krankenhaus befindlicher Oberarzt treffen kann, ist sicherlich nicht pauschal zu beantworten und verlangt eine Einzelfallbetrachtung, ggf. sogar unter Einbeziehung der zuständigen Datenschutzaufsichtsbehörde.

Anders kann es bei SaaS-Lösungen aussehen, die bspw. im Rahmen von Telemonitoring und auf Basis einer informierten Einwilligung des Patienten vom Auftraggeber dem Patienten zur Verfügung gestellt werden und die nicht von einem Krankenhaus angeboten werden, welches das jeweilige Landesrecht beachten muss. Wird eine weltweite Erreichbarkeit oder ein weltweites Monitoring gewünscht, ist eine entsprechende Beschränkung auf die EU/EWR nicht umsetzbar. Auch hier muss die Rechtslage entsprechend beurteilt und gesehen werden, wie ein ggf. weltweit gewünschter Zugriff realisiert werden kann.

Zu Ziffer 10

10.	Identitäts- und Berechtigungsmanagement (IDM)	☐ C5 Zusatzkriterium IDM-02: Der Auftragnehmer bietet dem Auftraggeber einen Self-Service an, mit welchem diese Zugangs- und Zugriffsberechtigungen eigenständig vergeben und ändern können. ☐ Der Auftragnehmer sorgt durch technische Maßnahmen dafür, dass die Nutzer keine Leistungen beauftragen können, welche nicht vom Leistungsumfang des Vertrages umfasst sind.

Cloud-Dienstleistungen können Funktionen für einen Self-Service für Nutzer beinhalten. Das kann auch eine Steuerung (u. a. Erweiterung) des Leistungs- und Nutzungsumfangs durch speziell autorisierte Nutzer bedeuten. Eine Einschränkung der Ausweitung des Leistungsumfangs kann daher nicht immer absolut sichergestellt werden, sondern wird durch die Berechtigungsvergabe nur eingegrenzt. Kommt es trotz der vertraglichen Vereinbarung zu einer ungewollten Änderung des Leistungsumfangs, kann es sein, dass der Auftragnehmer gegenüber dem Auftraggeber haftet.

Zu Ziffer 12

12.	Endgeräte/Zugang	☐ webbasiert ☐ webbasiert optimiert für mobile Endgeräte ☐ nicht unterstützte Browser: _____ Anforderungen an webbasierten Zugang: ☐ keine Plug-Ins, Add-Ons ☐ zugelassene Plug-Ins, Add-Ons ☐ sonstige Sicherheitseinstellungen (ggf. Anlage) ☐ Terminalserver/ graphischer Remote Zugriff (zum Beispiel RDS oder RDP): _____ ☐ VPN ☐ VPN-Anforderungen: _____ ☐ API ☐ API-Anforderungen: _____ **Über native Zugriffssoftware** _____ (Name) **für** ☐ PC/Notebooks, ☐ Windows ab Version _____ ☐ andere: _____ ☐ mobile Geräte (Apps) ☐ iOS ab Version _____ ☐ Android ab Version _____ ☐ andere mobile OS (Bezeichnung) _____ ☐ besondere Systemvoraussetzungen beim Auftraggeber _____ ☐ technische Anforderungen für den Zugang gemäß Anlage _____ ☐ Der Auftragnehmer wird den Auftraggeber auf dessen Anforderung bei deren Installation durch telefonische Anleitung und, soweit durch den Auftraggeber der Zugang ermöglicht wird, durch Remoteservice unterstützen. Dies gilt auch für neue Programmstände der Zugriffssoftware. ☐ Gemäß Anlage zur Einbeziehung auftragnehmerseitiger AGB, dort Anhang II. zur Kategorie Endgeräte/Zugang. ☐ _____

Cloud-basierte Systeme sind häufig webbasiert. In hybriden Einsatzszenarien mit Cloud- und On-Premises-Anwendungen gibt es noch weitverbreitete Integrationswege zu bestehender Drittsoftware, welche bei webbasierter Cloud-Software systembedingt zusätzliche Plug-Ins benötigen. Dazu können Integrationen über das Dateisystem (bspw. GDT) oder Aufrufe von nicht-webbasierter Drittsoftware auf dem Nutzer-PC zählen. Daher kann ein Ausschluss von Plugins oder Add-Ons zu Verhandlungsbedarf von Cloud-Anbietern führen bzw. bestimmte Integrationsszenarien verhindern.

Zu Ziffer 13

13.	Speicher- Größe	☐ Keine Speicherung beim Auftragnehmer
	(für Speicherung von Auftrag-geberdaten)	☐ Speicherung beim Auftragnehmer ☐ feste Größe: _____ GB ☐ dynamisch: mind. _____ GB bis maximal: _____GB ☐ dynamische Anpassung im laufenden Betrieb (kein Neustart) ☐ keine Limitierung des Speicherumfangs

Weder im EVB-IT Cloud-Vertrag noch in den dazugehörigen AGB wird festgelegt, ob beim Auftragnehmer Daten gespeichert werden oder nicht; dies ist letztlich von der ausgeschriebenen Leistung abhängig.

Ein Cloud-Dienstleister muss immer gewisse Daten, auch personenbezogen Daten, speichern, die zur Erbringung des Dienstes erforderlich sind wie z. B. Login-Daten der Beschäftigten des Auftragnehmers. Der in Ziff. 13 genutzte Begriff der „Auftraggeberdaten“ kann daher zwangsläufig nicht auf diese für die Leistungserbring zwingend erforderlichen Daten anwendbar sein, sondern nur auf die Daten, die Bestandteil der Leistungsbeschreibung sind, wie z. B. Abrechnungsdaten der Beschäftigten, Gesundheits- oder Sozialdaten.

Einerseits kann festgelegt werden, dass keine Speicherung derartiger Daten beim Auftragnehmer erfolgt.

Andererseits kann eine Speicherung dieser Daten beim Auftragnehmer vereinbart werden. Ist dies der Fall, wird der vereinbarte Speicherplatz regelhaft auch Einfluss auf die Kosten der Dienstleistung haben. Daher ist in diesen Fällen anzugeben, mit welchen Speichergrößen der Auftragnehmer rechnen muss. Kann der Auftraggeber keine Angabe machen, wird häufig ein dynamischer Preis für diesen Teil der Leistungserbringung vereinbart, der abhängig von der Nutzung des Speicherplatzes ist.

Zu Ziffer 15

15.	Bandbreite der Anbindung des Auftragnehmers an das Internet, die für den Auftraggeber zur Verfügung steht	☐ _____ Mbit/s ☐ asynchron Uplink: _____Mbit/s Downlink: _____Mbit/s ☐ dynamisch: mind. _____ Mbit/s bis maximal: _____ Mbit/s ☐ _____

Informationen zur verfügbaren Bandbreite sind je nach Anwendung von sehr hoher Relevanz für den Bieter. Datenintensive und latenzsensible Anwendungen (z. B. bildgebende und molekulardiagnostische Verfahren) benötigen möglicherweise deutlich mehr Bandbreite als heute mehrheitlich verfügbar[24].

Neben der Planung des Datenvolumens der eigentlichen Nutzerdaten sind bei Clouds in Kombination mit Managed Cloud Services (z. B. Automatisierung von Routineaufgaben, Release- und Patchmanagement) heute auch infrastrukturbezogene Datenvolumen von hoher Relevanz. Automatisierte Updates werden heute häufig durch die Verteilung von fertigen, vorkonfigurierten Systemabbildern von zentralen Verteilungsservern umgesetzt. Durch Automatisierung und moderne DevOps-Prozesse wird faktisch auch deutlich häufiger ein Update verteilt als im klassischen IT-Betrieb. Diese Softwareverteilungsprozesse können durch Häufigkeit und Einzelgröße der Abbilder eine signifikante Bandbreite belegen.

[24] Siehe z. B. den Zwischenbericht zum Digitalradar unter https://www.digitalradar-krankenhaus.de/download/220914_Zwischenbericht_DigitalRadar_Krankenhaus.pdf

Zu Ziffer 16

16.	Datensicherung*	Ergänzend zu Ziffer 7 EVB-IT Cloud-AGB gilt Folgendes: ☐ Der Auftragnehmer ist zur Erstellung von Backups der Daten des Auftraggebers verpflichtet. ☐ Gegenstand des Backups ☐ ist das Image Backup (komplettes Image der virtuellen Maschinen) ☐ sind folgende Daten _____ (z.B. sämtliche Anwendungsdaten) ☐ sind _____ ☐ Das Backup erfolgt in folgendem Format: _____. ☐ Das Backup erfolgt _____ (z.B. stündlich, transaktionsorientiert). ☐ Das Backup erfolgt an folgendem Ort _____ (z.B. gesondertem Server oder anderem Rechenzentrum, jeweils gemäß Standortvorgabe in Ziffer 4 EVB-IT Cloud-AGB auf _____ (Server, Band). ☐ Eine Kopie des Backups erfolgt an folgendem Ort _____ (z.B. gesondertem Server oder anderem Rechenzentrum, jeweils gemäß Standortvorgabe in Ziffer 4 EVB-IT Cloud-AGB) auf _____ (Server, Band). ☐ Eine Löschung des Backups erfolgt ☐ frühestens nach _____ (z.B. 2 Wochen, 6 Monaten) ☐ gemäß Anlage Nr. _____ ☐ Weitere Regelungen zur Datenlöschung gelten gemäß Anlage Nr. _____ (während der Vertragslaufzeit) oder nach Vertragsende wenn vereinbart. ☐ Eine Löschung des Backups erfolgt gemäß Anlage Nr. _____ ☐ Regelungen zum Backup gemäß Anlage Nr. _____. (z.B. Backup-Konzept) ☐ Abweichend von Ziffer 7.2 EVB-IT Cloud-AGB ist der Auftragnehmer nicht verpflichtet, einzelne vom Auftraggeber zuvor gelöschten Dateien wiederherzustellen, sondern lediglich den Datenbestand insgesamt auf den vorherigen und soweit vorhanden und vom Auftraggeber gewünscht, auf die davor liegenden Stände wiederherzustellen ☐ Der wiederhergestellte Stand wird dem Auftraggeber auf dessen Wunsch gesondert zur Verfügung gestellt wird. ☐ Zusätzlich zum C5 Basiskriterium OPS-08 ist der Auftragnehmer verpflichtet, den Auftraggeber auf dessen Anforderung über die Ergebnisse der durchgeführten Wiederherstellungstests zu informieren. Wiederherstellungstests sind in das Notfallmanagement des Auftragnehmers eingebettet. ☐ Weitere Regelungen zur Datenlöschung gemäß Anlage Nr. _____ (während der Vertragslaufzeit oder nach Vertragsende). ☐ Gemäß Anlage zur Einbeziehung auftragnehmerseitiger AGB, dort Anhang II. zur Kategorie Datensicherung*. ☐ _____ ☐ Der Auftraggeber ist für folgende Datensicherungen* selbst verantwortlich, wobei der Auftragnehmer die dazu erforderlichen Funktionalitäten zur Verfügung stellt: _____

Es sind seitens des Bieters/Auftragnehmers nach dem EVB-IT Cloud **keine Datensicherungen geschuldet**. Der Auftraggeber muss daher selbst dafür Sorge tragen, dass die in der Cloud betriebenen Anwendungen sowie die entsprechenden Daten regelmäßig gesichert werden.

Soll eine Datensicherung vom Bieter/Auftragnehmer übernommen werden, muss dies und auch der Umfang der Backup-Pflichten ausdrücklich vertraglich vereinbart werden. Dies kann über Punkt 16 des Kriterienkatalogs geregelt werden oder über eine eigenständige Anlage vertraglich vereinbart werden. Es empfiehlt sich, bei Bedarf einer Datensicherung ebenfalls direkt Löschpflichten zuzuweisen oder auf entsprechende Anlagen zu verweisen.

Bei Ziffer 16 werden z. T. nur Daten inkl. Anwendungsdaten adressiert, nicht jedoch die Anwendungen selbst. Sollen ebenfalls die Anwendungen gesichert werden, muss im zweiten Ankreuzfeld von Ziff. 16 entweder das „Image Backup“ ausgewählt werden oder über die dritte Möglichkeit der Gegenstand des Backups als Freitext angegeben werden.

Zu Ziffer 17

17.	Datenexport/ Datenimport	☐ Zusätzlich zu Ziffer 7.3 EVB-IT Cloud-AGB gilt: ☐ Für folgende Teile der Leistung _____ (z.B. Datenbankdaten) erfolgt unabhängig von einem ggf. vereinbarten Backup ein Datenexport durch den Auftragnehmer. Der Datenexport erfolgt _____ (z.B. täglich, wöchentlich) in folgendem Format _____ (z.B. .csv, .vhd) an folgendem Ort _____ (z.B. gesonderter Server oder anderes Rechenzentrum) auf _____ (Server, Band). ☐ Für folgende Teile der Leistung _____ (z.B. Datenbankdaten) erfolgt ein Datenimport durch den Auftragnehmer. Der Datenimport erfolgt _____ (z.B. täglich, wöchentlich) in folgendem Format _____ (z.B. .csv, .vhd) von folgendem Ort _____ (z.B. gesonderter Server oder anderes Rechenzentrum gemäß Standortvorgabe in Ziffer 4 EVB-IT Cloud-AGB) von (Server, Band). ☐ Für den Datenexport bzw. Datenimport verwendet der Auftragnehmer folgenden Standard _____. ☐ Dem Auftraggeber stehen für den eigenen Datenimport und Datenexport folgende Möglichkeiten zur Verfügung: _____ (z.B. Nennung der Schnittstelle und deren Spezifikation).

Mitunter wird gewünscht, dass Daten zu Statistikzwecken ausgewertet werden können, z. B. für die betriebswirtschaftliche Bewertung wie Top-Zuweiser-Statistiken oder für Zwecke der Qualitätskontrolle. Ziff. 7.3 der EVB-IT Cloud AGB sieht vor, dass der Auftraggeber benötigte Daten selbstständig exportieren kann.

Evtl. will der Auftraggeber aber auch regelmäßig Daten durch den Auftragnehmer bereitgestellt bekommen. Hier besteht die Möglichkeit, entsprechende Dienstleistungen des Auftragnehmers vorzusehen.

Zu Ziffer 18

18.	IT Sicherheit	☐ Abweichend von Ziffer 1.2 EVB-IT Cloud-AGB ist nicht nur die Einhaltung der C5 Basiskriterien, sondern auch der C5 Zusatzkriterien geschuldet ☐ Abweichend von Ziffer 1.2 EVB-IT Cloud-AGB ist nicht nur die Einhaltung der C5 Basiskriterien, sondern auch der folgenden C5 Zusatzkriterien geschuldet ☐ CRY-03: Die für die Verschlüsselung verwendeten privaten Schlüssel sind ausschließlich und ohne Ausnahme dem Kunden nach geltenden rechtlichen und regulatorischen Verpflichtungen und Anforderungen bekannt. ☐ AM-05: Physische Assets der internen und externen Mitarbeiter unterliegen einer zentralen Verwaltung. Die zentrale Verwaltung ermöglicht eine Software-, Daten- und Richtlinienverteilung sowie eine Remote-Deaktivierung, -Löschung, oder -Sperrung. ☐ OPS-22: Sicherheitspatches werden ab dem Zeitpunkt ihrer Verfügbarkeit* in Abhängigkeit des nach der jüngsten Version des Common Vulnerability Scoring Systems (CVSS) eingeordneten Schweregrades der dadurch adressierten Schwachstellen eingespielt: • Kritisch (CVSS = 9.0 - 10.0): 3 Stunden • Hoch (CVSS = 7.0 - 8.9): 3 Tage • Mittel (CVSS = 4.0 - 6.9): 1 Monat • Niedrig (CVSS = 0.1 - 3.9): 3 Monate ☐ Abweichend bzw. ergänzend zu Ziffer 6.2 EVB-IT Cloud-AGB wird vereinbart, dass ☐ das vom Auftragnehmer implementierte Sicherheitskonzept und sein ISMS auf ISO 27001 und BSI IT-Grundschutz in der jeweils geltenden Fassung basiert. ☐ das Notfall-Management gemäß ☐ BSI-Standard 100-4 bzw. nach dessen Inkrafttreten BSI Standard 200-4 ☐ ISO 22301 ☐ _____ erfolgt. ☐ die Parteien für den Not- und Krisenfall besondere Vereinbarungen gemäß Anlage Nr. treffen, die auch die erforderliche Beteiligung des BSI einschließen. ☐ der Auftragnehmer die Umsetzung der Vorgaben zur IT-Sicherheit ☐ durch entsprechende Zertifikate ☐ durch folgende Zertifikate _____ ☐ durch _____ (z.B. C5 Testat nach BSI) nachweisen muss. ☐ der Auftragnehmer auf Anforderung des Auftraggebers die verwendeten Verschlüsselungs- und Authentifikationsmechanismen offenlegt. ☐ Abweichend von Ziffer 1.2 EVB-IT Cloud-AGB wird vereinbart, dass die aus Anlage Nr. _____ ersichtlichen C5 Basiskriterien nicht geschuldet werden. Soweit nicht in der Anlage konkrete Alternativen vorgesehen sind, sieht der Auftragnehmer angemessene Alternativen zur Erfüllung der entsprechenden Anforderungen vor. ☐ Dem Auftraggeber ist eine Schnittstelle zum Monitoring* der Leistungen und der Cloud-Infrastruktur zur Verfügung zu stellen. ☐ Der Schutzbedarf der vertragsgegenständlichen Daten des Auftraggebers ergibt sich aus Anlage Nr. _____. ☐ Ein CERT des Auftraggebers kann angebunden werden gemäß Anlage Nr. _____. ☐ Zusätzlich zum C5 Basiskriterium OPS-19 finden Penetrationstests nicht nur einmal jährlich, sondern halbjährlich statt. Diese müssen darüber hinaus zwingend durch unabhängige Externe durchgeführt werden. Internes Personal für Penetrationstests darf die externen Dienstleister dabei unterstützen. ☐ Ergibt das Prüfungsergebnis gemäß Ziffer 6.4.2 EVB-IT Cloud AGB keine oder nur unwesentliche Beanstandungen, trägt der Auftraggeber die beim Auftragnehmer anfallenden notwendigen Kosten des Auftragnehmers (auch interne Kosten) und etwaiger Unterauftragnehmer bis zu einem Höchstbetrag von _____Euro netto je Prüfung. ☐ Dem Auftraggeber steht das Prüfungsrecht gemäß Ziffer 6.4.2 EVB-IT Cloud AGB anlassunabhängig zu. Ergibt das Prüfungsergebnis keine Beanstandungen, trägt der Auftraggeber die beim Auftragnehmer anfallenden notwendigen Kosten bis zu einem Höchstbetrag von _____ Euro netto.

Der Kriterienkatalog sieht in Nr. 18 verschiedene Möglichkeiten zur Differenzierung im Hinblick auf die IT-Sicherheit vor, erlaubt jedoch nur eine Erhöhung der Anforderungen bzgl. der IT-Sicherheit. So kann

z. B. vereinbart werden, dass abweichend von Ziffer 1.2 der EVB-IT Cloud AGB nicht nur die Einhaltung der C5-Basiskriterien, sondern zusätzlich die Einhaltung der C5-Zusatzkriterien zu erbringen sind.

Hier ist allerdings zu beachten, dass eine pauschale Forderung aller Zusatzkriterien bzw. die explizite Forderung von OPS-22 im Medizinumfeld mit anderen Regulierungen kollidieren kann.

OPS-22 regelt die Dokumentation von Schwachstellen, das Zusatzkriterium fordert die Einspielung von Sicherheitspatches ab dem Zeitpunkt der Verfügbarkeit. Nach Verfügbarkeit von Sicherheitspatches von in Medizinprodukten verwendeten Drittkomponenten, unterlaufen die Medizinprodukte i. d. R. aufwendige Revalidierungen, bevor die Sicherheitspatches durch den Medizinprodukthersteller freigegeben werden (eventuell erst nach Erstellung eines eigenen Service-Releases). Insofern können Sicherheitspatches entlang der Software-Lieferkette eine unterschiedliche Interpretation von Verfügbarkeit haben.

Das Kriterium CRY-03 regelt die Verschlüsselung gespeicherter Daten, das Zusatzkriterium fordert die ausschließliche Kenntnis der eingesetzten Schlüssel durch den Auftraggeber (= Cloud-Kunden).

SaaS Anwendungen implementieren häufig mehrschichtige Verschlüsselungsarchitekturen: Hardware (Bus und Speicher, Secure Enclaves), OS (Dateisystem), DB (Datenbank-Files), Applikation (Zertifikate und Applikationsschlüssel). In geteilten SaaS-Anwendungen sind die allermeisten der dabei verwendeten Schlüssel geteilt mit allen Kunden und adressieren unterschiedlichste Angriffsszenarien. Durch bestimmte verfügbare Implementierungen kann dabei das verwendete Schlüsselmaterial auch mit niemandem geteilt und bekannt sein (Zero-Trust-Ansätze). Eine Forderung des Zusatzkriteriums kann daher zu Einschränkungen der Anbieterseite und zu privaten bzw. Hybrid-Cloud-Umgebungen führen.

Zu Ziffer 19

19.	Verfügbarkeit*	☐ Abweichend von Ziffer 8 EVB-IT Cloud-AGB ☐ schuldet der Auftragnehmer während der Betriebszeit* eine Verfügbarkeit* von mindestens der Verfügbarkeitsklasse* _____ im Bezugszeitraum, ☐ ist der Bezugszeitraum* der _____ ☐ verstehen sich alle Zeitangaben als Angaben statt nach mitteleuropäischer Zeit (MEZ) bzw. Sommerzeit (MESZ) nach _____ ☐ ist die Betriebszeit* die Zeit von _____bis _____ (hier Tage angeben) von _____ bis _____ Uhr; ☐ besteht in der Zeit von _____ bis _____ Uhr eine Kernbetriebszeit* den besonderen Leistungsmerkmalen gemäß Anlage Nr. _____ ☐ ist die Zeit von _____ bis _____ Uhr am _____ (hier Tag angeben) Zeit geplanter Nichtverfügbarkeit (z.B. für Wartungsarbeiten) und wird bei der Berechnung der Verfügbarkeit* nicht berücksichtigt, ☐ In Ergänzung zu Ziffer 8 der EVB-IT Cloud-AGB und der Definition zur Verfügbarkeit* gilt die Leistung auch dann als nicht verfügbar, wenn im ☐ Durchschnitt einer Stunde in der Betriebszeit ☐ Durchschnitt für die Betriebszeit eines Tages ☐ _____ folgendes gegeben ist: ☐ Das Antwortzeitverhalten der Funktion _____ (z.B. Bezeichnung einer konkreten Abfrage und der Ausgabe einer entsprechenden Antwort) ist schlechter als _____ (z.B. Sekunden, Minuten).

Krankenhäuser müssen 24 Stunden am Tag Patienten versorgen, auch an Sonn- und Feiertagen. Entsprechend Ziff. 8.3 EVB-IT Cloud AGB ist die Zeitspanne von 04:00 bis 08:00 Uhr an Sonntagen Zeit geplanter Nichtverfügbarkeit, d. h., die Cloud-Leistung kann ggf. an 52 Tagen im Jahr sonntags in

diesem Zeitraum nicht zur Verfügung stehen. Unzweifelhaft bedürfen auch Cloud-Systeme einer regelmäßigen Wartung, die vertraglich vereinbarte Zeitspanne umfasst jedoch etwa 8,7 Tage oder – anders ausgedrückt – etwa 2,7 % der Zeitdauer eines Jahres.

Weiterhin ist zu beachten, dass dieser Zeitraum gerade im Krankenhaus die Arbeit in der Patientenversorgung deutlich beeinträchtigen kann. Zwar beginnen Patientenvisiten Sonntag meistens nach 8.00 Uhr, jedoch endet der Nachtdienst im Pflegebereich i. d. R. zwischen 6.00 und 7.00 Uhr. D. h. in den Zeitraum von 04:00 bis 08:00 Uhr steht an Sonntagen evtl. die Patientendokumentation für die Übergabe vom Nacht- an den Frühdienst nicht zur Verfügung, der Nachtdienst kann ggf. seinen gesetzlich vorgeschriebenen Dokumentationspflichten nicht genügen.

Da all diese Zeiten, wo der Cloud-Dienst ggf. nicht nutzbar ist, auf die „Verfügbarkeit“ nicht angerechnet werden, sollte seitens des Auftraggebers geprüft werden, ob unter Ziff. 19 Anpassungen bzgl. der vereinbarten Zeiten für Wartung erforderlich sind.

Zu Ziffer 22

22.	**Protokollierung**	Der Auftragnehmer führt folgende Protokolle: ☐ Protokolle über die Zugriffe auf die vom Auftraggeber genutzten Leistungen einschließlich der entsprechenden Daten und Datensicherungen*. Protokolliert werden muss dabei mindestens, durch wen, wann, wie und wie lange ein Zugriff erfolgte. ☐ Protokolle über sämtliche Zugriffe auf Infrastrukturkomponenten. Protokolliert werden müssen dabei insbesondere: An- und Abmeldungen, Installation, Deinstallation und Modifikation von Anwendungen, Änderungen von Berechtigungen und Änderungen im Benutzermanagement. Die Erfassung und Protokollierung weiterer Daten (auch Metadaten) erfolgt in dem im Vertrag vereinbarten Umfang. ☐ Protokolle über den Sicherheitsstatus des Cloud-Managementsystems (Vollständigkeit, Verfügbarkeit*, Integrität und Vertraulichkeit der verarbeiteten Daten). ☐ Protokolle über Art und Zeitpunkte der durchgeführten Datensicherungsmaßnahmen und Rücksicherungen. Der Auftraggeber hat das jederzeitige Recht, diese Protokolle einzusehen und in elektronisch bearbeitbarer Form abrufen zu können. ☐ Die Protokolle sind mindestens: ☐ sechs Monate aufzubewahren. ☐ _____ Monate aufzubewahren. ☐ Die Protokolle sind revisionssicher aufzubewahren. ☐ Gemäß Anlage zur Einbeziehung auftragnehmerseitiger AGB, dort Anhang II. zur Kategorie Protokollierung.

Hier legt der Auftraggeber fest, welche Protokolle seitens des Auftragnehmers geführt werden sollen. Dabei ist zu berücksichtigen, dass der datenschutzrechtlich Verantwortliche für die Protokollierung wie auch der Protokolle der Auftraggeber ist, sofern die Protokolle personenbezogene Daten wie z. B: IP-Adressen beinhalten.

D. h.: Sind personenbezogene Daten in den Protokollen, darf der Auftraggeber nur die Protokollierung von erforderlichen Daten veranlassen und muss diese Erforderlichkeit nachweisen können. Der Auftragnehmer darf ohne die explizite Beauftragung des Auftraggebers somit keine eigenständigen Protokolle erfassen, welche personenbezogenen Daten des Auftraggebers enthalten.

Auch dürfen die Protokolle nur für den Zeitraum aufbewahrt werden, der zur Erreichung des Zweckes erforderlich ist bzw. den ein Gesetz vorschreibt. Ggf. kann man sich auch an Gesetzen orientieren, die

Behörden für ähnliche Aufgaben Zeiten vorgeben. § 5 Abs. 2 BSIG[25] schreibt beispielsweise die Höchstdauer von 18 Monaten für Protokolldaten vor, die zu Zwecken der Erkennung, Eingrenzung oder Beseitigung von Störungen, Fehlern oder Angriffen der Kommunikationstechnik eingesetzt werden.

[25] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), § 5. Online, abrufbar unter https://www.gesetze-im-internet.de/bsig_2009/__5.html

Anlage zur Einbeziehung von auftragnehmerseitigen AGB

Einleitung

Der EVB-IT Cloud Vertrag bietet, für die EVB-IT Vertragsmuster ansonsten unüblich, verschiedene Möglichkeiten, auch vertragliche Regelungen der auftragnehmerseitigen AGB miteinzubeziehen. Dies erfolgt über die Anlage zur teilweisen Einbeziehung der AGB des Anbieters. Cloud-Lösungen werden von Auftragnehmern/Bietern regelmäßig eher nur nach hochstandardisierten Geschäftsmodellen angeboten werden, die Möglichkeit zur Einbeziehung auftragnehmerseitigen AGB soll die Beschaffung erleichtern.[26]

Eine vollständige, ausschließlich nachrangig anzuwendende Einbeziehung von Auftragnehmer-AGB ist im Vertrag selbst unter Ziffer 1.2.4 durch Nutzung des ersten Ankreuzfeldes möglich.

Die Anlage zur Einbeziehung von auftragnehmerseitigen AGB sieht hingegen zwei Möglichkeiten zur partiellen Einbeziehung der AGB der Anbieter vor. Hierbei wird dem Grundsatz einer kontrollierten Einbindung gefolgt. Daher können in der Anlage nicht grundsätzlich alle auftragnehmerseitigen AGB pauschal eingebunden werden, sondern es muss konkret angegeben werden, welche Klauseln der auftragnehmerseitigen AGB eines Anbieters einbezogen werden sollen.

Folgende zwei Möglichkeiten der Einbeziehung auftraggeberseitiger AGB gibt es:

a) Abschnitt „I. Anhang zum EVB-IT Cloudvertrag“ wird teilweise eine nachrangige Einbeziehung der AGB des Anbieters ermöglicht. Hier muss der Anbieter eintragen, welche seiner Regelungen **nachrangig** gegenüber den Regelungen des EVB-IT Cloud gelten sollen.
b) Der Abschnitt „II. Anhang zum Kriterienkatalog“ bietet die Möglichkeit, einzelne auftraggeberseitige AGB auch **vorrangig** einzubeziehen. Hierbei erfolgt eine Vorauswahl des Auftraggebers, für welche Bereiche einem Bieter ermöglicht wird, seine AGB zu genau diesem Vertragsbestandteil anzugeben, damit diese aufraggeberseitigen Regelungen im Falle einer Auftragsvergabe vorrangig angewendet werden.

Der Auftraggeber muss im Vergabeverfahren prüfen, ob die AGB-Bedingungen, unter welchen Bieter ihre Dienstleistung anbieten, für ihn akzeptabel sind. Dies beinhaltet insbesondere die Prüfung, ob der Auftraggeber seinen gesetzlichen Verpflichtungen wie beispielsweise

- Beschränkung von Daten-Zugriffen durch den Dienstleister auf das absolut erforderliche Maß oder
- für den Auftraggeber geltende Meldepflichten gegenüber Behörden wie das BSI

unter Einbeziehung der auftraggeberseitigen AGB nachkommen kann.

[26] CIO Bund: EVB-IT Cloud: Hinweise zur Nutzung – Kurzfassung, Kap. 3 „Elemente und Aufbau der EVB-IT Cloud“ Tabelle Zeile 4. Online, zitiert am 2023-08-18; verfügbar unter https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-beschaffung/evb-it-bvb/basisvertraege/cloud/hinweise-fuer-die-nutzung-der-evb-it-cloud.pdf;jsessionid=3B0CCEDC80454620C85C3BEF42D6A4C9.1_cid332?__blob=publicationFile&v=1

Abschnitt „I Anhang zum EVB-IT Cloudvertrag“

Der Einbezug dieses Anhangs ist optional.

Auftragnehmerseitige AGB können entweder Allgemeine Geschäftsbedingungen (AGB) des Auftragnehmers selbst sein, als auch AGB eines Unterauftragnehmers des Auftragnehmers oder Lieferanten.

Insbesondere AGB des Cloudanbieters, in dem die Lösung gehostet wird, bspw. eines Hyperscalers, häufig bei internationalen Anbietern auf Englisch als „Terms and Conditions“ oder „Service Terms“ bezeichnet, könnten unter den Bereich der „Auftragnehmerseitigen AGB“ erfasst werden.

Es empfiehlt sich zudem ein Abgleich der Vereinbarungen aus den in der Regel nicht verhandelbaren AGB eines Cloudanbieters mit den Vorgaben des EVB-IT Cloudvertrages.

Zur **nachrangigen Einbeziehung** auftragsnehmerseitiger AGB bestehen grundsätzlich zwei Möglichkeiten:

- Möglichkeit 1: Aufnahme der AGB in der Tabelle zu Nr. 1.2.4 Cloudvertrag
- Möglichkeit 2: Aufnahme in der Tabelle in der Anlage zum Kriterienkatalog zur Einbeziehung von auftragnehmerseitigen AGB zum Vertrag in Ziff. I und dort beigefügt als Anhang.

Sofern die auftragnehmerseitigen AGB nicht gemäß einer der Möglichkeiten aufgeführt sind, werden sie nicht einbezogen und sind automatisch ausgeschlossen.

Die auftragnehmerseitigen AGB dürfen auf Basis der Nummer 1.2.4 des Vertrages durch einen dynamischen Änderungsvorbehalt durch den Auftragnehmer bzw. einen Unterauftragnehmer aktualisiert werden, solange die Änderungen nicht zum Nachteil des Auftraggebers ausfallen.

Abschnitt „II Anhang zum Kriterienkatalog“

Der Einbezug dieses Anhangs ist optional.

Im Gegenzug zu Anhang I zum Kriterienkatalog, bietet Anhang II die Möglichkeit, einzelne Regelungen basierend auf den auftragnehmerseitigen AGB, oder AGB seiner Unterauftragnehmer, vorrangig einzubeziehen.

Wie bereits im Hinweisfeld zum Anhang II (Zeile 4) zum Kriterienkatalog beschrieben, müssen abweichende Regelungen zu den EVB-IT Cloud AGB in dieser Tabelle aktiviert, also aktiv angekreuzt werden. Die Entscheidung, welche Abweichungen möglich sein sollen, **trägt allein der Auftraggeber**.

Hierzu aktiviert er die jeweiligen Kategorien in Spalte 2. Die hier referenzierten Regelungen aus den auftragnehmerseitigen AGB in den jeweils ausgewählten Kategorien, gelten nach Vereinbarung **vorrangig zu den EVB-IT Cloud AGB**. Dieser Anhang ist also dafür gedacht, **gezielt von den EVB-IT Cloud AGB-Regelungen abzuweichen**.

Im Umkehrschluss ergibt sich somit auch die Intention der CIO Bund, vorrangige Regelungen durch die Einbeziehung auftragnehmerseitige AGB nur in ausgewählten Kategorien zu ermöglichen. Eine pauschale Einbeziehung der auftragnehmerseitigen AGB ist ausgeschlossen, um die Vergleichbarkeit der Angebote in Vergabeverfahren der öffentlichen Hand zu gewährleisten, da AGB unterschiedlicher Auftragnehmer bzw. Bieter schwer vergleichbar sind. Es empfiehlt sich für die Vergabestelle, im Vorfeld diejenigen Kategorien auszuwählen, in denen abweichende Regelungen denkbar wären und diese ggfs. als Bewertungskriterien über die Leistungsbewertungsmatrix abzufragen.

Auftragnehmerseitige AGB müssen immer als Anhang (ggfs. in elektronischer Form) dem EVB-IT Cloudvertrag bzw. der Anlage zum Kriterienkatalog beigefügt werden. Ein Verweis auf die Website des Auftragnehmers ist unzulässig.

Zudem ist hervorzuheben, dass je Zeile nur eine Ziffer/ein Paragraf der auftragnehmerseitigen AGB auszufüllen ist. Sofern die Anzahl der Zeilen nicht ausreicht, muss der Bieter über eine Bieterfrage die Ergänzung weiterer Zeilen durch die Vergabestelle erbitten. Andernfalls ist es ihm nicht gestattet, zusätzliche Zeilen zu ergänzen.

Sofern in der obenstehenden Tabelle keine Abweichungen vereinbart werden, bzw. im Kriterienkatalog, richten sich die Regelungen zu den genannten Kategorien aus dem Kriterienkatalog nach den EVB-IT Cloud AGB:

3. Leistungsort: Ziffer 4 der AGB;
5. Übergabepunkt: Ziffer 5 der AGB, dort „Zugriff/Speicherplatz“;
7. Nutzer: Ziffer 14 der AGB „Nutzungsrechte“;
11. Sonstige Nutzungsumfang/Lizenzmetrik: Ziffer 14 der AGB „Nutzungsrechte“;
12. Endgeräte/Zugang: Ziffer 5 der AGB, dort „Zugriff/Speicherplatz“;
16. Datensicherung: Ziffer 7 der AGB;
20. Gutschrift bei Nichtverfügbarkeit: in den AGB nicht explizit geregelt;
22. Protokollierung: in den AGB nicht explizit geregelt, jedoch ergeben sich Nachweispflichten aus Ziffer 6 der AGB „Datenschutz, IT-Sicherheit und Vertraulichkeit“ sowie Ziffer 8 AGB zur „Verfügbarkeit“;
24. Reporting: Ziffer 9 der AGB.

Ergänzende Vertragsbedingungen für Cloudleistungen – EVB-IT Cloud-AGB

Abschnitt „1 Gegenstand des Vertrages“

Zu Ziffer 1.2

> 1.2 Der Auftragnehmer erbringt die Leistungen unter Einhaltung des bei Vertragsschluss jeweils aktuellen Cloud Computing Compliance Criteria Catalogue - C5 (Basiskriterien). Zudem beachtet der Auftragnehmer die durch den Auftraggeber zum Vertragsinhalt gemachten Sicherheitsanforderungen, z.B. aus seiner Sicherheitsrichtlinie im Sinne des Mindeststandard(s) des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Nutzung externer Cloud-Dienste.
>
> Sofern sich der Anforderungskatalog C5 (Basiskriterien) während der Laufzeit des Vertrages ändert, wird sich der Auftragnehmer bemühen, auch die neuen bzw. geänderten Anforderungen innerhalb angemessener Frist zu erfüllen. Sollte der Auftragnehmer nicht innerhalb von zwölf Monaten (vorbehaltlich einer anderen vom Gesetzgeber vorgegebenen Umsetzungsfrist, die in jedem Fall einzuhalten ist) ab der Veröffentlichung des Nachfolgedokumentes gegenüber dem Auftraggeber auf Anforderung erklären, dass er die neuen und die geänderten Anforderungen erfüllt, hat der Auftraggeber ein mit einer Frist von einem Monat auszuübendes Sonderkündigungsrecht bezogen auf die betroffenen Leistungen. Der Auftraggeber verliert das Sonderkündigungsrecht nicht dadurch, dass er es nicht unverzüglich ausübt. Die Erneuerung eines etwaigen Testats erfolgt im üblichen Prüfungsturnus.

Der Auftragnehmer soll entsprechend der Vorgabe seine Leistungen unter Einhaltung des bei Vertragsschluss jeweils aktuellen Cloud Computing Compliance Criteria Catalogue - C5 (Basiskriterien) erbringen. Hierbei ist zu beachten, dass eine Zertifizierung nach BSI C5 nicht möglich ist, lediglich eine Testierung ist vorgesehen. Das BSI erkennt zwei Testate an: Typ 1 und Typ 2:

- Bei einem Typ 1 Testat gibt ein Auditor 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. D. h., der Auditor prüft nicht, ob die Kontrollen angewendet werden, sondern nur, ob die vorhandenen Kontrollen die Erfordernisse erfüllen würden, wenn die Kontrollen auch angewendet würden.
- Hingegen umfasst ein Typ 2 Testat auch eine Prüfung der Wirksamkeit der Kontrollen, denn neben der Aussage zur Angemessenheit umfasst das Prüfungsurteil in einem Typ 2 Testat immer auch eine Aussage über die Wirksamkeit der Kontrollen in dem jeweiligen Prüfungszeitraum.

Nach Auffassung des BSI ist eine Wirksamkeitsprüfung (Typ 2) erforderlich, um eine angemessene Aussagekraft zu erzielen[27].

Entsprechend § 33 Abs. 1 Vergabeverordnung[28] können öffentliche Auftraggeber Bescheinigungen von einer Konformitätsbewertungsstelle einfordern, d. h. Zeugnisse von Zertifizierungs- und Inspektionsstellen. Bei einem Testat handelt es sich mangels einer entsprechenden Stelle jedoch nicht um ein entsprechendes Zeugnis.

[27] Siehe BSI FAQ zu C5, Abschnitt „Zugrundeliegende Prüfungsmethodik“. Online, zuletzt abgerufen 2023-07-23 unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Einfuehrung/Pruefer/Pruefer_node.html

[28] https://www.gesetze-im-internet.de/vgv_2016/__33.html

Daher verlangt Ziffer 1.2 nicht die Vorlage eines entsprechenden Testats, sondern die Einhaltung der im BSI C5 hinterlegten Anforderungen. Wie der Auftragnehmer die Einhaltungen nachweist, liegt im Ermessen des Auftraggebers.

Zu beachten: Bei Abweichungen von den C5-Basiskriterien seitens des Auftragnehmers resp. von Unterauftragnehmern ist eine Bieteranfrage erforderlich, ob eine explizite Vereinbarung hinsichtlich der Abweichung im Cloud-Vertrag möglich ist.

Insbesondere bei einer SaaS-Dienstleistung ist zu beachten, dass keine gemeinsame Testierung gefordert ist. Seitens eines IaaS- oder PaaS-Anbieters, den der SaaS-Anbieter einsetzt, reicht die Vorlage eines C5-Testats aus, sodass in diesen Fällen der SaaS-Anbieter nur die Nachweise für seine eigene Dienstleistung erbringen muss.

Zu beachten ist, dass der Auftragnehmer immer auch ein Informationssicherheits-Managementsystem (ISMS) gemäß ISO 27001 einschließlich eines Notfall-Managements aufweisen muss (siehe Ziffer 6.2.1)

Zu Ziffer 1.3

> 1.3 Der Auftragnehmer ist verpflichtet, seine Leistungen ständig mit geeigneten technischen Mitteln (Monitoring*) zu überwachen. Die Reportingpflicht aus Ziffer 9 wird hierdurch nicht erweitert.

Zu beachten ist, dass je nach Ausgestaltung des Monitorings auch personenbezogene Daten wie z. B. IP-Adressen verarbeitet werden. Ziffer 1.3 stellt keinen Erlaubnistatbestand zur Verarbeitung personenbezogener Daten wie beispielsweise von Beschäftigtendaten dar, daher muss im Falle der Verarbeitung personenbezogener Daten im Rahmen des Monitorings neben der Erforderlichkeit insbesondere auch die Rechtsgrundlage der Verarbeitung dargestellt werden.

Zuständig hierfür ist der Auftraggeber, entsprechend Ziffer 17.3 muss der Auftragnehmer aber auch selbstständig prüfen, ob personenbezogene Daten im Rahmen des Auftrags verarbeitet werden dürfen. Es ist Auftragnehmern daher anzuraten, im Falle der Verarbeitung personenbezogener Daten beim Monitoring 1) den Auftraggeber darüber zu informieren und 2) sich vom Auftraggeber die Rechtmäßigkeit prüfbar bestätigen zu lassen.

Zu Ziffer 1.4

> 1.4 Der Auftragnehmer stellt die Leistungen frei von Schaden stiftender Software zur Verfügung. Dies gilt auch für etwaige dem Auftraggeber überlassene Software (z.B. Zugangssoftware*). Der Auftragnehmer gewährleistet darüber hinaus, dass die Leistungen frei von Funktionen sind, die die Integrität, Vertraulichkeit und Verfügbarkeit der Daten des Auftraggebers oder vom Auftraggeber eingebrachte andere Daten bzw. von ihm eingebrachte Software gefährden und den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen durch
>
> - Funktionen zum unerwünschten Absetzen/Ausleiten von Daten,
> - Funktionen zur unerwünschten Veränderung/Manipulation von Daten oder der Ablauflogik oder
> - Funktionen zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen.
>
> Unerwünscht ist eine mögliche Aktivität einer Funktion, wenn die Aktivität so weder vom Auftraggeber in seiner Leistungsbeschreibung gefordert, noch vom Auftragnehmer unter konkreter Beschreibung der Aktivität und ihrer Funktionsweise angeboten, noch den Anforderungen des Anforderungskataloges C5 gemäß Ziffer 1.2 genügt.

Die Software darf keine unerwünschte Funktion bzgl. Verarbeitung von Daten beinhalten. Grundsätzlich kann auch eine Fernwartungssoftware unter diese Regelung fallen. Hier müssen ggf. Besonderheiten aus dem jeweiligen Landeskrankenhausgesetz beachtet werden. Z. B. verlangt § 38 Abs. 2 Krankenhausgesetz für das Land Mecklenburg-Vorpommern, dass

eine über drei Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer außerhalb des Krankenhauses nur zulässig ist,
wenn die Patientendaten auf getrennten Datenträgern gespeichert sind,
die der Auftragnehmer für den Krankenhausträger verwahrt.

Weiterhin muss geprüft werden, ob seitens Auftragnehmer eine „konkrete Beschreibung“ der Aktivitäten sowie der Funktionsweise vorhanden ist. Häufig finden sich nur allgemeine Hinweise, wie Cloud-Leistungen erbracht werden, ohne dass die Art und Weise der Leistungserbringung konkret geprüft werden kann.

Unerwünscht ist eine mögliche Aktivität einer Funktion, wenn die Aktivität so weder vom Auftraggeber in seiner Leistungsbeschreibung gefordert noch vom Auftragnehmer unter konkreter Beschreibung der Aktivität und ihrer Funktionsweise angeboten, noch den Anforderungen des Anforderungskataloges C5 gemäß Ziffer 1.2 genügt.

Abschnitt „2 Art und Umfang der Leistungen“

Zu Ziffer 2.1.1

> 2.1.1 Soweit eine SaaS*- oder PaaS*-Leistung geschuldet ist, stellt der Auftragnehmer dem Auftraggeber ab dem vereinbarten Bereitstellungszeitpunkt die im Vertrag vereinbarte Anwendung/Plattform zur Nutzung in einer vom Auftragnehmer betriebenen Cloudinfrastruktur einschließlich der notwendigen Zugänge zur Verfügung. Der Auftragnehmer sorgt für die vereinbarte Verfügbarkeit gemäß Ziffer 8.1, die vereinbarte Qualität der Leistung (funktional und nichtfunktional) sowie für die Sicherheit im Rahmen seines Verantwortungsbereichs während der gesamten Laufzeit der Leistung. Insbesondere hat der Auftragnehmer die Cloudinfrastruktur und die Anwendung bzw. Plattform so zu dimensionieren, dass diese mit einer im Hinblick auf die zu erwartenden bzw. vereinbarten Zugriffe angemessenen Reaktions- und Ausführungsgeschwindigkeit und mit einem für die bestimmungsgemäße Nutzung ausreichendem bzw. dem vereinbarten Speicherplatz verfügbaren aktuellen Sicherheitspatches und auch im Übrigen den vereinbarten Anforderungen entsprechend zur Verfügung steht.
>
> Soweit bei PaaS* der Auftraggeber Anwendungen auf der Plattform betreibt, ist er für diese, deren Verfügbarkeit, Inhalte und Architektur sowie deren Leistungsfähigkeit ebenso wie für seine Entwicklungstätigkeiten verantwortlich. Der Auftraggeber wird ohne vorherige Zustimmung des Auftragnehmers keine Penetrationstests in der jeweiligen Cloudinfrastruktur durchführen oder autorisieren.
>
> Darüber hinaus ergibt sich der Umfang der Leistungen aus dem Vertrag.

Gemäß Ziffer 2.1.1 darf der Auftraggeber ohne vorherige Zustimmung des Auftragnehmers keine Penetrationstests in der jeweiligen Cloudinfrastruktur durchführen oder autorisieren. Jedoch können entsprechende Penetrationstests für den Nachweis einer sicheren Verarbeitung erforderlich sein. Viele Cloud-Anbieter führen für ihr System Penetrationstests durch, was jedoch nicht die eingesetzte Infrastruktur des Auftragnehmers beinhaltet. Um das gesamte System zu testen, muss also Infrastruktur des Auftraggebers sowie die genutzten Bestandteile des Auftragnehmers in entsprechende Sicherheitstests einbezogen werden.

Auftragnehmer sollten sich daher vertraglich seitens des Auftragnehmers zusichern lassen, dass Auftragnehmer entsprechende Penetrationstests unter Beachtung der Sicherheitsbelange und der Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie der weiteren Kunden des Auftragnehmers zulassen und unterstützen, insbesondere nicht ohne konkrete Begründung verweigern.

Soweit bei PaaS der Auftraggeber Anwendungen auf der Plattform betreibt, ist er für diese, deren Verfügbarkeit, Inhalte und Architektur sowie deren Leistungsfähigkeit ebenso wie für seine Entwicklungstätigkeiten verantwortlich. Der Auftraggeber wird ohne vorherige Zustimmung des Auftragnehmers keine Penetrationstests in der jeweiligen Cloudinfrastruktur durchführen oder autorisieren.

Abschnitt „3 Nutzungsverbote“

Zu Ziffer 3.2

> 3.2 Soweit der bestimmungsgemäße Gebrauch der Leistung nicht explizit beschrieben ist, ist eine Verwendung der Leistung im Hochrisikobereich ausgeschlossen (Betrieb von Kernenergieanlagen, Flugsicherungssystemen, Kriegswaffen, lebenserhaltenden Apparaten oder vergleichbare risikobehaftete Anwendungen, bei denen Leistungsstörungen typischerweise unmittelbar zum Tod von Menschen oder zu Großschadenslagen führen).

Gemäß Ziffer 3.2 ist der Cloud-Einsatz im Hochrisikobereich nicht statthaft, wenn der bestimmungsgemäße Gebrauch dies nicht explizit beschreibt. Im Bereich der Gesundheits- bzw. Patientenversorgung wird eher regelhaft von einem Hochrisikobereich auszugehen sein: Liegen bereits dokumentierte, aber aufgrund eines Cloud-Ausfalls nicht zur Verfügung stehende Daten wie beispielsweise Blutgruppe oder Allergien zur Behandlung eines Patienten nicht vor, kann dies den Tod eines Patienten zur Folge haben. Patientendatenmanagementsysteme unterstützen die Arbeit auf Intensivstationen, OP und Aufwachraum, sind diese Systeme und damit die darin enthaltenen Daten jedoch nicht nutzbar, kann dies direkte Auswirkungen auf die Gesundheit von Patienten haben.

Daher sollte im Rahmen von Ausschreibungen unter Nutzung der EVB-IT Cloud immer der bestimmungsgemäße Gebrauch dahingehend ausgestaltet werden, dass jedermann ersichtlich ist, welche Hochrisikobereiche von der Cloud-Dienstleistung umfasst werden.

Abschnitt „4 Leistungsort“

Zu Ziffer 4

Die Verarbeitung ist gemäß Ziff. 4 nur in der EU/EWR und der Schweiz zulässig. Dabei ist zu beachten, dass eine Verarbeitung in Art. 4 Ziff. 2 DS-GVO sehr weitreichend definiert ist. Greift im Rahmen der Fernwartung ein Beschäftigter eines Auftragnehmers aus einem Land auf Daten eines Auftraggebers zu, so werden Daten im Land des zugreifenden Beschäftigten verarbeitet.

Somit ist auch eine Fernwartung nur aus den in Ziffer 4 genannten Ländern statthaft.

Eine Ausnahme wird nur erlaubt, wenn der Auftraggeber in der Administrationskonsole (Self-Service-Portal o. Ä.) zusätzlich weitere Regionen für die Leistungen auswählte. Es ist also ein aktiver Prozess durch den Auftraggeber erforderlich, eine alleinige vertragliche Regelung, insbesondere durch AGB des Auftragnehmers, wird hier nicht ausreichen.

Gerade bei Einsatz von amerikanischen Cloud-Anbietern ist seitens dieser eine rein europäische Speicherung meistens möglich, nicht jedoch eine Verarbeitung der Kunden-Daten ausschließlich in der EU/EWR. Hier ist darauf zu achten, dass Cloud-Anbieter (Auftragnehmer) Kunden (= Auftraggeber) ggf. vertraglich verpflichten, in einer Administrationskonsole eine Verarbeitung von Daten des Auftraggebers auch in anderen Ländern im zwingend erforderlichen Umfang zu erlauben.

Auftraggeber wiederum sollten sich in diesen Fällen vom Auftragnehmer darstellen lassen

a) warum der Zugriff aus diesen Ländern zwingend erforderlich ist und nicht aus den EU/EWR heraus erfolgen kann (der Verantwortliche muss gemäß Art. 5 Abs. 2 DS-GVO u. a. den Nachweis der Erforderlichkeit führen),
b) wie die Sicherheit der Verarbeitung in jedem der vom Auftragnehmer geforderten Länder gewährleistet ist und
c) wie in Ländern ohne Angemessenheitsbeschluss die Vorgaben aus Kap. V DS-GVO für jedes der geforderten Länder unter Beachtung der im Schrems I und Schrems II Urteil des EuGH dargestellten Vorgaben erfüllt werden,

bevor eine Freischaltung des jeweiligen Landes in einer Managementkonsole vorgenommen wird.

Abschnitt „5 Zugriff/Speicherplatz“

Zu Ziffer 5.3

> 5.3 Der Auftragnehmer ist verpflichtet, den Zugriff auf die Daten des Auftraggebers durch unberechtigte Stellen und Personen mit angemessenen Maßnahmen zu verhindern.

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.

Hier muss der Auftraggeber dafür Sorge tragen, dass vertraglich geregelt wird, dass ausschließlich deutsches Recht zur Beurteilung der Frage „berechtigter vs. unberechtigter Zugriff“ anwendbar ist.

Abschnitt „6 Datenschutz, IT-Sicherheit und Vertraulichkeit“

Zu Ziffer 6.1.1

> 6.1.1 Die Parteien werden die bei der Erbringung der Leistung jeweils auf sie anwendbaren Bestimmungen über den Datenschutz in der jeweils geltenden Fassung einhalten. Der Auftragnehmer verfügt über eine hinreichende Dokumentation über die Umsetzung der gesetzlichen Anforderungen, die der Auftragnehmer dem Auftraggeber auf Anforderung zugänglich macht.

Es 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.

Entsprechend § 1.2.1 des Cloud-Vertrages gilt ein Vertrag zur Auftragsverarbeitung nachrangig gegenüber dem Kriterienkatalog für Cloudleistungen inklusive Anlage zur Einbeziehung von auftragnehmerseitigen AGB mit Anhang I und II. Ziffer 24 enthält die Klausel hinsichtlich abweichender Normen; Ziffer 6.1.1 derselben Vertragsbedingungen wird man wahrscheinlich als eine abweichende Norm betrachten müssen.

D. h., wenn hierüber entsprechende Länder außerhalb der EU/EWR zugelassen werden, ist es fraglich, ob Regelungen im Vertrag zur Auftragsverarbeitung vorrangig gegenüber dieser Regelung anwendbar sind und somit für einen in einem Drittland tätigen (Unter-)Auftragnehmer über eine Regelung des Vertrages zur Auftragsverarbeitung (auch) das europäische sowie deutsche Datenschutzrecht anwendbar ist.

Um Rechtssicherheit zu erhalten, sollten Auftraggeber über die Rechtswahl vertragsseitig nur deutsches Recht zulassen. Bestehen Auftragnehmer auf die Anwendbarkeit von nicht-deutschem Recht, ist eine gründliche Prüfung, ob der Auftraggeber den Vertrag unter diesen Bedingungen abschließen darf, anzuraten.

Zu Ziffer 6.1.2

> 6.1.2 Der Auftragnehmer sorgt dafür, dass alle Personen, die von ihm mit der Verarbeitung personenbezogener Daten des Auftraggebers betraut sind, die auf den Auftragnehmer anwendbaren Bestimmungen über den Datenschutz beachten. Soweit eine Verpflichtung auf das Datengeheimnis erforderlich ist, ist diese spätestens vor der erstmaligen Aufnahme der Tätigkeit vorzunehmen und dem Auftraggeber auf Verlangen vorzulegen.

Im Gesundheitsbereich werden regelhaft Daten von Patienten (bei Leistungserbringern) oder Versicherten (Leistungsträgern) verarbeitet. Diese Daten unterliegen grundsätzlich Verbot einer unbefugten Offenbarung gemäß § 203 StGB[29]. Entsprechend § 203 Abs. 4 StGB muss in diesen Fällen das Personal von eingesetzten Dienstleistern zur Geheimhaltung verpflichtet werden.

Gesetzliche Krankenversicherungen gehören zu den in § 35 SGB I[30] genannten Leistungsträgern und unterliegen zusätzlich dem Sozialgeheimnis. Entsprechend § 35 Abs. 6 i. V. m. § 35 Abs. 1 S. 2 SGB I

[29] § 203 StGB „Verletzung von Privatgeheimnissen“. Online, zuletzt abgerufen 2023-08-23 unter https://www.gesetze-im-internet.de/stgb/__203.html

[30] § 35 SGB I „Sozialgeheimnis“. Online, zuletzt abgerufen 2023-08-23 unter https://www.gesetze-im-internet.de/sgb_1/__35.html

müssen Beschäftigte von Auftragsverarbeitern zur Einhaltung des Sozialgeheimnisses verpflichtet werden.

Im Bereich der Verarbeitung von Patientendaten muss gemäß Art. 9 Abs. 3 DS-GVO gewährleistet werden, dass

> diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet wird
> und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt,
> oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

Die in Ziffer 6.1.2 angesprochene Verpflichtung auf das Datengeheimnis, welche für Auftragsverarbeiter durch Art. 28 Abs. 3 S. 2 lit. b DS-GVO eine Pflicht darstellt, reicht daher nicht aus, sondern es muss vertraglich vereinbart werden, dass für den Auftraggeber rechtlich geforderte Verpflichtungen durch den Auftragnehmer verbindlich geregelt werden.

Dies kann beispielsweise im Rahmen des in Ziffer 6.1.3 dargestellten Auftragsverarbeitungsvertrages nach Art. 28 DS-GVO erfolgen.

Zu Ziffer 6.2.1

> 6.2.1 Der Auftragnehmer verfügt für die Bereitstellung der Leistung (inklusive der dazu notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten) über ein angemessenes, dokumentiertes und implementiertes Sicherheitskonzept und ein Informationssicherheits-Managementsystem (ISMS) jeweils gemäß ISO 27001 einschließlich eines Notfall-Managements. Das Sicherheitskonzept hat sich an ISO 27017 auszurichten. Sofern personenbezogene Daten verarbeitet werden, hat es sich zudem an ISO 27018 auszurichten.
>
> Soweit vereinbart, weist der Auftragnehmer dies durch gültige Zertifikate oder gleichwertige Nachweise nach. Sicherheitskonzept, ISMS und Zertifikate müssen, soweit auf die zu erbringende Leistung anwendbar, diese vollumfänglich abdecken und sind entsprechend des festgelegten Prüfungsturnus im relevanten Standard zu erneuern.

Hier ist zu beachten, dass das geforderte 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 (was im Bereich der Gesundheitsversorgung vermutlich regelhaft gegeben sein wird), auch an EN ISO/IEC 27018 ausrichten muss.

Je nach Festlegung des Auftraggebers muss der Auftragnehmer dies durch gültige Zertifikate oder gleichwertige Nachweise nachweisen.

Hinweis:

> Verträge wie der EVB-IT Cloud-Vertrag werden ausschließlich zwischen den Vertragspartnern abgeschlossen, nicht mit Dritten wie Unterauftragnehmern des Auftragnehmers. Wenn im EVB-IT Cloud die Erfüllung von Anforderungen gefordert und durch einen Bieter resp. späteren Auftragnehmer zugesichert werden, darf der Auftragnehmer ausschließlich Unter-Auftragnehmer einsetzen, welche die Erfüllung der vertraglich vereinbarten Leistungen ermöglichen. Weiterhin muss der Auftragnehmer alle vertraglich zugesicherten Anforderungen, welche auf den Unter-Auftragnehmer zutreffen, vertraglich an diesen weiterreichen.

Beispiel:

- Ein Softwareanbieter setzt einen Cloud-Anbieter ein, um eine SaaS-Lösung anzubieten. Ziffer 6.2.1 erfordert die Erfüllung von ISO/IEC 27001 in Kombination mit EN ISO/IEC 27017 sowie der EN ISO/IEC 27018. EN ISO/IEC 27017 und EN ISO/IEC 27018 adressieren ausschließlich Cloud-Anforderungen, welche der Softwareanbieter einkauft. Daraus folgt bzgl. der Erbringung der geschuldeten Leistungen, dass die Anforderungen zwischen Bieter/Auftragnehmer und Unter-Auftragnehmer durch entsprechende Vertragsgestaltung zwischen Bieter/Auftragnehmer und Unter-Auftragnehmer wie folgt gewährleistet sein müssen:
  - Bieter/Auftragnehmer: Nachweis der Erfüllung der ISO/IEC 27001 durch eine geltende Zertifizierung;
  - Unter-Auftragnehmer: Nachweis der Erfüllung der ISO/IEC 27001 beinhaltend die Anforderungen der EN ISO/IEC 27017 und EN ISO/IEC 27018 durch eine geltende Zertifizierung.

Zu Ziffer 6.3.1, 6.3.2

> 6.3.1 Die Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten vertraulichen Informationen, Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln, insbesondere nicht an unberechtigte Dritte weiterzugeben oder anders als zu vertraglichen Zwecken zu verwerten. Die vorgenannte Pflicht zur Vertraulichkeit schränkt jedoch keine Partei darin ein, für sie tätige Personen, die Zugang zu vertraulichen Informationen hatten, in anderen Projekten einzusetzen. Der Erfahrungsaustausch des Auftraggebers mit und innerhalb der öffentlichen Hand bleibt unbenommen, ebenso wie die Erfüllung gesetzlicher Pflichten.
>
> 6.3.2 Vertrauliche Informationen sind Informationen, die ein verständiger Dritter als schützenswert ansehen würde oder die als vertraulich gekennzeichnet sind; dies können auch solche Informationen sein, die während einer mündlichen Präsentation oder Diskussion bekannt werden. Vertrauliche Informationen dürfen ausschließlich zum Zweck der Erfüllung der Verpflichtungen aus dem Vertrag eingesetzt bzw. verwertet werden. Die Verpflichtung zur Vertraulichkeit gilt nicht für Informationen, die den Parteien bereits rechtmäßig bekannt sind oder außerhalb des Vertrages ohne Verstoß gegen eine Vertraulichkeitsverpflichtung bekannt werden.

In Ziffer 6.3.1 verpflichten sich die Vertragsparteien, vertrauliche Informationen, Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln. In Ziffer 6.3.2 werden „vertrauliche Informationen“ als Informationen, welche „ein verständiger Dritter als schützenswert ansehen würde oder die als vertraulich gekennzeichnet sind“, definiert.

Beachtet werden muss, dass Geschäftsgeheimnisse in § 2 Ziff. 1 GeschGehG[31] definiert wird.

Weiterhin muss bei der Verarbeitung von Sozialdaten beachtet werden, dass Betriebs- und Geschäftsgeheimnisse eines dem Sozialgeheimnis unterstehenden Auftraggeber entsprechend § 35 Abs. 4 SGB I[32] Sozialdaten gleichstehen, somit entsprechender Schutzbedarf auch für diese Daten besteht. Nach § 35 Abs. 6 SGB I gilt diese Regelung auch für Auftragsverarbeiter.

[31] § 2 GeschGehG „Begriffsbestimmungen“. Online, zuletzt abgerufen 2023-08-23 unter https://www.gesetze-im-internet.de/geschgehg/__2.html

[32] § 35 SGB I „Sozialgeheimnis“. “. Online, zuletzt abgerufen 2023-08-23 unter https://www.gesetze-im-internet.de/sgb_1/__35.html

Zu Ziffer 6.4.2

> 6.4.2 Bestehen Zweifel des Auftraggebers in Bezug auf die vom Auftragnehmer nach Ziffer 6.4.1 zur Verfügung gestellten Unterlagen, die der Auftragnehmer auf Nachfrage innerhalb angemessener Frist auszuräumen nicht in der Lage ist, ist der Auftragnehmer verpflichtet, entsprechend qualifiziertem bzw. ausgebildetem Personal des Auftraggebers oder einer vom Auftraggeber beauftragten unabhängigen zur Berufsverschwiegenheit verpflichteten Prüfungsgesellschaft während der normalen Geschäftszeiten Zugang insbesondere zu den für die Verarbeitung der Daten des Auftraggebers relevanten Verarbeitungssystemen, Einrichtungen sowie zu unterstützenden Unterlagen zu gewähren, sodass der Auftraggeber prüfen kann, ob der Auftragnehmer die Vorgaben einhält. Die Prüfung ist unter Beachtung der Sicherheitsbelange und der Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie der weiteren Kunden des Auftragnehmers durchzuführen. Der Auftragnehmer ist verantwortlich dafür, dass die Prüfung gleichwohl effektiv und im erforderlichen Umfang erfolgen kann. Jede Partei trägt die ihr entstehenden Kosten für derartige Prüfungen selbst. Soweit zielführend, sollte sich die Prüfung an dem Leitfaden „Anwendung des BSI C5 durch Interne Revision und Informationssicherheit" der ISACA Germany Chapter e.V. orientieren. Die Grundsätze von Verhältnismäßigkeit und Wirtschaftlichkeit sind dabei grundsätzlich im Interesse aller Parteien zu wahren. Sofern das Prüfungsergebnis lediglich unwesentliche Beanstandungen ergibt, zahlt der Auftraggeber eine Vergütung, sofern eine solche für diesen Fall im Kriterienkatalog vorgesehen ist.

Bei Zweifeln an der Erbringung der vereinbarten Leistungen steht dem Auftragnehmer eine Prüfung der Auftragnehmer auch vor Ort zu.

Dabei soll sich die Prüfung, soweit zielführend, dem Leitfaden „Anwendung des BSI C5 durch interne Revision und Informationssicherheit"[33] der ISACA Germany Chapter e. V. orientieren. Dies wird regelhaft nur der Fall sein, wenn es um die Prüfung der Einhaltung der Anforderungen des BSI C5 Anforderungskatalog handelt.

Entsprechend Ziffer 6.4.2 Satz 4 trägt bei dieser Prüfung jede Partei die eigenen Kosten. Allerdings enthält Ziffer 6.4.2 Satz 7 eine Ausnahme: Sofern das Prüfungsergebnis lediglich unwesentliche Beanstandungen ergibt, zahlt der Auftraggeber eine Vergütung, sofern eine solche für diesen Fall im Kriterienkatalog vorgesehen ist.
Hinsichtlich dieser Regelung erscheint es sinnvoll, dass im Rahmen des Vertragsabschlusses

a) festgelegt wird, welche Kriterien erfüllt sein sollten, damit ein Auftragnehmer „Zweifel" an der Erbringung der vereinbarten Leistungen haben darf und
b) definiert wird, was unter „unwesentlichen" und „wesentlichen" Beanstandungen zu verstehen ist,

denn im Prüfungsfall sind streitige Auslegungen häufig nur schwierig einvernehmlich zu klären.

SaaS-Anbieter müssen vertraglich die Pflicht an Unterauftragnehmer, insbesondere IaaS- und PaaS-Unterauftragnehmer, weitergeben. Hierbei ist zu beachten, dass insbesondere Hyperscaler in ihren Standardbedingungen regelmäßig kein allgemeines Audit-Recht vorsehen und häufig auch keine Audit-Rechte in ihren Rechenzentren akzeptieren, soweit es nicht ausnahmsweise eine gesetzliche Verpflichtung für den Auftraggeber zur Vereinbarung solcher Audit-Rechte gibt. SaaS-Anbieter müssen daher eine entsprechende Auswahl seitens ihrer Unterauftragnehmer treffen, damit den vertraglichen Verpflichtungen genügt werden kann.

[33] BSI: C5 und IT-Revision. Hier auch Download-Möglichkeit des Leitfadens. Online, zuletzt abgerufen 2023-07-23 unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Im_Kontext/C5_und_IT_Revision/C5_und_IT_Revision_node.html

Abschnitt „7 Datensicherungsservice / Backup / Herausgabe- und Löschungsanspruch“

Es sind seitens des Bieters/Auftragnehmers nach dem EVB-IT Cloud **keine Datensicherungen geschuldet**. Der Auftraggeber muss daher selbst dafür Sorge getragen werden, dass die in der Cloud betriebenen Anwendungen sowie die entsprechenden Daten regelmäßig gesichert werden.

Soll eine Datensicherung vom Bieter/Auftragnehmer übernommen werden, muss das „Ob“ und der Umfang der Backup-Pflichten ausdrücklich über den Kriterienkatalog (Abschnitt 1 „Kriterien“, Ziff. 16) oder über eine eigenständige Anlage vertraglich vereinbart werden.

Zu Ziffer 7.3

> 7.3 Die Leistung ist so auszugestalten, dass die Daten des Auftraggebers entweder zu jeder Zeit selbstständig durch den Auftraggeber oder, soweit dies aus technischen Gründen nicht möglich ist, mit Unterstützung durch den Auftragnehmer aus der Cloudinfrastruktur in einem marktüblichen Austauschformat exportiert werden können. Damit muss auch der Export von vom Auftraggeber bestimmten Teilen der Daten möglich sein. Soweit die Daten verschlüsselt sind, ist diese Pflicht nur dann erfüllt, wenn der Auftraggeber über den Schlüssel verfügt. Für den Export der Daten und deren Sicherung bei dem Export ist der Auftraggeber verantwortlich.

Art. 2 Ziff. 13 Richtlinie (EU) 2019/1024[34] 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.

Da Art. 20 DS-GVO die Weitergabe personenbezogener Daten auf Antrag einer betroffenen Person in einem „strukturierten, gängigen und maschinenlesbaren Format“ beschreibt, wird angeraten, die europäische Definition im Kontext der Ziffer 7.3 vertraglich durch eine entsprechende Anforderung im Rahmen der Ausschreibung festzuhalten, damit der Auftraggeber seinen gesetzlichen Anforderungen nachkommen kann. Ein „marktübliches Austauschformat“ wird ggf. nicht den aus der DS-GVO resultierenden gesetzlichen Anforderungen genügen.

[34] 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

Abschnitt „8 Verfügbarkeit“

Die prozentuale Verfügbarkeit errechnet sich nur aus dem Zeitraum, in dem die Leistungen vertragsgemäß hätten zur Verfügung stehen müssen. Ziffern 8.2 und 8.3 enthalten Regelungen, wo die Nichtverfügbarkeit der vertraglich vereinbarten Leistungen nicht die Verfügbarkeit berühren.

Wenn beispielsweise der Auftragnehmer wirklich jeden Sonntag zwischen 4:00 und 8:00 Uhr eine Wartung durchführt (siehe Ziffer 8.3) und die vertraglich vereinbarte Leistung nicht zur Verfügung steht, dann kann immer noch eine 100%ige Verfügbarkeit gegeben sein, wenn ansonsten keine Ausfälle auftreten, welche die Verfügbarkeit beeinträchtigen.

Zu Ziffer 8.2

Die Kernbetriebszeit wird im Kriterienkatalog bei Ziffer 19 (Überschrift „1. Kriterien“) festgelegt.

Zu Ziffer 8.3

8.3 Bezüglich der Verfügbarkeit gilt Folgendes:

- Der Auftragnehmer schuldet während der Betriebszeit* eine Verfügbarkeit von mindestens der Verfügbarkeitsklasse* VK1 im Bezugszeitraum.
- Der Bezugszeitraum ist der Kalendermonat.
- Alle Zeitangaben verstehen sich als Angaben nach mitteleuropäischer Zeit (MEZ) bzw. Sommerzeit (MESZ).
- Die Betriebszeit* ist die Zeit von Montag bis Sonntag von 0:00 bis 24:00 Uhr.
- Die Zeit von 04:00 bis 08:00 Uhr ist an Sonntagen Zeit geplanter Nichtverfügbarkeit (z.B. für Wartungsarbeiten) und wird bei der Berechnung der Verfügbarkeit nicht berücksichtigt.
- Ausfallzeiten*, die auf einem der folgenden Ereignisse beruhen, mindern die Verfügbarkeit nicht:
  - Probleme innerhalb des Netzwerks oder der Infrastruktur des Auftraggebers oder von vom Auftraggeber beauftragten Dritten,
  - Ausfall/Beeinträchtigung der Netzanbindung des Auftraggebers,
  - Ausfälle/Beeinträchtigungen, die auf dem Handeln oder Unterlassen des Auftraggebers oder eines nicht vom Auftragnehmer beauftragten Dritten beruhen,
  - nicht vertragsgemäße Nutzung der Leistung des Auftragnehmers durch den Auftraggeber,
  - Versäumnisse des Auftraggebers, vereinbarte Vorgaben zu erforderlichen Konfigurationen und Architekturen einzuhalten sowie fehlerhafte Eingaben beziehungsweise Anweisungen durch Nutzer des Auftraggebers,
  - Handlungen nicht autorisierter Nutzer, soweit die Handlungsmöglichkeit des nicht autorisierten Nutzers dem Auftraggeber zuzurechnen ist (bspw. durch die Nichtbeachtung angemessener Sicherheitsverfahren),
  - Aussetzen des Zugangs durch einen Sicherheitsvorfall* zum Schutz auch des Auftraggebers, sofern die internen Richtlinien (operative Maßnahmen), die Grundlage der Erfüllung der C5 Anforderungen sind, vergleichbar mit den IT-Grundschutz Bausteinen DER.2.X „Security Incident Management“ des BSI sind und aufgrund der Schwere des Sicherheitsvorfalls* eine Aussetzung als Maßnahme erlauben,
  - Ereignisse, die auf höherer Gewalt beruhen und nicht durch angemessene Maßnahmen des Auftragnehmers kompensiert werden können.
- Der Auftragnehmer ist für die Messung der Verfügbarkeit verantwortlich.

Krankenhäuser müssen 24 Stunden am Tag Patienten versorgen, auch an Sonn- und Feiertagen. Entsprechend Ziffer 8.3 ist die Zeitspanne von 04:00 bis 08:00 Uhr an Sonntagen Zeit geplanter Nichtverfügbarkeit, d. h., die Cloud-Leistung kann ggf. an 52 Tagen im Jahr sonntags in diesem Zeitraum nicht zur Verfügung stehen.

Unzweifelhaft bedürfen auch Cloud-Systeme einer regelmäßigen Wartung, aber die dargestellte Zeitspanne umfasst etwa 8,7 Tage oder – anders ausgedrückt – etwa 2,7 % der Zeitdauer eines Jahres.

Weiterhin ist zu beachten, dass dieser Zeitraum gerade im Krankenhaus die Arbeit in der Patientenversorgung deutlich beeinträchtigen kann. Zwar beginnen Patientenvisiten Sonntag meistens nach 8.00 Uhr, jedoch endet der Nachtdienst im Pflegebereich i. d. R. zwischen 6.00 und 7.00 Uhr. D. h. in den Zeitraum von 04:00 bis 08:00 Uhr steht an Sonntagen evtl. die Patientendokumentation für die Übergabe vom Nacht- an den Frühdienst nicht zur Verfügung, der Nachtdienst kann ggf. seinen gesetzlich vorgeschriebenen Dokumentationspflichten nicht genügen.

Daher sollte seitens des Auftraggebers geprüft werden, ob im Kriterienkatalog unter Ziffer 19 (Überschrift „1. Kriterien“) Anpassungen bzgl. der vereinbarten Zeiten für Wartung erforderlich sind.

Insbesondere sollte im Kriterienkatalog die Kernbetriebszeit festgelegt werden, in welcher nach Ziffer 8.2 eine Verfügbarkeit gewährleistet werden muss.

Abschnitt „9 Reportingpflichten“

Zu Ziffer 9.1

> 9.1 Bezüglich der Pflichten des Auftragnehmers zum Reporting wird Folgendes vereinbart:
>
> - Der Auftragnehmer ist für das laufende monatliche Reporting an den Auftraggeber verantwortlich; Reporting umfasst in Bezug auf die Verfügbarkeit sowie etwaige vereinbarte Reaktions- und Wiederherstellungszeiten mindestens folgende Informationen:
>   - Aufzeichnung der Zeiten der Verfügbarkeit und der Nichtverfügbarkeit,
>   - die sich daraus errechnende Verfügbarkeit/ Nichtverfügbarkeit pro Bezugszeitraum und
>   - im Bezugszeitraum aufgetretene, die Leistung betreffende und ggf. bereits behobene sicherheitsrelevante Störungen*,
>   - im Bezugszeitraum vom Auftraggeber gemeldete Störungen sowie deren Bearbeitungsstand (ggf. über ein eingesetztes Ticketsystem)
>   - Aufzeichnung der Überschreitung (in Minuten) von vereinbarten Reaktions- oder Wiederherstellungszeiten pro Überschreitungsfall.
> - Das Reporting umfasst im Falle einer nutzungsabhängigen Vergütung alle vergütungsrelevanten Parameter.
> - Das Reporting umfasst zudem etwaig geschuldete Gutschriften, wobei diese alternativ in der Abrechnung ausgewiesen werden können.

Das monatliche Reporting soll dem Auftraggeber einen möglichst detaillierten und umfassenden Überblick über bestimmte Kennzahlen und eventuelle Störungen des vergangenen Monats geben.

Der Auftraggeber muss insbesondere monatlich berichten, wie lange sein Cloud-Dienst in diesem Zeitraum nicht verfügbar war und was dies für die prozentuale Verfügbarkeit bedeutet. Insbesondere bei SaaS ist dabei zu beachten, dass dies die seitens Unterauftragnehmer bereitgestellten Ressourcen ebenfalls umfasst. Hier ist seitens SaaS-Anbieter darauf zu achten, dass nur Unterauftragnehmer eingesetzt werden können, die ein entsprechendes Reporting unterstützen.

Abschnitt „10 Störungsklassifizierung“

Die Begriffsbestimmungen enthalten lediglich die Definition der Störung:

> „Beeinträchtigung der Eignung der Leistung zur vertraglich vereinbarten, bzw. soweit eine solche Vereinbarung fehlt, zur vorausgesetzten oder sonst zur gewöhnlichen Verwendung. Dies gilt unabhängig von einem Vertreten müssen und unabhängig davon, ob diese Abweichung bereits bei Leistungsbeginn vorlag.“

Somit wird die Zuordnung einer Störung in eine der Störungsklassen ggf. seitens Auftraggeber und Auftragnehmer unterschiedlich bewertet. Daher ist anzuraten, in der Ausschreibung bereits festzulegen, wie die Gruppierung von Störungen in die drei Störklassen erfolgt.

Ein Beispiel, wie man im Kontext der Patientenversorgung bei einer Ausschreibung eine Klassifizierung vornehmen könnte:

> Eine schwerwiegende Störung liegt insbesondere vor, wenn Bereiche der Patientenversorgung durch einen Ausfall der Leistung eingeschränkt wird oder sogar nicht möglich ist. Zur Patientenversorgung gehören auch die Dokumentation sowie Abrechnung erbrachter Leistungen der Patientenversorgung.
>
> Eine erhebliche Störung liegt insbesondere vor, wenn die Störung Geschäftsprozesse und Arbeitsabläufe behindern.
>
> Eine leichte Störung liegt insbesondere vor, wenn die Nutzung der von der Störung betroffenen Leistung keine Auswirkungen auf die Patientenversorgung hat und alle wesentlichen Funktionalitäten ohne Beeinträchtigung seitens der Beschäftigten des Auftraggebers nutzbar sind.

Abschnitt „11 Störungsbeseitigung“

Im Vertrag 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 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 besitzen.

Die Wiederherstellungszeiten werden im Kriterienkatalog für Cloudleistungen unter Ziffer 21 vereinbart.

Abschnitt „12 Änderung der Leistung nach Vertragsschluss durch den Auftragnehmer“

> **12 Änderung der Leistung nach Vertragsschluss durch den Auftragnehmer**
>
> Um die Funktionalität der Leistungen zu verbessern oder die Leistungen dem Stand der Technik anzupassen, kann der Auftragnehmer die Leistungen nach Vertragsbeginn ohne Zustimmung des Auftraggebers anpassen. Eine solche Änderung darf aber nicht dazu führen, dass dem Auftraggeber die ursprünglich vereinbarten Funktionalitäten nicht mehr zur Verfügung stehen oder ursprünglich vereinbarte Anforderungen nur noch wesentlich eingeschränkt erfüllt werden. Wesentlich und damit unzulässig sind Änderungen bzw. Einschränkungen in jedem Fall dann, wenn diese zu einer schlechteren Bewertung der Leistungen im Vergabeverfahren geführt hätten.

In Ziffer 12 wird vom Auftraggeber verlangt, den Nachweis über „wesentliche“ Einschränkungen Zweifelsfall über Bewertungskriterien aus dem Vergabeverfahren zu führen. Hierzu muss nachgewiesen werden, dass die Einschränkungen im Vergabeverfahren zu einer schlechteren Bewertung geführt hätten.

Damit dies überhaupt möglich ist, müssen im Vergabeverfahren entsprechende Bewertungskriterien bzgl. der Funktionalitäten festgelegt werden.

Kerngedanke von CIO Bund und Bitkom bei der Vertragsgestaltung war vielleicht, dass Funktionalitäten, welche im Vergabeverfahren nicht entsprechend berücksichtigt wurden, bei der täglichen Arbeit keine Rolle spielen.

Im täglichen Leben wird immer wieder beobachtet, dass „eh da“-Funktionalitäten, also Funktionalitäten, die von allen Anbietern bekanntermaßen gleichermaßen angeboten werden, in Ausschreibungen nicht oder nur im geringen Umfeld berücksichtigt werden. Es ist daher seitens Auftraggeber schon im Vorfeld der Ausschreibungen darauf zu achten, dass alle benötigten oder gewünschten Funktionalitäten im Ausschreibungsverfahren entsprechend beschrieben und in den Bewertungskriterien berücksichtigt werden – auch wenn man zum Zeitpunkt der Ausschreibung davon ausgeht, dass alle Anbieter die Funktion gleichwertig anbieten und die Funktion die Bewertung voraussichtlich nicht ändern wird; man weiß nicht, ob dies in wenigen Jahren anders aussieht, man die Funktion in der gewünschten Form selber aber immer noch benötigt.

Abschnitt „13 Pflichten und Leistungen im Zusammenhang mit dem Vertragsende“

Zu Ziffer 13.2.2

> 13.2.2 Soweit sich die Migration verzögert, gleichgültig aus welchem Grund, wird der Auftragnehmer einmalig die Leistung auf Anforderung des Auftraggebers im bisherigen Umfang über das ursprüngliche Vertragsende hinaus weiter erbringen, bis die Übertragung erfolgreich vollzogen ist, unabhängig hiervon maximal jedoch für einen Zeitraum von sechs Monaten. Die Leistungserbringung erfolgt zu den bisherigen Konditionen. Für den Fall, dass dem Auftragnehmer darüber hinaus durch notwendige Leistungen Mehraufwände entstehen, kann der Auftragnehmer eine angemessene Anpassung der Vergütung verlangen.

Entsprechend Ziffer 13.2.2 kann es bei der Migration vorkommen, dass der Auftragnehmer über Vertragsende hinaus Leistungen erbringt. Werden im Rahmen der vereinbarten Leistungen personenbezogene Daten verarbeitet, muss auch in diesem Fall ein Vertrag zur Auftragsverarbeitung existieren, da ohne einen entsprechenden Vertrag ansonsten der Auftragnehmer entsprechend Art. 28 Abs. 10 DS-GVO[35] datenschutzrechtlich als Verantwortlicher anzusehen ist und somit eine eigene Rechtsgrundlage zur Verarbeitung der personenbezogenen Daten des Auftraggebers benötigt.

Einen Erlaubnistatbestand wird der Auftragnehmer regelhaft nicht vorweisen können, was einen bußgeldbewehrten Verstoß nach Art. 83 Abs. 5 DS-GVO[36] darstellt, welcher mit Geldbußen von bis zu 20 Millionen Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden kann.

Zu Ziffer 13.3.1

> 13.3.1 Soweit sich nach der Verfügbarmachung gemäß Ziffer 13.1 an den dort genannten Gegenständen und/oder an den gespeicherten Daten Änderungen oder Ergänzungen ergeben haben, sind diese auf Anforderung des Auftraggebers erneut zur Verfügung zu stellen, soweit sie nicht rechtmäßig gelöscht wurden.

Sollte der in Ziffer 13.3.1 genannte Zeitpunkt sich nach Vertragsende befinden (die Möglichkeit wird in Ziffer 13.3.3 genannt), so ist zu beachten, dass der Auftragnehmer nach Vertragsende nicht mehr als Auftragsverarbeiter für den Auftragnehmer tätig ist. Zumindest personenbezogene Daten muss der Auftragnehmer mit Vertragsende löschen, wenn der Auftragsnehmer keine eigene Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten des Auftragnehmers nach Vertragsende besitzt.

Zeichnen sich im Rahmen der Migration entsprechende Konstellationen ab, sollten sich Auftraggeber und Auftragnehmer überlegen, ob während der Vertragslaufzeit über eine vertragliche Ergänzung bzgl. Migrationsprozess nachgedacht wird, der dem Auftragnehmer eine rechtskonforme Speicherung der Daten des Auftraggebers bis zum erfolgreichen Ende des Migrationsprozesses erlaubt.

[35] Artikel 28 Datenschutz-Grundverordnung „Auftragsverarbeiter“. Online, zuletzt abgerufen 2023-08-23 unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679#d1e3162-1-1

[36] Artikel 83 Datenschutz-Grundverordnung „Allgemeine Bedingungen für die Verhängung von Geldbußen“. Online, zuletzt abgerufen 2023-08-23 unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679#d1e6235-1-1

Abschnitt „15 Unterauftragnehmer“

Zu Ziffer 15.1

> 15.1 Der Auftragnehmer darf zur Leistungserbringung Unterauftragnehmer nur einsetzen oder eingesetzte Unterauftragnehmer nur auswechseln, wenn der Auftragnehmer den bzw. die Unterauftragnehmer und deren jeweiligen Leistungsbereich (Art und Umfang der Auslagerung an den Unterauftragnehmer) benennt. Die Benennung kann entfallen, wenn es sich nur um Zulieferer oder solche Unternehmen handelt, deren Leistung keine vereinbarten C5-Kriterien betreffen und die nicht in die Erbringung der Leistungen eingebunden sind oder lediglich Nebenleistungen erbringen.

Nach Ziffer 15.1 kann ein Auftragnehmer ohne vorherige Zustimmung des Auftraggebers Unterauftragnehmer einsetzen, wenn die Leistung des Unterauftragnehmers „keine vereinbarten C5-Kriterien betreffen und die nicht in die Erbringung der Leistungen eingebunden sind oder lediglich Nebenleistungen erbringen“.

Hierbei ist zu beachten, dass bei der Verarbeitung personenbezogener Daten Art. 28 Abs. 2 S. 1 DS-GVO[37] ein Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch keinen weiteren Auftragsverarbeiter in Anspruch nehmen darf. Art. 28 Abs. 2 S. 2 DS-GVO verlangt ergänzend, dass im Fall einer allgemeinen schriftlichen Genehmigung der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

Im Kontext von Ziffer 15.1 muss zwingend beachtet werden, ob eingesetzte Unterauftragnehmer personenbezogene Daten verarbeiten oder potenziell bearbeiten könnten. Ist dies der Fall, muss der Auftraggeber zustimmen oder – im Falle einer allgemeinen schriftlichen Genehmigung zur Hinzuziehung von Unterauftragnehmern – die Möglichkeit zum Widerspruch erhalten.

Gerade im Kontext der Gesundheitsversorgung wird die Verarbeitung personenbezogener Daten die Regel sein, daher ist grundsätzlich Ziffer 15.3 auszuwählen. Dies kann nur im Vertrag unter Ziffer 8.4 geschehen. Hierbei ist allerdings zu beachten, dass im Vertrag fälschlicherweise auf Ziffer 15.2 statt Ziffer 15.3 verwiesen wird; eine Korrektur ist hier unumgänglich, wenn Ziffer 15.3 genutzt werden soll.

Zu Ziffer 15.3

> 15.3 Soweit vereinbart, gilt alternativ zu Ziffer 15.1, dass der Auftragnehmer zur Leistungserbringung Unterauftragnehmer nur einsetzen oder eingesetzte Unterauftragnehmer nur auswechseln darf, wenn der Auftragnehmer den bzw. die Unterauftragnehmer namentlich benennt und der Auftraggeber dem Einsatz ausdrücklich zustimmt. Voraussetzung für eine Zustimmung ist zunächst, dass sich der Unterauftragnehmer, soweit dies seine Leistungen betrifft, zuvor dem Auftragnehmer gegenüber mindestens in gleichem Umfang zur Einhaltung der vertraglichen Regelungen verpflichtet hat, wie der Auftragnehmer gegenüber dem Auftraggeber und der Auftragnehmer dies dem Auftraggeber auf Verlangen nachweist. Eine Zustimmung ist auch dann erforderlich, wenn der Auftragnehmer eine Leistung, die er bisher über einen Unteraufragnehmer erbringt, nunmehr selbst durchzuführen beabsichtigt. Der Auftraggeber wird zustimmen, wenn sich unter Berücksichtigung des neuen Unterauftragnehmers oder des Auftragnehmers anstelle des alten Unterauftragnehmers keine andere Zuschlagsentscheidung ergeben hätte und auch sonst kein sachlicher Grund dem Einsatz des Unterauftragnehmers entgegensteht. Die Einarbeitung des neuen Unterauftragnehmers erfolgt auf Kosten des Auftragnehmers. Für die im Angebot des Auftragnehmers oder sonst im Vergabeverfahren benannten Unterauftragnehmer gilt die Zustimmung des Auftraggebers als erteilt.

[37] Artikel 28 Datenschutz-Grundverordnung „Auftragsverarbeiter“. Online, zuletzt abgerufen 2023-08-23 unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679#d1e3162-1-1

Ziffer 15.3 enthält eine Art. 28 Abs. 2 DS-GVO entsprechende Regelung, sodass ausschließlich diese Ziffer bzgl. Einsatz Unterauftragnehmer genutzt werden darf, wenn (auch) personenbezogene Daten verarbeitet werden.

Hier ist allerdings zu beachten, dass im Vertrag fälschlicherweise auf Ziffer 15.2 statt Ziffer 15.3 verwiesen wird; eine Korrektur ist hier unumgänglich, wenn Ziffer 15.3 genutzt werden soll.

Abschnitt „17 Mitwirkung des Auftraggebers“

Im EVB-IT Cloud werden Auftraggeber und Auftragnehmer eigene Verantwortlichkeiten zugeteilt, daher wird auch von einer „Shared Responsibility“ gesprochen. Aufgrund dieser geteilten Verantwortlichkeiten bei der Nutzung von Cloud-Leistungen spielen die Mitwirkungspflichten des Auftraggebers, die in Ziffer 17 beschrieben werden, bei den EVB-IT Cloud für den Auftragnehmer eine besondere Rolle.

Es handelt sich bei den Mitwirkungspflichten des Auftraggebers jedoch lediglich um Obliegenheiten, nicht um Rechtspflichten. Somit können diese Mitwirkungspflichten des Auftraggebers rechtlich nicht eingefordert werden, aber die Nichterfüllung dieser Mitwirkungspflichten können für den Auftraggeber Nachteile beinhalten.

> Beispiel: Führt eine Verletzung von Obliegenheitspflichten des Auftraggebers (beispielsweise Remotezugang ist durch einen Fehler des Auftraggebers entgegen der in Ziff. 17.7 enthaltenen Vorgabe nicht möglich) zu Ausfallzeiten, so führt dies gem. Ziff. 8.3 der EVB-IT Cloud AGB nicht zu einer Minderung der Verfügbarkeit.

Zu Ziffer 17.2

> 17.2 Der Auftraggeber unterhält angemessene Sicherheitsstandards für die Nutzung der Leistungen durch seine Nutzer. Dem Auftraggeber obliegt es, die „Korrespondierenden Kriterien für Kunden“ aus dem jeweils für die vertragliche Leistung gemäß Ziffer 1.2 vereinbarten Stand des Anforderungskatalogs C5 des BSI zu beachten.

Entsprechend Ziffer 17.2 muss der Auftraggeber angemessene Sicherheitsstandards für die Nutzung der Leistungen durch seine Nutzer unterhalten. Insbesondere muss der Auftraggeber, die „Korrespondierenden Kriterien für Kunden“ aus dem Anforderungskatalog C5 des BSI zu beachten:

> Aus Kap. 2.1 BSI C5 Kriterienkatalog:
>
> „Für ausgewählte C5-Kriterien sind korrespondierende Kriterien für Kunden angegeben, die aufzeigen sollen, wo potenziell Mitwirkungspflichten bestehen. Es handelt sich dabei allerdings um keine abschließende und für alle Cloud-Dienste allgemein gültige Aufstellung.“

Dabei ist zu beachten, dass entsprechend BSI C5 Kriterienkatalog Cloud-Anbieter Kunden bei der Identifizierung jener C5-Kriterien unterstützen sollen, indem diese Kriterien bei der Erstellung der Systembeschreibung identifiziert und benannt werden.

Daher sollten sich Auftraggeber und Auftragnehmer intensiv mit den korrespondierenden Kriterien für Kunden des BSI C5-Katalogs auseinandersetzen.

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.).

Zu Ziffer 17.3

> 17.3 Der Auftraggeber ist dafür verantwortlich, dass die Systeme und Daten, die er dem Auftragnehmer im Zuge der Leistungserbringung zugänglich macht, auch durch den Auftragnehmer dafür betrieben bzw. verarbeitet werden dürfen.
>
> Im Rahmen der Auftragsverarbeitung prüft der Auftraggeber eigenverantwortlich, ob die von ihm im Zusammenhang mit der Nutzung der Leistung an den Auftragnehmer übermittelten Daten personenbezogene Daten darstellen und die Verarbeitung dieser personenbezogenen Daten im Wege der Auftragsverarbeitung zulässig ist.

Entsprechend Ziffer 17.3 ist der Auftraggeber dafür verantwortlich, dass die Systeme und Daten, die er dem Auftragnehmer im Zuge der Leistungserbringung zugänglich macht, auch durch den Auftragnehmer betrieben bzw. verarbeitet werden dürfen.

Somit ist allein der Auftraggeber für die Prüfung verantwortlich, ob Daten – insbesondere personenbezogene Daten – in eine Cloud ausgelagert werden dürfen und welche rechtlichen Anforderungen, z. B. bzgl. der geografischen Lokalisierung der Verarbeitung (z. B. nur Deutschland oder auch EU/EWR oder sogar Drittstaaten), dabei zu beachten sind. Hierbei ist zu beachten, dass der Begriff der „Verarbeitung“ in Art. 4 Ziff. 2 DS-GVO sehr weit gefasst ist. So umfasst die Verarbeitung grundsätzlich auch eine Fernwartung. Greifen also im Rahmen einer Fernwartung Beschäftigte eines Auftragnehmers aus Indies oder den USA auf in Europa gespeicherte Daten zu, erfolgt eine Verarbeitung in diesem Drittland, in sich die vom Auftragnehmer beschäftigte Person aufhält.

Im Zuge der Verarbeitung von Patientendaten sind in Deutschland diverse Rahmenbedingungen zu beachten:

- Sozialdaten: Sozialgeheimnis muss entsprechend § 35 Abs. 6 SGB I beachtet werden, desgleichen Vorgaben zur Auftragsverarbeitung in § 80 SGB X
- Bundesrechtliche Vorgaben, wie z. B.
    - § 75b SGB bzgl. der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung bzw. korrespondierend
    - § 85c SGB V hinsichtlich der IT-Sicherheit in Krankenhäusern
    - oder auch das in § 203 StGB verankerte Offenbarungsverbot verbunden mit dem in § 203 Abs. 4 StGB verankerten Verpflichtungsgebot für Auftragsverarbeiter
- Landesrechtliche Vorgaben, wie z. B. Landeskrankenhausgesetze oder Berufsordnungen für Ärzte/Apotheker
- Usw.

Hier ist also eine entsprechende Prüfung durch den Auftraggeber im Vorfeld der Auftragsvergabe unerlässlich.

Desgleichen verlangt Art. 28 Abs. 1 DS-GVO eine Prüfung sowohl vor Auftragsvergabe als auch während der Auftragsverarbeitung, ob der Auftragsverarbeiter „hinreichende Garantien“ im Sinne der DS-GVO bietet; falls nicht, darf der Auftragsverarbeiter keine personenbezogenen Daten des Verantwortlichen verarbeiten.

Zu Ziffer 17.9

> 17.9 Der Auftraggeber ergreift wirtschaftlich angemessene Maßnahmen, um einen nicht autorisierten Zugrif bzw. eine nicht autorisierte Nutzung über die ihm zur Verfügung gestellten Zugänge zu verhindern ode zu beenden.
>
> Unbenommen ist die Pflicht des Auftragnehmers, angemessene Maßnahmen zu treffen, die Leistung und die Zugänge dazu vor nicht autorisiertem Zugriff zu schützen. Der Auftraggeber haftet nicht fü unautorisierten Zugriff, wenn dieser durch eine solche Maßnahme des Auftragnehmers hätte verhinder werden können.

Entsprechend Ziff. 17.9 haftet der Auftraggeber nicht für einen unautorisierten Zugriff auf Daten, wenn dieser unautorisierte Zugriff durch eine solche Maßnahme des Auftragnehmers hätte verhindert werden können.

Kommt es in diesen Fällen (= unautorisierter Zugriff durch Beschäftigte des Auftragnehmers) zu einer Datenpanne und folgen Schadensersatzklagen oder Sanktionen wie ein Bußgeld durch Datenschutz-Aufsichtsbehörden, so haftet im Innenverhältnis der (für die Tat allein verantwortliche) Auftragnehmer gegenüber dem Auftraggeber.

Hierbei sind die in Ziff. 19 EVB-IT AGB beschriebenen Haftungsbeschränkungen zu beachten.

Abschnitt „18 Rechte des Auftraggebers bei Mängeln der Leistungen“

> **18 Rechte des Auftraggebers bei Mängeln der Leistungen**
>
> Der Auftragnehmer hat dem Auftraggeber die vereinbarte Leistung während der Vertragslaufzeit vertragsgemäß zur Verfügung zu stellen. Für die Zeit, in der die Nutzbarkeit der Leistung wegen eines Mangels oder einer Schlechtleistung gemindert ist, hat der Auftraggeber nur eine angemessen herabgesetzte Vergütung für die Leistung zu entrichten, soweit für diese Schlechtleistung nicht eine andere Kompensation (wie Nichterfüllungsgutschriften) vereinbart ist.
>
> Die sonstigen gesetzlichen Ansprüche des Auftraggebers wegen Mängeln oder Schlechtleistung bleiben unberührt.

Entsprechend Ziffer 18 muss die Nutzbarkeit der Cloud-Leistung wegen eines Mangels oder einer Schlechtleistung gemindert sein, damit der Auftraggeber die vereinbarte Vergütung für die Leistung herabsetzen kann oder bei fortdauernder Mangelhaftigkeit ggf. auch den Vertrag kündigen kann (siehe Ziffer 20).

Bei Cloud-Dienstleistungen wird i. d. R. die (Public-/Hybrid-) Cloud-Leistung gemietet, nicht gekauft. Entsprechend § 536a Abs. 1 BGB[38] haftet ein Vermieter (= Auftragnehmer) verschuldensunabhängig für Mängel an der Mietsache vor ihrer Überlassung und verschuldensabhängig für spätere Mängel. Gemäß § 536 Abs. 1,2 BGB erfordern Mängelansprüche

- entweder einen Mangel am Mietgegenstand, welcher die Tauglichkeit zum vertragsgemäßen Gebrauch des Mietgegenstand (= Cloud-Leistung) aufhebt (§ 536 Abs. 1 BGB),
- oder das Fehlen zugesicherter Eigenschaften (§ 536 Abs. 2 BGB).

Weiterhin kann der Auftragnehmer aufgrund bestehender Mängel Ansprüche

- auf die Wiederherstellung der vertragsgemäßen Gebrauchstauglichkeit (§ 535 Abs. 1 BGB),
- auf Schadensersatz
- sowie auf Aufwendungsersatz gemäß § 536a BGB

gegenüber dem Auftragnehmer erheben.

[38] § 536a BGB „Schadens- und Aufwendungsersatzanspruch des Mieters wegen eines Mangels“. Online, zuletzt abgerufen 2023-08-23 unter https://www.gesetze-im-internet.de/bgb/__536a.html

Abschnitt „19 Haftungsbeschränkung“

Die Haftungsregelungen bei den EVB-IT Cloud finden sich in Ziffer 19 der EVB-IT Cloud AGB, ergänzende bzw. abweichende Bedingungen können im Vertrag unter der Ziffer 6 getroffen werden.

Zu Ziffer 19.1

> 19.1 Bei leicht fahrlässigen Pflichtverletzungen wird die Haftung für den Vertrag insgesamt grundsätzlich auf den Auftragswert* beschränkt. Die Haftung in diesem Fall beträgt jedoch mindestens das Doppelte und maximal das Vierfache der Vergütung, die für das erste Vertragsjahr zu zahlen ist. Beträgt der Auftragswert* weniger als 50.000,- Euro wird die Haftung auf 50.000,- Euro beschränkt. Im Falle von Sachschäden ist die Haftung auf eine Million Euro beschränkt, wenn der Auftragswert* geringer als eine Million Euro ist.

In Ziffer 19.1 der EVB-IT Cloud AGB finden sich jedoch weitere Regelungen bzgl. der Haftungshöhe, die sich im Gegensatz zu allen anderen EVB-IT z. B. auch an der Laufzeit orientieren und im ersten Vertragsjahr andere Haftungssummen vorsehen als in der restlichen Laufzeit.

Zu Ziffer 19.2

> 19.2 Soweit nicht anders vereinbart, sind Ansprüche aus entgangenem Gewinn ausgeschlossen.

Entsprechend Ziff. 19.2 sind Ansprüche aus entgangenem Gewinn ausgeschlossen. Auftraggeber der öffentlichen Hand sind im Regelfall nicht auf Gewinnerzielung ausgerichtet, Auftraggeber der Privatwirtschaft hingegen schon. Dementsprechend muss geprüft werden, ob die Klausel für einen privaten Auftraggeber so genutzt werden kann oder ob eine Anpassung erforderlich ist.

Wird z. B. ein Praxisinformationssystem oder ein Krankenhausinformationssystem in die Cloud ausgelagert und ein Ausfall verhindert eine Patientenbehandlung bzw. die Dokumentation und Abrechnung dieser Leistungen über einen gewissen Zeitraum, können entsprechende Verluste für eine Arztpraxis oder ein (privates) Krankenhaus existenzbedrohend sein. Hier wird seitens Auftraggeber ggf. Anpassungsbedarf an dieser Klausel bestehen.

Abschnitt „20 Laufzeit und Kündigung“

Zu Ziffer 20.2

> 20.2 Zudem kann der Vertrag von jedem Vertragsteil bei Vorliegen eines wichtigen Grundes - ohne Einhaltung einer Kündigungsfrist - innerhalb einer angemessenen Zeit ab Kenntnis des Kündigungsgrundes ganz oder teilweise gekündigt werden. Ein wichtiger Grund liegt vor, wenn Tatsachen gegeben sind, aufgrund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalles und unter Abwägung der Interessen der Vertragspartner die Fortsetzung des Vertrages nicht mehr zugemutet werden kann. Besteht der wichtige Grund in der Verletzung einer vertraglichen Pflicht, ist die Kündigung erst nach erfolglosem Ablauf einer zur Abhilfe gesetzten Frist oder nach erfolgloser Abmahnung zulässig, soweit nicht gemäß § 314 i.V.m. § 323 Absatz 2 BGB eine Fristsetzung entbehrlich ist. Im Falle der Kündigung aus wichtigem Grund hat der Auftragnehmer Anspruch auf Vergütung für die bis zum Wirksamwerden der Kündigung aufgrund des Vertrages erbrachten Leistungen. Die Vergütung entfällt aber für solche Leistungen, für die der Auftraggeber darlegt, dass sie für ihn aufgrund der Kündigung ohne Interesse sind.

Die Kündigung aus wichtigem Grund ist gesetzlich in § 648a BGB[39] geregelt, dabei wird der Rechtsbegriff „wichtiger Grund“ in § 648a BGB nicht näher konkretisiert. § 648a Abs. 1 S. 2 BGB enthält nur eine generalklauselartige Umschreibung dieses Begriffs, welche sich an die Formulierung in § 314 Abs. 1 S. 2 BGB[40] anlehnt. § 648a Abs. 1 S. 2 BGB:

> „Ein wichtiger Grund liegt vor, wenn dem kündigenden Teil unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses bis zur Fertigstellung des Werks nicht zugemutet werden kann.“

Diese Formulierung wird nahezu wortgleich in Klausel 20.2 wiederholt.

Bei einem „wichtigen Grund“ muss es sich dementsprechend um eine schwerwiegende Vertragsstörung handeln. Eine entsprechend schwerwiegende Vertragsstörung kann auf einer einzelnen schwerwiegenden Vertragsverletzung beruhen, aber sich auch aus der Kumulation mehrerer Pflichtverletzungen, welche für sich genommen vielleicht nicht zur außerordentlichen Kündigung ausreichen würden, resultieren.

Entsprechend der Kommentarliteratur kann ein entsprechender „wichtiger Grund“ beispielsweise vorliegen[41],

- wenn nachhaltig gegen Vertragspflichten verstoßen wird,
- wenn der Dienstleister die Arbeiten grundlos einstellt oder die Erfüllung des Vertrages unberechtigt und endgültig verweigert,
- wenn der Dienstleister unsubstantiierte Mehrforderungen stellt,
- „wenn eine Vertragspartei, sei es der Unternehmer oder der Besteller, das für die Durchführung des Vertrages erforderliche Vertrauensverhältnis massiv erschüttert und damit den Vertragszweck erheblich und auf Dauer gefährdet“[41]
- oder bei einem groben Vertrauensbruch vorliegen.

Letzterer kann z. B. in einem entsprechenden Sicherheitsvorfall begründet liegen, wenn durch Missachtung vertraglicher Zusicherungen die IT-Sicherheit durch den Dienstleister gefährdet und

---

[39] § 648a BGB „Kündigung aus wichtigem Grund“. Online, zuletzt abgerufen 2023-08-23 unter https://www.gesetze-im-internet.de/bgb/__648a.html

[40] § 314 BGB „Kündigung von Dauerschuldverhältnissen aus wichtigem Grund“. Online, zuletzt abgerufen 2023-08-23 unter https://www.gesetze-im-internet.de/bgb/__314.html

[41] Busche J.: § 648a BGB, Rn. 3. In: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6. Verlag C. H. Beck, 9. Auflage 2023. ISBN 978-3-406-76670-1

hierdurch Dritte möglicherweise Zugriff auf Daten des Auftraggebers hätten erhalten können oder sogar erhielten.

Ein wichtiger Grund zur Kündigung des Vertragsverhältnisses durch den Dienstleister kann beispielsweise vorliegen, wenn der Auftraggeber erforderliche Mitwirkungshandlungen nachdrücklich verweigert oder Geschäftsgeheimnisse (siehe auch Ziffer 6.3.1) des Auftragnehmers ohne dessen Wissen an Dritte wie beispielsweise Konkurrenten weitergibt. Im letzteren Fall muss dem Auftraggeber der Tatbestand, dass es sich um Geschäftsgeheimnisse des Auftragnehmers handelt, bekannt sein.

Zu beachten ist, dass grundsätzlich eine Betrachtung des Einzelfalls und einer Abwägung der sich daraus ergebenden beiderseitigen Interessen erforderlich ist.

Abschnitt „21 Haftpflichtversicherung“

Eine „marktübliche Industriehaftpflichtversicherung“ wird regelhaft keine Cyberversicherung beinhalten. Ein Vorfall bei dem Cloud-Dienstleister CloudNordic[42] zeigt, dass Daten von Kunden in der Cloud nicht zwangsläufig sicher sind. Ein Verlust aller Kundendaten wird die Haftungshöhe einer Versicherung wahrscheinlich übersteigen.

Somit wird die Deckung einer marktüblichen Industriehaftpflichtversicherung ggf. den Verlust des Auftraggebers nicht abdecken. Es kann – je nach Sensibilität und Wert der Daten – daher ratsam sein, zumindest ein Backup der Daten abseits der Cloud zu besitzen.

[42] Bericht zum Vorfall z.B. verfügbar bei

- Heise online: Ransomware-Angriff: Alle Daten bei CloudNordic futsch. Bericht vom 2023-08-23. Online, zuletzt abgerufen 2023-08-23 unter https://www.heise.de/news/Ransomware-Angriff-Alle-Daten-bei-CloudNordic-futsch-9282877.html
- Securityweek: Hosting Provider CloudNordic Loses All Customer Data in Ransomware Attack. Bericht vom 2023-08-24. Online, zuletzt abgerufen 2023-08-23 unter https://www.securityweek.com/hosting-provider-cloudnordic-loses-all-customer-data-in-ransomware-attack/

Abschnitt „23 Textform“

23 Textform

Soweit nichts anderes geregelt ist, bedürfen vertragliche Mitteilungen und Erklärungen mindestens der Textform. Auch Eintragungen in der Administrationskonsole* entsprechen der Textform. Für Störungsmeldungen und Mängelrügen ist der Eintrag in ein Ticketsystem ausreichend.

Die Textform ist im § 126b BGB wie folgt definiert:

> „Ist durch Gesetz Textform vorgeschrieben, so muss eine lesbare Erklärung, in der die Person des Erklärenden genannt ist, auf einem dauerhaften Datenträger abgegeben werden. Ein dauerhafter Datenträger ist jedes Medium, das
>
> 1. es dem Empfänger ermöglicht, eine auf dem Datenträger befindliche, an ihn persönlich gerichtete Erklärung so aufzubewahren oder zu speichern, dass sie ihm während eines für ihren Zweck angemessenen Zeitraums zugänglich ist, und
> 2. geeignet ist, die Erklärung unverändert wiederzugeben.“

Somit genügt den Anforderungen an die Textform beispielsweise eine E-Mail oder ein Scan eines Dokumentes ebenso wie ein konventionelles Dokument in Papierform.

Abschnitt „24 Anwendbares Recht, Gerichtsstand“

Zu Ziffer 24.1

> 24.1 Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss der Normen, die in eine andere Rechtsordnung verweisen, und unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG).

Ziffer 24.1 enthält die Regelung, dass bei Normen, die in eine andere Rechtsordnung verweisen, dass Recht der Bundesrepublik Deutschland nicht anwendbar sein muss.

Eine „Norm“ ist dabei nicht zwingend eine gesetzliche Regelung. Auch vertragliche Regelungen können den Charakter einer Norm aufweisen.

So könnte beispielsweise auch Ziffer 6.1.1, nach welcher die Vertragspartner die jeweils auf sie anwendbaren Bestimmungen über den Datenschutz in der jeweils geltenden Fassung anzuwenden haben, als entsprechende Norm aufgefasst werden.

Abschnitt „Begriffsbestimmungen“

Zu Verfügbarkeitsklassen

Verfügbarkeitsklassen	Klassifizierung der Verfügbarkeit gemäß HV Kompendium des BSI Band G, Kapitel 2 in der zum Zeitpunkt des Vertragsschlusses aktuellen Version.

In der Begriffsbestimmung wird einerseits auf das HV Kompendium des BSI Band G, Kapitel 2 verwiesen, andererseits konkrete Angaben zur Verfügbarkeit vereinbart. Im Zweifelsfall wird man die in der Tabelle angegeben Werte als vertraglich bindend ansehen müssen.

Zu beachten ist, dass die unter 8.3 angegebenen Bedingungen die Verfügbarkeit trotz evtl. nicht vorhandener Nutzbarkeit der Leistung beeinträchtigen.

Die prozentuale Verfügbarkeit errechnet sich nur aus dem Zeitraum, in dem die Leistungen vertragsgemäß hätten verfügbar sein müssen. Wenn beispielsweise der Auftragnehmer wirklich jeden Sonntag zwischen 4:00 und 8:00 Uhr eine Wartung durchführt und die vertraglich vereinbarte Leistung nicht zur Verfügung steht, dann kann immer noch eine 100%ige Verfügbarkeit gegeben sein, wenn ansonsten keine Ausfälle auftreten, welche die Verfügbarkeit beeinträchtigen.

Abkürzungen

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BHO	Bundeshaushaltsordnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
C5	Cloud Computing Compliance Criteria Catalogue
CIO	Chief Information Officer
DIN	Deutsche Institut für Normung e. V.
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)
EN	Europäische Norm
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EVB	Ergänzende Vertragsbedingungen
EWR	Europäische Wirtschaftsraum
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
HGrG	Gesetz über die Grundsätze des Haushaltsrechts des Bundes und der Länder
Hs.	Halbsatz
IaaS	Infrastructure as a Service
IEC	Internationale Elektrotechnische Kommission (International Electrotechnical Commission
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
IT	Informationstechnik, informationstechnisches…
Kap.	Kapitel
lit.	littera (lat. „Buchstabe“)
MCS	Managed Cloud Services
Nr.	Nummer
PaaS	Platform as a Service
RL	Richtlinie
Rn.	Randnummer
S.	Satz
SaaS	Software-as-a-Service
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
SÜG	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen
Urt.	Urteil
vgl.	vergleiche
VO	Verordnung
Ziff.	Ziffer