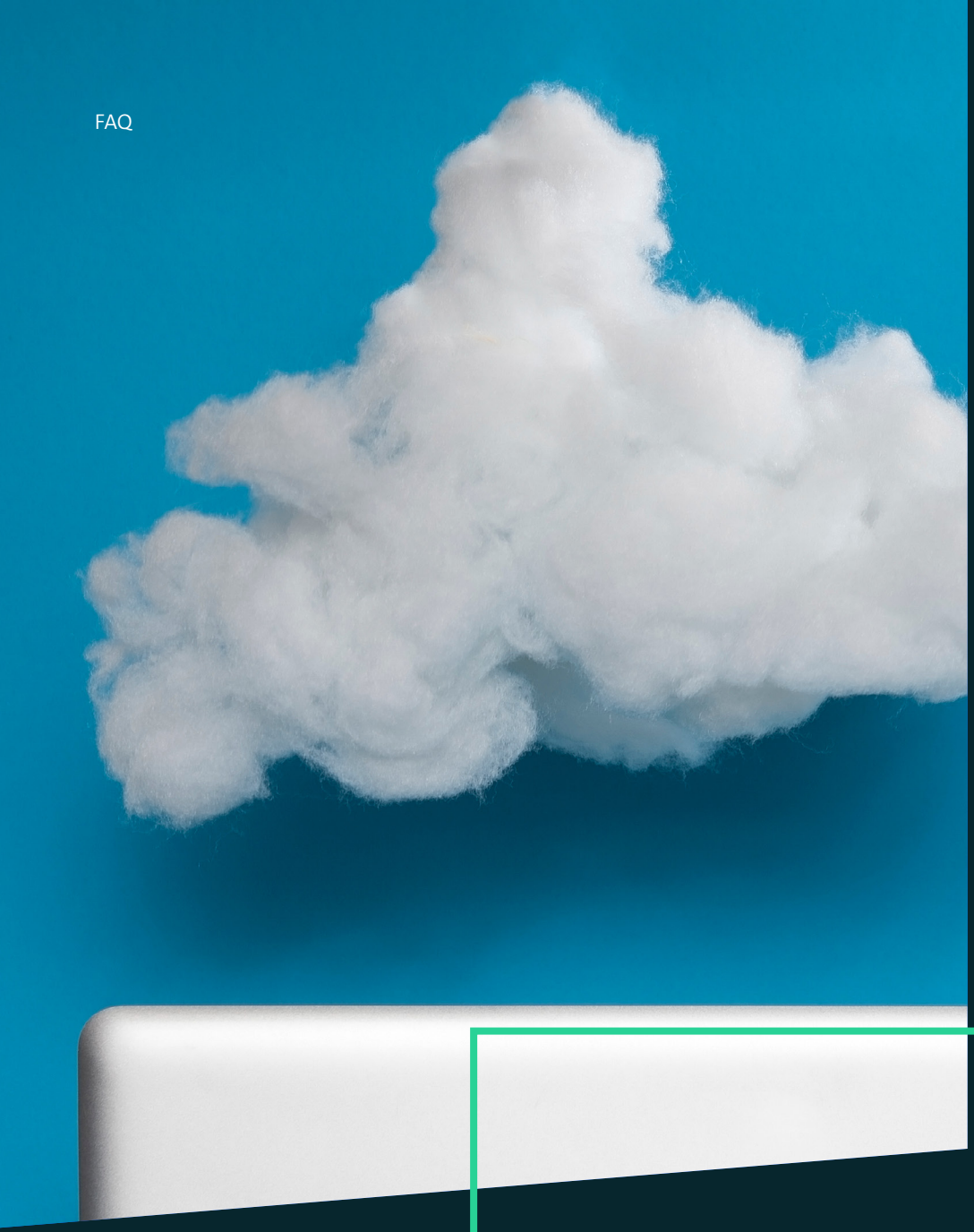
FAQ

bitkom



Frequently Asked Questions zu den EVB-IT Cloud

Herausgeber

Bitkom e. V.
Albrechtstraße 10
10117 Berlin
Tel.: 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Autoren

Marc Danneberg | Bitkom
Thomas H. Fischer (ab 1.7.2022 Arnecke Sibeth Dabelstein) | Waldeck
Claudius Grupp | Sopra Steria

Satz & Layout

Katrin Krause | Bitkom

In diesen FAQ werden Fragen zu den EVB-IT Cloud zusammenfassend erläutert. Es handelt sich hierbei nicht um eine vollständige Kommentierung, insbesondere können die FAQ nicht die eigene rechtliche Prüfung der einschlägigen Regelungen in den EVB-IT Dokumenten ersetzen.

Stand 25.04.2022

Abkürzungen

AGB

Ergänzende Vertragsbedingungen für Cloudleistungen (EVB-IT Cloud AG)

Cloudvertrag

Vertrag über die Cloudleistungen (EVB-IT Cloudvertrag)

Kriterienkatalog

Anlage Kriterienkatalog für Cloudleistungen zum EVB-IT Cloudvertrag

1 Gegenstand der EVB-IT Cloud

1.1 Welche Leistungen werden erfasst?

Es werden alle Cloud-Services erfasst, das heißt

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- Managed Cloud Services (MCS)
- Leistungen bei Vertragsende

Die einzelnen Services sind in den AGB auf den Seiten 18 ff. unter **Begriffsbestimmungen** definiert. Wie immer bei den EVB-IT weist ein * am Wortende auf eine Begriffsbestimmung in den AGB hin.

Zusätzlich sehen die EVB-IT Cloud die Vereinbarung besonderer initialer Leistungen (Nr. 3.2.1 Cloud-Vertrag) sowie Leistungen bei Vertragsende (Nr. 3.2.3 Cloud-Vertrag) vor. Derartige Leistungen können den eigentlichen SaaS, PaaS oder IaaS Service vor- bzw. nachgelagert oder aber Teil des MCS Services sein.

Zum Überblick über die vereinbarten Leistungen sieht Nr. 2 des Cloud-Vertrages Auswahlfelder vor. Die MCS-Leistungen können in Nr. 2 des Kriterienkatalogs weiter spezifiziert werden.

1.2 Worin besteht der Unterschied zwischen Public Cloud und Private Cloud?

Bei Public Cloud werden die Ressourcen für eine Vielzahl nicht näher bestimmter Kunden bereitgestellt, während bei einer Private Cloud eine Cloudlösung speziell für einen Kunden angeboten wird. Es existieren aber auch verschiedene andere Modelle wie beispielsweise die Hybrid-Cloud. Die EVB-IT erfassen im Standard die Public Cloud. Nr. 1 des Kriterienkatalogs sieht für alle weiteren Cloud-Modelle den Verweis auf eine Anlage vor, um näher zu bestimmen, welcher Typus von Cloud Gegenstand des Vertrages ist.

1.3 Wird ein bestimmter Vertragstypus (bspw. der Mietvertrag) den EVB-IT zugrunde gelegt?

Auf die Festlegung auf einen bestimmten Vertragstypus wurde bewusst verzichtet. Zwar scheint der Mietvertrag hier naheliegend, jedoch ist zu beachten, dass Miete im Sinne von § 535 Abs. 1 BGB den Gebrauch einer Mietsache zum Gegenstand hat. Bei Cloud Services wird hingegen regelmäßig ein bestimmter Service bereitgestellt.

1.4 Inwieweit wird die im Cloud Umfeld notwendige »geteilte Verantwortlichkeit« zwischen Auftraggeber und Auftragnehmer berücksichtigt?

Die verschiedenen Service-Modelle verlangen ein unterschiedlich hohes Maß an Mitwirkung auf Seiten des Auftraggebers (Shared Responsibility). Da für alle Cloud Services die Verpflichtung zur Einhaltung der C5 Basiskriterien gilt (Ziff. 1.2 AGB, siehe auch FAQ Ziff. 3 BSI Anforderungskatalog C5), sind von Seiten des Auftraggebers auch die sogenannten »Korrespondierenden Kriterien für Kunden« des C5 Anforderungskataloges zu beachten (Ziff.17.2 AGB). Die weiteren Mitwirkungsobliegenheiten des Auftraggebers ergeben sich aus Ziff. 17 AGB. Hierzu gehört beispielsweise das Ergreifen wirtschaftlich angemessener Maßnahmen, um einen nicht autorisierten Zugriff beziehungsweise eine nicht autorisierte Nutzung über die ihn zur Verfügung gestellten Zugänge zu verhindern oder zu beenden (Ziff. 17.9 AGB), oder auch die Verpflichtung zur Nutzung der bereitgestellten Administrationskonsole (Ziff. 17.8 AGB).

