Stand: Februar 2017

Cloud Computing Verträge

Checklist für Unternehmen – darauf ist zu achten!

VORBEMERKUNG

Diese Checkliste dient Unternehmen als Orientierungshilfe bei der Beschaffung von Cloud-Diensten. Sie enthält eine überblicksartige Darstellung der wesentlichen Eckpunkte, die beim Abschluss eines Vertrages über die Inanspruchnahme eines Cloud-Dienstes zu beachten sind.

Zu vielen in dieser Checkliste angesprochenen Punkten gilt, dass eine interessengemäße, präzise vertragliche Abbildung der vom Kunden gewünschten Rechtsfolgen dringend zu empfehlen ist, da das Gesetz dem Kunden – etwa für den Fall des Exits aus der Cloud – keine hinreichend konkreten Anspruchsgrundlagen an die Hand gibt.

Die Checkliste ist so aufgebaut, dass sie zunächst die vom Kunden zu stellenden Fragen aufwirft und sodann einen kurzen Überblick über die Rechtslage gibt sowie die im Interesse des Kunden typischerweise empfehlenswerten Regelungen erläutert.

Die Checkliste richtet sich ausschließlich an Unternehmenskunden (nicht an Verbraucher).

Die in dieser Checkliste enthaltenen Empfehlungen können eine individuelle Rechtsberatung natürlich nicht ersetzen.

I. FRAGEN VOR DEM GANG IN DIE CLOUD

Im Rahmen von Cloud Computing Diensten werden Softwareprogramme oder andere IT-Leistungen (wie z.B. Speicherplatz oder Rechenleistungen) in virtualisierter Form bereitgestellt (nachfolgend "**Cloud-Dienst**"). Im Wege des Cloud Computing werden Standardsoftware ("*Software-as-a-Service*" – "*SaaS*"), standardisierte Plattformen ("*Platform-as-a-Service*" – "*PaaS*") oder Infrastruktur ("*Infrastructure-as-a-Service*" – "*IaaS*") angeboten.

Cloud-Dienste unterscheiden sich in der Art der Bereitstellung grundlegend von der Bereitstellung von Software auf herkömmliche Weise: Anders als bei der Überlassung von Software auf einem Datenträger oder im Wege des Downloads wird Software als Cloud-Dienst nicht auf einem Server des Kunden installiert, sondern auf Servern des Anbieters. Der Anbieter wartet die Software auf seinen eigenen Servern und stellt die jeweils aktuelle Version von dort aus seinen Kunden bereit. Die Software wird dabei nicht nur einem dezidierten Kunden zur Verfügung gestellt, sondern einer Vielzahl von Kunden, die diese nach Bedarf abrufen.

Bevor sich der Kunde entscheiden kann, ob die Inanspruchnahme von Cloud Diensten für ihn möglich und passend ist, gilt es, die folgenden Fragen sorgfältig zu prüfen:

1. Darf überhaupt ein Cloud Dienst verwendet werden?

- Greifen bereichsspezifische gesetzliche Restriktionen ein? Hat der Wirtschaftsprüfer dazu Stellung genommen, ob der Gang in die Cloud möglich ist?

- Gibt es unternehmenseigene Compliance-Vorschriften, die diesen Sachverhalt regeln?

In einigen Bereichen gibt es strenge branchenspezifische regulatorische Anforderungen, wie z.B. bei Finanzdienstleistungen und Versicherungen.

Bei Berufsgeheimnisträgern (etwa Versicherungen) sind die strengen strafrechtlichen Grenzen des § 203 StGB zu beachten.

Auch datenschutzrechtlich ist zu prüfen, ob die Verarbeitung der Daten in der Cloud bei einem externen Anbieter in der konkreten Konstellation zulässig ist (dazu näher unter Ziffer II.6).

Darüber hinaus können interne Richtlinien im Unternehmen selber es verbieten, bestimmte Bereiche auszulagern. Dies gilt es vorher zu analysieren.

2. Was müssen Kunden beim Gang in die Cloud beachten?

- Muss der Betriebsrat eingebunden werden?

- Müssen betriebsinterne Compliance-Vorschriften beachtet werden?

- Gibt es zwingend anwendbare inländische oder ausländische Compliance-Regelungen, z.B. MaRisk, SOX 404, § 25 a KWG?

Insbesondere, wenn Mitarbeiterdaten betroffen sind, kann der Betriebsrat Mitspracherechte, zumindest aber Informationsrechte, haben. Wird der Betriebsrat trotz entsprechender Verpflichtung des Kunden nicht beteiligt, so kann ihm ein Unterlassungsanspruch zustehen; unter Umständen kann der Betriebsrat sogar verlangen, dass Maßnahmen wieder rückgängig gemacht oder entfernt werden.

Insbesondere bei börsennotierten Unternehmen können zusätzliche Compliance-Vorgaben, einschließlich selbst gesetzter Compliance-Richtlinien ("Code of Compliance") eingreifen. Die Abstimmung mit internen oder externen Rechtsberatern zur Einhaltung der entsprechenden Vorgaben ist unbedingt notwendig. Ein Verstoß kann für Kunden und deren Management erhebliche Konsequenzen haben und sogar strafbar sein.

3. Prüfung der Dienste

- Passt die Art des Dienstes zum Bedarf des Kunden?
- Wird nutzungsabhängig abgerechnet?

Cloud-Dienste zeichnen sich durch ein hohes Maß an Standardisierung aus und werden an eine Vielzahl von Kunden erbracht. Von daher ist genau zu prüfen, welches Angebot für den eigenen Bedarf geeignet erscheint. Kundenspezifische Anpassungen der Dienste sind in der Regel nicht vorgesehen und erfolgen nur in Einzelfällen.

Weitere typische Merkmale von Cloud-Diensten sind die nutzungsabhängige Vergütung und Skalierbarkeit. Es sollte darauf geachtet werden, dass die Vergütung in Abhängigkeit von der tatsächlichen Nutzung transparent geregelt ist.

4. Prüfung des Anbieters

- Ist der Anbieter vertrauenswürdig?
- Welche Folgen hätte ein Ausfall des Anbieters (etwa bei Betriebseinstellung oder Insolvenz)? Welche Ausweichmöglichkeiten gibt es?
- Ist der Anbieter Generalunternehmer oder stehen Verträge mit mehreren Anbietern über einzelne Cloud-Dienste im Raum?

Der Kunde sollte sorgfältig prüfen, ob der Anbieter den spezifischen Anforderungen des Kunden genügt. Typischerweise kann der Kunde aus einer Vielzahl von Anbietern auswählen. Bei der Auswahl sollte er insbesondere auch auf entsprechende Zertifizierungen und Gütesiegel des Anbieters achten. Dies gilt sowohl für den Bereich der technischen Sicherheit (also die sicherheitsrelevanten Zertifizierungen nach ISO 27001, etc.), organisatorischer Auditierbarkeit von Dienstleister (SSAE16, etc.) als auch Datenschutz-Zertifizierungen z.B. nach dem „Trusted Cloud“ Standard und entsprechenden Fortführungen nach Artikel 42, 43 Datenschutz-Grundverordnung (DS-GVO).

Auch bei einem vertrauenswürdigen Anbieter sollte die Möglichkeit eines flexiblen Umstiegs auf alternative Anbieter von vornherein bedacht werden (Vermeidung eines "Vendor Lock-in").

Wichtig für den Kunden ist auch die Anzahl der Vertragspartner, denen er sich gegenüber sieht. Hat er mit einem Generalunternehmer zu tun, so braucht der Kunde nur einen Vertrag zu verhandeln und abzuschließen. Verträge mit mehreren Vertragspartnern bedeuten für den Kunden einen größeren Aufwand bei der Verhandlung und der Verwaltung der Verträge und bergen zudem das Risiko erschwerter Schuldzuweisung im Haftungsfall ("fingerpointing"). Jedoch bieten mehrere Verträge mit verschiedenen Vertragspartnern mitunter größere Flexibilität als der Abschluss eines einzigen Vertrags mit einem Generalunternehmer.

II. FRAGEN DER VERTRAGSGESTALTUNG

1. Rechtswahl und Gerichtsstand

- Welches Recht ist anwendbar? Welche Gerichte sind für Streitigkeiten zuständig?

Rechtswahl und Gerichtsstandsklausel sind wichtige Weichenstellungen für den Vertrag. Die Rechtswahl entscheidet darüber, welchem Recht der Vertrag unterliegt und welches Recht damit für die Auslegung des Vertrags maßgeblich ist. Die Gerichtsstandsklausel regelt, vor welchen Gerichten etwaige Streitigkeiten ausgetragen werden.

