Checkliste mit Erläuterungen für Cloud Computing-Verträge

für Software as a Service in der Public Cloud
im B2B-Geschäftsverkehr

BITKOM

Impressum

Herausgeber: BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner: Thomas Kriesel, Tel.: 030.27576-146, t.krieselbitkom.org

Gestaltung / Layout: Design Bureau kokliko / Matthias Winter (BITKOM)

Titelbild: © Jakub Jirsák – Fotolia.com

Checkliste mit Erläuterungen für Cloud Computing-Verträge

für Software as a Service in der Public Cloud im B2B-Geschäftsverkehr

Inhaltsverzeichnis

Danksagung

Die vorliegende Checkliste zur Gestaltung von Cloud Computing-Verträgen ist eine Publikation des BITKOM-Arbeitskreises »ITK-Vertrags- und Rechtsgestaltung«. Der Arbeitskreis besteht aus Experten der BITKOM-Mitgliedsunternehmen und befasst sich mit Fragen rund um Vertragsgestaltung und -abwicklung in der ITK-Branche.

Für die Mitarbeit an diesem Leitfaden danken wir folgenden Personen, die mit ihrer Expertise und wertvollen praktischen Erfahrung die Erstellung der vorliegenden Publikation möglich gemacht haben:

- Alexandra Deutschendorf, Atos Worldline GmbH
- Jens Konradi, T-Systems International GmbH, stellvertretender Vorsitzender des Arbeitskreises
- Claudia Riffer, Deutsche Telekom AG
- Martin Schweinoch, SKW Schwarz Rechtsanwälte, Vorsitzender des Arbeitskreises
- Dr. Christian Weitzel, Harder Rechtsanwälte
- Oliver Zigan, I.T.E.N.O.S. GmbH

Im Übrigen danken wir für ihre wertvollen Hinweise:

- Dr. Alexander Duisberg, Bird & Bird LLP
- Martin Erben, SAP AG
- Nicolas Hamers, Sage Software GmbH
- Christof Höfner, Vistaprint Schweiz GmbH
- Christoph Stieler, SAP AG
- Olaf Vogel, Deutsche Telekom AG
- Dagmar Ueberfeldt-Lang, Sage Software GmbH

Besonderer Dank gebührt Rechtsanwalt und Steuerberater Thomas Kriesel, dem zuständigen Bereichsleiter des BITKOM, der mit großem Engagement und ebenso großer Ausdauer die Erarbeitung dieser Checkliste begleitet und stets konstruktiv unterstützt hat.

Anregungen zu dieser Checkliste zur Gestaltung von Cloud Computing-Verträgen richten Sie bitte an die Hauptgeschäftsstelle des BITKOM, Thomas Kriesel, oder an den Vorsitzenden des Arbeitskreises, RA Martin Schweinoch.

Berlin, Juli 2014

Martin Schweinoch
Vorsitzender des Arbeitskreises ITK-Vertrags- und Rechtsgestaltung

1 Einführung

1.1 Vorbemerkungen

Regelungen in Cloud-Verträgen können in vier grundlegende Kategorien unterteilt werden:

- Beschreibung der angebotenen Cloud-Leistung (Leistungsbeschreibung, Nutzungsumfang),
- Definition der Leistungsgüte und Folgen unzureichender Leistungserbringung (Service Levels),
- kaufmännische Parameter (Vergütung, Laufzeit, Vergütungsparameter und Vergütungsanpassung) und
- sonstige Regelungen (z. B. Verzug, Gewährleistung, Haftung, Rechtswahl, Datenschutz).

Diese unterschiedlichen, miteinander in Wechselwirkung stehenden Regelungsfelder sollten in einem Cloud-Vertrag abgedeckt sein und werden in dieser Checkliste dargestellt und kurz erläutert. Der Aufbau dieser Checkliste folgt jedoch nicht dieser Kategorisierung, sondern der Abfolge einer typischerweise in der Praxis verwendeten Vertragsgliederung.

! Hinweis zum Gebrauch dieser Checkliste:
Nach einer kurzen Einführung in die vertragsrechtliche Systematik von Cloud-Verträgen (Kapitel 1) werden die empfohlenen Regelungsinhalte für Cloud-Verträge als Stichworte in Form einer Checkliste aufgezählt (Kapitel 2). Die Stichworte werden in Kapitel 3 kurz erläutert. Einige besonders relevante Regelungsbereiche werden dann in Kapitel 4 weiter vertieft.

Der Darstellung in dieser Checkliste wird das Modell eines Vertrages über den Bezug von Software as a Service (SaaS) aus einer Public Cloud zugrunde gelegt. Das Geschäftsmodell SaaS ist in der hier zugrunde gelegten Ausgestaltung dadurch gekennzeichnet, dass der Anbieter in seiner Verantwortung gewartete Anwendungsprogramme in standardisierter Art und Weise bereitstellt. Dabei richtet sich sein Angebot an eine unbestimmte Vielzahl von Kunden und soll als Massengeschäft abgewickelt werden. Der Anbieter kann also typischerweise besondere Anforderungen einzelner Kunden nicht berücksichtigen. Der Anbieter betreut die bereit gestellten Anwendungen und die zugehörige Infrastruktur. Der Kunde kümmert sich darum, die für ihn spezifische Konfiguration einzurichten.

! Hinweis zum Anwendungsbereich dieser Checkliste:
Diese Checkliste gibt Hinweise für die Gestaltung eines Vertrages zwischen Unternehmen (B2B) zum Bezug einer Software aus einer Public Cloud im Massengeschäft. Für andere Cloud-Geschäftsmodelle sind eventuell abweichende oder zusätzliche Vertragsabsprachen erforderlich, auf die in dieser Checkliste nicht eingegangen wird.

Die notwendige Hardware stellt der Anbieter und wartet sie auch. Dabei wird das Verständnis zugrunde gelegt, dass in einer Public Cloud auf einer Hardware-Einheit (Speichermedium, Server) Daten mehrerer Kunden verarbeitet werden, wobei der Anbieter die Aufteilung und Zuordnung der Hardware pro Kunde steuert. Die eingesetzte Hardware kann sich entweder im Eigentum des Anbieters befinden oder von diesem bei Dritten geleast oder angemietet sein. Außerdem gehört regelmäßig die Bereitstellung von Speicherkapazitäten für die Anwendungsdaten zum Leistungsumfang des Anbieters.

Der vertragliche Rahmen in dieser Checkliste ist für ein Geschäft konzipiert, das nicht auf einen einmaligen Leistungsaustausch, sondern auf eine Leistungserbringung über einen längeren Zeitraum ausgerichtet ist.

Die Ausführungen gelten ausschließlich für Verträge zwischen Unternehmen (B2B). Dabei steht die Perspektive der Anbieter im Vordergrund.

Für die rechtliche Betrachtung in dieser Checkliste wird deutsches Recht zugrunde gelegt.

Ein weiterer wichtiger Punkt zum Einsatz von Cloud-Verträgen: In aller Regel richtet sich ein Cloud-Angebot an eine Vielzahl von Nutzern. Dafür werden typischerweise gleichlautende standardisierte Vertragstexte verwendet, die bereits vor Vertragsabschluss zumindest in einzelnen Festlegungen in Textform vorliegen. Solche vorformulierten Vertragsbedingungen unterliegen als allgemeine Geschäftsbedingungen (AGB) den spezifischen Einschränkungen der vertraglichen Gestaltungsfreiheit durch das AGB-Recht. Die Vereinbarkeit einzelner vertraglicher Regelungen mit dem AGB-Recht ist auch vom konkreten Geschäftsmodell und von der Angemessenheit für den Kunden abhängig. Die konkreten Formulierungen bedürfen daher einer besonderen rechtlichen Prüfung durch einen qualifizierten Juristen. Auf die Ausformulierung einzelner vertraglicher Regelungen wird deshalb in diesem Leitfaden bewusst verzichtet.

1.2 Vertragstypologische Einordnung

Ein Vertrag über SaaS in einer Public Cloud ist nach der Rechtsprechung rechtlich wie der ASP-Vertrag als Mietvertrag einzuordnen (vgl. BGH, Urteil vom 4. März 2010 – III ZR 79/09, Rz. 19). Demnach hat der Anbieter dem Kunden den Gebrauch der gemieteten Software für die Mietdauer gegen Vergütung zu gewähren. Dafür muss der Kunde die Software nicht selbst besitzen. Es genügt vielmehr, dass er die Software nutzen kann. In der Praxis werden mit der bloßen Bereitstellung der Nutzungsmöglichkeit einer Software weitere Leistungen, z. B. Datenspeicherung oder Hotline, verbunden. Dies kann zu einer abweichenden vertragstypologischen Einordnung führen, wenn die anderen Leistungen die Bereitstellung von Software in den Hintergrund drängen. Die Betrachtung in dieser Checkliste beschränkt sich auf die Bereitstellung der Nutzungsmöglichkeit einer Software als Hauptleistung. Dafür wird von Mietvertragsrecht als maßgeblicher Grundlage ausgegangen.

1.3 Aufbau der Vertragsdokumente

Aus rechtlicher Sicht ist es nicht entscheidend, ob Leistungsbeschreibung, Preise, Mitwirkungspflichten usw. in einem einheitlichen Vertragsdokument enthalten sind oder ob hierzu auf Anlagen zum Vertrag verwiesen wird. Für einen modularen Aufbau mit der Verlagerung bestimmter Vertragsinhalte in Anlagen spricht oft ein übersichtlicheres Hauptdokument, die Zuständigkeitsverteilung in Unternehmen und die Flexibilität, die durch Hinzufügung oder Streichung ergänzender Vertragsanlagen erreicht werden kann.

Für diese Checkliste spielt es keine Rolle, an welcher Stelle die Vertragsinhalte geregelt werden. Sie geht daher auf diesen Punkt nicht weiter ein. Wichtig ist bei einem modularen Aufbau, dass die Anlagen spätestens bei Abschluss des Vertrages komplett vorliegen und dokumentiert in den Vertrag einbezogen werden. Ansonsten wird kein vollständiger Vertrag geschlossen oder der geschlossene Vertrag ist wegen Fehlens der vertraglichen Mindestinhalte unwirksam.

1.4 Dokumentierter Vertragsabschluss

Ein Cloud-Vertrag bedarf nach deutschem Recht grundsätzlich keiner besonderen Form. Das bedeutet, Verträge über Cloud-Leistungen könnten z. B. auch über Telefon oder im Austausch von E-Mails abgeschlossen werden. Einzelne Vertragsbestandteile können aber sehr wohl eine besondere Form erfordern. So ist z. B. die Vereinbarung einer Auftragsdatenverarbeitung (vgl. dazu unten Kapitel IV.8) schriftlich abzuschließen. Es ist insgesamt zu empfehlen, alle Vereinbarungen, die

für eine Cloud-Leistungsbeziehung gelten sollen, in geeigneter Form festzuhalten und für beide Seiten zu dokumentieren.

> ! Achten Sie auf einen dokumentierten und beweisbaren Vertragsschluss (einschließlich Archivierbarkeit)!

Hat der Anbieter eine schriftliche Fixierung der für ihn wesentlichen Vertragsinhalte zur mehrmaligen Verwendung bereits vor Vertragsabschluss vorgenommen, handelt es sich insoweit im Rechtssinn bereits um Allgemeine Geschäftsbedingungen (AGB). Damit unterliegen solche vertraglichen Festlegungen den besonderen Anforderungen von § 307 des Bürgerlichen Gesetzbuchs (BGB). Das bedeutet, der gewerbliche Cloud-Nutzer darf im Vertrag nicht unangemessen durch die Vorgaben des Anbieters benachteiligt werden. Die daraus folgenden Einschränkungen sind in dieser Checkliste berücksichtigt.

1.5 Interessen der Parteien eines Cloud-Vertrages

Das Interesse des Anbieters einer SaaS-Lösung besteht darin, mit überschaubarem und kalkulierbarem Aufwand einer großen Vielzahl von Kunden eine Software zugänglich zu machen und dabei die ihm zur Verfügung stehenden Ressourcen effizient auszunutzen. Um die gewünschten Skaleneffekte und die darauf beruhenden Kostenvorteile zu erzielen, muss er sein Angebot in hohem Maß standardisieren, Anpassungen seines Angebots an die speziellen Bedürfnisse einzelner Kunden wird der Anbieter daher typischerweise vermeiden wollen.

Der Vorteil des Kunden liegt regelmäßig in der Nutzung und Abrechnung der Leistung nach seinem Bedarf. Daher wird er auf eine flexible Erweiterbarkeit des Angebots, aber auch auf unkomplizierten Ein- und Ausstieg in die Nutzung Wert legen. Außerdem wird er darauf bedacht sein, dass Daten, die für sein eigenes Unternehmen von besonderer Relevanz sind oder einem besonderen gesetzlichen Schutz unterliegen, gegen Verlust und unberechtigten Zugriff besonders geschützt sind und ggf. in seinen eigenen IT-Systemen unproblematisch weiter verarbeitet werden können. Daraus können besondere Anforderungen an Datensicherheit und Datenschutz und sonstige spezifische Bedürfnisse resultieren.

Da die Interessen der Parteien im Einzelfall und die verschiedenen Geschäftsmodelle der Anbieter von Cloud-Leistungen sehr unterschiedlich sein können, ist stets darauf zu achten, dass die Verträge zwischen Anbieter und Kunde an das konkrete Geschäftsmodell und an die jeweiligen individuellen Bedürfnisse der Parteien angepasst werden.

2 Checkliste für Cloud Computing-Verträge

Die nachfolgende Checkliste legt eine Einordnung des SaaS-Vertrages als Mietvertrag zugrunde (vgl. oben Kapitel 1.2). Das Gesetz verlangt zwingende Mindestinhalte, damit überhaupt ein Vertrag zustande kommt (Vertragsparteien, Leistung, Gegenleistung). Nur diese zwingenden Mindestinhalte zu vereinbaren, ist für Cloud-Leistungen nicht praxisgerecht und berücksichtigt nicht hinreichend die Bedürfnisse von Anbieter und Kunden in solchen Leistungsbeziehungen. Die folgende Checkliste führt typische Regelungsthemen für Cloud-Leistungen am Beispiel eines SaaS-Vertrages für die Public Cloud im Geschäftsverkehr zwischen Unternehmen (B2B) auf. Die vertraglichen Absprachen sollten in geeigneter Form dokumentiert werden. Die Gliederungsziffern in der nachfolgenden Aufzählung kennzeichnen keine Wertigkeit oder Rangfolge, sondern sollen nur der leichteren Orientierung dienen.

Folgende Inhalte sollten in einem Cloud Computing-Vertrag vereinbart werden:

1. Bezeichnung der Vertragsparteien

2. Vertragsgegenstand (hier: SaaS aus einer Public Cloud im B2B-Geschäftsverkehr)

   - Bezeichnung der Software
   - Service Levels (z. B. Verfügbarkeit der Leistung)
   - Weitere Leistungspflichten (z. B. Anwenderunterstützung, Back-up-Services)

3. Art und Umfang der Nutzung (einschließlich Nutzungsrechte)

4. Nutzungsvoraussetzungen

5. Mitwirkungspflichten des Kunden

6. Vergütung und Zahlungsmodalitäten
   (z. B.: Monatliches Entgelt / Entgelt pro Woche / Tag)

7. Vertragslaufzeit

8. Gewährleistung für Sach- und Rechtsmängel

9. Haftung

10. Datenschutz / Datensicherheit

11. Vertraulichkeit

12. Einschaltung von Subunternehmern

13. Transition und Exit-Management

14. Gerichtsstand

15. Rechtswahl

16. Vertragssprache

Die einzelnen hier aufgeführten Punkte werden in den Erläuterungen zu dieser Checkliste näher betrachtet (vgl. unten 3) und vereinzelt vertieft dargestellt (vgl. unten Kapitel 4).

3 Erläuterungen zur Cloud-Checkliste

Zum Mindestinhalt eines Cloud-Vertrages gehören die Bezeichnung der Vertragsparteien (vgl. Kapitel 3.1), die Festlegung des Vertragsgegenstandes (vgl. 3.2) und die Vereinbarung der Vergütung (vgl. Kapitel 3.6). Fehlt einer dieser grundlegenden Punkte, kommt ein Vertrag nicht zustande. In der Praxis werden jedoch regelmäßig weitere, von den gesetzlichen Vorschriften abweichende Vereinbarungen getroffen, um den Besonderheiten einer Cloud-Geschäftsbeziehung besser gerecht zu werden. Dabei sollte darauf geachtet werden, dass die jeweils vereinbarten Regelungen der konkreten Geschäftsbeziehung auch angemessen sind. Beispielsweise sind Vereinbarungen zu Rechtswahl und Vertragssprache nur erforderlich für grenzüberschreitende Cloud-Beziehungen.

3.1 Bezeichnung der Vertragsparteien

Zu empfehlen ist eine genaue und eindeutige Bezeichnung der Vertragsparteien: bei Unternehmen zumindest mit Firma, Rechtsform, Firmensitz und unterschriftsberechtigtem Vertreter. Im Zweifel kann man sich die Vertretungsberechtigung des Verhandlungspartners nachweisen lassen (z. B. durch Handelsregisterauszug).

3.2 Vertragsgegenstand

! Ohne Beschreibung der wesentlichen Leistungsinhalte ist jeder Vertrag riskant oder sogar hinfällig!

Mit dem Vertragsgegenstand wird die hauptsächliche Vertragsleistung beschrieben, also hier die Bereitstellung einer Software; dies umfasst:

- die Bezeichnung der zur Nutzung bereit gestellten Software,
- Art der Nutzung, hier: Zugriff auf Software im Rechenzentrum.

Es ist zu empfehlen, den Leistungsgegenstand, d. h. die zur Verfügung gestellte Software, näher zu konkretisieren.

- Alternative 1: Nur eine bestimmte Version der Software ist zugänglich zu machen; die Version sollte im Vertrag festgeschrieben werden; trotzdem kann es notwendig sein, Updates zur Verfügung zu stellen, um den vertraglich vereinbarten Gebrauch zu erhalten oder um die Software weiter anbieten zu können;
- Alternative 2: Der Kunde soll stets die aktuelle Version der Software nutzen können; im Vertrag sollte niedergelegt werden, auf welche Art und Weise Inhalte von Updates sowie Zeitpunkt und Verfahren ihrer Einspielung angekündigt werden.

Für den Anbieter ist es empfehlenswert, allen Kunden einheitlich entweder Alternative 1 oder 2 anzubieten. Ansonsten kann er seine Infrastruktur nicht mehrfach nutzen und seine Pflegeaufwände erhöhen sich.

! Ohne anders lautende vertragliche Regelungen darf der Kunde einen uneingeschränkten Gebrauch der Software erwarten, auch bei Release-Wechseln und bei Wartung der Software. Außerdem kann der Kunde erwarten, dass keine Umstellung seiner Nutzung erfolgt und die Verwendbarkeit seiner Daten nicht beeinträchtigt wird.

Wegen Branchenüblichkeit bietet es sich an, die Vereinbarung folgender zusätzlicher Leistungspflichten in Betracht zu ziehen:

- Reaktionszeit bei Störung (Hotline als zusätzliche Leistung gegen zusätzliche Vergütung);
- Zusätzliche Back-up-Services (gegen gesondertes Entgelt);
- Anwenderunterstützung für Software (nur bei gesonderter Vereinbarung als Zusatzleistung gegen gesonderte Vergütung).

Hierbei ist darauf zu achten, dass nicht ohnehin (gesetzlich) geschuldete Pflichten gesondert in Rechnung gestellt, sondern vielmehr die Zusatzleistungen transparent dargestellt werden. Weitere Einzelheiten zu Leistungspflichten im Cloud-Vertrag finden sich in Kapitel 4.2.

Zusätzlich zu den reinen Cloud-Leistungen kann der Anbieter optional weitere Leistungspflichten (regelmäßig gegen gesonderte Vergütung) übernehmen:

- Übernahme von Daten und / oder Anwendungsprogrammen aus den Systemen des Kunden bei Vertragsbeginn;
- Customizing: Anpassung des Anwendungsprogramms an die Bedürfnisse des Kunden oder (nach Transition) an die Umgebung des Anbieters;
- Change-Management bei Beendigung der Vertragsbeziehung;
- Call-Center zur Unterstützung der Nutzung durch den Kunden;
- Schulung von Mitarbeitern des Kunden im Umgang mit der bereit gestellten Software.

3.3 Art und Umfang der Nutzung

Im Regelfall erfolgt der Zugriff des Kunden auf die Cloud-Software über einen Browser ohne zusätzliche Client-Software. Der Anbieter betreibt die Software in seiner Verantwortung auf von ihm kontrollierter Hardware. Dafür benötigt der Kunde wohl kein eigenes urheberrechtliches Nutzungsrecht (vgl. unten 4.4). Die in dieser Checkliste beschriebene Konstellation legt den Regelfall zugrunde.

Alternativ kann der Kunde Software zur Nutzung auf eigenen Rechnern (»Client«) erhalten, die in Verbindung mit der im Rechenzentrum vom Anbieter bereitgestellten Software arbeitet. Hieran muss dem Kunden ein Nutzungsrecht eingeräumt werden, wie an anderer, dem Kunden überlassener Software auch.

Der Nutzungsumfang der beim Anbieter bereit gestellten Software sollte klar und unmissverständlich definiert werden, z. B. durch:

- Anzahl der gleichzeitigen Zugriffe auf die Software;
- Herkunft der Nutzer der Software (eine Firma, ein Konzern, bestimmte Länder usw.);
- Dedizierte Nutzer (»named user«) oder gleichzeitige Zahl von Nutzern (»concurrent user«);
- Etwaige weitere Präzisierungen (eigene Zwecke, keine Untervermietung, usw.).

3.4 Nutzungsvoraussetzungen beim Kunden

Soweit sie nicht bereits im Rahmen der Leistungsbeschreibung definiert wurden, sollten die Nutzungsvoraussetzungen beim Kunden in einer vertraglichen Regelung niedergelegt werden. Im Regelfall hat der Kunde selbst für einen Internetzugang bis zum Übergabepunkt des Anbieters zu sorgen, damit er die Leistung des Anbieters in Empfang nehmen und nutzen kann. Das bedeutet, dass der Kunde die technischen Anforderungen zur Nutzung des Clients oder Browsers für den Zugriff auf die zur Nutzung bereitgestellte Software erfüllen muss (z. B. Einsatz eines VPN-Client).

! Die Beschreibung der Nutzungsvoraussetzungen beim Kunden sollte als Voraussetzung der Leistungserbringung, nicht als „Mitwirkungspflicht" des Kunden formuliert sein. Da der Kunde nach dem Leitbild des gesetzlichen Mietrechts nicht verpflichtet ist, Nutzungsvoraussetzungen zu schaffen, ist die Vereinbarung solcher Pflichten in AGB möglicherweise unwirksam.

Ist für die Nutzung der vertraglichen Cloud-Leistung Voraussetzung, dass weitere nicht zum vertraglichen Leistungsumfang gehörende Hard- oder Software vorhanden ist, sollte diese zusätzliche Hard- oder Software bezeichnet werden.

Es ist nicht Aufgabe des Anbieters, die gesetzlichen Anforderungen zu beachten, denen der Kunde unterliegt. Soweit notwendig, hat der Kunde darauf zu achten, dass seine Anforderungen an die Cloud-Leistungen entsprechend vereinbart werden.

3.5 Mitwirkungspflichten des Kunden

Bei den vertraglichen Pflichten des Kunden sind Informationspflichten und Mitwirkungspflichten zu unterscheiden.

Dem Kunden können Mitwirkungspflichten auferlegt werden, um die Vertragsdurchführung zu ermöglichen oder zu erleichtern, z. B. Übergabe einer Liste mit zugriffsberechtigten Nutzern, um die nutzungsgemäße Abrechnung (für pay per user) oder den Nachweis der Nutzungsüberschreitung (misuse) zu ermöglichen.

Informationspflichten des Kunden können z. B. sein:

- Aktuelle Nutzeranzahl, nutzende Unternehmen (sonstige Konzernunternehmen / Tochtergesellschaften), Länderabdeckung, Datenvolumen, Zeitprofil der Nutzung;
- Von der üblichen Nutzung abweichende Nutzungsart oder Nutzungsinhalte;
- Besonderheiten mit potentieller Auswirkung auf Cloud Services, insbesondere Qualität, Lösungswege und Hintergrund (soweit bekannt).

Mitwirkungspflichten des Kunden können z. B. sein:

- Auswahl einer für seine Zwecke und seine Anforderungen geeigneten Cloud-Lösung;
- Beschreibung der eigenen aktuellen IT-Umgebung und Beschreibung von technischen Schwierigkeiten auf Anforderung des Anbieters im Einzelfall;
- Aufrechterhaltung eines angemessenen IT-Sicherheitsniveaus (Firewall, SPAM-Filter, Virenschutz usw.);
- Ermöglichung von Audits durch den Anbieter (Nutzeranzahl, Länderabdeckung usw.);
- Einholung notwendiger Genehmigungen;

- Erfüllung von Informationspflichten gegenüber Dritten (Behörden/Kunden);
- Kontrolle/Überwachung des Zugangs zu Cloud Services;
- Bereitstellung ausreichender Connectivity / Bandwidth und Erfüllung anderer notwendiger technischer Voraussetzungen;
- Zustimmung zu und Unterstützung bei notwendigen und angemessenen Anpassungen des Leistungsumfangs.

Informations- und Mitwirkungspflichten sind als vertragliche Nebenpflichten anzusehen. Die Verletzung von Nebenpflichten kann zur Folge haben, dass der Kunde dem Anbieter dadurch entstehende Nachteile ausgleichen muss.

3.6 Vergütung und Zahlungsmodalitäten

> **!** Ohne ausdrückliche Vereinbarung zur Vergütung kann der Vertrag unwirksam sein.

Wie die Regelung der Vergütung im Detail ausgestaltet wird, ist aus rechtlicher Sicht nicht relevant. Es sind hier ganz unterschiedliche Regelungen denkbar, z. B.

- Vergütung pro Nutzer;
- Fixpreis / Flatfees: Hierbei wird gegen eine feste Zahlung pro Abrechnungseinheit – typischerweise eine Zeiteinheit wie Monat, Quartal oder Jahr – eine vom Nutzungsumfang unabhängige Vergütung zwischen Anbieter und Kunde vereinbart;
- Pay per Use: Kunde zahlt nur die tatsächlich abgerufenen Leistungen;
- Mischmodelle: feste Basiszahlung pro Abrechnungszeitraum, ergänzt durch eine von der tatsächlichen Nutzung abhängige flexible Vergütung;
- Preisanpassung: z. B. Anpassung an die Preisentwicklung der zur Verfügung gestellten Software (bei Vereinbarung von Preisanpassungen ist das AGB-Recht besonders zu beachten);
- Zahlungszeitpunkt für die Vergütung: Vorauszahlung oder nachträgliche Abrechnung.

3.7 Vertragslaufzeit

Da es sich bei dem hier betrachteten Cloud-Vertrag (SaaS in einer Public Cloud) um einen Mietvertrag handelt, gilt ohne eine weitere Vereinbarung hierzu das BGB, das für Miete im Grundtypus ein unbefristetes Vertragsverhältnis mit sehr kurzen Kündigungsfristen für beide Seiten vorsieht. Allerdings kann hiervon durch eine Vereinbarung im Vertrag abgewichen werden. Die sinnvolle Vertragsdauer richtet sich nach der spezifischen Cloud-Leistung und den Bedürfnissen im Einzelfall. In Betracht kommen

- Alternative 1: keine feste Vertragsdauer;
- Alternative 2: feste Vertragsdauer oder feste Mindestvertragsdauer;
- Alternative 3: feste Vertragsdauer mit Verlängerung (ausdrücklich zu vereinbaren oder automatisch).

Typischerweise strebt der Cloud-Nutzer eine gewisse Flexibilität der Vertragslaufzeit und eine Möglichkeit zur kurzfristigen Vertragsbeendigung an. Andererseits hat der Anbieter ohne eine Mindestmietzeit keinen gesicherten und kalkulierbaren Umsatz und der Nutzer keine langfristig gesicherte Nutzungsmöglichkeit.

Anstelle einer festen Vertragslaufzeit oder auch zusätzlich kann die Möglichkeit zur Kündigung vereinbart werden. Möglich ist auch zu vereinbaren, dass sich die Vertragslaufzeit automatisch um einen bestimmten Zeitraum

verlängert, wenn nicht bis zu einem bestimmten Zeitpunkt (z. B. Monatsende) eine Kündigung ausgesprochen wird (oben Alternative 3).

Zu bedenken (und ggf. zu regeln) sind:

- Kündigungsfristen;
- Formalanforderungen (z. B. Schriftform der Kündigung);
- außerordentliche Kündigungsrechte und deren Voraussetzungen (z. B. Überschreitung des Nutzungsumfangs durch den Kunden).

Zu verschiedenen Kündigungsmöglichkeiten vgl. auch unten Kapitel 4.5.

3.8 Gewährleistung für Sach- und Rechtsmängel

Für mietvertragliche Gestaltungen, die einem SaaS-Vertrag für die Public Cloud zugrunde liegen, kommen bei Mängeln der Leistung die gesetzlichen Gewährleistungsrechte gemäß der §§ 535 ff. BGB zur Anwendung, soweit sie nicht wirksam vertraglich modifiziert sind. Für eine solche Modifizierung in Standard-Verträgen ist allerdings das Recht der Allgemeinen Geschäftsbedingungen (§§ 305 ff. BGB) zu beachten, das den Spielraum für Abweichungen von den gesetzlichen Gewährleistungsrechten eng begrenzt.

Der Anbieter hat nach § 535 BGB die Nutzung der SaaS-Anwendung zum vertragsgemäßen Gebrauch zu ermöglichen und während der Mietzeit diesen Zustand zu erhalten. Kann der Anbieter den vertragsgemäßen Gebrauch nicht ermöglichen oder entfällt dieser während der Mietzeit, liegt ein Mangel vor.

Bei Mängeln wird zwischen Rechts- und Sachmangel unterschieden. Bei einem Rechtsmangel kann der Anbieter dem Kunden den Gebrauch der SaaS-Anwendung nicht ermöglichen, da ein Recht eines Dritten entgegensteht. Ein Sachmangel liegt bei einer erheblichen Abweichung der vertraglich vereinbarten Soll- von der Ist-Beschaffenheit vor.

Bei einem Mangel kann der Kunde folgende Ansprüche / Rechte geltend machen, soweit diese nicht wirksam vertraglich modifiziert wurden:

- Zurückbehaltungsrecht;
- Mietminderung;
- Mangelbeseitigungsanspruch / Ersatzvornahme;
- Schadensersatzanspruch;
- Kündigung.

Eine nähere Erläuterung zu Gewährleistungsansprüchen des Kunden findet sich in Kapitel 4.6.

3.9 Haftung

Soweit keine vertraglichen Gewährleistungsregeln vorrangig eingreifen, gilt im Verhältnis zwischen Anbieter und Kunde das gesetzliche Haftungsregime für die schuldhafte Verletzung vertraglicher und gesetzlicher Pflichten. Nach diesem Haftungsregime wird unabhängig vom Grad des Verschuldens Schadensersatz ohne Begrenzung geschuldet. Die Haftung umfasst auch Pflichtverletzungen des zur Vertragsdurchführung eingesetzten Personals (§ 278 BGB).

Beispiel: Der Kunde wird hinsichtlich der SaaS-Anwendung fahrlässig falsch beraten, ein Mangel liegt jedoch nicht vor. Durch die Falschberatung entsteht dem Kunden ein Schaden. Diesen kann er vollumfänglich geltend machen. In diesem Zusammenhang ist es unerheblich, ob eigene Mitarbeiter des Anbieters oder Unterauftragnehmer den Schaden verursacht haben.

Als sonstiges Haftungsszenario kommt die Verletzung von Rechten eines Dritten durch den Anbieter in Betracht,

z. B. wegen Nichtbeachtung von Lizenzbedingungen (Drittanspruch).

Für den Anbieter empfiehlt sich daher eine vertragliche Beschränkung von Voraussetzungen und Umfang der Haftung. In Standard-Verträgen unterliegen solche vom Anbieter vorgeschlagenen Vereinbarungen engen Beschränkungen ihrer Wirksamkeit durch das AGB-Recht (§ 305 ff. BGB). Die Rechtsprechung hält zu weitgehende Haftungsbeschränkungen regelmäßig für unwirksam und wendet dann die unbegrenzte gesetzliche Haftung an. Eine Haftungsbeschränkung sollte daher möglichst individuell mit dem Kunden vereinbart werden, soweit dies möglich ist.

3.10 Datenschutz

Beim Cloud Computing kommt es ganz häufig zur Verarbeitung personenbezogener Daten, selbst wenn dies nicht Inhalt des Cloud-Vertrages ist. Das Bundesdatenschutzgesetz (BDSG) schreibt einen besonderen Schutz von personenbezogenen Daten vor, der auch beim Cloud Computing aufrecht erhalten bleiben muss. Daten sind personenbezogen, wenn sie Informationen über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person enthalten (§ 3 Abs. 1 BDSG), z. B. Name, Anschrift, Verdienst, Kontonummer, Kaufverhalten. Verlagert der Kunde personenbezogene Daten in die Cloud und lässt sie dort nach seiner Weisung und seinen Vorgaben verarbeiten, handelt es sich um eine Datenverarbeitung im Auftrag nach § 11 BDSG. Bei einer Auftragsdatenverarbeitung bleibt der Kunde für die Einhaltung der datenschutzrechtlichen Anforderungen für personenbezogene Daten, die von ihm erhoben, gespeichert oder verarbeitet werden, selbst verantwortlich. Daran ändert sich durch die Nutzung von Cloud-Leistungen nichts. Das BDSG verlangt bei einer Auftragsdatenverarbeitung u.a. eine gesonderte Vereinbarung zwischen Kunde (= Auftraggeber i.S.d. Datenschutzrechts) und Anbieter (= Auftragnehmer i.S.d. Datenschutzrechts), die gemäß § 11 Abs. 2 S. 2 BDSG schriftlich abzuschließen ist. Für weitere Details vgl. unten Kapitel 4.8.

3.11 Vertraulichkeit und Datensicherheit

Bei der Datensicherheit stehen die Schutzziele Integrität der Daten (Schutz vor Veränderung und Löschung) und Abwehr von unbefugter Einsichtnahme und unbefugten Zugriffen auf Informationen im Mittelpunkt. Der Anbieter von Leistungen in einer Public Cloud strebt einen hohen Automatisierungs- und Standardisierungsgrad an, um die Kostenvorteile des Cloud Computing zu realisieren. Daher kann er – wenn er nicht gerade eine Sicherheitslösung anbietet – auf die besondere Schutzbedürftigkeit sensibler Informationen nicht in jedem Fall verstärkt Rücksicht nehmen. Z. B. werden die Daten bei Übertragung zwischen einer Public Cloud und dem Nutzer oft nicht verschlüsselt, eine Lokalisierung der Cloud-Ressourcen ist nicht immer möglich, Zugriffskontrolle und Disaster Recovery (Wiederherstellung des Datenbestandes nach unbeabsichtigtem Verlust) gehören nicht immer zum Standard-Angebot des Cloud-Betreibers. Deshalb sollte der Kunde seine Daten vor der Übertragung in die Cloud intern klassifizieren und festlegen, welche Daten bei einem Anbieter auf welche Weise gespeichert werden dürfen und welches Niveau an Datensicherheit jeweils erforderlich und zu vereinbaren ist.

Ist dagegen die Verarbeitung personenbezogener Daten in der Cloud im Vertrag vereinbart, muss sich der SaaS-Kunde schon aufgrund gesetzlicher Vorgaben des Bundesdatenschutzgesetzes (BDSG) bestimmte Kontrollrechte in Bezug auf die Sicherheit der Datenverarbeitung einräumen lassen. Ferner hat der Anbieter technisch-organisatorische Maßnahmen zum Schutz der Daten zu treffen und eine Beschreibung dieser Maßnahmen bereit zu halten.

Ungeachtet dessen sollte der Anbieter ein Mindestschutzniveau bereitstellen und im Vertrag niederlegen. So sollte z. B. eine Vermischung von Daten verschiedener Kunden ausgeschlossen sein, entweder im Wege einer logischen Trennung durch Virtualisierung oder durch eine physische Trennung und Installation von Zugriffskontrollen. Außerdem kann die kontinuierliche Aufrechterhaltung von bewährten IT-Sicherheitszertifizierungen vereinbart werden. Die Einhaltung gängiger IT-Sicherheitsstandards

lässt sich durch eine Zertifizierung z. B. nach ISO 27001 nachweisen.

Weitere mögliche Maßnahmen zur Gewährleistung der Datensicherheit sind die Aufnahme einer Vertraulichkeitsklausel in den Vertrag, eine Verschlüsselung der Daten und eine Begrenzung des Personenkreises, der auf die Daten zugreifen darf.

3.12 Einschaltung von Subunternehmern

Grundsätzlich ist der Anbieter berechtigt, bei der Leistungserbringung Subunternehmer einzuschalten. Die Übernahme einzelner (Teil-)Leistungen durch einen Subunternehmer ändert nichts an den Vertragspflichten des Anbieters gegenüber dem Kunden. Für die Einschaltung von Subunternehmern ist grundsätzlich keine Zustimmung des Kunden erforderlich. Eine Ausnahme besteht jedoch bei der Verarbeitung personenbezogener Daten, die vom Kunden stammen. Die Einbindung von Subunternehmern bei der Verarbeitung oder Speicherung personenbezogener Daten muss vertraglich geregelt werden (§ 11 Abs. 2 Nr. 6 BDSG). Ferner muss der Cloud-Anbieter mit den eingeschalteten Unterauftragnehmern eine schriftliche Vereinbarung zur Auftragsdatenverarbeitung zugunsten des Kunden schließen. Es muss gewährleistet sein, dass der Kunde die Datenherrschaft behält und die Erfüllung seiner datenschutzrechtlichen Verpflichtungen auch gegenüber den Subunternehmern durchsetzen kann. Einzelheiten hierzu sind in Kapitel 4.8 dargestellt.

3.13 Transition und Exit-Management

Je nach Bedeutung der Cloud-Leistung für das Unternehmen des Kunden hat dieser einen unterschiedlich großen Bedarf an Vorkehrungen dafür, dass die Cloud-Leistung aus unvorhergesehenen Gründen eingestellt wird. Solche Gründe können z. B. sein: Insolvenz des Anbieters, Insolvenz eines Subunternehmers, außerordentliche Kündigung des Kunden, Fusion des Anbieters. In diesen Fällen kann es erforderlich werden, die beim Anbieter verarbeiteten Daten in einem geordneten Verfahren an den Kunden zurück zu übertragen. Andererseits kann der Kunde auch ein Interesse an der Löschung seiner Daten haben. Für die Beendigung des Cloud-Vertrages sollte daher ein Exit-Management vereinbart sein, das diesen Anforderungen Rechnung trägt. Eine vollständige Absicherung gegen eine unvorhersehbare Beendigung des Cloud-Vertrages wäre nur bei Sicherung der Daten im Unternehmen des Kunden gegeben. Folgende Punkte können als Best Practice im Rahmen des Exit-Managements im Sinne einer kundenorientierten Cloud-Dienstleistung je nach typischem Bedarf des Kunden geregelt werden:

- Die Herausgabe der von dem Kunden in die Cloud eingestellten Daten in einem geeigneten Format, z. B. in einer CSV-Datei (comma separated value);
- Die Plicht des Anbieters, die Kundendaten proaktiv herauszugeben (anstatt den Kunden lediglich darüber zu informieren, dass dieser die Daten zur Sicherung herunterladen kann);
- Die Regelung eines ausreichenden Zeitraums, in dem die Daten nach Vertragsende noch für den Kunden vorgehalten werden;
- Die vertraglich zugesicherte und ggf. ausdrücklich bestätigte Löschung der Daten von allen Speichermedien des Anbieters.

Daneben könnte bei Vertragsbeendigung z. B. vereinbart werden:

- Unterlagen zur Verfügung zu stellen;
- Schulungen für Personal des Kunden oder des neuen Anbieters durchzuführen;
- Nutzungsrechte über das Vertragsende hinaus einzuräumen;
- Regelung über gesonderte Vergütung von Exit-Leistungen.

Die Erfahrung zeigt, dass bei Vertragsschluss getroffene Regelungen über Exit-Management und Exit-Support in der Regel nicht alle Eventualitäten vorhersehen. Aus diesem Grund sollte ein Kontingent von Leistungstagen für Maßnahmen eingeplant und kalkuliert werden, die im Zusammenhang mit einer Beendigung der Leistungsbeziehung notwendig sind. Dies gilt insbesondere für eine möglicherweise unverzichtbare Zusammenarbeit zwischen dem bisherigen und einem neuen Anbieter.

3.14 Gerichtsstand

Mit einer Gerichtsstandklausel können die Vertragsparteien bestimmen, vor welchem Gericht Rechtsstreitigkeiten aus dem Vertrag auszutragen sind. Falls vertraglich nichts vereinbart ist, gilt als Gerichtsstand der Sitz des Beklagten (§ 12 ZPO). Meist wird der Anbieter den Gerichtsstand an seinem Unternehmenssitz vertraglich festlegen.

> **!** In AGB-Verträgen ist eine Gerichtsstandsklausel nicht beliebig möglich. Der Gerichtsstand muss einen Bezug zu einer Vertragspartei oder zur Leistungserbringung haben.

Der Gerichtsstand hat Auswirkungen auf die Vollstreckbarkeit einer späteren Gerichtsentscheidung. Außerdem wird ein Gerichtsverfahren immer dann schwierig, wenn sich die Richter mit einer Rechtsordnung auseinandersetzen müssen, in der sie nicht ausgebildet wurden. Ist der Vertrag z. B. auf Deutsch abgefasst und liegt der Gerichtsstand in Deutschland, sollte auch deutsches Recht anwendbar sein.

3.15 Rechtswahl

Eine Rechtswahlklausel sollte in den Vertrag aufgenommen werden, wenn die Cloud-Leistung grenzüberschreitend erbracht wird. Diese Checkliste geht von der Geltung des deutschen Rechts aus.

> **!** In AGB-Verträgen ist eine Rechtswahl nicht uneingeschränkt möglich. Dadurch können keine zwingenden Regelungen einer nationalen Rechtsordnung (z. B. aus dem Urheberrecht) umgangen werden.

Es gehört zu den Charakteristika von Cloud-Leistungen, dass sie aus mehreren, auch während der Leistungserbringung wechselnden Ländern erbracht werden. Wegen der möglichen Vielzahl von Rechtsordnungen, die auf diese Weise durch eine Cloud-Leistung berührt werden können, ist eine Wahl der maßgeblichen Rechtsordnung im Vertrag zu empfehlen. Grundsätzlich sind die Parteien eines Vertrages bei der Wahl des anwendbaren Rechts frei. Ausnahmen bestehen aber, um zu verhindern, dass durch die Rechtswahl zwingende Regelungen einer nationalen Rechtsordnung umgangen werden. So richten sich z. B. Urheberrechte nach dem Recht des Staates, in dem sie entstanden sind. Auch für deliktische Ansprüche oder andere außervertragliche Schuldverhältnisse kann das anwendbare Recht nicht durch vertragliche Abreden gestaltet werden.

Auch bei zulässiger Rechtswahl ist für das Cloud Computing nicht jede Rechtsordnung zweckmäßig. Anwendbares Recht, Vertragssprache und Gerichtsstand sollten im Vertrag aufeinander abgestimmt werden. Ansonsten können sich Probleme bei der Auslegung rechtlicher Begriffe ergeben.

Treffen die Parteien eines Cloud-Vertrages trotz Bezugs zu mehreren (mindestens zwei) verschiedenen Staaten keine ausdrückliche Rechtswahl, kommt die EG-Verordnung Nr. 593/2008 vom 17. Juni 2008 (»Rom I«) über das auf vertragliche Schuldverhältnisse anzuwendende Recht zur Anwendung.

3.16 Vertragssprache

Die Vertragssprache kann von den Parteien in AGB nur eingeschränkt frei vereinbart werden. Die Vertragssprache muss einen Bezug zu mindestens einer Partei oder zur Leistungserbringung haben. Da die Gerichtssprache vor deutschen Gerichten deutsch ist (vgl. § 184 GVG), drohen bei Klagen über fremdsprachige Verträge Übersetzungskosten und z. T. erhebliche Verständnisschwierigkeiten. Dem kann man entgehen, indem man z. B. die deutsche Vertragsversion im Vertrag als verbindlich erklärt und die englische Version nur als zusätzliche Information dient (Vorrangklausel). Steht dieser Weg nicht offen, sollten bei den zentralen Begriffen zumindest in Klammern die Begriffe der anwendbaren Rechtsordnung in der Originalsprache hinzugefügt werden. Bei Verträgen in englischer Sprache und anwendbarem deutschen Recht sollten also die entsprechenden deutschen Rechtsbegriffe in Klammern hinter den englischen Begriffen eingefügt werden. Aus Sicht einer deutschen Vertragspartei ist die Wahl von Deutsch als Vertragssprache und die Vereinbarung von deutschem Recht ratsam.

4 Vertiefung ausgewählter Themen

4.1 Nähere Vereinbarung des Vertragsgegenstands

Es gibt keine gesetzlichen Anforderungen an die Ausgestaltung von Leistungsbeschreibung und Leistungspflichten in Cloud-Verträgen. Fehlen konkrete Vereinbarungen im Vertrag, gilt für die hier als Beispiel dienenden SaaS-Verträge in der Public Cloud das gesetzliche Mietrecht (vgl. oben Kapitel 1.2). Danach hat der Anbieter die Pflicht, die Mietsache (hier also die Software) in einem zum vertraglichen Gebrauch geeigneten Zustand bereitzustellen und während der Vertragslaufzeit in diesem Zustand zu halten.

Die Vertragspartner können jedoch die Inhalte der gegenseitigen Leistungs- und Vergütungspflichten definieren. Es empfiehlt sich, von dieser Möglichkeit Gebrauch zu machen und die Leistungspflichten im Vertrag vollständig und abschließend zu formulieren. Die Konkretisierung des Leistungsgegenstands ist einer gerichtlichen Nachkontrolle nach den Grundsätzen des AGB-Rechts entzogen (vgl. BGH, Urteil vom 12. Dezember 2000 – XI ZR 138/00).

Doch Vorsicht: Anders als die reine Beschreibung der Leistung unterliegen die in AGB niedergelegten Sanktionen für Nicht- oder Schlechterfüllung oder deren Einschränkungen einer vollen gerichtlichen Nachkontrolle. Es bedarf hoher Sorgfalt, den Leistungsumfang so festzulegen, dass diese Festlegung nicht als Ausschluss gesetzlich festgelegter Sanktionen interpretiert und dann für unwirksam gehalten wird. Es ist daher empfehlenswert, im Vertragstext deutlich zwischen Leistungsbeschreibung und Sanktion zu unterscheiden.

Grundsätzlich muss der Anbieter das Zweckmäßige und Zumutbare zur Vertragserfüllung leisten. Die Anforderungen an ihn sind umso höher, je sensibler die ihm anvertrauten Daten sind. Dem Anbieter fällt jedoch keine Pflicht zu, sich nach der Sensibilität und der Schutzbedürftigkeit der ihm vom Kunden übermittelten Daten zu erkundigen. Insbesondere kann Anbietern, die unspezifische, auf die Verarbeitung nicht explizit schutzwürdiger Daten ausgerichtete Software anbieten, keine solche Erkundigungspflicht zugeschrieben werden. Es obliegt vielmehr dem Kunden, Erkundigungen einzuholen und zu beurteilen, ob das Schutzniveau eines konkreten Cloud-Angebotes für die in Frage stehenden Daten ausreichend ist. Teilweise finden sich daher in Cloud-Verträgen Regelungen, wonach sich der Kunde davon überzeugt hat, dass das Sicherheitsniveau und die technischen Voraussetzungen eines Cloud-Angebots seinen Anforderungen im konkreten Fall entsprechen. Der Anbieter hätte nur dann eine Hinweispflicht, wenn er positive Kenntnis von einem besonderen Schutzbedürfnis der Kundendaten hat und erkennen müsste, dass die von ihm angebotenen Leistungen dieses Schutzniveau unterschreiten.

Die Verarbeitung von nicht-personenbezogenen Daten in einer Public Cloud ist ohne die Erfüllung von speziellen technischen, rechtlichen oder tatsächlichen Anforderungen zulässig.

Sobald jedoch personenbezogene Daten gleich welcher Art und in welchem Umfang in einer Public Cloud verarbeitet werden, greifen datenschutzrechtliche Anforderungen (z. B. aus dem BDSG, TMG oder SGB I; für besondere Arten personenbezogener Daten gelten teilweise weitere spezielle Regelungen). Hierbei ist zu beachten, dass das BDSG die Auffangregelung für den Fall darstellt, dass keine spezialgesetzliche Regelung zum Datenschutz existiert. Adressat dieser gesetzlichen Vorgaben ist zunächst der Kunde. Der Anbieter sollte jedoch proaktiv Vorkehrungen treffen und Vereinbarungen bereithalten, da mit entsprechenden Anfragen von Kunden zu rechnen ist. Zu den vertraglichen Vereinbarungen in diesen Fällen siehe unten Kapitel 4.8.

Auch wenn die Frage, welche Daten in der Cloud verarbeitet werden sollen, in die Verantwortung des Kunden fällt, können der Auslagerung von gesetzlich besonders

geschützten Daten (z. B. Daten, die dem Arzt- oder Anwaltsgeheimnis unterliegen) in eine Public Cloud gesetzliche Verbote entgegenstehen (z. B. § 203 StGB). Eine Verlagerung solcher Daten in eine Cloud wäre allenfalls unter besonderen Vorkehrungen zulässig.

4.2 Konkretisierung des Leistungsumfangs

Die vertragstypischen Leistungspflichten eines SaaS-Anbieters umfassen insbesondere die Bereitstellung und Wartung der benötigten Software, Hardware und Infrastruktur. Zusätzlich schuldet der Anbieter:

- Einräumung von Nutzungsmöglichkeiten für die Anwendungsprogramme (Lizenzierung (falls erforderlich), Verbindung zum Internet);
- Betrieb und Pflege der Anwendungsprogramme, hierzu gehören auch Bereitstellung und Aufspielung von Patches;
- Speicherung und Sicherung der Anwendungsdaten des Kunden; dazu gehören Betrieb einer Firewall und sonstiger üblicher Sicherheitsmaßnahmen sowie übliche Prävention gegen Datenverlust;
- Reporting zum Nutzungsumfang durch den Kunden als Berechnungsgrundlage für die Vergütung;
- Bereitstellung der Kundendaten bei Beendigung der Vertragsbeziehung, soweit der Kunde die Daten nicht ohnehin nach seinen Bedürfnissen übertragen, löschen und auf eigenen Datenträgern sichern kann.

Bei einem Vertrag über die Nutzung von Software sollte zunächst der Leistungsumfang der Software anhand von wesentlichen Merkmalen beschrieben werden, z. B. durch:

- Einsatzbereich der Software;
- Leistungsumfang (Module, Funktionen o. ä.);
- Skalierbarkeit (Möglichkeit zur Erweiterung der Nutzerzahl).

Die Konkretisierung der zu erbringenden Leistung und die Festlegung von Sanktionen bei unzureichender Leistungserbringung werden oft als Service Level Agreement (SLA) vereinbart. Ein SLA beschreibt im Einzelnen die Parameter der zu erbringenden Leistung in messbaren Einheiten, enthält Sanktionen bei Nichterreichen der Parameter und typischerweise auch den Messpunkt. Bleibt der Anbieter hinter diesen Anforderungen zurück, liegt eine Pflichtverletzung vor. Häufig wird dann das zu leistende Entgelt gemindert oder ein Schadensersatzanspruch gegen den Anbieter begründet.

Ein einzelner Service Level umfasst regelmäßig drei Komponenten und oft Sanktionen:

- Kurzbezeichnung (»Service Item«), z. B. »Reaktionszeit«;
- Beschreibung der geschuldeten Leistung zu diesem Aspekt (»Service Level Specification«), z. B. »Der Anbieter stellt dem Kunden eine Hotline zur Beantwortung von Anfragen bereit«;
- Messbare Zielvorgabe zur Leistungserfüllung (»Service Level Objective«), typischerweise als Leistungsparameter (Key Performance Indicator »KPI«) und Messpunkt; z. B.: »Eingehende Anfragen des Kunden werden innerhalb von zwei Stunden während der Betriebszeit per E-Mail bestätigt«;

  Wichtig: Bei einigen Service Levels sind ein genauer Messpunkt und sogar ein Messverfahren zu vereinbaren, sonst läuft die Vereinbarung ins Leere.

- Ggf. Sanktionen (nicht für jeden Service Level erforderlich); z. B. »Für jede vollendete Stunde Überschreitung ist ein Service Credit von x verwirkt.«

Typische und regelmäßig in Cloud-Verträgen anzutreffende SLA betreffen:

- Verfügbarkeit: die Verfügbarkeit des Softwarezugriffs wird ausgedrückt als prozentualer Zeitanteil der Betriebszeit, in dem die Nutzung uneingeschränkt möglich ist (z. B. 98 Prozent). Wichtig: Ohne Angabe des Bezugszeitraumes wird keine klare Vereinbarung getroffen. Die Unterschiede sind beträchtlich: Eine Verfügbarkeit von 99,5 Prozent über ein ganzes Jahr erlaubt eine Nichterreichbarkeit des Cloud-Dienstes (»down time«) von rund 43 Stunden; 99,5 Prozent bezogen auf einen Monat entspricht nur rund 3,5 Stunden Nutzungsausfall. Vorsicht ist geboten bei unrealistischen Verfügbarkeiten! Eine Verfügbarkeit von 99,99 Prozent bedeutet max. eine Minute Ausfallzeit pro Woche bzw. max. 52 Minuten Ausfallzeit im Jahr. Im Vergleich dazu bedeutet 99,9 Prozent max. zehn Minuten Ausfallzeit pro Woche oder max. 8,5 Stunden Ausfallzeit im Jahr. Andererseits ist aus Sicht des Kunden nicht für jede Anwendung eine permanente Hochverfügbarkeit erforderlich, so z. B. für Anwendungen, die nur während üblicher Bürozeiten genutzt werden. Zu beachten ist, dass eine höhere Verfügbarkeit auch deutlich höhere Kosten bedeutet oder gar nicht angeboten wird.

> **!** Achten Sie bei der Angabe von Verfügbarkeiten eines Cloud-Angebots auf den Bezugszeitraum und auf die Definition von Ausfallzeiten.

Ferner ist zu klären, ob Zeiten von Nichterreichbarkeit eines SaaS-Angebotes wegen geplanter oder ungeplanter Wartung oder die Überschreitung einer Reaktionszeit bei Störungen als Ausfallzeit anzusehen ist oder nicht. Es ist branchenüblich, Wartungszeiten zu vereinbaren, in denen die Cloud-Leistung nicht verfügbar ist.

Der Messpunkt für die Verfügbarkeit sollte im Rechenzentrum des Anbieters liegen, und dies sollte auch im Vertrag festgehalten sein. Ansonsten könnten Netzausfälle in die Risikosphäre des Anbieters fallen, obwohl er diese nicht beeinflussen kann. Der Anbieter hat allerdings dafür zu sorgen, dass die von ihm betriebenen Server an das Internet angebunden und funktionstüchtig sind.

- Reaktionszeit bei Störung: Hierbei wird festgelegt, was der Anbieter bei einer Störung wie schnell unternehmen muss.

Service Items, die für die Skalierbarkeit einer Cloud-Leistung von besonderer Bedeutung sind, betreffen z. B.:

- Elastizität: Fähigkeit zur Erweiterung von Ressourcen (meist im Rahmen bestimmter Grenzwerte wie Bandbreite, Speicherkapazität usw.); ein möglicher Mehrbedarf des Kunden sollte bereits bei Vertragsgestaltung mitbedacht werden. Entsprechend sollte auch die Vergütung für eine Ausweitung des Nutzerkreises oder der Speicherkapazität im ursprünglichen Vertrag geregelt sein.

- Agilität: Geschwindigkeit, mit der ein Provider auf Skalierungsanforderungen reagiert.

Ob diese Kriterien der Skalierbarkeit im Detail im Cloud-Vertrag vereinbart werden, ist den Parteien überlassen.

Weitere denkbare bzw. sinnvolle Service Levels regeln z. B.:

- Betriebszeit: Zeitraum innerhalb eines Tages, in der die Software genutzt werden kann, z. B. zwischen neun und 17 Uhr. Dies sollte insbesondere dann geregelt werden, wenn Anbieter und Kunde ihren Sitz in verschiedenen Zeitzonen haben und der Anbieter die Software nur zeitlich beschränkt zugänglich machen will. Wichtig: Ergeben sich aus dem Vertrag keine zeitlichen Vorgaben für die Nutzung des Cloud-Angebots, steht dem Kunden der Online-Zugriff auf den Rechner des Anbieters grundsätzlich unbeschränkt zu. Eine solche unbeschränkte Nutzungsmöglichkeit lässt sich nicht durch abweichende AGB wirksam beschränken (vgl. BGH, Urteil vom 12. Dezember 2000 – XI ZR 138/00).

! Das AGB-Recht lässt es nicht zu, alle Sanktionen für Verzug oder Schlechterfüllung pauschal in einem SLA zu regeln (z. B. über Pönale oder Credit Points). Es bedarf hier also stets noch Auffangregelungen zu Einzelfällen der Schlechtleistung und sonstiger Haftung. Die vertraglichen Sanktionen für die Unterschreitung eines Service Levels sind daher zu etwaigen gesetzlichen Folgen in ein Verhältnis zu setzen (Einzelheiten hierzu sprengen den Rahmen dieser Checkliste).

- Ort der Datenspeicherung und -verarbeitung: Wird im Vertrag keine besondere Ortsbestimmung vereinbart, kann der Anbieter die Cloud-Leistung aus einem Land seiner Wahl erbringen. Auch kann er die Anwendungsdaten seiner SaaS-Lösung beliebig zwischen Standorten in verschiedenen Ländern verschieben. Nicht in allen Staaten existiert jedoch ein gleich hohes Niveau für den Datenschutz oder ähnliche Standards für die Daten-sicherheit wie in Europa. In manchen Ländern haben auch Behörden oder gar Dritte leichteren Zugang zu Cloud-Daten als in Europa. Dies kann Konflikte mit dem deutschen Datenschutzrecht und anderen gesetzlichen Regelungen gegen unbefugten Datenzugriff verursachen. In letzter Konsequenz kann die Anwendung des deutschen Datenschutzrechts dazu führen, dass personenbezogene Daten nicht in Ländern außerhalb des Europäischen Wirtschaftsraums (EWR) verarbeitet werden dürfen. Es sollte deshalb vertraglich vereinbart werden, in welchen Ländern und unter welchen rechtlichen Rahmenbedingungen die Anwendungsdaten des Kunden gespeichert und verarbeitet werden dürfen. Dem Kunden ist vor Nutzung einer SaaS-Anwendung eine Analyse seiner Daten und ggf. eine Trennung in personenbezogene, anderweitig schutzbedürftige und unkritische Daten anzuraten. Bei Bedarf kann der Speicherort der Daten auch im Vertrag festgelegt werden. Da dies den Anbieter in einer effizienten Nutzung seiner Ressourcen einschränken kann, wird er solchen Regelungen regelmäßig nicht ohne entsprechenden Vergütungsaufschlag zustimmen können.

Nicht nur für die Vertragsbeziehung insgesamt, sondern auch für einzelne Leistungskomponenten kann die Regelung zusätzlicher Punkte in einem SLA wichtig sein. Solche Punkte wären z. B.:

- Rahmenbedingungen;
- Berichtswesen (»Reporting«);
- Kommunikationspartner und -wege;
- Eskalationswege;
- Mitwirkungspflichten und Vorleistungen des Kunden.

4.3 Verfahren bei Vertragsänderung

Beim Cloud Computing können sowohl Leistungsinhalt (z. B. Bereitstellung neuer Software-Funktionen) als auch Leistungsumfang (z. B. weitere Nutzer, Bereitstellung zusätzlicher Speicherkapazität) geänderten Bedürfnissen des Nutzers angepasst werden. Bestimmte Erweiterungen und Anpassungen der vereinbarten Leistungen können bereits im Vorfeld vertraglich geregelt werden. Typischerweise werden z. B. Regelungen für die charakteristische Flexibilität und Skalierbarkeit vereinbart.

Für eine Leistungsänderung außerhalb der bereits vertraglich vereinbarten Bandbreiten und für nicht

vorhersehbare Leistungsänderungen empfiehlt es sich, ein formales Verfahren (Change-Request-Verfahren) zu definieren. Dabei ist zu beachten, dass im Rahmen eines Change-Request-Verfahrens der ursprüngliche Vertrag geändert wird. Daher sollten die Parteien klar festlegen, inwieweit vom ursprünglichen Vertrag abweichende Vereinbarungen gelten sollen und welche Teile des ursprünglichen Vertrags fortgelten sollen. Allerdings wird ein Change-Request-Verfahren regelmäßig nur in Frage kommen, wenn es sich um eine größere SaaS-Vertragsbeziehung mit verschiedenen unterschiedlichen Leistungspflichten handelt. Im Massengeschäft wäre die vielfache Durchführung eines formalen Vertragsänderungsverfahrens unverhältnismäßig und zu aufwändig.

4.4 Nutzungsumfang der bereitgestellten Software

Die Nutzung der im Rahmen eines SaaS-Geschäftsmodells bereit gestellten Software kann inhaltlich, zeitlich und räumlich zwischen dem Anbieter und seinen Kunden festgelegt werden. Inhaltliche Festlegungen beziehen sich auf das »Wie« der Nutzung, also die Art und Weise, in welcher die Software genutzt wird. Des Weiteren ist festzulegen, »Wer« die Software nutzen darf. Eine räumliche Festlegung bezeichnet das geographische Einsatzgebiet der Software, also z. B. Deutschland, Europa oder weltweit.

Für alle Arten von SaaS gilt: Der Anbieter muss für ausreichende Nutzungsrechte an der von ihm eingesetzten Software sorgen. Er muss insbesondere berechtigt sein, die Software im Rahmen eines Cloud Computing-Angebots für alle Länder, in denen ein Cloud-Zugang eröffnet wird, und mindestens für die Dauer seines Vertragsverhältnisses zu den Kunden der Cloud einzusetzen. Nach deutschem Urheberrecht muss der Rechtsinhaber einer Software seine Zustimmung zur Nutzung der Software im Rahmen eines Cloud-Angebotes geben (§ 69c UrhG). In dem Vertragsmodell, das diesem Leitfaden zugrunde liegt (SaaS in einer Public Cloud im B2B-Bereich), nimmt der Kunde keine Vervielfältigungshandlungen der Software im urheberrechtlichen Sinn vor. Der Anbieter muss gewährleisten, dass der Kunde die bereitgestellte Software unbeeinträchtigt von Rechten Dritter und vertragsgemäß nutzen kann.

Exkurs: Manche Software-Hersteller verlangen besondere Lizenzen ihrer Software, wenn diese im Cloud-Umfeld eingesetzt werden soll. Dies sollte der Anbieter mit seinem Software-Anbieter im Vorfeld abklären. Der Anbieter muss sicherstellen, dass die von ihm angebotene Software im Cloud-Umfeld und im beabsichtigten Umfang eingesetzt werden kann. Dies ergibt sich aus den Lizenzen des Software-Herstellers.

Der Anbieter benötigt vom Software-Anbieter (soweit diese nicht identisch sind) ein Nutzungsrecht an der Software, die ihm die Erbringung der Cloud Computing-Leistungen ermöglicht. Häufig ist ein entsprechendes Nutzungsrecht erforderlich für eine »unbegrenzte« Anzahl von Kunden, die jeweils wiederum »beliebig« viele Nutzer haben können. Die meisten bestehenden Software-Überlassungsverträge enthalten diese Berechtigung nicht, müssen also um entsprechende Regelungen erweitert werden. Darüber hinaus benötigt der Anbieter häufig das Recht, die Software auf »beliebig« vielen Servern zu installieren und dies möglicherweise weltweit.

4.5 Kündigungsmöglichkeiten

Soweit im Vertrag keine abweichenden Regelungen getroffen sind, gelten für eine Vertragsbeendigung durch Kündigung folgende Grundsätze:

Ordentliche Kündigung: Im Rahmen einer ordentlichen Kündigung können beide Parteien den Vertrag durch entsprechende Mitteilung mit einer Kündigungsfrist beenden. Dafür muss weder ein Kündigungsgrund vorliegen noch angegeben werden. Die Vereinbarung einer festen Laufzeit oder einer Mindestlaufzeit schließt regelmäßig eine ordentliche Kündigung während dieser Laufzeit aus.

Kündigung aus wichtigem Grund: Bei Vorliegen eines wichtigen Grundes kann jede Partei den Vertrag durch entsprechende Mitteilung auch fristlos kündigen. Liegt der wichtige Grund in einer Pflichtverletzung der anderen Partei, muss zuvor eine Abmahnung mit Nachfristsetzung zur Bereinigung der Pflichtverletzung erfolgen (§ 543 Abs. 3 BGB).

4.6 Gewährleistung und Haftung des Anbieters

Die Gewährleistungsansprüche des Kunden hängen entscheidend davon ab, welche Leistungen und welcher Leistungsstandard vertraglich vereinbart sind. Die gesetzlichen Gewährleistungsrechte für Mängel und die Haftungsvorschriften des BGB werden den Interessen der Vertragspartner einer Cloud-Geschäftsbeziehung häufig nicht gerecht und führen vielfach nicht zu praktikablen Ergebnissen. Daher ist zu empfehlen, die geschuldete SaaS-Leistung und die Folgen einer Unterschreitung der Leistungsanforderungen in Form eines SLA im Vertrag selbst festzulegen (vgl. oben 2.2). Daneben sollten im Vertrag auch Haftungsfragen angemessen geregelt werden. Bei vertraglichen Abweichungen von den gesetzlichen Vorgaben sind die Anforderungen des AGB-Rechts zu beachten.

Entspricht die Cloud-Leistung nicht dem vertraglich geschuldeten Leistungsumfang oder der vertraglich geschuldeten Leistungsqualität, stehen dem Kunden grundsätzlich folgende gesetzliche Gewährleistungsansprüche zu:

a) Zurückbehaltungsrecht

Eine unvollständige oder nicht fristgemäße Bereitstellung der Leistung berechtigt den Kunden, die Zahlung des Mietzinses bis zur Einräumung der vollen Nutzungsmöglichkeit zurückzuhalten.

Beispiel: Die SaaS-Anwendung steht für einen kompletten Monat nur mit einem Teil des Leistungsumfangs (80 Prozent) zur Verfügung. Es besteht ein Zurückbehaltungsrecht am Mietzins, bis der Mangel behoben ist. Nachdem der Mangel beseitigt wurde, muss der Kunde den zurückbehaltenen Mietzins an den Anbieter auskehren.

Das Zurückbehaltungsrecht ist vertraglich abdingbar (auch formularmäßig in AGB).

b) Mietminderung

Darüber hinaus hat der SaaS-Kunde bei einem Mangel ein Minderungsrecht, wenn der Gebrauch nicht nur unerheblich eingeschränkt ist.

Beispiel: wie Buchstabe a). Der Kunde kann die Miete hier um 20 Prozent mindern.

Dieses Minderungsrecht ist jedoch grundsätzlich vertraglich beschränkbar.

c) Mangelbeseitigungsanspruch / Ersatzvornahme

Kommt der Anbieter mit der Beseitigung des Mangels in Verzug, so kann der Kunde gemäß den gesetzlichen Vorschriften den Mangel selbst beseitigen und Ersatz der erforderlichen Aufwendungen verlangen.

Beispiel: Die vertraglich vereinbarten SaaS-Anwendungen fallen komplett aus. Der Kunde setzt dem Anbieter eine angemessene Frist zur Beseitigung des Mangels. Der Mangel ist nach Ablauf der Frist nicht beseitigt worden.

In diesem Beispielsfall könnte der Kunde im Rahmen der Gewährleistung eine Ersatzvornahme durchführen. Bei SaaS-Leistungen erscheint dies aber schon wegen des fehlenden Zugriffs des Kunden auf die dazu notwendige Infrastruktur praktisch nicht möglich.

d) Schadensersatzanspruch

Neben den aufgezeigten Ansprüchen / Rechten kann der Kunde in folgenden Fällen Schadensersatz verlangen:

- Mangel ist bei Vertragsschluss vorhanden

  Beispiel: Die SaaS-Anwendung ist mit einem von Anfang an vorhandenen Programmierfehler behafte. Dabei ist nicht relevant, ob der Fehler die Gebrauchstauglichkeit der Software erst später konkret beeinträchtigt oder für einen Schaden ursächlich ist.

  Hier besteht nach dem Gesetz eine Garantiehaftung des Anbieters. Dies ist eine Durchbrechung der sonst im BGB vorhandenen Verschuldenshaftung und wird üblicherweise im Vertrag ausgeschlossen. Der Haftungsausschluss ist insoweit auch in AGB zulässig.

- Mangel entsteht später und ist vom Anbieter zu vertreten

  Beispiel: Durch fahrlässiges Handeln des Anbieters kommt es zu einem Ausfall nach Einspielung eines notwendigen Patches.

  Hier haftet der Anbieter auf Schadensersatz. Diese Regelung ist ebenfalls abdingbar (aber nur durch Individualvereinbarung, nicht in AGB).

- Anbieter befindet sich mit der Beseitigung des Mangels in Verzug

  Beispiel: Die vertraglich vereinbarten SaaS-Anwendungen fallen komplett aus. Der Anbieter haftet auf Schadensersatz. Auch diese Regelung ist abdingbar (aber nur durch Individualvereinbarung, nicht in AGB).

e) Außerordentliche Kündigung

Soweit ein erheblicher Mangel vorliegt und dieser nicht (nach Setzung einer angemessenen Frist) beseitigt wird, kann der Kunde den Vertrag zudem außerordentlich kündigen, wenn eine Fortsetzung des Vertrages unzumutbar ist.

Beispiel: Die vertraglich vereinbarten SaaS-Anwendungen fallen komplett aus; auch innerhalb einer angemessenen Nachfrist tritt keine Besserung ein. Der Kunde kann hier außerordentlich kündigen. Die Voraussetzungen für die außerordentliche Kündigung können individualvertraglich in gewissen Grenzen gestaltet werden.

f) Haftung

Gesetzlich ist nach deutschem Recht eine zwingende Haftung für Vorsatz vorgesehen, die durch Vertrag nicht abgeändert werden kann. Üblich sind bei IT-Verträgen indes Vereinbarungen über Haftungs(-höchst-)beträge bei fahrlässig verursachten Schäden. Ebenso wie der Kunde ein Interesse am Ersatz solcher Schäden hat, hat der Anbieter ein nachvollziehbares Interesse daran, auf dem Wege der Haftung nicht das Geschäftsrisiko des Kunden zu übernehmen.

Während individuell vereinbarte Haftungsbeschränkungen in weitem Umfang zulässig sind, sind Haftungsbeschränkungen in AGB nur in bestimmten Grenzen rechtlich wirksam. Nicht selten werden Haftungshöchstbeträge als Prozentsätze der vertraglichen Vergütung festgelegt. Geschieht dies in AGB, besteht das Risiko für den Anbieter, dass diese Begrenzung von der Rechtsprechung nicht anerkannt wird. Sind AGB unwirksam, finden insoweit die gesetzlichen Vorschriften Anwendung.

4.7 Mitwirkungspflichten des Kunden

Da der Anbieter zugelieferten Daten ihre Schutzbedürftigkeit nicht ansieht, gehört es zu den Pflichten des Kunden, die Daten zu kategorisieren und z. B. als datenschutzrechtlich relevant gesondert zu speichern. Meist besteht eine solche Pflicht des Kunden schon von Gesetzes wegen. Solange der Kunde selbst Änderungen im Datenbestand vornimmt, bleibt er Herr der Daten, auch wenn er sich bei der Datenverarbeitung des Anbieters als Dienstleister bedient. Der Kunde ist also weiterhin im datenschutzrechtlichen Sinn für die von ihm dem Anbieter überlassenen personenbezogenen Daten verantwortlich und muss die rechtskonforme Datenverarbeitung sicherstellen.

Sobald für den Umgang mit den in die Cloud gestellten Daten besondere Vorkehrungen erforderlich sind, muss der Kunde den Anbieter darauf hinweisen. Zusätzlich zu der Hinweispflicht auf besondere rechtliche Anforderungen an die Datenhaltung muss der Kunde auch prüfen, ob der Anbieter mit seinem Angebot solche spezifischen rechtlichen Anforderungen überhaupt abdecken kann. Auch über mögliche technische Schwierigkeiten bei der Datenverarbeitung sollte der Kunde berichten. Die an den Anbieter übergebenen Daten sollten schon bei Vertragsschluss spezifiziert werden. Falls der Anbieter daraufhin zusätzliche Schutzmaßnahmen einrichten muss, ist ggf. eine Vertragsanpassung erforderlich.

Je mehr der Kunde dem Anbieter über die Natur der überlassenen Daten mitteilt, desto höher sind die Sorgfaltspflichten des Anbieters beim Umgang mit den Daten. Allerdings wird der Anbieter erhöhten Sorgfaltspflichten nicht mehr im Massengeschäft, sondern nur mit individuell auf die Bedürfnisse des Kunden angepassten Angeboten nachkommen können, wobei sich die Vergütung entsprechend erhöht. Erhält der Anbieter keine entsprechenden Informationen, kann er nicht haftbar gemacht werden.

Mitwirkungspflichten treffen den Kunden auch bei Vertragsanpassungen (change request) und bei der Einrichtung einer für Datenübermittlung und -verarbeitung tauglichen IT-Umgebung (z. B. beim Format der übermittelten Daten). Der Kunde ist schließlich auch dafür verantwortlich, dass die zu verarbeitenden Daten in verarbeitungsfähiger Form in den Verantwortungsbereich des Anbieters gelangen.

4.8 Datenschutz

a) Relevanz des Datenschutzrechts

Datenschutzrechtliche Vorschriften finden dann Anwendung, wenn und soweit personenbezogene Daten (§ 3 Abs. 1 BDSG) von den Cloud-Leistungen betroffen sind (zum Begriff der personenbezogenen Daten vgl. oben Kapitel 3.10). Nicht anwendbar ist das Datenschutzrecht auf anonymisierte personenbezogene Daten (§ 3 Abs. 6 BDSG), wenn die Daten also derart verändert wurden, dass ein Personenbezug durch den Anbieter oder durch Dritte nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand herstellbar ist. Durch eine Pseudonymisierung (§ 3 Abs. 6a BDSG) wird die Anwendbarkeit des Datenschutzrechts grundsätzlich nicht ausgeschlossen, da mit Hilfe weiterer Informationen das Pseudonym wieder aufgelöst werden kann.

b) Verarbeitung personenbezogener Daten beim Cloud Computing

Beim Cloud Computing ist die Verarbeitung von personenbezogenen Daten in zweierlei Hinsicht möglich:

- Zum einen im Rahmen einer Auftragsdatenverarbeitung; hier werden dem Anbieter personenbezogene Daten gemäß § 11 BDSG zur Verarbeitung durch den Kunden als verantwortlicher Stelle i.S.d. Datenschutzrechts überlassen.

- Zum anderen kann der Anbieter selbst zur verantwortlichen Stelle werden, indem er die Daten der Kunden (Name, Standort, IP-Adresse usw.) im Rahmen der Cloud-Nutzung erhebt bzw. verarbeitet. Die Erhebung und Verarbeitung von personenbezogenen Daten durch den Anbieter zur Durchführung und Dokumentation seiner vertraglichen Beziehung mit dem jeweiligen Kunden ist von der Auftragsdatenverarbeitung zu unterscheiden. Die Datenerhebung und -verarbeitung zur Vertragsdurchführung ist auf der Grundlage von § 28 Abs. 1 S. 1 Nr. 1 BDSG zulässig. Insoweit bedarf es keiner vertraglichen Regelung mit dem Kunden, dessen Daten betroffen sind.

Die Ausführungen im Folgenden beziehen sich ausschließlich auf die Verarbeitung von Kundendaten in der Cloud (im Sinne des ersten Gliederungspunktes).

Das Datenschutzrecht verwendet eine eigene Terminologie, die für die Darstellung in diesem Kapitel übernommen wird. Eine Person oder ein Unternehmen, das personenbezogene Daten über andere Personen erhebt, verarbeitet oder nutzt, wird als verantwortliche Stelle bezeichnet (§ 3 Abs. 7 BDSG). In einer Geschäftsbeziehung, die eine Verarbeitung personenbezogener Daten zum Inhalt hat, ist der Kunde als verantwortliche Stelle anzusehen. Nutzt der Kunde für seine Datenverarbeitung die Dienste eines SaaS-Anbieters, liegt regelmäßig eine Auftragsdatenverarbeitung vor. Dabei gilt der Kunde aus datenschutzrechtlicher Sicht als Auftraggeber, der Anbieter als Auftragnehmer.

c) Auftragsdatenverarbeitung

Die Auftragsdatenverarbeitung in der Cloud unterscheidet sich in den rechtlichen und vertraglichen Anforderungen nicht wesentlich von der herkömmlichen Auftragsdatenverarbeitung (zu den Besonderheiten vgl. unten d)). Der Auftraggeber bleibt als verantwortliche Stelle für die Daten verantwortlich, auch wenn er für die Datenverarbeitung Cloud-Leistungen in Anspruch nimmt.

Diese Verantwortung kann nicht auf den Auftragnehmer ausgelagert werden (§§ 3 Abs. 7, 11 Abs. 1 S. 1 BDSG). Die Auftragsdatenverarbeitung stellt eine privilegierte Art der Datenverarbeitung dar; denn durch die weisungsgebundene Beauftragung gelten nicht die strengeren Anforderungen der Datenübermittlung an Dritte. Vielmehr muss der Auftraggeber für die Datenverarbeitung so haften, wie wenn er sie selbst durchführen würde. Dies gilt jedoch nur für die Verarbeitung von Daten durch einen Auftragnehmer innerhalb des Europäischen Wirtschaftsraumes (EWR). Außerhalb dieses Gebietes wird ein Auftragnehmer einem sonstigen Dritten gleichgestellt.

Wesentliche Voraussetzungen für eine Auftragsdatenverarbeitung gemäß § 11 BDSG sind:

- Der Auftraggeber trifft die Entscheidungen über die Datenverarbeitung und erteilt entsprechende Weisungen an den Auftragnehmer.

- Der Auftraggeber hat den Auftragnehmer unter Berücksichtigung der Eignung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sogfältig auszuwählen (§ 11 Abs. 2 S. 1 BDSG).

- Der Auftrag bedarf der Schriftform (§ 11 Abs. 2 S. 2 BDSG), wobei der in dieser Vorschrift enthaltene 10-Punkte-Katalog den Mindestumfang der vertraglich zu regelnden Punkte bestimmt (vgl. Hinweis unten).

- Ferner ist sicherzustellen, dass der Auftragnehmer die Daten nur im Rahmen der durch den Auftraggeber erteilten datenschutzrelevanten Weisungen erhebt, verarbeitet oder nutzt (§ 11 Abs. 3 BDSG). Der Auftraggeber sollte seine Weisungen dokumentieren, am besten schriftlich erteilen.

- Schließlich muss der Auftraggeber die Einhaltung der Weisungen überprüfen (§ 11 Abs. 2 S. 4 BDSG).

10-Punkte-Katalog mit Mindestinhalten für einen Auftrag zur Datenverarbeitung:

1. Gegenstand und Dauer des Auftrags;
2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen;
3. die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen;
4. Berichtigung, Löschung und Sperrung von Daten;
5. die nach § 11 Absatz 4 BDSG bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen;
6. etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen;
7. Kontrollrechte des Auftraggebers und entsprechende Duldungs- und Mitwirkungspflichten des Auftragnehmers;
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen;
9. Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält;
10. Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Um Unternehmen bei der Umsetzung der Anforderungen in § 11 Abs. 2 BDSG zu unterstützen, hat BITKOM eine Mustervertragsanlage zur Auftragsdatenverarbeitung erarbeitet, die auf der BITKOM-Homepage frei verfügbar ist (vgl. www.bitkom.org/de/themen/50792_78385.aspx).

d) Besonderheiten der Auftragsdatenverarbeitung in der Cloud

Im Vergleich zur herkömmlichen Auftragsdatenverarbeitung ergeben sich folgende Besonderheiten bei der Auftragsverarbeitung in der Cloud, die von den Parteien vertraglich zu regeln sind:

- Wahrnehmung der Kontrollpflichten durch den Auftraggeber: Die räumliche Flexibilität in Bezug auf die Datenverarbeitung ist häufig ein wesentlicher Bestandteil von Cloud-Leistungen. Soweit dies der Fall ist, muss vertraglich sichergesellt werden, dass der Auftraggeber (SaaS-Kunde) zeitnah darüber informiert wird, wenn die Verarbeitung seiner Daten räumlich an einen anderen Standort verlagert wird. Damit kann sichergestellt werden, dass der Auftraggeber möglicherweise bestehenden Kontrollpflichten in Bezug auf den konkreten Standort nachkommen kann.

- Alternativ dazu kann auch bei Vertragsschluss eine Liste mit Orten vereinbart werden, an denen der Auftragnehmer generell und ohne weitere Information die Verarbeitung der personenbezogenen Daten des Auftraggebers vornehmen darf. Dem Auftraggeber muss es freistehen, für die vereinbarten Standorte die notwendigen Kontrollen durchzuführen bzw. durchführen zu lassen. Allerdings ist eine Kontrolle vor Ort nicht gesetzlich zwingend und nicht in jedem Fall verhältnismäßig. Alternativ kann der Anbieter eine Zertifizierung durch externe Sachverständige durchführen lassen, die eine Datenverarbeitung im Einklang mit den gesetzlichen Vorgaben bestätigt, und dieses Zertifikat dem Auftraggeber als Nachweis ordnungsgemäßer Datenverarbeitung zur Verfügung stellen. Allerdings besteht bislang kein gesetzlicher Rahmen für die Anerkennung bestimmter Zertifikate, so dass insoweit nach derzeitigem Stand eine Abstimmung bzgl. des Zertifikats mit den zuständigen Datenschutzbehörden zu empfehlen ist. Ferner können die Parteien ein regelmäßiges Reporting des Auftragnehmers an den Auftraggeber für gewisse Parameter der Datenverarbeitung vereinbaren.

- Weisungsrecht des Auftraggebers und Durchführungskontrolle: Um seiner Verantwortlichkeit nach dem Datenschutzrecht nachzukommen, muss sich der Auftraggeber, der personenbezogene Daten in die Cloud transferieren will, in Bezug auf die Verarbeitung dieser Daten gewisse Weisungsrechte vorbehalten (§ 11 Abs. 2 Nr. 9 BDSG). Es muss gewährleistet sein, dass der Auftragnehmer die Weisungen des Auftraggebers in Bezug auf die personenbezogenen Daten umsetzt und dass der Auftraggeber diese Umsetzung kontrollieren kann. Dies gilt vor allem in Bezug auf die Kontrolle einer ordnungsgemäßen Löschung der Daten durch den Auftragnehmer. Soweit der Kunde die Anforderungen des Datenschutzrechts in der Cloud selbst umsetzen kann, bedarf es keiner datenschutzrechtlicher Weisungen. Sollen darüber hinaus gehende Weisungsrechte vereinbart werden, ist bei der Vertragsformulierung darauf zu achten, dass diese Weisungsrechte nicht den Standard-Prozessen des Auftragnehmers zuwider laufen. Für Weisungen des Auftraggebers, die über die Standard-Prozesse des Auftragnehmers hinausgehen, kann die Durchführung eines Change-Request-Verfahrens vereinbart werden, was im standardisierten Massengeschäft jedoch allenfalls eingeschränkt möglich sein wird.

- Verpflichtung zum Datengeheimnis: Als Auftragnehmer einer Auftragsdatenverarbeitung hat der SaaS-Anbieter gemäß § 5 BDSG seine Mitarbeiter schriftlich zur Einhaltung des Datengeheimnisses zu verpflichten.

- Einschaltung von Subunternehmern durch den Auftragnehmer: Soweit der Auftragnehmer Subunternehmer in die Verarbeitung personenbezogener Daten einschalten möchte, muss er eine entsprechende Untervereinbarung mit dem Subunternehmer abschließen, die das angemessene Datenschutzniveau weiterhin gewährleistet. Hat der eingeschaltete Subunternehmer seinen Sitz außerhalb des EWR, ist zwischen ihm und dem Auftraggeber (SaaS-Kunde) eine eigene Vereinbarung zur Auftragsdatenverarbeitung abzuschließen. Es wird aber von den deutschen Datenschutzbehörden nicht beanstandet, wenn in einem solchen Fall der Auftragnehmer (SaaS-Anbieter) in Vertretung und im Namen des Auftraggebers die Vereinbarung zur Auftragsdatenverarbeitung mit dem Subunternehmer abschließt. Eine entsprechende Vollmacht hierfür sollte sich der Auftragnehmer ggf. bereits im SaaS-Vertrag vom Auftraggeber einräumen lassen.

- Verlagerung der Verarbeitung von personenbezogenen Daten: Eines der Kernprobleme des globalen Cloud Computing bei Verarbeitung personenbezogener Daten ist die Verlagerung der Datenverarbeitung in ein Land außerhalb des EWR. Eine solche Verlagerung ist nach deutschem Recht nur zulässig, wenn zum einen für die Übermittlung der Daten eine gesetzliche Erlaubnis oder die Einwilligung der Betroffenen vorliegt und zum anderen sichergestellt ist, 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 für Andorra, Argentinien, Australien, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Kanada (teilweise), Schweiz, Uruguay und Neuseeland). Für alle anderen Staaten außerhalb des EWR muss ein angemessenes Datenschutzniveau durch zusätzliche Maßnahmen hergestellt werden. In Betracht kommen insbesondere:

  - Zertifizierung des Auftragnehmers nach dem US-EU Safe Harbor-Abkommen (dabei muss der Auftraggeber auch prüfen, ob der Auftragnehmer die Vorgaben des Abkommens einhält);

  - Vereinbarung der EU-Standardvertragsklauseln zwischen der verantwortlichen Stelle (Auftraggeber) und dem jeweiligen Auftragnehmer außerhalb des Europäischen Wirtschaftsraums ggf. erweitert durch nationale Vorgaben (z. B. BDSG);

  - Vereinbarung von Binding Corporate Rules (diese sind von den Aufsichtsbehörden zu genehmigen);

  - Einwilligung aller Betroffenen (kaum praxisrelevant).

- Legale Möglichkeiten Dritter zum Datenzugriff: Im Rahmen von Datenschutz und Datensicherheit kann die Pflicht eines SaaS-Anbieters immer nur darin bestehen, unbefugten Zugriff auf die ihm anvertrauten Daten zu verhindern. Allerdings kann der Anbieter gesetzlich verpflichtet sein, befugten Dritten (z. B. Behörden oder Geheimdiensten) Einblick in und Zugriff auf die bei ihm gespeicherten Daten zu gewähren (in Deutschland ist dies z. B. im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses niedergelegt). Soll die Datenverarbeitung in ein Land ausgelagert werden, in dem legal auf eine Weise auf Daten zugegriffen werden kann, die im Land des Auftraggebers illegal wäre, sind diese Zugriffsmöglichkeiten – soweit möglich – vertraglich explizit auszuschließen. Wenn das nicht wirksam möglich ist (etwa, weil die Zugriffsmöglichkeiten zugunsten einer Behörde bestehen), kann vereinbart werden, dass der SaaS-Kunde über solche Zugriffe, soweit rechtlich möglich, informiert wird, damit er sich dagegen wehren kann. Die negativen praktischen Folgen eines Datenzugriffs in bzw. aus einem Drittstaat können durch eine Pseudonymisierung oder Verschlüsselung der Daten verringert werden.

Liste der Abkürzungen

AGB	Allgemeine Geschäftsbedingungen: Vertragsinhalte, die von einer Vertragspartei vorgegeben werden
ASP	Application Service Providing: Bereitstellung von individuellen IT-Leistungen über das Internet
B2B	business to business: Geschäftsverkehr zwischen Unternehmen
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof: höchstinstanzliches Gericht für Rechtsprechung im Zivilrecht in Deutschland
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
bzw.	beziehungsweise
EWR	Europäischer Wirtschaftsraum
ggf.	gegebenenfalls
i.S.d.	im Sinne des
SaaS	Software as a Service: Geschäftsmodell im Cloud Computing, bei dem der Anbieter Anwendungsprogramme in standardisierter Form für eine Vielzahl von Kunden bereitstellt
SGB	Sozialgesetzbuch
SLA	Service Level Agreement: Vereinbarung von Leistungsparametern und von Sanktionen bei ihrer Unterschreitung
StGB	Strafgesetzbuch
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)
usw.	und so weiter
vgl.	vergleiche
z. B.	zum Beispiel
ZPO	Zivilprozessordnung

BITKOM vertritt mehr als 2.200 Unternehmen der digitalen Wirtschaft, davon gut 1.400 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 200 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. Mehr als drei Viertel der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils knapp 10 Prozent kommen aus sonstigen Ländern der EU und den USA, 5 Prozent aus anderen Regionen. BITKOM setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org