IT-Cluster Wien | Gruppe Cloud Computing

Herausgeber: Paul Meinl

Software as a Service – Verträge richtig abschließen

2., erweiterte Auflage

wirtschaftsagentur wien

Ein Fonds der Stadt Wien

Unterstützt von:

COMPUTERWELT

Stadt Wien
Wien ist anders.

Von der Europäischen Union zu 50% kofinanziert.

EUROPÄISCHE UNION
Europäischer Fonds
für regionale Entwicklung
Mit Europa für Wien

eu.Wien.at

Vorwort

Liebe Leserinnen und Leser,

Gerhard Hirczi
Geschäftsführer
Wirtschafts-
agentur Wien

als Teilbereich des Cloud-Computing zählt Software as a Service (SaaS) zu den Megatrends der heutigen Informationstechnologie. Die Idee ist so einfach wie zukunftsweisend: Die Software und IT-Infrastruktur wird bei externen IT-Dienstleistern betrieben und vom Kunden als Service genutzt. Das SaaS-Modell bietet für Unternehmen zahlreiche Vorteile: Zum einen aufgrund der flexibleren, standortunabhängigen Zugriffsmöglichkeiten, zum anderen werden die IT-Kosten reduziert und besser plan- und steuerbar.

Unbedingt berücksichtigt werden muss in diesem Zusammenhang jedoch die Frage der IT-Sicherheit und der rechtlichen Aspekte dieses Outsourcings. Wer ist für welche Systemteile verantwortlich, was passiert im Störungsfall, wie wird der Datenschutz gewährleistet – diese und viele andere Fragen sind in der Entscheidung für oder gegen die Nutzung von Software as a Service entscheidend.

Der IT-Cluster der Wirtschaftsagentur Wien setzt sich seit Jahren mit den rechtlichen Aspekten und Details von SaaS auseinander und präsentiert mit dem vorliegenden Leitfaden einen umfassenden Überblick über alle relevanten Fragestellungen. Es handelt sich bereits um die zweite, überarbeitete Neuauflage, die aufgrund der großen Nachfrage und des positiven Feedbacks aus der Branche erstellt wurde.

Ich wünsche Ihnen eine spannende Lektüre!

Ihr

Gerhard Hirczi
Geschäftsführer Wirtschaftsagentur Wien

Inhalt

Einleitung

Paul Meinl
Richter,
ehemaliger
Geschäftsführer
der factline
Webservices
GmbH
(factline.com)

„Application Service Providing“, „Software as a Service“ und nun **„Cloud Computing“** – unter immer neuen Namen werden seit über zehn Jahren Trends vorhergesagt, Marktpotentiale in astronomischen Größenordnungen identifiziert und neue Internet-Zeitalter ausgerufen. Auch wenn überzogene Erwartungen enttäuscht wurden, das Konzept, Software und Infrastruktur als Dienstleistung über das Internet anzubieten, ist unbestreitbar zu einer wesentlichen Säule moderner Informationstechnologie geworden.

Vor diesem Hintergrund ist wohl auch das folgende, Oracle-CEO Larry Ellison zugeschriebene[1] Statement zu „Cloud Computing“ zu verstehen:

> *„The interesting thing about cloud is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of this announcements... Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop? We'll make cloud computing announcements. I'm not going to fight this thing. But I don't understand what we would do differently in the light of cloud computing other than change the wording of some of our ads.“*

Auch zum Start unserer Arbeitsgruppe im Jahr 2004 wurden intensive Diskussionen über Begriffsdefinitionen geführt. Diese waren durchaus wichtig, um ein gemeinsames Verständnis zu zentralen Merkmalen zu entwickeln. Auf dieser Grundlage war es dann allerdings möglich, die Auseinandersetzung mit Begriffsabgrenzungen recht bald zugunsten der Bearbeitung zentraler rechtlicher und technischer Fragen ad acta zu legen.

Die verschiedenen Begriffe dienten uns nun hauptsächlich dazu, an aktuelle Trends angelehnte Namen für unsere Aktivitäten zu finden: Unter dem Titel „Rahmenbedingungen für Application Service Providing“ wurde ein Leitfaden zu „Software as a Service“ erarbeitet, der nun in zweiter Auflage durch die Gruppe „Cloud Computing“ publiziert wird...

Dennoch – oder gerade deswegen – war es uns wichtig, in dieser Auflage auch die wesentlichen Merkmale von „Cloud Computing“ näher darzustellen. Diese Aufgabe hat dankenswerter Weise Herr KommR Hans-Jürgen Pollirer

---

1 *http://gevaperry.typepad.com/main/2008/09/larry-ellisons-anti-cloud-computing-rant.html*

übernommen, der auf den folgenden Seiten in seinem Gastbeitrag eine systematische Einordnung der verschiedenen Begrifflichkeiten und ihrer wesentlichen Eigenschaften vornimmt.

Der geradezu reißende Absatz der 1. Auflage und das positive Feedback haben uns gezeigt, dass wir mit diesem Leitfaden eine Lücke füllen konnten. Wir sehen uns daher in unserem Vorhaben bestärkt, mit diesem Leitfaden der weiterhin herrschenden Unsicherheit beim Umgang mit SaaS wirksam entgegenzutreten.

Bei der Entwicklung dieser „Gebrauchsanweisung" wurde darauf geachtet, die grundlegenden, **allgemein relevanten Rahmenbedingungen** abzudecken. Es wurde stets versucht, eine zu Anbietern und Kunden neutrale Stellung einzunehmen und beide Sichtweisen ausreichend zu berücksichtigen; dies mit dem Ziel, einen **Interessensausgleich** zwischen diesen beiden Positionen zu ermöglichen.

Der Leitfaden soll als Grundlage für eine **zielgerichtete Diskussion** zwischen Anbieter und potenziellem Kunden dienen. Er ermöglicht es interessierten Kunden, die richtigen Fragen zu stellen und so die relevanten Rahmenbedingungen abzuklären. Außerdem soll er den Vergleich zwischen Alternativangeboten erleichtern. Anbietern wiederum gibt er die Möglichkeit, sich auf die entsprechenden Kundenfragen vorzubereiten sowie die Qualität ihres Angebots zu prüfen. Darüber hinaus leistet er einen Beitrag zu höherer Sicherheit in rechtlicher Hinsicht, indem er es erleichtert, den bestehenden gesetzlichen Bestimmungen beginnend mit den vorvertraglichen Aufklärungspflichten bis zur Phase nach Vertragsabschluss (z.B. Pflicht zur Datenlöschung) zu entsprechen.

Neu integriert wurden in diese Auflage praktische Hilfsmittel für Vertragsverhandlungen: Eine **„Themenübersicht"** dient zur zielgerichteten Vorbereitung, eine **„Checkliste"** als Arbeitsunterlage für die Vertragsverhandlungen. Überdies steht ein umfangreicher **„Fragenkatalog"** auf unserer Internetplattform **http://saas.clusterwien.at** zum Download zur Verfügung. Werden die in diesen Unterlagen angeführten Fragen zwischen Kunden und Anbieter hinreichend präzise diskutiert und beantwortet, dann liegt eine **solide Basis für die weitere Zusammenarbeit** vor.

Wie schon bei Erstellung der 1. Auflage engagierte sich neben Mitgliedern des IT-Clusters Wien auch der Arbeitskreis für IT-Leistungsverträge und -Rechtspolitik der **Österreichischen Computergesellschaft (OCG)** unter großen Einsatz für die Erstellung dieser Auflage. Vielen Dank für die unermüdliche Mitarbeit!

saas.clusterwien.at

Zum Begriff Cloud Computing

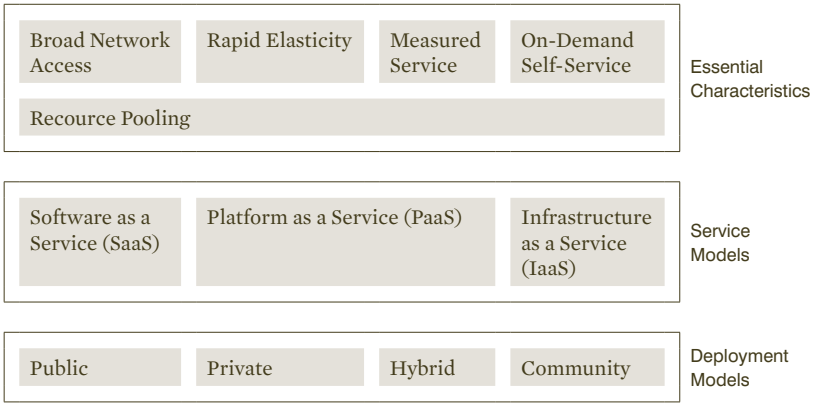
Gastkommentar von KommR Hans-Jürgen Pollirer, Obmann der Bundessparte Information und Consulting in der Wirtschaftskammer Österreich

„Software as a Service“ (SaaS) ist ein Teilbereich des heutigen IT-Megatrends, nämlich des „Cloud Computing“, wobei gerade SaaS für die kleinstrukturierte Wirtschaft Österreichs[1] große Chancen bietet, IT-Leistungen kostengünstig beziehen zu können. Die im vorliegenden Leitfaden enthaltenen Fragen machen aber deutlich, dass der SaaS-Anbieter sorgfältig auszuwählen und der Vertragsgestaltung entsprechendes Augenmerk zu widmen ist.

„Cloud Computing“ stellt eigentlich einen Sammelbegriff für bereits seit längerem existierende IT-Konzepte wie Outsourcing, Grid-Computing sowie Application-Service-Providing (ASP) als Vorläufer des SaaS dar.

Von den vielen – durchaus unterschiedlichen – Definitionen von Cloud Computing hat sich in der Fachwelt jene des U.S. National Institute of Standards and Technology (NIST)[2] durchgesetzt:

NIST Visual Model of Cloud Computing Definition[3]



1 *99,6 % der insgesamt ca. 300.000 österreichischen Unternehmen sind nach der Definition der europäischen Union KMUs, also Kleinstunternehmen sowie kleine und mittlere Unternehmen mit weniger als 250 Mitarbeitern, wobei 88 % aller österreichischen Unternehmen weniger als 10 Mitarbeiter beschäftigen.*

2 *http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf*

3 *Vgl Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 14, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf*

NIST definiert Cloud Computing zunächst durch das notwendige Vorhandensein von 5 **EIGENSCHAFTEN** (Essential Characteristics), unterscheidet 3 verschiedene **SERVICE MODELLE** (Service Models) und schlussendlich 4 unterschiedliche **BETRIEBSMODELLE** (Deployment Models): Im Einzelnen beinhalten diese Bezeichnungen Folgendes:

EIGENSCHAFTEN

- **Breitbandnetzwerkzugang** – der Cloud-Nutzer kann in Echtzeit unter Einsatz von Standardtechnologie über Mobiltelefone, Laptops und PDAs auf die verschiedenen Cloud-Dienste zugreifen.

- **Schnelle Elastizität** – die notwendigen Ressourcen werden schnell und elastisch – in manchen Fällen auch automatisch – dem Cloud-Nutzer bedarfsgerecht zur Verfügung gestellt. Der Cloud-Nutzer gewinnt dadurch die Illusion, dass er unbeschränkten Zugriff auf die Ressourcen hat.

- **Messbare Dienste** – die Cloud-Systeme verfügen über eingebaute Kontroll- und Messfunktionen, die – abhängig von der Art des Cloud-Dienstes – den Ressourcenverbrauch optimieren. Dadurch wird sowohl dem Cloud-Provider als auch dem Cloud-Nutzer entsprechende Transparenz in Bezug auf die in Anspruch genommenen Dienste gewährleistet.

- **On-Demand Self-Service** – der Cloud-Nutzer kann Dienste und Ressourcen selbständig anfordern, ohne dass eine menschliche Interaktion mit dem Cloud-Provider notwendig ist.

- **Ressourcen-Pooling** – die Ressourcen des Cloud-Anbieters werden gebündelt und den Cloud-Nutzern entsprechend ihren Anforderungen dynamisch zur Verfügung gestellt. Die angebotenen Dienste sind durch eine Ortsunabhängigkeit gekennzeichnet. Das bedeutet, dass der Cloud-Nutzer weder eine Kontrolle hat, noch über das Wissen verfügt, woher die ihm angebotenen Dienste geografisch kommen. Im besten Fall kann er den Ort der Dienstleistung auf einem höheren Abstraktionsniveau feststellen (z.B. Land, Staat oder Rechenzentrum).

CLOUD SERVICE MODELLE

Das NIST-Modell unterscheidet 3 verschiedene archetypische Service Modelle, in der Fachliteratur auch kurz als das „SPI-Modell“ bezeichnet (Software, Plattform und Infrastruktur). Diese 3 Modelle unterscheiden sich hinsichtlich des Inhaltes der dem Cloud-Nutzer zur Verfügung stehenden Services.

- **Software as a Service (SaaS)** – bei diesem Cloud-Service verwendet der Cloud-Nutzer die ihm vom Cloud-Provider angebotenen Softwareanwendungen, die auf einer Cloud-Infrastruktur betrieben werden. Der Cloud-Nutzer greift über verschiedene Endgeräte über einen Webbrowser auf die gewünschten Softwareanwendungen zu. Der Cloud-Nutzer hat keinerlei Kontrolle, weder über die ihm zur Verfügung gestellte Cloud-Infrastruktur noch über die Softwareanwendungen. Typische Beispiele für SaaS sind z.B. salesforce.com, SAP Business by Design, Apple iWork.com, Google Apps for Business, Microsoft CRM online.

- **Platform as a Service (PaaS)** – diese Variante bietet dem Cloud-Nutzer die Möglichkeit, eigene Softwareanwendungen innerhalb einer ihm über eine Plattform zur Verfügung gestellten Entwicklungsumgebung zu erstellen und zu betreiben. Im Gegensatz zu SaaS behält der Cloud-Nutzer bei dieser Serviceform die Kontrolle über die Softwareanwendung. Als Beispiel für PaaS kann man Google Apps Engine, Windows Azure und IBM Smart Business Developement anführen.

- **Infrastructure as a Service (IaaS)** – Sinn und Zweck dieses Cloud-Services ist es, dem Cloud-Nutzer Rechenzeit, Speicherplatz, Netzwerk und andere IT-Komponenten zur Verfügung zu stellen, sodass er in die Lage versetzt wird, seine Softwareanwendungen nach seinem Belieben zu betreiben. Bei diesem Cloud-Service hat der Cloud-Benutzer keinerlei Kontrolle in Bezug auf die Cloud-Infrastruktur, jedoch sehr wohl über Betriebssysteme, Speicher, eingesetzte Softwareanwendungen und unter Umständen eine eingeschränkte Kontrolle über einzelne Netzwerkkomponenten (z.B. Firewall). Typische Beispiele für diesen Cloud-Dienst sind Oracle, IBM und Amazon EC2 und S3.

BETRIEBSMODELLE

Ungeachtet der 3 Cloud-Service Modelle – SaaS, PaaS und IaaS – unterscheidet NIST 4 verschiedene Betriebsmodelle, und zwar die:

- **Öffentliche Cloud** – bei diesem Betriebsmodell wird die Cloud-Infrastruktur der Öffentlichkeit oder auch einer großen Industriegruppe durch einen Cloud-Anbieter zur Verfügung gestellt.

- **Private Cloud** – bei dieser Variante steht die Cloud-Infrastruktur nur einer geschlossenen Gruppe (z.B. Konzern) zur Verfügung, wobei die Cloud-Infrastruktur nicht unbedingt an einem Standort installiert sein muss und auch durchaus durch einen Dritten (z.B. Dienstleister) betrieben werden kann.

- **Community Cloud** – bei diesem Betriebsmodell schließen sich mehrere Cloud-Anbieter zusammen und servicieren eine spezifische Cloud-Nutzergruppe, die gemeinsame Anforderungen aufweist.

- **Hybride Cloud** – darunter versteht man den Zusammenschluss von mindestens zwei verschiedenen Cloud-Modellen, wobei die einzelnen Cloud-Anbieter unabhängig bleiben, aber über standardisierte oder proprietäre Technologien so verbunden sind, dass sowohl die Daten- wie auch die Softwareinteroperabilität unterstützt wird.

1.0

Der SaaS-Vertrag

1.1 Vertragliche Regelung aller voraussichtlich strittigen Punkte

Um nachträgliche Streitigkeiten um oder über einen Vertrag möglichst zu vermeiden, ist es sinnvoll, schon in der Vorbereitung zu einem Vertrag die **möglichen Streitigkeiten** vorherzusehen und entsprechende Regelungen zu vereinbaren. Dabei ist allerdings im Auge zu behalten, dass nicht das Recht nur auf einer Seite und die Pflichten bei der anderen Partei festgelegt werden. Solche Regeln werden von den Gerichten häufig wegen schwerer Äquivalenzstörungen als sittenwidrig und somit als ungültig erachtet. Man erreicht damit also das Gegenteil dessen, was man ursprünglich wollte.

Am häufigsten entstehen Vertragsstreitigkeiten, weil beide Seiten sich nicht wirklich den Kopf darüber zerbrochen und geklärt haben, was sie eigentlich wollen und was wirklich geleistet werden kann. Zu oft fließen in die Beschreibung der Leistung Überlegungen ein, die entweder vage Werbeaussagen enthalten oder Wunschdenken wiedergeben.

Tritt man in Vertragsverhandlungen ein, sollten daher beide Parteien **möglichst offen** miteinander reden. Dies ist in der Anfangsphase aus Gründen der Geheimhaltung oder aus der Befürchtung heraus, durch das Ansprechen unangenehmer Wahrheiten den Vertragsabschluss zu gefährden, oft schwierig, aber unvermeidbar. Verschweigt man nämlich in dieser Phase zu viel, dann riskiert man gravierende Schwierigkeiten bei der Vertragserfüllung, da über bestimmte wichtige Punkte kein tatsächliches Einvernehmen hergestellt wurde. Dies kann zur Folge haben, dass die fehlende Aufklärung des Vertragspartners als Verschulden gewertet wird und zum Schadenersatz führt. Dieser wird dann allerdings außerhalb der vertraglichen Regelung und nach den gesetzlichen Bestimmungen bewertet.

Offenheit zwischen Kunden und Anbietern – schon in der Anfgangsphase – vermeidet Schwierigkeiten bei der Vertragserfüllung.

Die **Leistungsbeschreibung** und die **Gegenleistung in Geld** sind durch nichts ersetzbar und die wichtigsten Teile eines Vertrags. Ist man sich darüber einig, kommt in aller Regel ein gültiger Vertrag zustande. Die

weiteren sehr wichtigen Punkte sind die Art, der Ort und die Zeit der Erfüllung des Vertrags. Insbesondere die Zeit wird oft strittig, weil die Partei, die die Leistung erbringen soll, sich oftmals überschätzt und Zusagen macht, die sie nicht einhalten kann, nur um den Auftrag zu erhalten. Die dadurch geweckten Erwartungen werden enttäuscht und der Vertrag gerät in eine Schieflage, die vermieden werden kann, wenn man realistische Zeitangaben macht.

1.2 Vertragsinhalt

1.2.1 Vertragsgegenstand

Eine klare, eindeutige und verständliche Beschreibung des Vertragsgegenstands ist die Voraussetzung für einen guten Vertrag.

Wie bereits oben angedeutet, ist die Beschreibung des Vertragsgegenstandes der **wichtigste Teil** eines guten Vertrags. Jeder Aufwand, der in diese Beschreibung gesteckt wird, ist in der Regel dann gut angelegt, wenn die Beschreibung möglichst klar, eindeutig und verständlich ist. Man verlasse sich nicht auf ohnehin bekannte Begriffe oder gar Abkürzungen. Die andere Partei könnte das alles ganz anders interpretieren und der Streit liegt auf der Hand. Dies bedeutet nicht, dass romanhafte Beschreibungen verfasst werden sollen. Ziel muss sein, dass das, was die beiden Vertragsparteien wollen, auch für einen vernünftigen Dritten verständlich und eindeutig beschrieben wird. Da die Leistungsbeschreibung dennoch sehr kompliziert ausfallen kann, ist es mitunter durchaus sinnvoll, eine Kurzfassung in den Vertragstext und die eigentliche Leistungsbeschreibung in einen (rechtlich ebenso verbindlichen) Anhang zu verlegen. Sinnvoll kann es weiters sein, Zwischenziele („Milestones“) in die Leistungsbeschreibung aufzunehmen, damit man daran die Erfüllung des Vertrags kontrollieren kann.

Ein nicht zu vernachlässigender Punkt ist der Einfluss höherer Gewalt auf den Vertragsgegenstand. Beim klassischen Mietvertrag ist die herrschende Meinung und Rechtsprechung, dass der vom Vermieter unverschuldete Untergang der gemieteten Sache oder deren weitgehende Unbrauchbarkeit den Mietvertrag beenden. In Analogie zum Mietvertrag würde auch der unverschuldete Untergang der IT-Infrastruktur des Service-Anbieters oder deren weitgehende Unbrauchbarkeit – durch

welche Einflüsse auch immer – den Vertrag beenden. Das kann aber vom Kunden in der Regel nicht ohne Weiteres hingenommen werden und zwar vor allem dann nicht, wenn dadurch die Existenz seines Unternehmens bedroht wäre. Das bedeutet, dass in den Fällen, in denen existenzielle Leistungen zum Service-Anbieter ausgelagert werden, dieser in jedem Fall eine Ersatzlösung anbieten muss, die diese Bedrohung des Kunden vermeidet. Die Lösung liegt in redundanten IT-Infrastrukturen, die physisch getrennt sind und bei Großstörungen der einen IT-Infrastruktur die angebotenen Dienste schnell übernehmen können. Dies bleibt natürlich nicht ohne Einfluss auf die Kosten.

1.2.2 Begriffsbestimmungen

Da vor allem mit der Fachsprache nicht vertraute Parteien oft hilflos diversen Fachbegriffen und Abkürzungen gegenüberstehen (die noch dazu in unterschiedlicher Bedeutung verwendet werden), ist die Verwendung von Begriffsbestimmungen in einem Vertragswerk sehr hilfreich. Dies kann den Vertrag auch erheblich übersichtlicher gestalten, weil der gerade verwendete Fachbegriff nicht immer erläutert oder umschrieben werden muss. Insbesondere Abkürzungen werden in der IT-Branche sehr häufig verwendet und müssen daher unbedingt in ihrer Bedeutung festgelegt werden.

1.2.3 Bereitstellung, Betrieb und Betreuung

Im Verbindung mit der Leistungsbeschreibung ist darzustellen, wie die vereinbarte Leistung erbracht werden soll, d.h. mit welchen Verfügbarkeiten die leistungsempfangende Partei rechnen kann. Jedenfalls muss ein Messzeitraum definiert werden, weil die Verfügbarkeit ein Wahrscheinlichkeitsurteil dafür ist, in welchem Zeitraum die Leistung im Wesentlichen zur Verfügung steht. Ein Beispiel, wie dies geregelt werden kann, ist in Abschnitt → 3.2 dargestellt. Da es für einen Kunden durchaus **unterschiedliche Bedürfnisse** hinsichtlich der Verfügbarkeit der Dienste an verschiedenen Arbeitsplätzen geben kann, steht hier eine Reihe von vertraglichen Verfügbarkeiten zur Diskussion. Sie müssen aber alle hinsichtlich des Messzeitraums klar geregelt werden. Siehe dazu näher → 3.2.

1.2.4 Probleme, Fehler und Störungen

Einen nicht zu vernachlässigenden Einfluss auf die Vertragsgestaltung hat die sorgfältige Definition von Störungen.

Störungen werden hinsichtlich ihrer Ursachen und Konsequenzen unterschieden und haben Einfluss auf die Gewährleistung.

Relevant ist in diesem Zusammenhang die Unterscheidung folgender, oft synonym verwendeter Begriffe: Unter **Störung** ist eine offenkundig gewordene Beeinträchtigung zu verstehen, die sowohl technische und organisatorische **Fehler** als auch negative externe Einflüsse auf die Software-Dienstleistung (z.B. Blitzschlag, Hochwasser, Stromausfall über längere Zeit) umfasst. „**Mangel**“ wiederum ist ein juristischer Begriff, an den sich wichtige rechtliche Konsequenzen knüpfen. Er ist im ☞ ABGB im Rahmen der vertraglichen Gewährleistung (§ 922ff, siehe auch → 1.2.19) definiert und umfasst jede Art der Abweichung von der geschuldeten Leistung. Mangelhaft können daher auch nicht-technische Leistungen wie Dokumentation, Schulung oder Störungsbehebung sein. Relevant ist die Unterscheidung unter anderem deswegen, da sich nicht jeder Fehler im IT-System in einer Störung und damit in einem Gewährleistungspflichten auslösenden Mangel äußern muss.

Der in den internationalen Standards (☞ ITIL Vers. 2 und 3) und auch in der Literatur[1] oft verwendete Begriff „**Problem**“ für Fehler oder Störungen ist in diesem Zusammenhang ungenau und irreführend. Diesen Begriff sollte man in diesem Zusammenhang vermeiden, weil er nicht den im vorherigen Absatz dargelegten Sachverhalt abdeckt[2].

Art, Zeitpunkt und Ort der Störung müssen gemeldet und danach reproduzierbar erfasst werden.

Da der Vertragsgegenstand in der Regel möglichst ununterbrochene Dienstleistungen zum Inhalt hat, ist die **Erfassung** von Beeinträchtigungen dieser Dienstleistungen, also Störungserfassung und Störungsmeldung, eine wichtige Aufgabe für beide Seiten, um die Wiederherstellung der ununterbrochenen Dienstleistungen zu ermöglichen und außer Streit zu stellen. Dazu muss der Service-Anbieter eine Ansprechstelle einrichten, wo seine Kunden die von ihnen erfassten Störungen melden können. Damit die vertraglich

---

1 *z.B. Heinrich, Informationsmanagement, 2002*

2 *Problem (gr.* Πρόβλημα*, próblema = „das, was [zur Lösung] vorgelegt wurde“) nennt man eine Aufgabe oder Streitfrage, deren Lösung mit Schwierigkeiten verbunden ist.*

vereinbarte Verfügbarkeit auch kontrolliert werden kann, müssen dort Art, Zeitpunkt und, soweit lokalisierbar, Ort der Störung gemeldet, reproduzierbar (schriftlich oder durch Sprachaufzeichnung) festgehalten und mit einem eindeutigen Kennzeichen (Namen oder Nummer) versehen werden. Der Erhalt ist dem Melder zu bestätigen („Trouble Ticket"). Nach Behebung der Störung oder nach Schätzung der Behebungszeit ist dem Melder die Behebung (Uhrzeit und Art des Fehlers) oder die geschätzte Behebungszeit auf dem gleichen oder einem vergleichbaren Weg mitzuteilen. Schriftliche Meldungen mit Empfangsbestätigung mittels gesicherter Verfahren sind rein telefonischen Meldungen vorzuziehen, wenn sie möglich sind und die Art der Störung nicht diese Form verhindert.

Die Protokolle dieser Störungsmeldungen, deren Klassifizierung und die ermittelten Behebungszeiten bilden die Grundlage für die Berechnung der Verfügbarkeit der Dienstleistungen. Bedienungsfehler durch den Kunden, die nicht auf Einschulungs- oder Dokumentationsfehler zurückzuführen sind und zu Störungsmeldungen führen, fallen aus der Dienstleistung des Anbieters heraus und können von diesem zu vereinbarten Sätzen abgerechnet werden.

1.2.5 Datensicherung und Datenschutz

Werden in einer Software-Dienstleistung personenbezogene Daten verwendet, dann ist unbedingt das ☞ DATENSCHUTZGESETZ 2000 in der geltenden Fassung einzuhalten. Als personenbezogene Daten gelten auch – entsprechend der österreichischen Rechtsordnung und dem DSG 2000 – alle betriebsinternen und geheimhaltungsfähigen Daten eines Unternehmens. Das Datenschutzgesetz definiert alle Daten, mit deren Hilfe eine Person (oder ein Unternehmen) identifiziert oder identifizierbar ist, als personenbezogen. Handelt es sich um so genannte „sensible Daten" (Rasse oder Ethnie, Religion oder Weltanschauung, politische Gesinnung, Gewerkschaftszugehörigkeit, Gesundheit, Sexualverhalten), dann gilt ein generelles Verarbeitungsverbot mit gesetzlichen Ausnahmen und besonderen Auflagen.

Die **Verfassungsbestimmung** des § 1 DSG 2000 legt fest (Abs. 1 bis 4):

Jeder hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten.

Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

Diesen verfassungsmäßigen Rahmen führen dann § 6 und § 7 näher aus. Die §§ 8 und 9 legen die Regeln für nichtsensible und sensible Daten fest. Sehr wichtig ist auch der § 14 DSG 2000, der ganz allgemein die abstrakten Anforderungen an eine Datenverarbeitung festlegt (siehe dazu näher → 2.2.1). Diese **gelten für jeden Anbieter** von Software als Dienstleistung, der personenbezogene Daten verarbeitet. Da wie oben dargestellt auch Firmendaten als personenbezogen gelten, sind **in der Praxis fast alle Softwaredienstleistungen dem Datenschutzgesetz unterworfen.** Das bedingt, dass das Datenschutzgesetz in jedem Fall beachtet werden muss (siehe auch → 2.1.6 und → 2.2.1).

Hervorzuheben ist noch das in § 1 Abs 3 festgelegte Recht jedes Betroffenen auf umfassende „Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden“ sowie „das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.“ Dies wird in den §§ 26-29 DSG 2000 konkretisiert (siehe dazu auch → 2.3.3).

1.2.6 Systemvoraussetzungen beim Kunden

Damit der Service-Anbieter seine Leistung im gewünschten Ausmaß erbringen kann, sind beim Kunden oftmals **bestimmte technische Voraussetzungen** notwendig. Diese muss der Anbieter dem Kunden in ausreichender und verständlicher Form vor Vertragsabschluss mitteilen. Dies schließt auch die entsprechende Beratung über die Verbindung zwischen Anbieter und Kunden ein (Stand- oder Wählverbindung, Bandbreite, Fehlerrate, verwendbare Protokolle, Softwareschnittstellen, geeignete Netzanbieter). Ferner muss geklärt werden, wer diese Verbindungen beschafft, wer sie wartet und wer die Kosten trägt (wobei die unmittelbare Wartung der Verbindungsleitung wohl vom Netzanbieter übernommen wird). Für die Meldung einer möglichen Störung an den Netzanbieter kann sowohl der Service-Anbieter (fachlich kompetenter) als auch der Kunde verantwortlich sein.

Anbieter haben Kunden vor Vertragsabschluss die erforderlichen technischen Voraussetzungen mitzuteilen.

1.2.7 Leistungsänderungen und Updates

Updates sollten als Vertragsbestandteil verpflichtend im Leistungsumfang enthalten sein.

Es kann für den Service-Anbieter sinnvoll bzw. technisch oder kostenmäßig sogar zwingend sein, bestimmte Erweiterungen (Updates) oder Änderungen des IT-Systems innerhalb des vertraglichen Leistungsumfangs durchzuführen. Zwingende Änderungen ergeben sich meist daraus, dass ein Hersteller von Hard- oder Software die älteren Hardware-Teile oder Funktionen nicht mehr weiter betreuen kann oder will. Änderungen und Erweiterungen dieser Art muss er daher für den Kunden ab einem bestimmten Zeitpunkt verpflichtend machen.

Technisch notwendige Leistungsänderungen sind entweder konkret vorweg oder in Form eines Vertragsänderungsrechts des Anbieters zu vereinbaren.

Grundsätzlich sind Leistungsänderungen durch den Anbieter entweder im Vertrag vorweg zu vereinbaren – soweit sie schon konkret erfasst werden können – oder zum gegebenen Zeitpunkt in Form eines **verbindlichen Anbots** dem Kunden vorzulegen. Dieses Angebot kann der Kunde entweder annehmen oder ablehnen.

Auch Änderungen, die aufgrund technischer Gegebenheiten kaum vermeidbar sind, müssen in Form eines Vertragsänderungsrechts des Anbieters vereinbart werden. Dafür sollte ein zulässiger Rahmen festgelegt werden. Dem Kunden steht allerdings für diesen Fall ein ordentliches oder zumindest ein außerordentliches Kündigungsrecht zu. Wird eine für den Kunden existentielle Dienstleistung berührt, muss diese Leistungsänderung so frühzeitig durch den Anbieter angekündigt werden, dass der Kunde einen Ersatz finden und einrichten kann. Auch diese Frist sollte im Vertrag vereinbart werden.

1.2.8 Ergänzende vertragliche Leistungen

Notwendige nachträgliche Änderungen des Leistungsumfangs sind vorausschauend zu regeln.

Verträge über eine längere Zeit sind in der Regel Einflüssen ausgesetzt, die ergänzende Leistungen und damit eine **Änderung des vereinbarten Leistungsumfangs** notwendig machen. Diese Einflüsse können aus dem Bereich des Service-Anbieters, dem des Kunden oder auch von außen kommend (wirtschaftlich oder rechtlich) wirksam werden. Es empfiehlt sich daher, in den Vertrag eine Klausel aufzunehmen, die diese Einflüsse vorausschauend regelt. Dabei sind zwei grundsätzliche Formen zu unterscheiden: jene Änderungen, die **konkret vorhersehbar** und üblich sind

und daher meist in der vertraglichen Leistung enthalten sein sollten, und jene Änderungen, die zwar im Prinzip vorhersehbar, aber im Einzelnen und in ihren Auswirkungen **noch nicht bestimmbar** sind (wie z.B. angekündigte Gesetzesänderungen, Software-Releases oder Hardware-Änderungen). Für die zweitgenannten Fälle ist es sinnvoll, dem Anbieter die Pflicht aufzuerlegen, dem Kunden, sobald er die Wirkung der Änderung erkennen und kostenmäßig berechnen kann, ein verbindliches Angebot samt einer Beschreibung der Auswirkungen zu legen, das dieser innerhalb einer bestimmten Frist annehmen oder ablehnen kann. Bei zwingenden Änderungen kann dem Kunden ein ordentliches oder außerordentliches Kündigungsrecht des Vertrags zustehen.

Da Gesetzeskonformität meistens Vertragsinhalt und daher Teil der Leistung ist, muss jedoch für solche Gesetzesänderungen, die eine Änderung der Leistung in erheblichem Umfang notwendig machen, die Angebotspflicht des Anbieters wie vorhin beschrieben gewählt werden.

Der Kunde kann den Service-Anbieter aber auch auffordern, eine gewünschte Leistungserweiterung, die der Kunde genau beschreiben oder mit dem Anbieter verhandeln muss, innerhalb einer vereinbarten und bestimmten Frist anzubieten.

1.2.9 Testen neuer Anwendungsmodule und deren Übernahme

Werden vertraglich vereinbarte neue Leistungen eingeführt, muss es möglich sein, diese einschließlich der notwendigen Rahmenbedingungen vor deren Übernahme zu testen. Unter Umständen hat der Service-Kunde dazu entsprechende Testdaten zeitgerecht nach Ankündigung durch den Anbieter zur Verfügung zu stellen. Erst nach positivem Abschluss der vereinbarten Tests muss der Kunde die neuen Leistungen übernehmen, die sodann vom Anbieter in den realen Betrieb überführt und vereinbarungsgemäß abgerechnet werden.

Achtung, bei gemeinsam erarbeiteten Zusatzentwicklungen nicht auf eine Regelung der Werknutzungsrechte vergessen!

Zusätzlich ist von den Parteien bei Abschluss der Zusatzvereinbarung zu regeln, wem die **Werknutzungsrechte** an dieser Entwicklung zustehen und, soweit dem Kunden ein Miturheberrecht zugerechnet werden kann, welcher Erlösanteil ihm dann zustehen soll und wie dieser nachvollziehbar abzurechnen ist. Bei Entwicklungen, die zu Patenten

führen, ist zu regeln, wer die Patente wo anzumelden hat, wer die Patentgebühren zahlen soll und wer die Verteidigung der Patente und auch die Lizenzgewährung wie abzuwickeln hat.

1.2.10 Dokumentation und Hinterlegung des Quellcodes

Da die SaaS zugrundeliegende Anwendung immer ein sehr komplexes System ist, besteht die Notwendigkeit, dem Kunden eine entsprechende **Dokumentation**, soweit sie ihn betrifft, zu übergeben. Diese Dokumentation muss so gestaltet sein, dass der Kunde sie auch anwenden kann. Sie sollte im Sinne der vertraglichen Leistungen vollständig sein und Bedienungsfehler weitgehend ausschließen (☞ USABILITY). Bei Vertragsende – aus welchem Grund auch immer – darf sie der Kunde behalten (aber nicht an Dritte weitergeben), schon um bei eventuellen Gerichtsverfahren entsprechende Beweismittel zur Verfügung zu haben.

Hinterlegung des Quellcodes samt Dokumentation sichert dem Kunden einer Individualsoftware Weiterverwendung nach Vertragsende.

Soweit der Service-Anbieter für den Kunden **Individualsoftware** entwickelt und zur Benützung zur Verfügung gestellt hat, empfiehlt es sich, den Anbieter zu verpflichten, den Quellcode dieser Software samt der Dokumentation darüber (Programmpflichtenheft, Programmflusspläne, Datenflusspläne, Testverfahren usw.) einschließlich aller erfolgten Änderungen in versiegelter Form zur Verfügung zu stellen, damit der Kunde bei Vertragsende diese Software auch bei einem dritten Anbieter weiterverwenden kann, ansonsten ist ein Anbieterwechsel unmöglich. Soweit der Anbieter diese Sachen dem Kunden nicht direkt zur Verfügung stellen will, kann auch ein Verwahrer bestimmt werden, der sie zu genau definierten Bedingungen herauszugeben hat („Hinterlegung“).

1.2.11 Schulung und Support

Bei komplexen Leistungen ist eine Einschulung des Personals notwendig, das die angebotenen Leistungen anwenden soll. Es ist daher vertraglich zu vereinbaren, wann welche Anwendungen geschult werden, welches Ziel in dieser Schulung erreicht werden soll (nur Anwendung oder auch „Train the Trainer“) und welche vorausgesetzte Qualifikationen das zu schulende Personal haben muss, damit die Schulung Erfolg versprechend ist.

1.2.12 Verfügbarkeit der Gesamtleistung

Wie schon in → 1.2.3 dargelegt, sind bei der Festlegung der Verfügbarkeit der Leistungen bestimmte Parameter zu vereinbaren, um für beide Seiten verständliche und akzeptable Bedingungen zu erzielen. Der Service-Kunde hat naturgemäß andere Interessen als der Anbieter. Ein Kompromiss ist notwendig und muss vertraglich festgelegt werden. Überspitzte Forderungen von beiden Seiten sind nicht zielführend. Niemand kann eine 100%ige Verfügbarkeit einhalten und sie ist in der Regel auch nicht notwendig. Leistungen von zentraler Bedeutung erfordern meist eine höhere Verfügbarkeit als periphere. Es ist daher für beide Seiten wichtig, die angestrebten und vertretbaren Mittelwerte der Verfügbarkeiten für jede identifizierbare Leistung sowie deren gerade noch zulässigen oberen oder unteren Grenzwert zu vereinbaren. Ein entsprechendes Beispiel ist in → 3.2 dargestellt.

Die zu vereinbarende Verfügbarkeit hängt von den konkreten Anforderungen des Einzelfalls ab.

1.2.13 Entgelt und Zahlungsbedingungen

Die Vereinbarung des Entgelts für bestimmte Leistungen gilt abgesehen von der Verhandlungsphase als relativ unproblematisch, weil es der offenkundige und leicht erfassbare Teil eines Vertrags ist. Steht dem aber eine sehr differenzierte Leistungserbringung gegenüber, dann kann die Bestimmung der verschiedenen Entgeltbestandteile die gleiche Komplexität wie die Leistungserbringung annehmen. In der Regel sollte man daher diesem Abschnitt eines Vertrags die gleiche Sorgfalt und nicht nur Verhandlungsintensität widmen wie der Leistungsbeschreibung und der Verfügbarkeit. Insbesondere die Entgeltminderungen für Minderleistungen werfen erhebliche Schwierigkeiten auf, was ihre absolute oder relative Größe und ihre Abrechnung betrifft.

Das so beliebte und in Vertragsmustern zumeist enthaltene Verbot, Gegenforderungen wie z.B. Pönalen, Entgeltminderungen, Schadenersatzleistungen usw. vom zu leistenden Entgelt abzuziehen („**Aufrechnungsverbot**“), ist fehleranfällig und kontraproduktiv. Die Möglichkeit, mit einer Gegenforderung aufzurechnen, stellt nämlich für beide Seiten eine zusätzliche Sicherheit dar. Denn trennt man die wechselseitigen Forderungen strikt voneinander, so kann es passieren, dass eine eigene Zahlung in voller Höhe erbracht werden muss, während

Das gerne vereinbarte Aufrechnungsverbot bietet mehr Nach- als Vorteile.

eine Gegenforderung, z.B. aufgrund von Zahlungsschwierigkeiten des Geschäftspartners, unsicher ist und (zum Teil) ausfällt. Ein Nachteil kann allerdings dadurch entstehen, dass der Vertragspartner versucht, die Durchsetzung einer Forderung durch frei erfundene Gegenforderungen zu blockieren. Ein Aufrechnungsverbot sollte trotzdem eher nicht in den Vertrag aufgenommen werden. Zu beachten ist außerdem, dass bei Verbrauchergeschäften die Wirksamkeit vereinbarter Aufrechnungsverbote gesetzlich beschränkt ist (§ 6 Abs. 1 Z 8 ☞ KSCHG[3]). Dies kommt unter Umständen auch bei Geschäften zwischen zwei Unternehmen in Betracht, wenn sich das Kompensationsverbot in AGB, also dem „Kleingedruckten", befindet. Die Fristen für die Zahlungen und ihre Randbedingungen, sowie die Sanktionen bei deren Verletzung sind notwendige Bestandteile der Zahlungsbedingungen.

Ähnlich dem Aufrechnungsverbot wird auch des Öfteren ein sogenanntes „☞ZESSIONSVERBOT" vereinbart. Ein vertragliches Zessionsverbot verbietet die Abtretung (§ 1396a ABGB) der Forderung an einen Dritten. Es schränkt daher den finanziellen Spielraum der betroffenen Partei ein, erspart der anderen Partei aber (va. buchhalterischen) Aufwand.

1.2.14 Dauer und Kündigung

Ein SaaS-Vertrag ist **auf Zeit angelegt** und unterliegt daher anderen rechtlichen Bedingungen als ein Kaufvertrag. Dies gilt vor allem dann, wenn der Zeitraum unbefristet sein soll. Es ist besonders wichtig, dass beide Vertragspartner ihre Standpunkte offenlegen, um einen Zeitplan zu vereinbaren, der keine Seite vor unlösbare oder besonders nachteilige Probleme stellt. Dazu gehört die grundlegende Entscheidung, ob ein befristetes oder unbefristetes Verhältnis eingegangen werden soll.

Bei unbefristeten Verträgen sind (ausgewogene) Kündigungsfristen zu vereinbaren.

Wird der Vertrag befristet abgeschlossen, z.B. zwölf Monate oder drei Jahre, dann wissen beide Seiten, wann der Vertrag zu Ende ist und können sich darauf einstellen. Soll der Vertrag unbefristet sein, sind

---

3 *Nach dieser Bestimmung kann der Verbraucher mit jeglicher Forderung aufrechnen, wenn der Unternehmer zahlungsunfähig ist; davon unabhängig kann er mit Forderungen kompensieren, die mit jener des Unternehmers rechtlich zusammenhängen; und schließlich mit rechtskräftig festgestellten und vom Unternehmer anerkannten Forderungen.*

unbedingt **Kündigungsfristen** zu vereinbaren. Diese sollten so bemessen sein, dass jede Seite sich auf einen möglichst reibungslosen Übergang bei Ende des Vertrags vorbereiten kann. Die konkrete Dauer der Fristen hängt stark von den Umständen des Einzelfalls ab. Sie müssen aber jedenfalls ausgewogen sein und den Interessen beider Seiten entsprechen. Auch die Vereinbarung unterschiedlicher Kündigungsfristen für die Vertragsparteien ist möglich. Als Sicherheitsfrist wird oftmals ein ein- oder beidseitig befristeter Kündigungsverzicht gewählt.

Die **außerordentliche Kündigung** ist ein vertraglich nicht ausschließbares Recht, dessen Ausübung sofort wirksam wird. Unter fairen Bedingungen kann es aufgeschoben werden. Die außerordentliche Kündigung ist grundsätzlich immer dann anwendbar, wenn wesentliche Bedingungen des Vertrags nicht eingehalten werden oder ein objektiv begründeter Vertrauensverlust zum Vertragspartner eingetreten ist, d.h. die Fortsetzung des Vertrags bis zum nächsten ordentlichen Kündigungstermin oder dem befristeten Vertragsende nicht zumutbar ist. Sie kann aber auch vertraglich für bestimmte Vertragsverletzungen vereinbart werden.

Besonders zu beachten ist für jedes Vertragsende, was mit den Daten in der Verfügungsgewalt des Service-Anbieters geschieht und welche Ersatzsoftware für die Weiterführung der Leistung bereitsteht. Da in der Mehrzahl personenbezogene Daten beim Anbieter gespeichert sein werden, muss die **vollständige Übergabe** dieser Daten an den Kunden ausdrücklich und sorgfältig geregelt werden. Darüber hinaus ist für alle diese Daten eine **Löschungsverpflichtung** des Anbieters zu vereinbaren, die von diesem innerhalb einer zu vereinbarenden Frist durchzuführen und dem Kunden nachzuweisen ist. Kritisch ist dies für alle Daten im Backup, weil diese häufig auf Bändern, DVDs oder ähnlichen Medien gespeichert werden. Deren Löschung ist in der Regel umständlich und aufwändig. Dennoch ist sie rechtlich zwingend notwendig (siehe dazu → 2.3.2). Die Kontrolle der wirklichen Löschung erfordert große Sachkenntnis und sollte daher einer kompetenten Außenstelle überlassen werden. Die für die Löschung anfallenden Kosten sind Teil der Leistung des Anbieters, sollten aber im Vertrag ausdrücklich geregelt werden.

Das DSG 2000 verpflichtet zur vollständigen Übergabe und Löschung aller Kundendaten nach Vertragsende!

Im Konkursfall des Anbieters (nach neuem Insolvenzrecht) wird der Kunde die Löschung der Daten wohl auf eigene Kosten übernehmen müssen, weil in dieser Situation kaum noch ein geregelter Ablauf beim Anbieter stattfinden wird. Der Kunde sollte unverzüglich Maßnahmen ergreifen, die eine Löschung der Daten sicherstellen.

1.2.15 Geheimhaltungspflichten

Eine vertragliche Geheimaltungsverpflichtung ist sinnvoll, ihr Umfang sollte jedoch realitätsnahe festgelegt und nicht überspannt werden.

Kunden sind natürlich nicht daran interessiert, dass ihre Daten an die Öffentlichkeit gelangen oder gar in falsche Hände geraten. Geheimhaltungspflichten sind bereits in diversen Gesetzen geregelt. Es empfiehlt sich trotzdem, die Geheimhaltung vertraglich zu regeln, wobei man aber berücksichtigen muss, dass Menschen immer Fehler machen. Die Auswirkungen dieser Fehler können gravierend bis gleich Null sein. Entsprechend sollte die Sanktion vereinbart werden. Die häufig verwendete allumfassende Geheimhaltung auf „ewige“ Zeiten (offenbar gemeint ist auf Lebenszeit des Verpflichteten) mit rigiden Sanktionen schießt meistens weit über das Ziel hinaus. Als Sanktion für Geheimhaltungsverletzungen wird meist eine **Konventionalstrafe** (auch Pönale genannt) einschließlich eines darüber hinaus gehenden Schadenersatzes vereinbart.

Mitarbeiter beider Seiten sind ausdrücklich und nachweisbar zur Geheimhaltung zu verpflichten.

Dieses Pönale ist zwar wegen des Dienstnehmerhaftpflicht-Gesetzes (DHG) nur unter erschwerten Bedingungen an die **Mitarbeiter** überbindbar, es ist aber trotzdem sehr wichtig, dass auch die Mitarbeiter beider Seiten entsprechende Vereinbarungen, am besten mit konkret genannten Inhalten, schriftlich abschließen. Dies stellt ihre Aufmerksamkeit und die Beachtung dieser Bedingungen sicher. Eine **zeitliche Befristung** dieser Verpflichtungen ist sinnvoll, weil insbesondere nach dem Ausscheiden eines Mitarbeiters dessen Aufmerksamkeit nachlässt und eines Tages auch nicht mehr zumutbar ist. Nur für besonders kritische oder sensible Daten wird ein langer Zeitraum für die Geheimhaltung vertretbar sein.

1.2.16 Besondere Rechte und Pflichten

Abmachungen bei der Umsetzung können Vertragsänderung bewirken.

Jede Vereinbarung enthält Randbedingungen, die besondere Aufmerksamkeit verlangen. Dies können z.B. vereinbarte Wartungszyklen oder Software-Releases sein. Durch die praktische Handhabung auf der Umsetzungsebene können sich dabei Änderungen der vertraglichen Rechte und Pflichten ergeben (indem man sich auf konkrete Vorgangsweisen einigt oder diese stillschweigend akzeptiert). Änderungen bzw. konkrete Umsetzungen sollten daher in regelmäßigen Abschnitten in Besprechungen überprüft und mit dem Vertrag in Einklang gebracht werden. Damit diese Vereinbarungen nicht unvermutet eine unbeabsichtigte Vertragsänderung hervorrufen, ist es praktisch, solche Abmachungen zwischen den Parteien als bloße Durchführung und nicht als Änderung des Vertrags zu qualifizieren.

Größere Sicherheit bietet die Bildung eines nicht in die direkte Umsetzung involvierten „Koordinationsgremiums“, an das regelmäßig Bericht zu erstatten ist. Dessen Aufgabe ist es, darüber zu wachen, dass die „gelebte“ Wirklichkeit mit der „vertraglichen“ in Einklang bleibt. Zu beachten ist, dass z.B. die Vereinbarung der Schriftlichkeit von Vertragsänderungen hier keine Abhilfe schaffen kann, sondern eine entsprechende Klausel sogar selbst durch Abweichen in der Praxis abbedungen werden kann (siehe dazu auch → 1.2.24).

1.2.17 Entwicklungsmaschine

In Ausnahmefällen kann es notwendig werden, dass für bestimmte Softwareentwicklungen eine eigene Entwicklungsmaschine notwendig ist, um die Eingriffe in den laufenden Betrieb durch Testläufe zu verhindern. Dies muss jedoch ausdrücklich vereinbart werden. Inhaltlich entspricht dies einem zusätzlichen eigenen Werkvertrag für solche absehbaren zeitlichen Prozesse. Zu regeln wäre: Wer stellt die Maschine mit welcher Kapazität wann und wo zur Verfügung und wie darf sie verwendet werden.

1.2.18 Datenschutzregistermeldungen

Eine Meldungspflicht an das Datenschutzregister ist abzuklären und ihre Durchführung zu regeln.

Wie in → 1.2.5 näher ausgeführt, sind die im SaaS-Modell üblicherweise verarbeiteten Daten meist personenbezogene Daten, für die das Datenschutzgesetz Regeln festgelegt hat. Unter bestimmten Voraussetzungen (siehe § 17 ☞ DSG 2000) kann die Meldung der Datenverarbeitung an das Datenschutzregister entfallen. In allen anderen Fällen ist dies zu melden. Da zu dieser Meldung eine gewisse Sachkenntnis gehört (§ 19 DSG 2000), die nicht überall verfügbar ist, empfiehlt es sich, den Sachkundigeren mit den Meldungen an das Datenschutzregister zu betrauen. Dieser muss allerdings auch die schadenersatz- und verwaltungsrechtliche Haftung für fehlerhafte Meldungen übernehmen. Die DVR-Meldungen müssen zukünftig elektronisch (über Internet) erfolgen. Muster sind auf der Homepage der DSK (www.dsk.gv.at) zu finden.

1.2.19 Gewährleistung

Der Anbieter hat eine mängelfreie Leistung zu gewährleisten, Mängel sind in erster Linie kostenfrei zu beheben!

Die vertragliche Gewährleistung ist in den §§ 922ff ☞ ABGB geregelt und bestimmt die Haftung von Vertragspartnern für die **Mangelhaftigkeit der erbrachten Leistung**. Unter Mangel versteht man ein Abweichen der erbrachten Leistung von den vertraglich geschuldeten oder üblicherweise vorausgesetzten Eigenschaften (siehe auch → 2.1.4). Gewährleistungspflichten bestehen selbstverständlich auch für neue Entwicklungen und Entwicklungsversionen.

Das österreichische Gewährleistungsrecht ist ein **zweistufiges System**. Primär ist dem schlecht erfüllenden Anbieter die Möglichkeit zur Verbesserung innerhalb einer angemessenen Frist zu geben, deren Aufwand bereits zwingend im Entgelt für die Leistung enthalten ist. Ist dies nicht möglich, da es sich um einen unbehebbaren[4] Mangel handelt, kommen die sekundären Gewährleistungsbehelfe zum Zug: **Preisminderung** oder **Wandlung** (Auflösung des Vertrags). Wandlung

4 *Unbehebbar ist ein Fehler auch dann, wenn er nur mit unverhältnismäßig hohem Aufwand verbessert werden kann oder der Gewährleistungsverpflichtete den Mangel nicht behebt.*

ist jedoch nur bei „nicht geringfügigen[5]“ Mängeln möglich, bei einem geringfügigen Mangel kann nur Preisminderung verlangt werden.
Die gesetzliche Gewährleistungspflicht beträgt in Österreich bei beweglichen Sachen zwei Jahre. Die Gewährleistungsfrist beginnt mit der vollständigen Ablieferung der Leistung.

Die Beschränkung oder gar der Ausschluss der Gewährleistung ist in IT-Verträgen nahezu die Regel. Oft werden die die Gewährleistungsbeschränkungen gekonnt in den ☞ AGB des Vertrages verschleiert[6]. Die dabei angewandten Methoden reichen von der offenen Beschränkung, über ideologisch-rhetorische Argumente, Einführung von unterschiedlichen Fehler- und Mangelbegriffen, Einteilung der Software in Wartungsklassen und deren Umstufung bis zu Beschränkungen der Rechtsbehelfe und des Ersatzes der Fehlerbehebung durch neue Releases. Diese Art ist besonders beliebt bei standardisierter Software. Derartige Beschränkungen der Gewährleistungspflicht sind in vielen Fällen sittenwidrig und damit nicht gültig.

Beschränkungen der Gewährleistungsplicht sind nur in Ausnahmefällen sachlich gerechtfertigt.

In der Praxis ergeben sich Schwierigkeiten bei der Bestimmung des Umfanges der Gewährleistung dadurch, dass bestimmte Software-Pakete von der Wartung ausgeschlossen werden, z.B. weil deren Einführung in die Gesamt-Software bisher nicht erfolgreich durchgeführt werden konnte. Der Service-Anbieter tut gut daran, solche Teile von der Hauptleistungspflicht und damit auch von der Gewährleistung ausdrücklich auszuschließen. Dies ist insbesondere dann wichtig, wenn die Software nicht von ihm stammt und in der Dokumentation Eigenschaften versprochen wurden, die praktisch ohne grundlegende Änderung der Software nicht zu implementieren sind. Die Auswirkungen eines solchen Ausschlusses auf andere Teile der Software sind aber oft unvorhersehbar.

---

5 *Traditionell wird ein Mangel als „nicht geringfügig“ definiert, wenn er den üblichen oder ausdrücklich vereinbarten Gebrauch der Sache verhindert oder die Sache eine vereinbarte Eigenschaft nicht besitzt.*

6 *Details dazu in Ertl/Wolf, Die Software im österreichischen Zivilrecht, 225ff, 304ff; Ertl, Allgemeine Geschäftsbedingungen der Softwareverträge, in EDV&Recht 1/94, 19ff; Staudegger, Rechtsfragen bei Individualsoftware, 1995, 102 ff.*

Eine der besonderen Schwierigkeiten des SaaS-Vertrags ist die Verschränkung zwischen **Dauer- und Zielschuldverhältnis**. Der übergeordnete Rahmen ist das Dauerschuldverhältnis, einzelne Leistungen jedoch können Zielschuldverhältnisse sein. Die gewährleistungsrechtlichen Folgen sind zum Teil unterschiedlich. Um die richtige Zuordnung festzustellen, ist jeweils zu prüfen, wie sich ein Fehler auf diese beiden unterschiedlichen Schuldstrukturen auswirkt. So gibt es Fehler des Rahmenvertrags (Dauerschuldverhältnis), die als Fehler in der Einzelleistung in Erscheinung treten. Umgekehrt muss nicht jeder Fehler der Einzelleistung auch ein Fehler des Rahmenvertrags sein.

Unbehebbare Mängel im Dauerschuldverhältnis können (analog der Zinsminderung des § 1096 ABGB[7]) durch Minderung des Entgelts bis zu einem bestimmten Grade ausgeglichen werden. Dies gilt jedoch nur für geringfügige unbehebbare Mängel. Ist der Fehler nicht geringfügig, dann bleibt nur die außerordentliche Kündigung, ev. einschließlich einer Schadenersatzforderung. Eine Minderung des Entgelts auf Null ist dem Service-Anbieter jedenfalls nicht zuzumuten, weil ja damit seine Leistungspflicht unentgeltlich für die Vertragsdauer aufrecht bliebe.

Mangel	Gesamtleistung	Einzelleistung	Rechtsfolge	Kommentar
unbehebbar	nicht geringfügig	nicht geringfügig	Wandlung der Einzelleistung, außerordentliche Kündigung des Gesamtvertrags	Konkreter Wert der Einzelleistung ist zu ermitteln
	geringfügig	nicht geringfügig	Wandlung der Einzelleistung und Entgeltminderung der Dauerleistung	Schwierig ist meist Bestimmung der konkreten Entgeltminderung für Dauerleistung durch Wegfall der Einzelleistung
	geringfügig	geringfügig	Entgeltminderung	Bewertung der Einzelleistung in Geld notwendig, sowie Minderung des Entgelts für Dauerleistung (s.o.)
behebbar	nicht geringfügig	nicht geringfügig	Behebungspflicht und Entgeltminderung bis zur Verbesserung	Entgeltminderung nach Paketen; auch hier kann die Bewertung der Einzelleistung schwierig sein
	geringfügig	nicht geringfügig		
	geringfügig	geringfügig		

7 *§ 1096 Abs. 1, 2. Satz ABGB: "Ist das Bestandstück bei der Übergabe derart mangelhaft, oder wird es während der Bestandzeit ohne Schuld des Bestandnehmers derart mangelhaft, dass es zu dem bedungenen Gebrauch nicht taugt, so ist der Bestandnehmer für die Dauer und in dem Maße der Unbrauchbarkeit von der Entrichtung des Zinses befreit."*

Mängel in den Einzelleistungen (Mängelbehebung oder Änderungen und Ergänzungen des Software-Pakets) haben je nach Art des Mangels verschiedene Rechtsfolgen. Nicht geringfügige unbehebbare Fehler führen im Regelfall zur Wandlung des Vertrages (wobei vom Gewährleistungsberechtigten immer auch die Preisminderung gewählt werden kann). Die Auflösung des Vertrags über die Einzelleistung ist bei einer SaaS-Vereinbarung jedoch nicht ohne weiteres möglich bzw. sinnvoll. So mindert eine nicht erbrachte Einzelleistung oft auch die gesamtvertragliche Leistung, ohne dass aber deswegen gleich auch der Gesamtvertrag aufgelöst werden soll. Eine Beschränkung der Rechtsfolgen auf die vereinbarte Einzelleistung greift also unter Umständen zu kurz, die direkte Ausdehnung auf den Gesamtvertrag hingegen zu weit. Zur Klärung der Rechtsfolgen sind daher immer auch die Bedeutung der konkreten Einzelleistung im Gesamtgefüge des Softwarepakets und die vereinbarte und erwartete Wirkung auf die Gesamtleistung zu beurteilen. Die oben dargestellte Tabelle gibt eine Übersicht über die möglichen Fälle und deren Wirkungen.

Nicht geringfügige unbehebbare Fehler führen im Regelfall zur Wandlung des Vertrages.

Problematisch ist die Wandlung der Einzelleistung, weil bei der Rückabwicklung der Einzelleistung der Kunde so zu stellen ist, dass gemäß § 921 ABGB zweiter Satz „...kein Teil aus dem Schaden des anderen Gewinn zieht." Dies bedeutet aber, dass dem Service-Kunden auch das bereits empfangene Entgelt zurückzuzahlen ist. Da in den SaaS-Verträgen meist ein laufendes Entgelt zu zahlen ist, kann der Einzelleistung nicht unmittelbar ein Teil des Entgeltes zugeordnet werden. Dies kann zu Streitigkeiten führen. Es ist daher dringend anzuraten, schon bei der Vertragsverhandlung diese Szenarien zu diskutieren und eine Formel der Entgeltbestimmung in den Vertrag aufzunehmen. Eine Vorwegregelung hilft die im Anlassfall widerstreitende Interessenlage auf eine für beide Parteien faire Weise ohne Gerichtsverfahren zu lösen.

Es wird auch in Erinnerung gerufen, dass die Gewährleistung **verschuldensunabhängig** ist. Liegt ein Verschulden für den Fehler vor, dann haftet der Anbieter über die Rechtsfolgen der Gewährleistung hinaus auch für den verschuldeten Schaden z.B. an anderen Sachen oder im Vermögen des Kunden. Gemäß § 1298 ABGB hat der Anbieter zu beweisen, dass ihn kein Verschulden am Fehler trifft. Er gilt überdies als

Fachmann im Sinne des § 1299 ABGB und haftet daher nach Maßgabe der dafür vorausgesetzten Kenntnisse und Fähigkeiten, auch wenn er diese persönlich nicht besitzt.[8]

1.2.20 Schadenersatz

Massive Einschränkungen von Schadenersatzansprüchen widersprechen einem ausgewogenen Vertragsverhältnis.

Schadenersatzansprüche werden in Software-Verträgen oft massiv eingeschränkt, sei es durch Ausschluss bestimmter Verschuldensstufen (z.B. Fahrlässigkeit), sei es durch Beschränkung auf bestimmte Schadensarten. Dies widerspricht einem ausgewogenen Vertragsverhältnis.

Einschränkungen der Schadenersatzhaftung sind nach der Rechtsprechung grundsätzlich für die Fälle der leichten Fahrlässigkeit zulässig (vgl. aber § 6 Abs. 2 Z 5 KSchG[9]). Im Bereich der groben Fahrlässigkeit ist die Rechtsprechung stark einzelfallbezogen. Eine volle Haftung auch für leichte Fahrlässigkeit entspricht dem Gesetz und ist die gerechteste Lösung. Einschränkungen dieser Haftung sollten nur in gut begründeten Fällen und nur auf Grund einer adäquaten Gegenleistung erfolgen. Der nicht unübliche Ausschluss von Vermögensschäden betrifft in SaaS-Verträgen meistens die Hauptleistung und bedeutet somit den Ausschluss jeglicher Haftung. Dies führt zu einer groben Benachteiligung des Service-Kunden und wäre daher gemäß § 879 Abs. 3 ABGB[10] nichtig.

Im Schadensfall muss bei Vertragsverletzungen jedenfalls der Schädiger beweisen, dass ihm kein Verschulden für den Schaden

---

8 *§ 1299 ABGB lässt es hier an Eindeutigkeit nicht fehlen: „Wer sich zu einem Amte, zu einer Kunst, zu einem Gewerbe oder Handwerke öffentlich bekennet; oder wer ohne Not freiwillig ein Geschäft übernimmt, dessen Ausführung eigene Kunstkenntnisse, oder einen nicht gewöhnlichen Fleiß erfordert, gibt dadurch zu erkennen, dass er sich den notwendigen Fleiß und die erforderlichen, nicht gewöhnlichen, Kenntnisse zutraue; er muss daher den Mangel derselben vertreten.“ […]*

9 *In Verbrauchergeschäften ist eine Beschränkung oder der Ausschluss von Schadenersatzpflichten überhaupt nur dann zulässig, wenn der Unternehmer beweist, dass dies im Einzelnen konkret ausgehandelt worden ist.*

10 *§ 879 Abs. 3 ABGB: „Eine in Allgemeinen Geschäftsbedingungen oder Vertragsformblättern enthaltene Vertragsbestimmung, die nicht eine der beiderseitigen Hauptleistungen festlegt, ist jedenfalls nichtig, wenn sie unter Berücksichtigung aller Umstände des Falles einen Teil gröblich benachteiligt.“*

vorgeworfen werden kann. Darüber hinaus sei darauf hingewiesen, dass nach der Rechtsprechung des ☞ OGH ein größeres Unternehmen, das juristisch beraten wird und trotz allem gesetzeswidrige Klauseln in seinen Vertrag aufnimmt, schadenersatzpflichtig wird, unabhängig davon, um welche Klausel es sich handelt.[11]

Zu beachten ist sinnvollerweise auch der Fall, dass Dritte im Zusammenhang mit dem Vertrag Schadenersatzforderungen gegen einen der Vertragspartner geltend machen. Zu klären ist dabei, ob und wie in so einem Fall ein allfälliger Schadensausgleich zwischen den Parteien erfolgen soll.

1.2.21 Leistungsbefreiungen und Höhere Gewalt

Im Vertragsgegenstand wird der Umfang der Leistungsverpflichtung beschrieben, bestimmte Bereiche können in diesem Punkt dann davon gezielt ausgenommen werden. Höhere Gewalt in ihren vorhersehbaren Ausdrucksformen sollte zur Klarstellung inkludiert werden (siehe → 1.2.1).

Es ist unvermeidbar, dass die gesetzliche Regelung für bestimmte Bereiche des Geschäftslebens nicht immer sachgerecht ist.[12] Insbesondere die Fälle der Höheren Gewalt, also Ursachen und Einflüsse, auf die keine der Vertragsparteien einen vernünftigen und vorhersehbaren Einfluss nehmen kann, sollten für den individuellen Fall ausreichend beschrieben werden und als Höhere Gewalt im Vertrag geregelt werden (siehe dazu aber auch → 2.1.9).

Ein Begriff der höheren Gewalt, der für alle Rechtsgebiete gleich gilt und im Gesetz ausdrücklich verankert ist, existiert allerdings nicht. Daher müssen die Parteien sich bei der Vertragsabfassung der Mühe der Eingrenzung und Formulierung unterziehen. Je enger die Voraussetzungen für Höhere Gewalt gezogen werden, umso höher ist der Preis, weil sich damit das Risiko erhöht, dass ein Schadenseintritt

---

11 10 Ob 23/04m (JBL 2005, 443 = ecolex 2005/205)

12 Das Gesetz kann, soll es nicht endlos lang und dementsprechend unübersichtlich und widersprüchlich werden, nur auf Normalfälle Rücksicht nehmen und muss die Regelung im Einzelfall den Vertragsparteien überlassen.

nicht als Höhere Gewalt eingestuft wird. Die Versicherbarkeit dieser Risken und ihrer Kosten ist ein brauchbarer Hinweis auf das höhere Risiko.

1.2.22 Unternehmensveräußerung

Für Fall der Unternehmensveräußerung frühzeitige Informationspflicht und außerordentliches Kündigungsrecht vereinbaren!

Die Zeitungen sind voll von Unternehmenszusammenschlüssen und Unternehmensübernahmen, seien sie nun freundlich oder feindlich. Solche Vorhaben können in manchen Fällen aber für eine der beiden Vertragsparteien einen erheblichen Nachteil bedeuten, insbesondere dann, wenn einem plötzlich die Konkurrenz gefährlich nahe kommt. Es sollte daher in solchen Fällen eine frühzeitige Informationspflicht des anderen Vertragspartners und ein außerordentliches Kündigungsrecht vereinbart werden.

1.2.23 Insolvenz und Liquidation

Während des Sanierungsverfahrens sind Verträge nur aus wichtigem Grund kündbar; der Insolvenzfall selbst zählt nicht!

Durch die Insolvenzgesetz-Novelle 2010 wurde der früher mögliche „Ausgleich“ durch das **„Sanierungsverfahren“** ersetzt. Dieses wurde wesentlich erweitert und ergänzt. Nunmehr sind Vertragsverhältnisse während der Sanierungsphase durch Vertragspartner des insolventen Unternehmens **nur aus wichtigem Grund kündbar** (wenn die Auflösung des Vertrags nicht zur Abwendung schwerer persönlicher oder wirtschaftlicher Nachteile unerlässlich ist). Die Verschlechterung der wirtschaftlichen Situation und ein Rückstand von vor Eröffnung des Insolvenzverfahrens fällig gewordenen Zahlungen berechtigen ausdrücklich nicht zur Kündigung! Dies kann vertraglich nicht abweichend geregelt werden. Erst wenn die Sanierung fehlschlägt, tritt der Konkurs ein und es gelten die Konkursregeln – allerdings in einer etwas härteren Form als bisher.

Der **Konkurs** ist immer auch ein Nachteil für den Vertragspartner, da dessen Ansprüche im Insolvenzfall ausnahmslos in Geld bewertet und zu einem unter 20% liegenden Anteil, wenn überhaupt, befriedigt werden. Dazu kommen zusätzliche Kosten der Geltendmachung der Ansprüche. Entgegenstehende Vertragsklauseln sind in der Regel unwirksam, weil fast immer die anderen Gläubiger dabei benachteiligt werden, was einem Vertrag zu Lasten Dritter gleichkäme.

Problematisch ist vor allem der Konkurs des Service-Anbieters, da dann der Kunde Gefahr läuft, die Kontrolle über seine Daten zu verlieren – und damit womöglich selbst auch in den Konkurs gerissen zu werden. Dem ist vertraglich vorzubeugen (siehe → 1.4.1).

Die **Liquidation** des Anbieters ist generell weniger gefährlich, außer sie erfolgt unangekündigt und abrupt. Da dies aber nicht auszuschließen ist, sind die gleichen Maßnahmen wie für den Konkurs auch in diesem Fall zielführend.

1.2.24 Sonstiges

Unter „Sonstiges" werden in der Regel alle verbleibenden Klauseln zusammengefasst, die sich sonst keinem Punkt des Vertrages zuordnen lassen.

Schiedsgericht statt staatliche Gerichtsbarkeit?

Typischerweise wird hier zum Beispiel vereinbart, Streitigkeiten statt vor den staatlichen Gerichten vor einem **Schiedsgericht** auszutragen. Die Vorteile eines Schiedsgerichts liegen darin, dass sie unter Ausschluss der Öffentlichkeit tagen und dass deren Schiedssprüche fast in allen Staaten der Welt anerkannt werden und vollstreckbar sind. In einfachen Fällen können sie auch schneller als ein staatliches Gericht sein. Ist der Fall allerdings kompliziert und verlangt besondere Sachkunde, dann dauert das Schiedsverfahren genauso lange wie der staatliche Prozess. Manchmal wird als Vorteil auch noch vorgebracht, dass sachkundige Schiedsrichter gewählt werden können. In der Praxis ist die spezielle Sachkunde eines Schiedsrichters aber selten, man sollte sich daher nicht darauf verlassen. Außerdem kann der Schiedsrichter durch die Parteien nicht gut nach Art eines Sachverständigen befragt werden.

Durch die in der Zivilprozessnovelle 2006 eingeführte Möglichkeit für Parteien, die Verfahrensordnung des Schiedsgerichts stark zu beeinflussen, lassen sich Schiedsverfahren beschleunigt durchführen. Dabei ist allerdings darauf zu achten, dass die Rechtsordnung des Landes, in dem der Schiedsspruch vollstreckt werden soll, in den wesentlichen Teilen eingehalten wird. Andernfalls ist der Schiedsspruch wegen Verletzung des „☞ ORDRE PUBLIC" nicht vollstreckungsfähig.

Nachteile eines Schiedsgerichts: höhere Kosten, Intransparenz der Rechtslage, fehlende Zwangsmittel.

Nachteile eines Schiedsgerichts sind die meistens höheren Kosten und die aufgrund des Ausschlusses der Öffentlichkeit weitgehende Intransparenz der Rechtslage. Außerdem können im Beweisverfahren keine Zwangsmittel, z.B. hinsichtlich der Aussage von Zeugen oder der Herausgabe von Urkunden Dritter, ergriffen werden. Ein Schiedsgerichtsverfahren kann daher für die schwächere Partei von Nachteil sein. Damit ein gültiges Schiedsverfahren eingeleitet werden kann, ist eine einwandfreie und gültige Schiedsklausel im Vertrag notwendig.

SaaS-Verträge sind häufig grenzüberschreitend. Dann sind neben dem ☞ ABGB und dem ☞ UGB unter Umständen auch das **UN-Kaufrechtsübereinkommen** und die EU-Verordnungen **Rom I** (für Vertragsverhältnisse) und **Rom II** (für außervertragliche Schuldverhältnisse) anwendbar, außer diese wurden absichtlich und ausdrücklich ausgeschlossen. Es müssen die Vertragsparteien entscheiden, welche Rechtswahl sie treffen wollen, wobei kaum vorhersehbar ist, welche Rechtsordnung im konkreten Streitpunkt von Vorteil sein wird. Der Einschluss dieser transnationalen Bestimmungen setzt jedenfalls deren Kenntnis und sinnvolle Anwendung voraus. Insbesondere kann der Einschluss dann von Vorteil sein, wenn die mögliche fremde Rechtsordnung weitgehend unbekannt oder stark vom nationalen Recht unvorteilhaft abweicht. Das UN-Kaufrecht gilt immer in internationalen Verträgen, wenn es nicht ausdrücklich ausgeschlossen wird. Die EU-Vollstreckungs-Verordnung vereinfacht und beschleunigt sehr die Exekution innerhalb der EU. Das sollte bei den Vertragsverhandlungen berücksichtigt werden.

Die sehr beliebte „**Salvatorische Klausel**“, die besagt, dass die eventuelle Ungültigkeit einer Bestimmung des Vertrags die anderen Bestimmungen unberührt lässt und die ungültige Klausel durch eine ihr nahekommende gültige Klausel ersetzt werden soll, ist vielfach nutzlos. Zum Einen haben sowohl staatliche Gerichte als auch Schiedsgerichte ohnehin den Vertrag in der Regel so auszulegen, dass er aufrecht bleibt (geltungserhaltende Auslegung). Zum Anderen kann der Ersatz einer ungültigen Klausel durch eine ihr nahekommende oder gleichwertige gültige Bestimmung in der Regel nicht durchgeführt werden, weil damit der

Sinn der gesetzlichen Ungültigkeitsregel (u.a. § 879 Abs. 1 ABGB[13] und § 6 Abs. 3 KSchG[14]) unterlaufen würde. Das wird von den Gerichten daher nicht zugelassen. Die salvatorische Klausel ist also in der Regel nutzlos, da sie etwas vortäuscht, was nicht umgesetzt werden kann.

In manchen Fällen wird die Salvatorische Klausel allerdings ganz gezielt eingesetzt. So ist es nicht unüblich, in ☞ AGB ganz offensichtlich sittenwidrige Normen aufzunehmen, also etwa eine so gut wie vollständige Freizeichnung von Gewährleistungs- und Schadenersatzpflichten. Wie weit eine solche vertragliche Freizeichnung geht, ist oft strittig, aber der Aufsteller der AGB bemüht sich gar nicht erst, eine Formulierung zu finden, die etwa den Ansprüchen der Gerichte genügen könnte. Vielmehr soll der Vertragspartner durch die ganz allgemeine Formulierung bewusst mit einem künstlich geschaffenen Rechtsunsicherheitsrisiko belastet werden.

Die Vereinbarung der **Schriftlichkeit des Vertrags** ist fast immer eine Selbstverständlichkeit. Sie besagt, dass alle Vereinbarungen und Änderungen zu dem Vertrag schriftlich abgeschlossen werden müssen, damit sie wirksam werden. Dieser Formvorbehalt hat aber nicht die absolute Wirksamkeit, die ihm oft unterstellt wird, weil für derartige Verträge nach dem österreichischen Privatrecht Formfreiheit gilt. Dies hat zur Folge, dass die Parteien im Einvernehmen auch jederzeit vom vereinbarten Formvorbehalt abweichen können, auch mündlich! Diese Abweichung muss nicht einmal ausdrücklich, sondern kann auch implizit erfolgen. Der ☞ OGH sieht allerdings die Abweichung vom Formvorbehalt auf Grund von nicht-ausdrücklichen Erklärungen sehr kritisch und beurteilt sie streng. Wegen der besseren Beweislage wird jedenfalls dringend empfohlen, die Verträge sowie alle Ergänzungen und Änderungen schriftlich abzuschließen.

Von einem vertraglich vereinbarten Schriftlichkeitsgebot kann jederzeit einvernehmlich abgegangen werden – sogar mündlich!

13 *§ 879 Abs. 1 ABGB: „Ein Vertrag, der gegen ein gesetzliches Verbot oder gegen die guten Sitten verstößt, ist nichtig."*

14 *§ 6 Abs. 3 KSchG: „Eine in Allgemeinen Geschäftsbedingungen oder Vertragsformblättern enthaltene Vertragsbestimmung ist unwirksam, wenn sie unklar oder unverständlich abgefasst ist."*

1.3 Streitfall

1.3.1 Verfahren zur außergerichtlichen Streitbeilegung

Kommt es zu Streitigkeiten zwischen den Parteien, dann ist es für beide Seiten von Bedeutung, diese so schnell und sauber wie möglich wieder aus der Welt zu schaffen. Das kann mittels der staatlichen Gerichte oder mittels eines vereinbarten Schiedsgerichtes erfolgen (→ 1.2.24). Davor kann es jedoch noch sinnvoll sein, einen **Mediator** einzuschalten, der kein Urteil fällt, sondern beiden Parteien hilft, aufeinander zuzugehen und den entstandenen Konflikt im Gütlichen zu beenden. Es besteht dabei allerdings die Gefahr der Verschleppung.

Vor allem im amerikanischen Rechtsbereich sind verschiedene Verfahren entstanden, gerichtliche Prozesse dadurch zu vermeiden, dass beide Seiten einander auffordern, alle den Streit betreffenden und vorhandenen Beweismittel zu sammeln und der Gegenpartei vorzulegen. Beide Geschäftsleitungen treten sodann zusammen und versuchen den Streitfall mit entsprechender Rechtsberatung gütlich zu lösen. Falls es zu keiner Einigung kommt, kann immer noch ein Gericht angerufen werden. Beide Parteien sind jedoch verpflichtet, sich auf die gesammelten und vorgelegten Beweismittel zu beschränken und bei darüber hinaus gehenden Beweismitteln zu begründen, warum sie nicht schon vorher vorgelegt wurden.

1.4 Insolvenzfall

1.4.1 Zugriff auf Daten unabhängig vom Verfahren

Für den Konkursfall ist sicherzustellen, dass weiter auf Unternehmensdaten und Programme zugegriffen werden kann.

Der Konkurs einer Vertragspartei ist immer auch ein Nachteil für den Vertragspartner. Besonders kritisch ist die Situation im Fall eines Konkurses des Service-Anbieters, weil dadurch die komplette Verfügungsgewalt über die Daten und Programme des Unternehmens auf den **Masseverwalter** übergeht. Dieser vertritt ausschließlich die Interessen der Unternehmensgläubiger, die sich von denen des

ursprünglichen Unternehmens und nunmehrigen Gemeinschuldners komplett unterscheiden können – vor allem im Fall, dass das Unternehmen nicht fortgeführt werden soll. Außerdem fehlt es ihm nicht selten an Erfahrung im IT-Geschäft.

Es ist daher zwischen beiden Parteien zu klären, wie für den Fall der Insolvenz des Anbieters vorzusorgen ist. Die vereinbarte Lösung sollte sicherstellen, dass im Konkursfall auf die Unternehmensdaten und die verwendeten Programme kurzfristig zugegriffen werden kann. Eine vorausschauende vertragliche Lösung für den Insolvenzfall sollte zwar versucht werden, aber man muss dabei berücksichtigen, dass Insolvenzrecht weitgehend zwingendes Recht ist und daher mit einem Vertrag nicht umgangen werden kann. Diese Schwierigkeit wurde durch die Insolvenzrechtsnovelle 2010 verschärft.

Der beste Schutz wird dadurch erreicht, dass die Daten des Kunden sein **„Eigentum“** bleiben und als solche im Herrschaftsbereich des Service-Anbieters erkennbar sind. Das setzt allerdings voraus, dass sie physisch abgrenzbar sind (eigener Server) und dem Kunden am besten täglich oder zumindest wöchentlich in irgendeiner Form zur Verfügung gestellt werden (Rückspielen der verwendeten und verarbeiteten Daten als Backup). Da die Daten alleine für die weitere Verwendung aber zu wenig sein werden, ist auch über die verwendete und aktuelle Verarbeitungssoftware eine vorausschauende Vereinbarung zu treffen. Dies kann dadurch erfolgen, dass diese in der jeweils aktuellsten Form samt einer Installations- und Benützungsanleitung bei einer vertrauenswürdigen Stelle hinterlegt wird, sodass der Kunde im Falle des Konkurses die Verarbeitung seiner Daten in vertretbarer Zeit bei sich selbst oder bei einem anderen Anbieter wieder aufnehmen kann.

Eine weitere Möglichkeit zur Ausschließung der Probleme im Konkursfall des SaaS-Anbieters ist eine **Drei-Parteien-Lösung**. Dabei wird neben der Vereinbarung mit dem eigentlichen Vertragspartner ein zusätzlicher Vertrag mit einem weiteren SaaS-Anbieter abgeschlossen. In diesem wird die regelmäßige Übernahme der Daten und eine Fortsetzung des Dienstes bei bestimmten Arten des Ausfalles des Primär-Anbieters vereinbart. Auch zwischen den beiden Anbietern wird ein Vertrag geschlossen, der die Modalitäten der Übernahme der Daten

Bei einer Drei-Parteien-Lösung sichert ein zusätzlicher Vertragspartner die Fortsetzung des Dienstes bei Ausfall des SaaS-Anbieters.

und der Dienstleistung festlegt. Diese Lösung ist derzeit noch nicht sehr verbreitet, könnte aber von SaaS-Anbietern im wechselseitigen Verbund mit anderen standardisiert angeboten werden. Auf diese Weise ließen sich mit relativ geringen Zusatzkosten Verlässlichkeit und Sicherheit des Software-Dienstes enorm erhöhen.

Ohne solche Vereinbarungen kann es jedenfalls leicht geschehen, dass der Service-Anbieter im Falle seines Konkurses den oder die Kunden mit in die Insolvenz zieht oder zumindest schwer schädigt, ohne dass ein äquivalenter Schadenersatzanspruch durchsetzbar ist.

Für den Fall der Exekution Informationspflicht des Anbieters vorsehen.

Eine weitere Gefahr entsteht dadurch, dass ein Gläubiger des Anbieters per Gericht **Exekution** auf einzelne Sachen des Anbieters führt. Der Anbieter kann dies nur aktiv verhindern, wenn er den Gläubiger und eventuell auch den Gerichtsvollzieher und den Insolvenzverwalter darauf hinweist, dass dadurch auf fremde oder mit fremden Rechten behaftete Sachen zugegriffen wird. Jedenfalls sollte in dem Vertrag daher auch eine Verpflichtung des Anbieters vorgesehen werden, in einem Fall des exekutiven Zugriffs auf Sachen, Daten und Programme, die dem Kunden gehören oder den Leistungsumfang zwischen Anbieter und Kunden entscheidend berühren, zum einen Insolvenzverwalter, Gläubiger und Gerichtsvollzieher auf diese Gefahr sofort hinzuweisen und zum anderen den Kunden über dieses Ereignis zu informieren. Dann kann nämlich der Kunde beim Exekutionsgericht mit der Exszindierungsklage gemäß § 37 Exekutionsordnung (EO) gegen diese Exekution vorgehen und diese möglicherweise verhindern.

1.5 Compliance

In vielen Industriestaaten hat das Verhalten so mancher Unternehmen in den vergangenen Jahren zu erheblichen Auswüchsen und nachteiligen wirtschaftlichen Folgen geführt. Dies verstärkte die heute als „Compliance“ bezeichnete Forderung von Gesellschaft und Politik an die leitenden Personen in multinationalen Organisationen, sich an **gesetzliche Regeln** zu halten und bestimmte **ethische Grundsätze**

zu beachten. Dies sollte an sich eine Selbstverständlichkeit sein. Dennoch verleiten die zwar ähnlichen, in der Durchführung und in Einzelfragen jedoch verschiedenen Rechtsordnungen international operierende Unternehmen häufig dazu, die Unterschiede zum Nachteil von Kunden und Finanzbehörden auszunützen, um einen Vorteil für das Unternehmen zu erzielen. Die Compliance-Anforderungen an diese Unternehmen sollen dies nun verhindern.

Als kritisch für einen österreichischen SaaS-Anbieter oder SaaS-Kunden sind die Forderungen der USA im Rahmen des **Sarbane-Oxley-Act (SOX)** und die Kreditvergaberichtlinien von **Basel II** zu sehen. Zum Beispiel verlangt der SOX von Unternehmen, sofern sie in den USA an der Börse gehandelt werden, Daten Dritter (wie Kunden-, Lieferanten- oder Personaldaten) weiterzugeben. Diese Forderungen widersprechen den EU-Richtlinien für Datenschutz. Die Kreditvergaberichtlinien gemäß Basel II sind für die EU verpflichtend und daher zu beachten.

Die Compliance-Anforderungen richten sich natürlich auch **an SaaS-Anbieter und –Kunden**. Diese haben sich mit ihnen vertraut zu machen und in ihrer Geschäftsgebarung und damit auch in der gegenseitigen Vertragsbeziehung darauf Rücksicht zu nehmen. Eine weitergehende Anleitung dazu ist an dieser Stelle nicht möglich, da die konkreten Anforderungen im Einzelfall doch sehr verschieden sind.

Sowohl Anbieter als auch Kunden haben Compliance-Anforderungen zu beachten.

2.0

Datenschutz & -sicherheit

2.1 Technische Sicherheit

2.1.1 Redundante Speicherverbünde

Erhöhung der Ausfallsicherheit ab RAID-Level 1

Der Massenspeicher, auf dem die operativen Daten gehalten werden, muss gegen die Schadwirkung des Ausfalls einer technischen Komponente gesichert sein. In der Regel werden Festplattenspeicher verwendet. Diese werden durch **Redundanzkonzepte** ausfallsicher gemacht. Ein gängiges Konzept ist die Organisation mehrerer physikalischer Festplatten in einem Festplattenverbund (☞ RAID). Die Zahl hinter der Bezeichnung „RAID" gibt den so genannten **RAID-Level** und damit den internen Aufbau des Speicherverbundes an. Die einzelnen Arten unterscheiden sich im Verhalten bei Lese- und Schreiblast sowie im Verhältnis von Brutto- zu Netto-Kapazität. Zu beachten ist, dass erst ab RAID-Level 1 die Ausfallsicherheit erhöht wird, RAID-0 bietet keine Redundanz! Ein höherer RAID-Level bietet nicht notwendigerweise mehr Sicherheit. Zurzeit sind Speicherverbünde mit RAID-Level 5 üblich, RAID-Level 6 bietet zusätzliche Redundanz (zwei Einheiten können ausfallen, ohne Datenverlust zu verursachen).

2.1.2 Datenaktualität

Wenn Sicherheitskopien der operativen Daten angelegt werden, dann bestimmt die Häufigkeit der Kopienerstellung die minimale Aktualität der Daten bei einer Wiederherstellung. Diese Aktualität ist im Wesentlichen bei Datenverlust durch Benutzerfehler oder bei massiven Schadereignissen interessant, weil geringfügige Schadereignisse durch Redundanzkonzepte abgefangen werden (zum Beispiel der Ausfall einer Festplatte, siehe → 2.1.1).

Tägliches Back-up ist Mindest-anforderung.

Die einzufordernde Aktualität ist von der Art der Daten und der Häufigkeit der Änderungen abhängig. Als zurzeit übliches Mindestmaß kann die Erstellung einer **täglichen Kopie** angesehen werden.

2.1.3 Datenwiederherstellung

Bei Eintritt eines Schadensfalles, der eine Wiederherstellung der operativen Daten notwendig macht, ist die dafür notwendige Zeitspanne eine

interessante Größe. Betrachtet wird dabei die Frist vom Bekanntwerden des Datenverlustes beim Service-Anbieter bis zur vollständigen Inbetriebnahme der Daten der letzten Sicherung. Diese Zeit sollte natürlich möglichst kurz sein, die konkrete Anforderung ist aber stark von der Art der Anwendung abhängig.

Zu unterscheiden ist dabei, ob der gesamte Datenbestand wiederhergestellt werden muss, oder ob nur ein Teil der Daten betroffen ist. Im Allgemeinen ist mit Datenwiederherstellung (oft auch „Data Recovery“) die Wiederherstellung des gesamten Datenbestandes gemeint. Je nach Anwendung und Ausstattung des Anbieters können aber auch punktuelle Wiederherstellungen eventuell durch Versionierung der Daten auf Dateiebene möglich sein.

2.1.4 Wiederherstellung zu bestimmtem Stichtag

Bei der Datenarchivierung werden Sicherungskopien der Datenstände länger als bis zur Durchführung des nächsten Sicherungslaufes aufbewahrt. Die Anzahl der archivierten Datensicherungen und der überstrichene Zeitraum sind von der Art der Anwendung abhängig. Meist werden gemischte Konzepte verwendet, bei denen das Speichermedium mit dem Alter der Daten günstiger, aber auch langsamer wird und die Anzahl der Kopien mit dem Alter reduziert wird.

Die Wiederherstellung zu bestimmten Stichtagen ist besonders für die gesetzlich vorgeschriebene Auskunftserteilung notwendig.

Die Wiederherstellung zu bestimmten Stichtagen ist besonders für die gesetzlich **vorgeschriebene Auskunftserteilung** nach § 26 ☞ DSG 2000 notwendig, wenn dem Betroffenen angegeben werden muss, wann und wie lange bestimmte Daten gespeichert oder wann sie gelöscht wurden. Die unvollständige oder mangelhafte Auskunft kann von der Datenschutzkommission mit Verwaltungsstrafen geahndet werden. Aber auch steuerrechtlich relevante Daten sind eine typische Anwendung für die Wiederherstellung zu einem bestimmten Stichtag. In diesem Bereich kann darauf in der Regel nicht verzichtet werden. Für diese Fälle gilt eine gesetzliche Aufbewahrungspflicht von sieben Jahren. Um dieser zu entsprechen, ist es meistens notwendig, sowohl die Datenbank als auch die Applikation, die das Lesen der Daten erst ermöglicht, verfügbar zu halten.

2.1.5 Laufende Überwachung der Systeme

Eine laufende Überwachung der System-Hardware und der generellen Erreichbarkeit des Systems ist selbstverständlich.

Um auf etwaige Fehlfunktionen von Systemen reagieren zu können, müssen diese laufend überwacht werden. Die Erkennung eines Fehlerereignisses wird meist mittels **automatischer Überwachungssysteme** realisiert, wobei die Art und Auswahl der überwachten Systemzustände für unterschiedliche Qualitätsstufen, sowie die dadurch vermiedenen Gefahren darzustellen sind. Welche Systemzustände konkret überwacht werden müssen, hängt vom erforderlichen bzw. gewünschten Sicherheitsniveau ab. Die Überwachung der System-Hardware sowie der generellen Erreichbarkeit des Systems ist jedenfalls als selbstverständlich zu betrachten. Je nach Anwendung kann zusätzlich die Kontrolle einzelner Dienste notwendig sein.

Ferner ist zu beachten, innerhalb welchen Zeitraums Bedienpersonal von Fehlerereignissen informiert wird und in welcher Zeit darauf reagiert werden kann.

2.1.6 Räumliche Trennung

Um Datenverlust beim **Eintritt massiver Schadereignisse** (z.B. Feuer, Überflutung, Erdbeben) vorzubeugen, ist es notwendig, Sicherungskopien in getrennten Räumlichkeiten zu lagern.

Gemäß § 14 Abs. 1 ☞ DSG 2000 ist unter „Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.“ Absatz 2 konkretisiert diese Norm in Ziffer 4 dahingehend, dass „die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln“ ist.

Damit verlangt der Gesetzgeber implizit, dass die Datenverarbeitung – gleichgültig wer sie durchführt – so zu organisieren ist, dass der Verlust der Daten und auch der unbefugte Zugriff auf sie und deren Zerstörung verhindert werden kann. Die praktische Umsetzung dieser Norm bedeutet aber, dass eine Kopie der Daten und der Programme getrennt von der

normalen Verarbeitung in sicherer Umgebung aufzubewahren ist. Dies ist in der Regel nur durch eine strikte räumliche Trennung möglich.
Wie weit diese räumliche Trennung nun gehen muss, hängt von den konkreten Umständen ab. Sicher ist damit nicht gemeint, dass die Entfernung viele Kilometer betragen muss, aber auch nicht, dass ein schlichter Blechschrank im Serverraum ausreichend ist.

2.1.7 Schutz vor Schadsoftware

Der Schutz vor Schadsoftware ist eine beiderseitige Verpflichtung.

Der Einsatz von Schutzsoftware gegen Schädlinge wie Computer-Viren, -Trojaner und -Würmer ist heutzutage selbstverständlich. Unterschiede können sich beim Update-Management und der entsprechenden Schulung der Mitarbeiter ergeben. Der Schutz des Systems vor Schadsoftware ist eine **beidseitige Verpflichtung** und kann sich nicht auf eine Firewall und ein Anti-Virenprogramm beschränken. Die Organisation der Zugriffe von innen auf außen liegende Server als auch von außen auf die innen liegenden Server einer Datenverarbeitung muss konkreten und ständig aktualisierten **Regeln** unterworfen werden, um die Einschleusung von Schadsoftware soweit wie möglich zu verhindern oder zumindest durch regelmäßige Kontrolle zu entdecken. Immer häufiger kommen sogenannte Intrusion Prevention Systeme (☞ IPS) zum Einsatz, die den Datenverkehr nicht nur auf Netzwerkebene, sondern auch auf Protokollebene überwachen.

Es ist hinreichend bekannt, dass die **größte Gefahr durch (Fehl-) Bedienung durch Mitarbeiter** des eigenen Unternehmens und des Dienstleisters ausgeht. Aber auch die Angriffe von außen nehmen an Heftigkeit, Raffinesse und Komplexität ständig zu. Daher ist diesem Bereich eine ständige Aufmerksamkeit zu widmen und diese durch entsprechende Protokollierung nachzuweisen.

2.1.8 Netzwerksicherheit

Auch die Netzwerke sind gegen Störungen und Ausfall zu sichern.

So wie Server und Peripheriegeräte gegen Schadsoftware, Angriffe und Manipulationen von innen und außen geschützt werden müssen, sind auch die Netzwerke und ihre einzelnen Komponenten gegen derartige Gefahren sowie gegen Störungen und Ausfall zu sichern. Dies erfordert technische und organisatorische Regeln sowie Überwachungsmaßnahmen, die der regelmäßigen Kontrolle sowie der Protokollierung bedürfen.

Firewalls und andere aktive Netzkomponenten müssen auf dem aktuellen Stand der Betriebssoftware gehalten werden. Der Zugang zu diesen Elementen ist streng zu regeln, um eine Manipulation zu erschweren. Nach Möglichkeit sind nur verschlüsselte Zugänge zu verwenden, die Authentifizierung sollte auf Zertifikaten basieren.

2.1.9 Sicherheit der technischen Einrichtung

Damit die oben genannten Sicherheiten gegen den Verlust und die Zerstörung der Daten auch wirksam werden, sind entsprechende bauliche, elektrische und organisatorische Regeln beim Aufbau und beim Betrieb einer IT-Anlage, die auch für Dritte Dienstleistung erbringt, zu beachten und ständig zu aktualisieren.

Dazu gehören in baulicher Hinsicht die **Einhaltung von Mindestnormen** für Wände, Fußböden und Decken, um Sicherheit gegen Feuer, Wasser und Einbruch zu bieten.

Das gesamte IT-Netzwerk ist außerdem sowohl gegen Blitzschlag als auch gegen Überspannungen aus der Stromversorgung abzusichern. Grundvoraussetzung dafür ist eine korrekte Blitzschutzanlage des Gebäudes und die ordnungsgemäße Erdung (Sternerdung aller Erdungsleitungen an einem Punkt). Dies allein reicht jedoch nicht. Es sind überdies auch die Leitungen der internen Netze im Serverraum sowie die nach außen oder zu Peripheriegeräten führenden so zu legen, dass keine Flächen entstehen, die die starken hochfrequenten Schwingungen eines Blitzeinschlages aufnehmen können. Dies könnte Zerstörungen an der empfindlichen Elektronik verursachen.

Der Schutz des Serverraums gegen Hochwasser und auch gegen Löschwasser (bei externem Feuer) ist vorweg zu planen und sicherzustellen. Brandmeldeanlagen und Löscheinrichtungen im Serverraum sind unverzichtbare Einrichtungen.

Wie weit eine Videoüberwachung des Zutritts zum Serverraum und innerhalb des Serverraums durchzuführen ist, muss im Einzelfall entschieden werden (wegen der notwendigen Genehmigung durch die Datenschutzkommission). Der Einbruchschutz ist in Räumen, in denen

kritische Netzkomponenten (Switches, Router und Verteiler) untergebracht sind, ebenso wie für den Serverraum selbst zu regeln.

2.2 Organisatorische Sicherheit

2.2.1 Schutz vor Zugriff durch nicht-berechtigte Personen

Achtung, der Schutz vor unberechtigtem Zugriff hat auch die Sicherungskopien zu umfassen!

Für den Schutz des Zugriffes auf Daten ist auf den **Umgang mit Passwörtern**, die Art der **Authentifizierung**, die **Zugriffsregelungen** sowie die **Klassifizierung der Daten** nach Vertraulichkeit und Integrität zu achten. Nicht vergessen werden darf, dass diese Schutzmaßnahmen immer auch die Sicherungskopien zu umfassen haben.

Zu klären ist vorrangig,

- wer wann welchen Zugriff auf welche Daten hat,
- ob es eine „☞ SECURITY POLICY“ gibt (die intern bekannt ist),
- ob Log-Daten über jeden Zugriff vorliegen und
- welche Schutzmaßnahmen gegen Zugriff durch Dritte getroffen werden.

Zugriffsberechtigungen sind transparent und eindeutig zu regeln. Dies gilt auch für die Mitarbeiter des Kunden!

Wie in → 1.2.5 dargestellt, unterliegen die meisten Daten eines Unternehmens dem DSG 2000 auch dann, wenn sie keine Daten von physischen Personen sind, sondern z.B. nur die Anlagenbuchhaltung umfassen. Es sind daher praktisch alle verarbeiteten Informationen eines Unternehmens datenschutzrechtlich relevant und damit schutzwürdig und geheimhaltungspflichtig. Entsprechend transparent und eindeutig ist der Datenzugriff zu regeln. Dies betrifft auch die Mitarbeiter des Kunden! Zugriffsberechtigungen sind durch entsprechende Maßnahmen (z.B. sichere Authentifizierung und Protokollierung durch digitale Signaturen) zu sichern. Ein entsprechendes Gesamtkonzept, das sowohl den Zugriff und die Authentifizierung durch Mitarbeiter des Kunden als auch durch die Mitarbeiter des Anbieters darstellt und überprüfbar macht, ist zwingend notwendig.

Zur Verdeutlichung sei an dieser Stelle § 14 Abs. 1 und Abs. 2 DSG 2000 vollständig zitiert:

Datensicherheitsmaßnahmen

§ 14 (1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht zugänglich sind.

(2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,

1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

2.2.2 Patch-Management

☞ PATCH-Management legt fest, welches System zu einer bestimmten Zeit um welche Patches erweitert werden soll. Vorzusehen ist es sowohl bei der Server-Software als auch bei der eventuell zum Einsatz kommenden Client-Software. Durch den Einsatz unterstützender Software kann der Überblick über Versionsstände sowie der zeitliche Ablauf der Umstellung erleichtert, teilweise automatisiert werden. Unabhängig davon müssen diese Prozesse beschrieben und die Befugnisse, wer wo welche Patches einbringen darf, klar geregelt sein.

2.2.3 Trennung von Entwicklung und Produktion

Produktiv- und Testsysteme sind unbedingt zu trennen.

Eine Trennung zwischen Produktiv- und Test-Systemen ist unbedingt notwendig. Nur durch umfangreiche Tests auf einem eigenen, dem Produktiv-System nahezu identischen System können Änderungen und Erweiterungen an Applikationen mit hoher Sicherheit und realitätsnah getestet werden.

Art und Umfang der Tests sollten dokumentiert sein, ebenso die Ergebnisse. Automatische Testumgebungen erleichtern die Testarbeit und sorgen für konstante Qualität.

2.2.4 Verwendung von Echtdaten im Testbetrieb

Beachtung von Datenschutz für den Fall von Tests mit Echtdaten.

In erster Linie sind für Applikationstests systematische Testdaten zu verwenden. In manchen Fällen ist dieser Ansatz nicht ausreichend und es sind Echtdaten oder Auszüge daraus für Tests heranzuziehen. In diesem Fall muss auf die Einhaltung des Datenschutzes geachtet werden. Außerdem müssen in diesem Fall Rechte und Möglichkeiten der Tester dem gesteigerten Sicherheitsniveau angepasst werden. Ebenso hat die Protokollierung der Zugriffe einer höheren Sicherheitsstufe zu genügen.

2.3 Allgemeines

2.3.1 Datenverfügbarkeit bei Nichtverfügbarkeit des Software-Dienstes

Der Verfügbarkeit der im SaaS-Modell verarbeiteten Daten für den Fall der Nichtverfügbarkeit des Software-Dienstes sollte große Beachtung geschenkt werden. Ein kurzfristiger Ausfall des Dienstes und damit der Daten behindert meist nur den Betriebsablauf im Unternehmen und kann verschmerzt und ein etwaiger Schadensausgleich im Entgelt geregelt werden. Wesentlich schwerwiegender für ein Unternehmen wirkt sich dagegen die längerfristige oder andauernde Nichtverfügbarkeit der Daten aus.

Die Anforderungen an die Aktualität der verfügbaren Daten bzw. an die Art der Zurverfügungstellung hängen vom Einzelfall ab und können nur konkret festgelegt werden. Auf eine Diskussion dieses Aspektes sollte nicht verzichtet werden!

Voraussetzung für die Software-unabhängige Datenverfügbarkeit ist im Wesentlichen eine **Exportfunktion**, die Daten so zur Verfügung stellt, dass sie mit allgemein verfügbarer Software gelesen werden können. Es empfiehlt sich, vertraglich festzuhalten, mit welcher konkreten Software die Daten lesbar sein sollen.

Die Software-unabhängige Datenverfügbarkeit ist durch eine Exportfunktion sicherzustellen.

Besonders kritisch ist die Situation im Falle einer Insolvenz des Service-Anbieters, weil dadurch die Verfügungsgewalt über die Daten und Programme des Unternehmens auf den Insolvenzverwalter übergeht (siehe dazu ausführlich → 1.4.1).

2.3.2 Löschung von Daten

Sowohl auf Wunsch des Kunden als auch durch gesetzliche Verpflichtung kann ein Service-Anbieter **zur Löschung von Daten verpflichtet** werden. Je nach Auftrag kann sich dies auf den aktuellen Datenbestand oder auf alle, also auch die archivierten Daten beziehen. Unterschieden werden muss ebenfalls, ob es sich um eine

Ein Service-Anbieter kann zur Löschung von Daten verpflichtet werden.

Löschung aller Daten eines Kunden oder einiger definierter Daten handelt.

Auf diese Weise kann eine Löschanforderung mitunter einen **erheblichen Aufwand** für den Anbieter bedeuten. Daher ist es empfehlenswert, im Vorhinein abzuklären, welche Anforderungen technisch möglich und mit welchem Aufwand sie verbunden sind. Dabei müssen eventuelle rechtliche Rahmenbedingungen, wie etwa die Aufbewahrungspflicht laut § 14 Abs. 1 (siehe → 2.2.1)oder § 27 Abs. 3 bis 7 DSG 2000 beachtet werden.

Die strenge Verpflichtung des DSG 2000 zur unwiderruflichen Datenlöschung umfasst auch alle Backups!

Bei gesetzlich vorgeschriebenen Löschanforderungen (§ 27 und § 28 DSG 2000) genügt es nicht, die Daten in der üblichen Art, also mit einem einfachen Systembefehl zu löschen. Laut Gesetz muss nämlich sichergestellt sein, dass die Daten unwiderruflich gelöscht sind und auf keinen Fall wiederhergestellt werden können. Zu beachten ist, dass diese Anforderung auch die üblicherweise vorliegenden Backups umfasst! Überdies ist ein rechtlich anerkannter Nachweis über die Löschung zu erbringen, etwa in Form einer signierten ☞ LOG-DATEI.

2.3.3 Datenschutz

Für den Datenschutz sind die Bestimmungen des ☞ DSG 2000 einzuhalten. Kunde und Anbieter sollten in diesem Zusammenhang die Art der zu verarbeitenden Daten prüfen und sich mögliche **gesetzliche Einschränkungen** bei der Verarbeitung und dem Zugriff bewusst machen.

Jedermann hat das Recht auf Auskunft über ihn betreffende Daten.

Das DSG 2000 gibt dem Betroffenen das verfassungsmäßig gewährleistete Recht, **jederzeit Auskunft** über die über ihn verarbeiteten Daten, ihre Herkunft, die Übermittlungsempfänger und den Zweck der Verarbeitung und ihre Rechtsgrundlagen in verständlicher Form zu erhalten (§ 26), wobei eine Auskunft im Jahr sogar unentgeltlich zu geben ist. Damit ist auch das Recht verbunden, die verarbeiteten Daten richtig stellen und löschen zu lassen. Damit diese Auskunft überhaupt gegeben werden kann, sind sowohl technische als auch organisatorische Regelungen vorzusehen. Sie sind abstrakt

in § 14 DSG (siehe → 2.2.1) niedergelegt und jedenfalls einzuhalten. Andernfalls muss man mit Einsichtnahmen und Empfehlungen der Datenschutzkommission, nachteiligen Urteilen der Zivilgerichte (z.B. zu Schadenersatzpflichten) und auch Verwaltungsstrafen rechnen.

3.0

Ausfallsicherheit

3.1 Aufklärung durch den Anbieter

In der Verhandlungsphase hat der Service-Anbieter die Pflicht, aktiv auf die Thematik „Ausfallsicherheit“ hinzuweisen, die wesentlichen Rahmenbedingungen zu erläutern und den konkreten Bedarf mit dem Kunden abzustimmen. Dieser ist dabei zumindest darüber zu informieren, was dazu üblicherweise in vergleichbaren Fällen vereinbart wird, also „verkehrsüblich“ ist. Diese Aufklärung ist von grundlegender Bedeutung. Den Anbieter trifft diesbezüglich eine **vorvertragliche Aufklärungspflicht**: Er muss die Bedeutung des Dienstes für den Kunden ermitteln, um dann die notwendige Verfügbarkeit zu bestimmen. Ein Verstoß kann Schadenersatzpflichten zur Folge haben.

Anbieter unterliegt einer (vorvertraglichen) Aufklärungspflicht.

3.2 Vereinbarung der zulässigen Ausfallzeiten

Für die Erfüllung dieses Kriteriums sind zumindest die gewünschten **Betriebszeiten**, der **Messzeitraum** (Monat/Jahr/Quartal) sowie die **prozentuelle Verfügbarkeit** innerhalb des Messzeitraums und der Betriebszeiten zu bestimmen.

Festlegung von Betriebszeiten, Messzeitraum und prozentueller Verfügbarkeit.

An Hand eines Beispiels soll anschaulich dargestellt werden, wie unterschiedliche Interpretationen oder Sichtweisen die Werte der Ausfallzeiten beeinflussen:

> Zwischen Anbieter und Kunde wird eine Verfügbarkeit von 99% vereinbart (ohne den Messzeitraum festzulegen).
> In den ersten beiden Monaten steht die Software in der für den Kunden kritischen Zeit von 8:00 bis 18:00 Uhr für insgesamt 84 Stunden nicht zur Verfügung. Aus Sicht des Kunden bedeutet dies eine Verfügbarkeit des Software-Dienstes von lediglich 80%, da er den Anteil an den für ihn kritischen 420 Geschäftsstunden (21 Arbeitstage á 10 Stunden mal 2

Monate) bemisst. Der Anbieter jedoch kann ohne schlechtes Gewissen behaupten, die vereinbarte Verfügbarkeit eingehalten zu haben, wenn er als Messzeitraum ein Jahr „Rund-um-die-Uhr“ Betrieb annimmt. Die 84 Stunden Ausfall bedeuten in dieser Berechnung eine Verfügbarkeit von 99,041%, gemessen an gesamt 8760 Stunden (365 Tage á 24 Stunden). Bei dieser Berechnung darf der Dienst in den folgenden 10 Monaten allerdings nur noch maximal 3,6 Stunden ausfallen.

Das Beispiel zeigt die unterschiedlichen Interpretations-möglichkeiten, wenn keine Messzeiträume vereinbart werden. Wäre als Messzeitraum die Geschäftszeit von 8:00 bis 18:00 Uhr während eines durchschnittlichen Monats mit 21 Arbeitstagen – also eine Zeitspanne von insgesamt 210 Stunden – vereinbart worden, so würde eine Verfügbarkeit von 99% den Ausfall von 2,1 Stunden bedeuten und wäre noch hinnehmbar.

Die Anforderungen an die Verfügbarkeit können je nach Art des Arbeitsplatzes und der Leistung stark variieren.

Bei der Vertragsvereinbarung ist weiters darauf zu achten, dass die Anforderungen an die Verfügbarkeit je nach Art des Arbeitsplatzes und der Leistung **stark variieren** können. Zum Beispiel sind die Leistungen für bestimmte Arbeitsplätze auf die Zeit von 8:00 bis 18:00 Uhr wochentags beschränkbar, wobei eine durchschnittliche Ausfallzeit von 2h/Monat hinnehmbar ist und einer Verfügbarkeit von etwa 99,1% entspricht. Die untere Grenze wird bei 97% liegen, was eine Ausfallzeit von etwa 6,6h/Monat bedeutet. Hingegen kann für unternehmenskritische Dienste eine Verfügbarkeit von Montag bis Samstag von 7:00 bis 20:00 Uhr (insgesamt also 318 Stunden im Monat) bei einer möglichen Ausfallzeit von durchschnittlich rund einer Viertelstunde pro Monat notwendig sein. Dies entspricht einer Verfügbarkeit von 99,93% pro Monat. Die untere Grenze wird bei 99,5%, also etwa 1,7h pro Monat für solche Leistungen liegen. Müssen mehrere Zeitzonen bedient werden, steigt die notwendige Verfügbarkeit solcher Leistungen schnell auf 99,95% pro Monat und mehr. Für diese Fälle müssen dann schon sehr ausgefeilte Konzepte mit geregelten Wartungsfenstern, Stundenplänen und Ankündigungsfristen erarbeitet werden.

Unter Umständen ist es sinnvoll, über die Mindestanforderung der vertraglichen Festlegung einer Gesamtverfügbarkeit hinauszugehen und

zum Beispiel unterschiedliche Kategorien von „Ausfall“ einzuführen: „Komplettausfall“, „Teilausfall“, „unwesentliche Einschränkung“.

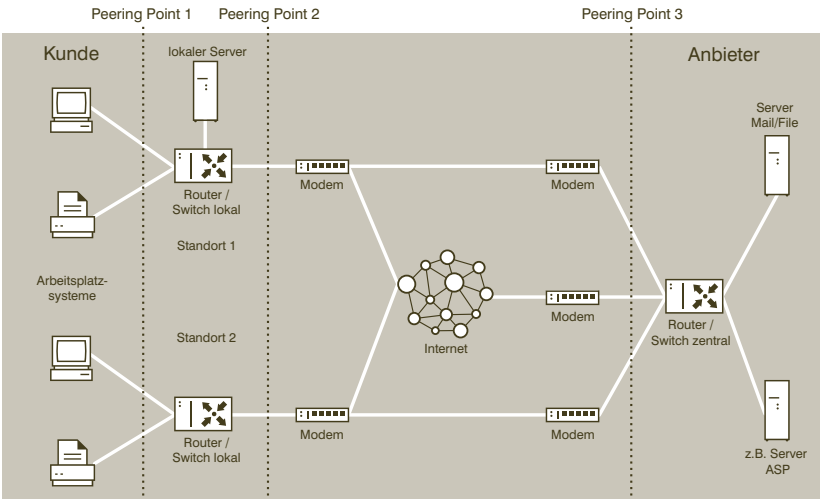
3.3 Festlegung der Methode der Feststellung eines Ausfalls

Es empfiehlt sich in jedem Fall festzulegen, wie ein Ausfall tatsächlich festgestellt wird und wie dabei konkret vorgegangen wird. Die Messung ist abhängig von der konkreten Leistung. Ist zum Beispiel eine „Erfüllung vor Ort“ vereinbart, hat die Messung auch die Verfügbarkeit des lokalen Internets zu umfassen. Um eine derartige Ausuferung zu vermeiden, empfiehlt es sich, die Verfügbarkeit bis zu einem bestimmten **Peering Point** zu vereinbaren.

Verfügbarkeit am besten bis zu bestimmtem Peering Point vereinbaren.

Dabei bestehen grundsätzlich mehrere Varianten, wo der Peering Point liegt und was für Bereiche er umfasst. Die folgende Grafik zeigt die verschiedenen Möglichkeiten.

Muster für ein SaaS-Service



Die für den Software-Anbieter günstigste Lösung ist ein Peering Point am Ausgang seines zentralen Routers (Peering Point 3). Dann haftet er nur für diejenigen Komponenten, die er unter seiner unmittelbaren Kontrolle hat, nämlich Server, zentraler Router und die Verkabelung dazwischen. Der Kunde hingegen muss sich um die Beschaffung und Einrichtung aller Komponenten wie Modems, Leitungen, Router, Firewalls, eventuelle lokale Server und Arbeitsplatzgeräte sowie um die Verkabelung dazwischen selbst kümmern und deren störungsfreien Betrieb aufrechterhalten.

Die für den Kunden wiederum günstigste Lösung ist, wenn der Peering Point direkt bei seinen Geräten, mit denen die Software-Dienstleistung genutzt wird, liegt (Peering Pont 1). Denn dann übernimmt der Anbieter Beschaffung, Einrichtung und störungsfreien Betrieb aller Komponenten von seinem Server bis hin zu den Endgeräten beim Kunden. Dies ist insbesondere dann eine für den Kunden sinnvolle Lösung, wenn er über wenig oder gar keine Sachkenntnis betreffend IT-Einrichtungen und deren Betrieb verfügt; vorausgesetzt natürlich, der Anbieter kann diese Leistungen überhaupt erbringen.

Ein Kompromiss ist Peering Point 2. Der Anbieter ist dann für die Datenübertragung bis zum Kunden verantwortlich, er besorgt und betreut die Mietleitung oder auch das Internet-Service bis zum Kunden. Die lokale Vernetzung ist dann Sache des Kunden.

Bei der Ermittlung der Verfügbarkeit des Software-Services ist dann jedenfalls die Reihenschaltung der einzelnen Komponenten zu berücksichtigen, die sich aus der Grafik ergibt. Für Redundanzkonzepte wird auch die Parallelschaltung von Geräten verwendet. Für jede dieser Schaltungskonzepte kann man die resultierende Zuverlässigkeit und die Verfügbarkeit berechnen. Kompliziert wird diese Berechnung für gemischte Reihen- und Parallelschaltungen. Für die Ermittlung der Verfügbarkeit für alle drei Konzepte wird auf die Literatur zur „**Zuverlässigkeitsanalyse**“ verwiesen.

3.4 Definierte Folgemaßnahmen

Zur Vermeidung von Streitigkeiten ist es wichtig festzulegen, welche Maßnahmen vom Service-Anbieter und eventuell auch vom Kunden bei Nichtverfügbarkeit der Software-Dienstleistung zu setzen sind.
Wesentlich ist dabei vor allem, eine **konkrete Vorgangsweise** zu vereinbaren (siehe auch → 1.2.4). Zum Beispiel:

Für den Fall der Nichtverfügbarkeit sollte eine konkrete Vorgangsweise vereinbart werden.

- Als Reaktion auf eine Störungsmeldung durch den Kunden wird auf dem Rechner des Kunden eine Messung durchgeführt (Ansprechstellen vereinbaren, mit denen die Behebung des Ausfalls erarbeitet wird).
- Eskalationsmanagement: Dafür wird festgelegt, welche hierarchischen Stellen auf der verantwortlichen Seite angesprochen werden, wenn die vorhergehende Stelle einen Ausfall nicht beheben konnte.
- Welche wechselseitigen Pflichten sind von den Vertragsparteien zu erfüllen, damit der vertraglich vereinbarte Zustand wieder erreicht werden kann?

3.5 Vereinbarung einer (finanziellen) Sanktion bei Überschreitung

Für den Fall der Überschreitung der vereinbarten Ausfallszeiten sind Sanktionen zu vereinbaren. Dafür gibt es grundsätzlich zwei Möglichkeiten: **Entgeltminderung** oder **Pönalzahlung** (pauschalierter Schadenersatz).

Kunden unterliegen einer Schadensminderungspflicht!

Zu beachten ist allerdings, dass den Kunden eine Schadensminderungspflicht trifft. Dies bedeutet, dass er ihm zumutbare Maßnahmen ergreifen muss, um den durch den Ausfall entstehenden Schaden möglichst gering zu halten. Vom Anbieter kann dies im Streitverfahren eingewendet werden.

Achtung! Für den Anbieter kann sich im Fall einer außergewöhnlichen Störung eine Warnpflicht ergeben, auch wenn diese nicht ausdrücklich vereinbart wurde. Deren Versäumnis kann eine Schadenersatzpflicht des Anbieters begründen.

4.0

Betriebsverhalten

4.1 Antwortzeitverhalten

4.1.1 (Vor-)vertragliche Aufklärung durch den Anbieter

Hier gelten die Ausführungen zu → 3.1 in gleicher Weise. Den Service-Anbieter trifft in der Verhandlungsphase die Pflicht, aktiv auf die Thematik des Antwortzeitverhaltens seines Dienstes hinzuweisen, die wesentlichen Rahmenbedingungen zu erläutern und den konkreten Bedarf mit dem Kunden abzustimmen. Ein Verstoß gegen die vorvertragliche Aufklärungspflicht kann schadenersatzrechtliche Konsequenzen haben.

4.1.2 Bestimmung der Parameter für das Antwortzeitverhalten

Der Begriff Antwortzeitverhalten wird häufig auch als „**Performance**“ eines Dienstes umschrieben, ist allerdings präziser und wird daher hier bevorzugt verwendet.

Unter **Antwortzeitverhalten** versteht man im Allgemeinen jenes Zeitintervall, das vom Auslösen einer Anfrage bis zum Erscheinen der Antwort auf dem Bildschirm oder bis zum Beginn der gewünschten Reaktion auf einem Arbeitsplatzgerät dauert. Dieses Zeitintervall soll erfahrungsgemäß bei Bildschirmarbeiten im Durchschnitt nicht länger als eine Sekunde dauern. Längere Zeiten können sich nämlich über einen Monat auf beträchtliche Wartezeiten summieren. So werden z.B. bei Buchhaltungsarbeiten täglich bis zu 300 Anfragen oder Buchungssätze eingegeben. Eine durchschnittliche Wartezeit von zwei Sekunden summiert sich also auf 600 Sekunden pro Tag. Bei durchschnittlich 21 Arbeitstagen ergibt dies pro Monat 12.600 Sekunden oder 3,5 Stunden Arbeitszeit...

Höhere Antwortzeiten können sich zu beträchtlichen Wartezeiten summieren.

Gemessen wird die Antwortzeit in der Regel mittels Systemsoftware am Arbeitsplatzgerät. Zur Kontrolle sollte darüber ein laufendes Protokoll geführt werden. Damit können auch die Vereinbarungen im Servicelevel-Agreement überwacht werden.

Planen kann man die Antwortzeit mittels der sinngemäß angewandten ☞ VERKEHRSTHEORIE. In der Telekommunikationsbranche wurden

bereits seit Jahrzehnten entsprechende Formeln und Tabellen erstellt, die auch auf IT-Komponenten anwendbar sind.

Festzulegen sind durchschnittliche Antwortzeit, zu erreichender Prozentsatz und Messzeitraum.

Die Zusage des Anbieters sollte folgende Punkte umfassen: die **durchschnittliche Antwortzeit**, den zu erreichenden **Prozentsatz** und den **Messzeitraum**. Dieser sollte die die durch Messung über mindestens eine Woche zu ermittelnde Hauptverkehrsstunde umfassen. Diese Messung ist öfter zu wiederholen, weil sie sich durch Organisationsänderungen und andere Mitarbeiter verschieben kann.

Eine Vereinbarung betreffend Antwortzeitverhalten könnte also z.B. lauten:

- Antwortzeit: maximal 0,9 Sekunden; die Antwort ist also in weniger als 0,9 Sekunden am Schirm
- Prozentsatz: 95%; die Antwortzeit von maximal 0,9 Sekunden wird in 95% aller Fälle unterschritten (oder: nur 5% der Antwortzeiten überschreiten 0,9 Sekunden)
- Messzeitraum: 10:15 bis 11:15 Uhr; in diesem Zeitraum, in dem im Regelfall der höchste Verkehr auftritt, werden die angegebenen Werte erreicht

4.1.3 Festlegung der Messmethode

Wichtig ist die Vereinbarung des maßgeblichen Messorts.

Der Anbieter sollte dazu entsprechende Mess-Software anbieten. Es gibt bewährte Messmethoden.

Wichtig ist dabei, auch den Messort (siehe auch → 3.3 und die Grafik) zu definieren. Dieser ist in Abhängigkeit vom Umfang der vertraglich vereinbarten Leistung festzulegen. Eventuell kann auch eine Kontrollmöglichkeit auf einem Arbeitsplatzgerät (PC) angeboten werden.

4.1.4 Definierte Folgemaßnahmen

Wie näher in → 3.4 ausgeführt, sollten konkrete Maßnahmen, die vom Anbieter und eventuell auch vom Kunden bei verzögerter Antwortzeit zu setzen sind, vereinbart werden.

4.1.5 (Finanzielle) Sanktion bei Überschreitung

Die Vereinbarung einer finanziellen Sanktion ist eine sinnvolle Maßnahme, um die Einhaltung der vereinbarten Parameter zu gewährleisten. Der Schaden durch eine Überschreitung der als zulässig vereinbarten Wartezeit ist einfach feststellbar. Es ist Ersatz für die Überschreitung der zulässigen Wartezeit zu leisten und zwar als **Entgeltminderung** oder pauschalierter **Schadenersatz**.

Der tatsächliche Schaden ist oft schwer festzustellen, mitunter könnte er sowohl für den einen als auch für den anderen Vertragspartner ruinös sein. Ziel ist daher, eine faire Entschädigung zu vereinbaren.

Das Ziel: eine faire Entschädigung für den entstandenen Schaden.

4.1.6 Schutz des Gesamtsystems gegen punktuelle Überlastung

Für die reibungslose Nutzung einer Software-Dienstleistung kann es von großer Bedeutung sein, welche Vorkehrungen der Service-Anbieter für den Fall von **Belastungsspitzen** getroffen hat. In vielen Fällen ist es für den Service-Anbieter sinnvoll, vertraglich die Möglichkeit zu vereinbaren, durch teilweise Einschränkung des Dienstes (der Rechenkapazität) das System vor Überlastungen zu schützen – insbesondere wenn diese durch Kundenfehlbedienung oder Überschreitung der vereinbarten Maximallast verursacht wurden.

4.2 Organisatorische & technische Skalierbarkeit

4.2.1 Offenlegung systembezogener Parameter durch den Anbieter

Der Service-Anbieter muss Aussagen zu den Belastungsgrenzen des Systems treffen können. Die konkreten Anforderungen an die Skalierbarkeit hängen naturgemäß stark vom konkreten Bedarf des Kunden ab.

Aussagen zu den Belastungsgrenzen des Systems müssen möglich sein!

5.0

Glossar

Glossar

ABGB
„Allgemeines Bürgerliches Gesetzbuch“; die wichtigste Kodifikation des Zivilrechts in Österreich, seit 1812 in Kraft und damit das älteste gültige Gesetzbuch im deutschsprachigen Rechtsraum.

AGB
„Allgemeine Geschäftsbedingungen“; vorformulierte Vertragsbedingungen des Leistungsanbieters (umgangssprachlich oft auch „das Kleingedruckte“ genannt)

Application Service Providing (ASP)
Ursprünglich gebräuchlicher Begriff für „Software as a Service (SaaS)“, wird mittlerweile weitgehend synonym verwendet.

Dauerschuldverhältnis
Vertragsverhältnis, das auf Dauer angelegt ist, sich also nicht in einem einmaligen Leistungsaustausch erschöpft (z.B. Miete, Dienstverhältnis); Zielschuldverhältnis: Der Leistungsinhalt steht bei Vertragsschluss schon (vollständig) fest bzw. ist zumindest bestimmbar (z.B. Kauf- oder Werkvertrag).

DSG 2000
das geltende (österreichische) Datenschutzgesetz

Intrusion Prevention System (IPS)
IPS ist ein Schutz- und Kontrollsystem, das in eine Datenleitung integriert alle ein- und ausgehenden Daten überwacht (ähnlich einer Firewall). Wenn das IPS ein verdächtiges Datenpaket entdeckt, wird dieses nicht in das Netzwerk gelassen und sofort blockiert.

ITIL

„IT Infrastructure Library“; eine Sammlung von Good Practices in einer Reihe von Publikationen, die eine mögliche Umsetzung eines IT-Service-Managements (ITSM) beschreiben und inzwischen international als De-facto-Standard hierfür gelten. In dem Regel- und Definitionswerk werden die für den Betrieb einer IT-Infrastruktur notwendigen Prozesse, die Aufbauorganisation und die Werkzeuge beschrieben. Die ITIL orientiert sich an dem durch den IT-Betrieb zu erbringenden wirtschaftlichen Mehrwert für den Kunden. Dabei werden die Planung, Erbringung, Unterstützung und Effizienz-Optimierung von IT-Serviceleistungen im Hinblick auf ihren Nutzen als relevante Faktoren zur Erreichung der Geschäftsziele eines Unternehmens betrachtet. (Quelle: Wikipedia)

KSchG

österreichisches Konsumentenschutzgesetz

Log-Daten bzw. Log-Datei

automatische Protokollierung aller oder bestimmter Aktionen in einem Computersystem

OGH

„Oberster Gerichtshof“; die höchste Instanz in Zivil- und Strafsachen in Österreich und damit maßgeblich für die Rechtsfortbildung

Ordre public

(franz. für öffentliche Ordnung), als „Grundwertungen einer Rechtsordnung“ zu verstehen. Die allgemeine Regel besagt sinngemäß, dass eine ausländische Entscheidung nicht anerkannt und damit nicht vollstreckbar wird, wenn die Anerkennung der öffentlichen Ordnung (ordre public) des Staats, in dem sie geltend gemacht wird, offensichtlich widersprechen würde. Innerhalb der EU wurde die Anwendung des „Ordre public“ durch die EU-Vollstreckungs-Verordnung weitgehend ausgeschaltet. Diese bestimmt, dass ein zu vollstreckendes Gerichts- oder Schiedsgerichtsurteil aus einem EU-Mitgliedstaat nicht mehr in dieser Hinsicht überprüft werden darf. Dem liegt der Gedanke zugrunde, dass die Grundwertungen der Rechtsordnungen der EU-Mitgliedstaaten untereinander und mit der EU-Grundrechtscharta in Einklang stehen.

Patch

Als Patch wird eine Auslieferung eines (kleinen) Software-Paktes verstanden, das beispielsweise dazu dient, Sicherheitslücken zu schließen, Software-Fehler zu beheben oder die Programm-Funktionalität zu erweitern.

RAID

„Redundant Array of Independent Disks“ (deutsch: redundante Anordnung unabhängiger Festplatten; urspr. „Redundant Array of Inexpensive Disks“); bei RAID-Systemen werden mehrere physische Festplatten in einem Verbund so organisiert, dass ein Teil der Plattenkapazität zur Speicherung gleichartiger Information verwendet wird. Auf diese Weise können bei einem Plattenausfall die Daten wiederhergestellt bzw. höhere Transferraten erzielt werden. RAID-Systeme bieten die Möglichkeit, (ausgefallene) Festplatten während des laufenden Betriebs auszutauschen. Die einzelnen Konfigurationen werden als RAID-Level bezeichnet.

Software as a Service (SaaS)

Mit Software as a Service (SaaS) bezeichnet man die Bereitstellung von Anwendungen und Programmfunktionalitäten zur Nutzung über ein Computernetzwerk. Ein Application Service Provider stellt dabei entweder marktgängige Standard-Software oder Software, die speziell für diesen Zweck entwickelt wurde, sowie die dafür notwendige Infrastruktur zur Verfügung. Die Anwendung wird üblicherweise von einer Vielzahl von Anwendern genutzt. Die Bezahlung erfolgt in der Regel nach einem Dienstleistungsvertrag, z.B. abhängig von der Anzahl der getätigten Transaktionen oder als monatlicher Fixbetrag. Der SaaS-Anbieter sorgt für die Softwarelizenz, die Pflege und den Update. Für den Nutzer stellt er in geeigneter Form Support zur Verfügung.

Security Policy

Damit sind unternehmensinterne Sicherheitsrichtlinien gemeint. Eine Security Policy hat die Sicherstellung von Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität der Informationen zum Ziel und muss von allen Mitarbeitern zur Kenntnis genommen, verstanden und beachtet werden.

UGB

„Unternehmensgesetzbuch“; eine in vielen Bereichen modernisierte Version des alten HGB (Handelsgesetzbuch), löste dieses mit 1.1.2005 ab.

Usability

„Benutzerfreundlichkeit“; die Bedienungsqualität eines Systems aus Sicht eines Benutzers. Hohe Usability zeigt sich in einfach handhabbaren, möglichst intuitiv verständlichen Interaktionsmöglichkeiten.

Verbrauchergeschäft

Gemäß § 1 Abs. 1 KSchG handelt es sich dabei um Rechtsgeschäfte, an denen einerseits jemand beteiligt ist, für den das Geschäft zum Betrieb seines Unternehmens gehört, und andererseits jemand, für den dies nicht zutrifft (der „Verbraucher“). In der Geschäftssprache wird meistens die Bezeichnung „B2C“ („Business to Consumer“) verwendet.

Verkehrstheorie

Die Verkehrstheorie untersucht als Teilgebiet der Nachrichtentechnik das Verhalten von Nachrichtenquellen und deren Wechselwirkung mit den nachrichtentechnischen Anlagen. Diese lassen sich mit Hilfe der Verkehrstheorie so dimensionieren, dass Blockierungen wegen Überlastung ein vertretbares Maß nicht überschreiten. Die festgestellten Gesetzmäßigkeiten gelten in beschränktem Maße auch für den Datenverkehr.

Zessionsverbot

(auch „Abtretungsverbot“) Damit wird einem oder beiden Vertragspartnern vertraglich verboten, Forderungen aus dem Vertrag an einen Dritten zu übertragen. Der häufigste Anwendungsfall ist die Veräußerung von Forderungen an eine „Factorbank“. Dabei wird eine Forderung auf einen Betrag x um den (sofort zahlbaren) Preis y (geringer als x) verkauft. Dies hilft bei Liquiditätsproblemen aus der Klemme, weil man für die Forderung x, auch wenn sie noch nicht fällig ist, schon jetzt zumindest den Betrag y erhält und darüber verfügen kann.

6.0

Hilfsmittel für die Vertrags-verhandlung

Themenübersicht für die Verhandlungsvorbereitung

Download Themenübersicht: http://saas.clusterwien.at/1681145.0

Bevor man in Gespräche mit dem potentiellen Vertragspartner geht, ist es sinnvoll, die eigenen Vorstellungen an Hand der folgenden Punkte zu definieren. Selbst wenn beim gewünschten Service kein Spielraum für die Vertragsgestaltung besteht, kann man so bestehende Risiken durch Vergleich der eigenen Vorstellungen mit den Geschäftsbedingungen besser einschätzen. Und wo mangels genauer Angaben des Anbieters keine Klarheit erzielt wird, sollte man versuchen, mögliche Folgen besonders sorgfältig abzuschätzen.

- ☐ Welche Software (Eigenschaften) ?
- ☐ Wie bereitgestellt (Verfügbarkeit, Messzeitraum)?
- ☐ Wie werden Störungen/Probleme gemeldet und beseitigt?
- ☐ Viren und Malwareschutz (wer und wie und Aktualisierungszeitraum)?
- ☐ Wie sieht die Datensicherung aus?
- ☐ Wie wird der Datenschutz gewährleistet?
- ☐ Welche Voraussetzungen liegen bei mir vor (Welche und wie viele Personen sind für diesen Vertrag vorbereitet worden und dann aktiv involviert? Welche Hardware und welche Software zur Verbindung zum Anbieter stehen bereit? Welche der vorhergehenden und nachstehenden Ansprüche sind bei mir komplementär als Leistungen vorhanden?
- ☐ Wie werden Leistungsänderungen/Upgrades durch mich/durch den Vertragspartner gemeldet und behandelt?

- ☐ Wie sieht die Dokumentation der Software aus und welche ist notwendig auf Grund des Ausbildungsstandes des eigenen Personals?
- ☐ Welche Schulungen sind notwendig und werden wie durchgeführt?
- ☐ Auf welche Dauer ist die Leistung angelegt?
- ☐ Welche Kündigungsfristen sind vorgesehen?
- ☐ Wie sehen die Geheimhaltungsverpflichtungen zeitlich und bezüglich Pönale aus?
- ☐ Ist eine „Nondisclosure Vereinbarung" notwendig?
- ☐ Gibt es besondere Rechte und Pflichten für den Vertragspartner und für mich? (Meldepflichten, Leistungsbereitstellungen, Rechtliche Fragen und Leistungen, betriebliche Leistungen)
- ☐ Wie werden Neuentwicklungen/Updates durchgeführt und in den Betrieb überführt?
- ☐ Wer macht Datenverarbeitungsregistermeldungen und wie? (Erfüllung des österr. DSG2000 und ev. EU-RL 95/46/EG und EU-RL 2002/58/EG)
- ☐ Wie sieht die Gewährleistung aus?
- ☐ Welche Schadenersatzregelungen sind notwendig und durchführbar?
- ☐ Welche Leistungsbefreiungen im Sinne Höherer Gewalt sind vereinbar?
- ☐ Wie werden Streitbeilegungen durchgeführt?
- ☐ Wie wird der Konkursfall des Vertragspartners und die Sicherung der eigenen Interessen behandelt?

Hat man die eigene Erwartungshaltung zu jedem Punkt geklärt, ist man bereit für vorbereitende Vertragsverhandlungen.

Download Themenübersicht: http://saas.clusterwien.at/1681145.0

Checkliste für die Vertragsverhandlung

Download Checkliste: http://saas.clusterwien.at/1681135.0

Diese Checkliste ist für einfachere Fälle von SaaS-Vertragsverhandlungen gedacht. Sollte ihr Umfang nicht ausreichen, steht ein **umfassender Fragenkatalog** unter http://saas.clusterwien.at/1681140.0 zum Download zur Verfügung.

Am sinnvollsten ist es, wenn die Checkliste von beiden Vertragsparteien gemeinsam als Grundlage für die Verhandlungsgespräche herangezogen wird. Da sich diese oft über mehrere Tage erstrecken, sollten die einzelnen, erfolgreich abgeschlossenen Punkte abgehakt und mit Datum versehen werden. In einem wichtigen Begleitprotokoll sind die Ergebnisse zu jedem Punkt schriftlich festzuhalten. Das Begleitprotokoll und die Frageliste werden von beiden Parteien unterzeichnet und dienen als Beweismaterial und Anhang zum SaaS-Vertrag. Dies erhöht die Chancen, die wesentlichen Streitfragen vor Abschluss des Vertrags und seiner Umsetzung zu klären.

Nr.	Bezeichnung	☞ SaaS LF	☑	Datum

Leistung und Entgelt

	1.1 Vertragsgegenstand			
1	Sind die wesentlichen Eigenschaften der einzusetzenden Software/Hardware bekannt (Funktionen, Speicherplatz, Benutzerzahlen, Transaktionsvolumen, Antwortzeitverhalten, usw)?	→ 1.2.1 → 1.2.3 → 1.2.12 → 4.1	☐	
2	Begriffsbestimmungen geklärt und festgeschrieben (Glossar und Abkürzungsverzeichnis)?	→ 1.2.2	☐	
	1.2 Bereitstellung, Betrieb und Betreuung			
3	Wann kann Testbetrieb, wann Echtbetrieb aufgenommen werden?	→ 1.2.3 → 1.2.9	☐	

Nr.	Bezeichnung	☞ SaaS LF	☑	Datum
4	Wie erfolgt die Übernahme bestehender Daten bei Betriebsbeginn (Medien, Formate, Strukturen)?		☐	
5	Sind Betriebszeiten und Anforderungen erfüllbar?	→ 1.2.3	☐	
	1.3 Verfügbarkeit der Gesamtleistung			
6	Welche Verfügbarkeit kann der Anbieter für seine Leistungen und für welchen Messzeitraum zusichern und zu welchen Kosten?	→ 1.2.12 → 3.2 → 3.3	☐	
	1.4 Kundenspezifische Entwicklungen			
7	Welche zukünftigen Ergänzungen/ Erweiterungen sind bereits geplant?	→ 1.2.7 → 1.2.8	☐	
8	Wenn Ergänzungen/Erweiterungen zwingend sind, wie weit ist der Anbieter bereit, dem Kunden ein Kündigungsrecht einzuräumen?	→ 1.2.7 → 1.2.14	☐	
	1.5 Datenschutz und Datensicherung			
9	Wie sieht die Datensicherung aus?	→ 1.2.5	☐	
10	Wie werden der Datenschutz gewährleistet und das Datenschutzgesetz umgesetzt ?	→ 1.2.5 → 1.2.18	☐	
11	Wie sieht der Zugriff auf die Daten-Back-ups aus (auch bzgl. notwendiger Änderungen oder Löschungen, § 27 DSG 2000)?	→ 2.1.4	☐	
	1.6 Systemvoraussetzungen beim Kunden			
12	Welche Systemvoraussetzungen (Hard- u. Software) werden beim Kunden verlangt?	→ 1.2.6	☐	
13	Welche Updatezyklen bei Hard- und bei Software sind absolut notwendig?	→ 1.2.7	☐	
14	Welche Netzwerkvoraussetzungen (Bandbreite, Router, Protokolle, Netzadressen) werden erwartet und sind erfüllbar?	→ 2.1.8	☐	

Nr.	Bezeichnung	☞ SaaS LF	☑	Datum
15	Wer ist für das Netz beim Kunden verantwortlich?	→ 3.3	☐	
	1.7 Schulung und Support			
16	Welche Schulung mit welchen Inhalten und in welchem Umfang (Personen) kann der Anbieter anbieten bzw durchführen?	→ 1.2.11	☐	
17	Welche Voraussetzungen muss das zu schulende Personal mitbringen?	→ 1.2.11	☐	
18	Kosten und Zeitraum der Schulung (pro Person und Modul)?	→ 1.2.11 → 1.2.13	☐	
	1.8 Entgelt und Zahlungsbedingungen			
19	Wie werden die Leistungen des Anbieters abgerechnet (einzeln, pauschal, nach Zeit oder nach Beanspruchung von Komponenten)?	→ 1.2.13	☐	
	1.9 Dauer und Kündigung			
20	Welche Vertragsdauer strebt der Anbieter an (unbefristet, befristet, Kündigungsverzicht einseitig oder zweiseitig)?	→ 1.2.14	☐	
21	Welche Regelungen (Datenübergabe und Löschung usw) sind für das Vertragsende vorgesehen?	→ 1.2.14 → 2.3.1	☐	
22	Wie und in welcher Zeit kann der Anbieter nach Vertragsende die Löschung von Backups verlässlich durchführen und dokumentieren?	→ 1.2.14	☐	
	1.10 Gewährleistung			
23	In wieweit ist der Anbieter bereit, die gesetzliche Gewährleistung für seine Leistungen zu übernehmen (entsprechend §§ 922- 933 und §§ 1096- 1097 ABGB)?	→ 1.2.19	☐	
24	Welche Fristen werden für die Meldungen von Mängeln vereinbart?	→ 1.2.19	☐	

Nr.	Bezeichnung	☞ SaaS LF	☑	Datum
	1.11 Schadenersatz			
25	In wieweit ist der Anbieter und der Kunde bereit auch für leichte Fahrlässigkeit zu haften?	→ 1.2.20	☐	
26	Wie wird der Ausgleich zwischen den Parteien in Bezug auf Schadenersatzforderungen Dritter durchgeführt (Verletzungen der Rechte Dritter durch eine der Vertragsparteien)?	→ 1.2.20	☐	
	1.12 Leistungsbefreiung und Höhere Gewalt			
27	Welche Ereignisse sind als Höhere Gewalt anzusehen und welche sonstigen äußeren Einflüsse sollen in die Leistungsbefreiung aufgenommen werden?	→ 1.2.21	☐	
	1.13 Unternehmensveräußerung			
28	Welche Unternehmen sind derzeit für den Kunden/Anbieter jedenfalls nicht annehmbar, wenn diese den Anbieter/Kunden freundlich oder feindlich übernehmen oder eine Fusion zwischen diesen und dem Anbieter/Kunden bevorsteht oder diese einen wesentlichen Einfluss auf den Anbieter/Kunden ausüben können?	→ 1.2.22	☐	
	1.14 Konkursfall			
29	Welche Vorkehrungen werden getroffen, dass im Konkurs des Anbieters der Kunde Zugriff auf seine Daten hat?	→ 1.4	☐	
30	Ist ein Backup der Daten des Kunden und der vom Anbieter verwendeten Software außerhalb seines Herrschaftsbereiches möglich und zu welchen Kosten?	→ 1.4	☐	

Nr.	Bezeichnung	☞ SaaS LF	☑	Datum
31	Ist eine alternativer Anbieter für den Fall des Konkurses denkbar und kann der Anbieter einen insolvenzrechtlich zulässigen Anbieter benennen?	→ 1.4	☐	
	1.15 Compliance			
32	Unterwirft sich der Anbieter den österreichischen Corporate Governance Regeln?	→ 1.5	☐	
33	Wenn der Kunde die Sarbane Oxley Act (USA, SOX) einhalten muss, ist der Anbieter dann darauf vorbereitet und stimmt zu, dass US-zertifizierte Fachleute seine Leistungen in Hinblick auf Konformität mit dem SOX überprüfen?	→ 1.5	☐	

Datenschutz- und Datensicherheit

	2.1 Technische Sicherheit			
	2.1.1 Redundante Speicherverbünde			
34	Welche Redundanzkonzepte werden angewendet, sind verfügbar?	→ 2.1.1	☐	
	2.1.2 Datenaktualität			
35	Wie oft wird eine Datensicherung angelegt (Zeitabstand/Art)?	→ 2.1.2	☐	
36	Wo befinden sich die Backup Daten und sind diese physisch gesichert?		☐	
	2.1.3 Datenwiederherstellung			
37	Wie erfolgt die Datenwiederherstellung nach einem Schadensfall?	→ 2.1.3	☐	
38	Welche Zeitspanne muss dafür eingeplant werden?	→ 2.1.3	☐	
39	Ist eine Differenzierung nach den Datenbeständen möglich?	→ 2.1.3	☐	

Nr.	Bezeichnung	☞ SaaS LF	☑	Datum
40	Wird die Datenwiederherstellung auch testweise und in welchen Abständen durchgeführt?		☐	
	2.1.4 Schutz vor Schadsoftware			
41	Welche Sicherungen verwendet der Anbieter gegen Schadsoftware und welche sollte der Kunde verwenden?	→ 2.1.7	☐	
42	Wie häufig werden oder sollen diese Schutzprogramme aktualisiert werden?	→ 2.1.7	☐	
	2.2 Organisatorische Sicherheit			
	2.2.1 Schutz vor Zugriff durch nicht berechtigte Personen			
43	Welche Methoden der Passwortsicherheit werden für die Mitarbeiter des Kunden bzw des Anbieters vorgeschlagen?	→ 2.2.1	☐	
44	Erlauben die Datenbanken einen differenzierenden Zugriffsschutz auf Daten und Datensätze sowie auf die verwendeten Programme?	→ 2.2.1	☐	
	2.3 Allgemeines			
	2.3.1 Datenverfügbarkeit bei Nichtverfügbarkeit des Software-Dienstes			
45	Kann der Anbieter eine Exportfunktion bereit stellen, die die Daten des Kunden so zur Verfügung stellt, dass diese auch von anderen Programmen gelesen und verarbeitet werden können?	→ 2.3.1	☐	
46	Müssen diese Programme bereits jetzt konkret angegeben werden?	→ 2.3.1	☐	

Nr.	Bezeichnung	☞ SaaS LF	☑	Datum
47	Wie oft und auf welche Weise kann der Anbieter im Rahmen des rechtlich zulässigen die Daten des Kunden ihm so zur Verfügung stellen, dass auch ein exekutiver Eingriff auf den Anbieter den Kunden nicht am Zugriff auf seine Daten behindert?	→ 2.3.1	☐	
48	Wie kann der Anbieter sicherstellen, dass die von ihm verwendeten Programme dem Kunden im Falle eines exekutiven Zugriffs Anbieter im Rahmen des rechtlich zulässigen zur Nutzung zur Verfügung stehen?	→ 2.3.1	☐	
	2.3.2 Löschung von Daten			
49	Ist die Löschung von einzelnen Daten / gesamten Datensätzen auf Wunsch des Betroffenen und/oder durch gesetzliche Verpflichtungen auch in allen Backups möglich (§ 6 Abs 1 Z 5 DSG 2000)?	→ 2.3.2	☐	
50	Ist die Sperrung von Datensätzen für bestimmte Zeiträume in den Datenbanken möglich (§26 Abs 7 DSG 2000)?	→ 2.3.2	☐	
	2.3.3 Datenschutz			
51	Sind der Anbieter und seine Mitarbeiter mit dem Datenschutzgesetz vertraut?	→ 2.3.3	☐	
52	Haben seine Mitarbeiter entsprechende Belehrungen erhalten und Erklärungen unterschrieben? Sind diese einsehbar?	→ 2.3.3	☐	
53	Sind die dem Kunden bereitgestellten Datenbanken datenschutzrechtlich so gestaltet, dass sie die Anforderungen der §§ 6, 7, 9, 14 und 26 DSG 2000 erfüllen können?	→ 2.3.2 → 2.3.3	☐	
54	Ist der Anbieter bereit, die Datenschutzkommission oder von ihr beauftragte Sachverständige jederzeit in seinen Räumen die gesetzlich vorgesehenen Untersuchungen vornehmen zu lassen?	→ 2.3.3	☐	

Nr.	Bezeichnung	☞ SaaS LF	☑	Datum

Ausfallsicherheit

	3.1 Aufklärung durch den Anbieter			
55	Ist der Anbieter bereit, das Thema Ausfallsicherheit vor Vertragsabschluss im Detail verständlich darzustellen und zu erläutern?	→ 3.1	☐	
	3.2 Vereinbarung der zulässigen Ausfallzeiten			
56	Hat der Kunde seine gewünschten Betriebszeiten bekanntgegeben? Hat er die prozentuellen Verfügbarkeiten für alle Bereiche vollständig definiert?	→ 3.2	☐	
57	Wurden auch die entsprechenden Messzeiträume vorgeschlagen?	→ 3.2	☐	
	3.3 Festlegung der Methode der Feststellung eines Ausfalls			
58	Wurden verschiedene Ausfallszenarien untersucht und konkretisiert?	→ 3.3	☐	
59	Wie werden Ausfälle erkannt?	→ 3.3	☐	
60	Sind die Verantwortungsbereiche dafür geklärt worden?	→ 3.3	☐	
61	Sind die eventuellen externen Dienstleister miterfasst und die Übernahme in die Verantwortung zugeordnet worden?	→ 3.3	☐	
	3.4 Definierte Folgemaßnahmen			
62	Sind die Reaktionen auf eine Störungsmeldung durch den Kunden besprochen und die Messmethoden sowie die Organisationseinheiten für die Behebung durch den Anbieter festgelegt worden? Wie funktioniert die Eskalation?	→ 3.4	☐	

Nr.	Bezeichnung	☞ SaaS LF	☑	Datum
63	Wurden dabei auch die wechselseitigen Pflichten zur Wiederherstellung des vertragsgemäßen Zustandes vereinbart?	→ 3.4	☐	

Download als PDF

Themenübersicht:
http://saas.clusterwien.at/1681145.0

Checkliste:
http://saas.clusterwien.at/1681135.0

Fragenkatalog:
http://saas.clusterwien.at/1681140.0

Gesamter Leitfaden:
http://saas.clusterwien.at/1681130.0

Impressum:
Erstellt durch die Arbeitsgruppe „Rahmenbedingungen für Cloud Computing“ unter der Leitung von Mag. Paul Meinl

Texte:
Ing. Dr. Eike Wolf, Univ.-Prof. Dr. Gunter Ertl und Mag. Paul Meinl

Mitarbeit:
Dipl.-Ing. Helmut Maschek, Peter Ranisch, Dr. Ulrich Schönbaumsfeld, Rüdiger Schultz, Mag. Günter Wildmann

Ermöglicht wurde die Umsetzung durch die intensive Zusammenarbeit des IT-Clusters mit mehreren Partnerunternehmen. Besonderer Dank an die Firma factline Webservices GmbH und an Paul Meinl für die Gruppenleitung. Maßgeblich unterstützt wurde die Arbeit auch von der Österreichischen Computergesellschaft (OCG) und der Arbeitsgemeinschaft für Datenverarbeitung (ADV).

Aus Gründen der Lesbarkeit wurde in diesem Leitfaden nur die männliche Sprachform gewählt. Alle personenbezogenen Aussagen gelten jedoch selbstverständlich stets für Frauen und Männer gleichermaßen. Leider entsprechen die männlichen Bezeichnungen in hohem Maße auch den tatsächlichen Verhältnissen der (österreichischen) IT-Landschaft, wie bedauernswerterweise auch die Zusammensetzung unserer Arbeitsgruppe beweist.

Gestaltung: November Design & PR GmbH, www.november.at
Druck: gugler cross media
April 2012

Ihre Meinung ist uns wichtig. Schreiben Sie uns an itcluster@wirtschaftsagentur.at.
Der IT-Cluster Wien ist ein Angebot der Wirtschaftsagentur Wien.

Besuchen Sie unsere Internetplattform unter:
http://saas.clusterwien.at

Hier finden Sie:

- den gesamten Leitfaden in aktualisierter Fassung,
- Hilfsmittel für Vertragsverhandlungen zum Download,
- weiterführende Informationen und
- die Möglichkeit zum fachlichen Austausch.

IT-Cluster Wien:
www.clusterwien.at/it

Stadt Wien
Wien ist anders.

EUROPÄISCHE UNION
Europäischer Fonds
für regionale Entwicklung
Mit Europa für Wien

eu.Wien.at