1.1 Rechtswahl

Der Kunde sollte prüfen, ob der Vertrag deutschem Recht unterliegt und auf einen Gerichtsstand am Sitz des Kunden (oder zumindest in Deutschland) hinwirken. Grundsätzlich sind die Parteien eines B2B-Vertrages bei der Wahl des anwendbaren Rechts frei. Insbesondere in stark angelsächsisch geprägten Branchen wie etwa der Finanzbranchen ist allerdings eine Rechtswahl deutschen Rechts erfahrungsgemäß sehr schwierig oder gar nicht möglich, wenn der Anbieter aus diesem Rechtskreis kommt.

Die Sprache des Vertrages ist nicht ausschlaggebend für das anwendbare Recht. Ist der Vertrag in deutscher Sprache verfasst, führt das nicht etwa automatisch zur Anwendbarkeit deutschen Rechts. Stimmt die Vertragssprache nicht mit der Sprache des anwendbaren Rechts überein (Beispiel: englischsprachiger Vertrag nach deutschem Recht), kann es zu Auslegungsschwierigkeiten bei einzelnen Begriffen oder gesamten Klauseln kommen. Dies gilt insbesondere etwa für Regelungen zu Mängelrechten oder Haftung, etwas weniger bei Regelungen eher operativen Inhalts, wie z.B. Vereinbarungen zu Change Request Verfahren. Missverständnisse lassen sich vermeiden, indem zur Klarstellung die gemeinten Rechtsbegriffe in der Originalsprache eingefügt werden, z.B. in Klammern hinter den übersetzten Begriff.

Treffen die Parteien keine Regelung über die Rechtswahl, so kommt regelmäßig das Recht des Staates zur Anwendung, in dem die Partei, die die vertragstypische Leistung zu erbringen hat, ihren Sitz hat. Das ist bei einem Cloud-Dienst typischerweise der Staat, in dem der Anbieter seinen Sitz hat. Fehlt in einem Vertrag eines ausländischen Anbieters eine Rechtswahlklausel, muss der Kunde daher von der Geltung ausländischen Rechts ausgehen, sofern er nicht ausdrücklich eine ergänzende Vereinbarung mit dem Anbieter trifft.

Zudem ist zu beachten, dass eine Regelung zu Rechtswahl sich lediglich auf das zwischen den Parteien anwendbare Recht auswirkt, jedoch nicht auf zwingendes Recht, wie etwa Datenschutzrecht oder Steuerrecht.

Anmerkung:
Die Ausführungen in dieser Checklist richten sich nach der deutschen Rechtslage.
Ist die Anwendung deutschen Rechts gegenüber einem konkreten Anbieter nicht durchsetzbar, ist die Beratung durch einen mit der anwendbaren ausländischen Rechtsordnung vertrauten Rechtsanwalt unverzichtbar.

1.2 Gerichtsstand

Der Gerichtsstand ist entscheidend für die gerichtliche Rechtsdurchsetzung im Streitfall. Die zuständigen Gerichte sollten typischerweise in dem Staat liegen, dessen Recht Anwendung finden soll. Denn für Richter an einem nationalen Gericht ist es schwierig und in jedem Fall zeitaufwändig, einen Sachverhalt nach einer fremden Rechtsordnung entscheiden zu müssen.

Alternativ können sich die Parteien darauf einigen, dass sie im Streitfall anstelle eines staatlichen Gerichtsverfahrens ein Schiedsverfahren durchführen. Ein solches Verfahren kann schneller sein als ein Verfahren vor ordentlichen Gerichten; es kann zudem gerade bei Streitigkeiten im IT-Bereich den Vorteil haben, dass die von den Parteien selbst eingesetzten Schiedsrichter über besondere Sachkunde verfügen. Die Kosten eines Schiedsverfahrens liegen – vor allem bei niedrigen Streitwerten – möglicherweise jedoch höher als bei einem ordentlichen Gerichtsverfahrens. Bei der Gestaltung einer Schiedsklausel ist insbesondere darauf zu achten, dass Voraussetzungen und Reichweite des Schiedsverfahrens sowie die anwendbaren Schiedsregeln eindeutig vereinbart werden. Insbesondere muss deutlich werden, ob die Parteien auf die Anrufung staatlicher Gerichte gänzlich verzichten wollen. In diesem Fall entfällt die Möglichkeit einer Berufungsinstanz. Die Entscheidung für ein Schiedsverfahren ist damit von großer Tragweite und sollte wohlüberlegt sein.

1.3 Beispielklausel für Rechtswahl und Gerichtsstand

> ***1. Rechtswahl***
>
> *Dieser Vertrag sowie alle aus oder im Zusammenhang mit ihm entstehenden Streitigkeiten unterliegen dem Recht der Bundesrepublik Deutschland unter Ausschluss des einheitlichen UN-Kaufrechts (CISG).*
>
> ***2. Gerichtsstand***
>
> *Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist [Ort des Kunden].*

2. AGB oder Individualvertrag

- Legt der Anbieter Allgemeine Geschäftsbedingungen vor oder soll der Kunde auf die Ausgestaltung des Vertrags Einfluss nehmen können?

Der hohe Standardisierungsgrad von Cloud-Diensten führt in der Regel dazu, dass auch die Verträge mit den Kunden standardisiert sind. Der Anbieter legt dem Kunden in solchen Fällen seinen Standardvertrag vor (nach deutschem Recht handelt es sich dabei um Allgemeine Geschäftsbedingungen ("AGB")), wobei für den Kunden typischerweise wenig bis kein Verhandlungsspielraum besteht.

Nach deutschem Recht unterliegen AGB strengen inhaltlichen Anforderungen, wobei das deutsche AGB-Recht nicht nur Verbraucher, sondern auch Unternehmen vor unangemessener Benachteiligung schützt. Die Möglichkeiten des Anbieters, seine Haftung gerichtlich durchsetzbar zu beschränken und seine Rechtsposition zu optimieren, sind daher begrenzt. Bestimmungen in AGB des Anbieters, die zu Lasten des Kunden über diesen Rahmen hinausgehen, sind unwirksam.

Dennoch ist dem Kunden typischerweise nicht anzuraten, sich auf die AGB-rechtliche Unwirksamkeit für ihn besonders nachteiliger Regelungen zu verlassen und von einer Verhandlung von vornherein abzusehen. Der Einwand AGB-rechtlicher Unwirksamkeit führt in außergerichtlichen Auseinandersetzungen zumindest gegenüber einem ausländischen Anbieter selten zum nachhaltigen Erfolg; will man eine Klausel gerichtlich überprüfen, steht oft der Zeit- und Kostenaufwand und die mit einem Gerichtsverfahren verbundene Störung der Vertragsbeziehung nicht im Verhältnis. Zudem besteht – gerade in internationalen Sachverhalten – stets das Risiko, dass das Gericht dem Einwand der Unwirksamkeit nicht folgt.

Vom Anbieter vorgelegte AGB sind daher sorgfältig zu prüfen und zumindest an für den Kunden neuralgischen Punkten gegebenenfalls zu verhandeln.

Praxishinweis:
*Oftmals besteht der Anbieter auf dem Einsatz seines Standardvertrags. Der Kunde hingegen verlangt dezidiert abweichende Regelungen zu seinen Gunsten. Eine pragmatische Lösung liegt dann häufig im Abschluss einer **Ergänzungsvereinbarung**, durch die die Vertragsparteien einzelne Klauseln der Allgemeinen Geschäftsbedingungen des Anbieters ändern oder streichen. Mit diesem in der Praxis häufig gewählten Weg wird ein Standard-Vertrag "teil-individualisiert"; der Kunde kann damit punktuell seine kommerziellen und rechtlichen Anliegen in den Vertrag einbringen.*

*Wesentlich ist in jedem Fall eine eindeutige Vereinbarung zur **Geltungsreihenfolge** verschiedener Vertragsbestandteile. Dies gilt besonders dann, wenn die vom Anbieter vorgelegte Standardvertragsdokumentation – wie dies gerade bei US-Anbietern typisch ist – aus einem umfangreichen und ggf. unübersichtlichen Konvolut verschiedener Vertragsdokumente besteht.*

3. Leistungsbeschreibung/Nutzungsrechte/Mehrbedarf

3.1 Leistungsbeschreibung und Lizenzen

- Ist die Leistungsbeschreibung ausreichend? Passt der dort beschriebene Dienst zum Bedarf des Kunden?

- Erhält der Kunde ausreichende Nutzungsrechte für seinen Bedarf? Welche Nutzungsrechte werden dem Kunden im Einzelnen eingeräumt?

Die Nutzungsbefugnis des Kunden ist bei einem Cloud-Dienst in aller Regel im Sinne eines mietähnlichen Verhältnisses zeitlich befristet. Der Kunde erwirbt sämtliche zur Erbringung des Cloud-Dienstes erforderlichen Leistungen als einheitliches Leistungspaket, einschließlich des Betriebs und der fortlaufenden Fehlerbehebung der genutzten Software. Einzelheiten der geschuldeten Leistungen sind in der Leistungsbeschreibung und ggf. dem Service Level Agreement ("SLA"), festgelegt. Der Anbieter hostet den Dienst bei sich (oder durch einen von ihm beauftragten Dienstleister) und rechnet ihn z.B. monatlich gegenüber dem Kunden ab. Da der Anbieter den bereitge-

stellten Dienst während der Vertragslaufzeit ständig wartet und weiter entwickelt, umfasst das Nutzungsrecht des Kunden die Software in der jeweils aktuellen Version.

Bei der Vertragsgestaltung ist darauf zu achten, dass die durch den Cloud-Anbieter zu erbringende Leistung im Rahmen einer Leistungsbeschreibung so genau wie möglich bestimmt wird, um die vereinbarten Funktionalitäten genau zu beschreiben und ggf. Unterschreitungen feststellen zu können. Die Leistungsbeschreibung kann sich aus dem Hauptvertrag ergeben oder als separate Anlage dem Vertrag angehängt werden. Bei dynamischen Verweisen auf Weblinks des Anbieters ist Vorsicht geboten, da sich im Nachhinein oft nicht mehr der im Zeitpunkt des Vertragsschlusses maßgebliche Vertragsinhalt verbindlich feststellen lässt. Hier kann eine Fixierung auf einem physischen Datenträger hilfreich sein. Soweit ein Anbieter die Funktionalitäten einschränken möchte, ist eine angemessene Vorankündigung (beispielsweise von einem halben Jahr) vertraglich zuzusichern. Ähnliche Informationspflichten sind sinnvoll um sicherzustellen, dass der Anbieter den Kunden rechtzeitig auf technische Änderungen hinweist, die Änderungen etwa hinsichtlich der Schnittstellen, der datenschutzrechtlichen und sicherheitstechnischen Einstellungen betreffen.

Zudem muss der geplante Nutzungsumfang ausdrücklich beschrieben werden. Die Einräumung urheberrechtlicher Nutzungsrechte (im Sinne der §§ 69a ff. UrhG) an Software ist zwar an sich nur dann im engeren Sinne erforderlich, wenn der Kunde überhaupt selbst Vervielfältigungshandlungen vornimmt, wozu es bei der Nutzung eines Cloud-Dienstes – je nach der technischen Gestaltung im Einzelfall – jedoch nicht notwendigerweise kommt. Für den Kunden ist es aber in jedem Fall sinnvoll, seine (nicht-ausschließlichen, zeitlich befristeten) Nutzungsrechte vertraglich ausdrücklich festzuschreiben.

3.2 Mehrbedarf

- Ist Flexibilität hinsichtlich einer möglichen Mehrnutzung des Kunden gesichert?
- Welche Bedingungen gelten bei Mehrbedarf?

Die Skalierbarkeit ist typischerweise ein Hauptgrund, die Cloud zu nutzen. Eine vertragliche Zusicherung der Verfügbarkeit von zusätzlichen Ressourcen ist die konsequente Umsetzung des Cloud-Vorteils. Ohne eine ausdrückliche Vereinbarung ist es unsicher, ob zum jeweiligen Zeitpunkt auch die notwendigen Ressourcen zur Verfügung stehen. Eine Zusicherung unbegrenzter Skalierbarkeit ist dafür typischerweise nicht erforderlich. Der mögliche Mehrbedarf des Kunden während der Vertragslaufzeit kann und sollte bereits im Vorhinein bedacht und vertraglich adressiert werden. Preise für zusätzliche Nutzer oder zusätzliche Speicherkapazität können schon vorab vertraglich geregelt werden. Anderer, nicht vorhersehbarer Änderungsbedarf aufgrund von Kundenwünschen ist über ein vertraglich festzulegendes Änderungsverfahren (sog. Change Request-Verfahren) zu berücksichtigen.

4. Service Level

4.1 Verfügbarkeit

- Enthält der Vertrag präzise Zusicherungen über die Verfügbarkeit der Dienste?

- Müssen geplante Downtimes (Wartungsfenster) vorher mit dem Kunden abgestimmt oder zumindest angekündigt werden?

- Ist die Dauer geplanter Downtimes beschränkt?

Der Vertrag über den jeweiligen Cloud-Dienst sollte die Verfügbarkeit des Dienstes in demjenigen Umfang garantieren, den der Kunde hinsichtlich des konkret betroffenen Dienstes, also der Anwendung, Plattform oder Infrastruktur, benötigt. Je nach der Bedeutung des Cloud Dienstes für den Kunden (und den möglichen Konsequenzen eines Ausfalls) muss der Kunde prüfen, ob die vom Anbieter angebotene Verfügbarkeit ausreicht.

Bei der Beurteilung einer angebotenen Verfügbarkeit (etwa 99,7 %) kommt der zugeordneten Zeiteinheit (etwa "pro Jahr", "pro Quartal" oder "pro Monat") entscheidende Bedeutung zu.

Die vertraglich festgelegte Leistung wird üblicherweise in einem Service Level Agreement (SLA) beschrieben. Es ist besonders darauf zu achten, dass die zugesicherten Verfügbarkeiten nicht dadurch "ausgehöhlt" werden, dass geplante Downtimes bei der Berechnung der Verfügbarkeit pauschal ausgeklammert werden oder ein pauschaler Vorbehalt für vom Anbieter nicht verschuldete Downtimes (etwa bei Stromausfall) gemacht wird. Bei der Zusage von Verfügbarkeiten geht es letztlich genau darum, dass der Anbieter eine bestimmte Verfügbarkeit unabhängig von seinem Verschulden garantiert. Um Streit darüber zu vermeiden, sollten die Parteien vertraglich regeln, welche Partei die Einhaltung der Service-Level misst und auf welcher Messbasis dies erfolgt.

Insbesondere für Kunden, die den Dienst im Rahmen eines Geschäftsbetriebes einsetzen, der saisonabhängig funktioniert oder der auf bestimmte Ereignisse ausgerichtet ist, muss der Kunde darauf achten, dass die für sein Geschäft wichtigen Zeiträume von etwaigen Downtimes ausgenommen werden. Diese sind genau zu spezifizieren und ausdrücklich aufzunehmen (so z.B. der Ausschluss bestimmter Geschäftszeiten oder Monate, z.B. Dezember, aus den Wartungsintervallen).Des Weiteren kann es – je nach Geschäftsmodell – im Interesse des Kunden liegen, dass die Downtimes möglichst nicht in mehreren Intervallen, sondern "am Stück" erfolgen.

Standardverträge von Anbietern enthalten meist umfassende Haftungsausschlüsse für Konnektivitätsausfälle. Soweit dies auch Konnektivitätsausfälle in der Sphäre des Anbieters umfasst, sollte sich der Kunde auf Haftungsausschlüsse allenfalls in eng umschriebenen Fällen einlassen.

Achtung:
Im Bereich der Service Levels weichen die Interessen des Anbieters ggf. erheblich von denen des Kunden ab. Achten Sie deshalb darauf, dass Sie vertraglich die von Ihnen benötigte Leistung absichern und Ihre Interessen ausreichend schützen!

4.2 Vertragsstrafen/Pönalen

- Sind Reaktions- und Fehlerbehebungszeiten in den Service Levels definiert?

- Sind die Zeiten ausreichend für den Einsatz des Dienstes im Unternehmen des Kunden?

- Ist für den Fall der Nichteinhaltung der SLA eine Vertragsstrafe vereinbart? Sind die vereinbarten Vertragsstrafen für den Anbieter hinreichend abschreckend, um die Einhaltung der Service Levels sicherzustellen?

Als Hebel für die Durchsetzung der garantierten Verfügbarkeit sollten Vertragsstrafen vereinbart werden. Bietet ein Anbieter standardmäßig bestimmte Vertragsstrafen für den Fall der Nicht-Einhaltung der Service Levels an, so ist aus Sicht des Kunden besonders darauf zu achten, dass diese verschuldensunabhängig greifen.

5. Change Request

- Ist ein detailliertes Verfahren geregelt, wie Änderungsverlangen des Kunden umgesetzt werden sollen?

- Wie ist es mit Vertragsanpassungen aufgrund der Veränderung gesetzlicher Rahmenbedingungen?

Der Kunde sollte evaluieren, ob ihm die Standard-Möglichkeiten des Cloud-Dienstes ausreichen oder ob er darauf angewiesen ist, dass – ggf. auch erst im Laufe der Nutzung des Dienstes – Anpassungen notwendig werden. Viele Dienste erlauben überhaupt keine kundenspezifischen Anpassungen.

Kommen Anpassungen nach dem individuellen Bedarf des Kunden in Fragen, so sollte der Kunde mit dem Anbieter ein detailliertes Change Request-Verfahren für den Fall von Anpassungen während der Vertragslaufzeit vereinbaren. In einer Change Request Klausel ist – wie aus anderen IT-Projekten gewohnt – zu beschreiben, wer und auf welchem Wege Änderungen vorschlagen kann, wie eine Entscheidung über das Änderungsverlangen gefällt und als Vertragsergänzung aufgenommen werden soll. Die Parteien sollten zudem vereinbaren, dass, bevor keine Entscheidung über das Änderungsverlangen herbeigeführt ist, der ursprüngliche Vertrag weiterhin Anwendung findet, sofern der Kunde nicht ausdrücklich schriftlich eine Aussetzung verlangt.

Eine separate Frage betrifft die allgemeine Compliance mit gesetzlichen Rahmenbedingungen. Hier sollte der Vertrag idealerweise eine allgemeine Verpflichtung des Anbieters zur Wahrung aller gesetzlichen Anforderungen bei seiner Leistungserbringung enthalten. Ändern sich die Anforderungen, so sollte der Anbieter entsprechende Anpassungen für den Kunden kostenfrei vornehmen. Handelt es sich um branchenspezifische regulatorische Anforderungen, die den Kunden treffen, muss man sehr genau diskutieren, ob es sich ggf. um kostenpflichtige Anpassungen handeln soll oder nicht.

6. Datenschutz

6.1 Anwendbares Gesetz

- BDSG oder DS-GVO?

Das deutsche und europäische Datenschutzrecht wurde durch die europäische Datenschutzgrundverordnung (DS-GVO) umfassend neu gestaltet. Die DS-GVO ist ab dem Stichtag 25. Mai 2018 als europäische Verordnung direkt in allen EU-Mitgliedsstaaten anwendbar und löst damit das BDSG ab. Ab diesem Tag gilt ausschließlich die DS-GVO, soweit nicht spezifische Ausnahmebereiche (wie z.B. beim Arbeitnehmerdatenschutz) sich vorrangig nach bestehendem bzw. nationalen Datenschutz richten. Die

folgende Darstellung gibt die jeweiligen datenschutzrechtlichen Aspekte sowohl nach BDSG als auch der DS-GVO wieder.

6.2 Anwendbarkeit des Datenschutzrechts

- Sind personenbezogene Daten betroffen?

Personenbezogene Daten *sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Da der Begriff sehr weit gefasst ist, kommt es bei der Inanspruchnahme von Cloud Services sehr häufig zu einer Übermittlung personenbezogener Daten an den Anbieter. Personenbezogene Daten sind zum Beispiel Name, Adresse, Telefonnummer, E-Mail-Adresse, Geburtsdatum, aber auch die IP Adresse oder sonstige auf eine zumindest bestimmbare natürliche Person bezogene Angaben oder Informationen.*

Sofern in dem zu prüfenden Szenario keine personenbezogenen Daten über den Cloud-Dienst gespeichert oder verarbeitet werden, ist das Datenschutzrecht nicht anwendbar.

Sind jedoch personenbezogene Daten betroffen, muss datenschutzrechtlich geprüft werden, ob und unter welchen Voraussetzungen die Inanspruchnahme von Cloud Services in der konkreten Konstellation zulässig ist.

Datenschutzrechtlich besonders komplex wird es, wenn Daten in ein ***Drittland*** *(außerhalb von EU/EWR) transferiert und dort verarbeitet werden oder sogenannte* ***besondere Arten personenbezogener Daten*** *betroffen sind (z.B. Gesundheitsdaten oder Daten zur religiösen Überzeugung oder Gewerkschaftszugehörigkeit, vgl. § 3 Abs. 9 BDSG bzw. Art. 9 Abs. 1 DS-GVO). Es gelten in diesem Fall höhere Zulässigkeitsanforderungen; zudem sind zusätzliche datenschutzrechtliche Absicherungen erforderlich (s.u.).*

Im Folgenden werden die wichtigsten Eckpunkte für die rechtmäßige Verarbeitung von Daten in der Cloud skizziert; eine umfassende Darstellung würde angesichts der Komplexität des Datenschutzrechts den Rahmen dieser Darstellung jedoch sprengen.

6.3 Schriftlicher Auftragsdatenverarbeitungsvertrag

- Sind die Voraussetzungen für eine zulässige Auftragsdatenverarbeitung erfüllt?

- Liegt ein schriftlicher Vertrag vor?

Eine schriftliche Auftragsdatenverarbeitungsvereinbarung ("ADV") ist erforderlich, wenn der Anbieter personenbezogene Daten des Kunden im Auftrag des Kunden verarbeitet. Dadurch wird der Anbieter zum Auftragnehmer, wohingegen der Kunde für die Art und Weise der Datenverarbeitung datenschutzrechtlich weiterhin uneingeschränkt verantwortlich bleibt. Um die ordnungsgemäße Datenverarbeitung im Auftrag abzusichern, ist darauf zu achten, dass eine ausreichend detaillierte und den Vorgaben von § 11 BDSG genügende schriftliche ADV mit dem Anbieter geschlossen wird. Dieser sollte einen entsprechenden Entwurf von sich aus vorlegen.

Nach der DS-GVO muss der Vertrag nicht mehr schriftlich abgeschlossen werden, es genügt auch die elektronische Form (Art. 28 Abs. 9 DS-GVO).

Der Kunde muss in der ADV unter anderem genau festlegen, auf welche Weise und wie lange der Anbieter die Daten verarbeiten und dass dies ausschließlich nach den Weisungen des Kunden erfolgen darf. Ferner ist der Kunde verpflichtet, die Einhaltung datenschutzrechtskonformer technischer und organisatorischer Schutzmaßnahmen durch den Anbieter wiederkehrend zu überprüfen.

Die ADV muss die folgenden Punkte enthalten:

6.3.1 Beschreibung von Gegenstand und Dauer

- Ist der Gegenstand der ADV nachvollziehbar beschrieben und ist die Dauer der ADV festgelegt?

Die ADV muss den Zweck der Datenverarbeitung für einen Dritten verständlich und abschließend wiedergeben. Dabei darf keine Datenverarbeitung auf Vorrat vereinbart werden; vielmehr müssen die derzeit vorgenommenen oder konkret geplanten Verarbeitungszwecke korrekt beschrieben und erfasst werden.

Des Weiteren muss die Dauer der ADV bestimmt werden. Sinnvollerweise wird die Dauer der ADV an die Laufzeit des Cloud-Vertrags gekoppelt.

6.3.2 Beschreibung der zu verarbeitenden Daten

- Welche Daten werden verarbeitet?
- Welche Personen sind betroffen?
- Sind besondere personenbezogene Daten betroffen?

Der Vertrag muss genau beschreiben, welche Datenkategorien verarbeitet werden (z.B. Name, Adresse, Telefonnummer etc.) und welche Personengruppen davon betroffen sind, also ob es sich z.B. um Kundendaten oder Beschäftigtendaten handelt. Besonders wichtig wird die detaillierte Beschreibung, wenn es um besondere Arten personenbezogener Daten geht (z.B. Gesundheitsdaten, vgl. § 3 Abs. 9 BDSG bzw. Art. 9 Abs. 1 DS-GVO).

6.3.3 Weisungsrecht des Kunden

- Sind Regelungen zur Einhaltung der Weisungen des Kunden getroffen?

Die Weisungsgebundenheit des Anbieters ist aufzunehmen und die Art der Weisungserteilung genau zu beschreiben. Die Gewährleistung der Weisungsbefugnis des Kunden ist das zentrale Element der Auftragsdatenverarbeitung. Kommt es zu Datenschutzverstößen oder Sicherheitspannen beim Anbieter, ist für die datenschutzrechtliche Haftung des Kunden entscheidend, dass dieser nachweisen kann, dass er den Auftragnehmer ordnungsgemäß angewiesen hat.

6.3.4 Kontrollrechte

- Sind dem Kunden ausreichende und durchsetzbare Kontrollrechte eingeräumt?

Die wirksame Datenverarbeitung im Auftrag setzt voraus, dass der Kunde vor Aufnahme der Datenverarbeitung den Anbieter unter datenschutzrechtlichen Gesichtspunkten sorgsam ausgewählt hat und dass er vor der Erteilung des Auftrags und auch danach regelmäßig kontrolliert, ob der Anbieter die gesetzlich geforderten technischen und organisatorischen Maßnahmen und die vertraglich vereinbarten Regelungen einhält. Dafür kann sich der Kunde ein Zutrittsrecht für die Räumlichkeiten des Anbieters einräumen lassen, zumindest im Sinne eines "Vorbehalt der Einzelfallkontrolle". Es ist jedoch nicht zwingend, dass der Kunde die Kontrollen vor Ort persönlich durchführt; vielmehr kann er damit externe Dritte beauftragen. Es empfiehlt sich eine klare Regelung zur Kostentragung insbesondere für den Fall, dass der Audit entsprechende Compliance-Verstöße oder sonstige Unzulänglichkeiten zutage fördert. In Zukunft wird die Vor-Ort-Kontrolle weitgehend durch das Vertrauen auf technische Zertifikate ersetzt, wenn solche Zertifikate auf einem nach der DS-GVO anerkannten Zertifizierungsstandard beruhen und von einer entsprechend akkreditierten Zertifizierungsstelle ausgestellt sind. Die Arbeiten der "Trusted Cloud" Initiative und des "TCDP Standard" haben hier eine Vorreiterrolle.

6.3.5 Umgang mit Betroffenenrechten

- Finden sich Regelungen zum Umgang mit Ansprüchen von Betroffenen auf Auskunft, Berichtigung, Löschung und Sperrung ihrer Daten?
- An wen kann sich der Betroffene wenden?

Jeder Betroffene einer Datenverarbeitung hat die unverzichtbaren Rechte auf Auskunft darüber, welche Daten über ihn gespeichert werden, auf Berichtigung der Daten, wenn diese falsch sind, und auf Löschung, wenn die Speicherung der Daten nicht mehr gerechtfertigt ist, weil die Rechtsgrundlage für eine länger andauernde Speicherung fehlt (z.B. wenn der Vertrag mit dem Betroffenen, zu dessen Zweck die Daten gespeichert wurden, seitens des Kunden erfüllt wurde). An die Stelle der Löschung tritt die Sperrung, wenn der Löschung gesetzliche Aufbewahrungspflichten der Kunden entgegenstehen.

Soweit der Kunde keine tatsächliche Verfügungsgewalt über die beim Anbieter gespeicherten Daten besitzt, ist entscheidend, dass in dem Vertrag vorgesehen ist, dass der Anbieter den Kunden bei der Beantwortung von Anfragen von Betroffenen unterstützt.

6.3.6 Technische und organisatorische Maßnahmen

- Regelt die ADV konkrete Schutzmaßnahmen gegen Zugriffe von unberechtigten Dritten auf den Datenbestand?
- Sind diese Maßnahmen im Einzelnen aufgezählt und verständlich beschrieben?
- Wie steht es insgesamt um Security?

Eine Voraussetzung für die rechtmäßige Auftragsdatenverarbeitung ist, dass der Anbieter die gesetzlich geforderten angemessenen Schutzmaßnahmen vorhält, um die Daten gegen Zugriffe unberechtigter Dritter zu schützen (sog. technische und organisatorische Maßnahmen gemäß § 9 Satz 1 BDSG i.V.m. Anlage zu § 9 BDSG bzw. gemäß Art. 28 Abs. 1 DS-GVO)). Im BDSG sind die zu ergreifenden Maßnahmen katalogartig aufgelistet, wobei die Maßnahmen in der ADV jeweils noch weiter zu spezifi-

zieren sind. Die technischen und organisatorischen Maßnahmen sollten für Dritte und insbesondere die Aufsichtsbehörden nachvollziehbar und kontrollierbar beschrieben werden. In der Praxis wird diese Auflistung typischerweise als Anlage zur ADV genommen.

Datensicherheit ist – über den Bereich des Schutzes personenbezogener Daten hinaus – eine zentrale Schutzthematik in jedem Dienstleistervertrag und bei Cloud-Diensten allemal. Neben angemessenen Schutzmaßnahmen sind auch die vertraglich Absicherung von Disaster Recovery Maßnahmen von zentraler Bedeutung. Es empfiehlt sich, dem Vertrag ggf. entsprechende Sicherheitskonzepte beizufügen, damit der Umfang der vom Anbieter zu treffenden Maßnahmen nicht im Streitfall hinreichend klar beschrieben ist.

6.3.7 Unterauftragsverhältnisse

- Enthält die ADV eine Regelung zu Unterauftragnehmern?
- Werden bestimmte Unterauftragnehmer bereits konkret benannt?

Als verantwortliche Stelle ist der Kunde gesetzlich verpflichtet, die Kontrolle über die Datenverarbeitung zu behalten. Aus diesem Grund dürfen die Daten nicht ohne weiteres an sonstige Auftragnehmer ohne das Wissen des Kunden weiter übergeben werden. Der Kunde muss mit dem Auftragnehmer in der ADV daher eine Regelung zu den Voraussetzungen der Einbeziehung von Unterauftragnehmern treffen.

Der Regelungsinhalt kann hier im Einzelnen variieren: Jede Einbeziehung eines Unterauftragnehmers kann an die Zustimmung oder zumindest die Information des Kunden geknüpft werden. Nach der Auffassung der Datenschutzbehörden muss jede Einbeziehung eines Unterauftragsnehmers von der Zustimmung des Auftraggebers abhängig gemacht werden. Bestimmte Unterauftragnehmer können bereits namentlich im Vertrag benannt werden. In jedem Fall muss der Aufragnehmer (d.h. der Cloud-Anbieter) sich dazu verpflichten, mit jedem Unterauftragnehmer eine der ADV entsprechende Unterauftragsdatenverarbeitungsvereinbarung abzuschließen. Zusätzliche Komplexität erlangt dieser Punkt, wenn der Auftragnehmer oder ein Unterauftragnehmer außerhalb von EU/EWR sitzt.

Nach der DS-GVO bedarf die Einbeziehung von Unterauftragnehmern einer gesonderten oder allgemeinen schriftlichen Genehmigung. Soweit der Auftraggeber (Kunde) eine allgemeine Genehmigung erteilt hat, hat der Auftragnehmer (Cloud-Anbieter) die Pflicht, den Auftraggeber über jede Änderung in Bezug auf Ersetzung und Hinzuziehung eines Unterauftragnehmers zu informieren. Der Auftraggeber erhält das Recht, gegen diese Änderung Einspruch zu erheben (Art. 28 Abs. 2 DS-GVO).

6.3.8 Informationspflichten bei Datensicherheitspannen

- Regelt der Vertrag die Pflicht des Anbieters, den Kunden bei Datensicherheitspannen sofort zu informieren?

Gelangen bestimmte besonders geschützte Daten (z.B. Kreditkartendaten oder Gesundheitsdaten) an die Öffentlichkeit oder ist ein Zugriff durch nichtberechtigte Dritte möglich, dann ist der Kunde als verantwortliche Stelle gem. § 42a BDSG dazu verpflichtet, die Betroffenen sowie die verantwortliche Aufsichtsbehörde darüber unver-

züglich zu informieren. Weitergehende gesetzliche Benachrichtigungspflichten treffen zudem die Anbieter von Telekommunikationsdiensten oder Telemediendiensten.

Nach der DS-GVO ist die Schwelle zur Meldepflicht im Fall einer Datenschutzverletzung heruntergesetzt: Auf die Art der Daten kommt es für das Eingreifen der Meldepflicht nicht mehr an. Entscheidend ist nur, ob die Datenschutzverletzung zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Je nach Größe des Risikos muss die Meldung entweder (nur) gegenüber der Behörde erfolgen, oder zusätzlich gegenüber den Betroffenen.

Ein Datenleck wird typischerweise zuerst vom Anbieter erkannt, weil dieser die Daten verwaltet. Deshalb muss vertraglich geregelt sein, dass der Anbieter den Kunden im Fall eines Verdachts auf eine Datensicherheitspanne unverzüglich informieren muss, damit der Kunde seine gesetzlichen Benachrichtigungspflichten erfüllen kann. Die Regelung einer Frist, innerhalb derer der Anbieter die Datensicherheitspanne dem Kunden melden muss, sollte allenfalls ergänzend vereinbart werden, da der Anbieter von Gesetzes wegen „unverzüglich" informieren muss, was im Einzelfall bereits innerhalb weniger Stunden bedeuten kann.

Darüber hinaus sollte geregelt werden, dass sich der Anbieter als weisungsgebundener Vertragspartner des Kunden nicht direkt an die Behörden oder Betroffenen wenden darf.

6.3.9 Rückgabe der Daten nach Beendigung des Auftrags

- Finden sich ausreichende Regelungen zur Herausgabepflicht des Anbieters der für den Kunden in der Cloud gehaltenen Daten?
- Hat der Kunde ein Recht, die Löschung mitsamt Löschungsnachweis zu verlangen?

Nach Beendigung des Vertrags ist zu gewährleisten, dass der Anbieter die Daten wieder an den Kunden in einem allgemein verwendbaren Format herausgibt, da ab diesem Zeitpunkt der Anbieter keine Berechtigung mehr hat, die Daten bei sich vorzuhalten. An die Stelle der Rückgabe kann die Löschung der Daten durch den Anbieter treten, sofern der Kunde dies verlangt. Die Löschung ist sodann durch den Anbieter dem Kunden zu bestätigen.

Praxishinweis:
Als verantwortliche Stelle haften Sie für die Einhaltung der Datenschutzgesetze. Verstöße können zu empfindlichen Bußgeldern führen. Daher empfiehlt sich eine sorgfältige Überprüfung, ob alle organisatorischen und materiell-rechtlichen Regelungen zur Wahrung des Datenschutzes eingehalten sind. Achten Sie auf ausreichende Dokumentation und Information durch Ihren Anbieter!

6.4 Übermittlung von personenbezogenen Daten ins EU/EWR-Ausland?

- Wo werden Daten verarbeitet?
- Gibt es Regelungen zu der Übermittlung von Daten in andere Länder? Sind die Empfänger-Staaten ausdrücklich benannt?

Der Kunde sollte zunächst in Erfahrung bringen, in welchen Ländern die Daten gespeichert und verarbeitet werden. Sodann ist zu prüfen, ob die geplante Datenübermittlung ins EU/EWR-Ausland datenschutzrechtlich zulässig ist.

6.5 Ist die Übermittlung ins EU/EWR-Ausland datenschutzrechtlich zulässig?

- Ist die geplante Übermittlung ins EU/EWR-Ausland überhaupt zulässig? Gelten besondere Zulässigkeitsvoraussetzungen?

Für die Übermittlung von Daten in sog. Drittländer, d.h. Staaten außerhalb der EU/des EWR, gelten besonders hohe Anforderungen.

Es ist eine zweistufige Prüfung vorzunehmen, ob ein solcher Transfer zulässig ist:

Zum einen muss für die Übermittlung der Daten eine gesetzliche Erlaubnis oder die Einwilligung der Betroffenen vorliegen.

Zum anderen ist sicherzustellen, dass für die Verarbeitung der Daten ein aus EU-Sicht angemessenes Datenschutzniveau erreicht wird. Für bestimmte Staaten hat die Europäische Kommission dies verbindlich festgestellt (derzeit gilt dies für Andorra, Argentinien, Australien, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Kanada (für den nicht-öffentlichen Bereich), Schweiz, Uruguay und Neuseeland). Für alle anderen Staaten, die nicht Mitglied der EU oder des EWR sind, lässt sich ein angemessenes Datenschutzniveau nur durch zusätzliche Maßnahmen herstellen. In Betracht kommen insbesondere der Abschluss der von der Europäischen Kommission veröffentlichten Standardvertragsklauseln oder (für US-Anbieter) eine EU-US Privacy Shield Zertifizierung (unter Beachtung der von den deutschen Aufsichtsbehörden aufgestellten zusätzlichen Anforderungen). Da die europäische Rechtsprechung sich immer wieder mit internationalen Datentransfers befasst, ist regelmäßig zu überprüfen, ob die gewählten rechtlichen Absicherungen zum Datentransfer aus der EU bzw. dem EWR noch tragfähig sind.

Sämtliche erforderlichen Maßnahmen sind vor, spätestens aber zeitgleich mit dem Gang in die Cloud umzusetzen.

Zu beachten ist auch, dass nach überwiegender Ansicht der Aufsichtsbehörden besondere personenbezogene Daten im Sinne des § 3 Abs. 9 BDSG bzw. Art. 9 Abs. 1 DS-GVO (z.B. Gesundheitsdaten) nur mit entsprechender Einwilligung der Betroffenen in Drittländer transferiert werden dürfen.

6.6 Sanktionen

Verstöße gegen datenschutzrechtliche Bestimmungen können nach dem BDSG mit Bußgeldern von nunmehr bis zu 50.000,00 EUR bei einfacheren Ordnungswidrigkeiten, bei schwererwiegenden Ordnungswidrigkeiten wie unbefugter Datenerhebung und Verarbeitung mit bis zu 300.000,00 EUR geahndet werden. Übersteigt der wirtschaftliche Vorteil, den ein Täter aus der Ordnungswidrigkeit gezogen hat, diesen Betrag, so sind sogar höhere Bußgelder möglich und der gesamte Überschuss wird abgeschöpft (§ 43 BDSG).

Die DS-GVO sieht einen wesentlich schärferen Sanktionsrahmen vor: Bußgelder können bis zu EUR 20 Mio. oder 4% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens betragen (Art. 83 DS-GVO).

6.7 IT-Sicherheit

- Erfüllt der Anbieter IT-sicherheitsrechtliche Anforderungen?

Kunden sind gesetzlich verpflichtet, ihre IT-Systeme gegen unberechtigte Zugriffe Dritter zu schützen. Diese Verpflichtung ergibt sich aus datenschutzrechtlicher Sicht aus § 9 Satz 1 BDSG i.V.m. Anlage zu § 9 BDSG bzw. Art. 32 DS-GVO. Weitere IT-sicherheitsrechtliche Verpflichtungen ergeben sich z.B. aus § 13 TMG, der sich an Anbieter geschäftsmäßig angebotener Telemedien richtet, nach dem BSIG für Betreiber „kritischer Infrastrukturen“ und nach dem TKG für Anbieter von Telekommunikationsdienstleistungen. Bei der Umsetzung der Verpflichtung ist der Stand der Technik zu berücksichtigen. Die Ermittlung des Standes des Technik ist in erster Linie eine technische, weniger eine juristische Aufgabe.

Vor diesem Hintergrund ist es von besonderer Bedeutung, einen Anbieter auszuwählen, der über entsprechende Nachweise der *IT Sicherheit etwa aufgrund geeigneter Zertifizierungen verfügt. Eine Zertifizierung i.S.d. Art. 42, 43 DS-GVO ist in Zukunft ein maßgeblicher Anhaltspunkt dafür, dass der Anbieter seinen datenschutzrechtlichen Verpflichtungen zur Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen nachkommt.*

Die Zertifizierung des Anbieters sollte vertraglich vereinbart werden, einschließlich der Verpflichtung des Anbieters, die Zertifizierung aufrechtzuerhalten. Soweit eine Zertifizierung nicht vorliegt oder nicht ausreichend ist, sollte ein einheitlich hohes Datensicherheitsniveau entsprechend den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vereinbart werden (siehe etwa Sicherheitsempfehlungen für Cloud Computing Anbieter).

7. Preisanpassung

- Wie lange gelten die vereinbarten Preise?

- Wenn eine Preisanpassungsklausel in dem Vertrag enthalten ist: Ist diese transparent und angemessen?

Standardverträge von Anbietern enthalten oft Preisanpassungsklauseln, die dem Anbieter eine Erhöhung der Preise ermöglichen oder nach denen sich die vereinbarten Preise evtl. sogar automatisch erhöhen. Das Ziel des Kunden muss es natürlich sein, die Preise für die Dauer der Laufzeit fix zu vereinbaren. Sollte dies nicht durchsetzbar sein, ist für den Kunden allenfalls eine gedeckelte Preiserhöhung nach Ablauf eines bestimmten Zeitraums oder ein Inflationsausgleich (Indexklausel) akzeptabel. Mit Blick auf Skaleneffekte und dies sich über Zeit verringernden Stückkosten der IT ist zudem über Preisüberprüfungsklauseln (Benchmarking) nachzudenken.

8. Geheimhaltung

- Werden Know-how und vertrauliche Unternehmensdaten ausreichend geschützt?

- Finden sich ausreichende Geheimhaltungspflichten des Anbieters?

Der Cloud-Vertrag muss Regelungen enthalten, durch die sich der Anbieter zur Geheimhaltung verpflichtet. Anbieter verarbeiten oftmals die Datenbestände von mehreren Kunden, die im Wettbewerbsverhältnis zueinander stehen können. Der Vertrag muss die Geschäftsinteressen des Kunden ausreichend vor einer Offenlegung gegenüber anderen Kunden und sonstigen Dritten schützen. Im Regelfall wird eine Verletzung der Geheimhaltungspflicht mit einer Vertragsstrafe belegt.

9. Beendigung des Vertrages

9.1 Kündigungsregelungen

- Sind ausreichend flexible Kündigungsrechte eingeräumt, damit der Kunde sich bei Bedarf von dem Anbieter lösen kann?

Der Kunde sollte darauf achten, dass er den Vertrag bei Bedarf kurzfristig kündigen kann, um sich die nötige Flexibilität für seine Planung zu erhalten. Es ist dabei – wie bei jedem Dauerschuldverhältnis – zwischen ordentlichen und außerordentlichen Kündigungsrechten bzw. Sonderkündigungsrechten zu unterscheiden. Kommt es dem Kunden darauf an, sich von einem Vertrag mit längerer Laufzeit in bestimmten Konstellationen vorzeitig lösen zu können, so muss er entsprechende Sonderkündigungsrechte verhandeln. Es spricht einiges dafür, die Kündigungsrechte im Vertrag asymmetrisch auszugestalten.

9.2 Exit-Management

- Ist sichergestellt, dass der Kunde beim Ausstieg an seine Daten herankommt?

- Wer hält die Rechte an den Daten? Ist verankert, dass der Anbieter die Daten nach Vertragsbeendigung herausgibt? Ist eine saubere Löschung der Daten beim Ausstieg des Kunden geregelt? Kann der Kunde die Bestätigung der Löschung verlangen?

Der Kunde sollte darauf achten, dass der Vertrag seine Interessen im Beendigungsszenario ausreichend schützt und absichert. Entscheidend ist, dass der Anbieter verpflichtet ist, die herauszugebenden Daten ausreichend lange und in einem für den Kunden verwendbaren Format vorzuhalten und ggf. auch bei der Übertragung der Daten an den Kunden oder einen anderen Dienstleister aktiv mitzuwirken. Es kann angemessen sein, dass der Anbieter dafür eine gesonderte Vergütung verlangt.

Außerdem muss der Anbieter verpflichtet sein, sämtliche bei ihm vorhandene Daten nach Beendigung des Vertrages und der Abwicklung der Herausgabe sicher und dauerhaft zu löschen und eine solche Löschbarkeit schon beim technologisch Lösungsansatz für den angebotenen Dienst zu implementieren ("privacy by design"). Der Kunde sollte unbedingt den Nachweis der sicheren Löschung der Daten verlangen. Allerdings sollte die Löschung (einschließlich etwaiger Back-ups) nach einer vorbestimmten, hinreichend langen Frist erfolgen, so dass sich der Kunde darauf einrichten kann, eine Migration seiner Datenbestände durchzuführen.

Denkbar ist, dass die in der Cloud gespeicherten Daten als Datenbank urheberrechtlich oder leistungsschutzrechtlich schutzfähig sind. Liefert der Kunde beispielsweise

Rohdaten bzw. eine zu bearbeitende Datenbank, so ist nicht auszuschließen, dass mit der Bearbeitung/Strukturierung der Rohdaten bzw. mit Weiterentwicklung einer Datenbank u.U. der Provider (und nicht der Kunde) als Hersteller der Datenbank die Rechte an dieser erwirbt. Im Vertrag sollte daher zumindest klarstellend geregelt werden, dass alle etwaigen Rechte an den Daten dem Kunden zustehen.

9.3 Datenexport/-import

- Ist geregelt, in welchen Datenformaten die Daten von dem Anbieter an den Kunden oder einen übernehmenden Drittanbieter zu übergeben sind?

Der erfolgreiche Export in der Cloud gespeicherter Daten aus einer Cloud-Lösung bei Vertragsende sowie ihr Import in ein anderes System (des Kunden oder eines neuen Anbieters) bedeuten oft eine wesentliche tatsächliche Herausforderung. Das Exit-Szenario sollte daher unbedingt bereits bei Vertragsschluss durchdacht und vertraglich detailliert abgebildet werden. Dazu gehören konkrete Regelungen zum technischen Format, in dem die Daten herauszugeben sind, ebenso wie Regelungen zur Modalität der Datenherausgabe (typischerweise per Download, evtl. aber auch auf einem physischen Datenträger). Je nach technischer Gestaltung kann die Definition der für einen Datenexport verwendeten Schnittstelle sinnvoll sein.

Um im Voraus abzusichern, dass der Anbieter die Daten bei Vertragsende (oder ggf. auf Verlangen des Kunden auch vorher) herausgeben kann, sollte der Anbieter bereits während der Vertragslaufzeit zu einem regelmäßigen Back-up der Daten des Kunden verpflichtet werden.

Die regelmäßige Back-up Verpflichtung hilft auch in dem Fall, dass die Daten des Kunden beim Anbieter beschlagnahmt werden. In einem solchen Falle ist es wichtig zu gewährleisten, dass der Geschäftsbetrieb ungestört fortgeführt werden kann und die Daten weiterhin verfügbar sind.

Praxishinweis:
Achten Sie darauf, dass die Regelungen sowie die tatsächlichen technischen Gegebenheiten Ihnen nach Möglichkeit ein einfaches "Plug&Pull" ermöglichen, damit Sie nicht von einem Anbieter abhängig werden.

9.4 Beispielklausel

Herausgabe von Daten bei Beendigung des Vertrags

Die folgenden Bestimmungen finden immer dann Anwendung, wenn dieser Vertrag endet oder rückabgewickelt wird, unabhängig davon, aus welchem Grund dies erfolgt, also etwa bei Auslaufen des Vertrags, bei ordentlicher oder außerordentlicher Kündigung oder im Falle eines Rücktritts.

1. Erbringung von Unterstützungsleistungen

Auf Verlangen des Kunden erbringt der Anbieter alle zu einer erfolgreichen Datenübermittlung an den Kunden oder einen vom Kunden bestimmten Dienstleister erforderlichen und angemessenen Unterstützungsleistungen.

2. Datenherausgabe/ -löschung

Bei Beendigung des Vertrages gibt der Anbieter dem Kunden alle Daten lesbar und vollständig heraus, die der Anbieter vom Kunden im Zusammenhang mit dem Vertrag erhalten hat. Das Format der Daten

wird [in einer Anlage zum Cloud-Vertrag] zwischen dem Kunden und dem Auftraggeber vereinbart. Der Anbieter hat die Daten auf Anforderung des Kunden entweder auf einem von dem Kunden spezifizierten Datenträger oder per Datenfernübertragung herauszugeben.

Nach Beendigung des Vertrags und Abwicklung der Datenherausgabe wird der Anbieter sämtliche bei ihm verbliebene Kopien und Daten löschen bzw. vernichten und dem Kunden die Löschung/Vernichtung schriftlich bestätigen.

Ein Zurückbehaltungsrecht steht dem Anbieter hinsichtlich der Daten des Kunden nicht zu.

Alle etwaigen Rechte an Daten, die während der Vertragslaufzeit auf Veranlassung des Kunden beim Anbieter gespeichert oder von ihm verarbeitet werden, stehen im Verhältnis zwischen dem Kunden und dem Anbieter während der gesamten Vertragslaufzeit allein und ausschließlich dem Kunden zu.

10. Sub-Unternehmer-Regelungen

- Ist bereits festgelegt, welche Sub-Unternehmer eingesetzt werden sollen? Sind die zur Leistungserbringung eingesetzten Sub-Unternehmer bekannt?

- Kann der Kunde dem Einsatz von Sub-Unternehmern widersprechen, z.B. wenn es sich um Wettbewerber von ihm handelt?

In den meisten Fällen wird ein Anbieter seinerseits mit weiteren Anbietern (z.B. von externen Serverkapazitäten) arbeiten und diese als Sub-Unternehmer einsetzen. Da solche Sub-Unternehmer oftmals als fester Bestandteil in das Geschäftsmodell des Anbieters eingebunden (und auch eingepreist) sind, ist ein Zustimmungsvorbehalt des Kunden regelmäßig nicht durchsetzbar. Dennoch sollte dem Kunden zumindest eine Kontrollmöglichkeit hinsichtlich der Lokalität der Daten und Serverstandorte eingeräumt werden und die Gruppe der in Frage kommenden Sub-Unternehmer eingegrenzt werden. In jedem Fall sollte die Sourcing-Strategie des Anbieters transparent dargestellt sein. Bindet der Anbieter Sub-Unternehmer ein, so ist darauf zu achten, dass der Anbieter vertragliche Verpflichtungen (z.B. in Bezug auf den Datenschutz) an seinen Sub-Unternehmer weitergibt und ihn darauf verpflichtet.

Das gilt insbesondere mit Blick auf die datenschutzrechtlichen Vorgaben für den Transfer von Daten in Drittländer außerhalb der EU/des EWR (dazu ausführlich oben unter Ziffer 6).

11. Haftung

- Enthält der Vertrag unangemessene Haftungsbeschränkungen?

Nach deutschem Recht haftet der Anbieter grundsätzlich für alle Schäden, die durch sein Verschulden (d.h. vorsätzlich oder fahrlässig) verursacht werden. Die unbeschränkte gesetzliche Verschuldenshaftung ist der gesetzliche Ausgangspunkt für vereinbarte Haftungsbeschränkungen oder Ausschlüsse.

In Allgemeinen Geschäftsbedingungen können Anbieter ihre gesetzliche Haftung nur in sehr begrenztem Umfang durchsetzbar beschränken: Gerichtlich durchsetzbar ist lediglich die Beschränkung der Haftung für leichte (einfache) Fahrlässigkeit. Eine Beschränkung der Haftung für grobe Fahrlässigkeit oder Vorsatz ist unwirksam. Im Rahmen der leichten Fahrlässigkeit sind (lediglich) folgende Beschränkungen wirksam:

- *Beschränkung der Haftung für die leicht fahrlässige Verletzung von sog. wesentlichen Vertragspflichten/Kardinalpflichten, wobei diese im Vertrag begrifflich zu definieren sind, auf den Ersatz des zum Zeitpunkt des Vertragsschlusses "typischerweise vorhersehbaren Schaden"; sowie*

- *Ausschluss der Haftung für die fahrlässige Verletzung von nicht-wesentlichen Vertragspflichten.*

Soweit ein Standardvertrag eines Anbieters eine Haftungsbeschränkung vorsieht, die über die vorstehend genannten Beschränkungen hinausgeht, ist die entsprechende Haftungsbeschränkung nach deutschem Recht typischerweise unwirksam.

Soweit Haftungshöchstgrenzen mit dem Anbieter vereinbart werden (Haftungs-Caps), ist kundenseitig unbedingt zu prüfen, ob die vom Anbieter vorgesehene Höchstgrenze den konkreten Schadensrisiken der spezifischen Situation gerecht wird oder zu gering bemessen ist.

Achtung:
Haftungsklauseln sind oft komplex und für den juristischen Laien kaum in ihrer vollen Auswirkung zu erfassen. Gerade im Bereich der Haftung weichen die Interessen des Anbieters typischerweise erheblich von denen des Kunden ab. Achten Sie deshalb unbedingt darauf, dass Sie für den Schadensfall hinreichend abgesichert sind.

12. Versicherungspflicht für Anbieter

- Verpflichtet sich der Anbieter zum Abschluss einer Versicherung für etwaige Schäden bei Kunden?

- Wenn ja, reicht die Deckungssumme für den Schaden aus, der im Haftungsfall beim Kunden typischerweise entstehen kann?

Ausreichender Versicherungsschutz des Anbieters ist insbesondere bei der Verlagerung größerer Funktionsbereichen in die Cloud unabdingbar und sollte vertraglich verankert werden. Dabei sollte der Kunde prüfen, ob die angegebene Versicherungssumme ausreichend hoch ist, um die im konkreten Szenario typischerweise zu befürchtenden Schäden abzudecken. Ist dies nicht der Fall, sollte ggf. über eine Erhöhung verhandelt werden.

13. Sachmängel

Nach deutschem Recht haftet der Anbieter für die Fehlerfreiheit der zu erbringenden Dienste während der Laufzeit des Cloud-Vertrags im Ausgangspunkt nach mietrechtlichen Grundsätzen. Dies bedeutet, dass der Anbieter grundsätzlich für Sachmängel sowie für Rechtsmängel des Dienstes einzustehen hat.

Ein Sachmangel eines Cloud-Dienstes liegt vor, wenn dieser nachteilig von der vertraglich vereinbarten Beschaffenheit abweicht. Die Tauglichkeit zu dem von den Vertragsparteien vereinbarten vertraglichen Gebrauch muss aufgehoben oder gemindert sein. Dabei bleiben nur unerhebliche Abweichungen außer Betracht.

Stellt der Anbieter den Dienst nicht mängelfrei zur Verfügung, so gibt das Gesetz dem Kunden bestimmte Mängelrechte an die Hand. Diese umfassen die angemessene

Minderung der Vergütung sowie unter bestimmten Voraussetzungen Rücktritt und Schadensersatz.

Da in der Praxis oftmals die Schwierigkeit der genauen vertraglichen Typisierung eines Cloud-Dienstes besteht, ist es dringend zu empfehlen, die Mängelrechte vertraglich zu regeln, um für die Vertragsparteien Klarheit zu schaffen. Dabei ist insbesondere daran zu denken, das Verhältnis zwischen SLAs und Mängelrechten eindeutig zu regeln. Der Anbieter wird meist versuchen, den Kunden für den Fall einer Unterschreitung der Service Levels ausschließlich auf die im SLA vereinbarten Vertragsstrafen zu verweisen und darüber hinausgehende Minderungsansprüche (oder sogar Mängelansprüche überhaupt) auszuschließen. Dies mag für den Kunden im Einzelfall kalkulierbar und akzeptabel sein, soweit es um Mängel geht, die gerade in der Unterschreitung eines Service Levels liegen und sofern das Rücktrittsrecht des Kunden unberührt bleibt (oder an das wiederholte Auftreten entsprechender Mängel außerordentliche Kündigungsrechte des Kunden geknüpft sind).

Praxisrelevanter wird die Frage nach Mängelansprüchen in Fehlerkonstellationen, die keinen konkret vereinbarten Service Level verletzen. Es ist daher wesentlich, dass der Kunde zumindest für derartige Konstellationen seine gesetzlichen Mängelansprüche behält.

14. Schutzrechte Dritter / Freistellung

14.1 Rechtsmängel

- Steht der Anbieter dafür ein, dass die bereitgestellte Software frei von Rechten Dritter ist?

Wie bereits dargestellt, haftet der Anbieter nach deutschem Recht während der Laufzeit des Cloud-Vertrags grundsätzlich für die Sach- und Rechtsmängelfreiheit des Cloud-Service, d.h. auch für die Freiheit von Rechten Dritter.

Ein Rechtsmangel liegt vor, wenn dem Kunden der vertragsgemäße Gebrauch des Cloud-Dienstes durch das Recht eines Dritten ganz oder teilweise entzogen wird, beispielsweise, wenn der Anbieter nicht die notwendigen Rechte zur Bereitstellung der Software als Cloud-Dienst hat.

Im Falle eines Rechtsmangels hat der Kunde nach deutschem Recht grundsätzlich die gleichen Rechtsbehelfe wie bei einem Sachmangel, nämlich Minderung sowie unter bestimmten Voraussetzungen Rücktritt sowie Schadensersatz. Enthält der Vertrag für den Fall von Rechtsmängeln eine hinreichende Freistellungsklausel (dazu sogleich), ist eine separate Regelung zu den gesetzlichen Mängelrechten für den Kunden daneben typischerweise entbehrlich.

14.2 Freistellung

- Verpflichtet sich der Anbieter, den Kunden von Ansprüchen Dritter freizustellen?

Nach dem Vorbild US-amerikanischer Verträge ist es auch hierzulande inzwischen üblich, dass der Anbieter den Kunden von Ansprüchen Dritter wegen der Verletzung von IP-Rechten freistellt. Der Kunde sollte daher darauf achten, dass der Vertrag für den

Fall von Rechtsmängeln eine umfassende Freistellungsklausel zugunsten des Kunden enthält.

Es ist dabei interessengerecht, wenn dem Kunden gewisse Mitwirkungspflichten bei der Verteidigung gegen die Inanspruchnahme durch Dritte auferlegt werden. Auch ist es üblich, dass der Kunde im Falle seiner Inanspruchnahme durch einen Dritten den Anbieter umgehend zu informieren hat.

Das nachfolgende Textbeispiel gibt eine Orientierung, wie eine individuell verhandelte Freistellungsklausel in der Praxis aussehen kann:

1. Freistellung
1.1 Der Auftragnehmer garantiert, dass die von ihm erbrachten Dienste frei von Schutzrechten Dritter sind und keine sonstigen Rechte Dritter verletzt werden.
1.2 Macht ein Dritter geltend, dass die Inanspruchnahme des Dienstes durch den Auftraggeber ein Urheberrecht, Patentrecht, Markenrecht, Geschmacksmusterrecht, Gebrauchsmusterrecht und/oder ein sonstiges Schutzrecht des geistigen Eigentums (nachfolgend: "Schutzrechte Dritter") verletzt, hat der Auftragnehmer auf seine Kosten nach Wahl des Auftraggebers diesem entweder das Recht zur Nutzung des Dienstes zu verschaffen oder den betroffenen Dienst bei Aufrechterhaltung [des Qualitätsstandards und Erfüllung aller Anforderungen gemäß dem SLA] derart zu ändern oder zu ersetzen, dass er keine Schutzrechte Dritter mehr verletzt.
1.3 Der Auftragnehmer verpflichtet sich, den Auftraggeber ferner von sämtlichen Ansprüchen freizustellen, die Dritte wegen Schutzrechtsverletzungen gegen den Auftraggeber geltend machen, sowie dem Auftraggeber sämtliche Aufwendungen und Schäden zu ersetzen, die dem Auftraggeber aus der Geltendmachung derartiger Ansprüche entstehen.
Eventuell:
1.4 *Der Auftragnehmer ist berechtigt und verpflichtet, alle Rechtsstreitigkeiten, die sich aus der Geltendmachung derartiger Ansprüche ergeben, auf eigene Kosten zu führen. Der Auftraggeber ist verpflichtet, den Auftragnehmer unverzüglich über geltend gemachte Ansprüche in Kenntnis zu setzten. Er ist dem Auftragnehmer gegenüber zur Unterstützung im angemessenen Umfang verpflichtet.*

15. Schulungen

Bei Cloud-Diensten ist, anders als bei der Implementierung von Software im Unternehmen selbst, Schulungs-Know-how beim Kunden typischerweise nur im Sinne der Anwenderschulung erforderlich, da der Betrieb der Software gerade beim Anbieter liegt. Es ist bei Bedarf darauf zu achten, dass gegebenenfalls Einführungsschulungen für die Anwender der Software verfügbar sind.

* * *

Kontakt:

Kanzlei Bird & Bird LLP
Dr. Henriette Picot
Partner
Email: henriette.picot@twobirds.com
www.twobirds.com

VOICE - Bundesverband der IT-Anwender e.V.
Patrick Quellmalz
Email: patrick.quellmalz@voice-ev.org
www.voice-ev.org