Die größte Bedeutung hat die Shared Responsibility bei IaaS. Hier ist klargestellt, dass der Zugang zur vereinbarten Cloud-Infrastruktur dem Auftraggeber zur eigenverantwortlichen Nutzung überlassen wird (Ziff. 2.3.2 AGB) und er die Verantwortung für die Einhaltung der vereinbarten Zugriffs- und Systemvoraussetzungen für die nicht vom Auftraggeber bereitgestellten Anwendungen / Inhalte hat (Ziff. 2.2.2 AGB). Aber auch bei PaaS erfolgte die Klarstellung, dass der Auftraggeber für die von ihm auf der Plattform betriebenen Anwendungen die Verantwortung trägt (Ziff. 2.1.1 Abs. 2 AGB).

Mitwirkungsleistungen können bei MCS aber auch auf den Auftragnehmer übertragen werden (Nr. 2 Kriterienkatalog).

1.5 Sind auch initiale Leistungen mit umfasst?

Initiale Leistungen sind diejenigen Leistungen, die vor der Nutzung der Services erforderlich sind (Setup). Sie können mit vereinbart werden (Nr. 3.2.1 Cloud-Vertrag) oder auch Gegenstand einer gesonderten Beauftragung sein, beispielsweise durch den Abschluss eines EVB-IT Dienstleistungsvertrages.

1.6 Was ist bei Nr. 2 des Vertragsmusters unter »Leistungen bei Vertragsende« zu verstehen?

Die Servicemodelle sehen regelmäßig im Standard keine Migrationsunterstützung zum Zeitpunkt des Vertragsendes vor. Daher sind diese Leistungen (siehe insbesondere Ziff. 13.2 AGB) bei Bedarf explizit im Cloud-Vertrag festzulegen. Wie bei den EVB-IT üblich, ist die Notwendigkeit einer expliziten Vereinbarung durch »soweit vereinbart« kenntlich gemacht.

1.7 Was sind »sonstige Leistungen« nach Nr. 2 des Vertragsmusters?

Die sonstigen Leistungen sind nicht näher bestimmt. Es wird auf eine Anlage verwiesen (Nr. 3.2.2.1 Cloud-Vertrag).

1.8 Wer stellt bei Managed Cloud Services (MCS) die Cloud-Infrastruktur?

Es sind zwei Varianten vorgesehen. Bei der Variante 1 erbringt der Auftragnehmer zusätzlich zu den MCS-Leistungen auch die IaaS-Leistung selbst oder durch einen Subunternehmer (Ziff. 2.3.2 AGB). Bei der Variante 2 ist der Auftragnehmer für die IaaS-Leistung selbst nicht verantwortlich, übernimmt aber gegebenenfalls die Integration und Steuerung des IaaS-Serviceanbieters (Ziff. 2.3.3 AGB).

1.9 Warum sieht der Kriterienkatalog bei MCS eine Ausfülloption vor, die sich auf Mitwirkungsleistungen des Auftraggebers bezieht (Nr. 2)?

Die MCS-Leistungen können auch die Übernahme von Leistungen erfassen, die im Standard zu den Mitwirkungsobliegenheiten des Auftraggebers nach Ziff. 17 AGB gehören.

1.10 Wie werden Leistungen einbezogen, bei denen es sich nicht um Cloud-Leistungen handelt?

Diese Leistungen können als sonstige Leistungen einbezogen werden (Nr. 2 i.V.m. Nr. 3.2.2 Cloud-Vertrag).

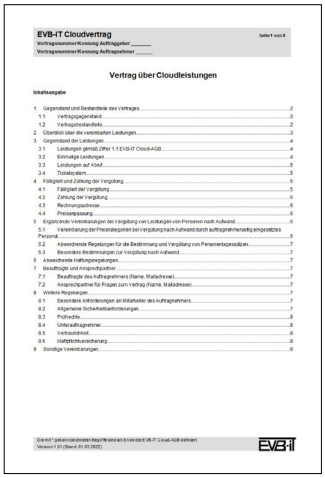
1.11 Inwieweit können die Leistungen während der Vertragslaufzeit durch den Auftragnehmer angepasst werden, beispielsweise wegen technischer Weiterentwicklungen?

Es gehört zu den wesentlichen Merkmalen von Cloud-Leistungen, dass sie stetig weiterentwickelt werden. Vorgesehen ist daher ein Recht zur Anpassung der Leistungen, um Funktionalitäten zu verbessern oder Leistungen dem Stand der Technik anzupassen (Ziff. 12 AGB). ABER:

- Funktionalitäten müssen erhalten bleiben;
- Vereinbarte Anforderungen dürfen nicht wesentlich eingeschränkt sein;
- Die Änderungen hätten nicht zu einer Schlechterbewertung im Vergabeverfahren führen dürfen.

2 Aufbau der EVB-IT

2.1 Welche Dokumente werden Teile des Vertrages?


EVB-IT Cloudvertrag

Vertragsnummer/Kennung Auftraggeber _____
Vertragsnummer/Kennung Auftragnehmer _____

Vertrag über Cloudleistungen

Inhaltsangabe

1 Gegenstand und Bestandteile des Vertrages ... 2
1.1 Vertragsgegenstand ... 2
1.2 Vertragsbestandteile ... 2
2 Überlick über die vereinbarten Leistungen ... 3
3 Gegenstand der Leistungen ... 4
3.1 Leistungen gemäß Ziffer 1.1 EVB-IT Cloud-AGB ... 4
3.2 Einmalige Leistungen ... 4
3.3 Leistungen auf Abruf ... 5
3.4 Teilabnahme ... 5
4 Fälligkeit und Zahlung der Vergütung ... 5
4.1 Fälligkeit der Vergütung ... 5
4.2 Zahlung der Vergütung ... 6
4.3 Rechnungsadresse ... 6
4.4 Preisanpassung ... 6
5 Ergänzende Vereinbarungen bei Vergütung von Leistungen von Personen nach Aufwand ... 6
5.1 Vereinbarung der Preisabgaben bei Vergütung nach Aufwand durch auftragnehmerseitig eingesetztes Personal ... 6
5.2 Abweichende Regelungen für die Bestimmung und Vergütung von Personentagessätzen ... 7
5.3 Besondere Bestimmungen zur Vergütung nach Aufwand ... 7
6 Abweichende Haftungsregelungen ... 7
7 Besuftragte und Ansprechpartner ... 7
7.1 Beauftragte des Auftragnehmers (Name, Mailadresse) ... 7
7.2 Ansprechpartner für Fragen zum Vertrag (Name, Mailadresse) ... 7
8 Weitere Regelungen ... 7
8.1 Besondere Anforderungen an Mitarbeiter des Auftragnehmers ... 7
8.2 Allgemeine Sicherheitsanforderungen ... 7
8.3 Prüfrechte ... 8
8.4 Unteraufträgnehmer ... 8
8.5 Verbraucherschutz ... 8
8.6 Haftpflichtversicherung ... 8
9 Sonstige Vereinbarungen ... 8

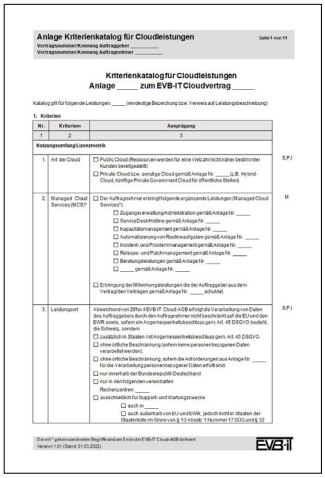
Die mit * gekennzeichneten Begriffe sind am Ende der EVB-IT Cloud-AGB definiert.
Version 1.01 (Stand: 01.03.2022)

EVB-IT

1. EVB-IT Cloudvertrag

Ranghöchstes Dokument

Durch Aufnahme als Anlage zu dem Cloudvertrag in die Tabelle Nr. 1.2.1 werden Dokumente Teil des Vertrages (beispielsweise Leistungsbeschreibung, Preisblatt, AVV, Angebot des Auftragnehmers).


Anlage Kriterienkatalog für Cloudleistungen

Vertragsnummer/Kennung Auftraggeber _____
Vertragsnummer/Kennung Auftragnehmer _____

Kriterienkatalog für Cloudleistungen
Anlage _____ zum EVB-IT Cloudvertrag _____

Katalog gilt für folgende Leistungen: _____ (eindeutige Bezeichnung bzw. Verweis auf Leistungsbeschreibung)

1. Kriterien

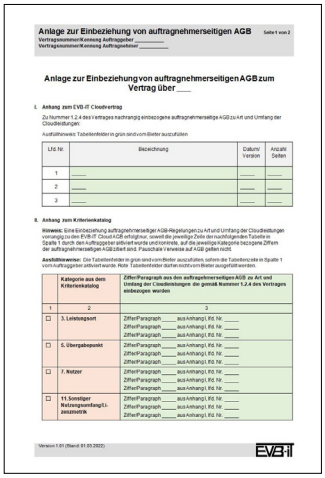
Nr.	Kriterium	Ausprägung	
1	2	3	
Nutzungsumfang/-Lizenzmetrik			
1.	Art der Cloud	☐ Public Cloud (Ressourcen werden für eine Vielzahl nicht näher bestimmter Kunden bereitgestellt) ☐ Private Cloud (bzw. sonstige Cloud gemäß Anlage Nr. _____ (z.B. Hybrid-Cloud, künftige Private-Government Cloud für öffentliche Stellen)	S,P,I
2.	Managed Cloud Services (MCS)*	☐ Der Auftragnehmer erbringt folgende ergänzende Leistungen (Managed Cloud Services*): ☐ Zugangsverwaltung/Administration gemäß Anlage Nr. _____ ☐ Service Desk/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.	M
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 BDG und § 30	S,P,I

Die mit * gekennzeichneten Begriffe sind am Ende der EVB-IT Cloud-AGB definiert.
Version 1.01 (Stand: 01.03.2022)

EVB-IT

2. Anlage Kriterienkatalog für Cloudleistungen

Kriterienkatalog, dient der Spezifizierung der Anforderungen an die konkrete Leistung. Bei unterschiedlichen Leistungen können auch mehrere Kriterienkataloge als Anlage zum Cloudvertrag genommen werden.


Anlage zur Einbeziehung von auftragnehmerseitigen AGB

Vertragsnummer/Kennung Auftraggeber _____
Vertragsnummer/Kennung Auftragnehmer _____

Anlage zur Einbeziehung von auftragnehmerseitigen AGB zum Vertrag über ___

I. Anhang zum EVB-IT Cloudvertrag

Zu Nummer 1.2.4 des Vertrages nachträglich einbezogene auftragnehmerseitige AGB zu Art und Umfang der Cloudleistungen

Ausfüllhinweis: Tabellenfelder in grün sind vom Bieter auszufüllen

Lfd. Nr.	Bezeichnung	Datum/ Version	Anzahl Seiten
1	_____	_____	_____
2	_____	_____	_____
3	_____	_____	_____

II. Anhang zum Kriterienkatalog

Hinweis: Eine Einbeziehung auftragnehmerseitiger AGB-Regelungen zu Art und Umfang der Cloudleistungen vorrangig zu den EVB-IT Cloud AGB erfolgt nur, soweit die jeweilige Zeile der nachfolgenden Tabelle in Spalte 1 durch den Auftraggeber aktiviert wurde und nominiert, auf die jeweilige Kategorie bezogene Ziffern der auftragnehmerseitigen AGB üblich sind. Pauschale Verweise auf AGB gelten nicht.

Ausfüllhinweise: Die Tabellenfelder in grün sind vom Bieter auszufüllen, sofern die Tabellenzeile in Spalte 1 vom Auftraggeber aktiviert wurde. Rote Tabellenfelder dürfen nicht vom Bieter ausgefüllt werden.

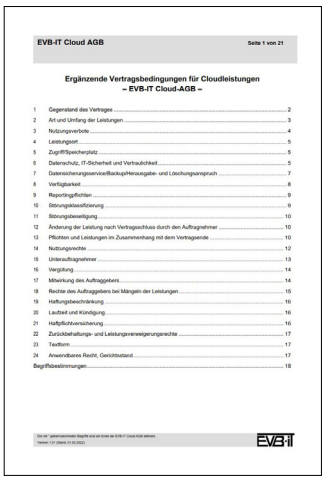
	Kategorie aus dem Kriterienkatalog	Ziffern/Paragraph aus den auftragnehmerseitigen AGB zu Art und Umfang der Cloudleistungen die gemäß Nummer 1.2.4 des Vertrages einbezogen wurden
1	2	3
☐	3. Leistungsort	Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____ Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____ Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____
☐	5. Übergabepunkt	Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____ Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____ Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____
☐	7. Nutzer	Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____ Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____ Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____
☐	11. Sonstiger Nutzungsumfang/-Lizenzmetrik	Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____ Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____ Ziffern/Paragraph _____ aus Anhang I, Bl. Nr. _____

Version 1.01 (Stand: 01.03.2022)

EVB-IT

3. Anlage zur Einbeziehung von auftragnehmerseitigen AGB

Anlage zum Kriterienkatalog. Die hier aufgeführten einzelnen Regelungen aus den auftragnehmerseitigen AGB gehen den EVB-IT Cloud AGB vor.



EVB-IT Cloud AGB Seite 1 von 21

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

Die mit * gekennzeichneten Begriffe sind am Ende der EVB-IT Cloud-AGB definiert.
Version 1.0? (Stand: 01.03.2022)

EVB-IT

4. EVB-IT Cloud AGB

5. Auftragnehmerseitige AGB Auftragnehmer

Durch den Cloudvertrag einbezogene auftragnehmerseitige AGB des Auftragnehmers selbst

6. Auftragnehmerseitige AGB Subunternehmer

Durch den Cloudvertrag einbezogene auftragnehmerseitige AGB des Subunternehmers des Auftragnehmers, beispielsweise eines Hyperscalers als Subunternehmer

Hinzu kommen weitere Dokumente wie die AVV, Preisblatt, das Angebot des Auftragnehmers, etc., jeweils in der Rangfolge eingeordnet, wie dies der Cloudvertrag in Nr. 1.2.1 vorsieht.

2.2 In welcher Rangfolge stehen die Inhalte der verschiedenen Dokumente zueinander?

Grundsätzlich stehen die Dokumente zueinander in der Reihenfolge wie zur Frage 2.1 aufgeführt. Ausgenommen von dieser Rangfolge sind Regelungen der auftragnehmerseitigen AGB, die in der Anlage auftragnehmerseitige AGB zum Kriterienkatalog aufgeführt sind (siehe hierzu Frage 4).

2.3 Wo werden Abweichungen zu den EVB-IT AGB vereinbart?

In jedem Dokument, das in der Rangfolge vor den EVB-IT AGB steht, können Abweichungen aber auch Ergänzungen aufgenommen werden. Vorgesehen sind entsprechende Optionen sowohl im Cloudvertrag als auch im Kriterienkatalog mit dessen Anhang zur Berücksichtigung auftragnehmerseitiger AGB. Der Kriterienkatalog ist insbesondere für leistungsbezogene Abweichungen und Ergänzungen gedacht. Hierin unterscheidet sich den EVB-IT Cloud von den bisherigen EVB-IT, die einen Kriterienkatalog nicht vorsehen, sondern vielmehr die Optionen im Vertragsmuster verorteten.

2.4 Inwieweit erfolgt die Ausfüllung der Dokumente durch den Auftragnehmer?

Der Auftraggeber kann im Rahmen des Vergabeverfahrens angeben, welche Angaben von dem Auftragnehmer selbst vorzunehmen sind (bspw. die Produktbezeichnungen in Nr. 3.1 Cloudvertrag oder die Bezeichnung der auftragnehmerseitigen AGB in Nr. 1.2.4 Cloudvertrag). Bereits vorgesehen sind Ausfüllfelder für Verweise auf die auftragnehmerseitigen AGB in der betreffenden Anlage zum Kriterienkatalog (siehe hierzu Frage 4).

2.5 Warum werden die VOL/B Vertragsbestandteil?

Nach § 29 Abs. 2 VGV / § 21 Abs. 2 UVgO ist die VOL/B in der Regel in den Vertrag einzubeziehen. Aufgrund des Detaillierungsgrades der aufgrund der Rangfolge vorgehenden Dokumente hat die VOL/B vorliegend aber keinen relevanten Regelungsgehalt.

3 BSI Anforderungskatalog C5

3.1 Was ist der BSI Anforderungskatalog C5?

Der Anforderungskatalog C5 (Cloud Computing Compliance Criteria Catalogue – C5:2020 | Kriterienkatalog Cloud Computing) wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben. Das BSI hat Sicherheitsziele definiert, aber offengelassen, wie diese erreicht werden. In einem Katalog von rund 125 Kriterien werden die Mindestanforderungen an sicheres Cloud Computing spezifiziert. Die aktuelle Version C5:2020 ist ↗hier abzurufen.

Der Anforderungskatalog C5 richtet sich sowohl an die Cloud-Anbieter, deren Prüfer, als auch an die Auftraggeber. Die Erfüllung der als Mindestanforderungen an die Informationssicherheit ausgestalteten Kriterien kann durch das Testat eines Wirtschaftsprüfers oder anderer geeigneter Prüfer nachgewiesen werden.

Der C5 Anforderungskatalog ist im Zusammenhang mit den Mindeststandards des BSI zur Nutzung externer Cloud-Dienste nach § 8 Abs. 1 Satz 1 BSIG von Bundesbehörden zu beachten. Diese Mindeststandards (Version 2.0 vom 7.7.2021) sind ↗hier abzurufen. Die einzelnen Anforderungen sind im Anforderungskatalog C5 jeweils untergliedert in

- Basiskriterium
- Zusatzkriterium
- Ergänzende Informationen

Der Auftragnehmer ist zur Einhaltung der Basiskriterien verpflichtet (Ziff. 1.2 AGB). Bei einem erhöhten Sicherheitsbedarf können die Zusatzkriterien ganz oder teilweise gefordert werden (Nr. 18 Kriterienkatalog).

3.2 Was sind die C5 Basiskriterien?

Basiskriterien sind für den Auftragnehmer verpflichtend und Grundlage der Testate. Zusatzkriterien müssen zusätzlich vereinbart werden.

3.3 Wie wirkt sich eine Anpassung des BSI Anforderungskatalog C5 auf laufende Vertragsbeziehungen aus?

Für den Fall der Erneuerung des Anforderungskataloges C5 (derzeitiger Stand C5:2020) ist eine Bemühungsregelung vorgesehen, die neu bzw. geänderten Anforderungen innerhalb angemessener Frist umzusetzen (Ziff. 1.2 Abs. 2 Satz 1 AGB). Es besteht allerdings keine zwingende Verpflichtung zur Umsetzung. Der Auftraggeber kann jedoch eine Bestätigung der Erfüllung anfordern. Bestätigt der Auftragnehmer dann nicht die Erfüllung der geänderten Kriterien, hat der Auftraggeber ein Sonderkündigungsrecht bezogen auf die betroffenen Leistungen (Ziff. 1.2 Abs. 2 Satz 2 AGB). Die Erklärung des Auftragnehmers muss innerhalb von 12 Monaten nach Veröffentlichung des Nachfolgedokuments erfolgen, sofern nicht vom Gesetzgeber eine kürzere Umsetzungsfrist vorgegeben ist.

3.4 Was ist der Unterschied zwischen einem Testat und einem Zertifikat?

Bei einem Testat wird der Auditor von dem Auditierten beauftragt und anschließend der Audit-Bericht zur Prüfung an die Zertifizierungsstelle geschickt. Entspricht der Bericht den Regularien, wird von der Zertifizierungsstelle das Zertifikat erteilt. Der Auditor erteilt das Testat. Ein »C5-Zertifikat« existiert bislang nicht.

3.5 Kann von dem Auftraggeber die Vorlage eines C5-Testats verlangt werden?

Nach § 33 Abs. 1 VgV können Bescheinigungen von einer Konformitätsbewertungsstelle eingefordert werden. Dies sind insbesondere Zertifizierungs- und Inspektionsstellen. An einer Zertifizierungsstelle fehlt es gerade bei einem Testat (siehe Antwort zu Frage 3.4). Die AGB verlangen auch nicht die Vorlage eines Testats, sondern vielmehr die Erfüllung der C5-Basiskriterien (Ziff.1.2 AGB). Auch wenn C5-Testate mittlerweile weit verbreitet sind (insbesondere bei den Anbietern von IaaS), liegen sie für einzelne Anwendungen oder Services zum Teil nicht oder noch nicht vor.

3.6 Warum wird der BSI »Kriterienkatalog C5« nicht als solcher, sondern als »Anforderungskatalog C5« bezeichnet?

Um eine Verwechslung mit der »Anlage Kriterienkatalog für Cloud-Leistungen« zu vermeiden, wird der Begriff des »Anforderungskatalogs« in den Dokumenten verwendet. Auch das BSI verwendet Kriterienkatalog und Anforderungskatalog synonym.

3.7 Müssen auf allen Cloud-Ebenen (SaaS, PaaS, IaaS) die C5-Kriterien erfüllt werden?

Ja, die C5-Anforderungen müssen auf allen Cloud-Ebenen erfüllt werden. Allerdings können bei einer Prüfung durch den Auditor bestehende Testate berücksichtigt werden. Bei der Prüfung eines SaaS muss daher beispielsweise keine eigene Prüfung bei dem Hyperscaler durchgeführt werden. Vielmehr genügt das Verlangen des C5-Testats durch den Hyperscaler.

3.8 Sind weitere Anforderungen an die IT-Sicherheit vorgesehen?

Der Auftragnehmer muss über ein angemessenes, dokumentiertes und implementiertes Sicherheitskonzept und ein Informationssicherheitsmanagementsystem gemäß ISO 27001 verfügen (Ziff. 6.2.1 AGB). Überdies hat der Auftragnehmer für die IT-Sicherheit im Rahmen seines Verantwortungsbereichs Sorge zu tragen (Ziff. 2.1.1 AGB für SaaS und PaaS, Ziff. 2.2.1 AGB für IaaS). Schließlich ist die modifizierte »technische No-Spy-Klausel« zu beachten (Ziff. 1.4 AGB).

3.9 Kann der Auftraggeber zusätzliche Anforderungen an die IT-Sicherheit stellen?

Es sind verschiedene Möglichkeiten vorgesehen, zusätzliche Anforderungen an die Sicherheit zu vereinbaren:

1. Vereinbarung aller oder bestimmter Zusatzkriterien des Anforderungskataloges C5 (Nr. 18 Kriterienkatalog)
2. Einbeziehung von Sicherheitsrichtlinien des Auftraggebers (Ziff. 1.2 Abs. 1 AGB)
3. Vereinbarung zusätzlicher Standards (Nr. 18 Kriterienkatalog)

3.10 Wie ist mit Abweichungen zu den C5-Basiskriterien umzugehen?

Da die AGB die ausnahmslose Erfüllung der C5-Basiskriterien vorsehen (Ziff. 1.2 Abs. 1 Satz 1 AGB), ist bei Abweichungen eine explizite Vereinbarung im Cloud-Vertrag oder eine entsprechende Antwort im Rahmen des Vergabeverfahrens auf eine Bieterfrage erforderlich.

3.11 Sind weitere BSI Dokumente (bspw. BSI IT-Grundschutz) oder ISO Normen einzubinden?

Als Standard ist dies nicht vorgesehen. Der Kriterienkatalog sieht jedoch entsprechende Optionen vor (Nr. 18 Kriterienkatalog).

4 Auftragnehmerseitige AGB

4.1 Was sind auftragnehmerseitige AGB?

Auftragnehmerseitige AGBs können sowohl die Allgemeinen Geschäftsbedingungen des Auftragnehmers selbst oder die eines Unterauftragnehmers oder Lieferanten des Auftragnehmers sein.

4.2 Inwieweit werden AGB der so genannten »Hyperscaler« eingebunden?

Ist der »Hyperscaler« Subunternehmer des Auftragnehmers, können dessen AGB ebenfalls als »auftragnehmerseitige AGB« (siehe Antwort Ziff. 4.1) eingebunden werden.

4.3 Wie können auftragnehmerseitige AGB eingebunden werden?

Es sind verschiedene Möglichkeiten zur Einbindung von auftragnehmerseitigen AGB vorgesehen:

Möglichkeit 1: Aufnahme 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 Ziff. I und dort Beifügung als Anhang.

4.4 Können die auftragnehmerseitigen AGB durch Verweis auf eine Website des Auftragnehmers eingebunden werden?

Dies ist nicht vorgesehen. Aus Gründen der Eindeutigkeit müssen die auftragnehmerseitigen AGB immer als Anlage bzw. Anhang (ggf. in elektronischer Form) dem Vertrag bzw. der Anlage zum Kriterienkatalog beigefügt werden.

4.5 Wie ist der Hinweis in der »Anlage zu den auftragnehmerseitigen AGBs« zu verstehen: »soweit die jeweilige Zeile der nachfolgenden Tabelle in Spalte 1 durch den Auftraggeber aktiviert wurde«?

Dem Bieter ist es nur erlaubt, eine Eintragung in der Spalte 3 mit einem Verweis auf die auftragnehmerseitigen AGB aufzunehmen, sofern in Spalte 1 das Auswahlfeld von dem Auftraggeber angekreuzt wurde.

4.6 Dürfen in der »Anlage zu den auftragnehmerseitigen AGB« in den einzelnen Zeilen der Spalte 3 mehrere Verweise / mehrere Ziffern der auftragnehmerseitigen AGB angegeben werden?

Nein, dies ist nicht möglich. »Ziffer / Paragraf« in der Spalte 3 ist wörtlich zu nehmen, d.h. es ist je Zeile nur eine Ziffer / ein Paragraf anzugeben, hingegen nicht mehrere Ziffern bzw. Paragrafen. Sollte die Anzahl der Zeilen nicht ausreichen, kann die Aufnahme weiterer Zeilen nicht durch den Bieter erfolgen. Der Bieter muss vielmehr durch eine Bieterfrage eine Ergänzung erbitten. Nur wenn der Auftraggeber dieser Bitte nachkommt, können weitere Ziffern angegeben werden. Dies gilt gleichermaßen für eine Ergänzung der Tabelle unter Ziff. 2 der Anlage zur Einbeziehung der auftragnehmerseitigen AGB um weitere Kategorien.

4.7 Welche Rangfolge besteht zwischen den auftragnehmerseitigen AGB und den EVB-IT Cloud AGB?

Die auftragnehmerseitigen AGB gelten grundsätzlich nachrangig zu den EVB-IT Cloud AGB (Nr. 1.2.4 Cloud-Vertrag). Über die Anlage zum Kriterienkatalog zur Einbeziehung von auftragnehmerseitigen AGB können jedoch einzelne Regelungen zu bestimmten Kategorien vorranging zu den EVB-IT Cloud AGB vereinbart werden (Ziff. II Anlage Kriterienkatalog).

4.8 Wie werden in den auftragnehmerseitigen AGB vorgesehene Nutzungsverbote einbezogen?

Eine vorrangige Einbeziehung von in den auftragnehmerseitigen AGB vorgesehenen Nutzungsverboten ist nicht vorgesehen. Jedoch wurden übliche Nutzungsverbote in den AGB aufgenommen. Neben Rechtsverletzungen (Ziff. 3.1 AGB) betreffen sie insbesondere die Verwendung der Leistungen im Hochrisikobereich (Ziff. 3.2 AGB). Ist der Gebrauch der Leistung aber gerade hierfür vorgesehen (beispielsweise für Flugsicherungssysteme), greift das Nutzungsverbot nicht.

Beim Verstoß gegen das Nutzungsverbot ist der Auftragnehmer – nach vorheriger Abmahnung – zur Aussetzung der betroffenen Leistungen berechtigt (Ziff. 3.3 AGB).

4.9 Können die auftragnehmerseitigen AGB innerhalb der Vertragslaufzeit angepasst werden?

Ein dynamischer Änderungsvorbehalt in den auftragnehmerseitigen AGB ist zulässig, soweit die Änderungen nicht zum Nachteil des Auftraggebers sind (Nr. 1.2.4 Cloud-Vertrag).

4.10 Werden auftragnehmerseitige AGB berücksichtigt, die nicht in den Dokumenten explizit aufgeführt sind?

Sind die auftragnehmerseitigen AGB nicht explizit aufgeführt, sind sie ausgeschlossen (Nr. 1.2.4 Cloud-Vertrag).

5 Administrationskonsole

5.1 Was ist unter einer Administrationskonsole zu verstehen?

Die Administrationskonsole dient der Verwaltung der Cloud-Services. Sie werden auch als Self-Services-Portale (SSP) bezeichnet.

5.2 Muss der Auftraggeber eine vom Auftragnehmer bereitgestellte Administrationskonsole nutzen?

Ja, der Auftraggeber muss die mit der Administrationskonsole bereitgestellten Funktionalitäten nutzen (Ziff. 2.1.5, 9.2, 17.8 AGB). Die Administrationskonsole dient gegebenenfalls auch für Störungsmeldungen (Ziff. 2.1.5, 9.2, 17.6 AGB) oder auch für die Entgegennahme von Mitteilungen (Ziff. 2.1.5, 9.2, 17.8, 23 AGB).

5.3 Wie wirken sich in der Administrationskonsole vom Auftraggeber vorgenommene Einstellungen auf die Leistungsbeziehungen aus? Können auch Leistungserweiterungen vorgesehen sein?

Einstellungen in der Administrationskonsole sind grundsätzlich rechtsverbindlich für die Festlegungen des Auftraggebers, so beispielsweise bei der Festlegung von Leistungsorten (Ziff. 4 AGB). Es können aber auch Leistungserweiterungen ausgelöst werden. Es ist Aufgabe des Auftraggebers durch eine Rechte- und Rollenstruktur Beauftragungen durch hierzu nicht Berechtigte zu verhindern (Ziff. 17.10 AGB).

6 Mitwirkung des Auftraggebers

6.1 Welche Mitwirkungsleistungen muss der Auftraggeber erbringen?

Die Mitwirkung des Auftraggebers ist in Ziff. 17 AGB geregelt. Als Folge der geteilten Verantwortlichkeiten bei der Nutzung von Cloud-Leistungen (»Shared Responsibility«) sind diese im Vergleich zu den übrigen EVB-IT umfangreicher ausgestaltet. Insbesondere muss auch der Auftraggeber angemessene Sicherheitsstandards für die Nutzung der Leistungen durch seine Nutzer gewährleisten und die »Korrespondierenden Kriterien für Kunden« aus dem Anforderungskatalog C5 beachten (Ziff. 17.2 AGB). Klargestellt ist weiterhin, dass der Auftraggeber für seinen Verantwortungsbereich auch eigenverantwortlich ist, so beispielsweise für die Zulässigkeit des Betriebs der von ihm eingebrachten Systeme bzw. die Verarbeitung der eingestellten Daten (Ziff. 17.3, 17.4 AGB, siehe zur Leistungsabgrenzung auch Ziff. 2.1.1 AGB für SaaS und PaaS sowie Ziff.2.2.2 AGB für IaaS). Zur Verpflichtung zur Nutzung der Administrationskonsole siehe auch Ziff. 5 FAQ.

6.2 Was sind die Rechtsfolgen, sollte der Auftraggeber Mitwirkungsleistungen nicht oder nicht vollständig erbringen?

Es handelt sich bei den Mitwirkungsleistungen um Obliegenheiten. Sie führen insbesondere dazu, dass hierdurch verursachte Ausfallzeiten nicht zu einer Minderung der Verfügbarkeit führen (Ziff. 8.3 AGB).

6.3 Wie können zusätzliche Mitwirkungsleistungen des Auftraggebers vereinbart werden?

Der Kriterienkatalog sieht die Möglichkeit vor, zusätzliche Mitwirkungsleistungen des Auftraggebers vorzusehen (Nr. 25 Kriterienkatalog).

7 Verfügbarkeit

7.1 Welche Anforderungen an die Verfügbarkeit sind im Standard vorgesehen?

Die Verfügbarkeit orientiert sich an typischen Verfügbarkeitsklassen im Rechenzentrumsbetrieb (siehe hierzu Begriffsbestimmungen AGB zu Verfügbarkeitsklassen). Der Standard ist VK1 (Ziff. 8.3 AGB).

7.2 Wie wird die Verfügbarkeit berechnet?

Siehe hierzu Ziff. 8.1 AGB.

7.3 Was fließt in die Berechnung der Verfügbarkeit mit ein?

Siehe hierzu Ziff. 8.3 AGB. In die Berechnung der Verfügbarkeit werden insbesondere Ursachen nicht einbezogen, die außerhalb des Verantwortungsbereichs des Auftragnehmers liegen.

Das Prinzip der geteilten Verantwortlichkeit findet auch hier seinen Niederschlag. So sind Ausfallzeiten dem Auftragnehmer nicht zuzurechnen, sofern es sich um Versäumnisse des Auftraggebers handelt wie die Nichteinhaltung vereinbarter Vorgaben zu erforderlichen Konfigurationen oder aber Ausfallzeiten, die auf Handlungen nicht autorisierter Nutzer zurückzuführen sind, soweit deren Handeln dem Auftraggeber zuzurechnen sind, beispielsweise durch die Nichtbeachtung angemessener Sicherheitsverfahren.

7.4 Kann der Zugang bei einem Sicherheitsvorfall ausgesetzt werden?

Ja, dies ist unter folgenden Voraussetzungen möglich (Ziff. 8.3 AGB):

1. Es muss sich um einen »Sicherheitsvorfall« handeln (zur Definition siehe Begriffsbestimmungen AGB).
2. Das Aussetzen muss auch dem Schutz des Auftraggebers dienen.
3. Die internen Richtlinien des Auftragnehmers müssen die Aussetzung als Maßnahme und der Schwere des Sicherheitsvorfalls vorsehen.
4. Die internen Richtlinien müssen vergleichbar mit den IT-Grundschutzbausteinen DER.2X »Security Incident Management« des BSI sein.

Hintergrund dieser Regelungen ist, dass eine schnelle Sperrung der Systeme nach außen in der sicherheitskritischen Situation den besten Schutz auch für die Daten des Auftraggebers bedeuten kann.

8 Prüfrechte des Auftraggebers

8.1 Welche Prüfrechte hat der Auftraggeber?

Die Prüfrechte des Auftraggebers (Ziff. 6.4 AGB) sind dreistufig aufgebaut.

Der Regelfall ist die Prüfung auf der Grundlage der vom Auftragnehmer überlassenen Berichte, insbesondere dem C5-Prüfungsbericht vom Typ 2 (Stufe 1, Ziff. 6.4.1 AGB).

Bestehen Zweifel an den überlassenen Unterlagen, ist dem Auftragnehmer die Möglichkeit zur Nachbesserung zu geben (Stufe 2, Ziff. 6.4.2 Satz 1 AGB).

Gelingt es dem Auftragnehmer nicht, diese Zweifel auszuräumen, besteht der Anspruch auf eine Prüfung vor Ort (Stufe 3, Ziff. 6.4.2 AGB). Diese Prüfung vor Ort ist an Bedingungen geknüpft:

1. Angemessene Vorankündigung (Ziff. 6.4.3 Satz 1 AGB) und Unterrichtung über den Prüfungsgegenstand (Ziff. 6.4.3 Satz 3 AGB).
2. Entsprechend qualifiziertes Personal (Ziff. 6.4.2 Satz 1 AGB).
3. Beachtung der Sicherheitsbelange und der Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie dessen Kunden (Ziff. 6.4.2 Satz 2 AGB).
4. Orientierung an dem Leitfaden »Anwendung des BSI C5 durch interne Revision und Informationssicherheit« der ISACA Germany Chapter e.V., soweit zielführend (Ziff. 6.4.2 Satz 5 AGB).
5. Beachtung der Grundsatz von Verhältnismäßigkeit und Wirtschaftlichkeit (Ziff. 6.4.2 Satz 6 AGB).

Mit den vorstehenden Regelungen wird dem Umstand Rechnung getragen, dass eine Vor-Ort-Prüfung zeit- und kostenintensiv ist und zudem ein eigenes Sicherheitsrisiko darstellen kann.

8.2 Wer trägt die Kosten der Vor-Ort-Prüfung?

Jede Partei trägt ihre eigenen Kosten (Ziff. 6.4.2 Satz 4 AGB). Im Kriterienkatalog kann vorgesehen werden, dass der Auftraggeber für die Prüfung eine Vergütung zahlt, sofern das Prüfungsergebnis lediglich unwesentliche Beanstandungen aufzeigt (Ziff. 6.4.2 Satz 7 AGB, Ziff. 18 Kriterienkatalog).

8.3 Was ist unter einer aktuellen C5-Berichterstattung vom Typ 2 zu verstehen?

Der Anforderungskatalog C5 sieht zwei Arten von Prüfungen und Berichterstattungen vor (siehe dort Ziff. 3.3.1). Während die Prüfung nach Typ 1 auf der Grundlage der Systembeschreibung erfolgt, führt der Prüfer bei der Prüfung nach Typ 2 zusätzliche Prüfungshandlungen zur Wirksamkeit der Kontrollen (Funktionsprüfung) durch.

9 Daten / Nutzungsrechte

9.1 Welche Nutzungsrechte werden dem Auftraggeber eingeräumt?

Der Auftraggeber erhält diejenigen Rechte, die für eine vereinbarungsgemäße Nutzung der Leistung erforderlich sind (Ziff. 14.1 Satz 1 AGB).

9.2 Kann der Auftraggeber die Leistungen weltweit nutzen?

Der Auftraggeber kann die Leistungen grundsätzlich weltweit nutzen. Ausgenommen sind hiervon diejenigen Länder, in denen der Auftragnehmer aufgrund staatlicher Rechtsakte

1. die Leistungen nicht anbietet und
2. der Zugang zu den Leistungen bestimmungsgemäß nicht möglich ist (Ziff. 14.1 Satz 3 AGB).

Damit werden insbesondere diejenigen Fälle erfasst, in denen der Auftragnehmer aufgrund von Exportkontrollvorschriften seine Leistungen nicht anbieten darf. Der Auftragnehmer muss allerdings durch technische Maßnahmen sicherstellen, dass ein Abruf der Leistung (also beispielsweise der Zugang auf einer Website) von den betreffenden Ländern technisch nicht möglich ist. Dies erfordert eine Geolokalisierung. Da eine Geolokalisierung technisch von einem Nutzer umgangen werden kann, genügt allerdings, wenn bei einer zutreffenden Geolokalisierung ein Zugang von staatlichen Rechtsakten gesperrt ist (Ziff. 14.1 Satz 4 AGB).

9.3 Welcher Unterschied besteht bei den Nutzungsrechten bei individuellen Leistungen des Auftragnehmers?

Abweichend von dem Grundsatz, dass Nutzungsrechte nur während der Vertragslaufzeit gelten und nur soweit bestehen, wie zur vertragsgemäßen Nutzung der Leistung erforderlich (Ziff. 14.1 AGB), entfällt bei individuellen Leistungen die zeitliche Beschränkung sowie die inhaltliche Beschränkung (Ziff. 14.2 AGB). Die Rechte sind vergleichbar mit den Nutzungsrechten beim Kauf von Standardsoftware ausgestaltet (vergleiche Ziff. 3.1 EVB-IT Überlassung-AGB (Typ A)). Die individuellen Leistungen müssen explizit als solche vereinbart werden. Diese individuellen Leistungsergebnisse können dann auch genutzt werden zur Erbringung von gewerblichen Leistungen an öffentliche Auftraggeber sowie für nicht-gewerbliche Leistungen an sonstige Dritte (Ziff. 14.2 a.E. AGB).

9.4 Wie werden die Leistungsergebnisse behandelt, die bei einer Nutzung der Cloud-Leistungen entstehen (beispielsweise einer Reisekostenabrechnung)?

An den durch die Nutzung der Cloud-Leistungen neu generierten Werken (nur an Werken kann ein Urheberrecht bestehen) stehen die Rechte hierzu ausschließlich dem Auftraggeber zu (Ziff. 14.3 Satz 1 AGB). Allerdings können diese neuen Werke auch vom Auftragnehmer bereitgestellte Inhalte umfassen (beispielsweise beim Datenbankabruf) oder überhaupt nicht unabhängig von den Cloud-Leistungen nutzbar sein. In diesen Fällen bleibt es bei den auf die Vertragslaufzeit befristeten und auf die Nutzung der Vertragsleistung beschränkten Rechte.

9.5 Welche Rechte bestehen für den Auftragnehmer bezüglich der von dem Auftraggeber eingebrachte Daten / Software?

Der Auftraggeber muss die von ihm eingebrachten jeweils bearbeiteten Daten (»Daten des Auftraggebers«) jederzeit selbst oder durch Unterstützung exportieren können (Ziff. 7.3 AGB). Verschlüsselte Daten muss er entschlüsseln können.

9.6 Welche Daten kann der Auftraggeber am Vertragsende herausverlangen?

Dem Auftraggeber muss die Möglichkeit gegeben werden, zu jeder Zeit selbständig oder mit Unterstützung des Auftragnehmers seine Daten zu exportieren (Ziff. 7.3 AGB).

9.7 Welche Löschungspflichten bestehen?

Der Auftragnehmer muss nur die Möglichkeit dem Auftraggeber einräumen. Wenn diese nicht besteht, ist er selbst auf Anforderung zur Löschung verpflichtet (Ziff. 7.1 AGB). Gegebenenfalls sind die besonderen Regelungen in der AVV zu personenbezogenen Daten zu beachten.

9.8 Warum sind Regelungen zum Backup in den AGB vorgesehen?

Es besteht keine im Standard vorgesehene Backup-Pflicht, da in Cloud-Umgebungen die Sicherung nicht als »Backup« funktioniert, sondern durch »Load Balancer« oder andere Methoden. Bei SaaS kann es jedoch notwendig sein, beispielsweise die Wiederherstellung versehentlich gelöschter Daten vorzusehen. Eine Backup-Funktionalität muss allerdings auch bei SaaS vereinbart sein (Ziff. 7.2 AGB »Soweit [...] vereinbart ist«). Differenzierte Regelungen zu einer Datensicherung finden sich als optionale Bestimmungen in Ziff. 16 Kriterienkatalog.

10 No-Spy-Klausel

10.1 Was ist unter der »technischen no-spy-Klausel« zu verstehen?

Die sogenannte »technische no-spy-Klausel« wurde in die verschiedenen EVB-IT Vertragstypen eingefügt, um zu gewährleisten, dass die Software keine unerwünschten Funktionen aufweist, die die Integrität, Vertraulichkeit und Verfügbarkeit von Software, Hardware oder Daten gefährden und den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen. Hierbei handelt es sich um Funktionen in der Software, über die ohne Kenntnis des Auftraggebers z.B. Daten ausgelesen oder verändert oder die Funktion der Software beeinflusst werden können (siehe auch ↗Handreichung des CIO Bund hierzu).

In die EVB-IT Cloud hat die technische no-spy-Klausel in Ziff. 1.4 AGB Eingang gefunden. Wie bei allen EVB-IT Vertragstypen besteht auch hier das Problem, wie die berechtigten Interessen des Auftraggebers an dem Schutz seiner Daten in eine Vertragsregelung gefasst werden können. Die dort in den Bullet-Points aufgeführten Funktion (Absatzen/Ausleiten von Daten, Veränderung/Manipulation von Daten, Einleiten von Daten) gehören gerade zu den Grundfunktionalitäten eines Cloud-Services. Entscheidend ist allein, ob die Funktion »unerwünscht« ist.

10.2 Wann ist eine Funktion unerwünscht?

Jede Funktion ist unerwünscht, die nicht in zumindest eine der folgenden Voraussetzung erfüllt:

1. Die Funktion wurde vom Auftraggeber gefordert.
2. Die Funktion wurde vom Auftragnehmer unter konkreter Beschreibung der Aktivität angeboten.
3. Die Funktion genügt Anforderungen des Anforderungskataloges C5.

10.3 Wie ist mit Funktionen umzugehen, die nach Ziff. 1.4 der AGB unerwünscht sind?

Die in den übrigen EVB-IT Vertragstypen vorgesehene Möglichkeit des »opt-in« (siehe bspw. Ziff. 2.3 EVB-IT Kauf) besteht auch hier, d.h. der Auftraggeber muss die Funktionalität ausdrücklich autorisieren.

11 Ort der Datenspeicherung / Datenverarbeitung

11.1 Wo dürfen Daten gespeichert und verarbeitet werden?

Daten dürfen gespeichert werden / verarbeitet werden (Ziff. 4 AGB) innerhalb

- der EU,
- des EWR
- der Schweiz (sofern Angemessenheitsbeschluss nach Art. 45 DSGVO besteht).

Von dieser grundsätzlichen Festlegung ausgenommen sind Metadaten (siehe hierzu Frage 11.3).

Diese Festlegung kann geändert werden durch

1. den Kriterienkatalog (Ziff. 3),
2. Verweis auf die auftragnehmerseitigen AGB (Anlage zum Kriterienkatalog zur Einbeziehung von auftragnehmerseitigen AGB Ziff. II, Kategorie Leistungsort),
3. Einstellungen des Auftragnehmers in der Administrationskonsole (Ziff. 4 AGB).

Zu beachten sind ggf. weitere Vorgaben zur Verarbeitung bezogener Daten in der AVV.

11.2 Besteht ein Unterschied zwischen dem Ort der Datenspeicherung und dem Ort der Datenverarbeitung

Es wird nicht nach dem Ort der Datensicherung und dem Ort der Datenverarbeitung differenziert. Ist beispielswiese eine Datenspeicherung nur innerhalb der EU zulässig, muss auch jede Verarbeitung der Daten innerhalb der EU erfolgen. Zur Ausnahme bei der Verarbeitung der Metadaten siehe Frage 11.3.

11.3 Welche Sonderregelung besteht für Metadaten und was ist unter Metadaten zu verstehen?

Vereinfacht dargestellt sind Metadaten alle Daten, die nicht Inhaltsdaten sind.

Vorliegend maßgeblich ist die Definition im Anforderungskatalog C5 OPS 11. Danach sind Metadaten Daten, die beim Auftragnehmer durch die Nutzung seines Dienstes durch den Auftraggeber anfallen und keine Inhaltsdaten sind. Dazu gehören u. a. Anmelde/Abmelde-Zeiten, IP-Adressen, GPS-Position des Kunden, welche Ressourcen (Netz, Storage, Computer) genutzt wurden, auf welche Daten wann zugegriffen wurde, mit wem Daten geteilt wurden, mit wem kommuniziert wurde, etc. Diese Daten werden zum Teil für Abrechnungszwecke und für das (Security) Incident Management verwendet. Sie sind darüber hinaus aber auch geeignet, Kundenverhalten und (je nach Cloud-Dienst) ein Großteil von Entscheidungs-

und Arbeitsprozessen für den Auftragnehmer transparent zu machen. Zudem beziehen sich Metadaten auf Daten, die beim Zugriff des Cloud-Anbieters auf Kundendaten (beispielsweise zur Indexierung) entstehen.

Die Ausnahmeregelung für Metadaten in Ziff. 4 AGB ermöglicht es somit Aufgaben der Steuerung der Cloud-Dienste auch außerhalb des festgelegten Leistungsortes zu erbringen, sofern keine Inhaltsdaten verarbeitet werden. Zudem ist jeweils zu prüfen, inwieweit bei der Verarbeitung personenbezogener Daten die AVV Regelungen trifft, die zusätzlich zu beachten sind.

11.4 Wie ist der Datenschutz in den EVB-IT gereglt?

Es wird auf die anwendbaren Bestimmungen über den Datenschutz (Ziff. 6.1.1 AGB) sowie auf die abzuschließende Auftragsverarbeitungsvereinbarung (AVV, Ziff. 6.1.3 AGB) verwiesen. Ein Muster für die AVV ist aufgrund der unterschiedlichen Zuständigkeiten der Aufsichtsbehörden nicht vorgesehen.

12 Unterauftragnehmer

12.1 Wer ist als Unterauftragnehmer zu qualifizieren?

Die AGB enthalten keine eigene Definition von Subunternehmern. Vorgesehen ist nur eine negative Abgrenzung, welche Subunternehmer jedenfalls nicht zu benennen sind (Ziff. 15.1 AGB). Dies sind

- Zulieferer oder
- Unternehmen, deren Leistungen keine vereinbarten C5-Kritieren betreffen und die nicht in die Erbringung der Leistungen eingebunden sind (Var. 1) oder Unternehmen, die lediglich Nebenleistungen erbringen (Var. 2).

Bei Zulieferern oder Unternehmen, die nicht in die Leistungserbringung eingebunden sind, handelt es sich allerdings regelmäßig auch nicht um Unterauftragnehmer.

12.2 Genügt die Benennung des Unterauftragnehmers oder ist eine Zustimmung des Auftraggebers vor Einsatz des Subunternehmers erforderlich?

Es genügt die Benennung (Ziff. 15.1 AGB). Eine ausdrückliche Zustimmung ist nur erforderlich, sofern dies vereinbart ist (Ziff. 15. 3 AGB, Nr. 8.4 Cloudvertrag). Die Zustimmung gilt als erteilt, wenn der Unterauftragnehmer im Angebot / im Vergabeverfahren benannt wurde.

12.3 Auf welchem Weg erfolgt die Benennung von Unterauftragnehmern?

Die Benennung kann über die vereinbarten Mitteilungswege erfolgen. Es genügt aber auch die Benennung durch eine für den Auftraggeber zugänglichen Webseite in Verbindung mit einer individuellen Nachricht wie eine Push-Nachricht (Ziff. 15.3 AGB).

12.4 Was ist bei einem Wechsel eines Unterauftragnehmers zu beachten?

Es genügt grundsätzlich die Bekanntgabe über die Website mit Push-Nachricht (siehe Frage 12.3). Der Auftraggeber hat dann ein Widerspruchsrecht innerhalb einer Frist von 30 Tagen. Können sich die Parteien nicht innerhalb von 90 Tagen nach Zugang der Benachrichtigung einigen, hat der Auftraggeber ein außerordentliches Kündigungsrecht (Ziff. 15.2 AGB).

Etwas anderes gilt, sofern vereinbart wurde, dass der Auftraggeber dem Einsatz eines Unterauftragnehmers ausdrücklich zustimmen muss. In diesem Fall ist eine Zustimmung auch für den Wechsel des Subunternehmers erforderlich (Ziff. 15.3 AGB). Die Zustimmung ist

auch dann erforderlich, wenn der Auftragnehmer die Leistung selbst übernimmt, die zuvor ein Unterauftragnehmer erbrachte.

12.5 Müssen Vertragsänderungen im Verhältnis zum Unterauftragnehmer angezeigt werden?

Grundsätzlich müssen Vertragsanpassungen nicht gegenüber dem Auftraggeber angezeigt werden. Eine Ausnahme ist in Hinblick auf Vertragsänderungen erforderlich, die vereinbarte C5-Kriterien betreffen (Ziff. 15.2 AGB). Auch an dieser Stelle zeigt sich die Bedeutung des Anforderungskatalogs C5 sowie die Vorgaben der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021. Für die Mitteilung der Änderungen greift das gleiche Verfahren wie bei der Benennung von Unterauftragnehmern (siehe Frage 12.3).

12.6 Gelten die Regelung über Unterauftragnehmer auch für die Unterauftragnehmer des Unterauftragnehmers?

Ja, die Regelungen gelten für die gesamte Unterauftragnehmerkette (Ziff. 15.6 AGB).

13 Störungsbeseitigung

13.1 Warum wird bei der Störungsbeseitigung zwischen SaaS / PaaS einerseits und IaaS andererseits differenziert?

Die Regelung zur Störungsbeseitigung ist bei SaaS und PaaS (Ziff. 11.1 AGB) an die Bestimmungen zur Pflege von Standardsoftware angelehnt (vgl. Ziff. 2.2 EVB-IT Pflege S-AGB). Die Situation ist insbesondere beim Einsatz von Drittsoftware durch den SaaS / PaaS Anbieter vergleichbar.

13.2 Welche Maßnahmen muss der Auftragnehmer bei Störungen bei SaaS / PaaS ergreifen?

Sind keine Reaktions- oder Wiederherstellungszeiten vereinbart (siehe hierzu Ziff. 21 Kriterienkatalog), ist mit der Störungsbeseitigung nach Eingang der Meldung / Eintritt des vereinbarten Ereignisses innerhalb der vereinbarten Servicezeiten unverzüglich zu beginnen und die Störungsbeseitigung innerhalb angemessener Frist abzuschließen (Ziff. 11.1 AGB).

Anders als beispielsweise bei den EVB-IT Pflege S-AGB (Ziff. 4.1) sind keine Servicezeiten für den Fall vorgesehen, dass keine gesonderte Vereinbarung erfolgte. Es bedarf also einer Vereinbarung von Servicezeiten.

13.3 Welche Maßnahmen muss der Auftragnehmer bei Störungen bei IaaS ergreifen?

Sind keine Reaktions- oder Wiederherstellungszeiten vereinbart (siehe hierzu Nr. 21 Kriterienkatalog), ist mit der Störungsbeseitigung nach Eingang der Meldung / Eintritt des vereinbarten Ereignisses unverzüglich zu beginnen und die Störungsbeseitigung innerhalb angemessener Frist abzuschließen (Ziff. 11.2 AGB). Eine Sonderregelung für Drittsoftware besteht hier nicht.

Eine Regelung von Reaktions- und Wiederherstellungszeiten dürfte sich bei IaaS regelmäßig bereits deshalb erübrigen, weil der Auftragnehmer ohnehin die Verfügbarkeit nach VK 1 gewährleisten muss (siehe Frage 7.1).

14 Haftung

14.1 Wie ist die Haftung bei leicht fahrlässigen Pflichtverletzungen begrenzt?

Die Haftung ist bei leichter Fahrlässigkeit auf dem Auftragswert begrenzt (Ziff. 19.1 AGB). Damit orientiert sich die Haftungsbeschränkung an dem »EVB-IT Standard«.

Eine Sonderregelung betrifft das 1. Vertragsjahr. Hier beträgt die Haftung mindestens das Doppelte und maximal das Vierfache der Vergütung, die für das erste Vertragsjahr zu zahlen ist. Damit sollen die Fälle erfasst werden, bei denen die Vergütung sich ausschließlich nach dem tatsächlichen Abruf der Leistung bemisst und daher der Auftragswert zum Zeitpunkt des Schadenseintritts gering sein kann (siehe hierzu auch Frage 14.2).

Zusätzlich sind Mindesthaftungsobergrenzen vorgesehen. Beträgt der Auftragswert weniger als 50.000 EUR, wird die Haftung auf diesen Betrag beschränkt. Bei Sachbeschädigungen ist die Haftung auf eine Million beschränkt, sofern der Auftragswert geringer als eine Million ist. M.a.W: Es ist unabhängig von der Berechnung des Auftragswertes – jedenfalls bei Sachbeschädigungen – von einer Haftung bis zu einer Million bei einer fahrlässigen Pflichtverletzung auszugehen.

14.2 Wie berechnet sich der Auftragswert?

Der Auftragswert berechnet sich nach der zu zahlenden Vergütung (siehe Begriffsbestimmung AGB). Maßgeblich ist somit nur diejenige Vergütung, für die auch eine Zahlungspflicht besteht. Handelt es sich mithin um eine Vergütung nach Abruf (pay-as-you-go), steigt der Auftragswert mit der tatsächlichen Abnahmemenge. Zu beachten ist aber die Mindesthaftungssumme (siehe Frage 14.1).

14.3 Gelten über die Beschränkungen der leichten fahrlässigen Pflichtverletzungen hinaus Haftungsbeschränkungen?

Ansprüche aus Gewinn sind ausgeschlossen (Ziff. 19.3).

14.4 Wie sind Nichterfüllungsgutschriften in das Haftungsregime einzuordnen?

Sind Nichterfüllungsgutschriften (oder eine andere Form der Kompensation) vereinbart, greift das allgemeine Minderungsrecht nach Ziff. 18 AGB nicht.

Nichterfüllungsgutschriften können im Kriterienkatalog (Nr. 20) oder durch Verweis auf die auftragnehmerseitigen AGB (Ziff. II Kategorie Gutschriften bei Nicht-verfügbarkeit Anlage zur Einbeziehung auftragnehmerseitige AGB) vereinbart werden.

15 Vergütung

15.1 Warum sind keine für Cloud-Leistungen typischen Vergütungsregelungen vorgesehen?

Die Vergütungsmodelle zwischen den einzelnen Cloud-Diensten, aber auch innerhalb eines Cloud-Dienstes, sind zu unterschiedlich für den Versuch einer Standardisierung.

15.2 Können während der Vertragslaufzeit Preisanpassungen gefordert werden?

Die Möglichkeit der Preisanpassung setzt eine entsprechende Vereinbarung voraus. Eine Preisanpassung kann in Ziff. 4.4 Cloudvertrag vereinbart werden. Sofern nichts Weiteres vereinbart wird, gelten im Übrigen für die Preisanpassung die Regelungen in Ziff. 16 AGB.

15.3 Für welche Leistungen gelten die Regelungen zur Vergütung nach Zeitaufwand?

Die Regelung in Ziff. 16 AGB betreffen Personalleistungen, die nach Zeitaufwand abgerechnet werden (bspw. bei den initialen Leistungen nach Nr. 3.2.1.2 Cloudvertrag).

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom