EuroCloud AUSTRIA

EuroCloud.Austria

Leitfaden

Cloud Computing
Der gelebte Vertrag – Leistungsstörungen und Vertragshaftung in der Vertragsabwicklung

ÖSTERREICH

06

Der Druck dieses Leitfadens wurde freundlicherweise durch Sponsoren der EuroCloud.Austria finanziert:



























Impressum

EuroCloud.Austria
Verein zur Förderung von Cloud Computing
Museumstraße 5/14
1070 Wien

E-Mail: info@eurocloud.at
Web: http://www.eurocloud.at
Sitz des Vereins: Wien

Copyright: EuroCloud.Austria

Inhaltsverzeichnis

1	Vorwort	4
2	Überblick	5
3	Leistungsstörungen und Haftungsfragen	9
4	Straf- und verwaltungsstrafrechtliche Aspekte	14
5	Anspruchsdurchsetzung und Streitbeilegung	21
6	Checkliste Vertragselemente	29
7	Glossar Cloud Computing	35
8	Rechtlicher Hinweis	37
9	Autoren	39



Dr. Tobias Höllwarth
Vorstandsmitglied der EuroCloud.Austria
Cloud-Gütekriterien und Auditierung

1 Vorwort

Liebe Leserinnen und Leser!

Wer schon einmal einen Vertrag abgeschlossen hat, weiß, dass es trotz größter Sorgfalt bei der Vertragserstellung mitunter zu Situationen kommen kann, mit denen die Vertragsparteien nicht gerechnet haben, oder die für eine der beiden Seiten nicht zufriedenstellend sind. Bei Cloud Verträgen gilt dies umso mehr, da sie oft eine komplexe Dienstleistungsbeziehung regeln sollen, an deren Erbringung womöglich auch mehrere Sublieferanten beteiligt sind.

In solchen Situationen gilt es zu prüfen, ob die Leistung überhaupt noch erbringbar ist, oder ob diese mit Verzug oder mangelhaft erbracht wurde. Schließlich können auch interne oder externe Einflüsse (z.B. ein Hackerangriff) die Leistungserbringung stören. Jedenfalls ist es nötig, haftungsrechtliche Fragen und straf- und verwaltungsstrafrechtliche Aspekte zu klären.

Dieser Leitfaden behandelt Themen wie das Datengeheimnis, Meldepflichten und Datensicherheitsmaßnahmen. Außerdem werden die Möglichkeiten der Anspruchsdurchsetzung, Streitbeilegungsmaßnahmen oder Werkzeuge wie Preisminderung, Zurückbehaltungsrecht und Konventionalstrafen erörtert.

Somit behandelt dieser Leitfaden einen weiteren interessanten Aspekt rund um das Cloud Computing. Sowohl Anbieter wie auch Nutzer von Cloud Leistungen soll die Serie der Euro-Cloud Leitfäden bei der Bewältigung der Herausforderungen rund um Cloud Computing aktiv unterstützen.

Ich danke den Fachleuten Mag. Hackl (Ratiolegis), Dr. Klemm (Brenner & Klemm) und Mag. Peyerl (CHSH) dafür, dass sie diesen Leitfaden erstellt haben.

Wien, Februar 2013

Dr. Tobias Höllwarth
Vorstand EuroCloud.Austria

2 Überblick

2.1 Der Vertrag als Basis jeder Betrachtung

Der Vertrag kann einen Streitfall verhindern, daher sollte er sorgfältig gestaltet werden.

Bei der Vertragserstellung gehen die Vertragsparteien von bestimmten Erwartungen und Vorstellungen, Funktionalitäten und Verantwortlichkeiten aus. Darauf basierend wird der Vertrag erstellt und letztlich umgesetzt. Die Besonderheit bei Cloud Services liegt allerdings in ihren vielfältigen Kombinationsmöglichkeiten und scheinbar unendlichen Kapazitäten. Der Nutzer hat – je nach Bedarf – die Möglichkeit, zwischen verschiedenen Cloud Modellen und Typen zu wählen, wodurch sich auch unterschiedliche Anforderungen an die Vertragsgestaltung ergeben können.

Es sollte abgeklärt werden, ob Sub-Unternehmer eingesetzt werden, um vertragliche Verpflichtungen auch auf diese zu übertragen.

Zunächst ist zu hinterfragen, ob der Anbieter eines Cloud Dienstes der „einzige Vertragspartner" ist oder ob dem Nutzer mehrere Anbieter gegenüberstehen, um die gewünschten Cloud Services beziehen zu können. Ebenso denkbar ist, dass der ausgewählte Cloud Anbieter weitere Sub-Unternehmer zur Vertragsabwicklung heranzieht. Diesfalls ist darauf zu achten, dass auch auf die Sub-Unternehmer die aus dem Vertrag entstehenden Verpflichtungen zu übertragen sind. Da das Heranziehen von Sub-Unternehmern in der Praxis oftmals nicht offengelegt wird, sollte dies vom Nutzer der Cloud Services explizit hinterfragt und vertraglich geregelt werden.

Zumeist finden sich in den Verträgen typische Vertragsinhalte, wie

- Leistungsbeschreibung;
- Liefer- und Zahlungsmodalitäten;
- Gewährleistung und Haftung;
- Beendigungsbestimmungen;
- Rechtswahl/Gerichtsstand.

Im Zusammenhang mit Cloud Services ist zu prüfen, ob weitere Vertragsinhalte aufzunehmen sind. Dies wird primär davon abhängen, ob nur „cloudtypische" Standardservices bezogen werden, ob eine „private" oder „public" Cloud Umgebung gewählt wird oder gar eine komplette Auslagerung von IT-Services erfolgen soll. Wichtig ist auf jeden Fall, dass eine möglichst genaue und umfassende Leistungsbeschreibung ausgearbeitet wird. Dies setzt

voraus, dass sich der Nutzer selbst mit den unternehmensinternen Bedürfnissen (z.B. hohe Verfügbarkeitsstufe der Daten) und technischen Anforderungen (z.B. notwendige Schnittstellen, Datentrennung von anderen Kundendaten), insbesondere auch mit dem Grad der Schutzwürdigkeit (z.B. sensible Daten) der an den Cloud Anbieter überlassenen Daten (z.B. nur Speicherung oder Migration von Daten) auseinandersetzt.

Der Nutzer sollte die Unternehmensbedürfnisse gut kennen, bevor er den Vertrag abschließt.

Dies ist insofern wichtig, als es derzeit weder eine gesetzliche Regelung noch international anerkannte Standards für Cloud Dienste gibt. Im Streitfall ist es jedoch wichtig, den Inhalt der Schuld (die zu erbringende Leistung) genau bestimmen zu können. Dies erfolgt derzeit ausschließlich durch den Vertragsinhalt.

In der Praxis bestehen derzeit verschiedene Möglichkeiten, einen Cloud Vertrag abzuschließen. So bieten manche Anbieter an, einen individuellen Vertrag einschließlich Service Level Agreement abzuschließen, andere dagegen kontrahieren aufgrund der „Standardservices" nur auf Basis der vorgefertigten und meist einseitig zum Vorteil des Anbieters ausgestalteten Allgemeinen Geschäftsbedingungen. Dabei ist auch zu beachten, dass der Vertragspartner häufig das anwendbare Recht und auch den Gerichtsstand vorgibt, sodass der Nutzer im Streitfall oftmals mit ausländischem Recht bzw. mit einem im Ausland begründeten Gerichtsstand konfrontiert ist. Es ist daher im Interesse des Nutzers, bei der Auswahl des Cloud Anbieters dessen Flexibilität und Kompromissbereitschaft bei der Vertragsgestaltung zu hinterfragen.

Im Zusammenhang mit Cloud Services spielen insbesondere auch datenschutz und lizenzrechtliche Fragen eine Rolle (vgl. Leitfaden Cloud Services – Lizenzen im Cloudvertrag, 2012). Es ist daher von Relevanz, ob der Anbieter oder die von ihm beigezogenen Sub-Anbieter über die notwendigen Rechte verfügen, um Cloud Dienste ohne eine Verletzung von Rechten Dritter erbringen zu können bzw. ob der Anbieter möglicherweise Rechte an jenen Ergebnissen erwirbt, die der Kunde mittels der zur Verfügung gestellten Cloud Dienste entwickelt hat. Weiters führt die Verwendung bzw.

Überlassung personenbezogener Daten an den Cloud Anbieter, dem nach Datenschutzrecht definierten Dienstleister, generell zur Anwendung des Datenschutzgesetzes (DSG 2000), sodass die darin geregelten Verpflichtungen einzuhalten sind. So kann insbesondere das Thema Datensicherheit (organisatorische, technische und personelle Maßnahmen zum Schutz der Daten) und deren vertragliche Ausgestaltung eine große Herausforderung darstellen. Der Nutzer sollte daher zumindest Informationen über die geographischen Serverstandorte sowie über die vom Anbieter getroffenen Sicherheitsmaßnahmen einholen.

Der Nutzer hat regelmäßig zu prüfen, ob der Anbieter die Vereinbarungen einhält.

