Aus allen Wolken fallen – Risiken des Cloud Computings

MMag. Andreas Wiesauer, Univ.-Prof.in Dr. in Eveline Artmann, Univ.-Prof. Dr. Johannes Sametinger

Cloud Computing ist ein aktueller Trend im Bereich der Informationstechnologie. Vereinfacht ausgedrückt ist darunter eine neue Spielart der Auslagerung betrieblicher Informationssysteme zu verstehen. Wurde Cloud Computing bisher in der Praxis begeistert und nahezu kritiklos aufgenommen, mehrten sich im Dezember letzten Jahres die kritischen Stimmen[1]. Den Anlass dazu stiftete die Plattform WikiLeaks. Diese benutzte zur Speicherung und Bereitstellung ihrer Informationen einen Cloud-Dienst von Amazon. Im Dezember 2010, als WikiLeaks aufgrund der dort veröffentlichten vertraulichen Informationen immer mehr unter Druck geriet, war sie von einem Tag auf den anderen plötzlich nicht mehr erreichbar. Der Cloud-Dienstleister Amazon hatte – wohl aufgrund vorauseilenden Gehorsams gegenüber der US-Administration – seine Dienstleistung für WikiLeaks fristlos beendet. Begründet wurde dies mit einem Verstoß gegen die Nutzungsbedingungen. Dieses Beispiel stellt zweifellos ein Extrem dar. Es ist jedoch nicht auszuschließen, dass ein ähnliches Schicksal auch Unternehmen blüht, die sich auf Cloud-Dienste verlassen. Überhaupt scheint die Verfügbarkeit von Daten bei Dienstleistern teils dubiose Begehrlichkeiten der Staaten zu wecken[2]. Auch in einer globalisierten Welt sind Staaten nicht vor protektionistischen Anflügen gefeit. Dienstleister könnten somit von ihren Staaten durchaus unter Druck gesetzt werden, missliebige Konkurrenten inländischer Unternehmen durch Einschränkungen von Diensten zu behindern.

Der vorliegende Artikel zeigt Gefahren und Risiken des Cloud Computings auf. Während im angloamerikanischen Raum und in Deutschland die Thematik auch aus rechtlicher Perspektive diskutiert wird, fehlt eine solche Abhandlung hierzulande bislang. Der vorliegende Artikel soll die Diskussion dazu eröffnen.

1. Cloud Computing – Begriff und Abgrenzung

Die Idee des Cloud Computings ist trivial: Man bedient sich zur Erfüllung verschiedener Aufgaben nicht mehr eigener Informationssysteme, sondern „abonniert“ dafür Dienst(programm)e (Services) eines Dienstleisters. Beim Kunden verbleibt somit nur mehr die zur Nutzung der Dienste notwendige Infrastruktur, im Allgemeinen Arbeitsplatzrechner mit Betriebssystem und Client-Anwendungen (im Falle von Web-Anwendungen der Internet-Browser) sowie Netzwerkkomponenten (Router, Gateways).

Das Spektrum der Cloud-Dienste reicht dabei beispielsweise von einfachen Termin- und Aufgabenplanern über Textverarbeitungsprogramme bis hin zu vollständigen ERP-Systemen. Vereinzelt werden auch online verfügbarer Speicherplatz (z.B. Dropbox.com) oder Dienste für Synchronisation und Datensicherung von Mobiltelefonen (z.B. HTCSense.com) als Cloud-Dienste bezeichnet. Nahezu jeder über das Internet angebotene Dienst lässt sich derzeit als Cloud-Dienst anscheinend besser verkaufen.

Der Begriff „Cloud“ suggeriert dabei die Abstraktion dieser Dienste von technischen Gegebenheiten – die Cloud-Nutzer können je nach

---

[1] Vgl. Frankfurter Allgemeine Zeitung, Amazons Rauswurf nährt die Zweifel an der Cloud, 10.1.2011.

[2] Vgl. dazu die Vorkommnisse im Januar 2011 rund um das soziale Netzwerk Twitter, dem ein US-amerikanisches Gericht aufgetragen hat, Daten aller „Follower“ der Plattform WikiLeaks bzw. Julian Assanges an die US-Administration zu übermitteln, dazu näher Die Presse, USA zwingen Twitter zur Herausgabe von Wikileaks-Infos, 8.1.2011.

Bedarf benötigte Dienste aus einer virtuellen „Wolke“ von Diensten auswählen, siehe Abb. 1.

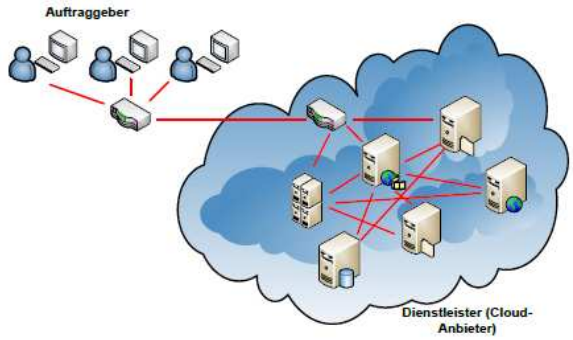

Abbildung 1. Cloud Computing

Die Vorteile dieses Konzepts sind Flexibilität und Skalierbarkeit, d.h. die bedarfsorientierte Nutzung der Dienste und damit verbundene Kosteneinsparungen. Müssen traditionelle IT-Infrastrukturen im Unternehmensbereich immer darauf ausgerichtet sein, auch unter Maximallast entsprechend zu funktionieren und damit ausreichende (und zu vielen Zeiten nicht benötigte) Ressourcen bereitzuhalten, so können beim Cloud Computing dynamisch zusätzliche Ressourcen angefordert und zugeschaltet werden, z.B. Speicherplatz oder Prozessorleistung. Ermöglicht wird dies durch das Konzept der Virtualisierung. Es wird dabei nicht konkrete Hardware bereit gestellt, auf der bestimmte Software oder Plattformen[3] ausgeführt werden, sondern „virtuelle“ Systeme, denen je nach Bedarf Ressourcen wie Speicher und Prozessorleistung zugeordnet werden können. Es erfolgt damit eine Abstraktion von der konkreten Hardware durch virtuelle Maschinen. Diese virtuellen Maschinen „simulieren“ Betriebssysteme und die darauf laufenden Anwendungsplattformen und stellen dadurch scheinbar unendliche Ressourcen zur Verfügung[4].

Im Unternehmensumfeld kann Cloud Computing als eine Variante des IT-Outsourcings betrachtet werden. Beim „klassischen“ Outsourcing erfolgt die Auslagerung vereinfacht ausgedrückt durch „Sale-and-Lease-Back“, d.h. durch den Transfer der Betriebsmittel (Hardware, Software aber auch Personal) hin zu den Dienstleistern, z.B. durch Neugründung eigener Gesellschaften, häufig in Form von Joint Ventures mit anderen Unternehmen. Die Dienstleister wurden dann für die Bereitstellung und Verwaltung der Ressourcen bezahlt. Cloud Computing lässt sich davon dadurch unterscheiden, dass kein solcher Transfer von Betriebsmitteln erfolgt. Der Dienstleister stellt die Ressourcen schon betriebsbereit zur Verfügung.

Ab Mitte der 1990er Jahre kursierte die Idee des Application Service Providing (ASP). „Service“ bezieht sich hier auf die Erbringung einer Dienstleistung, nämlich der Bereitstellung einer Anwendung und darf nicht mit dem Dienste-Konzept (Services) späterer Outsourcing-Trends verwechselt werden. Kern der Idee des ASP ist der Bereitstellung von Anwendungen (Standardsoftware wie Textverarbeitungsprogramme) über Kommunikationsnetzwerke durch darauf spezialisierte Dienstleister sowie die Bezahlung nach Inanspruchnahme (Pay-Per-Use)[5]. ASP konzentrierte sich dabei auf Einzelanwendungen, während beim Cloud Computing auch die Bereitstellung einzelner Dienste, ganzer Plattformen oder von Anwendungen in Form von kombinierbaren Diensten bezweckt wird. Auch das Konzept der Virtualisierung (s.o.) war dem ASP fremd.

Das beim Cloud Computing im Vordergrund stehende Dienste-Konzept ist nicht neu. Beeinflusst durch neue Strukturierungskonzepte zur Gestaltung von Software-Architekturen (Zerlegung großer Programme in einzelne, wiederverwendbare Einheiten die bestimmte Aufgaben erledigen, sog. „Services“) und die daraus entstehenden Service-Oriented-Architectures (SOAs) entstand die Überlegung, solche „Landschaften“ wiederverwendbarer Dienste Kunden zur Nutzung gegen Entgelt anzubieten. Damit

[3] Unter Plattform ist dabei eine Ablaufumgebung zu verstehen, auf der selbst entwickelte Dienste installiert werden können. Diese enthalten meist auch Entwicklungsumgebungen zur Implementierung solcher Dienste.

[4] *Weinhardt et al.*, Cloud-Computing – Eine Abgrenzung, Geschäftsmodelle und Forschungsgebiete, Wirtschaftsinformatik, 5/2009, 453.

[5] *Mäder*, Application Service Providing - Chancen und Risiken, ZfCM, 2007, 181.

entstand mit SaaS (Software-As-A-Service) ein neuer IT-Trend. Neu im Vergleich zu ASP ist nicht nur das Dienste-Konzept, sondern auch die technische Verbreitung, z.B. durch Web-Technologien. Als Einsatzbereiche für SaaS werden vor allem Anwendungen mit hohem Standardisierungsgrad, wie z.B. Customer-Relationship-Management (CRM) oder Enterprise-Resource-Planning (ERP) Systeme genannt[6]. Parallel dazu entwickelte sich das Konzept Platform-As-A-Service (PaaS) welches darauf abzielt, nicht nur einzelne Dienste, sondern gesamte Plattformen (zum Begriff der Plattform siehe FN 3) als Dienst anzubieten[7].

Nun fällt auf, dass Cloud Computing im Wesentlichen schon durch SaaS bzw. PaaS verwirklicht wird. Tatsächlich ist strittig, ob Cloud Computing Neuheitswert in technischer bzw. konzeptioneller Hinsicht aufweist oder nur ein „Marketing-Buzzword" darstellt[8]. *Armbrust et al.* bezeichnen Cloud Computing überhaupt als „alte Idee, deren Zeit nun gekommen scheint"[9]. Manche erblicken darin eine Kombination der oben genannten Trends mit dem Grid-Computing[10], andere wiederum sehen den Einsatz von Virtualisierungstechniken als Abgrenzungskriterium[11]. *Skillikorn* versteht unter Cloud Computing eine Form komponentenorientierter Anwendungsentwicklung (Entwicklung eigener Anwendungen durch „Zusammensetzung" von verfügbaren Cloud-Diensten)[12] – den Neuheitswert sieht er in einer Verschmelzung bekannter Konzepte mit neuen Technologien. Diese Definitionsversuche zeigen, dass es schwer fällt, Cloud Computing von anderen Trends abzugrenzen. Die Diskussion ist diesbezüglich noch im Fluss und wird in Zukunft eindeutigere Definitionen hervorbringen. Eines unterscheidet Cloud Computing jedoch von den Vorläufer-Trends: Während diesen eher mäßiger wirtschaftlicher Erfolg beschieden war und diese daher ein Schattendasein fristeten, könnte sich dies nach derzeitigem Stand für Cloud Computing aufgrund des derzeit enormen Interesses in Wissenschaft und Praxis anders darstellen.

Für eine rechtliche Analyse kann die genaue Abgrenzung jedoch offen bleiben. Wesentlich ist vielmehr, dass durch Cloud Computing Outsourcing-Vorgänge stattfinden. Die Datenhaltung der Informationssysteme erfolgt nicht mehr auf Servern innerhalb des Unternehmens, sondern eben „in der Cloud". Selbiges gilt für die Anwendungslogik, d.h. für die Abläufe und die Durchführung von Berechnungen. Lediglich die Benutzungsschnittstelle verbleibt beim Kunden, sei es in Form eigenständiger Anwendungen am Arbeitsplatzrechner („Rich"- oder „Fat"-Client) oder in Form webbasierter Anwendungen innerhalb eines Browsers. Dies macht permanente Kommunikationsvorgänge zwischen dem Kunden und dem Dienstleister notwendig, die im Rahmen der Anforderungen der IT-Sicherheit von Interesse sind. Generell stellt uns Cloud Computing bei der Sicherheit und beim Datenschutz vor neue Herausforderungen[13].

Der Vollständigkeit halber muss noch zwischen sog. „Private Clouds" und „Public Clouds" unterschieden werden. Private Clouds werden von Unternehmen eigenständig aufgebaut und ausschließlich intern genutzt (Auftraggeber und

---

[6] *Buxmann et al.*, Software as a Service, Wirtschaftsinformatik, 6/2008, 500.

[7] Der Vollständigkeit halber sei noch IaaS (Infrastructure-as-a-Service) erwähnt, bei dem Hardware zur Nutzung als Dienst überlassen wird.

[8] *Andresen*, Über die Wolken – Rechtsfragen des Cloud Computings, Linux-Magazin, 05/2010, 84.

[9] *Armbrust et al.*, A Berkeley View of Cloud Computing, Technical Report, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf (12.1.2011).

[10] Ein „Grid" ist ein Verbund von Hochleistungsrechnern, der zur Bewältigung von rechenintensiven Aufgabenstellungen, wie der Lösung komplexer mathematischer Probleme dient.

[11] *Weinhardt et al.*, Cloud-Computing, 453.

[12] *Skillikorn*, The Case for Datacentric Grids, Proceedings of the International Parallel and Distributed Processing Symposium 2002, 5.

[13] *Takabi et al.*, Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, Vol. 8, No. 6, Nov./Dec. 2010.

Dienstleister gehören zum selben Unternehmen). Dabei handelt es sich nur um eine andere Organisationsform der Informationsinfrastruktur und nicht um IT-Outsourcing. Daher sind im Folgenden nur Public Clouds von Interesse.

2. Rechtliche Aspekte

Ist die Heranziehung von Clouds zur Abwicklung betrieblicher Aufgaben aus rechtlicher Sicht zulässig? Und falls ja, welche Anforderungen sind dabei zu berücksichtigen? Fest steht, dass es keine Rechtsnormen gibt, die Cloud Computing explizit verbieten oder erlauben würden. Somit ist es erforderlich, folgende Fragestellungen zu untersuchen:

1. Welchen rechtlichen Anforderungen sind betriebliche Informationssysteme überhaupt ausgesetzt?
2. Welche Konsequenzen ziehen Verstöße nach sich?
3. Können die Anforderungen im Falle der Nutzung von Cloud Computing eingehalten werden bzw. welche Voraussetzungen müssen allenfalls beachtet werden?

Abgesehen von Spezialgesetzen, wie z.B. dem Datenschutzgesetz (DSG 2000) oder dem Telekommunikationsgesetz (TKG 2003) fehlen generelle Rechtsnormen, die sich direkt auf Informationssysteme beziehen. Die Anforderungen ergeben sich vielmehr aus allgemeinen, unternehmensbezogenen Rechtsvorschriften. Dabei sind vor allem die Bereiche Unternehmensrecht, Steuerrecht (z.B. Richtigkeit des Steuerausweises), Datenschutzrecht, Urheberrecht sowie Teilbereiche des Zivilrechts (Schadenersatzrecht, Vertragsrecht, E-Commerce-Recht, Publizitätsvorschriften[14]) aber auch das Arbeitsrecht[15] zu nennen. In diesem Rahmen können diese vielfältigen Vorschriften nur exemplarisch im Überblick dargestellt werden. Der Schwerpunkt liegt dabei auf den unternehmensrechtlichen und datenschutzrechtlichen Aspekten. Steuerrechtliche und arbeitsrechtliche Aspekte müssen außer Acht gelassen werden. Im Folgenden wird die Terminologie des Datenschutzgesetzes verwendet: Auftraggeber ist der Nutzer eines Cloud-Dienstes, Dienstleister der Anbieter desselben.

Im Zusammenhang mit rechtlichen Anforderungen an IT-Systeme stößt man zwangsläufig auf den Begriff IT-Compliance. Wir werden zunächst den Bedeutungsgehalt dieses Begriffes näher untersuchen. Anschließend werden wird die Anforderungen aus den unterschiedlichen Rechtsmaterien darstellen. Am Ende der Abschnitte sind rechtliche Auswirkungen für Cloud Computing jeweils blau hinterlegt.

2.1 IT-Compliance

Compliance bedeutet Erfüllung, Einhaltung oder auch Ordnungsmäßigkeit und meint die Einhaltung von regulativen Anforderungen und Vorgaben (Gesetze, Industrie-Normen, Standards, Verträge, etc.), denen Unternehmen im Rahmen ihrer Geschäftstätigkeit ausgesetzt sind[16]. Dabei kann Compliance sowohl als Zustand[17] – gemeint ist der nachweisbare Zustand, dass alle Vorgaben erfüllt werden – wie auch als Prozess interpretiert werden, nämlich als „Gesamtheit aller organisatorischen Aufsichts-, Schulungs-, und Kontrollmaßnahmen der Geschäftsleitung, (einschließlich der Einrichtung eines Dokumentations-, und Berichtswesens), welche einen Verstoß gegen gesetzliche Pflichten verhindern sollen“[18]. Dabei kommen unterschiedliche Klassen von Anforderungen in Betracht:

---

[14] Zur den Anforderungen für Zessionsvermerke in EDV-Buchhaltungen OGH 29. 10. 1997, 5 Ob 2155/96i = JBl 1998, 105.

[15] z.B. die Notwendigkeit der Zustimmung des Betriebsrates zur Einführung von Systemen, durch die (auch) Arbeitnehmerüberwachung ermöglicht wird gem. § 96 Abs 1 Z 3 ArbVG oder das Einsichtsrechts des Betriebsrats in Aufzeichnungen über Mitarbeiter gem. § 89 Z 1 ArbVG; zu verschiedenen arbeitsrechtlichen Problemen rund um die IT-Nutzung vgl. *Laimer/Mayr*, Zum Spannungsverhältnis von Arbeitgeber- und Arbeitnehmerinteressen rund um die EDV-Nutzung, RdA, 410.

[16] *Teubner/Feller*, Informationstechnologie, Governance und Compliance, Wirtschaftsinformatik, 5/2008, 400.

[17] *Rüter et al.*, IT-Governance in der Praxis, 200.

[18] *Rath*, Rechtliche Aspekte von IT-Compliance, 119.

1. von nationalen oder supranationalen Gesetzgebern erlassene Rechtsnormen,
2. die zwischen dem Unternehmen und seinen Geschäftspartnern abgeschlossenen Verträge (z.B. mit Herstellern und Lieferanten von Hard- und Software),
3. sowie Regelungen, denen sich die Unternehmen freiwillig unterwerfen (z.B. Standards, Normen, Prozeduren)[19].

Ob Verträge und freiwillige Regelungen vom Compliance-Begriff umfasst sind, ist strittig. Nach Ansicht mancher[20] kann aber auch die Unterwerfung unter freiwillige Regelungen Haftungsfolgen auslösen. Man denke etwa an eine Unterlassungsklage nach dem UWG, für den Fall, dass sich ein Unternehmen mit der Einhaltung eines Regelwerkes rühmt, dieses jedoch im Endeffekt nicht einhält. Deshalb ist eine demensprechend weite Auslegung des Compliance-Begriffs gerechtfertigt.

Die Beachtung von Rechtsnormen und die Einhaltung von Verträgen sind ohnehin selbstverständlich und bedürfen keiner weiteren Betonung. Compliance muss also eine darüber hinaus gehende Bedeutung haben. *Feltl/Pucher* betrachten folgerichtig Compliance als „umfassende Verpflichtung der geschäftsführenden Organe, geeignete organisatorische Vorkehrungen und Maßnahmen zu setzen, um ein rechtmäßiges Verhalten des Unternehmens sowie der Mitarbeiter zu gewährleisten“, somit als ein systematisches betriebliches Organisationskonzept[21]. Bestandteile dieses Organisationskonzepts sind die Festlegung von Verantwortlichkeiten, unternehmensinterne Richtlinien, deren Überprüfung (Audits), Schulungs-, und Disziplinarmaßnahmen sowie ein funktionierendes Berichtswesen[22]. Wesentlich für Compliance ist ein wirksames Risikomanagement, d.h. die Erkennung von drohenden Compliance-Verstößen (Risikoanalyse und –bewertung) und die Definition und Durchsetzung entsprechender Gegenmaßnahmen[23]. Das Organisationskonzept und dessen Umsetzung durch verschiedene Maßnahmen sollen (Dritten gegenüber) nachweisbar sein, weswegen diese auch entsprechend dokumentiert werden müssen.

IT-Compliance bezeichnet also – je nach Sichtweise – entweder den Zustand, dass alle Rechtsnormen und sonstige Regulative mit Bezug zu betrieblichen Informationssystemen erfüllt sind, oder die Umsetzung aller in ein betriebliches Organisationskonzept eingebetteten Maßnahmen, die zur Erreichung dieses Zustands gesetzt werden müssen.

Bevor nun dargestellt wird, zu welchen rechtlichen Anforderungen Informationssysteme „compliant“ sein sollen, muss noch diskutiert werden, warum Compliance für österreichische Unternehmen überhaupt relevant ist. Der Begriff selbst findet sich in Österreich nur im Bank- und Kapitalmarktrecht (vgl. den Compliance-Begriff des § 18 WAG sowie in der Emittenten-Compliance-Verordnung) und verpflichtet somit nur kapitalmarktorientierte Gesellschaften und Kreditinstitute. Aus der Verpflichtung zur Einhaltung der Grundsätze verantwortungsvoller Unternehmensführung (Corporate Governance) für börsennotierte Unternehmen, der allgemeinen Leitungsverantwortung des Vorstandes (§§ 70, 84 Abs 1 AktG), die ein entsprechend organisiertes Unternehmen verlangt (Kontroll- und Organisationsverantwortung) und der Verpflichtung der Einrichtung eines internen Kontrollsystems gemäß § 82 AktG (IKS; siehe dazu lit. c unter 2.2) wird jedoch eine Verpflichtung von Aktiengesellschaften zur Errichtung eines Compliance-Systems abgeleitet[24]. Entsprechendes gilt auch für GmbHs (§§ 25, 71 GmbHG). In Deutschland wird diese Verpflichtung als Ausfluss aus § 347 dHGB (inhaltsgleich zu § 347 UGB) auch für Geschäftsleiter einer OG bzw. KG

[19] *Rüter et al.*, IT-Governance in der Praxis, 195f.

[20] *Zahradnik*, Corporate Governance – Haftungsfragen, GeS, 2002, 59.

[21] *Feltl/Pucher*, Corporate Compliance im österreichischen Recht – Ein Überblick, wbl 2010, 266.

[22] ebenda, 271.

[23] *Rüter et al.*, IT-Governance in der Praxis, 192.

[24] Zur Argumentation im Detail *Feltl/Pucher*, Corporate Compliance, 266ff.

angenommen[25]. Als weitere Grundlagen für Compliance werden oftmals der Sarbanes-Oxlex-Act, die RL 2006/43/EG, aber auch (zumindest mittelbar) die Basel II (bzw. III)-Kriterien genannt[26] (zu deren Bedeutung und Anwendbarkeit siehe lit e unter 2.2).

Festzuhalten ist, dass außerhalb des Kapitalmarkt- bzw. Wertpapierrechts keine spezifischen rechtlichen Sanktionen für Compliance-Verstöße existieren. Die Folgen hängen daher von der konkret übertretenen Verpflichtung ab (Strafen oder Verlust von Berechtigungen bei Übertretung von Rechtsnormen, Schadenersatz aus Vertrag, Wettbewerbsklagen, etc.). Die Folgen einer Compliance-Verletzung sind daher primär wirtschaftlicher Natur und bestehen z.B. in einem Imageverlust oder gesunkenem Anlegervertrauen bei Bekanntwerden des Versagens des Compliance-Systems. In Betracht kommt allerdings eine Haftung des Vorstands bzw. der Geschäftsführung gegenüber der Gesellschaft bei einem fehlenden bzw. mangelhaften Compliance-System und daraus resultierenden Schäden nach § 84 Abs 2 AktG bzw. § 25 Abs 2 GmbHG.

Für Cloud Computing lässt sich daraus zunächst eine Verpflichtung zur sorgfältigen Ermittlung der Entscheidungsgrundlagen ableiten. Die handelnden Personen sind verpflichtet, sich mit Cloud Computing vertraut zu machen. Sie müssen die Risiken kennen und bewerten und Verpflichtungen festlegen, die Cloud-Dienstleister zu beachten haben. Anschließend müssen die potentiellen Dienstleister anhand dieser Erkenntnisse beurteilt und eine rationale Auswahlentscheidung getroffen werden. Während des aufrechten Dienstleistungsverhältnisses müssen Bedrohungen erkannt und darauf entsprechend reagiert werden (z.B. bei instabilen Machtverhältnissen im Land des Dienstleisters oder falls sich der Dienstleister wiederholt als unzuverlässig erwiesen hat). Der Dienstleister muss vertraglich dazu verpflichtet werden, entsprechende Maßnahmen zu ergreifen, um Schäden zu verhindern bzw. Risiken zu minimieren. Dies betrifft insbesondere die Maßnahmen zur Gewährleistung der IT-Sicherheit. Der Auftraggeber ist verpflichtet, sich von der tatsächlichen Durchführung der Maßnahmen zu überzeugen (z.B. in dem er Nachweise verlangt oder selbst kontrolliert).

2.2 Unternehmensrecht

Informationsinfrastrukturen stellen einerseits einen wesentlichen Vermögensgegenstand dar (Hardware, Software, Kommunikationsnetzwerke). Andererseits dienen sie als Mittel zur Durchführung betrieblicher Aufgaben, z.B. der Rechnungslegung. Daher kann hier zwischen Anforderungen, die den Erhalt und Schutz des Vermögensgegenstandes betreffen (lit. a) und jenen, die die Durchführung von betrieblichen Aufgaben regeln und somit mittelbar auf die Informationssysteme wirken, unterschieden werden (lit. b – e).

a) Informationsinfrastrukturen als Vermögensgegenstand

Die Informationssysteme sind, nicht zuletzt aufgrund der zunehmenden Vernetzung, vielfältigen Bedrohungen ausgesetzt, z.B. Naturgewalten, technischem Versagen oder Hackerangriffen. Unternehmen müssen daher das Risiko minimieren, aufgrund dieser Bedrohungen Schäden an der Informationsinfrastruktur zu erleiden. Diese Schäden bestehen nicht nur im Ausfall der IT, sondern auch im potentiellen Verlust immaterieller Vermögensgegenstände (Kundendatenbanken, Verfahrensanweisungen, Betriebs- und Geschäftsgeheimnisse), die durch die Informationssysteme verarbeitet werden.

Fraglich ist, welche Anforderungen sich aus rechtlicher Sicht für den Betrieb von Informationsinfrastrukturen ergeben. Nach § 347 UGB haben Unternehmer bei der Durchführung ihrer Tätigkeiten für die „Sorgfalt eines ordentlichen Unternehmers einzustehen“. Gemäß der herrschenden Ansicht wird damit ein objektiver Sorgfaltsmaßstab normiert, wobei allerdings branchenspezifische Gepflogenheiten und die

[25] *Rath*, Rechtliche Aspekte von IT-Compliance[2], 150.

[26] *Kreuzer*, Compliance, CFOaktuell 2009, 205.

Unternehmensgröße zu berücksichtigen sind[27]. Anzumerken ist, dass es sich nach hA bei dieser Bestimmung nur um eine nähere Ausgestaltung der Sachverständigenhaftung nach § 1299 ABGB handelt und ihr somit keine eigenständige Bedeutung zukommt[28].

Nach *Krejci* beinhaltet der Sorgfaltsmaßstab zumindest, dass die Unternehmer die Grundlagen für ihre Entscheidungen sorgfältig ermitteln und ihr Handeln an der Förderung des Unternehmenswohles ausrichten[29]. Umgelegt auf die Gestaltung von Informationsinfrastrukturen bedeutet dies, dass Risiken, denen die Informationsinfrastruktur ausgesetzt ist, fortlaufend analysiert und bewertet werden und dem Stand der Technik entsprechende Gegenmaßnahmen gesetzt werden müssen. Dazu gehören unter anderem kontinuierliche Marktbeobachtungen, z.B. Welche Verschlüsselungsalgorithmen gelten noch als sicher? Welche Angriffe auf Informationssysteme gibt es aktuell und wie schützt man sich dagegen? Es geht also in erster Linie um die Gewährleistung von IT-Sicherheit. Nach *Donner* empfiehlt sich dafür ein IT-Audit durch (externe) Sachverständige. Dieses Audit soll Schwachstellen nicht nur technischer, sondern auch organisatorischer und personeller Natur aufdecken und wirksame Gegenmaßnahmen aufzeigen[30]. Basierend auf den Ergebnissen ist ein Sicherheitskonzept zu erstellen, welches die Gegenmaßnahmen definiert und deren Durchführung regelt (Planung, Kontrolle, Verantwortlichkeiten). Über die Gewährleistung von IT-Sicherheit hinaus müssen Informationssysteme in der Lage sein, ihnen zugedachte Aufgaben zuverlässig und effizient zu erfüllen. Daher lässt sich aus dem unternehmerischen Sorgfaltsgebot eine Zweckmäßigkeitsforderung ableiten.

Diese Grundsätze gelten naturgemäß auch für die Heranziehung von Cloud-Diensten. Der Auftraggeber gibt dabei wesentliche Gestaltungs- und Kontrollmöglichkeiten ab. Er verliert den Einfluss auf seine Informationssysteme und ist dem Dienstleister diesbezüglich ausgeliefert. Daher wird es in seinem Interesse sein, sich Kontrollrechte insbesondere bezüglich der IT-Sicherheit vertraglich einräumen zu lassen. Zusätzlich muss er selbst kontinuierlich die Qualität (Leistungsanforderungen, Verfügbarkeit) der Dienste überwachen.

b) Rechnungslegung

Besonderen Bezug zu Informationssystemen haben die Vorschriften über die Rechnungslegung, wie z.B. die Bestimmungen über die Buchführung, das Inventar und die Erstellung des Jahresabschlusses. § 190 Abs 5 UGB erklärt dafür die Verwendung von Datenträgern und auch die elektronische Übermittlung von Schriftstücken für zulässig, sofern dabei die „inhaltsgleiche, vollständige und geordnete … Wiedergabe bis zum Ablauf der gesetzlichen Aufbewahrungsfristen jederzeit gewährleistet ist“ und die „Lesbarkeit in geeigneter Form sichergestellt ist“. Davon umfasst sind die nach den Grundsätzen ordnungsmäßiger Buchführung erforderlichen Unterlagen der laufenden Buchführung (die eigentlichen Bücher sowie Buchungsbelege), nach hA nicht jedoch übrige aufbewahrungspflichtige Unterlagen, wie insbesondere Jahres- und Konzernabschlüsse, (Konzern-)Lageberichte oder Prüfungsberichte[31]. Diese müssen aufgrund ihrer Bedeutung weiterhin (auch) in Papierform aufbewahrt werden.

Zu beachten ist, dass die Wiedergabe von Büchern und Belegen über den gesamten gesetzlich vorgeschriebenen Aufbewahrungszeitraum hinweg gewährleistet sein muss. Dies bedeutet, dass bei einem Wechsel auf andere Medientypen (z.B. von Bandlaufwerken auf CD/DVD) die Lesegeräte für den vorherigen Medientyp aufbewahrt werden müssen. Dies gilt auch beim Wechsel von Softwaresystemen, bei dem si-

[27] *Hasberger*, IT-Sicherheit und Haftung, ecolex 2007, 509.

[28] *Schauer* in *Krejci*, RK UGB § 347 Rz 1.

[29] *Krejci*, Gesellschaftsrecht I, 95.

[30] *Donner*, Ordnungsgemäßheit und Sicherheit von Informationssystemen (Teil I), VWT 2003, 55.

[31] Zur alten Bestimmung des § 189 HGB, die inhaltlich in § 190 UGB übernommen wurde, *Geist* in *Jabornegg*, Kommentar zum HGB § 189 Rz 32 bzw. *H.Torggler/U.Torggler* in *Straube*, HGB online § 189 Rz 23a.

chergestellt werden muss, dass die alten Datei- bzw. Datenformate lesbar bleiben – entweder durch Konvertierung und Import in das neue System oder Aufbewahrung der Daten gemeinsam mit einem funktionierenden Altsystem.

Die Buchhaltung unter Verwendung von Informationssystemen muss die vollständige und richtige Aufzeichnung aller für die Buchführung relevanter Geschäftsvorfälle gewährleisten und hat dabei die Grundsätze ordnungsmäßiger Buchführung einzuhalten. Die Geschäftsvorfälle müssen in chronologischer (Journalfunktion) wie auch in sachlich zusammengehöriger (Kontenfunktion) Weise dargestellt werden können[32]. Die zu diesem Zweck eingesetzten Anwendungsprogramme sind dabei, sofern der Datenbestand nicht fortlaufend ausgedruckt wird (was heutzutage eher die Ausnahme sein wird), als Bestandteil der Buchführung zu betrachten und unterliegen auch einer Systemprüfung im Zuge der Abschlussprüfung[33]. Sie müssen prüfbar und deshalb entsprechend dokumentiert sein. Festzuhalten bleibt, dass – die Beachtung der oben dargestellten Grundsätze vorausgesetzt – keine konkreten Anforderungen an die technische Gestaltung von IT-Buchführungen gestellt werden. Diese wären auch nicht zielführend, da sich durch den technischen Fortschritt ständig neue Möglichkeiten ergeben und den Unternehmen Handlungsspielraum genommen würde. Bei Beachtung der Grundsätze könnte somit auch eine Buchhaltung basierend auf einem Tabellenkalkulationsprogramm ausreichend sein.

Fraglich ist, wie beurteilt werden kann, ob ein Buchführungssystem die Grundsätze ordnungsmäßiger Buchführung einhält. Nach dem Fachgutachten der Kammer der Wirtschaftstreuhänder KFS/DV1[34] ist dies dann der Fall, wenn a) die Geschäftsvorfälle sich in ihrer Entstehung und Entwicklung verfolgen lassen und sich ein sachverständiger Dritter innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens schaffen kann (Grundsatz der Transparenz), b) durch wirksame Kontrollmaßnahmen sichergestellt wird, dass die Geschäftsvorfälle in der Datenverarbeitung vollständig, richtig und zeitgerecht erfasst werden (Grundsatz der Kontrollierbarkeit) und c) nachträgliche Veränderungen, durch die der originale Inhalt einer Buchung nicht mehr festgestellt werden kann, hintangehalten werden (Grundsatz der Funktionssicherheit).

Zur Gewährleistung dieser Grundsätze werden im Gutachten *technische*, *organisatorische* und *dokumentarische* Maßnahmen bzw. Vorkehrungen im Zuge der Anschaffung und der Nutzung des Buchhaltungssystems empfohlen. Diese Maßnahmen werden jedoch nur exemplarisch angeführt (vgl. die Vorbemerkungen zur kommentierten Fassung). Zu den technischen Maßnahmen zählt beispielsweise die Prüfung der Funktionsfähigkeit und Eignung von Hardware bzw. Software, technische Überwachung einzelner Komponenten, regelmäßige Prüfung auf Fehler (z.B. bei Festplatten) sowie Belastungstests, um garantieren zu können, dass das System jederzeit in der Lage ist, genügend gleichzeitige Transaktionen zu verarbeiten.

Organisatorische Maßnahmen haben die geeignete organisatorische Einordnung der IT-Buchführung in das Unternehmen zum Ziel. Sie betreffen die organisatorischen Prozesse mit Bezug zum Buchhaltungssystem, wie z.B. die Festlegung von Zuständigkeiten und Berechtigungen, die Sicherstellung der Einhaltung der Bedienungsvorschriften, Sicherung der Daten oder Maßnahmen zur Gewährleistung der Betriebsbereitschaft[35]. Dokumentarischen Maßnahmen umfassen die Dokumentation techni-

[32] *H.Torggler/U.Torggler* in *Straube*, HGB online § 189 Rz 24.

[33] *Lechner/Egger/Schauer*, Einführung in die Allgemeine Betriebswirtschaftslehre[19], 593.

[34] Fachgutachten des Fachsenats für Datenverarbeitung des Instituts für Betriebswirtschaft, Steuerrecht und Organisation der Kammer der Wirtschaftstreuhänder zur Ordnungsmäßigkeit von EDV-Buchführungen KFS/DV1, 1998, online im Internet http://www.kwt.or.at/de/ResourceImage.aspx?raid=734 (12.1.2011).

[35] *Lechner/Egger/Schauer*, Einführung ABWL[19], 593.

scher und organisatorischer Maßnahmen sowie die Verfahrensdokumentation. Die dokumentarischen Maßnahmen sollen dem sachverständigen Dritten helfen, das System prüfen und sich somit den entsprechenden Überblick über das Unternehmen verschaffen zu können[36]. Die Verfahrensdokumentation umfasst insbesondere die konkrete Aufgabenstellung des Systems (Anschaffungsauftrag an den Hersteller des Systems im Sinne einer Systemspezifikation[37]), Angaben des Herstellers über den Aufbau der Datensätze (z.B. relationale Datenbankschemata einschließlich des Tabellenaufbaus und der Datentypen der Tabellenzellen), die wesentlichen Verarbeitungsregeln (Kontrollfunktionen, Verhalten im Fehlerfall), die Funktionsweise der Datensicherung sowie Nachweise über Art und Anzahl durchgeführter Programmtests (Test-Dokumentation)[38].

Diese Anforderungen haben weitreichende Konsequenzen, falls Cloud-Dienste für buchführungsnahe Zwecke (z.B. Archivierung von Buchungsbelegen) herangezogen werden sollen. Sie bedeuten zunächst nichts anderes, als dass der Auftraggeber auf die Offenlegung der wesentlichen Gegebenheiten der Informationsinfrastruktur des Dienstleisters bestehen muss. Dabei werden sehr detaillierte Beschreibungen verlangt, u.a. Programmspezifikationen, Datenbankschemata oder die Funktionsweise von Sicherungsmechanismen. Für Cloud-Dienste muss dies auch die Funktionsweise der Virtualisierung, insbesondere des Lastausgleichs und damit des Wechsels zwischen verschiedenen Rechenzentren (siehe dazu unter 2.3), sowie die Behandlung von dabei auftretenden Fehlern umfassen (Synchronisationsfehler).

Abgesehen davon, dass eine solche vollständige Dokumentation wohl ein Ausmaß und Komplexität erreichen würde, die Einzelpersonen (z.B. die Abschlussprüfer) nur schwer überblicken können, empfiehlt es sich, diese Anforderungen einschränkend auszulegen. Auch im Falle der Nutzung eines unternehmensinternen Buchführungssystems (z.B. SAP) werden nicht alle Details über dieses System bekannt sein, da solche Kenntnisse über die Systeme von deren Herstellern nicht gewünscht sind. Eine solche Einschränkung entspricht wohl auch der Praxis. Dennoch ist ein gewisses Maß an Transparenz und Nachvollziehbarkeit erforderlich, auf dessen Regelung beim Vertragsschluss nicht vergessen werden darf.

Beachtet werden müssen jedenfalls die gesetzlichen Aufbewahrungszeiträume. Daher müssen mit dem Dienstleister diesbezügliche Vereinbarungen getroffen werden. So kann zum Beispiel vorgesehen werden, dass der Dienstleister in regelmäßigen Abständen den kompletten Datenbestand ein einem bestimmten Format an den Auftraggeber übermittelt.

c) Internes Kontrollsystem (IKS)

Beeinflusst von Zusammenbrüchen einiger großer US-Unternehmen, die auf ein mangelhaftes internes Kontrollsystem zurückzuführen waren, wurde in den USA der sog. Sarbanes-Oxley-Act (SOX) erlassen. Gemäß Section 404 SOX müssen nunmehr Unternehmensprozesse genau definiert, dokumentiert und Kontrollverfahren implementiert werden, die das Risiko falscher Bilanzausweise minimieren sollen[39]. Im Endeffekt wird damit eine Verantwortlichkeit des Managements für effiziente und nachvollziehbare interne Kontrollsysteme geschaffen. SOX gilt unmittelbar nur für den amerikanischen Jurisdiktionsbereich, ist aber auch für europäische Unternehmen bindend, die an US-amerikanischen Börsen notieren bzw. Tochterunternehmen US-amerikanischer Unternehmen sind[40]. Vielfach verlangen US-amerikanische Unternehmen in Verträgen mit ausländischen Unternehmen die Beachtung der SOX-Vorgaben[41].

---

[36] *H.Torggler/U.Torggler* in *Straube*, HGB online § 189 Rz 24b.

[37] Zum Begriff der Systemspezifikation vgl. *Sommerville*, Software Engineering[8], 136.

[38] Punkt II.2 KFS/DV1

[39] *Hasberger*, IT-Sicherheit, 508.

[40] *Hall/Liedtka*, The Sarbanes-Oxley Act: Implications for large-scale IT outsourcing. Communications of the ACM, 3/2007), 95.

[41] *Rath*, Rechtliche Aspekte von IT-Compliance[2], 153.

Beeinflusst von SOX verabschiedete die Europäische Union die Richtlinie 2006/43/EG[42]. Diese verfolgte eine ähnliche Zielsetzung, hat jedoch einen anderen Fokus. Inhaltlich adressiert die Richtlinie die Rolle und Pflichten der Abschlussprüfer in Bezug auf die Prüfung interner Kontrollsysteme, jedoch werden auch die Verpflichtungen der Organwalter zur Schaffung und Überwachung eben dieser Systeme betont[43].

Die RL 2006/43/EG wurde in Österreich durch das Unternehmensrechtsänderungsgesetz 2008 (URÄG 2008) umgesetzt. Aus dem neuen § 243a Abs 2 UGB ergibt sich nun für kapitalmarktorientierte Gesellschaften die Verpflichtung, die „wesentlichen Merkmale" ihres internes Kontrollsystems in Bezug auf die Rechnungslegung im Lagebericht zu dokumentieren. Damit wird aber nur eine Dokumentationspflicht statuiert, die Pflicht zur Errichtung eines solchen Systems war nicht neu, sondern ergab sich schon bisher für Aktiengesellschaften aus § 82 AktG bzw. für Gesellschaften mit beschränkter Haftung aus § 22 GmbHG[44]. Verlangt wird ein „den Anforderungen des Unternehmens" entsprechendes internes Kontrollsystem. Dieses umfasst nach der RV zum IRÄG 1997 „sämtliche aufeinander abgestimmte Methoden und Maßnahmen, die dazu dienen, das Vermögen zu sichern, die Genauigkeit und Zuverlässigkeit der Abrechnungsdaten zu gewährleisten und die Einhaltung der vorgeschriebenen Geschäftspolitik zu unterstützen"[45]. Dazu zählen nach Ansicht *Strassers* u.a. die sorgfältige Auswahl der Mitarbeiter, denen das Rechnungswesen anvertraut wird, die sorgfältige Auswahl des für die Zwecke des konkreten Unternehmens am besten geeigneten Buchhaltungssystems (IT-Systems) und der Aufbau eines Revisions- und Kontrollsystems unter Heranziehung von Kontroll- und Revisionsexperten[46].

Das IKS soll die Effektivität und Effizienz der Tätigkeiten des Unternehmens sicherstellen, die Zuverlässigkeit des Rechnungswesens und der Berichterstattung sowie die Einhaltung von Gesetzen und Regeln garantieren[47]. Für die Zielerreichung muss das IKS in der Lage sein, Fehler und Schwachstellen in den im Unternehmen ablaufenden Prozessen zu verhindern bzw. zumindest aufzudecken – insbesondere jene, die den Bestand des Unternehmens gefährden bzw. seine Wettbewerbsfähigkeit einschränken[48]. Im Mittelpunkt stehen daher die im Unternehmen ablaufenden Tätigkeiten. Diese sollen

1. für Externe nachvollziehbar sein (warum wird wann eine Tätigkeit wie ausgeführt),
2. kontrolliert werden (kein Vorgang bleibt ohne Kontrolle, „Vier-Augen-Prinzip"),
3. geteilt sein (für Durchführung und Kontrolle sind unterschiedliche Personen verantwortlich) und
4. nur für Berechtigte zugänglich sein (nur an einem Prozess beteiligte Mitarbeiter verfügen über notwendige Informationen)[49].

Bestandteil des IKS ist aber nicht nur die Kontrolle der einzelnen Tätigkeiten, sondern auch diese Tätigkeiten und Prozesse in ihrer Gesamtheit, um Schwachstellen bzw. Risiken im Prozessablauf identifizieren zu können. Daher muss das IKS auch ein für das Unternehmen angemessenes Risikomanagementsystem umfassen (Risikoanalyse, Risikobewertung, Durchsetzung von Gegenmaßnahmen).

Aus § 273 Abs 2 UGB ergibt sich eine Redepflicht[50] des Abschlussprüfers, wenn er im

---

[42] Richtlinie 2006/43/EG des europäischen Parlaments und des Rates über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, ABl. L 157/87; umgspr. „EURO-SOX"

[43] *Hasberger*, IT-Sicherheit, 509 mit besonderem Hinweis auf Art 41 (2) der RL 2006/43/EG.

[44] *Weber*, Das Unternehmensrechts-Änderungsgesetz 2008 im Überblick, ÖJZ 2008, 435.

[45] EBRV 734 BlgNR 20. GP, 64.

[46] *Strasser* in *Jabornegg/Strasser*, AktG II[5] §§ 77 bis 84 Rz 15.

[47] *Kreuzer*, IKS – Internes Kontrollsystem, CFOaktuell, 2010, 25.

[48] *Rüter et al.*, IT-Governance in der Praxis, 206.

[49] *Kreuzer*, IKS, 25.

[50] Zur inhaltsgleichen Bestimmung des § 273 Abs 2 HGB vgl. *Lechner* in *Straube*, HGB online § 273 Rz 26 ff.

Rahmen seiner Tätigkeit wesentliche Schwächen der internen Kontrolle in Bezug auf das Rechnungswesen entdeckt. Daraus ergibt sich – neben der Dokumentationspflicht für kapitalmarktorientierte Gesellschaften nach § 243a Abs 2 UGB – auch für nicht-kapitalmarktorientierte, prüfpflichtige Gesellschaften die Notwendigkeit der nachvollziehbaren Dokumentation des IKS (zumindest bezogen auf das Rechnungswesen).

Nachdem Informationssysteme Grundlage für nahezu alle Geschäftsprozesse sind, ist es augenscheinlich, dass der Betrieb von Informationssystemen Gegenstand von Kontrollmaßnahmen im Rahmen des IKS ist. Dies reicht vom Beschaffungsprozess (Auswahl geeigneter Hard- bzw. Software) über die Kontrolle der (teil-)automatisierten Abwicklung von Geschäftsprozessen (Nachvollziehbarkeit, Fehlerfreiheit) bis hin zu den Maßnahmen zur Gewährleistung von IT-Sicherheit. Daraus folgt, dass die Informationssysteme und die darauf bezogenen Unternehmensprozesse kontrollierbar sein und deswegen entsprechend dokumentiert sein müssen. Andererseits stellen Informationssysteme aufgrund der Erfassung aller Geschäftsvorfälle die technische Grundlage der IKS dar. So genannte „Business Information Warehouses" können über automatisierte Analysen der Geschäftsvorfälle die Lage des Unternehmens darstellen[51]. Diese sind dann selbst wieder Gegenstand von Kontrollmaßnahmen in Bezug auf die Richtigkeit der gelieferten Daten.

Es würde den ratio leges widersprechen, könnte sich der Auftraggeber durch Ausgliederung seiner Informationssysteme dieser Pflichten entledigen. Daher erstrecken sich die Verpflichtungen aus den Vorschriften zum IKS auch auf das Dienstleistungsverhältnis. Deshalb gilt es, die Qualität der Dienste fortlaufend zu überwachen und bei Abweichungen Maßnahmen zu ergreifen. Die Verpflichtung zur Überwachung und Kontrolle erstreckt sich aber auch auf die beim Dienstleister ablaufenden Prozesse. So ist zu kontrollieren, ob der Dienstleiter selbst über ein wirksames IKS verfügt und die oben ausgeführten Maßnahmen sorgfältig ausführt (Berechtigungskonzept, Dokumentation und Überwachung der Tätigkeiten,…).

d) Abschlussprüfung

Informationssysteme unterliegen Kontrollen („Audits") im Zuge der Prüfung des Jahresabschlusses. Das Fachgutachten KFS/DV2[52] gibt dafür Empfehlungen ab. Danach hat der Prüfer zunächst eine Gesamteinschätzung des IT-Risikos vorzunehmen, d.h. er hat abzuschätzen, ob sich durch den Einsatz von Informationssystemen Geschäfts- oder Kontrollrisiken ergeben, die für die Abschlussprüfung von Relevanz sind[53]. Bestehen nach Ansicht des Prüfers keine solchen Risiken, können weitere Prüfungshandlungen unterbleiben (unbeschadet der Prüfung der Ordnungsmäßigkeit der Buchführung, siehe dazu oben). Die Risiken werden in anwendungsunabhängige (Abhängigkeit von IT, Vornahme großer Änderungen, mangelndes Fachwissen und Ressourcen, ungeeignete IT-Strategie) und anwendungsabhängige Risiken (Fehler in Anwendungen führen zu einer falschen Darstellung im Jahresabschluss) eingeteilt.

Bestehen also nach Ansicht des Prüfers wesentliche Risiken, so hat er entsprechende Prüfungshandlungen vorzunehmen. Dabei kann es sich zum Beispiel um eine Kontrolle der IT-Prozesse (einschließlich der Maßnahmen im Rahmen des IKS), aber auch um Kontrolle von Programmen handeln. Bezüglich der Programmkontrolle wird zwar keine Analyse des Programmcodes verlangt, sehr wohl aber eine genaue Kenntnis der internen Abläufe des Programms sowie der Schnittstellen zu anderen

[51] *Rath*, Rechtliche Aspekte von IT-Compliance[2], 152.

[52] Fachgutachten des Fachsenats für Datenverarbeitung des Instituts für Betriebswirtschaft, Steuerrecht und Organisation der Kammer der Wirtschaftstreuhänder zur Abschlussprüfung bei Einsatz von Informationstechnik, 2004, online im Internet http://www.kwt.or.at/de/ResourceImage.aspx?raid=735 (12.1.2011).

[53] *Reimoser*, Das neue Fachgutachten KFS/DV2 "Abschlussprüfung bei Einsatz von Informationstechnik", - Auswirkungen auf die Abschluss- und IT-Prüfung, VWT 2005, 12.

Programmen. Einen weiteren Prüfungsgegenstand stellt der Zugriffsschutz dar – dabei ist zu prüfen, ob Unbefugte Daten in den Datenbanken ändern können. Dies erfordert eine Prüfung der IT-Sicherheit auf unterschiedlichen Ebenen (Mitarbeiter-PC, Netzwerk, Serverbetriebssystem, Datenbank)[54].

Somit wird vom Dienstleister auch Transparenz und Nachvollziehbarkeit gegenüber dem Abschlussprüfer gefordert. Im Bereich der Abschlussprüfung besteht allerdings seitens des Dienstleisters die Möglichkeit, das Fehlen wesentlicher Geschäftsrisiken glaubhaft zu machen. Durch entsprechende Nachweise, z.B. unterschiedliche ISO-Zertifizierungen im IT-Bereich, könnte der Abschlussprüfer vom Fehlen wesentlicher Risiken überzeugt werden. Um Komplikationen bei der Abschlussprüfung zu vermeiden, empfiehlt es sich, die Dienstleister bereits entsprechend auszuwählen bzw. im Vertrag ausdrücklich zu regeln, das Zertifizierungen bzw. sonstige Nachweise innerhalb angemessener Fristen erbracht werden müssen.

e) Basel II (III)

Nach *Hasberger* enthält auch die vom Baseler Ausschuss für Bankenaufsicht erarbeitete Rahmenvereinbarung „Basel II“ (bzw. die neue „Basel III“) für Informationssysteme mittelbar relevante Bestimmungen. Bei der Entscheidung über die Kreditvergabe sollen nämlich „operationelle Risiken“ berücksichtigt werden. Verfügt ein Unternehmen beispielsweise über mangelhafte IT-bezogene Kontroll- bzw. Risikomanagementsysteme oder fehlen angemessene Sicherheitsmaßnahmen, kann dies zu höheren Kreditzinsen oder auch Kreditabsagen führen[55].

Das Dienstleistungsverhältnis ist somit auch für Kreditgeber interessant. Um Probleme zu vermeiden, empfiehlt es sich, Dienstleister auszuwählen, die selbst über gute Ratings verfügen bzw. den Kreditgebern die Verlässlichkeit des Dienstleisters in geeigneter Form nachzuweisen (z.B. wiederum durch Zertifizierungen).

[54] ebenda, 12.

[55] *Hasberger*, IT-Sicherheit, 509.

Der Vollständigkeit halber sei noch auf spezielle Vorschriften für einzelne Branchen verwiesen, die sich natürlich auch auf die Informationsinfrastruktur auswirken können und die folglich ebenso beachtet werden müssen[56].

2.3 Datenschutz

Unternehmen verarbeiten regelmäßig personenbezogene Daten, zum Beispiel von Mitarbeitern, Lieferanten, Dienstleistern und (potentiellen) Kunden. Das Datenschutzgesetz 2000 (DSG 2000) schützt diese Betroffenen und gewährt ihnen ein Grundrecht auf den Schutz personenbezogener Daten, soweit ein schutzwürdiges Interesse besteht und nicht gewichtigere Interessen dem entgegenstehen (Verfassungsbestimmung mit Gesetzesvorbehalt in § 1 DSG). Dieser Bestimmung kommt unmittelbare Drittwirkung zu Gute, so dass die damit einhergehenden Rechte nicht nur gegenüber dem Staat, sondern gegenüber jedermann geltend gemacht werden können. Jedes Unternehmen ist somit Adressat dieser Verpflichtungen.

Für die Geltung des Grundrechts auf Datenschutz ist zunächst das Vorliegen eines schutzwürdigen Interesses iSd § 1 Abs 1 DSG Voraussetzung. Ein solches besteht dann nicht, wenn Daten allgemein bekannt sind oder nicht einer bestimmten Person zugeordnet werden können (Rückführbarkeit). Allgemein verfügbar sind Daten dann, wenn z.B. die Rechtsordnung sie öffentlich zugänglich macht (z.B. Informationen aus Grund- oder Firmenbuch) oder sonst *zulässigerweise* veröffentlicht wurden (z.B. Daten im Telefonbuch, Medienberichte)[57]. Daten, die also jemand in so genannten sozialen Netzwerken, wie Facebook oder MySpace, über sich veröffentlicht, sind richtigerweise nicht schutzwürdig. Die Kundendaten aber, die ein „Hacker“ beim Ausspähen eines Unternehmens erbeutet und anschließend im Internet publiziert, unterliegen hingegen sehr wohl dem Grundrecht auf

[56] z.B. das TKG 2003 oder die Chemikalien-Verordnung der EU (REACH). Näher dazu *Epner/Sickinger*, Einheitliche IT-Architektur - Softwarelösungen für Compliance-Vorgaben, CFOaktuell 2009, 171.

[57] *Dohr/Pollirer/Weiss*, DSG[2] § 1 Anm 7.

Datenschutz, da diese eben nicht zulässigerweise veröffentlicht wurden.

Nicht schutzwürdig sind ferner Daten, die nicht zu einer konkreten Person in Bezug gesetzt werden können. Damit sind Daten gemeint, die weder direkten noch indirekten Personenbezug iSd § 4 Z 1 DSG aufweisen. Direkt personenbezogen sind Daten, wie z.B. Geburtsdatum, Adresse, Geschlecht, Einkommen, Vermögen, Leumund, Intelligenzquotient, aber auch Werturteile (z.B. über die Bonität) sowie Fingerabdrücke, genetische Merkmale, Bilder oder die Stimme[58]. Unter indirekt personenbezogenen Daten werden solche Daten verstanden, die „in irgendeiner Weise verschlüsselt" sind und vom Verwender der Daten nur unter Zuhilfenahme ihm nicht zustehender Mittel entschlüsselt werden können[59]. Beispiele sind Listen von Kontonummern (ohne dazugehörige Namen bzw. Adressen) oder pseudonymisierte Daten (Ersetzung des Namens durch ein Pseudonym, z.B. eine bestimmte Buchstaben- und Ziffernfolge). Diese sind dann indirekt personenbezogen, wenn sich der Verwender nur auf illegalem Wege die Information beschaffen kann, um die Daten einer Person zuzuordnen.

Das Grundrecht kann aber auch Einschränkungen unterworfen sein. § 1 Abs 2 DSG enthält diesbezüglich eine Grundrechtsbeschränkung durch einen materiellen Gesetzesvorbehalt. Das Grundrecht auf Datenschutz ist dann nicht anwendbar, wenn lebenswichtigen Interessen des Betroffenen Vorrang einzuräumen ist (Umstände die sich auf das Leben des Betroffenen im medizinischen Sinn auswirken), er dem Grundrechtseingriff zustimmt oder überwiegende Interessen eines anderen vorliegen[60]. Die Zustimmung des Betroffenen kann ausdrücklich oder konkludent erfolgen. So wird zum Beispiel der Arbeitnehmer beim Eintritt in das Dienstverhältnis der Verarbeitung notwendiger Daten (Kontonummer, Sozialversicherungsnummer) konkludent zustimmen. Überwiegende Interessen liegen vor, wenn sie aus dem Recht bzw. der Gesamtrechtsordnung abgeleitet werden können. Wirtschaftliche Interessen sind nur dann überwiegende berechtigte Interessen, wenn sie von der Rechtsordnung zu solchen erklärt werden[61].

Liegt ein Anwendungsfall des Grundrechts vor, so gewährt das Datenschutzgesetz den Betroffenen verschiedene Ansprüche:

1. Recht auf Auskunft gemäß § 26,
2. Recht auf Richtigstellung oder Löschung gemäß § 27 DSG bzw. das
3. Widerspruchsrecht gemäß § 28 DSG.

Im Allgemeinen muss die Datenverarbeitung durch den Verwender den Grundsätzen der §§ 6ff DSG entsprechen. Diese verlangen eine mehrstufige Prüfung der Zulässigkeit der Datenverarbeitung. Nach den generellen Grundsätzen des § 6 DSG muss die Verarbeitung also nach Treu und Glauben[62] auf rechtmäßige Weise durchgeführt werden, darf nur zu eindeutig festgelegten Zwecken erfolgen, nicht über diese Zwecke hinausgehen und ist überhaupt nur so lange zulässig, wie für die definierten Zwecke erforderlich (es sei denn, dem würden gesetzliche Anforderungen entgegenstehen, wie z.B. die gesetzliche Aufbewahrungsfrist für Buchungsbelege).

§ 7 DSG definiert, unter welchen Umständen Daten konkret verarbeitet bzw. an Dritte übermittelt werden dürfen (gesetzliche Zuständigkeit bzw. rechtliche Befugnis). Gleichzeitig wird ein Verhältnismäßigkeitsgrundsatz statuiert (Eingriffe in das Grundrecht dürfen nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen). Die §§ 8, 9 DSG enthalten Regelungen für den

[58] ebenda, § 4.

[59] *Souhrada-Kirchmayer*, Das Datenschutzgesetz 2000, SozSi 1999, 938.

[60] *Jahnel*, Das Datenschutzgesetz 2000 - Wichtige Neuerungen, wbl 2000, 49.

[61] *Dohr/Pollirer/Weiss*, DSG[2] § 1 Anm 13.

[62] Der Grundsatz von Treu und Glauben beinhaltet beispielsweise, dass die Betroffenen über die Umstände der Datenverarbeitung nicht irregeführt oder im Unklaren gelassen werden, näher dazu vgl. *Grabenwarter*, Datenschutzrechtliche Anforderungen an den Umgang mit Kundendaten im Versandhandel, ÖJZ 2000, 861.

Schutz von nicht-sensiblen bzw. sensiblen Daten[63]. Für nicht-sensible Daten enthält § 8 eine Generalklausel sowie Beispiele, die keine Verletzung schutzwürdiger Geheimhaltungsinteressen darstellen; § 9 enthält eine taxative Aufzählung der zulässigen Fälle der Verarbeitung sensibler Daten.

Datenverarbeiter sind verpflichtet, für die Einhaltung dieser Grundsätze zu sorgen. Für Unternehmen bedeutet dies, dass Informationssysteme, mit denen personenbezogene Daten verarbeitet werden, diesen Grundsätzen entsprechen müssen bzw. dass den Ansprüchen Betroffener nachgekommen werden können muss. Daten müssen also vor unzulässiger Offenlegung geschützt werden, die Ansprüche auf Löschung oder Richtigstellung müssen erfüllt werden (z.B. Sicherstellung der Löschung auch auf etwaigen Sicherungskopien). Daher sind nicht nur technische Maßnahmen erforderlich, um die Daten zu schützen, sondern auch organisatorische Vorkehrungen. Dazu zählen u.a. die regelmäßige Überprüfung von Datenbeständen, ob diese den vorgesehenen Zwecken entsprechen, ob sie nicht über diese Zwecke hinausgehen und ob Daten noch benötigt werden oder gelöscht werden müssen. Die Datenverarbeiter müssen dabei nach dem Grundsatz von Treu und Glauben vorgehen – sie haben also die Daten nicht nur auf Antrag Betroffener zu prüfen, sondern diese Prüfung selbst regelmäßig durchzuführen.

Für die Datenverarbeitung durch Dienstleister enthält das Datenschutzgesetz spezielle Regelungen in den §§ 10f DSG. Diese erklären die Heranziehung von Dienstleistern (wie im Falle des Outsourcings bzw. Cloud Computings) explizit für zulässig, regeln allerdings damit verbundene Pflichten.

Voraussetzung für eine Zulässigkeit ist selbstverständlich die Einhaltung der Grundsätze des § 6 DSG durch den Auftraggeber (definierter Zweck, rechtliche Befugnis, keine Verletzung schutzwürdiger Geheimhaltungsinteressen). Eine weitere Prüfung der Einhaltung der Datenschutzgrundsätze, wie bei der Weitergabe an andere Auftraggeber gemäß § 7 Abs 2 DSG muss dabei im Verhältnis Auftraggeber – Dienstleister nicht erfolgen, sofern die Datenverarbeitung nicht außerhalb des EWR stattfindet. Damit sind Dienstleister innerhalb des EWR privilegiert, da für deren Heranziehung keine Zustimmung der Betroffenen gemäß § 12 Abs 3 Z 5 DSG erforderlich ist[64]. Für eine Zulässigkeit der Datenübermittlung in Nicht-EWR-Staaten muss demgegenüber eine Reihe von materiellen (u.a. Zustimmung der Betroffenen, Notwendigkeit zur Vertragserfüllung) und formellen (angemessenes Datenschutzniveau[65], Abschluss von sog. Standardvertragsklauseln gemäß Entscheidung 2004/915/EG der EU-Kommission[66]) Gründen vorliegen[67]. Liegen diese Gründe nicht vor, so ist um eine Genehmigung der Datenschutzkommission anzusuchen.

Besonderes gilt im Verhältnis zu den USA, da diesen im Allgemeinen kein angemessenes Datenschutzniveau zugebilligt wird. US-Unternehmen können gegenüber dem US-Handelsministerium erklären, dass sie sog. „Safe Harbour"-Grundsätze im Umgang mit Daten einhalten. Diese „Safe Harbour"-Grundsätze finden sich in einer Grundsatzvereinbarung des US-Handelsministeriums mit der EU-Kommission und enthalten grundsätzliche Datenschutzstandards. US-Unternehmen, die diese Erklärung abgegeben haben („Selbst-Zertifizierung") können als Dienstleister herangezogen werden[68].

Die Pflichten des Dienstleisters sind in § 11 DSG geregelt. Dazu zählen z.B. die Umsetzung der Datensicherheitsmaßnahmen des § 14 DSG, wie z.B. der Schutz der Daten vor zufälliger oder

[63] Sensible Daten sind Daten über die ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexualleben. Nicht-sensible sind alle übrigen personenbezogenen Daten.

[64] *Knyrim/Siegel/Autengruber*, Datenschutz und Datenrettung beim Outsourcing, ecolex 2004, 413.

[65] Welche Länder angemessenes Datenschutzniveau aufweisen, bestimmt eine VO des Bundeskanzlers.

[66] Siehe dazu *Dohr/Pollirer/Weiss*, DSG[2], § 13 Anm 8.

[67] Knyrim/Siegel/Autengruber, Datenschutz, 413.

[68] *Leissler*, Und die Daten fließen über den Atlantik ..., ecolex 2007, 748.

unrechtmäßiger Zerstörung oder Manipulation, die Sicherstellung ordnungsgemäßer Verwendung bzw. die Gewährleistung des Auskunfts-, Richtigstellungs- und Löschungsanspruchs oder der Schutz vor dem Zugriff Nicht-Berechtigter. Interessant ist hier auch, dass für den Fall, dass der Dienstleister selbst Dienstleister für die Datenverarbeitung heranzieht, der Auftraggeber dem zustimmen muss. Die Pflichten des § 11 DSG gelten kraft Gesetzes – sie müssen deshalb nicht zwingend Bestandteil des Vertrages zwischen Auftraggeber und Dienstleister sein. Nur eine etwaige Konkretisierung dieser Pflichten bedarf einer schriftlichen Vereinbarung iSd § 10 DSG.

Das österreichische DSG gilt grundsätzlich nur für Datenverarbeitung im Inland, ausnahmeweise jedoch auch für Datenverwendungen in EU-Mitgliedstaaten sofern diese Verwendung für einen Auftraggeber mit Sitz in Österreich erfolgt (§ 3 DSG). Wird also im Rahmen des Outsourcings ein Dienstleister aus dem EU-Ausland herangezogen, bedarf es – unbeschadet der Prüfung der grundsätzlichen Zulässigkeit (s.o) – jedenfalls einer Vereinbarung über die Grundsätze des § 11 DSG, da österreichische Gesetze naturgemäß diese Dienstleister nicht verpflichten können. Unbeschadet dessen wird, wie *Weiss et al.* anmerken, eine Vereinbarung in jedem Fall zweckmäßig sein (Nachweisbarkeit konkret vereinbarter Maßnahmen)[69]. Inhalt dieser Vereinbarung kann z.B. ein vom Dienstleister zu erstellendes Datenschutzkonzept bzw. Sicherheitskonzept oder die Überbindung von Verschwiegenheitspflichten sein. Den Auftraggeber trifft die Pflicht, die vom Dienstleister zu treffenden Maßnahmen zur Einhaltung der Pflichten regelmäßig zu kontrollieren[70].

Folglich ergibt sich für IT-Outsourcing im Allgemeinen eine grundsätzliche datenschutzrechtliche Zulässigkeit, soweit die oben genannten Grundsätze beachtet werden. Speziell für Cloud Computing und dessen zentrales Element der Virtualisierung ergibt sich jedoch eine besondere Situation: Gerade die großen Cloud-Anbieter verfügen über mehrere Rechenzentren in mehreren Ländern und ziehen diese zur Erbringung der „scheinbar unendlichen Ressourcen“ (s.o) flexibel heran. Damit ist gemeint, dass zwischen diesen Rechenzentren Lastausgleiche erfolgen, d.h. dass die Daten eines Auftraggebers nicht unbedingt in einem bestimmten Rechenzentrum gespeichert sind und dort verarbeitet werden, sondern – je nach Auslastung – zwischen diesen „wandern“ (siehe Abb. 2).

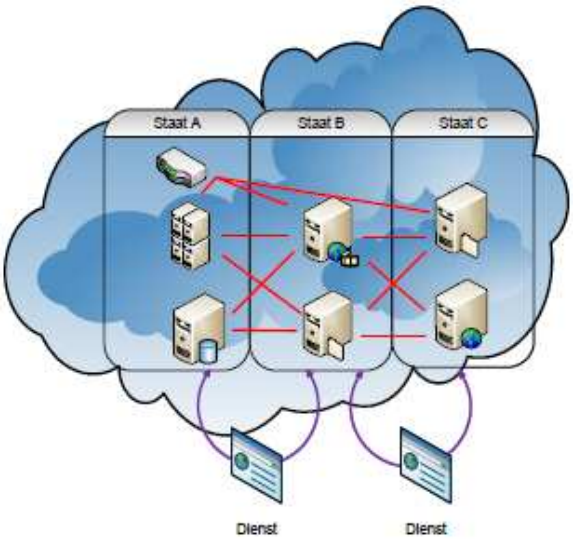

Abb. 2 Dienste-Transfer in der Cloud

Dies kommt heute schon in beträchtlichem Umfang vor[71]. Daher müsste der Auftraggeber vertraglich den Transfer in bestimmte Länder ausschließen, wenn diese nicht von seiner datenschutzrechtlichen Befugnis umfasst sind (z.B. wenn eine Zustimmung der Betroffenen zum Transfer ins Ausland nicht vorliegt). Dieser dynamische Ortswechsel der Daten kann aber bezüglich des Grundsatzes der Transparenz, der dem Datenschutzgesetz innewohnt, überhaupt problematisch sein. Diesem Grundsatz folgend, muss der Auftraggeber dem Betroffenen gegenüber jederzeit in der Lage sein, ihm Auskunft darüber zu geben, *wann, wo, wie* und *warum* seine Daten verarbeitet werden[72]. Dies

[69] *Dohr/Pollirer/Weiss*, DSG[2], § 11 Anm 6.

[70] *Souhrada-Kirchmayer*, DSG 2000, 938.

[71] *Schulzki-Haddouti,* Cloud Computing: Der Datenschutz verdampft, http://futurezone.orf.at/stories/1639608/ (4.09.2010)

[72] *Stanonik*, Trotz Wirtschaftskrise: Beim Outsourcing gilt es, den Datenschutz zu beachten!, ecolex 2009, 845.

ist im Falle von Clouds jedoch oft nicht möglich – der Auftraggeber bekommt vom Ortswechsel der Datenverarbeitung in der Regel nichts mit. Daher empfiehlt es sich, auch hierüber mit dem Dienstleister eine Vereinbarung zu treffen, beispielsweise in der Art, dass Aufzeichnungen im Sinne einer Logdatei geführt werden, die festhalten, wann wo welche Verarbeitung erfolgt ist.

Cloud-Dienstleister bieten ihre Dienste in der Regel mehreren Kunden an. Deshalb muss sichergestellt sein, dass die Datenbestände wirksam getrennt sind, d.h. dass Kunden nur auf ihre eigenen Daten Zugriff haben und nicht auch auf die anderer Kunden. Zu beachten ist ferner die Beendigung des Dienstleistungsverhältnisses bzw. eine potentielle Rückabwicklung. Hierbei muss sichergestellt sein, dass der Dienstleister alle personenbezogenen Daten entfernt und nicht etwa weitere Zwecke damit verfolgt.

Ein nicht zu unterschätzendes Risiko besteht für den Fall des Ausfalls des Dienstleisters (zum Beispiel durch Insolvenz, politische oder militärische Konflikte in instabilen Ländern). Auch aus diesem Grund empfiehlt es sich, den Dienstleister dazu zu verpflichten, dem Auftraggeber regelmäßig Kopien des kompletten Datenbestands zu übermitteln.

2.4 Urheber- und Vertragsrecht

Neben der Hardware (physische Komponenten von Rechner bzw. Rechnernetzwerken) bildet die Software (Computerprogramme) den wesentlichen Bestandteil von IT-Infrastrukturen. Software kommt in Form unterschiedlicher Kategorien in Unternehmen vor (Betriebssysteme, Datenbanken, Serveranwendungen, Textverarbeitungs- bzw. Tabellenkalkulationsprogramme, etc.). Aufgrund der Vielzahl an betrieblichen Aufgaben (Produktplanung, Konstruktion, Kalkulation, Rechnungslegung, Kundenmanagement,…) kommt auch eine Vielzahl unterschiedlicher Anwendungen zum Einsatz.

Software ist als Werk im Sinne des Urheberrechtsgesetz geschützt, wenn sie das Ergebnis einer eigenen geistigen Schöpfung des Urhebers ist (§ 40a UrhG). Daher müssen Unternehmen bei der Verwendung von Software die Grundsätze des UrhG bzw. die sich daraus ergebenden Rechte des Urhebers beachten (hier vor allem die in den §§ 14-18 UrhG genannten Verwertungsarten, wie z.B. Werknutzungs-, Werknutzungsbewilligungs-, Verbreitungs- bzw. Vervielfältigungsrechte).

Dies verursacht in der Praxis nicht zu unterschätzende Schwierigkeiten. Probleme entstehen zum einen durch die große Anzahl verschiedener Programme, die von Unternehmen eingesetzt werden, wie auch durch die unterschiedlichen Lizenzmodelle[73]. Diese Lizenzmodelle räumen dem Nutzer in der Regel kein Eigentumsrecht am Programm ein, sondern erlauben lediglich die Benutzung mit meist vielfältigen Beschränkungen (Nutzung nur auf Rechnern, die gemeinsam mit dem Programm erworben wurden, sog. *OEM-Lizenzen*[74], Nutzung auf einer bestimmten Anzahl von Rechnern, sog. *Volumenlizenzen*; bei Applikationsservern ist häufig die Anzahl der Clients, die auf diese zugreifen können beschränkt, sog. *Client-Lizenzen*). Daneben wird meist die Weitergabe[75] sowie Anpassungen (Modifikationen des Programmcodes) der Software vertraglich ausgeschlossen.

Grundsätzlich herrscht Uneinigkeit über die Beschaffenheit und Einordnung des Rechtsgeschäfts „Überlassung von Software gegen Entgelt“. Die Rechtsprechung[76] behandelt diese Überlassung mitunter als Kaufvertrag – und zwar auch bei entgegenstehendem Wortlaut der Vereinbarung. Dies erfolgt wohl vor dem Hintergrund, schuldrechtliche Bestimmungen (v.a. Gewährleistungsrecht) anwenden zu kön-

[73] *Gerick*, Software-Lizenzmanagement: Risiken und Kosten minimieren, CFOaktuell 2009, 260.

[74] OEM: Original Equipment Manufacturer

[75] Zur rechtlichen Zulässigkeit vgl. *Wiebe/Appl*, Urheberrechtliche Zulässigkeit des Erwerbs von "gebrauchten" Softwarelizenzen in Österreich, MR 2007, 186.

[76] OGH 14. 10. 1997, 5 Ob 504/96 = ecolex 1998, 127 (Wilhelm).

nen. Wie *Staudegger* anmerkt[77], ist es dazu allerdings zum einen gar nicht notwendig, die Parteienvereinbarung in einen Kaufvertrag „umzudeuten", da das Urheberrecht nach hA der Anwendbarkeit schuld- und sachenrechtlicher Bestimmungen nicht entgegensteht; zum anderen würde diese Umdeutung einen unzulässigen Eingriff in die Privatautonomie und den Grundsatz der Typenfreiheit im Vertragsrecht bedeuten (vor allem dann, wenn wie in OGH 14. 10. 1997, 5 Ob 504/96 zwischen den Parteien ausdrücklich nur ein unübertragbares und nicht ausschließliches Recht der Programmnutzung vereinbart wird). Somit sind, *Staudegger* folgend, die oben skizzierten Nutzungsbeschränkungen rechtlich wirksam. Im Allgemeinen wird daher in der Praxis an schon existierender Software eine (nicht-ausschließliche) Werknutzungsbewilligung erworben[78]. Unternehmen müssen daher wissen, welche Softwareprodukte zum Einsatz kommen und ob die Verwendung an jedem Arbeitsplatz durch Lizenzen gedeckt ist. Darüber hinaus wird verlangt, dass Unternehmen kontrollieren, ob Mitarbeiter unerlaubt Software installieren bzw. verwenden und damit Urheberrechtsverstöße begehen[79].

Ein Problem ergibt sich für Unternehmen aber nicht nur durch zu wenige Lizenzen (Unterlizenzierung), sondern auch durch zu viele (Überlizenzierung[80]). Der unternehmerischen Sorgfalt entspricht es, sowohl Über- als auch Unterlizenzierung zu verhindern. Zusätzlich beinhaltet der Schutz der Rechte des Urhebers auch die Verhinderung von Missbrauch. Es muss daher darauf geachtet werden, dass keine Sicherheitslücken in der Informationsinfrastruktur bestehen, durch die Software Unberechtigten zugänglich wird und dass Mitarbeiter die Software nicht an unberechtigte Dritte weitergeben.

Im Zusammenhang mit traditionellem IT-Outsourcing wurde der Urheberrechtsproblematik im wissenschaftlichen Diskurs breiter Raum gewidmet[81]. Dies rührt daher, dass dabei vom Auftraggeber eingesetzte Software an einen Dienstleister übertragen wird, was unter Umständen von urheberrechtlichen Nutzungsrechten nicht gedeckt ist[82]. Beim Cloud Computing spielt diese Thematik keine Rolle, da dieser Übergang nicht stattfindet. Der Dienstleister verwendet zur Realisierung der Dienste entweder selbst entwickelte oder von Dritten erworbene Software.

Beim Einsatz selbsterstellter Software ergibt sich urheberrechtlich keine Problematik, Beachtung verdient allerdings die Realisierung von Diensten mittels Software Dritter. Die Software wird auf den Rechnern des Cloud-Dienstleisters installiert und beim Betrieb (Nutzung des Dienstes) zumindest teilweise auf die Rechner des Auftraggebers (genauer in deren Arbeitsspeicher) übertragen. Somit liegt – nach in Deutschland herrschender Ansicht[83] – eine Vervielfältigung vor (§ 15 UrhG). Außerdem macht der Cloud-Dienstleister durch das Anbieten des Dienstes die Software öffentlich zugänglich (§ 16 Abs 1 UrhG) und zwar auch dann, wenn sie nur einzelnen Unternehmen angeboten wird, sofern eine entsprechend große Anzahl von Mitarbeitern Zugriff auf den Dienst erhält[84]. Diese Handlungen müssen von der urheber-

[77] *Staudegger*, Zur Qualifikation von Verträgen, die der Überlassung von Computersoftware dienen, JBl 1998, 604.

[78] Spezielle Probleme wie etwa die Auftragsanfertigung von Software durch Werk- oder Dienstvertrag sollen hier außer Acht gelassen werden; siehe dazu näher *E. Holzinger*, Rechtsgeschäftliche Übertragung von Software – Versuch einer systematischen Einordnung, EDVuR 1987, 10.

[79] *Gerick*, Software-Lizenzmanagement, 260.

[80] Nach einer Studie betrifft dies auf die Mehrzahl der Unternehmen; dazu *O'Neill*, Computerwoche vom 24. 9. 2008

[81] *Wimmers*, Darf ich das? Urheberrechtliche Probleme beim IT-Outsourcing, In: *Büchner/Dreier*, Von der Lochkarte zum globalen Netzwerk – 30 Jahre DGRI, 169ff.

[82] Zur Problematik vgl. *Bartsch*, Typische Regelungsschwerpunkte beim Outsourcing, EDVuR 1993, 42.

[83] *Schneider* in *Schneider*, Handbuch der EDV-Rechts[4], 542.

[84] Vgl. *Schumacher* in *Kucsko,* Kommentar zum Urheberrecht § 8 Punkt 3; der OGH spricht von einem „breiten Publikum" OGH 21. 4. 1998, 4 Ob 101/98a.

rechtlichen Befugnis des Cloud-Dienstleisters gedeckt sein. Es bedarf daher einer entsprechenden Vereinbarung.

Vereinzelt wird vertreten, dass der Auftraggeber, der Cloud-Dienste in Anspruch nimmt, selbst Vervielfältigungen vornimmt. Bei der Nutzung werden – technisch bedingt – typischerweise Teile der Software auf den Rechnern des Auftraggebers zwischengespeichert (im Arbeitsspeicher bzw. im Browser-Cache). Dabei handelt es sich aber um eine vorübergehende (flüchtige) Vervielfältigung, die nach § 41a UrhG zulässig ist[85]. Der Auftraggeber unternimmt selbst somit keine urheberrechtlich relevanten Handlungen. Er darf davon ausgehen, dass der Dienstleister über entsprechende Nutzungsrechte an den der Realisierung der Dienste zugrunde liegenden Software verfügt, da sonst ein Anbieten des Dienstes gar nicht in Betracht käme[86].

3. Vertragsverhältnis Auftraggeber – Dienstleister

Vereinzelt wurde bereits auf empfohlene Regelungen im Vertrag hingewiesen. Im Folgenden soll zunächst der Charakter des Vertrags zwischen Dienstleister und Auftraggeber untersucht werden. Anschließend werden die empfohlenen Regelungsschwerpunkte zusammengefasst.

3.1 Vertragstypus

Ein typischer Outsourcing-Vertrag enthält nicht nur die Kernleistung „Überlassung von Software gegen Entgelt“ sondern muss – wie oben ausgeführt – darüber hinausgehende Leistungen umfassen, z.B. Maßnahmen zur Datensicherung, Überwachung der Hardware, Fehlerbeseitigungen und Unterstützungsleistungen (Telefonsupport). Für IT-Outsourcing im Stile des ASP-Konzeptes wurde deshalb in der Vergangenheit ein gemischter Vertrag angenommen, wobei mietvertragliche Elemente im Vordergrund stehen[87]. Miete von Software (auch in der Form des Operating-Leasing) ist rechtlich zulässig und in der Praxis durchaus üblich[88]. Problematisch ist allerdings, dass die Dienste auf den Servern des Dienstleisters laufen und keine vollständige Übertragung der Software zum Auftraggeber und somit keine Besitzüberlassung[89] vorliegt. Die Notwendigkeit einer Besitzüberlassung für Bestandsverhältnisse wird allerdings verneint, wenn dem Nutzer der Zugang zur Bestandsache sowie deren bestimmungsgemäße Nutzung gewährt werden[90]. *Fallenböck/Trappitsch* gehen insofern im Falle von ASP von Software-Miete aus, wobei dies zu eng gefasst ist – die Bestandsache besteht ja nicht nur aus der Software, sondern auch aus der Infrastruktur (Hardware), die zum Betrieb der Software notwendig ist.

Für Cloud Computing stellt sich dies nicht anders dar. Soweit jedoch spezifische Leistungen erfolgen, z.B. eine benutzerspezifische Auswahl von Diensten aus dem Dienstsortiment des Dienstleisters, die Zuordnung von Hardwareressourcen durch Virtualisierung und die gemeinsame Bereitstellung dieser Dienste und der virtualisierten Hardware als Plattform (im Sinne eines „Gesamtpakets“) könnten auch werkvertragliche Elemente enthalten sein (die maßgeschneiderte Plattform bildet das Werk).

Die übrigen Pflichten des Dienstleisters sind nach dem Charakter der Vereinbarung zu beurteilen. So kann die Anfertigung von Sicherungskopien als Werkvertrag (wenn vollständige und fehlerfreie Kopien des Datenbestands geschuldet werden) oder Dienstvertrag (soweit nur das Bemühen um solche Kopien geschuldet ist) gewertet werden.

---

[85] *Vogel* in *Kucsko*, Kommentar zum Urheberrecht § 41a Punkt 5.

[86] *Nieman/Paul*, Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computing, K & R, 2009, 448.

[87] *Fallenböck/Trappitsch*, Application Service Providing (ASP) - rechtlich betrachtet, MR 2002, 3.

[88] *Blocher*, Sonderverträge der Softwareverträge (Teil 1), EDVuR 1994, 5.

[89] *Würth* in *Rummel,* ABGB[3], § 1090 Rz 2.

[90] So *Fallenböck/Trappitsch*, ASP unter Berufung auf BGH NJW-RR 1993, 178.

3.2 Empfohlene Regelungsschwerpunkte

Schon für das klassische IT-Outsourcing wurde die aufgrund des komplexen Sachverhalts notwendige Sorgfalt bei der Vertragsgestaltung zwischen Auftraggeber und Dienstleister thematisiert[91]. Deshalb soll hier ein kurzer Überblick über die zentralen Regelungsschwerpunkte bei Cloud-Dienstleisterverträgen gegeben werden. Aufgrund des anderen Paradigmas (kein Übergang von Hardware, Software, Personal und sonstigen Betriebsmitteln vom Auftraggeber auf den Dienstleister) können für das klassische IT-Outsourcing typische Regelungen entfallen (arbeitsrechtliche Vereinbarungen in Bezug auf Arbeitnehmerübernahme, Hardware- bzw. Software-Kaufverträge).

Zentralen Bestandteil bilden die Vereinbarungen über den Leistungsinhalt, wobei sowohl festgelegt werden sollte, welchen Funktionsumfang die Dienste besitzen (*was*, sog. funktionale Anforderungen) als auch in welcher Qualität die Leistungserbringung zu erfolgen hat (*wie*, sog. nicht-funktionale Anforderungen). Ersteres erfordert eine entsprechend detaillierte Beschreibung der Dienste, um im Streitfall den Inhalt der Schuld bestimmen zu können. Diese Beschreibung kann z.B. in Form einer Systemspezifikation[92], wie sie bei Aufträgen zur Herstellung von Individual-Software regelmäßig angefertigt wird, bestehen. Zumindest sollte sie Qualität eines (weniger detaillierten) Lastenhefts aufweisen.

Für Vereinbarungen über die nicht-funktionalen Anforderungen hat sich der Begriff *Service Level Agreements* (SLA) eingebürgert. Für alle diese gilt, dass unbedingt nachvollziehbare, messbare Größen für die Regelung der Dienstqualität heranzuziehen sind. Die nicht-funktionalen Anforderungen enthalten Zusicherungen über die Leistungsfähigkeit der Dienste (z.B. maximale Zeitdauer für die Abwicklung einer Transaktion, maximale Anzahl gleichzeitiger Transaktionen). Dies schließt auch die so genannten Verfügbarkeitsklauseln ein. Grundsätzlich wird vom Dienstleister die störungsfreie Bereitstellung der Dienste geschuldet[93]. Dass IT-Dienste rund um die Uhr ohne Unterbrechung zur Verfügung stehen, ist auch heute unrealistisch. Es kommt vor, dass diese aufgrund von Fehlern oder notwendiger Wartungsarbeiten deaktiviert werden müssen und sie der Auftraggeber in der Folge nicht nutzen kann („Downtime“). Die Verfügbarkeit sollte daher zwischen den Parteien vereinbart werden, wobei diese typischerweise in Prozent, also z.B. mit 98,5% im Monatsdurchschnitt, angegeben wird. Der OGH erachtete übrigens eine Verfügbarkeit von 92,8% im Jahre 1996 als zu gering[94]. Heute wird – ohne entsprechende Vereinbarungen – eine Verfügbarkeit von zumindest 98% anzunehmen sein, wobei man aufgrund der technischen Möglichkeiten der spezialisierten Dienstleister eventuell sogar höhere Verfügbarkeiten annehmen könnte. Die SLAs sollten darüber hinaus auch die Konsequenzen für Schlechtleistungen regeln – in Betracht kommen dafür z.B. Vertragsstrafen oder die Möglichkeit der Vertragsbeendigung, wenn die Leistung über einen zu definierenden Zeitraum nicht in der bedungenen Qualität erbracht wird.

Cloud Computing folgt primär dem Pay-Per-Use-Prinzip, wenngleich grundsätzlich auch Nutzungspauschalen in Betracht kommen. Daher ist auch unbedingt zu vereinbaren, anhand welcher Größen die Nutzung abgerechnet wird. Diese Größen hängen naturgemäß von der Art des Dienstes ab und können daher auch – bei Nutzung mehrerer Dienste – unterschiedlich sein. Beispiele sind die Anzahl der bearbeiteten Dokumente (bei einer Textverarbeitung als Dienst), Anzahl abgefragter oder geänderter Datensätze (Kundendatenbank) oder auch die Zeitdauer der Nutzung. Dafür sollten jedenfalls Nachweispflichten des Dienstleisters vereinbart werden.

---

[91] *Bartsch*, Typische Regelungsschwerpunkte beim Outsourcing, EDVuR 1993, 42.

[92] Zu den Begriffen Systemspezifikation und Lastenheft siehe u.a. *Heinrich*, Informationsmanagement, 160.

[93] *Fallenböck/Trappitsch*, ASP, 14.

[94] OGH 29. 5. 1996 5 Ob 504/96 = JBl 1997, 458ff; der Branchendurchschnitt lag damals bei 94%.

Der Vertrag sollte ferner die oben erwähnten Pflichten (Dokumentations- und Kontrollsystem, IT-Sicherheit) des Dienstleisters, die Einhaltung der Datenschutzgrundsätze, die Überwälzung etwaiger Geheimhaltungspflichten sowie Haftungsgrundsätze (Vermeidung übermäßiger Haftungsbegrenzungen seitens des Dienstleisters) regeln.

Empfehlenswert sind ferner Regelungen über die Modalitäten der Vertragsbeendigung[95]. Dabei sollten vor allem Mitwirkungspflichten des Dienstleisters bezüglich der Übertragung des Datenbestands zurück zum Auftraggeber (Rückmigration) oder zu einem anderen Dienstleister statuiert werden. Abschließend sei auf die aufgrund der Internationalität der Clouds unbedingt notwendigen Regelungen des anzuwendenden Rechts, etwaige Schiedsvereinbarungen sowie die Vereinbarung eines Gerichtstands verwiesen.

4. AGBs

In diesem Kapitel werden Auszüge aus den AGBs einzelner Cloud-Computing-Dienstleister auf ihre Übereinstimmung mit rechtlichen Anforderungen überprüft und eine Einschätzung vorgenommen, ob die Heranziehung dieser Dienstleister für österreichische Unternehmen ratsam erscheint. Eine solche Studie wurde von Mowbray Anfang 2009 durchgeführt und soll hier – unter Berücksichtigung etwaiger zwischenzeitlicher Änderungen und spezifischer österreichischer Rechtsanforderungen – als Grundlage verwendet werden.

4.1 Google Apps

Google Apps ist der Cloud-Dienst des Internet-Konzerns Google. Über Google werden verschiedene Anwendungen (E-Mail, Textverarbeitung, Tabellenkalkulation, Groupware,…) Unternehmen und Privatkunden angeboten. Auszüge aus den Google Apps Nutzungsbedingungen sind in Anhang A ersichtlich. Im Lichte obiger Ausführungen und der dort genannten Grundsätze erübrigt sich dazu jeglicher Kommentar. Immerhin rühmt sich Google, mittlerweile weltweit über zwei Millionen Unternehmenskunden für seine Dienstleistungen gewonnen zu haben. Ohne die Zulässigkeit und Wirksamkeit dieser Bestimmungen unter dem Aspekt der (noch) zulässigen Gewährleistungsausschlüsse und der Sittenwidrigkeit im Einzelnen diskutieren zu wollen, zeigt sich damit deutlich, dass sich gegenwärtig weder die Auftraggeber (wenn sie tatsächlich zu diesen Bedingungen kontrahieren), noch die Dienstleister der rechtlichen Rahmenbedingungen und ihrer Verantwortung bewusst sind.

4.2 Amazon

Nicht wesentlich anders stellt sich die Situation bei den Cloud-Diensten von Amazon dar. Die Punkte 11.5 und 11.8 der Nutzungsbedingungen enthalten ähnliche Einschränkungen (siehe Anhang B). Immerhin ist sich Amazon bewusst, dass diese Bedingungen nicht in allen Rechtsordnungen Bestand haben und den Kunden zusätzliche Rechte zukommen könnten (Punkt 11.8 vorletzter und letzter Satz). Außerdem gewährt Amazon den Kunden im Falle der Einstellung eines Dienstes (großzügige?) Schonfristen von 5-15 Tagen (begründete Einstellung, Punkt 3.4) bzw. von 60 Tagen (Einstellung ohne Angabe von Gründen, Punkt 3.3.2, beide nicht eigens abgebildet). Dies birgt interessante Feststellungen für den Fall WikiLeaks. Zunächst ist fraglich, ob eine begründete oder unbegründete Einstellung vorliegt. Amazon hat jedenfalls die Nutzung seiner Server für WikiLeaks gestoppt. Es wurde nicht bekannt, ob die Daten zusätzlich gelöscht wurden bzw. ob WikiLeaks die Möglichkeit bekam, die Daten zu migrieren. In diesem speziellen Fall war dies wohl nicht nötig, da bereits Kopien davon verfügbar waren. Dies wird für die meisten Unternehmen allerdings nicht der Normalfall sein.

4.3 Salesforce

Der Cloud-Dienstleister Salesforce.com gewährt in seinen Nutzungsbedingungen zumindest vereinzelte Zusicherungen. So sichert Salesforce seinen Kunden eine Haftungsfreistellung von Urheberrechtsansprüchen Dritter im Zuge der Nutzung der Cloud-Dienste zu (Punkt 10.1), verlangt aber im Gegenzug ähnliche Haftungs-

[95] *Bartsch*, Regelungsschwerpunkte, EDVuR 1993, 42.

freistellungen für Verstöße durch Verhalten des Kunden. Im Gegensatz zu den vorigen Dienstleistern gibt Salesforce eine rudimentäre Funktionsgarantie für seine Dienste ab (siehe Punkt 9.1, Anhang C)

Salesforce sichert also zu, dass die Dienste im Wesentlichen (arg. „materially“) so funktionieren, wie in der Dokumentation angegeben. Im Falle von Verstößen gegen diese Garantien werden allerdings keine Entschädigungsleistungen angeboten, sondern nur die Beendigung des Vertragsverhältnisses mit einer Frist von 30 Tagen ermöglicht und bereits im Voraus geleistete Zahlungen rückerstattet (Punkt 12.3 und 12.4).

4.4 Fazit

Diese ausgewählten Beispiele zeigen, dass die Praxis weit hinter den dargestellten rechtlichen Anforderungen zurückbleibt. Über nachzuweisende Kontroll- und Sicherheitsmaßnahmen des Dienstleisters oder einzuhaltende Sicherheitsstandards, sei es aus datenschutzrechtlicher, unternehmensrechtlicher oder sonstiger Perspektive, findet sich in den Nutzungsbedingungen nichts. Unternehmen, die einen Cloud-Dienstleister zu diesen Bedingungen heranziehen, setzen sich beträchtlichen Risiken aus. Dass faktisch keine Möglichkeit besteht, den Dienstleister zu kontrollieren und die Durchführung der geforderten Maßnahmen zu überwachen, muss den Unternehmern beim Abschluss eines solchen Vertrags klar sein. Er wird somit aufgrund Verschuldens für Schäden haften. Ein „sorgfältiger Unternehmer“ iSd des § 347 UGB wird ein solches Risiko nicht eingehen. Natürlich sei angemerkt, dass diese Beispiele Extreme darstellen. „Kleine“ Cloud-Dienstleister müssen sich bei den Nutzungsbedingungen nachgiebiger zeigen und ebenso wird sich die Situation entschärfen, wenn Auftraggeber und Dienstleister im selben Land ansässig sind, da in diesem Fall manche Verpflichtungen schon von Gesetzes wegen existieren (vgl. z.B. die Grundsätze des § 11 DSG).

Abschließend ist zu jedoch konstatieren, dass die rechtliche Zulässigkeit des Cloud Computings zumindest in der Gegenwart wohl eher eine Frage der Marktmacht der Auftraggeber ist. Große Unternehmen mögen in der Lage sein, mit den Dienstleistern Individualvereinbarungen zu schließen, die den rechtlichen Rahmenbedingungen entsprechen. So wie es einem österreichischen Kunden schwer fallen wird, mit seinem Stromlieferanten einen Individualvertrag anstelle der Standard-AGB-Verträge abzuschließen, wird ein österreichisches Klein- bzw. Mittelunternehmen wohl kaum in der Lage sein, großen Anbietern wie Microsoft, Google oder Amazon über deren AGBs hinausgehende Bedingungen zu „diktieren“ (besondere zu ergreifende Maßnahmen, Kontrollrechte, Nachweispflichten). Es bleibt somit nur, die AGB auf ihre rechtliche Konformität zu analysieren und den Dienstleister danach auszuwählen.

Damit Cloud Computing für die – oftmals als Kernzielgruppe der Clouds genannten – Klein- und Mittelbetriebe nicht nur wirtschaftlich sinnvoll, sondern auch rechtlich unbedenklich wird, bedarf es weiterer Initiativen. Dieser Bedarf wird teilweise schon erkannt. Eine Lösung wird in der Schaffung gesetzlicher Grundlagen für die Rechte und Pflichten von Auftraggebern und Dienstleistern gesehen. So wird in den USA die Forderung nach einem „Cloud-Computing-Act“ erhoben[96]. Geht man von der Asymmetrie im Verhältnis zwischen einem großen Cloud-Dienstleister und einem kleinen Auftraggeber aus, so hat diese Argumentation einiges für sich. Nicht übersehen werden darf dabei freilich, dass aufgrund der Internationalität der Clouds Regelungen einzelner Staaten das Problem nicht entschärfen werden. Dies betrifft insbesondere auch die Problematik der Rechtsdurchsetzung über Staatsgrenzen hinweg. Wer den Einsatz von Cloud Computing ernsthaft erwägt, sollte neben den Vorteilen in jedem Fall

[96] Rede von B. Smith (General Counsel Microsoft Corp.) anlässlich des Brookings Institution Policy Forum “Cloud Computing for Business and Society”, Building Confidence in the Cloud: The Need for Prompt Industry and Government Action for Cloud Computing , Washington D.C, 20.1.2010.

alle Risiken berücksichtigen und explizit abwägen[97].

5. Zusammenfassung

Um beurteilen zu können, ob Cloud Computing im Hinblick auf diese Anforderungen und Grundsätze zulässig ist, wurden die rechtlich relevanten Vorgänge beim Cloud Computing und dabei entstehende rechtliche Probleme dargestellt. Als Ergebnis ist festzuhalten, dass Cloud Computing nicht grundsätzlich unzulässig ist, dass aber in Bezug auf spezielle Problematiken v.a. vertragliche Vorkehrungen getroffen werden müssen. Für die Vertragsgestaltung muss deshalb entsprechende Sorgfalt aufgewendet werden.

Die Analyse der Dienstleister-AGBs und auch der Fall WikiLeaks haben gezeigt, dass diese Sorgfalt in der Praxis häufig unterbleibt. Da gerade kleine und mittlere Unternehmen nicht in der Lage sein werden, großen Dienstleistern die notwendigen Verpflichtungen aufzuoktroyieren, kommt für sie Cloud Computing gegenwärtig nicht in Betracht. Da jedoch viele solcher Unternehmen diese Dienste bereits nutzen und sich Cloud Computing zumindest momentan als ein unaufhaltsamer Trend darstellt, erscheint ein Tätigwerden der Gesetzgeber empfehlenswert (möglicherweise in Form eines internationalen Zertifizierungssystems für Cloud-Dienstleister). Damit könnte Rechtssicherheit sowohl für Auftraggeber als auch für Cloud-Dienstleister geschaffen werden.

6. Literatur

Andresen, Über die Wolken – Rechtsfragen des Cloud Computings, Linux-Magazin, 2010, 84.

Armbrust et al., A Berkeley View of Cloud Computing, Technical Report, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf (12.1.2011).

Bartsch, Typische Regelungsschwerpunkte beim Outsourcing, EDVuR 1993.

Blocher, Sonderverträge der Softwareverträge (Teil 1), EDVuR 1994.

Buxmann et al., Software as a Service, Wirtschaftsinformatik, 6/2008, 500.

Dohr/Pollirer/Weiss, DSG[2], Manz (2009).

Donner, Ordnungsgemäßheit und Sicherheit von Informationssystemen (Teil I), VWT 2003, 55.

European Network and Information Security Agency (ENISA), Security & Resilience in Governmental Clouds – Making an informed decision, 2011.

Fallenböck/Trappitsch, Application Service Providing (ASP) - rechtlich betrachtet, MR 2002, 3.

Feltl/Pucher, Corporate Compliance im österreichischen Recht – Ein Überblick, wbl 2010, 265.

Geist in *Jabornegg,* Kommentar zum HGB § 189 Rz 32, Springer (1997).

Gerick, Software-Lizenzmanagement: Risiken und Kosten minimieren, CFOaktuell 2009, 260.

Grabenwarter, Datenschutzrechtliche Anforderungen an den Umgang mit Kundendaten im Versandhandel, ÖJZ 2000, 861.

Hall/Liedtka, The Sarbanes-Oxley Act: Implications for Large-scale IT Outsourcing, Communications of the ACM, 3/2007, 95.

Hasberger, IT-Sicherheit und Haftung, ecolex 2007, 509.

Heinrich, Informationsmanagement[7], Oldenbourg (2002).

E. Holzinger, Rechtsgeschäftliche Übertragung von Software – Versuch einer systematischen Einordnung, EDVuR 1987, 10.

Jahnel, Das Datenschutzgesetz 2000 - Wichtige Neuerungen, wbl 2000, 49.

Knyrim/Siegel/Autengruber, Datenschutz und Datenrettung beim Outsourcing, ecolex 2004, 413.

Krejci, Gesellschaftsrecht I, Manz (2005).

Kreuzer, Compliance, CFOaktuell 2009, 205.

Kreuzer, IKS – Internes Kontrollsystem, CFOaktuell, 2010.

Laimer/Mayr, Zum Spannungsverhältnis von Arbeitgeber- und Arbeitnehmerinteressen rund um die EDV-Nutzung, RdA, 410.

Lechner/Egger/Schauer, Einführung in die Allgemeine Betriebswirtschaftslehre[19], Linde (2001).

Lechner in *Straube,* HGB online § 273 Rz 26 ff, Manz (2006).

Leissler, Und die Daten fließen über den Atlantik ..., ecolex 2007, 747.

Mäder, Application Service Providing - Chancen und Risiken, ZfCM, 2007, 181.

Nieman/Paul, Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computing, K & R 2009, 448.

[97] Siehe dazu auch *ENISA*, Security & Resilience in Governmental Clouds – Making an informed decision, 2011.

Rath, Rechtliche Aspekte von IT-Compliance, In: Wecker/van Laak (Hrsg.), Compliance in der Unternehmenspraxis, Springer (2008).

Rath, Rechtliche Aspekte von IT-Compliance[2], In: Wecker/van Laak(Hrsg.)[2], Compliance in der Unternehmenspraxis, Springer (2009).

Reimoser, Das neue Fachgutachten KFS/DV2 "Abschlussprüfung bei Einsatz von Informationstechnik", - Auswirkungen auf die Abschluss- und IT-Prüfung, VWT 2005, 12.

Rüter et al., IT-Governance in der Praxis, Springer (2006).

Schauer in *Krejci,* Reformkommentar UGB § 347, Manz (2007).

Schulzki-Haddouti, Cloud Computing: Der Datenschutz verdampft, http://futurezone.orf.at/stories/1639608/ (4.09.2010)

Schumacher in *Kucsko*, Kommentar zum Urheberrecht, Manz (2007).

Skillikorn, The Case for Datacentric Grids, Proceedings of the International Parallel and Distributed Processing Symposium 2002, 5.

Sommerville, Software Engineering[8], Addison-Wesley (2007).

Stanonik, Trotz Wirtschaftskrise: Beim Outsourcing gilt es, den Datenschutz zu beachten!, ecolex 2009, 845.

Staudegger, Zur Qualifikation von Verträgen, die der Überlassung von Computersoftware dienen, JBl 1998, 604.

Strasser in *Jabornegg/Strasser,* AktG II[5] §§ 77 bis 84, Manz (2010).

Straube/U.Torggler in *Straube,* HGB online Vorbemerkungen vor § 189, Manz (2006).

Souhrada-Kirchmayer, Das Datenschutzgesetz 2000, SozSi 1999, 938.

Takabi et al., Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, Vol. 8, No. 6, Nov./Dec. 2010.

Teubner/Feller, Informationstechnologie, Governance und Compliance, Wirtschaftsinformatik, 5/2008, 400.

H.Torggler/U.Torggler in *Straube,* HGB online § 189, Manz (2006).

Vogel in *Kucsko*, Kommentar zum Urheberrecht, § 41a, Manz (2007).

Weber, Das Unternehmensrechts-Änderungsgesetz 2008 im Überblick, ÖJZ 2008, 435.

Weinhardt et al., Cloud-Computing – Eine Abgrenzung, Geschäftsmodelle und Forschungsgebiete, Wirtschaftsinformatik 2009, 453.

Wiebe/Appl, Urheberrechtliche Zulässigkeit des Erwerbs von "gebrauchten" Softwarelizenzen in Österreich, MR 2007, 186.

Wimmers, Darf ich das? Urheberrechtliche Probleme beim IT-Outsourcing, In: Büchner/Dreier, Von der Lochkarte zum globalen Netzwerk – 30 Jahre DGRI (2007).

Würth in *Rummel,* ABGB[3], § 1090, Manz (2000).

Zahradnik, Corporate Governance – Haftungsfragen, GeS, 2002, 59.

7. Anhang A. Google AGB

Auszüge aus http://www.google.com/apps/intl/de/terms/user_terms.html

9. ÄNDERUNGEN AM SERVICE

Google behält sich jederzeit das Recht vor, Google-Services (oder Teile davon) mit oder ohne Ankündigung vorübergehend oder dauerhaft zu ändern, auszusetzen oder insgesamt einzustellen. Sie stimmen zu, dass Google in keinem Fall Ihnen oder Dritten gegenüber für das Ändern, Aussetzen oder Einstellen von Google-Services haftbar ist.

10. BEENDIGUNG

Sie können die Nutzung der Google-Services jederzeit einstellen. Sie stimmen zu, dass Google jederzeit und ohne Angabe von Gründen, auch bei einer bestimmten Zeit der Inaktivität, Ihren Zugriff auf die Google-Services beenden, die Bedingungen kündigen oder Ihr Konto vorübergehend sperren oder beenden kann. Im Fall der Beendigung wird Ihr Konto deaktiviert und Sie verlieren den Zugriff auf die Google-Services, Ihr Konto sowie sämtliche Dateien oder anderen Inhalt in Ihrem Konto.

Damit ist die Nutzung von Google Apps für sämtliche buchungsrelevante Zwecke (z.B. Erstellung und Speicherung von Rechnungen) faktisch ausgeschlossen. Jedes Dokument, das z.B. mit Google Docs erstellt wird, müsste daher lokal gespeichert und dessen Lesbarkeit sichergestellt werden. Interessant sind weiter die Punkte 13, 14 und 15 (die Punkte 14 und 15 sind auch im Original in Majuskeln geschrieben):

13. HAFTUNGSFREISTELLUNG

Sie sind verpflichtet, Google und zugehörige Zweigunternehmen, Führungskräfte, Vertreter, Angestellten, Inserenten, Lizenzgeber, Lieferanten und Partner (im Folgenden "Google und seine Partner") im Hinblick auf Ansprüche, die von Dritten im Zusammenhang mit Ihrer Nutzung der Google-Services, der Verletzung der Bedingungen oder anderen Aktionen in Zusammenhang mit der Nutzung der Google-Services erhoben werden, schadlos zu halten und von der Haftung freizustellen, einschließlich sämtlicher Verpflichtungen und Aufwendungen im Zusammenhang mit Ansprüchen, Verlusten (unmittelbaren Schäden und Folgeschäden), Gerichtsverfahren, Urteilen, Kosten der Rechtsverfolgung und Anwaltskosten. Sollte dieser Fall eintreten, wird Google Ihnen dies schriftlich mitteilen.

14. GEWÄHRLEISTUNGSAUSSCHLUSS

SIE STIMMEN AUSDRÜCKLICH ZU, DASS

a. …

b. GOOGLE UND SEINE PARTNER NICHT GARANTIEREN, DASS (i) DIE GOOGLE-SERVICES IHREN ANFORDERUNGEN ENTSPRECHEN, (ii) DIE GOOGLE-SERVICES UNUNTERBROCHEN, JEDERZEIT VERFÜGBAR, SICHER ODER FEHLERFREI SIND, (iii) DIE ÜBER DIE NUTZUNG DER GOOGLE-SERVICES ERHALTENEN ERGEBNISSE ZUTREFFEND UND ZUVERLÄSSIG SIND, (iv) DIE QUALITÄT DER VON IHNEN ÜBER DIE GOOGLE-SERVICES ERWORBENEN ODER ERHALTENEN PRODUKTE, SERVICES, INFORMATIONEN ODER SONSTIGEN MATERIALIEN IHREN ERWARTUNGEN ENTSPRICHT, UND (V) FEHLER IN DER SOFTWARE KORRIGIERT WERDEN.

15. HAFTUNGSBESCHRÄNKUNG

SIE STIMMEN AUSDRÜCKLICH ZU, DASS GOOGLE UND SEINE PARTNER IHNEN GEGENÜBER NICHT HAFTBAR SIND FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, SPEZIELLE, EXEMPLARISCHE SCHÄDEN ODER FOLGESCHÄDEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN INFOLGE VON ENTGANGENEM GEWINN, VERLUST VON GOODWILL, NUTZUNG, DATEN ODER ANDERE IMMATERIELLE VERLUSTE (AUCH WENN GOOGLE ODER SEINE PARTNER AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDEN) ALS FOLGE VON: (i) DER NUTZUNG ODER NICHTVERWENDBARKEIT VON GOOGLE-SERVICES; (ii) DEN KOSTEN FÜR DIE BESCHAFFUNG VON ERSATZWAREN UND -SERVICES, DIE DURCH DEN ERWERB ODER DEN ERHALT VON WAREN, DATEN, INFORMATIONEN ODER SERVICES, DEN ERHALT VON NACHRICHTEN ODER IN BZW. ÜBER GOOGLE-SERVICES EINGEGEBENE TRANSAKTIONEN ENTSTANDEN SIND; (iii) UNBERECHTIGTEM ZUGRIFF AUF IHRE TRANSAKTIONEN ODER IHRE DATEN ODER DIE UNBERECHTIGTE ÄNDERUNG AN DIESEN; (iv) AUSSAGEN ODER DEM VERHALTEN VON DRITTANBIETERN BEZÜGLICH DER GOOGLE-SERVICES; ODER (v) EINER ANDEREN ANGELEGENHEIT IN ZUSAMMENHANG MIT GOOGLE-SERVICES.

8. Anhang B. Amazon AGB

Auszüge aus http://aws.amazon.com/agreement

1.5. Disclaimers

WE AND OUR LICENSORS DO NOT WARRANT THAT THE SERVICE OFFERINGS WILL FUNCTION AS DESCRIBED, WILL BE UNINTERRUPTED OR ERROR FREE, OR FREE OF HARMFUL COMPONENTS, OR THAT THE DATA YOU STORE WITHIN THE SERVICE OFFERINGS WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. WE AND OUR LICENSORS SHALL NOT BE RESPONSIBLE FOR ANY SERVICE INTERRUPTIONS, INCLUDING, WITHOUT LIMITATION, POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS, INCLUDING THOSE THAT AFFECT THE RECEIPT, PROCESSING, ACCEPTANCE, COMPLETION OR SETTLEMENT OF ANY PAYMENT SERVICES. NO ADVICE OR INFORMATION OBTAINED BY YOU FROM US OR FROM ANY THIRD PARTY OR THROUGH THE SERVICES SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT.

11.8. Limitations of Liability

NEITHER WE NOR ANY OF OUR LICENSORS SHALL BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA OR OTHER LOSSES (EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) IN CONNECTION WITH THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, ANY SUCH DAMAGES RESULTING FROM: (i) THE USE OR THE INABILITY TO USE

THE SERVICES; (ii) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS AND SERVICES; OR (iii) UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR CONTENT. IN ANY CASE, OUR AGGREGATE LIABILITY UNDER THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT ACTUALLY PAID BY YOU TO US HEREUNDER FOR THE SERVICES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCORDINGLY, SOME OR ALL OF THE ABOVE EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU, AND YOU MAY HAVE ADDITIONAL RIGHTS.

9. Anhang C. Salesforce AGB

Auszüge aus http://www.salesforce.com/company/msa.jsp

9.1. Our Warranties.

We warrant that (i) the Services shall perform materially in accordance with the User Guide, and (ii) subject to Section 5.3 (Google Services; Anm: Salesforce nutzt selbst Google Services zur Erbringung seiner Dienstleistungen), the functionality of the Services will not be materially decreased during a subscription term. For any breach of either such warranty, Your exclusive remedy shall be as provided in Section 12.3 (Termination for Cause) and Section 12.4 (Refund or Payment upon Termination) below.