Es ist jedenfalls unabdingbar, dass der Cloud Nutzer über Datentransfers ins Ausland bzw. den Einsatz von Sub-Unternehmern informiert wird. Der Cloud Nutzer hat auf Basis aller Details zu entscheiden, ob die angebotene Dienstleistung in tatsächlicher und auch rechtlicher Sicht zum Unternehmen „passt". Insofern ist es für den Cloud Nutzer auch von großer Relevanz, ob der Anbieter auch allenfalls beim Nutzer bestehende branchenspezifische Besonderheiten einhalten kann. So kann die Vereinbarung von besonderen Geheimhaltungs- oder Meldepflichten für den Nutzer von Wichtigkeit sein (z.B. Einhaltung des Bankgeheimnisses oder Meldepflicht bei Datenmissbrauch). Wesentlich ist daher auch die Vereinbarung von Kontrollrechten des Nutzers, um feststellen zu können, ob sich der Cloud Anbieter an die vereinbarten Vertragsinhalte hält. Dem Nutzer sollte bewusst sein, dass durch die Virtualisierung und Dezentralisierung von Ressourcen – oftmals über die Grenzen hinweg – ein natürlicher Kontrollverlust eintritt und konkrete Überprüfungsmaßnahmen (z.B. externer Audit) mangels einer gesetzlichen Regelung derzeit noch eine vertragliche Regelung benötigen.

2.2 Was Sie in diesem Leitfaden erwartet

Bei allen Vorfällen ist daher wichtig, dass die „Störungen" – seien sie organisatorisch oder technisch bedingt – schnellstmöglich behoben werden. Dabei kann der Vertrag hilfreich sein, manchmal allerdings auch nur das rasche Tätigwerden, um Schaden zu verhindern oder zu minimieren. Primär

sollte daher versucht werden, dass sich die Vertragsparteien – je nach Vorfall – einvernehmlich über das weitere Vorgehen einigen. Sollte eine Einigung nicht erzielt werden können, ist es manchmal erforderlich, den Rechtsweg einzuschlagen, um weiteren Schaden zu verhindern oder eine bestimmte Handlung des Vertragspartners zu erzwingen.

Der Leitfaden soll Ihnen einen Kurzüberblick über die wichtigsten „Vertragsstörungen“ und „Haftungstatbestände“ geben und Ihnen die rechtlichen Lösungswege aufzeigen.

3 Leistungsstörungen und Haftungsfragen

3.1 Leistungsstörungen in der Vertragsabwicklung

Eine „Leistungsstörung" ist eine Abweichung vom Vereinbarten und sollte primär zwischen den Vertragsparteien gelöst werden.

Nach dem Abschluss des „Cloud Service Vertrags" beginnt die Phase der Vertragserfüllung. Es ist daher zu prüfen, ob Zeit, Ort und Inhalt der vereinbarten Leistung vertragsgemäß erfüllt werden. Während Zeit und Ort bei Cloud Services meist eine untergeordnete Rolle spielen, weil der Bezug der Services rasch und unproblematisch, oftmals per Mausklick über das Internet erfolgt, ist der Inhalt und insbesondere das reibungslose Funktionieren der Services nicht nur von faktischer, sondern auch von rechtlicher Relevanz.

Sogenannte „Leistungsstörungen" sind Störungen bei der Erfüllung des Vertrages. Es treten daher während der Vertragsabwicklung Hindernisse auf, die unvorhergesehen oder auch von einem Vertragspartner verursacht sein können.

Aus juristischer Sicht stellt sich daher immer die zentrale Frage: Was wurde im Vertrag für ein bestimmtes Ereignis vereinbart? Sofern sich im Vertrag eine Regelung für den konkreten Fall findet, so sind die Vertragsparteien jedenfalls angehalten, sich vertragsgemäß zu verhalten. Aber bereits aus der allgemeinen Fürsorgepflicht ergibt sich, dass der Vertragspartner über ein ungeplantes Ereignis ehestmöglich zu informieren und der Schaden weitestgehend zu minimieren ist.

Findet sich im Vertrag allerdings keine Regelung, kann es auch sein, dass das Gesetz eine Regelung für den konkreten Fall vorsieht. Oftmals kommt es jedoch – gerade im IT-Bereich – zu unvorhergesehenen Zwischenfällen, sodass es weder eine gesetzliche noch eine vertragliche Regelung dafür gibt.

Die Ereignisse, die sich während der Vertragserfüllung ereignen können, sind vielfältig, weshalb im Folgenden nur eine beispielhafte Aufzählung erfolgt:

» Die **Unmöglichkeit** der Leistung besteht in einem dauerhaften Hindernis der Leistungserbringung, sodass der Vertrag zumeist gar nicht in ein Abwicklungsstadium kommt. Dass eine Leistung endgültig unmöglich wird, könnte z.B. durch die Abhängigkeit von Dritten entstehen, die der Anbieter zur Leistungserbringung heranzieht (z.B. beim Anbieten von SaaS-Lösungen, wobei der Lizenzge-

ber ein Sub-Unternehmer ist, der die Software nicht vereinbarungsgemäß zur Verfügung stellt, weil er selbst nicht Rechteinhaber ist). Sofern die Erbringung der Leistung erst nachträglich (endgültig) unmöglich wird, führt dies in der Praxis zumeist zur Rückabwicklung des Vertrages.

» Vom **Verzug** spricht man, wenn die vereinbarte Leistung nicht zum Zeitpunkt der Fälligkeit erbracht wird. Im Verzugsfall kann der Cloud Nutzer auf die Vertragserfüllung bestehen oder unter Fristsetzung vom Vertrag zurücktreten. Ist der Verzug vom Cloud Anbieter verschuldet, so kann dies zusätzlich zu einem Schadenersatzanspruch des Nutzers führen.

» Die **mangelhafte Leistung** bedeutet, dass die Leistung nicht die gewöhnlich vorausgesetzten oder vereinbarten Eigenschaften aufweist (z.B. Qualität der Leistung, mangelnde System- oder Datenverfügbarkeit). Das Gesetz sieht bestimmte Regeln für den Gewährleistungsfall vor, wobei diese in einem bestimmten Rahmen auch vertraglich abgeändert werden können. Ob eine Leistung mangelhaft ist und der Anbieter dafür einzustehen hat, wird jedoch primär nach der vertraglichen Vereinbarung zu beurteilen sein, weshalb bei Cloud Diensten die Leistungsbeschreibung von großer Bedeutung ist (z.B. Wurde die Durchführung eines Back-ups vereinbart? Sind Patches/Updates einzuspielen?). Mangelhaftigkeit kann sich auch durch die mangelnde Datenseparation zu anderen Kundendaten des Anbieters ergeben, wodurch es zu einer unzulässigen Vermengung oder gar Veröffentlichung von Unternehmensdaten kommen kann.

  Ebenso kann es durch mangelhafte oder fehlende Datensicherheitsmaßnahmen zu externen (z.B. Hacker) oder internen (z.B. Mitarbeiter) Angriffen kommen, welche zu einem Datenverlust und/oder einer Datenveröffentlichung führen und so dem Cloud Nutzer einen großen Schaden verursachen können. Auch hinsichtlich eingesetzter Software kann es zu einem Rechtsmangel kommen, wenn die in der Cloud eingesetzte Software nicht oder nicht ausreichend lizenziert ist und der Nutzer vom Rechteinhaber in Anspruch genommen wird. In der Praxis finden sich daher häufig Haftungsausschlüsse und -beschränkungen, die – sofern rechtlich zulässig – für

den Nutzer sehr nachteilig sein können, weshalb dieser Punkt bereits bei der Vertragserstellung besondere Beachtung finden sollte.

» Weiters können auch Leistungsstörungen auftreten, die von keiner der Vertragsparteien verschuldet sind. Dabei ist an die sog. **„Höhere Gewalt“** zu denken. Dies bedeutet, dass ein unabwendbares Ereignis wie z.B. Naturkatastrophen jeder Art, Krieg, Unruhen oder Streiks eintritt, sofern dieses bei einem Dritten – also nicht bei den beiden Vertragsparteien – stattfindet.

  Fraglich ist jedoch, ob die Rechtsprechung derartige Ereignisse auch in Zukunft als von den Parteien „unverschuldet“ ansehen wird, wenn die Vertragspartner bewusst ihre Leistungen aus Ländern beziehen, die als politisch unsicher gelten (z.B. Stromausfälle oder Leistungsausfälle durch Streiks oder Unruhen, Datenverlust bei behördlicher Serverbeschlagnahme ohne Rechtsgrund). Beim Bezug von Cloud Services ist daher zu bedenken, dass ein gänzlicher Stillstand in der Vertragsabwicklung fatale Folgen für die Geschäftsprozesse des Cloud Nutzers haben kann.

3.2 Haftungsrechtliche Fragen

Neben den oben beschriebenen Leistungsstörungen kann das Verhalten eines Vertragspartners bei Vorliegen bestimmter Voraussetzungen auch zu einem Anspruch auf Schadenersatz führen. Dabei ist zwischen der vertraglichen und der deliktischen Haftung zu unterscheiden, wobei bei Cloud Diensten die Haftung durch die Verletzung von vertraglichen Pflichten im Vordergrund steht. Eine Schadenersatzpflicht besteht jedoch nur dann, wenn eine Handlung derart gesetzt wird, dass der daraus entstehende Schaden in rechtswidriger und schuldhafter Weise verursacht wurde. Dabei ist zunächst zu prüfen, ob sich der Schaden aus der Verletzung gesetzlicher oder vertraglich begründeter Verpflichtungen, wie sog. Schutz-, Sorgfalts- und Aufklärungspflichten ergibt (= Rechtswidrigkeit).

Weiters stellt sich die Frage, in welchem Maß der Vertragspartner diese Sorgfaltsverletzung gesetzt hat. Dabei kann er vorsätzlich oder (grob oder leicht) fahrlässig gehandelt haben, sodass sich der Umfang der Haftung auch nach dem Verschuldensgrad der Verletzung richtet. So kann es z.B. dann zu einer Haftung des Anbieters kommen, wenn ein Handeln die

Vertraulichkeit, die Integrität oder die Verfügbarkeit der ihm überlassenen Daten gefährdet bzw. verletzt. Ebenso hat der Anbieter zu haften, wenn die Datensicherheitsmaßnahmen nicht vereinbarungsgemäß erfüllt wurden (z.B. unangemessene oder nicht dem Stand der Technik entsprechende Schutzmaßnahmen, kein oder mangelhaftes Risiko- und/oder Notfallmanagement) und dadurch dem Nutzer ein Schaden entsteht. Gleichfalls, wenn die Datenverfügbarkeit nicht wie vereinbart geliefert wird und der Nutzer daher nicht – wie erforderlich – seine Geschäftsprozesse durchführen kann (z.B. Transaktionsdaten bei Banken, die ständig aktuell verfügbar sein müssen). Sofern ein Service Level Agreement vereinbart wurde, sind darin meist „Sanktionen" geregelt, der Totalausfall eines Systems, welcher durch den Anbieter verursacht wurde, führt jedoch zumeist zu einer davon unabhängigen Schadenersatzpflicht.

Im Zusammenhang mit Cloud Diensten ist zu beachten, dass der Cloud Anbieter auch für seine „Erfüllungsgehilfen" haftet

Im Zusammenhang mit Cloud Diensten ist zu beachten, dass der Cloud Anbieter auch für seine „Erfüllungsgehilfen" haftet, sodass ihm nicht nur seine eigenen Mitarbeiter, sondern auch die von ihm eingesetzten Sub-Unternehmer direkt zugerechnet werden. Der Nutzer sollte daher besonders darauf achten, dass der Anbieter die sich aus dem Vertrag ergebenden Verpflichtungen auf seine Sub-Anbieter überträgt. Gleichzeitig sollte sich auch der Anbieter gegenüber seinen Sub-Anbietern entsprechend vertraglich absichern. Dazu gehört nicht nur eine Haftungseinschränkung bei Verletzung der festgelegten Sorgfaltspflichten, sondern es sollte bereits im Vorfeld eine klare Regelung der Verantwortungsbereiche erfolgen.

Aber auch der Nutzer hat sich über eine mögliche Haftung Gedanken zu machen. Diese kann dann zum Tragen kommen, wenn er bei der Auswahl des Cloud Anbieters nicht sorgfältig agiert. Das Unternehmensgesetzbuch (§ 347 UGB) sieht diesbezüglich vor, dass Organwalter, wie z.B. Vorstandsmitglieder, Mitglieder des Aufsichtsrates und Geschäftsführer, für die Sorgfalt eines ordentlichen Unternehmers einzustehen haben.

Eine Konkretisierung dieser Sorgfaltspflicht findet sich insbesondere im GmbH-Gesetz sowie im Aktien-Gesetz, wonach der Vorstand bzw. der Geschäftsführer dafür zu sorgen haben, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen. Aus diesen Organisationsanforderungen lässt sich schließen, dass Maßnahmen zur Früherkennung von für das Unternehmen

maßgeblichen Entwicklungen zu treffen sind sowie ein Überwachungssystem und ein allgemeines Risikomanagement vorhanden sein müssen.

Dabei handelt es sich um Kernfunktionen der IT. Umso mehr haben die Organwalter diesen Sorgfaltsmaßstab bei der Auslagerung von Daten, Systemen und Geschäftsprozessen an einen Dritten zu beachten. Diese Pflicht normiert insbesondere auch das Datenschutzgesetz (§ 10 DSG). Bei mangelnder Prüfung und Kontrolle des Anbieters kann es daher – im Ernstfall – zu einer Mitschuld des Nutzers kommen, weil dieser selbst die notwendige Sorgfalt bei der Auswahl und Kontrolle des Anbieters außer Acht gelassen hat.

4 Straf- und verwaltungsstrafrechtliche Aspekte

Zunehmende Bedeutung des Datenschutzes

Die zunehmende Bedeutung des Datenschutzes sowohl im österreichischen als auch im europäischen Rechtsraum spiegelt sich nicht zuletzt in der Tatsache wider, dass die nationalen Gesetzgeber den Verstoß gegen datenschutzrechtliche Bestimmungen auch unter Strafe stellen. Auch wenn die Zahl der Verurteilungen bzw. der Verhängung von Verwaltungsstrafen äußerst gering ist, stellen deren Regelungen eine entsprechende Wertung des Gesetzgebers dar.

Unabhängig von der grundsätzlichen Strafbarkeit von vorsätzlichen Handlungen gegen das Datengeheimnis (wie z.B. Hacking-Angriffe), deren Strafbarkeit durch die entsprechenden Regelungen im österreichischen Strafgesetzbuch (StGB) sichergestellt ist, sieht insbesondere das Datenschutzgesetz Strafen bei Verstößen gegen datenschutzrechtliche Bestimmungen vor. Darunter fallen die Nichteinhaltung von Meldepflichten bzw. die Nichteinholung von erforderlichen Genehmigungen sowie auch Verstöße gegen Betroffenenrechte, wie Offenlegungs-, Auskunfts-, Richtigstellungs- und Löschungsverpflichtungen. Weiters sieht das Datenschutzgesetz ausdrücklich auch Verwaltungsstrafen bei Nichteinhaltung der vorgeschriebenen Datensicherheitsmaßnahmen vor.

Datenschutzrechtliche Bestimmungen treffen grundsätzlich sowohl den Cloud Nutzer als datenschutzrechtlichen Auftraggeber als auch den Anbieter als sog. Dienstleister, sodass die entsprechenden strafrechtlichen Bestimmungen beide Seiten betreffen und die Einhaltung der entsprechenden Regelungen auch von beiden Parteien sichergestellt werden muss.

4.1 Vorsätzliche Handlungen gegen das Datengeheimnis

Gemäß § 51 DSG ist die Verwendung von Daten in Gewinn- oder Schädigungsabsicht mit Freiheitsstrafe von bis zu einem Jahr bedroht. Die praktische Relevanz dieser Bestimmung für Cloud Verträge ist eher beschränkt, da bei Auswahl eines seriösen Cloud Anbieters in der Regel davon auszugehen ist, dass dieser nicht in krimineller Absicht Daten veruntreut oder missbraucht.

Hervorzuheben ist jedoch, dass die Verpflichtung zur Geheimhaltung bzw. der Einhaltung des Datengeheimnisses gemäß § 15 DSG grundsätzlich Auftraggeber, Dienstleister und auch deren Mitarbeiter (sohin sämtliche Arbeitnehmer oder sonstige arbeitnehmerähnliche Personen) trifft und de-

ren Verstoß daher grundsätzlich auch gegenüber jeder dieser Personen zu ahnden ist. Generell kann gesagt werden, dass jede von einem Vertragspartner gesetzte bzw. diesem zuzurechnende vorsätzliche Handlung zu einem Vertragsbruch führt und somit zu einer außerordentlichen Kündigung berechtigen kann.

Bei mangelhafter Überwachung oder Sicherheitsmaßnahmen mitunter Mithaftung von Dienstleister oder Auftraggeber

Häufigere Anwendungsfälle für diese Bestimmungen sind hier eher Mitarbeiter von Auftraggebern oder Dienstleistern, die rechtswidrig bzw. in entsprechender Schädigungsabsicht nach deren Kündigung Daten rechtswidrig weitergeben oder zerstören. Trifft den Dienstleister oder Auftraggeber aufgrund mangelhafter Sicherheitsvorkehrungen oder Aufsicht eine Mitschuld, kann dies sowohl vertragliche als auch verwaltungsstrafrechtliche Konsequenzen nach sich ziehen.

4.2 Verwaltungsstrafrechtliche Bestimmungen

Ebenfalls von Bedeutung sind in diesem Zusammenhang die verwaltungsstrafrechtlichen Bestimmungen des Datenschutzgesetzes, welche insbesondere nach der letzten Novelle bereits eine breite Palette von Tatbeständen sowohl für Auftraggeber als auch Dienstleister vorsehen. Auch hier finden sich Strafbestimmungen hinsichtlich vorsätzlicher Handlungen gegen das Datengeheimnis bzw. vorsätzlicher Verstöße gegen die diesbezüglichen Bestimmungen. Diese können im Rahmen der Abwicklung von Dienstleistungsverträgen bei mangelhafter Überwachung der Mitarbeiter bzw. bei Verstößen gegen bestimmte Fürsorgepflichten von Bedeutung sein.

Ebenfalls von praktischer Relevanz sind die Verwaltungsstrafbestimmungen hinsichtlich der Verletzung der Meldepflichten, Genehmigungspflichten, Sicherheitsmaßnahmen und Betroffenenrechte (grundsätzlich in § 52 Abs 2 DSG geregelt). Der für die Praxis dabei wohl bedeutsamste Fall ist der Verstoß gegen die mittlerweile umfangreichen Meldepflichten von Auftraggebern hinsichtlich der von ihnen betriebenen Datenanwendungen.

Auch wenn der Verstoß gegen Verwaltungsstrafbestimmungen nicht per se einen Vertragsbruch darstellt, haben diese sehr wohl einen Einfluss auf den gelebten Vertrag. Ein Dienstleister, der gegen Verwaltungsstrafbestimmungen verstößt, kann kaum noch als vertrauensvoller Vertragspartner betrachtet werden, was eine außerordentliche Kündigung des Cloud Vertrags rechtfertigt. Ebenfalls von Bedeutung ist in diesem Zusammenhang aber

auch die entsprechende Verteilung der Verantwortlichkeit der Vertragsparteien. Auch wenn ein Verstoß durch einen Dienstleister erfolgt, kann sich der Auftraggeber mitschuldig machen, wenn er diesen nicht entsprechend überwacht bzw. sich nicht durch entsprechende Regelungen im Dienstleistervertrag abgesichert hat.

4.3 Verstoß gegen Meldepflichten

Informations- und Warnpflichten für Dienstleister

Wie bereits erwähnt stellen die Bestimmungen hinsichtlich der Verletzung von Meldepflichten bzw. der unterlassenen Einholung von erforderlichen Genehmigungen zur Verarbeitung oder Übermittlung von Daten den in der Praxis wohl bedeutsamsten Fall dar. Viele Verstöße werden hier nicht bewusst, sondern schlicht aus Unkenntnis erfolgen. Für den Dienstleister sind diese Verpflichtungen grundsätzlich von nachgeordneter Bedeutung, da die Einholung der notwendigen Genehmigungen bzw. die Vornahme der behördlichen Registrierungen grundsätzlich den Auftraggeber treffen. Aufgrund der sich aus dem Vertrag ergebenden Fürsorgepflichten und der Tatsache, dass der Dienstleister in der Regel wohl auch über bessere Kenntnisse hinsichtlich der Systemfunktionalitäten oder der Datenspeicherung verfügt, können sich jedoch auch für den Dienstleister zumindest entsprechende Informations- und Warnpflichten ergeben.

Jedenfalls ist der Dienstleister zur Kooperation bei der Beschaffung notwendiger Informationen verpflichtet. Grundsätzlich wird sich dieser jedoch darauf verlassen dürfen, dass die Verarbeitung von Daten, die er von seinem Auftraggeber mit den entsprechenden Weisungen erhält, rechtmäßig erfolgt. Aus Sicht des Dienstleisters ist es hier freilich ratsam, eine entsprechende vertragliche Zusicherung durch den Auftraggeber vorzusehen, dass Letzterer zur Verarbeitung der betroffenen Daten berechtigt ist und die dafür notwendigen behördlichen Genehmigungen einholen wird.

Ein besonderes Problem bei Cloud Verträgen ist dabei natürlich die häufig bestehende Intransparenz auf beiden Seiten. Da weder dem Auftraggeber noch dem Dienstleister vollständig bekannt sein wird, wie die entsprechenden Daten erhoben wurden und wie diese in der Folge genutzt und verarbeitet werden, verfügt die jeweils andere Seite häufig nicht über ausreichende Informationen, um allfällige Verstöße überhaupt erkennen zu können. Auch für dieses Problem empfehlen sich umfassende vertragliche Regelungen, um einen entsprechenden Informationsfluss sicherzustellen bzw. notwendige Aufsichtsrechte zu erhalten.

4.4 Verstoß gegen Betroffenenrechte

Als Betroffene gelten nach dem Datenschutzgesetz grundsätzlich alle Personen, deren Daten gespeichert oder verarbeitet werden. Verstöße gegen Betroffenenrechte, nämlich die nicht fristgerechte Beauskunftung, Richtigstellung oder Löschung von Daten, stellen ebenfalls eine Verwaltungsübertretung dar. Diese können gemäß § 52 Abs 2a DSG zwar nur mit einer Geldstrafe von bis zu EUR 500,-- geahndet werden, werden jedoch in der Regel für den Vertrag von Relevanz sein, da eine Verwaltungsübertretung letztlich auch eine entsprechende Vertragsverletzung darstellen wird.

Deshalb sind auch hier die Vertragsparteien dazu angehalten, im Vertrag eine ausreichende Wahrnehmung der Betroffenenrechte vorzusehen und sicherzustellen. Diese kann in einer simplen Verpflichtung des Dienstleisters zur Weiterleitung allfälliger Anfragen und Anträge von Betroffenen an den Auftraggeber bis hin zur vollständigen Wahrnehmung dieser Aufgaben für den Auftraggeber bestehen.

Vertragliche Regelung für den Umgang mit Anfragen von Betroffenen von essentieller Bedeutung

Auch im Sinne des Dienstleisters ist es von hoher Bedeutung, vertraglich festzuhalten, wer für Anfragen und in welcher Form zuständig ist. Aufgrund der strengen Weisungsgebundenheit des Dienstleisters gemäß § 11 DSG dürfte der Dienstleister grundsätzlich ohne entsprechenden Auftrag bzw. Ermächtigung durch den Auftraggeber Anfragen von Betroffenen weder beantworten noch sonst bearbeiten. Vom Gesetz her ist der Dienstleister nur dazu verpflichtet, die technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunftsverpflichtungen – sofern möglich – zu schaffen, nicht jedoch diesen auch zu entsprechen. Durch ausreichende vertragliche Regelungen kann sichergestellt werden, wie der Dienstleister Anfragen von Betroffenen behandeln muss, ohne fürchten zu müssen, gegen den Cloud Vertrag zu verstoßen (Pflichtenkollision).

Eine allfällige Verantwortlichkeit für Verwaltungsübertretungen richtet sich freilich nach dem Verhalten beider Parteien. Unabhängig von der vertraglichen Regelung, wer für Anfragen zuständig ist, ist der Auftraggeber nach wie vor verpflichtet, deren Einhaltung durch den Dienstleister zu überwachen.

4.5 Außerachtlassung von Datensicherheitsmaßnahmen

§ 14 DSG enthält einen umfassenden Katalog an Datensicherheitsmaßnahmen, deren Einhaltung sowohl für Auftraggeber als auch Dienstleister verpflichtend ist. Die gröbliche Außerachtlassung der genannten Sicherheitsmaßnahmen stellt eine Verwaltungsübertretung dar, die mit Geldstrafen von bis zu EUR 10.000,-- zu ahnden ist.

Da der Gesetzgeber in § 14 DSG nur einen Mindestkatalog an Sicherheitsmaßnahmen normieren, ohne jedoch spezifische technische Anweisungen zu enthalten, sieht das Datenschutzgesetz darüber hinaus ausdrücklich vor, dass der Auftraggeber mit dem Dienstleister vertragliche Regelungen hinsichtlich der Ausgestaltung der vereinbarten Sicherheitsmaßnahmen zu treffen hat, um die Einhaltung dieser zu gewährleisten.

Vereinbarung von zu treffenden Sicherheitsmaßnahmen und Aufsichtsrechten im Vertrag

Weiters hat sich der Auftraggeber von den beim Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen. Daher sollten die vertraglichen Regelungen auch entsprechende Aufsichtsrechte und Berichtspflichten für den Dienstleister vorsehen. Nur so kann sich der Auftraggeber auch hinsichtlich allfälliger Verstöße absichern. Denn der Auftraggeber kann sich nicht bloß auf die gesetzliche Verpflichtung für den Dienstleister verlassen. Kümmert er sich nicht um eine entsprechende Überwachung des Dienstleisters, ist er für allfällige Verstöße ebenfalls haftbar.

Das Ausmaß dieser Aufsichtspflichten ist freilich auch von der Sensibilität der verarbeiteten Daten abhängig. Werden sensible Daten verarbeitet, sind die Ansprüche an die Auswahl und das Monitoring des entsprechenden Dienstleisters erheblich höher als beispielsweise bei der Verarbeitung von Daten für die Personalverrechnung durch einen spezialisierten Anbieter. Die vertraglichen Verpflichtungen an den Dienstleister sollten jedoch in der Regel – auch im Interesse des Auftraggebers – strenger und deutlicher ausgestaltet werden, als dies durch das Gesetz vorgeschrieben ist. Mit anderen Worten sollte ein Verstoß gegen Datensicherheitsmaßnahmen, der bereits als „gröblich", wie vom Gesetz gefordert, zu beurteilen ist, schon längst gegen die vertraglichen Sorgfaltspflichten des Dienstleisters verstoßen.

4.6 Data Breach Notification Duty

Unabhängig von einem allfälligen Verschulden des Auftraggebers oder Dienstleisters an einem Datenleck ist in diesem Zusammenhang jedenfalls

die durch die letzte Novelle des DSG eingeführte „Data Breach Notification Duty“ des § 24 Abs 2a DSG zu beachten. Diese verpflichtet den Auftraggeber, im Falle von Datenmissbrauch bzw. Fällen, in denen mit dem Missbrauch von gestohlenen oder sonst rechtswidrig verschafften Daten zu rechnen ist, die Betroffenen in geeigneter Weise zu informieren.

Vorsehung von Meldepflichten für den Dienstleister

Da die Meldepflicht laut dem Wortlaut des Gesetzes den Auftraggeber trifft, ist es hier in jedem Fall von besonderer Bedeutung, allfälligen Dienstleistern eine vergleichbare Berichtspflicht an den Auftraggeber aufzuerlegen. Ohne diese kann es unter Umständen nämlich so sein, dass der Auftraggeber, obwohl Adressat der Berichtspflicht, von einem allfälligen Verstoß gar nichts erfährt, weil ihn der Dienstleister nicht darüber informiert.

Mit der Vorsehung einer entsprechenden Meldepflicht sichert sich der Auftraggeber gegen dieses Informationsdefizit ab und kann sich auch im Falle eines Verstoßes am Dienstleister regressieren.

4.7 AUSBLICK: Änderungen der Strafbestimmungen durch die EU-Datenschutzverordnung

Dass die Bedeutung der strafrechtlichen Bestimmungen bzw. die Verantwortlichkeit von Auftraggebern und Dienstleistern zunehmen wird, ergibt sich nicht zuletzt auch aus dem derzeit vorliegenden Entwurf der Datenschutzverordnung der Europäischen Kommission (KOM 2010/609 endg.). Als Folge des in vielen Ländern festgestellten Trends der Außerachtlassung von datenschutzrechtlichen Bestimmungen aufgrund der teilweise vernachlässigbaren Höchststrafen (so sieht das österreichische Datenschutzgesetz derzeit eine Höchststrafe von lediglich EUR 25.000,-- vor) ist es offensichtlich die Absicht des europäischen Gesetzgebers, diesen Zuständen einen Riegel vorzuschieben.

Verschärfung der Straf- und Haftungsbestimmungen durch neue EU-Datenschutzverordnung

Der derzeitige Entwurf sieht nunmehr eine Höchststrafe von einer Million Euro bzw. bei internationalen Unternehmen 2 % des konzernweiten Umsatzes bei rechtswidriger Verarbeitung von personenbezogenen Daten vor. 0,5 % bei nicht rechtzeitiger Beauskunftung und 1 % des konzernweiten Umsatzes können bei nicht rechtzeitiger Datenlöschung verhängt werden. Sollten diese Werte tatsächlich auch Einzug in die letztlich zu erlassende Verordnung finden (wonach es derzeit aussieht), kann es sich kein in Europa tätiges Unternehmen mehr leisten, die Bestimmungen des Datenschutzes zu ignorieren.

Von essentieller Bedeutung für Verträge über Cloud Dienstleistungen ist darüber hinaus die derzeit ebenfalls vorgesehene Einführung einer Solidarhaftung von Auftraggebern und Dienstleistern. Künftig könnten dann – unabhängig vom tatsächlichen Verschulden – sowohl Auftraggeber als auch Dienstleister für jegliche Verstöße in Anspruch genommen werden. Auch für diese Fälle empfiehlt sich jedenfalls eine entsprechende vertragliche Regelung.

5 Anspruchsdurchsetzung und Streitbeilegung

Die oberste Prämisse im Falle eines Konfliktes ist eine schnelle und kostengünstige Streitbeilegung, ohne viel Porzellan zu zerbrechen oder eine Fortsetzung der Vertragsbeziehung zu gefährden.

Selbst größte Empathie, die subtilste Auseinandersetzung mit dem Standpunkt der Gegenseite und aufopfernde Kompromissbereitschaft führen aber nicht immer zum gewünschten Ziel, nämlich einer Einigung im Interesse beider Vertragsparteien.

Vorrang für Kompromisse, Gerichtsverfahren nur im Ausnahmefall

In diesem Fall sollte die Härte der eingesetzten (oder zumindest angedrohten) Sanktionen konsequent zunehmen. Die gerichtliche Auseinandersetzung, die in den meisten Fällen ein unwiederbringliches Scheitern der Vertragsbeziehung zur Folge hat, sollte ultima ratio sein!

Wie kann also einer der oben dargestellten Konflikte gelöst werden, ohne eine Katastrophe auszulösen?

5.1 Klare Vertragssprache

Der erste und wichtigste Schritt sollte schon im Vorfeld bei der Vertragsgestaltung gesetzt worden sein. Die meisten Konflikte entstehen durch unklare oder fehlende Regelungen einer potentiellen Streitfrage. Ein guter Vertrag sollte zum einen den Spielraum für Auffassungsunterschiede auf ein Minimum reduzieren. Zum anderen sollte er einen Streitbeilegungsmechanismus vorsehen, falls es dennoch zum Konflikt kommt.

5.2 Vertragliche Streitbeilegungsinstrumente

Idealerweise sieht der Vertrag vor, was im Konfliktfall zu tun ist. Ist das nicht der Fall, gilt die gesetzliche Regelung. Gerade bei Cloud Services ist das anwendbare Recht nicht immer eindeutig. Und falls es das ist, kann es unbekannt oder nachteilig sein. Daher kommt der vertraglichen Vorsorge umso größere Bedeutung zu.

Streitbeilegung im Vertrag geregelt

In Frage kommen bereits im Vertrag vorgesehene Zurückbehaltungsansprüche, Leistungsverweigerungsrechte, das Recht auf Preisminderung, auf Ersatzvornahme, Bucheinsicht, Konventionalstrafen, pauschalierter Schadenersatz, Beweislastumkehr und als letztes Mittel der Rücktritt vom Vertrag samt Rückabwicklungsanspruch.

5.3 Preisminderung

Vertragliche Sanktionen

Die Preisminderung ist ein Gewährleistungsbehelf. Sie ist an sich ein wirksames Mittel zur Durchsetzung der Gegenleistung. Allerdings nur, solange der Preis noch nicht zur Gänze bezahlt wurde. Zielsetzung sollte es sein, den Vertragspartner durch die Einbehaltung eines Entgeltteiles zum Einlenken zu bewegen. Dieses Vorhaben wird scheitern, wenn die Höhe des einbehaltenen Betrages außer Verhältnis zur aufgetretenen Leistungsstörung steht. Aufgrund der meist relativ geringen Gegenleistung (nutzungsabhängiges Entgelt) ist dieser Behelf bei Cloud Services wahrscheinlich mäßig relevant.

5.4 Zurückbehaltungsrecht

Verhältnismäßigkeit gegeben?

Gleiches wie für die Preisminderung gilt für die Zurückbehaltung (Retention). Die Retention des an sich geschuldeten Preises ist ein sehr effektives Mittel, den Vertragspartner „zur Vernunft zu bringen". Sie basiert – wie ein Gewährleistungsanspruch – auf der Einrede des nicht (gehörig) erfüllten Vertrages. Die Zulässigkeit dieses Schrittes hängt von seiner Verhältnismäßigkeit ab. Um eine Eskalation zu vermeiden, kann es sich empfehlen, den zurückbehaltenen Betrag gerichtlich oder bei einem Treuhänder zu hinterlegen, bis der Konflikt bereinigt ist. Ist die Zurückbehaltung vertraglich nicht vorgesehen, so riskiert man damit einen gravierenden Vertragsverstoß, was die Deeskalation des bestehenden Konfliktes nicht erleichtern wird.

5.5 Konventionalstrafe

Risiken erfassen und einschätzen

Effektiv ist auch die Vereinbarung einer Konventionalstrafe. Die Herausforderung besteht darin, genau die später konkret eintretende Leistungsstörung zu regeln, also mit einer Geldstrafe zu bedrohen. Ist die Konventionalstrafe nämlich in Form einer Generalklausel (also beispielsweise für sämtliche Fälle einer Beschlagnahme) vereinbart worden, so könnte ihre Durchsetzung schwierig werden, da die völlige Vernachlässigung des Verschuldensprinzips in manchen Rechtsordnungen sittenwidrig sein könnte. Wichtig ist, vorzusehen, dass mit der Inanspruchnahme der Konventionalstrafe weitere Schadenersatzansprüche nicht ausgeschlossen werden. Die Konventionalstrafe hat immer dann große Bedeutung, wenn Art und Umfang eines Verstoßes schwer zu ermitteln sind. In diesen Fällen soll alleine die Tatsache, dass es zu einem Verstoß kam, eine Sanktion auslösen (z.B. Nichteinhaltung von Maßnahmen zur Datensicherheit).

5.6 Treuhandinstrument

Bei komplexen Zusammenhängen und hoher Konfliktwahrscheinlichkeit könnte ein Treuhänder eingesetzt werden. Dieser kann von Anfang an oder erst bei Bedarf bestellt werden. Sein Treuhandauftrag könnte sein, das ihm übergebene Vertragsentgelt erst nach Vorliegen aller Voraussetzungen, also dem reibungslosen Ablauf des Cloud Services ohne Vorliegen von Leistungsstörungen oder Eintritt von Haftungen, an den Vertragspartner auszuzahlen.

Welcher Treuhänder?

Neben dem Vertragsentgelt macht vor allem die Hinterlegung des Sourcecodes Sinn (sofern es sich nicht um SaaS handelt, wo dies wohl irrelevant ist, weil keine Individualsoftware tangiert ist). Während bei der Hinterlegung des Entgelts die Sanierung der aufgetretenen Leistungsstörung (Verletzung von Vertragspflichten, Sorgfaltsverletzung, substantielle Datennichtverfügbarkeit) im Vordergrund steht, geht es bei der Hinterlegung des Sourcecodes vor allem um die Kontinuität der Leistungserbringung bei Vertragsübergang (beispielsweise bei Vertragsbeendigung, Insolvenz des Anbieters, Wegfall der Vertrauensbasis etc.).

Die Tücke liegt im Detail, vor allem in der Auswahl des Treuhänders. Für gewöhnlich werden Rechtsanwälte oder Ziviltechniker, mitunter Notare zu Treuhändern bestellt. Das Treugut kann im vorliegenden Fall recht komplex sein: So kommt es oft zu einer schwer differenzierbaren Gemengelage von Daten, Metadaten und Web-Anwendungen, überdies ist die Frage der Updateintervalle zu klären und zu kontrollieren. Schließlich ist die beste Dokumentation wenig wert ohne brauchbare Schnittstellendefinition. Daher empfiehlt sich ein Zusammenspiel zwischen dem klassischen (meist juristischen) Treuhänder und einem technischen Sachverständigen, der mit den aufgezeigten technischen Fragen nicht überfordert ist. Beide treten gemeinsam interdisziplinär als ein Team (eine Art Treuhandsenat) auf.

Definition des Treuhandauftrages

Sehr wichtig ist die Definition des Treuhandauftrages in der Treuhandvereinbarung. Die Treuhandvereinbarung kann bereits im ursprünglichen Vertrag enthalten sein, wird aber meist gesondert (im gleichen Zeitpunkt oder später) errichtet, da sie auch von den Treuhändern zu unterschreiben ist. Mit dieser Vereinbarung wird definiert, unter welchen Voraussetzungen die Treuhänder das Treugut (in den meisten Fällen einen Teil des Entgeltes oder den Sourcecode) an den Berechtigten herausgeben dürfen.

Da die Herausgabevoraussetzungen meist nur durch einen Sachverständigen geklärt werden können, empfiehlt es sich, bereits im Vertrag oder in der Treuhandvereinbarung einen Sachverständigen zu bestellen oder das Bestellverfahren zu regeln, sodass zumindest hierüber kein Streit entflammen kann. Alternativ könnte auch ein Schiedsgutachter bestellt werden. Der Unterschied zum schlichten Sachverständigen besteht darin, dass sich die Vertragsparteien der Entscheidung des Schiedsgutachters unanfechtbar unterwerfen, während das Befundergebnis eines schlichten Sachverständigen grundsätzlich (durch ein Gegengutachten) entkräftet werden kann.

5.7 Möglichkeiten außerhalb des Vertrages

5.7.1 Ersatzvornahme

Grundsätzlich kommt zur Durchsetzung eines Gewährleistungsanspruches auch eine Ersatzvornahme in Frage. Sie wird bei Cloud Services in der Regel aber an der technischen Komplexität der Materie und vor allem aus Datenschutzgründen scheitern. Das bedeutet aber nicht, dass ihre Androhung unzulässig wäre.

5.7.2 Aufrechnung

Am Rande erwähnt sei die Möglichkeit der Aufrechnung mit dem eigenen Anspruch gegen eine Forderung des Vertragspartners. Bei Cloud Services wird typischerweise einerseits eine Dienstleistung, andererseits Entgelt geschuldet, sodass der Aufrechnung als Druckmittel in der Praxis geringe Bedeutung zukommen wird, da sie die Gegenseitigkeit und Gleichartigkeit der aufgerechneten Forderungen voraussetzt.

5.7.3 Einstweilige Verfügung (EV)

Scheitern alle gütlichen Einigungsversuche, so wird gerichtliche Hilfe oder die Einschaltung des vereinbarten Schiedsgerichtes unumgänglich sein.

Zeitdruck

Das Problem besteht nun vor allem im zeitlichen Aspekt. Die Entscheidung des Schiedsgerichtes dauert unter Umständen einige Monate, das (erstinstanzliche!) Urteil eines staatlichen Gerichtes mitunter noch wesentlich länger.

In dieser Situation kommt ein Provisorialverfahren in Frage. Dieses Verfahren bietet die Möglichkeit, bestimmte Ansprüche (wie beispielsweise die Herausgabe von Daten, die Fortsetzung einer Vertragsbeziehung, die Vornahme bestimmter Handlungen) vor einer Entscheidung im Hauptverfahren einstweilig zu schützen.

Das Verfahren zur Erlangung einer einstweiligen Verfügung begnügt sich mit der bloßen Bescheinigung des Vorbringens (also der Behauptungen des Anspruchstellers). Im Gegensatz zum Hauptverfahren muss also kein aufwändiges Beweisverfahren durchgeführt werden, wodurch das EV-Verfahren gegenüber dem Hauptverfahren wesentlich kürzer ist.

Bescheinigung ersetzt Beweis

Als Beweis zugelassen werden sogenannte „parate Bescheinigungsmittel", also nur solche, die unverzüglich verfügbar sind. In der Praxis wird ein Anspruch daher meist mit Urkunden (Vertrag, Korrespondenz, Fotos, Screenshots etc.), mit eidesstattlichen Erklärungen von Zeugen (die Einvernahme wird nur in Ausnahmefällen, wenn der Zeuge unverzüglich verfügbar ist, zugelassen) oder mit vorgelegten Gutachten bescheinigt.

Subjektive Gefährdung

Voraussetzungen für eine EV sind das Bestehen eines Hauptanspruches und dessen konkrete subjektive Gefährdung.

Nach der Antragstellung wird dem Gegner – wenn überhaupt – eine kurze Äußerungsfrist eingeräumt. Der Äußerung und allenfalls Gegenäußerung folgt eine rasche Entscheidung, die binnen 14 Tagen mit Rekurs bekämpft werden kann. Die Rekursentscheidung kann binnen weiterer 14 Tage mit Revisionsrekurs bekämpft werden.

Eine EV kann grundsätzlich auch im Schiedsverfahren beantragt werden.

5.7.4 Schiedsverfahren

Als Schiedsverfahren bezeichnet man die außergerichtliche Konfliktbeilegung nach vereinbarten Prozessregeln durch ein Schiedsgericht. Das Schiedsgericht kann durch die Vertragsparteien bestimmt werden oder durch eine Organisation (z.B. internationale Handelskammer oder sonstige Interessensverbände) bereitgestellt werden.

Schiedsvereinbarung?

Voraussetzung für ein Schiedsverfahren ist das Vorliegen einer schriftlichen Schiedsvereinbarung.

ordre public

Der bestehende Konflikt wird (sofern es sich um einen privatrechtlichen Anspruch handelt) durch den Schiedsspruch beendet. Der Schiedsspruch tritt an die Stelle eines gerichtlichen Urteils, ist für die Parteien bindend und kann für vollstreckbar erklärt werden. Mit wenigen Ausnahmen (in der Regel Verstöße gegen Rechtsgrundsätze, den sogenannten „ordre public") entscheidet das Schiedsgericht als letzte Instanz, seine Entscheidung ist daher grundsätzlich unanfechtbar.

Vollstreckbarkeit?

Vor der Entscheidung für eine Schiedsvereinbarung sollte überprüft werden, ob Schiedssprüche im Sitzstaat des Vertragspartners (Convention on the Recognition and Enforcement of Foreign Arbitral Awards, NYC) vollstreckbar sind, da andernfalls ein entsprechender Schiedsspruch wertlos wäre.

Der große Vorteil des Schiedsverfahrens besteht in der Verfahrensdauer (schon durch den Wegfall der Anfechtungsmöglichkeit), die meist prognostizierbaren Kosten und die fachliche Qualifikation der Schiedstribunale (die sich oft aus Spezialisten der betroffenen Fachgebiete konstituieren).

Neben dem Schiedsverfahren nach rechtlichen Grundsätzen (arbitration) kommt auch ein Verfahren nach Billigkeit (Schiedsgutachterverfahren, adjudication) in Frage. Im Schiedsgutachterverfahren können die sonst zwingenden Verfahrensgarantien frei vereinbart werden, sodass noch schnellere, summarische Entscheidungen ermöglicht werden.

5.7.5 Gerichtliche Auseinandersetzung

Im worst case kommt es tatsächlich zu einer gerichtlichen Auseinandersetzung. Aber selbst in diesem Fall kann es unter dem Damoklesschwert des Gerichtsstreits noch immer zu einem außergerichtlichen oder mit Unterstützung des Richters zu einem gerichtlichen Vergleich kommen.

Gerichtskosten

Der Unterschied zu vorher besteht nun darin, dass die auflaufenden Kosten zu beachten sind. Beide Seiten sollten daher berücksichtigen, dass ein Vergleich oft bei wechselseitiger Kostenaufhebung geschlossen wird und diese daher den Vergleichsbetrag schmälern.

Beweislast

Eine gerichtliche Auseinandersetzung hat den Nachteil, dass der Prozessausgang ungewiss ist, weil er nicht nur von den Fakten, sondern vor allem von deren Beweisbarkeit abhängt. Daher sollte ein Prozess – egal ob aktiv

oder passiv geführt – akribisch vorbereitet werden. Zum einen ist auf die betroffenen Rechtsfragen einzugehen. Ihre Lösung hängt mitunter von der Weiterentwicklung der Rechtsprechung und von der Bereitschaft der Parteien, Rechtsfragen allenfalls erst in oberster Instanz klären zu können, ab. Vor allem ist aber auf die Qualität des Beweismaterials und seine Aufbereitung und überzeugende Darstellung im Prozess abzustellen. Hier hängt sehr viel vom Engagement der Partei und des vertretenden Rechtsanwaltes ab. Die Aufgabe des Anwaltes ist vor allem, eine möglichst realistische Risikoeinschätzung abzugeben. Auf Basis dieser Einschätzung ist letztlich auch bilanziell (durch entsprechende Rückstellungen) für den Prozessausgang Vorsorge zu treffen.

Streitwert

Die Kosten eines Zivilprozesses hängen von der Höhe des Streitwertes, von seiner Dauer, der Anzahl der involvierten Instanzen und der Anzahl an Prozessschritten ab. Je mehr Zeugen beantragt werden, umso länger dauert das Verfahren. Ein ganz erheblicher Kostenfaktor ist überdies der – im vorliegenden Zusammenhang wohl unerlässliche – Sachverständigenbeweis.

Prozesskostenfinanzierung

Seit einiger Zeit besteht auch in Österreich die Möglichkeit einer Prozesskostenfinanzierung durch hierauf spezialisierte Unternehmen. Im Gegenzug verpflichtet sich der Kläger, einen Anteil des erkämpften Streitwertes abzuliefern. Ob es zu einer Prozesskostenfinanzierung kommt, ist eine Frage der Risikoeinschätzung. Sie ist eine gangbare Alternative zum (zu diesem Zeitpunkt wohl gescheiterten) Vergleich mit dem Streitgegner, bei dem ja schließlich meist auch auf einen Teil des Anspruches verzichtet werden muss.

5.7.6 Anwendbares Recht

Zuständiges Gericht

Bei internationalem Bezug ist schon im Vertrag zu klären, welches Recht anwendbar sein soll. Die Rechtswahl hat größte Auswirkung auf die Kosten und natürlich die Chancen eines Rechtsstreites. Wird eine vertragliche Vereinbarung übersehen, so ist das anwendbare Recht – sofern vor gerichtlicher Einlassung keine Einigung erfolgt – als Vorfrage durch die Gerichte zu klären.

Das Gleiche gilt für die Gerichtszuständigkeit. Die Rechtswahl sagt grundsätzlich noch nichts über die Gerichtszuständigkeit aus. Sofern nach dem

anwendbaren Recht kein zwingender Gerichtsstand gegeben ist, sollte daher auch die Gerichtszuständigkeit im Vertrag geregelt werden.

5.7.7 Umsetzung gerichtlicher Entscheidungen

Auch gerichtliche Entscheidungen sind nicht in allen Staaten exekutiv durchsetzbar, also vollstreckbar. Bei der Regelung oder Auswahl des Streitbeilegungsmodus ist daher zu prüfen, ob Gerichtsentscheidungen des Gerichtsstaates im Sitzstaat des Vertragspartners durchsetzbar sind. So sind z.B. Gerichtsurteile in den USA (häufiger Serverstandort) nicht vollstreckbar.

6 Checkliste Vertragselemente



In Anlehnung an das EuroCloud SaaS-Gütesiegel werden die wichtigsten Fragen hinsichtlich der vertraglichen Ausgestaltung angeführt. Anbieter, die durch EuroCloud nach diesen Anforderungen geprüft wurden, erfüllen die Basisanforderungen für die Bereitstellung von Cloud-Diensten.

Das EuroCloud Star Audit Gütesiegel soll auch Anbietern eine wichtige Hilfestellung dabei liefern, das Vertrauen der Anwender zu angemessenen Konditionen zu gewinnen.

Es muss eine klare Abgrenzung zu den Anbietern geben, die ihr Angebot auf „Minimalspur" fahren, denn der Anwender kann nur mit erheblichem Aufwand und schlimmstenfalls erst im Eskalationsfall die wirklichen Defizite erkennen.

Konkret werden im EuroCloud Gütesiegel folgende Kategorien erfasst:

- Anbieterprofil
- Vertrag und Compliance
- Sicherheit
- Betrieb der Infrastruktur
- Betriebsprozesse
- Anwendung
- Implementierung

Durch ein Punktesystem und die Vorgabe von Mindestkriterien kann ein Anbieter Gütestufen von ein bis fünf Sternen erreichen.

Im Unterschied zu anderen Initiativen, bei denen entweder nur Teilbereiche berücksichtigt werden oder die Angaben ohne Gegenkontrolle als freiwillige Selbstverpflichtung zu sehen sind, wird beim EuroCloud Gütesiegel eine Validierung der Angaben durchgeführt und in vereinbarten Zeiträumen wiederholt, damit ein konkreter Nachweis der Angaben vorliegt. Zudem verpflichtet sich der Anbieter, signifikante Änderungen der Rahmenbedingungen (z.B. Ort der Leistungserbringung, Änderung der Subunternehmervereinbarungen) und kritische Vorfälle unverzüglich zu melden. Damit erfüllt das EuroCloud Gütesiegel die Anforderungen der Europäischen Union an eine externe Prüfung und Validierung von Cloud-Services.

Das SaaS-Gütesiegel wird seit 2011 offiziell vergeben. Folgende Punkte (überblicksartige Aufstellung) sollten bei der Vertragsgestaltung entsprechend umgesetzt werden und werden im Rahmen der EuroCloud Gütesiegel-Zertifizierung geprüft:

6.1 Vertragsabschluss und Vertragsgestaltung

» Wie wird der Vertrag geschlossen?
- online
- schriftlich
- Kann der Kunde auf einen schriftlichen Vertrag bestehen?

6.2 Überbindung auf Subunternehmer

» Hat der Auftragnehmer seine Subunternehmer an dieselben Verpflichtungen gebunden, die er gegenüber dem Auftraggeber eingeht?

» Bedarf der Einsatz/Wechsel von Subunternehmern der Zustimmung des Auftraggebers?

6.3 Leistungsverrechnung

» Wird die Nutzung des Services pauschal zeitabhängig berechnet?

» Wird die Nutzung des Services nach Verbrauch berechnet?
- Existieren Mengenrabatte/unterschiedliche Tarife in Abhängigkeit von der abgenommenen Servicemenge?
- Kann der Auftragnehmer seinen Tarif bei signifikanter Änderung des Nutzungsumfangs ändern?
- Gibt es eine Best-Price-Option?

» Wird optional eine Flatrate oder per user-Flatrate angeboten?

» Gibt es extra zu verrechnende Sonderleistungen? Wenn ja, welche?

6.4 Leistungsstörungen

» Leistungsstörung beim Auftragnehmer oder dessen Unterauftragnehmern
- Bestehen Regelungen zum Schadenersatz bei Leistungsstörungen?

» Streit über Leistungserbringung/Zahlungsverzug
  - Ist ein Zurückbehaltungsrecht an Daten des Auftraggebers oder ihm gegenüber zu erbringenden Leistungen vertraglich ausgeschlossen?
  - Ist auch im Fall von Streitigkeiten zur Leistungserbringung oder bei Zahlungsverzug ausgeschlossen, dass der Auftragnehmer die Daten ohne Zustimmung des Auftraggebers löscht?

6.5 Vertragskündigung

» Welche Kündigungsfristen sind für den Auftraggeber und den Auftragnehmer definiert?

» Gibt es eine demonstrative Liste der möglichen (außerordentlichen) Kündigungsgründe?

» Wenn ja, für wen?
  - Auftraggeber
  - Auftragnehmer

» Ist eine Vorankündigung von Änderungen bei der Diensterbringung von Subunternehmern vertraglich geregelt?

» Existieren Regelungen zur Mitwirkung des Auftragnehmers bei der Datenbereitstellung nach einer Vertragskündigung?

6.6 Insolvenz des Auftragnehmers

» Existieren Regelungen zum Schutz der Daten des Auftraggebers und der Verfügbarkeit der Anwendung bei Insolvenz des Auftragnehmers?

» Existiert ein Source Code Deposit?

» Ist die Software an eine bestimmte Plattform gebunden?

» Wird dem Auftraggeber ein Recht auf Herausgabe der letzten Datensicherung und Dokumentation eingeräumt?

6.7 Compliance

» Datenarchivierung

- Welche Normen zu unternehmens- und steuerrechtlichen Aufbewahrungspflichten und Aufbewahrungsfristen bei der Verwendung von Datenträgern werden eingehalten?
- Wie wird bei elektronischer Verarbeitung und Archivierung beim SaaS-Anbieter sichergestellt, dass die betroffenen Daten (etwa elektronische Rechnungen, Bücher, Aufzeichnungen und sonstige Unterlagen) während der gesetzlichen Aufbewahrungsfristen sicher aufbewahrt werden und deren vollständige, geordnete und inhaltsgetreue Wiedergabe, auch an die Behörden, möglich ist?
- Wie ist der Prozess einer kontinuierlichen Rückübermittlung solcher Daten an den Auftraggeber gewährleistet?

» Datenschutzrelevanz

- Werden innerhalb der Anwendung personenbezogene Daten im Sinne des DSG verwendet?
- Ist die Datenverwendung – soweit erforderlich – beim Datenverarbeitungsregister registriert?
- Sind die Mitarbeiter des Auftragnehmers nachweislich zur Einhaltung des Datengeheimnisses verpflichtet?
- Ist geregelt, welche Seite gegenüber den Kunden des Auftraggebers den Ansprechpartner für den Datenschutz darstellt?
- Sind Regeln für die Berichtigung, Löschung und Sperrung von Daten auf Antrag eines Betroffenen definiert?

» Auswahl Auftragnehmer und Subunternehmer

- Bietet der Auftragnehmer genügend Informationen zu seinem Unternehmen und seinen Unterauftragnehmern, um dem Auftraggeber eine fundierte Auswahl des Auftragnehmers zu ermöglichen?
- Werden die Unterauftragnehmer bekanntgegeben?

» Datenschutzniveau

- Ist – soweit einschlägig – auch außerhalb der EU (auch bei beteiligten Unterauftragnehmern) ein angemessenes Datenschutzniveau (z.B. über EU-Standardvertrag, Safe-Harbour-Regelung) hergestellt?

- Besteht die Möglichkeit, wenn aufgrund von gesetzlichen oder behördlichen Auflagen an den Auftraggeber erforderlich, die Orte der Datenhaltung auf Österreich oder die EU einzugrenzen?

» Beauftragung und Weisungsrecht

- Sind die Verantwortlichkeiten zwischen Auftraggeber (grundsätzliche datenschutzrechtliche Verantwortlichkeit) und Auftragnehmer (Umsetzung von Weisungen, technischen Schutzmaßnahmen etc.) sauber definiert?
- Ist der Umfang des Auftrags zur Datenverarbeitung hinreichend klar spezifiziert, insbesondere:
- Ist der Dienst grob beschrieben? Sind in der Beschreibung der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen dokumentiert?
- Sind die Dauer der Verarbeitung und die Löschung der Daten exakt definiert?
- Ist ein Entscheidungsspielraum des Dienstleisters zur Verarbeitung der Daten ausgeschlossen?
- Ist dokumentiert, ob und, wenn ja, wie sensible Daten im Sinne des DSG erhoben, verarbeitet oder genutzt werden?
- Ist das Weisungsrecht des Auftraggebers eindeutig definiert?

» Kommunikation

- Ist eine Kommunikationsregel etabliert für den Fall, dass Weisungen des Auftraggebers nach Meinung des Auftragnehmers gegen den Datenschutz verstoßen?
- Sind Sachverhalte definiert, die als mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen dem Auftraggeber angezeigt werden müssen?

» Umsetzung technischer und organisatorischer Datenschutzmaßnahmen
- Existiert eine Dokumentation/ein Konzept, welche technischen und organisatorischen Maßnahmen umgesetzt werden, um die Vorgaben des DSG zu erfüllen?
- Hat der Auftraggeber diesem Konzept (und Änderungen daran) zuzustimmen?

» Kontrollmöglichkeiten des Auftraggebers
- Existieren Regelungen zu Kontrollrechten des Auftraggebers und zu den entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers, insbesondere:
- Ist ein Kontrollrecht des Auftraggebers und/oder eines vom Auftraggeber beauftragten Dritten vor Ort beim Auftragnehmer oder seinen Subauftragnehmern ausdrücklich vereinbart?
- Existieren (kumulativ oder alternativ zu Kontrollen durch den Auftraggeber) regelmäßige Kontrollen/Audits und Zertifizierungen, die den Datenschutz beim Auftragnehmer und die Verpflichtungen gegenüber dem Auftraggeber kontrollieren und zertifizieren?
- Ist eine Regelung zur Mitwirkung des Auftragnehmers und zu den dadurch entstehenden Kosten getroffen?

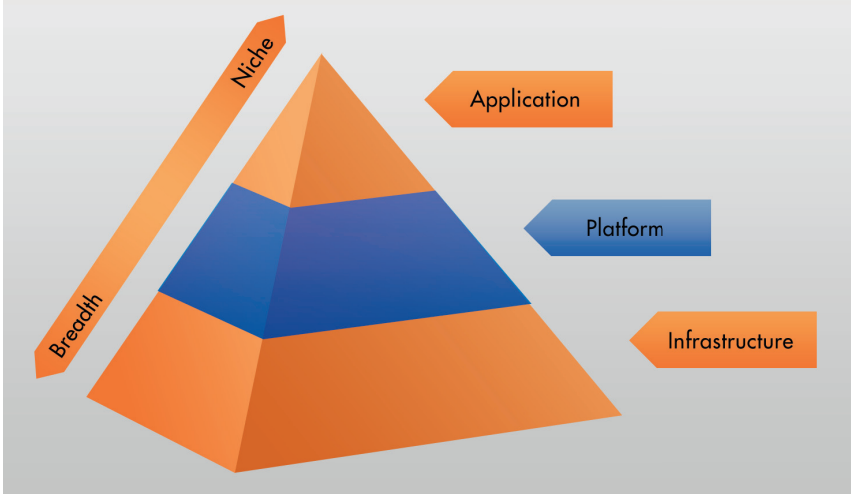
» Datenlöschung bei Vertragsende
- Existieren Regelungen zur Löschung der Daten und zur Rückgabe von Datenträgern nach Beendigung des Vertrags?
- Wird gewährleistet, dass die Daten auf Wunsch des Auftraggebers tatsächlich gelöscht werden?

7 Glossar Cloud Computing

Cloud Computing

„Cloud Computing ist ein Modell, das on-demand und online den Zugriff auf einen gemeinsamen Pool konfigurierbarer Computing-Ressourcen wie Netzwerke, Server, Speichersysteme, Anwendungen und Dienste ermöglicht. Diese können passgenau, schnell, kostengünstig und mit minimalem Verwaltungsaufwand bereitgestellt und abgerufen werden." *(Definition: NIST; National Institute of Standards and Technology, USA)*

Als Grundansatz für die Darstellung der verschiedenen Elemente des Cloud Computings wird oftmals das SPI-Modell herangezogen, welches die drei Serviceebenen – Infrastruktur, Plattform und Software – darstellt.



Hierbei werden die Ebenen aufeinander aufbauend dargestellt, wobei die jeweils unteren Ebenen auch unabhängig von der darüber liegenden Ebene genutzt werden können.

Public Cloud

IT-Dienstleistungen werden von einem Cloud-Anbieter bereitgestellt und können von jedem über das Internet genutzt werden.

Private Cloud

IT-Dienstleistungen werden aus den eigenen Rechenzentren bezogen. Alle Dienste und die Infrastruktur unterstehen einer Institution. Die Cloud kann durchaus von Dritten betrieben werden. Auf die Dienste wird entweder über das Intranet oder über VPN (Virtual Private Network) zugegriffen.

Hybride Cloud

ist eine Mischform bestehend aus einer Public Cloud und einer Private Cloud.

Föderierte Cloud

Hybride Cloud mit spezieller Sicherheitstechnik durch vertrauenswürdige Serviceanbieter im Bereich der Identifikation und Verschlüsselung.

IaaS: Infrastructure as a Service

Bereitstellung von Rechen- und Speicherkapazitäten als Service.

PaaS: Platform as a Service

Bereitstellung von „Middleware“ als Service.

SaaS: Software as a Service

Bereitstellung von Applikationen als Service.

XaaS: X as a Service

Bereitstellung von zusätzlichen Funktionen wie Geschäftsprozesse, Netzwerke, Kommunikation und weitere als Service.

8 Rechtlicher Hinweis

8.1 Allgemeines

Die in diesem Leitfaden zur Verfügung gestellten Informationen dienen der allgemeinen Darstellung spezieller rechtlicher Aspekte im Zusammenhang mit Cloud Computing, stellen keine Rechtsberatung dar und können auch keine Rechtsberatung ersetzen, da eine solche immer die Kenntnis aller Einzelumstände, insbesondere des konkreten Einzelfalls voraussetzt.

8.2 Inhalt des Leitfadens

Der Herausgeber/die Autoren übernehmen keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität der bereitgestellten Informationen. Dies gilt insbesondere im Hinblick auf neueste Entwicklungen in der Rechtsprechung oder der Gesetzeslage. Haftungsansprüche gegen den Herausgeber/die Autoren, die sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen.

8.3 Verweise und Links

Bei direkten oder indirekten Verweisen auf fremde Inhalte (z.B. „Links"), die außerhalb des Verantwortungsbereichs des Herausgebers/der Autoren liegen, würde eine Haftungsverpflichtung ausschließlich in dem Fall in Kraft treten, in dem der Herausgeber/die Autoren von den Inhalten Kenntnis hatten und es ihnen technisch möglich und zumutbar wäre, die Nutzung im Falle rechtswidriger Inhalte zu verhindern. Der Herausgeber/die Autoren erklären hiermit ausdrücklich, dass zum Zeitpunkt der Linksetzung keine illegalen Inhalte auf den zu verlinkenden Seiten erkennbar waren. Auf die aktuelle und zukünftige Gestaltung, die Inhalte oder die Urheberschaft der verlinkten Seiten haben der Herausgeber/die Autoren keinen Einfluss. Sie distanzieren sich ausdrücklich von allen Inhalten aller verlinkten Seiten, die nach der Linksetzung verändert wurden. Für illegale, fehlerhafte oder unvollständige Inhalte und insbesondere für Schäden, die aus der Nutzung oder Nichtnutzung solcherart dargebotenen Informationen entstehen, haftet allein der Anbieter der Seite, auf welche verwiesen wurde, nicht derjenige, der über Links auf die jeweilige Veröffentlichung lediglich verweist.

8.4 Urheberrecht

Die in diesem Leitfaden dargestellten Inhalte wie Texte, Graphiken oder Bilder sind nach dem österreichischen Urhebergesetz urheberrechtlich geschützt. Jede urheberrechtlich nicht gestattete Verwertung bedarf der vorherigen schriftlichen Zustimmung des Herausgebers. Beiträge Dritter sind als solche gekennzeichnet. Dies gilt insbesondere für Vervielfältigung, Bearbeitung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien. Die unerlaubte Vervielfältigung oder Weitergabe einzelner Teile oder des gesamten Leitfadens ist ausdrücklich nicht gestattet. Ausgenommen ist dabei der individuelle bzw. private Gebrauch, wobei die private Nutzung kein Recht zur Weitergabe an Dritte beinhaltet. Gleiches gilt für Veröffentlichungen oder sonstige Arbeiten.

8.5 Vergütung

Dieser Leitfaden wird den Adressaten/Empfängern kostenlos zur Verfügung gestellt.

9 Autoren

Die Autoren der Österreich-Version des Leitfadens sind:



Rechtsanwalt Mag. Christoph H. Hackl
c.hackl@ratiolegis.at
http://www.ratiolegis.at



Rechtsanwalt Dr. Martin Klemm, LL.M.
klemm@brenner-klemm.at
http://www.brenner-klemm.at



Rechtsanwältin Mag. Karin Peyerl
karin.peyerl@chsh.com
http://www.chsh.com

Der Druck dieses Leitfadens wurde freundlicherweise durch Sponsoren der EuroCloud.Austria finanziert:

EuroCloud.Austria
Verein zur Förderung von Cloud Computing
Museumstraße 5/14
1070 Wien

E-Mail: info@eurocloud.at
Web: http://www.eurocloud.at
Sitz des Vereins: Wien

Copyright: EuroCloud.Austria

Der Druck dieses Leitfadens wurde freundlicherweise durch Sponsoren der EuroCloud.Austria finanziert: