FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Marktanalyse und Vorgehensmodell für den betrieblichen Einsatz von Cloud Computing unter besonderer Berücksichtigung rechtlicher Aspekte

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Walter Hötzendorfer, BSc
Matrikelnummer 0425631

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer: O.Univ.-Prof. Dr. A Min Tjoa
DDr. Alexander Hampel

Wien, 08.10.2010

(Unterschrift Verfasser) (Unterschrift Betreuer)

Erklärung zur Verfassung der Arbeit

Walter Hötzendorfer, BSc
Hermanngasse 2a/II
1070 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, am 08.10.2010 Walter Hötzendorfer, BSc

Kurzfassung

Cloud Computing ist ein Konzept, das die Nutzung von skalierbaren IT-Infrastrukturen, Plattformen und Anwendungen ermöglicht, die on-demand über das Internet bezogen und nutzungsabhängig abgerechnet werden. Der Untersuchungsgegenstand der Diplomarbeit ist auf Public Clouds beschränkt, die im Gegensatz zu Private Clouds von einem Anbieter für eine große Zahl von Kunden betrieben werden. Die zugrundeliegende Infrastruktur wird somit von vielen Kunden gemeinsam genutzt. Die Arbeit untersucht die Einsatzmöglichkeiten von Cloud Computing in österreichischen Unternehmen und bezieht dabei IT-strategische und rechtliche Aspekte sowie die aktuelle Marktsituation mit ein. Zunächst werden Cloud Computing und dessen verschiedene Ausprägungen sowie verwandte Begriffe definiert. Dabei wird deutlich, dass Cloud Computing kein völlig neuer Ansatz ist, sondern sich aus bestehenden Konzepten entwickelt hat. Ein Schwerpunkt liegt dann auf der Aufarbeitung der rechtlichen Rahmenbedingungen des Cloud Computing in Österreich, insbesondere des Datenschutzrechts. Dieses kann in bestimmten Fällen die Einsatzmöglichkeiten von Cloud-Services erheblich einschränken. Nach IT-strategischen Überlegungen pro und contra Cloud Computing werden ausgewählte, auf dem Markt befindliche Cloud-Services untersucht. Dies umfasst eine Beschreibung der Angebote sowie eine Analyse der Vertragsbedingungen und sonstiger relevanter Kriterien. Aus diesen und den davor gewonnenen theoretischen Erkenntnissen wird anschließend ein Vorgehensmodell für die Entscheidungsfindung hinsichtlich der Nutzung von Cloud Computing abgeleitet. Dieses bildet eine systematische Zusammenstellung der Ergebnisse der Arbeit und kann somit von österreichischen Unternehmen verwendet werden, um – unter Einbeziehung ihrer individuellen Gegebenheiten – geeignete Einsatzmöglichkeiten für Cloud-Services zu ermitteln. Im darauffolgenden Kapitel wird dies für mehrere prototypische Klassen von Unternehmen exemplarisch durchgeführt. Abschließend wird ein Testprojekt vorgestellt, das im Rahmen der Diplomarbeit durchgeführt wurde, um Erfahrungen im praktischen Einsatz von Cloud-Services zu gewinnen.

Schlagwörter: Cloud Computing, Cloud-Service, IT-Strategie, explorative Marktanalyse, Vorgehensmodell, Recht, Vertragsbedingungen, Datenschutz

Abstract

Cloud computing is a concept for the provision of scalable IT infrastructure, platforms and applications that are used on-demand over the internet and billed by usage. The object of study of this master thesis is limited to public clouds which unlike private clouds are offered by a provider to a large number of customers, who consequently share the underlying infrastructure. The thesis analyzes the corporate use of cloud computing from an IT strategy point of view as well as its legal conditions and the current market situation from the perspective of Austrian companies as (potential) users of cloud services. At first, cloud computing, its various manifestations and related concepts are defined. It is shown that cloud computing is not something completely new, but has been developed from existing concepts. The following chapter deals with the legal conditions governing cloud computing in Austria, in particular with the Austrian Data Protection Act. Under certain circumstances data protection law can considerably restrict the use of cloud computing. After the discussion of IT strategic considerations concerning the strengths and weaknesses of cloud computing selected cloud services on the market are investigated. Descriptions of the services are given and their contract terms as well as further conditions important for deciding whether to use the services are analyzed. These findings as well as the results of the theoretical chapters are systematically aggregated into a procedure model for decision making on the corporate use of cloud-services, which is the major result of the thesis. Austrian companies can apply this model to support their decision making on the use of cloud-services. Based on the procedure model possible applications of cloud-services in different types of companies are evaluated. Finally, the last chapter presents a test project which was developed and implemented to gain experience in using cloud-services.

Keywords: cloud computing, cloud service, IT strategy, explorative market analysis, procedure model, law, contract terms, data protection

Vorwort und Danksagung

Dem Thema Cloud Computing wird derzeit in der IT-Branche und insbesondere in der Fachpresse beträchtliche Aufmerksamkeit zuteil. In der Unternehmenspraxis scheint Cloud Computing aber bisher nicht jene Bedeutung gewonnen zu haben, die Medien und Marketing vermuten lassen. Die vorliegende Diplomarbeit widmet sich daher der Frage, wie Cloud Computing in österreichischen Unternehmen eingesetzt werden kann, und den Entscheidungskriterien, die in diesem Zusammenhang relevant sind. Dies sind technische, wirtschaftliche und juristische Kriterien. Die vorliegende Diplomarbeit ist somit eine interdisziplinäre Arbeit an der Schnittstelle dieser drei Fachgebiete. Neben dem Studium der Wirtschaftsinformatik qualifiziert mich dazu das Studium der Rechtswissenschaften an der Universität Wien, das ich ebenfalls noch im Jahr 2010 abschließen werde.

Für die gemeinsame Entwicklung der Idee zu diesem Diplomarbeitsthema möchte ich meinem Betreuer, DDr. Alexander Hampel, meinen Dank aussprechen. Ebenso möchte ich all jenen Menschen danken, ohne deren Unterstützung das Verfassen dieser Diplomarbeit nicht möglich gewesen wäre. Mein herzlicher Dank gilt den Betreuern der vorliegenden Arbeit, DDr. Alexander Hampel und o.Univ.-Prof. Dr. A Min Tjoa für die gute Zusammenarbeit, das ideale Verhältnis von professioneller Betreuung und persönlichem Freiraum beim Verfassen der Arbeit und ihre hohe Flexibilität, insbesondere in der Abschlussphase.

Ganz besonders danke ich MMag. Susanne Oberpeilsteiner für ihre einzigartige Unterstützung und ihr Verständnis während meiner gesamten Studienzeit sowie während des Verfassens der Diplomarbeit und für das Korrekturlesen der Arbeit, das sie so hervorragend beherrscht.

Roman Fenkhuber danke ich für die gemeinsame Planung und Umsetzung des in Kapitel 7 vorgestellten Testprojekts. Ohne seinen Enthusiasmus, Neues auszuprobieren, seinen unermüdlichen Arbeitseinsatz und seine umfassenden Fachkenntnisse wäre dieses Testprojekt nicht durchführbar gewesen.

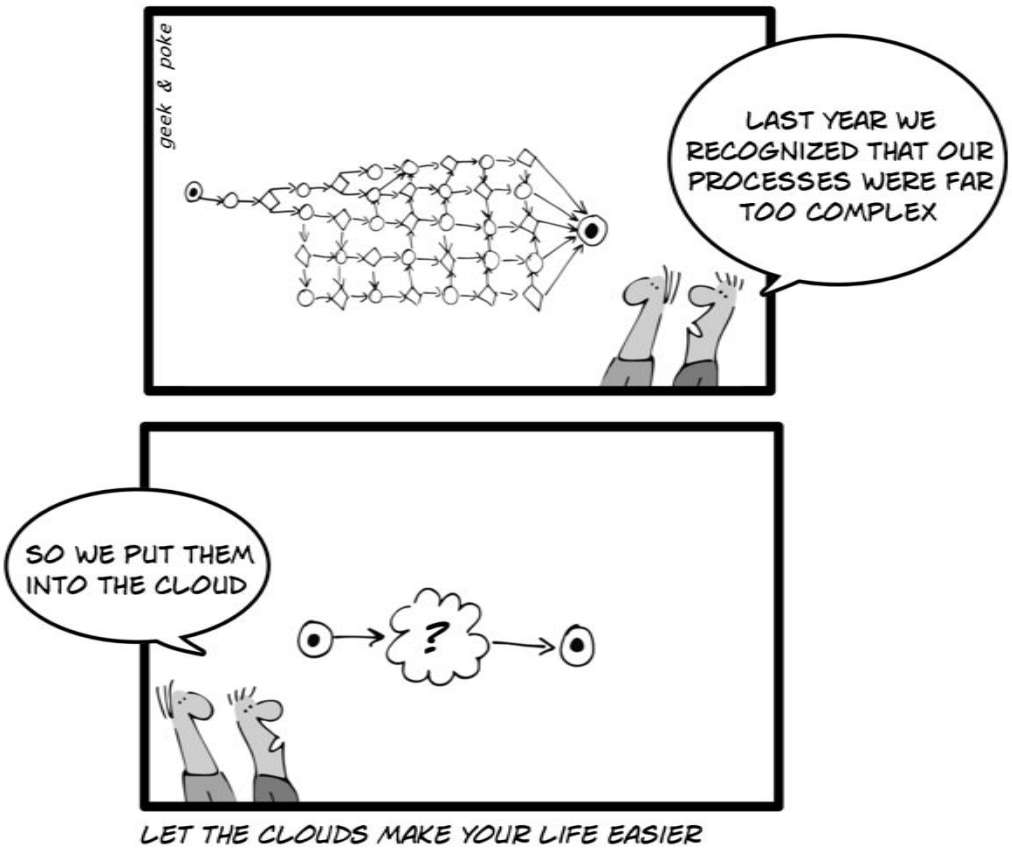
Mein Dank gilt auch Dr. Axel Anderl, LLM der mir als Ansprechpartner in juristischen Fragen zur Verfügung stand.

Meinen Eltern danke ich ganz besonders dafür, dass sie mich immer unterstützt haben, in allem, was ich machen wollte, und mir ermöglicht haben, in Wien zwei Studien zu absolvieren. Darüber hinaus bedanke ich mich auch bei allen anderen, die mich während meines Studiums unterstützt haben, insbesondere bei den Freunden, die ich an der TU Wien kennengelernt habe und die mit mir gemeinsam als unvergessliches

Team während des Wirtschaftsinformatikstudiums so viele spannende Herausforderungen gemeistert haben.

An dieser Stellte sei angemerkt, dass die vorliegende Diplomarbeit individuelle rechtsanwaltliche Beratung nicht ersetzten will und nicht ersetzen kann. Jegliche Haftung für alle juristischen und sonstigen Angaben in der vorliegenden Arbeit wird ausgeschlossen.

Darüber hinaus sei ausdrücklich darauf hingewiesen, dass sich alle personenbezogenen Formulierungen in der vorliegenden Arbeit grundsätzlich gleichermaßen auf Frauen und Männer beziehen.



Im Gegensatz zu diesem Beispiel haben noch nicht alle herausgefunden, wie sie Cloud Computing sinnvoll einsetzen können.
(Quelle: http://geekandpoke.typepad.com/.a/6a00d8341d3df553ef01156f3f1664970b-pi)

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ABGB	Allgemeines bürgerliches Gesetzbuch
ABl	Amtsblatt
Abs.	Absatz
AktG	Aktiengesetz
Arg.	Argument
Art	Artikel
ASP	Application Service Providing/Application Service Provider
AWS	Amazon Web Services
BCR	Binding Corporate Rules
BGBl	Bundesgesetzblatt
BHG	Bundesgerichtshof
BITKOM	[deutscher] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BSc	Bachelor of Science
BWG	Bankwesengesetz
bzgl.	bezüglich
bzw.	beziehungsweise
CPU	Central Processing Unit
CRM	Customer-Relationship-Management
d.h.	das heißt
dBDSG	deutsches Bundesdatenschutzgesetz
dRGBl	deutsches Reichsgesetzblatt
DSAV	Datenschutzangemessenheits-Verordnung
DSG 2000	Datenschutzgesetz 2000
DSK	Datenschutzkommission
DS-RL	Datenschutzrichtlinie
EBS	[Amazon] Elastic Block Storage
EC2	[Amazon] Elastic Compute Cloud
EC-RL	E-Commerce-Richtlinie
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGVVO	Europäische Gerichtsstands- und Vollstreckungsverordnung
EUR	Euro
EVÜ	Europäisches Schuldvertragsübereinkommen
EWR	Europäischer Wirtschaftsraum

f.	und der/die folgende
FAQ	Frequently Asked Questions
ff.	und die folgenden
FMA	Finanzmarktaufsichtsbehörde
Fn.	Fußnote
GB	Gigabyte
GBP	Pfund Sterling
gem.	gemäß
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	GmbH-Gesetz
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
idF	in der Fassung
IEC	International Electrotechnical Commission
IKS	internes Kontrollsystem
IP	Internet Protocol
IPR	Internationales Privatrecht
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Informationstechnologie/Information Technology
iVm	in Verbindung mit
JGS	Justizgesetzessammlung
JN	Jurisdiktionsnorm
KMU	kleine und mittlere Unternehmen
lit	litera (Buchstabe)
MiFID	Markets in Financial Instruments Directive
NAS	Network Attached Storage
NIST	[U.S.] National Institute of Standards and Technology
o.Ä.	oder Ähnliche(s)
o.J.	ohne Jahr
o.O.	ohne Ort
OeNB	Oesterreichische Nationalbank
OGH	Oberster Gerichtshof
PaaS	Platform as a Service
RDP	Remote Desktop Protocol

RGBl	Reichsgesetzblatt
RL	Richtlinie
Rom-I-VO	Rom-I-Verordnung
RTMP	Real Time Messaging Protocol
Rz.	Randzahl
S.	Seite
S3	[Amazon] Simple Storage Service
SaaS	Software as a Service
SAS 70	Statement on Auditing Standards No. 70
SOX	Sarbanes-Oxley Act
SQS	[Amazon] Simple Queue Service
SSH	Secure Shell
StMV 2004	Standard- und Muster-Verordnung 2004
TB	Terabyte
u.a.	unter anderem
UC	University of California
URÄG 2008	Unternehmensrechts-Änderungsgesetz 2008
URL	Uniform Resource Locator
USD	US-Dollar
VAG	Versicherungsaufsichtsgesetz
vgl.	vergleiche
VO	Verordnung
VPN	Virtual Private Network
WAG	Wertpapieraufsichtsgesetz
Z	Ziffer
z.B.	zum Beispiel

1. Einleitung

"The buzz around cloud computing has reached a fever pitch. Some believe it is a disruptive trend representing the next stage in the evolution of the Internet. Others believe it is hype, as it uses long established computing technologies. As with any new trend in the IT world, organizations must figure out the benefits and risks of cloud computing and the best way to use this technology."[1]

1.1. Problemstellung

Das Grundprinzip von Cloud Computing ist, unternehmensinterne IT-Infrastruktur durch on-demand-Services zu ergänzen bzw. zu ersetzen. In ähnlicher Weise, wie ein Unternehmen den benötigten Strom von einem Elektrizitätsversorger bezieht, anstatt ihn durch eigene Generatoren zu produzieren, können mittels Cloud Computing Speicherplatz, Rechenleistung, vollständige Software-Anwendungen und ähnliche Services von entsprechenden Anbietern über das Internet bezogen werden.

Mit dieser Beschreibung kann der Begriff Cloud Computing – dem Verständnis folgend, das der vorliegenden Diplomarbeit zugrundeliegt – vorerst knapp umrissen werden. Doch dieses Begriffsverständnis ist keineswegs allgemeingültig. Im Gegenteil, viele verschiedene, zum Teil bereits etablierte Konzepte werden – von aufstrebenden wie auch von etablierten Unternehmen – zunehmend mit dem Begriff „Cloud Computing" versehen.[2] Daher ist es zunächst nötig, Cloud Computing und verwandte Begriffe zu definieren und Grundbegriffe festzuhalten.

Cloud Computing ist in Mode. Es ist gegenwärtig eines der meistdiskutierten Themen der IT-Branche.[3] Jedoch zeichnet sich bereits ab, dass die Bedeutung des Cloud Computing über jene einer vorübergehenden Modeerscheinung hinausgehen könnte, wie dies beispielsweise *The Economist* prognostiziert: „The concept of computing as a basic utility delivered over the internet is here to stay."[4] Ob diese Prognose zutrifft, und ob dieses Konzept dann nach wie vor als „Cloud Computing" bezeichnet wird, oder zur Selbstverständlichkeit geworden ist, für die es keines speziellen Namens mehr bedarf, kann aus der Sicht des Autors erst in mehreren Jahren mit Gewissheit festgestellt werden.

Der Euphorie rund um Cloud Computing stehen derzeit aufseiten potenzieller Nutzer Unsicherheiten, insbesondere hinsichtlich der Sicherheit und Zuverlässigkeit,

---

1 Aus der Einleitung des Open Cloud Manifesto (Open Cloud Manifesto Discussion Group 2009, 1).
2 Berlich 2010, 37.
3 Marwan 2010.
4 The Economist 2010, 64.

gegenüber.[5] Die dauerhafte Etablierung des Konzepts Cloud Computing in der IT-Branche hängt unter anderem wesentlich davon ab, inwieweit diese Unsicherheiten ausgeräumt werden können. Um tatsächlich eingesetzt zu werden, muss Cloud Computing einerseits ausreichend Nutzen stiften und darf andererseits keine zu großen Risiken mit sich bringen. Daraus ergeben sich die wesentlichen Fragestellungen der vorliegenden Diplomarbeit: Welcher Nutzen kann für Unternehmen aus dem Einsatz von Cloud Computing generiert werden? Welche Risiken sind damit verbunden? Für welche betrieblichen Anwendungsfälle ist Cloud Computing geeignet und für welche nicht? Was ist beim Einsatz von Cloud Computing zu beachten?

1.2. Zielsetzung und Aufbau der Arbeit

Ziel der vorliegenden Diplomarbeit ist es, einen Leitfaden zum praktischen Einsatz von Cloud-Services in österreichischen Unternehmen zu erstellen, welcher die IT-strategische Entscheidungsfindung unterstützt und zur Klärung der gestellten Forschungsfragen beiträgt.

Die Basis dieses Vorhabens bildet Kapitel 2, in dem mehrere Definitionen des Begriffs Cloud Computing vorgestellt und ein eindeutiges Verständnis des Begriffs als Grundlage der vorliegenden Arbeit herausgearbeitet wird. Dies schließt eine detaillierte Beschreibung wichtiger Eigenschaften und verschiedener Erscheinungsformen des Cloud Computing mit ein. Darüber hinaus werden verwandte Begriffe definiert und deren Zusammenhang mit Cloud Computing erläutert.

Zwei weitere theoretische Kapitel legen anschließend wesentliche Grundlagen der Entscheidungsfindung über den Einsatz von Cloud Computing dar: In Kapitel 3 werden die rechtlichen Rahmenbedingungen des Cloud Computing aufgearbeitet. Daraus ergeben sich einerseits mögliche Risiken des Cloud Computing und andererseits zeichnen sich bereits geeignete und weniger bzw. nicht geeignete – weil rechtlich unzulässige – Einsatzgebiete ab. Kapitel 4 behandelt IT-strategische Überlegungen zum Cloud Computing, insbesondere dessen Stärken und Schwächen. Es dient damit ebenfalls der späteren Klärung der Frage, für welche Anwendungsfälle der Einsatz von Cloud-Services geeignet ist, beantwortet insbesondere die Frage nach dem Nutzengewinn durch Cloud Computing und zeigt weitere Risiken auf. In diese Darstellung der Schwächen bzw. Risiken fließen auch die Ergebnisse der rechtlichen Überlegungen aus Kapitel 3 ein.

Dieser umfassenden Darstellung der theoretischen Entscheidungsgrundlagen folgt in Kapitel 5 eine explorative Marktanalyse, in welcher bedeutende, auf dem Markt befindliche Cloud-Services untersucht werden. Dies umfasst eine Beschreibung der

[5] Siehe dazu Studien wie beispielsweise CA Technologies 2010 und Velte, Velte und Elsenpeter 2009, 35.

Angebote und eine Analyse der Vertragsbedingungen sowie sonstiger Kriterien, die für die Entscheidungsfindung bzgl. der Nutzung relevant sind. Als Quelle dient dabei primär die Website des jeweiligen Anbieters, auf welcher – dem Kriterium des „on-demand self-serivce“[6] entsprechend – auch die Vertragsbedingungen zu finden sind.

Im sechsten Kapitel werden dann die Schlussfolgerungen aus allen vorangehenden Kapiteln der Arbeit gezogen. Dies erfolgt im Rahmen eines Vorgehensmodells zur Entscheidungsfindung über den Einsatz von Cloud Computing in österreichischen Unternehmen. Kern dieses Vorgehensmodells ist ein Kriterienkatalog für die Entscheidungsfindung bzgl. der Nutzung von Cloud-Services. Mit Hilfe des Vorgehensmodells wird anschließend für mehrere prototypische Klassen von Unternehmen die Frage nach geeigneten betrieblichen Anwendungsfällen verschiedener Cloud-Services beantwortet. Kapitel 6 führt somit die Ergebnisse der Arbeit systematisch zusammen und unterstützt österreichische Unternehmen bei der Entscheidungsfindung über die Nutzung von Cloud Computing.

Abschließend wird in Kapitel 7 ein Testprojekt vorgestellt, in welchem mehrere Cloud-Services aktiv eingesetzt wurden, um einen Eindruck von der praktischen Nutzung von Cloud-Services zu erhalten. Dieses Projekt wurde eigens für die vorliegende Diplomarbeit konzipiert und umgesetzt.

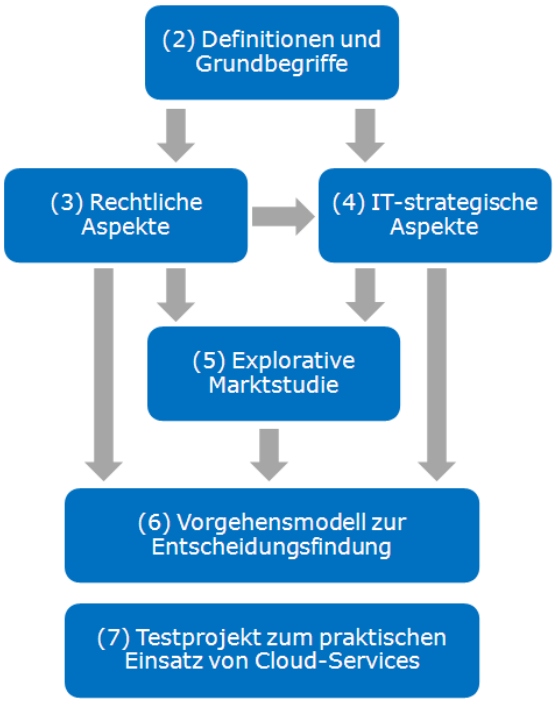


Abbildung 1 – Aufbau der Diplomarbeit mit Angabe der jeweiligen Kapitelnummer[7]

[6] Dieses Charakteristikum weisen gemäß der nachfolgenden Abgrenzung (Abschnitt 1.3) alle untersuchten Cloud-Services auf. Siehe dazu Tabelle 1, S. 28.

[7] Quelle: Eigene Darstellung.

1.3. Projektrahmenbedingungen

Das Vorbereiten und Verfassen der vorliegenden Diplomarbeit war ein interdisziplinäres Projekt an der Schnittstelle von Informatik, Betriebswirtschaftslehre und Rechtswissenschaft. Dies brachte eine hohe Komplexität mit sich und erforderte Kenntnisse sowie Unterstützung in all diesen Fachgebieten. Das benötigte Grundwissen, die Erfahrung und das Interesse zur Erstellung der Diplomarbeit erhielt der Autor in seinen Studien der Wirtschaftsinformatik an der TU Wien und der Rechtswissenschaften an der Universität Wien sowie aus seiner Berufserfahrung in beiden Fachbereichen.

Für den Erfolg des Projekts ebenso bedeutend wie die Qualifikationen des Autors war die Kooperation mit Experten der betroffenen Fachgebiete. Der promovierte Informatiker und Betriebswirt DDr. Alexander Hampel, Geschäftsführer der *ADAPCON Services GmbH* und Vorstandsmitglied des Forschungsförderungsvereins *Integration 3000*, war unverzichtbarer Ansprechpartner des Autors für das Gesamtprojekt und brachte zudem seine große Praxiserfahrung insbesondere in den Bereichen strategisches IT-Management, betriebliche Informationssysteme und IT-Governance ein. Roman Fenkhuber, Student der technischen Informatik und Philosophie und technischer Angestellter an der *Österreichischen Akademie der Wissenschaften*, konzipierte und implementierte gemeinsam mit dem Autor das in Kapitel 7 beschriebene Testprojekt zum praktischen Einsatz von Cloud-Services. Seine umfangreichen Linux-Administrations- und Networking-Kenntnisse waren dabei unerlässlich. Nur in Zusammenarbeit mit diesen geschätzten Kollegen und Experten ihrer jeweiligen Fachgebiete war es dem Autor möglich, eine interdisziplinäre Diplomarbeit auf fachlich hohem Niveau zu verfassen.

1.4. Abgrenzung

Der Untersuchungsgegenstand der Arbeit ist auf Public Clouds beschränkt. Diese werden im Gegensatz zu Private Clouds von einem Anbieter gegen Entgelt für eine große Zahl von Kunden zur Verfügung gestellt.[8] Nur diese unternehmensextern erbrachten Services sollen hinsichtlich ihrer Stärken, Schwächen und Einsatzmöglichkeiten analysiert und einzelne Anbieter näher beleuchtet werden. Es ist nicht Gegenstand der Arbeit, zu prognostizieren, wie sich Cloud Computing in der Zukunft entwickeln wird und welche Faktoren diese Entwicklung beeinflussen werden.

Zudem ist die gesamte Diplomarbeit – wie auch die dieser zugrunde liegende Definition des Begriffs Cloud Computing[9] – auf Cloud-Services eingeschränkt, welche die

[8] Näheres zu diesen Begriffen und zu dieser Abgrenzung siehe in Abschnitt 2.5, S. 31.
[9] Siehe Abschnitt 2.1, S. 23.

Eigenschaft des „on-demand self-service“[10] aufweisen. Dies sind Cloud-Services, die auf der Website des Anbieters ohne zwischenmenschliche Interaktion – in der Regel unter Verwendung einer Kreditkarte – gebucht und danach ohne nennenswerte Vorlaufzeit verwendet werden können. Wenn im Folgenden von Cloud-Services die Rede ist, sind darunter nur solche zu verstehen, die diese Eigenschaft aufweisen. Nicht behandelt werden somit Services, deren Einsatz zwingend den Abschluss eines individuell für den Einzelfall verhandelten Vertrages mit dem Anbieter erfordert.

Aufgrund der Ausrichtung auf Unternehmen in der Rolle der Nutzer von Cloud-Services wird auch eine Einschränkung auf kostenpflichtige Cloud-Services getroffen. Existiert sowohl eine kostenlose als auch eine – in der Regel auf Unternehmen ausgerichtete – kostenpflichtige Variante eines Cloud-Service, wurde letztere untersucht. Zwischen diesen Varianten bestehen häufig Unterschiede hinsichtlich der garantierten Servicequalität, der Haftung und sonstiger rechtlicher Gesichtspunkte. Zudem bieten kostenlose Services möglicherweise geringeren Datenschutz, da deren Anbieter versucht sein könnten, Einnahmen durch das Auswerten oder Verkaufen der Nutzerdaten zu erzielen.[11]

Ein wichtiges Thema im Zusammenhang mit Cloud Computing – und damit auch für die vorliegende Arbeit – sind Kosten. Diesbezügliche Überlegungen werden aber nur in abstrakter Form angestellt. Die konkreten Gesamtkosten des Einsatzes eines Cloud-Service müssen stets im Einzelfall bei der Entscheidungsfindung kalkuliert werden. Die direkten Kosten der Nutzung des Cloud-Service sind nur ein Teil dieser Kalkulation. Weitere bei der Kostenkalkulation zu berücksichtigende Aspekte werden im Rahmen von Kapitel 4 behandelt. Auf die Höhe der Kosten der einzelnen Cloud-Services wird nur beispielhaft, nicht aber umfassend eingegangen.

Zuletzt ist zu betonen, dass in der vorliegenden Arbeit organisatorische, wirtschaftliche und rechtliche Aspekte des Cloud Computing beleuchtet werden, technische Gesichtspunkte und Details zum Thema Informationssicherheit werden hingegen nur in dem dafür notwendigen Ausmaß behandelt.

---

[10] Zum Charakteristikum „on-demand self-service“ siehe Tabelle 1, S. 28.
[11] Velte, Velte und Elsenpeter 2009, 33.

2. Grundlagen

"The long dreamed vision of computing as a utility is finally emerging."[12]

2.1. Definitionen

Das Modell Cloud Computing ist nicht etwa plötzlich und überraschend entstanden, sondern basiert vielmehr auf bestehenden Konzepten. Es ist zum Teil eine logische Weiterentwicklung in der IT-Branche, die erst durch jüngste technische Entwicklungen ermöglicht wurde, zum Teil auch nur eine neue Bezeichnung für bereits Bestehendes. Dieser Abschnitt veranschaulicht dies, indem er Cloud Computing und verwandte Begriffe definiert und zueinander in Beziehung setzt.

Bereits 1961 skizzierte der Computing-Pionier John McCarthy in einer Rede eine Zukunft, in der Rechenleistung aus einem öffentlichen Versorgungsnetz, ähnlich wie Strom, Gas oder Wasser, bezogen wird.[13] Dieses Konzept wird als **Utility Computing** bezeichnet. Services werden vom Kunden nach Bedarf bezogen und entsprechend der tatsächlichen Nutzung abgerechnet,[14] wobei sich der Kunde nicht um die Details im Hintergrund zu kümmern braucht. Es handelt sich dabei um ein Geschäftsmodell, nicht um ein technisches Konzept.[15]

Ein solches ist hingegen **Grid Computing**. Darunter versteht man die Bündelung der Ressourcen mehrerer über ein Netzwerk verbundener, autonomer Rechner um an einer gemeinsamen Aufgabe zu arbeiten.[16] Grid Computing wurde ursprünglich für ressourcenintensive wissenschaftliche Anwendungen entwickelt.[17] Ein **Grid** kann definiert werden als „a type of parallel and distributed system that enables the sharing, selection, and aggregation of geographically distributed 'autonomous' resources dynamically at runtime depending on their availability, capability, performance, cost, and users' quality-of-service requirements".[18] Meist sind die Ressourcen nicht nur autonom und verteilt sondern auch im Eigentum mehrerer Organisationen. Im Gegensatz dazu ist Cloud-Computing-Infrastruktur in der Regel das Eigentum eines (kommerziellen) Anbieters und steht unter dessen zentraler Kontrolle.[19]

---

12 Armbrust et al. 2009, 19.
13 Foster et al. 2008, 1.
14 Buyya et al. 2009, 600.
15 Foster et al. 2008, 2.
16 Velte, Velte und Elsenpeter 2009, 8.
17 Buyya et al. 2009, 600.
18 Buyya et al. 2009, 601.
19 Baun et al. 2009, 4. Ausführliche Vergleiche der Konzepte Grid Computing und Cloud Computing finden sich in Buyya et al. 2009 und Foster et al. 2008.

Genau für das hier als „Cloud-Computing-Infrastruktur“ Bezeichnete steht der Begriff **Cloud**. Die Cloud ist die Hardware und Software im Rechenzentrum.[20] Ausführlicher kann die Cloud beschrieben werden als „a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers.”[21] Mit anderen Worten, die Cloud ist die technische Infrastruktur, welche die Umsetzung des Geschäftsmodells Utility Computing ermöglicht.

Noch bevor der Begriff Cloud Computing entstand, entwickelte sich ein Konzept, das heute als Teilaspekt des Cloud Computing gilt: **Software as a Service (SaaS)**. Darunter versteht man die Nutzung von Software, die auf der Infrastruktur des Anbieters läuft und von diesem bereitgestellt, betrieben und gewartet wird, mittels eines Thin Clients (häufig ein Webbrowser).[22] Heute wird SaaS in der Regel als eines von mehreren Service-Modellen des Cloud Computing, die auch als Ebenen oder Schichten des Cloud Computing bezeichnet werden können, betrachtet.[23]

Gemäß der Definition des *Reliable Adaptive Distributed Systems Laboratory* der *UC Berkeley* ist das – oben beschriebene – Utility Computing neben SaaS der zweite Teilaspekt von Cloud Computing. **Cloud Computing** ist demnach die „Summe“ von SaaS und Utility Computing.[24] Der Begriff Cloud Computing umfasst also einerseits Anwendungen und andererseits Infrastruktur, die über das Internet verfügbar gemacht und nutzungsabhängig verrechnet werden.

Doch Cloud Computing ist kein scharf abgegrenzter Begriff. Im Gegenteil, es existiert eine große Zahl von Definitionen von Cloud Computing.[25] Den meisten davon liegt allerdings ein ähnliches Verständnis zugrunde. Im Folgenden werden einige davon vorgestellt.

Der deutsche Branchenverband der Informations- und Telekommunikationsbranche, *BITKOM*, definiert Cloud Computing als „eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen. Diese werden in Echtzeit als Service über das Internet bereitgestellt und nach Nutzung abgerechnet“[26].

Eine etwas ausführlichere Definition von *Baun et al.* lautet: „Unter Ausnutzung virtualisierter Rechen- und Speicherressourcen und moderner Web-Technologien stellt

---

[20] Armbrust et al. 2009, 4.
[21] Buyya et al. 2009, 601.
[22] Näheres siehe unter Punkt 2.4.3.
[23] Näheres siehe in Abschnitt 2.4, S. 28.
[24] Armbrust et al. 2009, 4. Private Clouds (siehe dazu Abschnitt 2.5, S. 31) werden von dieser Definition ausdrücklich nicht erfasst.
[25] Geelan 2009 und Farber 2008.
[26] BITKOM 2009, 14.

Cloud Computing skalierbare, Netzwerk-zentrierte, abstrahierte IT-Infrastrukturen, Plattformen und Anwendungen als on-demand Dienste zur Verfügung. Die Abrechnung dieser Dienste erfolgt nutzungsabhängig“.[27]

Foster et al. definieren Cloud Computing sehr ähnlich als “large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet“[28].

Eine sehr weit gefasste und zugleich detaillierte Definition, stammt vom *U.S. National Institute of Standards and Technology (NIST)*[29]:

> “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.”

Die fünf grundlegenden, in dieser Definition angesprochenen Eigenschaften sind „on-demand self-service“, „broad network access“, „resource pooling“, „rapid elasticity“ und „measured service“. In der folgenden Grafik sind diese Eigenschaften, die drei verschiedenen Service-Modelle und die vier Deployment-Modelle dargestellt. Eine ausführliche Beschreibung all dieser Aspekte folgt im weiteren Verlauf dieses Kapitels.

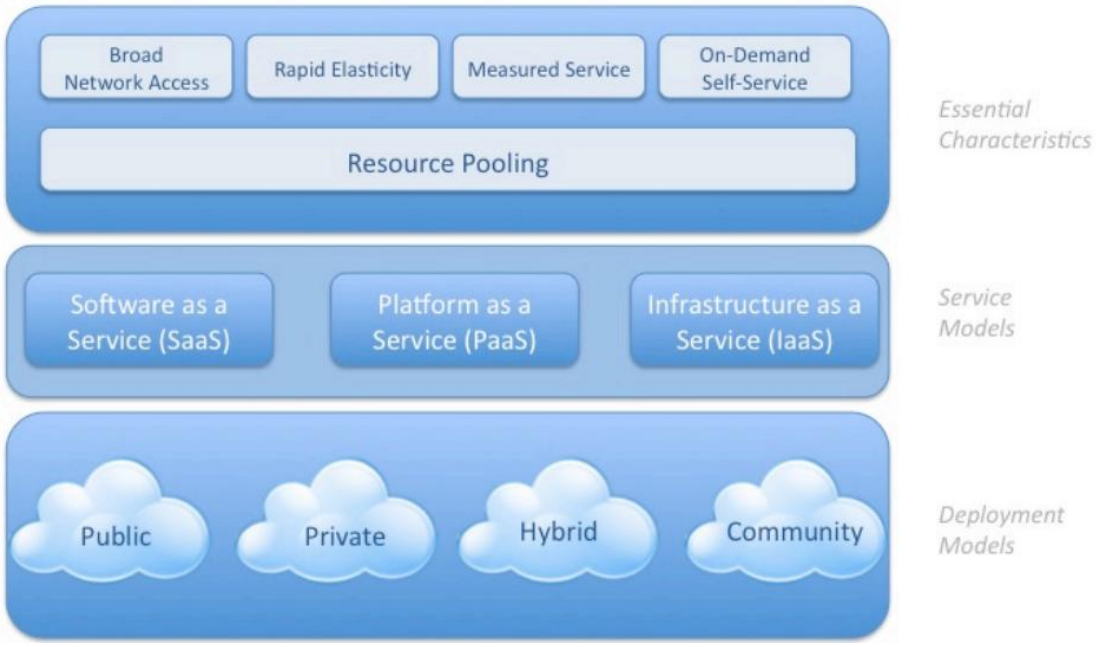


Abbildung 2 – Verschiedene Aspekte des Cloud Computing gemäß *NIST*-Definition[30]

[27] Baun et al. 2009, 4.
[28] Foster et al. 2008, 1.
[29] NIST 2009, Hervorhebungen im Original.

Das Verständnis von Cloud Computing in der vorliegenden Diplomarbeit basiert auf dieser Definition. Sie deckt viele unterschiedliche Sichtweisen des Begriffs Cloud Computing ab und erklärt das Konzept sehr ausführlich, indem sie dessen wichtigste Eigenschaften darlegt und dessen verschiedene Aspekte strukturiert. Bevor diese Eigenschaften und Aspekte näher erläutert werden, folgt ein kurzer Abschnitt über Herkunft und Geschichte des Begriffs Cloud Computing.

2.2. Begriffsherkunft und Geschichte

Der Begriff „Cloud Computing" hat sich aus der gebräuchlichen Metapher entwickelt, das Internet in Netzwerkdiagrammen als Wolke darzustellen.[31] Diese Wolke steht dafür, dass Weg und genaue Funktion der Datenübertragung zwischen zwei kommunizierenden Endpunkten in der Regel nicht bekannt und auch nicht von Interesse sind. Entscheidend ist das Ergebnis, die Übertragung der Daten zwischen zwei via Internet kommunizierenden Endpunkten. Wie bereits deutlich wurde, ist die Situation bei Cloud-Services[32] sehr ähnlich. Der Nutzer ist am Ergebnis, d.h. an der Erbringung des jeweiligen Service interessiert. Für die Bereitstellung der Infrastruktur und die komplexen Abläufe im Hintergrund der Serviceerbringung ist der Anbieter verantwortlich. Der Nutzer hat hierüber keine Kontrolle und benötigt kein diesbezügliches Fachwissen. Überdies ist ihm häufig der Standort des Rechenzentrums nicht bekannt, in dem die Datenverarbeitung erfolgt. Diese kann auch auf mehrere Rechenzentren verteilt sein.[33]

Bereits in Abschnitt 2.1 wurde implizit auf die historische Entwicklung des Cloud Computing eingegangen. Eine etwas andere Sicht auf diese Entwicklung bietet Abbildung 3. Sie zeigt die Evolution der Geschäftsmodelle der Internet Service Provider (ISP) vom reinen Zugangsprovider über das Hosting physischer Server hin zu SaaS, PaaS und IaaS.[34] Beachtenswert ist allerdings, dass bedeutende Anbieter von Cloud-Services sich nicht aus klassischen ISP entwickelt haben, sondern die benötigte Technologie und Infrastruktur zunächst für ihr Kerngeschäft – d.h. für interne Verwendung – entwickelt und erst dann begonnen haben, diese anderen Unternehmen gegen Entgelt zur Verfügung zu stellen.[35] Als Beispiele sind hier *Google* und *Amazon* zu nennen.

---

30 Quelle: Cloud Security Alliance 2009, 14

31 Rittinghouse und Ransome 2009, xxvi.

32 Der Begriff „Cloud-Service" bezeichnet im Folgenden alle Angebote und Leistungen, die unter die Definition von Cloud Computing fallen. Der Begriff „Dienstleistung" wird in diesem Zusammenhang nicht verwendet, um eine Irreführung im Hinblick auf dessen juristische Bedeutung im Sinne eines Dienstvertrages zu vermeiden (vgl. § 1151 ABGB).

33 Einige der juristischen Probleme des Cloud Computing können sich aus genau dieser Tatsache ergeben. Näheres dazu siehe in den nachfolgenden Kapiteln.

34 Zu diesen drei Cloud-Service-Modellen siehe Abschnitt 2.4.

35 Das prominenteste Beispiel in diesem Zusammenhang ist *Amazon*, dessen IT-Ressourcen für Spitzenzeiten wie z.B. das Weihnachtsgeschäft dimensioniert sein müssen, weshalb ein gro-

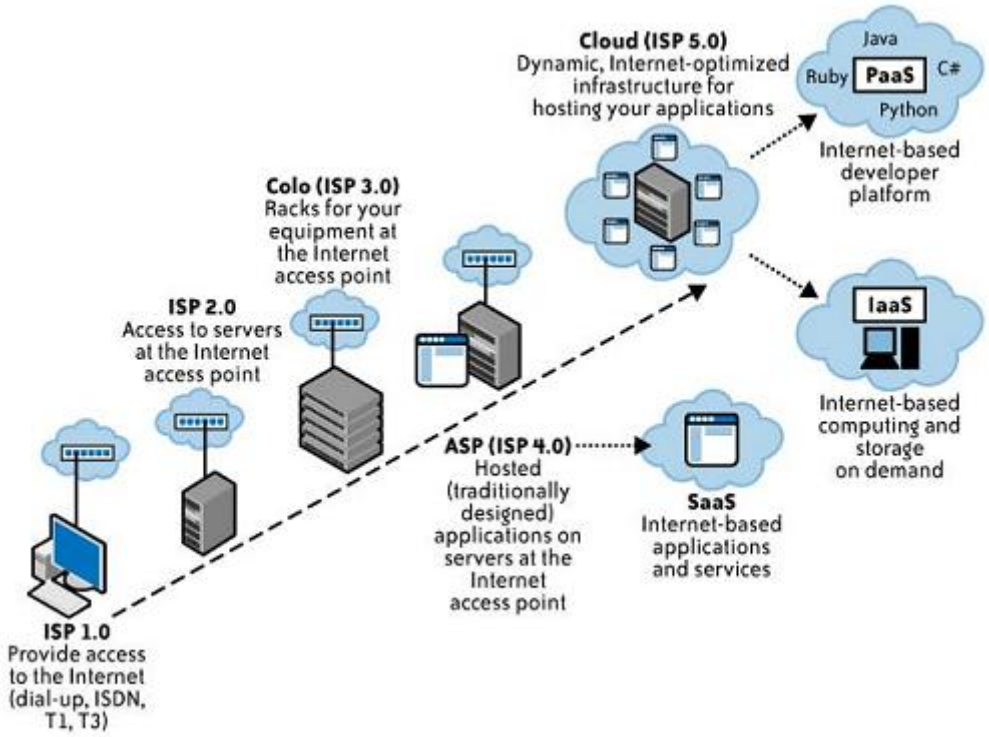


Abbildung 3 – Entwicklung der Internet Service Provider (ISP)[36]

2.3. Eigenschaften des Cloud Computing

Die wichtigsten Charakteristika des Cloud Computing nach der Definition des *NIST* sind in Tabelle 1 zusammengefasst:

Resource pooling (multi-tenancy)	Die Ressourcen des Anbieters (z.B. Massenspeicher, Rechenzeit, Speicher, Netzwerk-Bandbreite, virtuelle Maschinen etc.) werden als „Pool" verwaltet und von mehreren Nutzern gleichzeitig verwendet, indem verschiedene reale oder virtuelle Einheiten den Nutzern nach Bedarf zugewiesen werden. Der Nutzer weiß in der Regel nicht, wo sich die verwendeten physischen Ressourcen tatsächlich befinden.
On-demand self-service	Der Nutzer meldet sich auf der Website des Anbieters an und ruft die benötigten Ressourcen und/oder Services nach Bedarf ab, ohne dass menschliche Interaktion mit dem Anbieter nötig ist. Dies bedeutet, dass es sich um standardisierte Ressourcen bzw. Services handelt, d.h. der Nutzer kann lediglich aus einem beschränkten Angebot an Varianten wählen. Die Bezahlung erfolgt in der Regel mittels Kreditkarte.

ßer Teil davon meistens brach liegt und gegen Entgelt Dritten zur Verfügung gestellt werden kann (Baun et al. 2009, 40).

[36] Quelle: Mather, Kumaraswamy und Latif 2009, 4.

Broad network access	Die Ressourcen und/oder Services sind via Internet mittels Standard-Mechanismen abrufbar, sodass verschiedene Client-Plattformen verwendet werden können.
Rapid elasticity	Die Ressourcen können bei Bedarf rasch zur Verfügung gestellt und wieder freigegeben werden. Dies kann auch automatisch je nach Auslastung erfolgen. Aus der Sicht des Nutzers scheint kein Limit an unmittelbar verfügbaren Ressourcen zu bestehen.
Measured service	Die Nutzung der Ressourcen wird in abstrakten Einheiten (z.B. Speicherplatz, Rechenzeit, Bandbreite, aktive Nutzer etc.) gemessen. Dadurch entsteht Kostentransparenz und die Ressourcen können automatisch gesteuert und optimiert werden.

Tabelle 1 - Eigenschaften des Cloud Computing[37]

Eine typische, theoretisch aber nicht notwendige Eigenschaft des Cloud Computing ist die Virtualisierung von Ressourcen. Virtualisierung bedeutet, dass über den physischen Ressourcen eine abstrakte, logische Schicht liegt, auf welcher die Ressourcen verwaltet und dem Nutzer zur Verfügung gestellt werden.[38] Dies kann auf verschiedenen Ebenen erfolgen, z.B. als Betriebssystem-Virtualisierung, Massenspeicher-Virtualisierung, Datenbank-Virtualisierung, Software-Virtualisierung etc.[39] Somit besteht ein enger Zusammenhang mit den oben genannten Eigenschaften „resource pooling“ und „measured service“. Durch den Einsatz von Virtualisierung arbeiten in der Regel mehrere Nutzer von Cloud-Services zeitgleich mit denselben physischen Ressourcen. Die Virtualisierungs-Technologie ermöglicht dabei allerdings, dass jeder Nutzer diese wie dedizierte, d.h. ihm exklusiv zur Verfügung stehende Ressourcen verwenden kann.[40]

2.4. Cloud-Service-Modelle

Üblicherweise werden drei Service-Modelle des Cloud Computing unterschieden, so auch in der oben vorgestellten Definition des *NIST*. Diese Dreiteilung wird manchmal als „SPI Model“ bezeichnet, was für „software“, „platform“ und „infrastructure“ steht.[41] Die drei Service-Modelle können auch als verschiedene Ebenen oder Schichten des Cloud Computing betrachtet werden. Höhere Schichten können dabei Services der darunter liegenden Schichten zur Servicebereitstellung nützen. Dies muss aber nicht der

37 Quelle: NIST 2009 (mit eigenen Erläuterungen). Auf eine Übersetzung der Begriffe ins Deutsche wurde aus Gründen der Eindeutigkeit verzichtet.
38 Baun et al. 2009, 7.
39 Mather, Kumaraswamy und Latif 2009, 14.
40 Mather, Kumaraswamy und Latif 2009, 14.
41 Cloud Security Alliance 2009, 15.

Fall sein. Die drei Service-Modelle bzw. Schichten sind in Abbildung 4 dargestellt und werden nachfolgend erläutert.

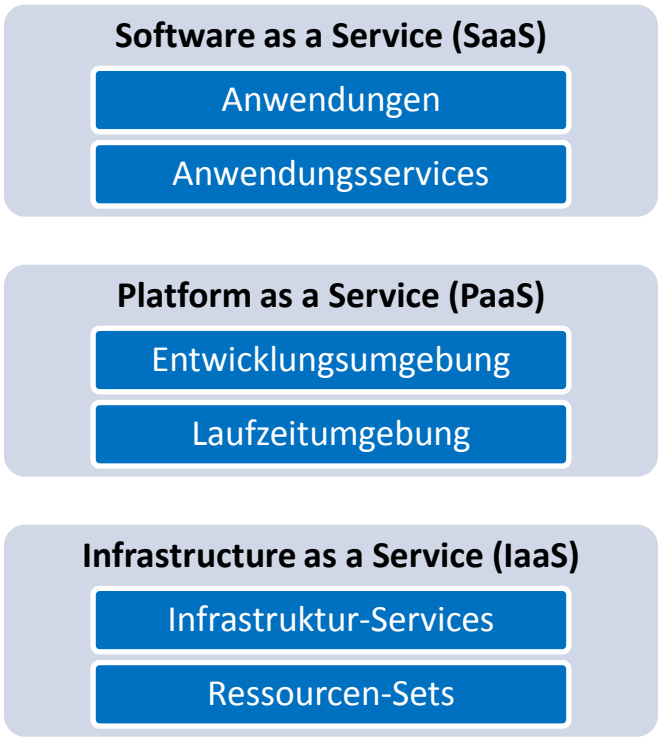


Abbildung 4 – Die drei Schichten (Service-Modelle) des Cloud Computing[42]

2.4.1. Infrastructure as a Service (IaaS)

Beim Service-Modell IaaS werden dem Nutzer abstrahierte Hardware-Ressourcen als Service – d.h. in einer Form, welche die in Abschnitt 2.3 genannten Eigenschaften aufweist – zur Verfügung gestellt.[43] IaaS kommt damit der ursprünglichen Idee des Utility Computing am nächsten.

Wie in Abbildung 4 ersichtlich, bilden Ressourcen-Sets die unterste Ebene des IaaS. Ein Ressourcen-Set kann vereinfacht als – meist virtueller – Server beschrieben werden, der in der Regel beliebig wie ein physischer, privater Server eingesetzt werden kann. Der Nutzer solcher Services kann mittels einer Benutzerschnittstelle eine bestimmte Menge von Ressourcen für sich allokieren, darauf Betriebssystem-Images anlegen, Instanzen davon starten und stoppen etc.[44] Aufgabe des Anbieters ist bei diesem Service-Modell Hosting und Management der Infrastruktur, während der Nutzer für

[42] Abbildung nach Baun et al. 2009, 28 und Lenk et al. 2009, 3.
[43] NIST 2009.
[44] Baun et al. 2009, 30.

Bereitstellung und Betrieb der gesamten Software oberhalb der Betriebssystem-Ebene verantwortlich ist.[45]

Die IaaS-Schicht umfasst auch Infrastruktur-Services. Diese befinden sich eine Ebene über den Ressourcen-Sets, da sie spezifischere Aufgaben erfüllen, wie z.B. das Speichern von Daten oder bestimmte Berechnungsaufgaben.[46]

Der wohl bedeutendste Anbieter von IaaS ist *Amazon Web Services*, der sowohl Infrastruktur-Services als auch Ressourcen-Sets anbietet. Auf *Amazon Web Services* wird – wie auf alle übrigen in diesem Abschnitt genannten Anbieter – in Kapitel 5 detailliert eingegangen.

2.4.2. Platform as a Service (PaaS)

Anbieter des PaaS-Modells stellen dem Nutzer zunächst eine Entwicklungsumgebung zur Verfügung. Dieser entwickelt damit Anwendungen, die dann auf der Plattform des Anbieters laufen.[47] Folglich kann PaaS wie in Abbildung 4 in zwei Komponenten – Entwicklungsumgebung und Laufzeitumgebung – eingeteilt werden. Die Entwicklungsumgebung unterstützt in der Regel Online-Zusammenarbeit über den gesamten Software-Entwicklungszyklus hinweg und ermöglicht das Testen und Debuggen der Anwendung in derselben Umgebung, in der diese später laufen soll.[48]

Die Laufzeitumgebung deckt auch Funktionen wie Lastverteilung, Skalierung, Ausfallsicherheit, Sicherheit etc ab.[49] Um die darunterliegende (Cloud-)Infrastruktur muss sich der Nutzer ebenfalls nicht kümmern, er hat lediglich Kontrolle über seine Anwendung und bestimmte Einstellungen der Laufzeitumgebung.[50] Dadurch kann sich der Nutzer auf die Implementierung der Benutzerschnittstelle und der Geschäftslogik konzentrieren, was den Softwareentwicklungsprozess vereinfacht und beschleunigt.[51]

Beispiele für PaaS-Angebote sind *Google App Engine* und *Microsoft Azure*.

2.4.3. Software as a Service (SaaS)

SaaS kann definiert werden als die Nutzung von Software, die auf (Cloud-)Infrastruktur des Anbieters läuft und von diesem bereitgestellt, betrieben und gewartet wird, mittels eines Thin Clients (häufig ein Web-Browser).[52] Nicht nur die Infrastruktur im Hintergrund, auf der die Software läuft, sondern auch die konkrete Software-Instanz wird von

45 Rittinghouse und Ransome 2009, 34 f.
46 Lenk et al. 2009, 2.
47 NIST 2009.
48 Mather, Kumaraswamy und Latif 2009, 20.
49 Rittinghouse und Ransome 2009, 50.
50 NIST 2009.
51 BITKOM 2009, 26.
52 NIST 2009.

vielen unabhängigen Nutzern des Service gemeinsam genutzt. Auf logischer Ebene steht jedem Nutzer jedoch eine unabhängige Instanz der Software zur Verfügung. Dies bedeutet, die gemeinsame Nutzung erfolgt für den Nutzer völlig unbemerkt und es ist auch sichergestellt, dass jeder Nutzer nur auf seine eigenen Daten zugreifen kann.[53]

Zur SaaS-Schicht gehören sowohl komplexe Anwendungen als auch vergleichsweise einfache Anwendungsservices, die nur eine spezifische Funktion erfüllen. Manche dieser Anwendungsservices können vom Nutzer unmittelbar verwendet werden, andere erhalten erst durch Einbindung in andere Anwendungen eine sinnvolle Funktion.[54]

SaaS ist vom verwandten, deutlich älteren Konzept Application Service Providing (ASP) zu unterscheiden. Der wesentliche Unterschied zwischen diesen beiden Software-Vertriebsmodellen ist, dass bei ASP für jeden Kunden eine eigene Installation betrieben wird.[55] Da diese einzelnen Instanzen getrennt gewartet werden müssen, ergibt sich ein klarer Kostenvorteil durch die gemeinsam genutzten Instanzen des SaaS-Modells im Vergleich zu ASP.

Bekannte SaaS-Angebote sind beispielsweise *Google Apps* und *Salesforce CRM*.

2.5. Cloud-Deployment-Modelle

Tabelle 2 listet die vier Deployment-Modelle des Cloud Computing gemäß der Definition des *NIST* auf und definiert sie.

Private Cloud	Die Cloud-Infrastruktur einer Private Cloud wird für eine bestimmte Organisation betrieben, entweder von dieser Organisation selbst oder von einem Dritten. Physisch kann die Cloud-Infrastruktur sowohl innerhalb der Unternehmensräumlichkeiten oder außerhalb davon betrieben werden.
Community Cloud	Eine Community Cloud wird von mehreren Organisationen gemeinsam genutzt, die dadurch ein gemeinsames Interesse verfolgen (z.B. Kostenersparnis, eine bestimmte Aufgabe, Sicherheitserfordernisse etc.).
Public Cloud	Die Cloud-Infrastruktur einer Public Cloud wird von einer Organisation betrieben, die Cloud-Services gegen Entgelt für die Allgemeinheit oder für eine große Gruppe von Organisationen anbietet.

53 Mather, Kumaraswamy und Latif 2009, 19.
54 Baun et al. 2009, 35.
55 BITKOM 2009, 27 und Pohle und Ammann 2009b, 625 f.

Hybrid Cloud	Eine Hybrid Cloud entsteht durch das Zusammenwirken der Infrastruktur zweier oder mehrerer Clouds (Private, Community oder Public). Diese bleiben eigenständige Clouds, werden aber durch standardisierte oder proprietäre Technologie verknüpft, sodass Daten und Anwendungen portiert werden können. Dies kann z.B. eingesetzt werden, um Lastspitzen, welche die Private Cloud einer Organisation überlasten würden, durch den Einsatz der Infrastruktur einer Public Cloud zu bewältigen.

Tabelle 2 – Die Deployment-Modelle des Cloud Computing[56]

Mit der Beschreibung der Deployment-Modelle ist die umfangreiche Erläuterung der Cloud-Computing-Definition des *NIST* nun abgeschlossen. Diese wurde der vorliegenden Diplomarbeit zugrunde gelegt, da sie dem Autor am besten geeignet scheint, das Konzept Cloud Computing umfassend zu beschreiben und zu strukturieren.

Demgegenüber ist die Definition der *UC Berkeley* etwas enger, denn sie schließt Private Clouds vom Begriff Cloud Computing – definiert als die Summe von SaaS und Utility Computing – aus. Wie in Abschnitt 1.3 erläutert, wird diese Abgrenzung in Bezug auf den Untersuchungsgegenstand der vorliegenden Diplomarbeit ebenfalls vorgenommen (nicht allerdings in Bezug auf die Definition des Begriffs Cloud Computing selbst): Der Untersuchungsgegenstand der Arbeit ist auf Public Clouds beschränkt, denn es werden – unternehmensexterne – Anbieter von Cloud-Services evaluiert und die rechtlichen Aspekte der Nutzung dieser externen Services dargestellt.[57] Gemäß den Definitionen dieses Abschnitts handelt es sich dabei um Public Clouds. Wenn in den nachfolgenden Kapiteln daher von Cloud Computing die Rede ist, sind entsprechend dem Untersuchungsgegenstand der vorliegenden Diplomarbeit stets Public Clouds gemeint.

2.6. Cloud Computing und IT-Outsourcing

In diesem Abschnitt wird IT-Outsourcing definiert und mit Cloud Computing in Beziehung gesetzt. Information Technology Outsourcing (IT-Outsourcing) kann beschrieben werden als das Abschließen von Verträgen mit externen Organisationen über die Erbringung von IT-Dienstleistungen, um die interne Erbringung dieser Dienstleistungen zu ersetzen.[58]

---

[56] Quelle: NIST 2009.

[57] Dies soll nicht darüber hinwegtäuschen, dass auch die Nutzung von Private Clouds rechtliche Konsequenzen haben kann. So ist z.B. das Datenschutzrecht auch im Verhältnis zwischen verschiedenen juristisch eigenständigen Gesellschaften eines Konzerns zu beachten. Dies wird allerdings im Rahmen der vorliegenden Arbeit nicht näher behandelt.

[58] Hirschheim und Dibbern 2009, 3 und Pohl 2009, 1.

Der oben definierte Untersuchungsgegenstand der vorliegenden Diplomarbeit – Cloud Computing, eingeschränkt auf Public Clouds – ist die externe Erbringung von IT-Dienstleistungen und daher eine Form des IT-Outsourcings. Im Gegensatz dazu werden viele Private Clouds nicht vom Begriff Outsourcing erfasst, und zwar jene, die vom Nutzer selbst betrieben werden. Private Clouds sind also nur dann eine Form des Outsourcings, wenn sie von einer externen Organisation betrieben werden.

Public Clouds sind hingegen – wie bereits erwähnt – aus der Sicht des Nutzers in jedem Fall eine Form des Outsourcings.[59] Ein wichtiger Unterschied des Cloud Computing zu anderen Formen des Outsourcings ist die Standardisierung. Der Nutzer von Cloud-Services hat zwar in der Regel die Wahl zwischen mehreren Varianten und Konfigurationen des jeweiligen Service, dennoch kauft er sozusagen „von der Stange". Eine individuell beim Anbieter bestellte und von diesem auf seine Bedürfnisse angepasste Leistung erhält der Nutzer von Cloud-Services nicht. Cloud Computing ist damit eine automatisierte, industrialisierte Form des IT-Outsourcings, in gewisser Weise daher dessen fortschrittlichste Form.[60]

Da Cloud Computing ein sehr junges Konzept ist, wurde es aus juristischer Sicht bisher nur spärlich aufgearbeitet. Durch die nahe Verwandtschaft zum IT-Outsourcing kann die juristische Literatur zu diesem Thema im nachfolgenden Kapitel zum Teil auch im Zusammenhang mit Cloud Computing fruchtbar gemacht werden.

[59] BITKOM 2009, 32.
[60] BITKOM 2009, 32.

3. Rechtliche Aspekte des Cloud Computing[61]

„Das deutsche und europäische Datenschutzrecht gehen im Prinzip davon aus, dass man jederzeit feststellen kann, wo sich die Daten auf den Rechnern und Speichern befinden."[62]

Wie die gesamte Diplomarbeit nimmt dieses Kapitel die Perspektive von Unternehmen mit Haupt- oder Zweigniederlassung[63] in Österreich in ihrer Rolle als (potenzielle) Nutzer von Cloud-Services ein. Für solche Unternehmen ist zunächst primär die österreichische Rechtsordnung maßgeblich. Diese sieht keine speziellen gesetzlichen Regelungen für Cloud Computing vor. Die rechtliche Situation im Zusammenhang mit Cloud Computing ist daher nach allgemeinen Regeln zu beurteilen.

Die aus der Sicht der genannten Nutzer wichtigsten rechtlichen Aspekte des Cloud Computing können in zwei Gruppen eingeteilt werden. Die erste Gruppe bildet das auf den Vertrag zwischen dem Anbieter und dem Nutzer eines Cloud-Service anzuwendende Recht. Dieses wird im ersten Teil dieses Kapitels behandelt. In der Praxis kommt in diesem Bereich – wie im Folgenden gezeigt wird – häufig nicht österreichisches Recht zur Anwendung, auch wenn der Nutzer des Cloud-Service ein österreichisches Unternehmen ist. Die zweite Gruppe umfasst verwaltungs- und aufsichtsrechtliche Vorschriften, die im zweiten Teil dieses Kapitels behandelt werden, wobei der Schwerpunkt auf dem Datenschutzrecht liegt. Österreichisches Recht ist hier im Gegensatz zum Vertragsrecht für österreichische Unternehmen in der Regel verbindlich.

Im Folgenden werden diese rechtlichen Rahmenbedingungen in der genannten Reihenfolge unter Berücksichtigung der österreichischen Literatur zum Thema Outsourcing und der einschlägigen Literatur zur deutschen Rechtsordnung dargelegt. Im Gegensatz zu Deutschland[64] gibt es in Österreich nach Wissensstand des Autors noch keine rechtswissenschaftlichen Veröffentlichungen zum Thema Cloud Computing. Da die meisten Anbieter von Cloud-Services weder Sitz noch Niederlassung in Österreich haben, wird in den folgenden Abschnitten zunächst jeweils die Frage behandelt, die

---

61 Für die gesamte vorliegende Diplomarbeit wurde eine einheitliche Zitierweise gewählt, welche sich von den üblichen juristischen Zitierregeln unterscheidet, wobei versucht wurde, die Unterschiede möglichst gering zu halten. Ebenfalls aus Gründen der Einheitlichkeit werden Abkürzungen auch in diesem Kapitel – entgegen der unter Juristen üblichen Schreibweise ohne Punkte („zB") – mit Punkten („z.B.") geschrieben, sofern die entsprechenden Wörter nicht ohnedies wegen der besseren Verständlichkeit ausgeschrieben werden. Eine Ausnahme hiervon bilden die Angaben von Rechtsnormen, die konventionsgemäß ohne Punkte geschrieben werden.

62 Spies 2009, XI.

63 Zu diesen Begriffen siehe allgemein Krejci 2008, 128 ff. Soweit notwendig wird später noch näher darauf eingegangen.

64 U.a. Niemann und Paul 2009, Pohle und Ammann 2009a, Pohle und Ammann 2009b, Schulz und Rosenkranz 2009, Nägele und Jacobs 2010 und Schuster und Reichl 2010.

Rechtsordnung welches Staates anwendbar ist. Aufgrund der genannten Einschränkung auf Unternehmen als Nutzer von Cloud-Services wird generell nicht auf etwaige abweichende Regelungen für Verbraucher eingegangen.

3.1. Vertragsrecht des Cloud Computing

Einleitend ist zu sagen, dass ein Vertrag über die Nutzung eines Cloud-Service aufgrund der für das Cloud Computing charakteristischen Standardisierung in der Regel zu den Konditionen des Anbieters abgeschlossen wird.[65] Dieser legt den Vertragsinhalt in der Form von Allgemeinen Geschäftsbedingungen (AGB)[66] fest. Jeder Nutzer muss – so er nicht darauf verzichten will – den Vertrag mit dem auf diese Weise vom Anbieter genau vorgegebenen Inhalt abschließen. Leistung und Gegenleistung, Anbieter- und Nutzerpflichten sowie alle sonstigen Konsequenzen des so entstandenen Rechtsverhältnisses richten sich dann grundsätzlich nach dem Vertragsinhalt.

Von dieser Grundregel gibt es jedoch mehrere Ausnahmen. Die erste und offensichtlichste betrifft den Fall, dass im Rahmen des Vertragsverhältnisses eine Situation eintritt, die die Parteien nicht vorhergesehen und daher im Vertrag nicht geregelt haben. Können sich die Parteien darüber nachträglich nicht einigen, muss nach allgemeinen Regeln der Rechtsordnung ermittelt werden, wie die Situation zu lösen ist.[67] Auch wenn der Vertrag unklar ist, können diese Regeln zur Auslegung herangezogen werden. Eine weitere Ausnahme betrifft Vertragsbestandteile, die aufgrund gesetzlicher Bestimmungen unzulässig sind, wie z.B. gröblich benachteiligende Klauseln.[68]

Aus den genannten Gründen muss zunächst jener Staat ermittelt werden, dessen Rechtsordnung auf den Vertrag zwischen dem Anbieter und dem Nutzer eines Cloud-Service anzuwenden ist. Anschließend muss der Vertrag in das Schema der gesetzlich vorgegebenen Vertragstypen dieser Rechtsordnung – z.B. Miet-, Dienst-, Werkvertrag – eingeordnet werden. Der Aufbau des vorliegenden Abschnitts richtet sich nach diesen Überlegungen.

3.1.1. Anwendbares Recht

Auf vertragliche Schuldverhältnisse mit Auslandsbezug ist – mit hier nicht relevanten Ausnahmen – die Verordnung (EG) Nr. 593/2008[69], genannt Rom-I-Verordnung

---

[65] Niemann und Paul 2009, 446. Siehe Charakteristikum „on-demand self-service“ in Tabelle 1, S. 28.

[66] Siehe dazu Punkt 3.1.5, S. 46.

[67] *Niemann und Paul* (2009, 446) gehen allerdings davon aus, dass diese Situation in der Cloud-Computing-Praxis nicht allzu häufig vorkommt.

[68] Siehe dazu Punkt 3.1.5, S. 46.

[69] Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I),

(Rom-I-VO), anzuwenden.[70] Diese regelt nicht inhaltliche Fragen des Vertragsrechts, sondern dient ausschließlich der Feststellung, das Recht welches Staates auf ein gegebenes Vertragsverhältnis anzuwenden ist.[71] Die Rom-I-VO gilt in allen EU-Mitgliedstaaten (mit Ausnahme von Dänemark).[72] Der erforderliche Auslandsbezug des Vertragsverhältnisses und das berufene, d.h. im Ergebnis anzuwendende Recht sind aber nicht auf diese Staaten beschränkt.[73] Dies bedeutet, welche Rechtsordnung anzuwenden ist, muss z.B. auch dann nach der Rom-I-VO geprüft werden, wenn ein österreichisches Unternehmen den Cloud-Service eines US-amerikanischen Unternehmens nützt, und dies kann durchaus zu dem Ergebnis führen, dass das Vertragsverhältnis US-amerikanischem Vertragsrecht unterliegt. Die Verordnung ist also nur dann nicht anzuwenden, wenn das gesamte Vertragsverhältnis keinen Bezug zu einem EU-Mitgliedstaat hat oder in reinen „Inlandsfällen". Wird ein Vertrag zwischen zwei österreichischen Unternehmen in Österreich abgeschlossen und besteht auch sonst kein Auslandsbezug, gilt von vornherein österreichisches Recht.

Die oben bereits angesprochenen, in der Cloud-Computing-Praxis regelmäßig den Vertragsinhalt bestimmenden AGB beinhalten häufig eine Rechtswahl.[74] Eine solche legt aktiv den Staat fest, dessen Rechtsordnung das Vertragsverhältnis unterliegen soll,[75] und ist gemäß Art 3 Rom-I-VO grundsätzlich zulässig. Die – im nächsten Absatz sogleich näher beschriebenen – Kollisionsnormen der Rom-I-VO, welche die anzuwendende Rechtsordnung festlegen, kommen dadurch nicht zur Anwendung.[76]

Wurde im Vertrag keine Rechtswahl getroffen, erfolgt eine so genannte objektive Anknüpfung, d.h. die anzuwendende Rechtsordnung ist anhand von Art 4 Rom-I-VO zu

---

ABl L 177, 6 vom 04.07.2008, berichtigt ABl L 309, 87 vom 24.11.2009. Zu den Ausnahmen vom Anwendungsbereich siehe Art 1 Abs 2 Rom-I-VO. Die Rom-I-VO gilt nur für nach dem 17.12.2009 abgeschlossene Verträge (Art 29 Rom-I-VO). Zur bisherigen und auf ältere Verträge grundsätzlich noch anwendbaren Rechtslage siehe z.B. Verschraegen in Rummel, Kommentierung zum EVÜ.

70 Art 1 Abs 1 Rom-I-VO.

71 Gem. Art 20 Rom-I-VO handelt es sich bei den Verweisungen der Rom-I-VO um Sachnormverweisungen. Dies bedeutet, dass allfällige Kollisionsnormen der berufenen nationalen Rechtsordnung – die möglicherweise ihrerseits wiederum auf eine andere Rechtsordnung verweisen könnten (Rück- oder Weiterverweisung) – nicht mehr angewendet werden dürfen.

72 Martiny in Sonnenberger 2009, Rz. 74 ff. zu Art 1 Rom-I-VO.

73 Art 2 Rom-I-VO.

74 Niemann und Paul 2009, 446. Zur Zulässigkeit der Rechtswahl in AGB siehe Martiny in Sonnenberger 2009, Rz. 13 zu Art 3 Rom-I-VO.

75 Rück- und Weiterverweisung (siehe Fn. 71) sind auch im Fall der Rechtswahl ausgeschlossen (Martiny in Sonnenberger 2009, Rz. 5 zu Art 20 Rom-I-VO).

76 Für Verbraucherverträge ist die Rechtswahl hingegen nur eingeschränkt möglich. Vgl. insbesondere § 13a KSchG (Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen werden (Konsumentenschutzgesetz - KSchG), BGBl 140/1979 idF BGBl I 66/2009).

ermitteln.[77] Grundgedanke dieser Bestimmung ist, einen Vertrag der Rechtsordnung jenes Staates zu unterstellen, mit dem er am engsten verbunden ist.[78] Von den konkreten Anknüpfungsregeln des Art 4 Abs 1 Rom-I-VO kommt im Zusammenhang mit Cloud Computing nur lit b in Betracht: „Dienstleistungsverträge unterliegen dem Recht des Staates, in dem der Dienstleister seinen gewöhnlichen Aufenthalt hat." [79] Verträge über Cloud-Services, die nicht als Dienstleistungsverträge zu qualifizieren sind, fallen unter die Generalklausel des Art 4 Abs 2 Rom-I-VO. Dieser bestimmt, dass der Vertrag dem Recht jenes Staates unterliegt, in dem die Partei, welche die für den Vertrag charakteristische Leistung zu erbringen hat, ihren gewöhnlichen Aufenthalt hat.[80] Im Zusammenhang mit Cloud Computing erbringt immer der Anbieter die charakteristische Leistung,[81] denn diese ist die Leistung, die den Vertrag von anderen Verträgen unterscheidet und gegen Entgelt erbracht wird.[82] Art 4 Abs 3 Rom-I-VO sieht noch eine Ausnahmeregelung vor, nach der in Abweichung von Abs 1 und 2 die Rechtsordnung eines anderen Staates anzuwenden ist, wenn der Vertrag eine offensichtlich engere Verbindung zu diesem aufweist. Art 4 Abs 4 Rom-I-VO legt schließlich für den Fall des Scheiterns einer Anknüpfung nach Art 1 und 2 die eingangs erwähnte Grundregel fest, dass der Vertrag dem Recht jenes Staates unterliegt, mit dem er am engsten verbunden ist. Die beiden letztgenannten Regeln sind aber im Zusammenhang mit Cloud Computing wohl von sehr geringer Bedeutung, weil die Anknüpfung nach der charakteristischen Leistung[83] in den allermeisten Fällen möglich sein wird.

An dieser Stelle ist auf Art 9 und Art 21 Rom-I-VO hinzuweisen, die unabhängig von der gemäß Rom-I-VO auf einen Vertrag anwendbaren Rechtsordnung – und damit auch unabhängig von einer Rechtswahl nach Art 3 Rom-I-VO – zur Anwendung öster-

---

77 Die Art 5-8 Rom-I-VO enthalten Sonderanknüpfungsregeln, die im vorliegenden Zusammenhang keine Rolle spielen. Dies u.a. deshalb, weil – wie eingangs bereits erwähnt – auf Verbraucherverträge nicht eingegangen wird.

78 Martiny in Sonnenberger 2009, Rz. 1 zu Art 4 Rom-I-VO. Vgl. auch Art 4 Abs 4 Rom-I-VO.

79 Gem. Art 19 Abs 1 Rom-I-VO ist der gewöhnliche Aufenthalt bei Unternehmern der Ort ihrer Hauptniederlassung und bei juristischen Personen, Gesellschaften und Vereinen der Ort ihrer Hauptverwaltung. Näheres siehe Martiny in Sonnenberger 2009, Rz. 4 ff. zu Art 19 Rom-I-VO.
Gem. Art 19 Abs 2 Rom-I-VO ist auf den Ort der Zweigniederlassung, Agentur oder sonstigen Niederlassung abzustellen, wenn diese für Abschluss und/oder Erfüllung des Vertrages verantwortlich ist. Näheres siehe Martiny in Sonnenberger 2009, Rz. 12 ff. zu Art 19 Rom-I-VO.

80 Zu den einzelnen Vertragstypen und damit zur Begründung der hier getroffenen Einordnung siehe Punkt 3.1.4, S. 43. Die Auslegung der relevanten Begriffe (z.B. „Dienstleistungsvertrag") erfolgt im Rahmen der Rom-I-VO zwar autonom, d.h. nach gemeinschaftsrechtlichen Grundsätzen und somit letztlich durch den EuGH (Martiny in Sonnenberger 2009, Vorbemerkung zu Art 1, Rz. 15 ff.). Da alle in Frage kommenden Bestimmungen hier allerdings zum selben Ergebnis führen, können Fragen der vertragstypologischen Einordnung nach autonomer Auslegung außer Betracht bleiben.

81 Niemann und Paul 2009, 446.

82 Martiny in Sonnenberger 2009, Rz. 148 zu Art 4 Rom-I-VO.

83 Art 4 Abs 2 Rom-I-VO.

reichischer Bestimmungen führen können, sofern ein österreichisches Gericht zu entscheiden hat.[84] Art 9 Rom-I-VO definiert eine so genannte Eingriffsnorm als „zwingende Vorschrift, deren Einhaltung von einem Staat als so entscheidend für die Wahrung seines öffentlichen Interesses, insbesondere seiner politischen, sozialen oder wirtschaftlichen Organisation, angesehen wird“, dass sie ungeachtet der nach Rom-I-VO anzuwendenden Rechtsordnung angewendet werden muss. In Art 21 Rom-I-VO findet sich der ordre-public-Vorbehalt, der besagt, dass ein Gericht eine nach Rom-I-VO anzuwendende Vorschrift nicht anwenden muss, wenn diese mit der öffentlichen Ordnung („ordre public“) des Gerichtsstaates unvereinbar ist. Welche Vorschriften der österreichischen Rechtsordnung als Eingriffsnormen gelten und welche Grundwerte der Rechtsordnung im Einzelnen die öffentliche Ordnung ausmachen, ist nicht ausdrücklich geregelt und zum Teil strittig.[85] Dieser Punkt bedürfte im vorliegenden Zusammenhang einer umfassenden Untersuchung und muss daher an dieser Stelle offen bleiben. Hier sollte lediglich darauf hingewiesen werden, dass nicht jede beliebige Klausel eines Vertrages, die gemäß der nach Rom-I-VO anzuwendenden Rechtsordnung zulässig ist, auch tatsächlich Bestand hat, wenn ein österreichisches Gericht darüber entscheidet. Ob eine konkrete Vertragsklausel unter Art 9 oder Art 21 Rom-I-VO fällt, bedarf einer ausführlichen Einzelfallprüfung.

3.1.2. Das E-Commerce-Gesetz und sein Einfluss auf das anzuwendende Recht

Basierend auf der europäischen E-Commerce-Richtline (EC-RL)[86] wurde in Österreich das E-Commerce-Gesetz (ECG)[87] erlassen, welches bestimmte rechtliche Aspekte von „Diensten der Informationsgesellschaft“ regelt, insbesondere das so genannte Herkunftslandprinzip und z.B. Informationspflichten vor und nach Vertragsabschluss, jedoch nicht etwa „den E-Commerce“ insgesamt. Die vom ECG nicht berührten Aspekte des E-Commerce sind nach allgemeinen Regeln zu beurteilen,[88] wie dies auch im vorliegenden Kapitel erfolgt. Anzumerken ist, dass das ECG nicht nur Verbrauchergeschäf-

---

84 Zur Gerichtszuständigkeit siehe Punkt 3.1.3, S. 41.

85 Siehe dazu z.B. Mankowski 2008, 146 f. und Verschraegen in Rummel, Rz. 12 f. zu Art 16 EVÜ, der Vorgängerbestimmung von Art 21 Rom-I-VO.

86 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), ABl L 178, 1 vom 17.07.2000.

87 Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG), BGBl I 152/2001.

88 Zankl 2002, Rz. 53.

te erfasst, sondern alle „Dienste der Informationsgesellschaft“, auch wenn ein solcher im konkreten Fall für einen Unternehmer erbracht wird.[89]

„Dienste der Informationsgesellschaft“ definiert das Gesetz als in der Regel gegen Entgelt und auf individuellen Abruf des Empfängers elektronisch im Fernabsatz bereitgestellte Dienste.[90] „Im Fernabsatz“ bedeutet dabei, dass Erbringer und Nutzer nicht am selben Ort anwesend sind, und „bereitgestellt“ meint nicht zwingend die elektronische Erbringung, sondern umfasst z.B. auch den Verkauf von Gütern via Internet, die dann auf anderem Wege geliefert werden.[91] Ein Cloud-Service ist ein solcher Dienst der Informationsgesellschaft im Sinne des ECG, denn er wird vom Nutzer individuell elektronisch abgerufen und Nutzer und Anbieter sind dabei nicht gleichzeitig anwesend.[92] Das ECG ist daher auf Cloud-Services anzuwenden, im Gegensatz zu vielen herkömmlichen Hosting- und ASP-Verträgen, die individuell unter Anwesenden – und daher nicht im Fernabsatz – abgeschlossen werden.

Aus diesem Grund kann sich das in § 20 ECG normierte Herkunftslandprinzip darauf auswirken, das Recht welches Staates auf den Anbieter eines bestimmten Cloud-Service anzuwenden ist. Es bildet damit eine Ausnahme zu den oben erläuterten Regelungen der Rom-I-VO über das anzuwendende Recht. Dies ist dann der Fall, wenn der Anbieter des Cloud-Service im Europäischen Wirtschaftsraum (EWR) niedergelassen[93] ist und die Nutzung ebenfalls im EWR stattfindet.[94] Das Herkunftslandprinzip besagt, dass sich die rechtlichen Anforderungen an einen solchen Anbieter „im koordinierten Bereich“ nach dem Recht jenes Staates richten, in dem er niedergelassen ist.[95] Der „koordinierte Bereich“ – gleichzusetzen mit dem (sachlichen) Anwendungsbereich des Herkunftslandprinzips[96] – erfasst alle in Bezug auf Dienste der Informationsgesellschaft einschlägigen Rechtsgebiete, sowohl des öffentlichen Rechts als auch des Privatrechts,[97] sofern nach § 21 ECG keine Ausnahme vom Herkunftslandprinzip besteht.

---

89 Krejci 2008, 281.
90 § 3 Z 1 ECG.
91 Krejci 2008, 281. Siehe dazu ausführlich Laga, Sehrschön und Ciresa 2007, 15 ff. und Zankl 2002, Rz. 61 ff.
92 Siehe Charakteristikum „on-demand self-service“ in Tabelle 1, S. 28.
93 Niedergelassen ist, wer „eine Wirtschaftstätigkeit mittels einer festen Einrichtung auf unbestimmte Zeit tatsächlich ausübt“ (§ 3 Z 3 ECG), wobei technische Einrichtungen, wie z.B. eine länderbezogene Top-Level-Domain oder ein Server für sich alleine noch keine Niederlassung begründen (Zankl 2002, Rz. 78). Bei mehreren Niederlassungen innerhalb des EWR wird das Recht jenes Staates anzuwenden sein, in dem der Mittelpunkt der Tätigkeiten liegt und in dem insbesondere die maßgeblichen Entscheidungen getroffen werden (Laga, Sehrschön und Ciresa 2007, 18 f.).
94 Gem. § 1 Abs 2 ECG ist das Herkunftslandprinzip auf den Verkehr von Diensten der Informationsgesellschaft innerhalb des EWR beschränkt.
95 § 20 Abs 1 ECG.
96 Laga, Sehrschön und Ciresa 2007, 20.
97 Zankl 2002, Rz. 84.

Insbesondere ist auch das Vertragsrecht einschließlich der Gewährleistungsregeln umfasst.[98]

Eine Ausnahme vom Herkunftslandprinzip betrifft die Rechtswahl.[99] Diese ist unabhängig vom ECG zu prüfen und richtet sich somit in den EU-Mitgliedstaaten (mit Ausnahme von Dänemark) nach der Rom-I-VO, sofern ein Auslandsbezug vorliegt. Wie oben dargelegt, ist die Rechtswahl gemäß Art 3 Rom-I-VO zulässig und geht somit dem Herkunftslandprinzip vor.[100] Die übrigen Ausnahmen des § 21 ECG sind im Zusammenhang mit Cloud-Services nicht relevant. Sofern keine Rechtswahl vorgenommen wurde, ist auf im EWR niedergelassene Anbieter von Cloud-Services somit grundsätzlich das Recht jenes Staates anzuwenden ist, in dem sie niedergelassen sind, und die entsprechenden Regelungen der Rom-I-VO kommen nicht zur Anwendung.

Die Anwendbarkeit des ECG selbst ist von der Anwendbarkeit des Herkunftslandprinzips zu trennen. Als logische Konsequenz des Herkunftslandprinzips gilt das ECG nicht für innerhalb des EWR aber außerhalb Österreichs niedergelassene Anbieter, denn auf diese ist die entsprechende nationale Umsetzung der EC-RL im Staat ihrer Niederlassung anzuwenden.[101] In Bezug auf alle übrigen Anbieter, d.h. jene, die entweder in Österreich oder nicht im EWR niedergelassen sind, richtet sich die Anwendbarkeit des ECG nach den allgemeinen Regeln Internationalen Privatrechts (IPR).[102]

Aufgrund des – abgesehen vom Herkunftslandprinzip – eingeschränkten Regelungsinhalts des ECG hat dessen Anwendbarkeit auf Cloud-Services allerdings im vorliegenden Zusammenhang keine weit reichenden praktischen Konsequenzen. Anbieter von Cloud-Services unterliegen dadurch jenen Anforderungen, die gemäß ECG ohnehin für die meisten kommerziellen Websites gelten. Dies sind insbesondere die Informationspflichten der §§ 5-8 ECG und die Vorschriften bezüglich Vertragsabschlüssen der §§ 9-12 ECG. Zudem gelten die Regeln zur Verantwortlichkeit von Diensteanbietern nach §§ 13-19 ECG. Da es sich bei all diesen Bestimmungen um keine Spezifika von Cloud-Services handelt und diese primär für Anbieter relevant sind, während in der vorliegenden Arbeit die Nutzer im Vordergrund stehen, wird hier nicht näher darauf eingegangen.

Zusammenfassend kann daher für die Cloud-Computing-Praxis gesagt werden, dass in der Regel auf den Vertrag zwischen dem Anbieter und dem Nutzer eines Cloud-

98 Zankl 2002, Rz. 87.
99 § 21 Z 5 ECG.
100 Zankl 2002, Rz. 349.
101 Laga, Sehrschön und Ciresa 2007, 5. Zur Diskussion über das Zusammenspiel von IPR und Herkunftslandprinzip siehe Laga, Sehrschön und Ciresa 2007, 97 ff. und Zankl 2002, Rz. 313 ff. mit weiteren Nachweisen.
102 Laga, Sehrschön und Ciresa 2007, 15.

Service das Recht jenes Staates anzuwenden ist, in dem der Anbieter seine Hauptniederlassung oder jene Zweigniederlassung hat, welcher der Vertrag zugerechnet werden kann.[103] Dies ergibt sich entweder aufgrund der Rechtswahl durch die Vertragsparteien – d.h. in der Praxis durch den Anbieter –, aufgrund des Herkunftslandprinzips des ECG, oder aufgrund der objektiven Anknüpfung nach Art 4 Rom-I-VO. Auf den Standort der Server, welcher aufgrund der Virtualisierung möglicherweise ohnehin schwierig zu ermitteln ist, kommt es also aus vertragsrechtlicher Sicht nicht an.

3.1.3. Gerichtsstand

Wie in Kapitel 5 gezeigt werden wird, legen die Anbieter von Cloud-Services in der Regel nicht nur das anzuwendende Recht sondern auch den Gerichtsstand für Rechtsstreitigkeiten aus dem Vertrag über die Nutzung des Cloud-Service in den AGB fest. Es stellt sich daher zunächst die Frage, ob solche Gerichtsstandsvereinbarungen in AGB gültig sind. Wie in der gesamten Arbeit werden auch hier Sonderregelungen für Verbraucher nicht betrachtet. Für zivilrechtliche Ansprüche mit Auslandsbezug[104] geht die Verordnung (EG) Nr. 44/2001 (EuGVVO)[105] in ihrem Anwendungsbereich den nationalen Bestimmungen vor.[106] Nach Art 23 EuGVVO können Parteien, wenn mindestens eine von ihnen ihren Wohnsitz, oder – im Falle von juristischen Personen – ihren Sitz, ihre Hauptverwaltung oder ihre Hauptniederlassung[107] in einem Mitgliedstaat der EU hat, die Zuständigkeit eines Gerichts oder der Gerichte eines EU-Mitgliedstaats vereinbaren. Dabei sind bestimmte Formvorschriften einzuhalten, von denen im vorliegenden Zusammenhang die Schriftform relevant ist, der die elektronische Übermittlung – also auch der Vertragsabschluss über eine Website[108] – gleichgestellt ist, wenn die Möglichkeit besteht, die AGB auszudrucken und dauerhaft zu speichern.[109] Die Vereinbarung eines Gerichtsstands, der innerhalb der EU liegt, in AGB ist somit grundsätzlich zulässig.[110]

Wird hingegen ein Gerichtsstand vereinbart, der nicht in einem EU-Mitgliedstaat liegt, richtet sich die Wirksamkeit dieser Vereinbarung nach dem nationalen Recht des

---

[103] So auch Nordmeier 2010, 152 und Martiny in Sonnenberger 2009, Rz. 237 zu Art 4 Rom-I-VO.

[104] Reine Inlandsfälle (Anbieter und Nutzer mit Sitz in Österreich) werden in der Praxis kaum vorkommen, da alle bedeutenden Anbieter von Cloud-Services ihren Sitz nicht in Österreich haben.

[105] Verordnung (EG) Nr. 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen, ABl L 12/01, 1 vom 16.01.2001.

[106] Rechberger und Simotta 2009, Rz. 98.

[107] Art 60 Abs 1 EuGVVO.

[108] Horn in Fucik, Klauser und Kloiber 2009, Anmerkungen zu Art 23 EuGVVO.

[109] Art 23 Abs 2 EuGVVO.

[110] OGH in 2 Ob 192/07k, 24.01.2008.

vereinbarten Gerichts. Für österreichische Unternehmen kann allerdings eine allfällige Unzulässigkeit einer solchen Gerichtsstandsvereinbarung nach österreichischem bzw. europäischem Recht dennoch relevant sein, weil in diesem Fall trotzdem ein österreichisches Gericht angerufen werden könnte. Ob hier zur Prüfung der Zulässigkeit der Vereinbarung die EuGVVO oder nationales Recht anzuwenden ist, ist strittig.[111] Geht man von der Anwendbarkeit der EuGVVO aus, gelten wieder oben genannte Formvorschriften. Folgt man hingegen der Ansicht, dass die Zulässigkeit nach nationalem Recht zu beurteilen ist, oder – wie *Burgstaller und Neumayr*[112] – dass dieses ergänzend zur EuGVVO gilt, sind (zusätzlich) die Regeln der Jurisdiktionsnorm (JN)[113] relevant. Die Vereinbarung der ausschließlichen Zuständigkeit eines ausländischen Gerichts nach § 104 JN wird als zulässig angesehen, wenn seine Urteile im Inland vollstreckbar sind.[114] § 104 JN erfordert allerdings den urkundlichen Nachweis der Vereinbarung, der wiederum einer Unterschrift[115] oder einer elektronischen Signatur bedarf.[116] Nach dieser Rechtsansicht wären Gerichtsstandsvereinbarungen im Rahmen der Vertragsbedingungen von Cloud-Services generell unzulässig. In diesem Fall würde sich der Gerichtsstand nach dem Gesetz richten. Für österreichische Unternehmen als Nutzer von Cloud-Services kann sich auf diese Weise die Möglichkeit ergeben, Anbieter von Cloud-Services in Österreich zu klagen, die ihren Sitz nicht innerhalb der EU haben und daher in der Regel versuchen werden, in den AGB einen Gerichtsstand außerhalb der EU zu vereinbaren. Solche Klagen können insbesondere auf den Gerichtsstand des Vermögens nach § 99 JN gestützt werden, sofern der Anbieter des Cloud-Service in Österreich Vermögen oder eine ständige Vertretung besitzt. Allerdings sollte nicht übersehen werden, dass in diesem Fall bei gültiger Rechtswahl, die vom Gerichtsstand völlig getrennt zu betrachten ist, dennoch ausländisches Recht anzuwenden sein kann.

Im Fall des Fehlens einer Gerichtsstandsvereinbarung richtet sich der Gerichtsstand nach der EuGVVO, sofern ein Auslandsbezug besteht und der Beklagte seinen (Wohn-)Sitz in einem EU-Mitgliedstaat hat.[117] Ist letzteres nicht der Fall und somit die EuGVVO nicht anwendbar, gilt das soeben für den Fall der Ungültigkeit der Gerichtsstandsvereinbarung Gesagte. Die Gerichtszuständigkeit ist dann nach den Geset-

111 Burgstaller und Neumayr in Burgstaller und Neumayr 2010, Rz. 9 zu Art 23 EuGVVO.
112 Burgstaller und Neumayr in Burgstaller und Neumayr 2010, Rz. 9 zu Art 23 EuGVVO.
113 Gesetz vom 1. August 1895, über die Ausübung der Gerichtsbarkeit und die Zuständigkeit der ordentlichen Gerichte in bürgerlichen Rechtssachen (Jurisdiktionsnorm - JN), RGBl 111/1895 idF BGBl I 58/2010.
114 Fucik in Fucik, Klauser und Kloiber 2009, Anmerkungen zu § 104 JN.
115 OGH in 2 Ob 159/08h, 22.01.2009.
116 Rechberger in Rechberger 2006, Rz. 10 zu § 104 JN.
117 Rechberger und Simotta 2009, Rz. 117.

zen jenes Staates zu beurteilen, in dem die Klage erhoben wurde. Für nähere Details zu möglichen Gerichtsständen sei auf die Literatur verwiesen.[118]

3.1.4. Vertragsrechtliche Einordnung

Da die meisten Anbieter von Cloud-Services weder ihre Hauptniederlassung noch eine Zweigniederlassung in Österreich haben, wird österreichisches Recht in der Praxis nach dem bisher Gesagten auf den Vertrag über einen Cloud-Service nur selten anzuwenden sein. Dennoch werden im Folgenden für diesen Fall – in der gebotenen Kürze – die Konzepte des Cloud Computing in das Begriffssystem des österreichischen Allgemeinen Bürgerlichen Gesetzbuchs (ABGB)[119] eingeordnet. Dies dient der ergänzenden Vertragsauslegung, insbesondere im Hinblick auf Haftung und Gewährleistung, und legt die gesetzlichen Leitbilder fest, anhand welcher die Zulässigkeit von Vertragsklauseln geprüft werden kann[120] – allerdings, wie gesagt, nur falls österreichisches Recht auf einen Vertrag anwendbar ist. Wenn dies nicht der Fall ist, kann das österreichische Vertragsrecht dennoch als Maßstab herangezogen werden, mit dem die Bedingungen eines Vertrags über einen Cloud-Service verglichen werden können, um abzuschätzen, wie vorteilhaft oder unvorteilhaft diese sind.

Bei Verträgen über Cloud-Services kann es sich um gemischte Verträge handeln. Das sind Verträge, die sich nicht einem einzelnen der gesetzlich geregelten Vertragstypen – z.B. Miet- oder Werkvertrag – zuordnen lassen, sondern aus mehreren dieser Vertragstypen zusammengesetzt sind, was zulässig und auch durchaus üblich ist.[121] Meistens wendet man bei solchen Verträgen nach der so genannten Kombinationstheorie auf jede einzelne darin festgelegte Leistungspflicht die Vorschriften jenes Vertragstyps an, dem diese Pflicht zuzuordnen ist.[122]

Die im Hinblick auf entgeltliche[123] Cloud-Services infrage kommenden Vertragstypen des österreichischen Rechts sind Mietvertrag, Werkvertrag und (freier) Dienstvertrag. Der Mietvertrag nach §§ 1090 ff ABGB ist ein Vertrag über die Überlassung einer unverbrauchbaren, beweglichen oder unbeweglichen, körperlichen oder unkörperlichen Sache zum Gebrauch.[124] Hauptpflicht des Vermieters ist es, die Mietsache in einem Zustand zu übergeben und zu erhalten, welcher den vertraglich bedungenen Ge-

---

[118] Z.B. Rechberger und Simotta 2009, Rechberger 2006, Fucik, Klauser und Kloiber 2009 und Burgstaller und Neumayr 2010.
[119] JGS 946/1811 idF BGBl I 135/2009.
[120] Zum Zweck der vertragsrechtlichen Einordnung ausführlich Grapentin 2009, 188 ff.
[121] Koziol und Welser 2007, 14.
[122] OGH in 7 Ob 120/98t, 10.08.1998 und Koziol und Welser, Bürgerliches Recht 2007, 14.
[123] Auf unentgeltliche Cloud-Services, welche meist anderen Vertragstypen zuzuordnen sind, wird hier nicht eingegangen. Die nachfolgend behandelten Vertragstypen setzen – mit Ausnahme des Dienstvertrages (Koziol und Welser 2007, 251) – ein Entgelt voraus.
[124] Koziol und Welser 2007, 216.

brauch ermöglicht.[125] Für die Begründung des Mietverhältnisses ist es nicht erforderlich, dass der Mieter den Besitz des Mietgegenstandes erlangt.[126] Der überlassene Gebrauch muss auch kein ausschließlicher sein, Mitbenützung oder zeitweilige Benützung kann ebenfalls Gegenstand eines Mietvertrages sein.[127] Dies gilt ebenso für die Benützung eines unselbständigen Teiles einer Sache.[128] Kein Mietvertrag liegt jedoch vor, wenn der Vermieter ein jederzeitiges Widerrufsrecht hat.[129]

In einem Dienstvertrag (§§ 1151 ff ABGB) verpflichtet sich jemand für bestimmte oder unbestimmte Zeit zu einer Dienstleistung für einen anderen. Geschuldet ist die Arbeit, nicht ein bestimmter Erfolg.[130] Die Arbeit erfolgt in persönlicher Abhängigkeit, d.h. insbesondere nach den Weisungen und unter der Aufsicht des Dienstgebers. Fehlt dieses Element, wird aber dennoch kein Erfolg geschuldet, handelt es sich um einen freien Dienstvertrag.[131]

Beim Werkvertrag (§§ 1165 ff ABGB) wird hingegen ein Erfolg geschuldet, d.h. ein bestimmtes Ergebnis und nicht nur die bloße Arbeit. Dies ist der wesentliche Unterschied zum Dienstvertrag[132] und hat weit reichende Konsequenzen. Insbesondere gilt für Werkverträge dasselbe Gewährleistungsregime wie für Kaufverträge.[133] Soweit zu den Grundregeln dieser Vertragstypen, die im Folgenden auf die einzelnen in Abschnitt 2.4 vorgestellten Cloud-Service-Modelle und deren verschiedene Ausprägungen angewendet werden. Die tatsächliche Einordnung eines konkreten Vertrages ist anhand der Gegebenheiten des Einzelfalles mithilfe der hier dargestellten Grundregeln vorzunehmen und kann daher von der nachfolgend getroffenen Einordnung abweichen.

Verträge über die Nutzung von IaaS haben in der Regel mietvertraglichen Charakter.[134] Dies gilt sowohl für Infrastruktur-Services als auch für Ressourcen-Sets. Der Anbieter überlässt dem Nutzer einen (virtuellen) Server (Ressourcen-Set) oder einzelne Komponenten davon (Infrastruktur-Service), wie dessen Rechenkapazitäten oder Speicherplatz[135], gegen Entgelt zum Gebrauch und sorgt dafür, dass der Cloud-Service benutzbar bleibt, indem er den entsprechenden Server in Betrieb und dessen Verbindung zum Internet aufrecht hält. Somit liegen die Eigenschaften eines Mietvertrages vor. Wie

---

[125] § 1096 ABGB.
[126] RIS-Justiz RS0025022 und Fallenböck und Trappitsch 2002.
[127] Würth in Rummel, Rz. 2 zu § 1090 ABGB.
[128] Binder in Schwimann, Rz. 2 zu § 1090 ABGB.
[129] Würth in Rummel, Rz. 4 zu § 1090 ABGB und Binder in Schwimann, Rz. 2 zu § 1090 ABGB.
[130] Koziol und Welser 2007, 249.
[131] Krejci in Rummel, Rz. 83 zu § 1151 ABGB und Koziol und Welser 2007, 249 f.
[132] Krejci in Rummel, Rz. 117 zu § 1166 ABGB und Koziol und Welser 2007, 255.
[133] § 922 ff iVm 1167 ABGB.
[134] Schulz und Rosenkranz 2009, 233 zur deutschen Rechtslage.
[135] Für die Zurverfügungstellung von Speicherplatz so auch Fallenböck und Trappitsch 2002, Thiele 2004 und Landesgericht Klagenfurt in 1 R 171/08d, 19.06.2008. Zur deutschen Rechtslage Grapentin 2009, 202 f.

oben erwähnt, spielt es dabei keine Rolle, dass der Nutzer nicht Besitz am physischen Server erlangt und diesen nicht alleine nutzt. Je nach Art und Umfang der vereinbarten weiteren Leistungspflichten des Anbieters – z.B. Datensicherung – können im Sinne der oben beschriebenen Kombinationstheorie zu den mietvertraglichen Elementen des Vertrages dienstvertragliche oder werkvertragliche hinzutreten.[136]

Im Fall der Überlassung von Rechenkapazität könnte an einen dienstvertraglichen Schwerpunkt des Vertrages gedacht werden, weil dabei ein vom Nutzer vorgegebener Vorgang – abstrakt formuliert: die Berechnung – vollzogen werden soll. Ein Werkvertrag kommt hingegen von vornherein nicht infrage, weil für die Berechnung und deren Ergebnis alleine der Nutzer verantwortlich ist und der Anbieter damit keinen Erfolg schuldet. Dies spricht allerdings nicht nur gegen den Werk- sondern auch gegen den Dienstvertrag, denn zwar handelt es sich um einen Vorgang, doch der Anbieter ist daran nicht beteiligt.[137] Der Nutzer führt die Berechnung auf einem Server des Anbieters aus, den ihm dieser zu diesem Zweck zur Verfügung stellt. Die Hauptleistung des Vertrages entspricht daher den Eigenschaften der Miete einer Sache. Analog wird von Lehre und Rechtsprechung auch im Zusammenhang mit dem Mobilfunkvertrag argumentiert.[138] Da das Mobilfunknetz vollautomatisch, ohne Zutun des Betreibers die Verbindung aufbaue, stelle der Betreiber kein Werk her, vielmehr weise die Nutzung des Mobilfunknetzes mietvertragliche Elemente auf. Somit hat auch die Überlassung von Rechenkapazität keinen dienstvertraglichen sondern einen – im vorhergehenden Absatz bereits erläuterten – mietvertraglichen Schwerpunkt.

SaaS-Verträge sind ebenfalls primär als Mietverträge zu qualifizieren.[139] Sowohl für die Bereitstellung der Software selbst, als auch für die Bereitstellung des Speicherplatzes – falls die in Zusammenhang mit dem Cloud-Service stehenden Daten beim Anbieter gespeichert werden – gilt das oben zu den IaaS-Verträgen Gesagte. Der Gegenstand der Nutzung ist gegenüber IaaS lediglich ausgedehnt und umfasst neben Server und Betriebssystem im Fall von SaaS auch Anwendungssoftware. Auch das verwandte ASP[140] wird in der Regel als Miete qualifiziert,[141] und SaaS unterscheidet sich von ASP – wie oben unter Punkt 2.4.3 angesprochen – im Wesentlichen nur durch die gemeinsame Nutzung einer einzigen Software-Instanz durch mehrere Nutzer. Da die nicht alleinige Nutzung der Mietsache – wie bereits mehrfach betont – an der Qualifi-

[136] Schulz und Rosenkranz 2009, 234 zur deutschen Rechtslage.
[137] Vgl. zur Abgrenzung von Werkvertrag und Mietvertrag Krejci in Rummel, Rz. 133 zu § 1166 ABGB.
[138] Zankl 2005, ihm folgend OGH in 6 Ob 69/05y, 21.04.2005.
[139] Pohle und Ammann 2009b, 626 f. zur deutschen Rechtslage.
[140] Siehe dazu Punkt 2.4.3, S. 30.
[141] Fallenböck und Trappitsch 2002, zur deutschen Rechtslage wurde dies höchstgerichtlich anerkannt: BGH in XII ZR 120/04, 15.11.2006, MMR 2007, 243.

kation als Mietvertrag allerdings nichts ändert, ist auch SaaS als Miete zu betrachten, wenn ASP als Miete qualifiziert wird.

Das Zurverfügungstellen einer Entwicklungsumgebung im Rahmen eines PaaS-Angebots wird ähnlich wie SaaS zu beurteilen sein, da es sich konzeptuell nicht wesentlich davon unterscheidet, denn auch eine Entwicklungssoftware kann als „Anwendungssoftware" betrachtet werden. Der Betrieb einer Laufzeitumgebung, auf der die Software des Nutzers unter dessen Kontrolle ausgeführt wird, hat ähnlichen Charakter, ist allerdings konzeptuell näher bei den Ressourcen-Sets (IaaS) anzusiedeln. Dies ändert allerdings nichts an der primär mietvertraglichen Qualifikation.

Zusammenfassend kann somit gesagt werden, dass trotz des Variantenreichtums des Cloud Computing Verträge über Cloud-Services in der Regel primär mietvertraglichen Charakter haben. Gehen die vereinbarten Leistungen des Anbieters über jene Tätigkeiten hinaus, die für die Aufrechterhaltung der Benützbarkeit der Mietsache erforderlich sind, treten dienstvertragliche oder werkvertragliche Elemente hinzu. Diese Vertragsteile sind dann – der eingangs beschriebenen Kombinationstheorie folgend – nicht nach Mietvertragsrecht, sondern nach Dienst- bzw. Werkvertragsrecht zu beurteilen.

3.1.5. Verwendung von Allgemeinen Geschäftsbedingungen

Wie bereits erwähnt, werden Verträge über Cloud-Services in den allermeisten Fällen durch Annahme der vom Anbieter für eine Vielzahl von Geschäften einheitlich vorformulierten Vertragsbedingungen geschlossen. Solche werden von der österreichischen Rechtsordnung als Allgemeine Geschäftsbedingungen (AGB) oder Vertragsformblätter bezeichnet.[142] Für AGB gelten einige besondere Regelungen, die im Wesentlichen dazu dienen, jenen Vertragspartner, von dem die AGB nicht stammen, vor Nachteilen zu schützen, und damit der Tatsache Rechnung tragen, dass ein potenzieller Nutzer nur unter den vorgegebenen Bedingungen abschließen kann, will er nicht auf das Angebot verzichten. Die im Folgenden behandelten Regeln der Geltungs- und Inhaltskontrolle gelten auch für Verträge zwischen Unternehmern.[143] Sie gelten allerdings – wie die obigen Ausführungen – nur für den Fall, dass österreichisches Vertragsrecht anwendbar ist.

Als Geltungskontrolle bezeichnet man die Regelung des § 864a ABGB, nach welcher für den Vertragspartner überraschende und nachteilige Bestimmungen in AGB

[142] Koziol und Welser 2006, 130 f. Eine Differenzierung der beiden Begriffe „AGB" und „Vertragsformblätter" erscheint nicht notwendig, weil die Ausdrücke im Gesetz stets gemeinsam verwendet werden (Krejci in Rummel, Rz. 232 zu § 879 ABGB). Im Folgenden wird der Begriff „AGB" verwendet.

[143] Krejci 2008, 275.

nicht Vertragsbestandteil werden, wenn der Vertragspartner nicht besonders darauf hingewiesen wurde. Diese Regelung soll solche Nachteile treffen, die zwar grundsätzlich durchaus zulässig sind, mit denen der Vertragspartner aufgrund der Umstände aber nicht zu rechnen brauchte und denen er bei Kenntnis nicht ohne weiteres zugestimmt hätte.[144]

Die Inhaltskontrolle nach § 879 Abs 3 ABGB zielt hingegen auf Bestimmungen in AGB ab, die den Vertragspartner unter Berücksichtigung aller Umstände noch deutlich stärker – „gröblich" – benachteiligen. Diese sind nichtig, sofern sie nicht eine der beiderseitigen Hauptleistungen festlegen. Der Begriff der Hauptleistungen ist dabei eng zu verstehen und umfasst nur jene Vertragsbestandteile, welche die individuelle zahlenmäßige Umschreibung der beiderseitigen Leistungen festlegen.[145] Nicht umfasst sind bereits die nähere Umschreibung der vertragstypischen Leistung und Vertragsbestandteile zu Fragen, die auch gesetzlich geregelt sind, für den Fall, dass ein Vertrag darüber keine Regelung vorsieht (dispositives Recht).[146] Somit unterliegen all diese Vertragsbestandteile dem Regime des § 879 Abs 3 ABGB, können also ungültig sein, wenn sie als gröblich benachteiligend zu qualifizieren sind. Ob eine Bestimmung gröblich benachteiligend ist, orientiert sich am Maßstab des dispositiven Rechts, sofern dieses für den konkreten Fall eine Regelung vorsieht.[147] Nicht jede Abweichung vom dispositiven Recht ist allerdings gröblich benachteiligend.[148] Insbesondere kann aber eine Abweichung vom dispositiven Recht dann gröblich benachteiligend sein, wenn sie sachlich nicht gerechtfertigt ist.[149]

Im Zusammenhang mit Cloud Computing kann der Inhaltskontrolle große praktische Bedeutung zukommen.[150] Dies gilt insbesondere für Verträge mit mietvertraglichem Charakter, denn es ist die Pflicht des Vermieters, den Mietgegenstand in brauchbarem Zustand zu erhalten und den Mieter im Gebrauch nicht zu stören.[151] Verträge über Cloud-Services sehen aber in der Regel Einschränkungen der Verfügbarkeit und Wartungsintervalle vor.[152] Auf das Konzept des Mietrechts umgelegt bedeutet dies aber

---

144 Krejci 2008, 275.
145 Krejci in Rummel, Rz. 238 zu § 879 ABGB, OGH in 1 OB 538/93, 01.05.1993, OGH in 3 Ob 146/99p, 24.05.2000 und OGH in 9 Ob 15/05d, 04.05.2006.
146 Krejci in Rummel, Rz. 238 zu § 879 ABGB und dem folgend OGH in 9 Ob 15/05d, 04.05.2006.
147 Apathy/Riedler in Schwimann, Rz. 30 zu § 879 ABGB, Bollenberger in Koziol, Bydlinski und Bollenberger, Rz. 23 zu § 879 ABGB und Krejci in Rummel, Rz. 240 zu § 879 ABGB mit weiteren Nachweisen.
148 Krejci in Rummel, Rz. 240 zu § 879 ABGB.
149 Bollenberger in Koziol, Bydlinski und Bollenberger, Rz. 23 zu § 879 ABGB und Krejci in Rummel, Rz. 240 zu § 879 ABGB mit weiteren Nachweisen.
150 Zum deutschen Recht vgl. Pohle und Ammann 2009b, 627.
151 § 1096 Abs 1 ABGB.
152 Siehe unten Kapitel 5, S. 81.

nichts anderes, als dass zu gewissen Zeiten der Gebrauch der Mietsache nicht möglich ist. Solche Einschränkungen können auch nicht – im Sinne der eben besprochenen Ausnahme – als Vertragsbestandteile verstanden werden, welche die Hauptleistung festlegen, da es sich dabei um Abweichungen von einer Regel des dispositiven Rechts – nämlich der Pflicht des Vermieters – handelt. § 879 Abs 3 ABGB ist daher anwendbar und eine gröbliche Benachteiligung des Nutzers durch die Einschränkungen zu prüfen. In der Regel werden solche Einschränkungen aber sachlich gerechtfertigt sein, da eine permanente Verfügbarkeit extrem schwierig aufrechtzuerhalten ist und die damit verbundenen Kosten meist nicht im Interesse des Nutzers sein werden. Ob einzelne Klauseln vordefinierter Vertragsbedingungen dann tatsächlich aufgrund der Geltungs- oder Inhaltskontrolle nicht Vertragsinhalt geworden sind, ist im Einzelfall anhand der hier dargelegten Regeln und der zahlreichen Beispiele aus der Judikatur[153] zu prüfen.

3.1.6. Die Rechtsnatur von Service Level Agreements

Der Begriff „Service Level Agreement“ (SLA) wird in der Praxis nicht einheitlich verwendet.[154] In der vorliegenden Diplomarbeit wird darunter – der wörtlichen Bedeutung folgend – die Beschreibung der Qualität und des Erfüllungsgrades der geschuldeten Leistung verstanden.[155] Darüber hinaus werden in einem SLA in der Regel auch Sanktionen für den Fall der Schlecht- oder Nichterfüllung definiert.[156] Damit ist im Zusammenhang mit Cloud Computing ein SLA – sofern ein solches vereinbart ist – ein wesentlicher Bestandteil des Vertrages über einen Cloud-Service. Über die Wirkung als Vertragsinhalt hinaus kommt einem SLA aber keine eigenständige rechtliche Bedeutung zu.

3.2. Cloud Computing und Datenschutz

3.2.1. Anwendbares Datenschutzrecht

Das europäische Datenschutzrecht folgt dem Grundsatz des Territorialitätsprinzips. Dies ist in Art 4 der Datenschutzrichtlinie (DS-RL)[157] verankert und bedeutet, dass sich der Datenschutz nach dem nationalen Recht jenes Staates richtet, in dem die daten-

---

153 Krejci in Rummel, Rz. 245b ff. zu § 879 ABGB, Apathy/Riedler in Schwimann, Rz. 32 f. zu § 879 ABGB und Bollenberger in Koziol, Bydlinski und Bollenberger, Rz. 24 f. zu § 879 ABGB.

154 Niemann und Paul 2009, 447, Schumacher 2006, Fn. 2.

155 Niemann und Paul 2009, 447, Schumacher 2006, 12.

156 Schumacher 2006, 13.

157 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281, 31 vom 23.11.1995. Dazu ausführlich Mayer-Schönberger und Brandl 2006, 11 ff.

schutzrechtlich relevanten Handlungen vorgenommen werden.[158] In Österreich ist Datenschutz im Datenschutzgesetz 2000 (DSG 2000)[159] geregelt, mit dessen Verabschiedung Österreich seiner Verpflichtung zur Umsetzung der DS-RL nachkam.

Gemäß den von Art 4 DS-RL vorgegebenen Prinzipien regelt § 3 DSG 2000 den räumlichen Anwendungsbereich des Gesetzes. Dem Territorialitätsprinzip entsprechend ist das DSG 2000 daher grundsätzlich auf jede Datenverwendung in Österreich anwendbar. Ob die Daten von österreichischen Staatsbürgern stammen, oder wo sie ursprünglich erhoben wurden spielt dabei keine Rolle. Der Begriff der Verwendung von Daten ist sehr weit definiert und umfasst jede Art der Handhabung von Daten.[160] Nur das reine Durchleiten der Daten durch Österreich ist von der Anwendung des DSG 2000 ausgenommen.[161]

Es bestehen zwei Ausnahmen vom Territorialitätsprinzip. Einerseits eine Einschränkung für Unternehmen, die ihren Sitz in einem anderen EU-Mitgliedstaat haben. Für diese gilt das nationale Recht ihres Sitzstaates, wenn die Datenverwendung zwar in Österreich erfolgt, der Zweck der Datenverwendung aber keiner in Österreich gelegenen Niederlassung[162] dieses Unternehmens zuzurechnen ist.[163] Andererseits eine Erweiterung des Anwendungsbereichs, denn das DSG 2000 gilt auch dann, wenn die Datenverwendung in einem anderen EU-Mitgliedstaat erfolgt, der Zweck der Datenverwendung aber einer in Österreich gelegenen Niederlassung zuzurechnen ist.

Österreichisches Datenschutzrecht und damit die nachfolgenden Ausführungen sind somit auf alle in Österreich vorgenommenen datenschutzrechtlich relevanten Handlungen von Unternehmen mit Sitz in Österreich oder mit Sitz außerhalb der EU anzuwenden, zudem auf solche Handlungen von Unternehmen mit Sitz in einem anderen EU-Mitgliedstaat dann, wenn die Handlungen einer in Österreich gelegenen Niederlassung zuzurechnen sind, und auf in einem anderen EU-Mitgliedstaat vorgenommene datenschutzrechtlich relevante Handlungen dann, wenn diese der österreichischen Niederlassung eines Unternehmens zugeordnet werden können, wo auch immer letzteres seinen Sitz hat.

---

158 Niemann und Paul 2009, 448.

159 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl I 165/1999 idF BGBl I 135/2009.

160 § 4 Z 8-11 DSG 2000. Näheres siehe unten sowie in Dohr et al. 2009, Anmerkungen 8-13 zu § 4 DSG 2000.

161 § 3 Abs 3 DSG 2000. Näheres siehe in Dohr et al. 2009, Anmerkung 4 zu § 3 DSG 2000.

162 § 4 Z 15 DSG 2000 definiert den Begriff Niederlassung weit, als „jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt."

163 § 3 Abs 2 DSG 2000.

3.2.2. Grundlagen des österreichischen Datenschutzrechts

Geschützt werden durch das DSG 2000 nicht etwa Daten an sich, sondern (natürliche und juristische) Personen vor dem Missbrauch ihrer Daten[164]. § 1 DSG 2000 normiert ein im Verfassungsrang stehendes Grundrecht auf Datenschutz, welches in den nachfolgenden Bestimmungen näher ausgestaltet und zum Teil eingeschränkt wird. Durchsetzen kann der Einzelne die ihm aus dem DSG 2000 erwachsenden subjektiven Rechte sowohl gegenüber dem Staat als auch gegenüber Privaten, denn das DSG 2000 gilt im öffentlichen und im privaten Bereich und sieht für beide Bereiche – mit wenigen Ausnahmen – dieselben Regelungen vor.[165]

Wie das bisher Gesagte – und auch der Langtitel des Gesetzes – bereits vermuten lässt, sind durch das DSG 2000 nur personenbezogene Daten geschützt. Diese definiert § 4 Z 1 DSG 2000 als Angaben über von der Datenverarbeitung Betroffene, deren Identität bestimmt oder bestimmbar ist. Solche Angaben sind z.B. Name, Adresse, Lebensgewohnheiten, Intelligenzquotient, aber auch Werturteile (z.B. „ist ein schlechter Zahler“) sowie Foto, Fingerabdruck etc.[166] Dies schließt auch indirekt personenbezogene Daten ein. Das sind Daten, die zwar ein berechtigter, vom Verwender verschiedener Dritter dem Betroffenen zuordnen kann, aus denen aber der Verwender nur mit Hilfe rechtlich für ihn nicht zulässiger Mittel auf die Identität des Betroffenen schließen kann.[167] Zu denken ist hier insbesondere an verschlüsselte oder pseudonymisierte Daten.[168] Letztere sind Daten, die anstatt des Namens der betroffenen Person eine eindeutige Nummer, Buchstabenkombination o.Ä. enthalten, welche nur vom Ersteller (mittels einer separaten Liste) wieder dem Namen der jeweiligen Person zugeordnet werden können. Für indirekt personenbezogene Daten gelten erleichterte Bestimmungen, insbesondere im Zusammenhang mit dem grenzüberschreitenden Datenverkehr.[169] Die erste wichtige Erkenntnis aus dem DSG 2000 im Hinblick auf Cloud Computing ist damit, dass jegliche Speicherung, Übertragung oder Verwendung von Daten, welche vollständig anonymisiert oder von vorn herein nicht personenbezogen sind, datenschutzrechtlich unbedenklich ist. Wenn daher im Folgenden im Zusammenhang mit

---

[164] *Dohr et al.* (2009, Anmerkung 2 zu § 4 DSG 2000) weisen darauf hin, dass der Gesetzgeber mit dem Begriff „Daten“ eher „Informationen“ im Sinne der Terminologie der angewandten Informatik meint, das sind Daten, die eine bestimmte Bedeutung, Wirkung und Relevanz haben.

[165] Jahnel 2003, 249. Zur Abgrenzung zwischen öffentlichem und privatem Bereich siehe § 5 DSG 2000. Zur Rechtsdurchsetzung siehe Punkt 3.2.6, S. 59.

[166] Pollirer, Weiss und Knyrim 2010, Anmerkung 2 zu § 4 DSG 2000.

[167] Mayer-Schönberger und Brandl 2006, 25.

[168] Pollirer, Weiss und Knyrim 2010, Anmerkung 2 zu § 4 DSG 2000.

[169] Siehe dazu unten Punkt 3.2.5, S. 56.

dem Datenschutz von „Daten“ die Rede ist, sind damit personenbezogene Daten gemeint.

Betroffene im Sinne des DSG 2000 können sowohl natürliche als auch juristische Personen sowie sonstige Personengemeinschaften sein, deren Daten verwendet werden.[170] Mit anderen Worten, jene Personen, auf die personenbezogene Daten „bezogen“ sind, die also durch das DSG 2000 geschützt werden sollen, werden als Betroffene bezeichnet. Das datenschutzrechtliche „Gegenüber“ der Betroffenen sind nach der Konzeption des DSG 2000 die Auftraggeber. Diese sind definiert als natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw. die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden, unabhängig davon, ob sie die Daten selbst verwenden oder damit einen Dienstleister beauftragen.[171] Dies wird in der Praxis häufig auf die Unternehmen zutreffen, die Cloud-Services nutzen.

Die dritte vom DSG 2000 vorgesehene Rolle ist jene des Dienstleisters. Dienstleister im Sinne des DSG 2000 sind natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw. Geschäftsapparate solcher Organe, wenn sie von Auftraggebern überlassene Daten im Rahmen der Herstellung eines Werkes verwenden.[172] Im Zusammenhang mit Cloud Computing kommt der Anbieter von Cloud-Services für die Rolle des Dienstleisters in Betracht. Die soeben beschriebenen Rollen und ihre Beziehungen, die im Laufe dieses Abschnitts noch ausführlich erläutert werden, sind in Abbildung 5 schematisch dargestellt.

[170] § 4 Z 3 DSG 2000. Der Schutz von Daten juristischer Personen ist eine Besonderheit des österreichischen Datenschutzrechts im internationalen Vergleich (Jahnel 2005, 200).
[171] § 4 Z 4 DSG 2000.
[172] § 4 Z 4 DSG 2000.

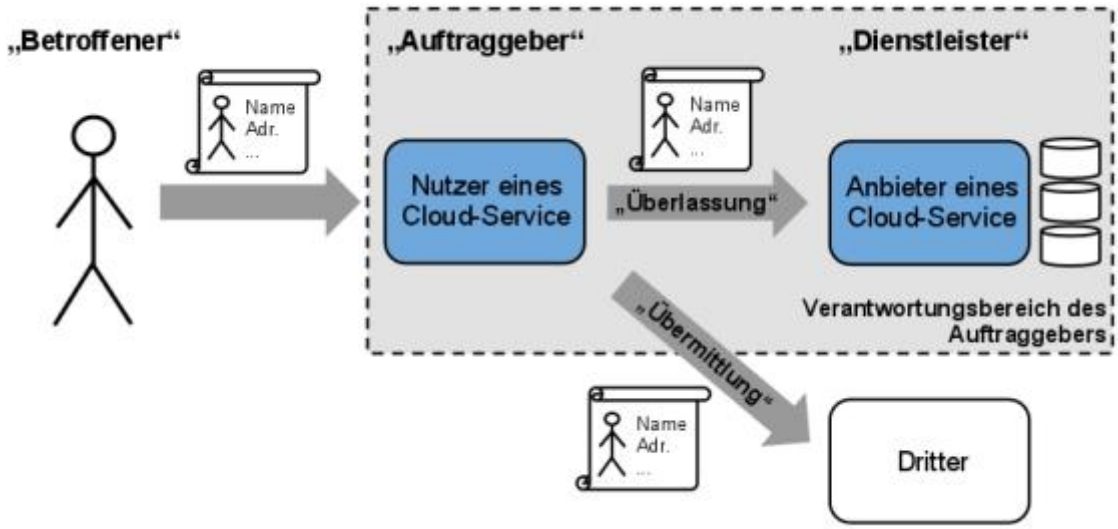


Abbildung 5 – Illustration der Rollen und Beziehungen des DSG 2000 im Kontext der Nutzung eines Cloud-Service (Die Schriftrolle symbolisiert die personenbezogenen Daten des Betroffenen. Zur „Überlassung“ siehe Punkt 3.2.3 (S. 53), zur „Übermittlung“ Punkt 3.2.4 (S. 56). Anzumerken ist, dass „Dienstleister“ und „Anbieter eines Cloud-Service“ nur unter den strengen, unter Punkt 3.2.3 beschriebenen Voraussetzungen gleichgesetzt werden dürfen.)[173]

Wie bereits erwähnt ist das Verwenden von Daten ein weit definierter Begriff, der jede Art der Handhabung von Daten umfasst, auch das bloße Speichern – und somit auch Webhosting – und bereits das Ermitteln sowie das Weitergeben.[174] Die Zulässigkeit der Datenverwendung richtet sich nach den §§ 6-9 DSG 2000. Daten dürfen insbesondere nur für festgelegte, eindeutige und rechtmäßige Zwecke verwendet werden und die Verwendung darf nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen verstoßen. Letzteres muss anhand des § 8 DSG 2000 bzw. im Fall von sensiblen Daten – das sind Daten über „rassische und ethnische Herkunft“, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben natürlicher Personen[175] – anhand des § 9 DSG 2000 geprüft werden.

Näheres zur Zulässigkeit der Datenverwendung – und auch zur Meldepflicht, die in § 17 DSG 2000 geregelt ist – kann hier außer Betracht bleiben, denn die allgemeinen Regeln zur Verwendung von Daten gelten ohnehin für jede Datenverwendung, unabhängig davon, ob die Daten im Rahmen der Nutzung eines Cloud-Service verwendet werden. Als generelle Voraussetzung für jede Verwendung von Daten ist die Zulässig-

[173] Quelle: Eigene Darstellung, erstellt mit *Google Apps* (siehe dazu Abschnitt 5.7, S. 111).
[174] § 4 Z 8-11 DSG 2000. Näheres siehe Dohr et al. 2009, Anmerkungen 4 und 8-13 zu § 4 DSG 2000. Zum Speichern (Webhosting) siehe DSK in K120.819/006-DSK/2003, 14.11.2003, dazu Knyrim 2004.
[175] § 4 Z 2 DSG 2000.

keit damit auch eine Voraussetzung für die rechtmäßige Überlassung von Daten, auf die im Folgenden näher eingegangen wird.

3.2.3. Überlassung von Daten an Dienstleister

Das DSG 2000 sieht eine spezifische Regelung für den Fall des Outsourcings der Verarbeitung personenbezogener Daten vor.[176] Wie in Abbildung 5 dargestellt, wird dies vom Gesetz als „Überlassen"[177] von Daten an einen Dienstleister bezeichnet. Ist daher vom „Überlassen" von Daten die Rede, bedeutet dies stets, dass der Empfänger der Daten als Dienstleister zu qualifizieren ist. Davon ist das „Übermitteln" zu unterscheiden, der Begriff für die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister.[178]

Die Überlassung von Daten an einen Dienstleister ist im Vergleich zur Übermittlung von Daten im Sinne des DSG 2000 gesetzlich privilegiert. Mit anderen Worten, die Voraussetzungen einer Überlassung sind weniger streng als jene einer Übermittlung.[179] Insbesondere bedarf es bei einer Überlassung nicht der Zustimmung des Betroffenen.[180] Dies erscheint gerechtfertigt, da der Auftraggeber nach dem Modell des Gesetzes bei der Überlassung im Gegensatz zur Übermittlung für die Datenverarbeitung verantwortlich bleibt.[181] Um dies sicherzustellen, muss der Dienstleister, an welchen Daten überlassen werden, die Voraussetzungen der §§ 10 und 11 DSG 2000[182] erfüllen. Diese umfassen die Gewährleistung einer rechtmäßigen und sicheren Datenverarbeitung[183] und die Pflichten, die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden[184] sowie weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen.[185] Dies bedeutet im Umkehrschluss, wenn der Dienstleister eigenständige Entscheidungen über die Verwendung der Daten trifft, liegt keine bloße Datenüberlassung, sondern eine – strengeren Voraussetzungen unterliegende – Datenübermittlung vor.[186] Genau genommen ist in diesem Fall die Bezeichnung „Dienstleister" im Sinne des DSG 2000 nicht mehr zutreffend.

---

176 Pohl 2009, 77 ff. Einschlägig sind die §§ 10-13 DSG 2000.
177 § 4 Z 11 DSG 2000.
178 § 4 Z 12 DSG 2000.
179 Knyrim, Siegel und Autengruber 2004.
180 Im Gegensatz zur Übermittlung von Daten (§ 7 Abs 2 DSG 2000) muss nicht geprüft werden, ob durch die Weitergabe der Daten schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt werden.
181 Dohr et al. 2009, Anmerkung 4 zu § 11 DSG 2000. Der Auftraggeber haftet für Auswahlverschulden im Hinblick auf den Dienstleister (Knyrim, Siegel und Autengruber 2004).
182 § 11 DSG 2000 befindet sich im Volltext in Anhang A.
183 § 10 Abs 1 Z 1 und § 11 Abs 1 Z 2 iVm § 14 DSG 2000. § 14 DSG 2000 befindet sich im Volltext in Anhang A.
184 § 11 Abs 1 Z 1 DSG 2000.
185 § 11 Abs 1 Z 3 DSG 2000.
186 Sehrschön 2010, 45 f. und Knyrim, Siegel und Autengruber 2004.

Voraussetzung der Datenüberlassung ist gemäß § 10 DSG 2000 auch eine Vereinbarung zwischen Auftraggeber und Dienstleister. Diese Vereinbarung kann Teil des zwischen Auftraggeber und Dienstleister geschlossenen Vertrages sein oder wird eigenständig abgeschlossen und in diesem Fall als Dienstleistervertrag bezeichnet.[187] Obwohl dies vom Gesetz nicht ausdrücklich gefordert ist, wird empfohlen, den Vertrag zu Beweiszwecken schriftlich abzufassen und auch die ohnedies kraft Gesetzes für den Dienstleister geltenden Pflichten[188] darin zu vereinbaren.[189] Vereinbarungen bezüglich der näheren Ausgestaltung der Dienstleisterpflichten müssen ohnehin schriftlich festgehalten werden.[190] Bei Überlassung von Daten in das Ausland ist eine Zusage des Dienstleisters über die Einhaltung der Dienstleisterpflichten erforderlich, die ebenfalls schriftlich vorliegen muss.[191]

Im Hinblick auf das Charakteristikum „on-demand self-service“ [192] ist eine solche verpflichtende Vereinbarung problematisch. Der Nutzer kann dem Anbieter keine Verpflichtungen auferlegen, wenn er dessen Vertragsbedingungen unverändert übernehmen muss. Denkbar ist jedoch, dass der Anbieter in Kenntnis der Rechtslage die entsprechenden Pflichten bereits in seine Vertragsbedingungen aufnimmt. Ist dies nicht der Fall, scheitert die Qualifikation der Weitergabe von Daten an einen Anbieter von Cloud-Services als Datenüberlassung im Sinne des DSG 2000. Allfällige, im Zusammenhang mit den überlassenen Daten stehende Verschwiegenheitspflichten des Auftraggebers müssen dem Dienstleister ebenfalls vertraglich überbunden werden (z.B. ärztliche Verschwiegenheitspflicht).[193] Hier scheidet allerdings die eben genannte Möglichkeit der pauschalen Aufnahme in die Vertragsbedingungen des Anbieters aus, weil Verschwiegenheitspflichten nutzerspezifisch sind und daher nur im Einzelfall vereinbart werden könnten. Da dies mit dem Kriterium des „on-demand self-service“ nicht vereinbar ist, scheitert somit ist die Weitergabe von Daten, die Verschwiegenheitspflichten unterliegen, an Anbieter von Cloud-Services, die dieses Kriterium erfüllen.

Darüber hinaus ist im Zusammenhang mit Cloud Computing die in § 10 Abs 1 letzter Satz DSG 2000 normierte Pflicht des Auftraggebers besonders zu beachten, sich von der Einhaltung der Vereinbarung mit dem Dienstleister durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffe-

[187] Knyrim, Siegel und Autengruber 2004.
[188] § 11 Abs 1 DSG 2000.
[189] Knyrim, Siegel und Autengruber 2004, Sehrschön 2010, 46 und Dohr et al. 2009, Anmerkung 4 zu § 10 DSG 2000.
[190] § 11 Abs 1 DSG 2000.
[191] § 12 Abs 5 DSG 2000. Näheres dazu siehe unter Punkt 3.2.5, S. 56.
[192] Zum Charakteristikum „on-demand self-service“ siehe Tabelle 1, S. 28.
[193] Dohr et al. 2009, Anmerkung 4 zu § 10 und Anmerkung 4 zu § 11.

nen Maßnahmen zu überzeugen.[194] Die korrespondierende Pflicht des Dienstleisters, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Dienstleisterpflichten notwendig sind, findet sich in § 11 Abs 1 Z 6 DSG 2000. Fraglich ist, inwieweit diese Kontrollpflicht des Auftraggebers im Fall eines standardisierten Cloud-Service, dessen Inanspruchnahme gänzlich ohne menschliche Interaktion auskommt, erfüllt werden kann. Zur entsprechenden Regelung des deutschen Bundesdatenschutzgesetzes (dBDSG)[195] – welcher allerdings der Passus „durch Einholung der erforderlichen Informationen" fehlt – wird zum Teil vertreten, dass Nutzer von Cloud-Services dieser Kontrollpflicht regelmäßig nicht ausreichend nachkommen können[196] bzw. dass dies zumindest problematisch sei[197]. Dies u.a. deshalb, weil dem Nutzer von Cloud-Services der tatsächliche physische Speicherort der Daten systembedingt nicht bekannt sei und er sich daher von der Einhaltung der vom Anbieter geforderten Schutzmaßnahmen im konkreten Rechenzentrum nicht überzeugen könne. Genau dies erfordere aber § 11 Abs 2 dBDSG iVm der Anlage zu § 9 dBDSG vom Nutzer.

Einer solchen Argumentation kann aber in Bezug auf die österreichische Rechtslage entgegengehalten werden, dass die Bereitstellung von Informationen durch den Dienstleister an den Nutzer zum Zwecke der Kontrolle im DSG 2000 – wie oben bereits angesprochen – ausdrücklich geregelt ist.[198] Übermittelt der Dienstleister dem Auftraggeber Informationen über die laufende Einhaltung der geforderten Sicherheitsmaßnahmen in allen in Frage kommenden Rechenzentren, spielt es keine Rolle, in welchem dieser Rechenzentren die Daten tatsächlich gespeichert sind.

Im Hinblick auf Cloud Computing zeigt sich, dass die Bedingungen für eine Qualifikation der Weitergabe von Daten an einen Anbieter von Cloud-Services als Datenüberlassung im Sinne des DSG 2000 sehr spezifisch und daher in der Praxis wohl meist nicht erfüllt sind. Dies betrifft insbesondere die Kontrollpflicht des Auftraggebers und die davor besprochenen Anforderungen an den Vertragsinhalt. Sind die Bedingungen einer Datenüberlassung nicht erfüllt, ist die Weitergabe von Daten an einen Anbieter von Cloud-Services nach der Konzeption des Gesetzes als Datenübermittlung zu qualifizieren.

---

194 Vgl. auch Art 17 Abs 2 DS-RL.

195 § 11 Abs 2 dBDSG.

196 Pohle und Ammann 2009a, 278

197 Niemann und Paul 2009, 449 und Schuster und Reichl 2010, 42, anderer Ansicht BITKOM 2009, 52. (Die Meinungen stammen zum Teil aus der Zeit vor der Neufassung des § 11 dBDSG, die allerdings für die hier einschlägige Rechtslage ohnehin keine nennenswerten Änderungen brachte.)

198 Dies einerseits durch die Auftraggeberpflicht des § 10 Abs 1 letzter Satz DSG 2000 („[…] durch Einholung der erforderlichen Informationen […]") und andererseits durch die Dienstleisterpflicht des § 11 Abs 1 Z 6 DSG 2000 („[…] dem Auftraggeber jene Informationen zur Verfügung zu stellen, […]").

3.2.4. Übermittlung von Daten an Dritte

Nach dem gesetzlichen Modell der Datenübermittlung ist der Empfänger der Daten selbst als Auftraggeber zu behandeln und muss daher seinerseits (im Verhältnis zum Betroffenen) die Anforderungen einer zulässigen Datenverwendung erfüllen. Dies gilt auch für den Dienstleister, wenn sich dieser nicht an die Anweisungen des Auftraggebers hält oder eigenständige Entscheidungen über die Datenverwendung trifft.[199] Zudem muss auch der Übermittler der Daten zu deren Verwendung befugt sein, damit die Übermittlung zulässig ist – eine Parallele zur Überlassung. Im Unterschied zu dieser muss aber bei der Datenübermittlung zusätzlich geprüft werden, ob diese gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen verstößt.[200]

Dies führt dazu, dass die Übermittlung von Daten in der Praxis[201] meist nur dann zulässig ist, wenn der Betroffene zugestimmt hat,[202] wenn es sich um indirekt personenbezogene Daten handelt,[203]oder die Übermittlung zur Erfüllung einer vertraglichen Verpflichtung des Auftraggebers gegenüber dem Betroffenen erforderlich ist.[204] Letzteres tritt im Zusammenhang mit Cloud Computing wohl nur selten ein, denn die meisten Aufgabenstellungen werden auch ohne Nutzung eines Cloud-Service erfüllbar sein.

3.2.5. Überlassung und Übermittlung von Daten in das Ausland

Eine besonders im Zusammenhang mit Cloud Computing sehr bedeutsame Einschränkung der Zulässigkeit einer Überlassung oder Übermittlung von Daten wurde oben noch nicht behandelt. Das bisher Gesagte gilt zunächst grundsätzlich nur für die Überlassung bzw. Übermittlung der Daten an Empfänger innerhalb des EWR.[205] Voraussetzung aller Überlassungen in das Ausland – d.h. auch in Mitgliedstaaten des EWR – ist zudem eine schriftliche Zusage des Dienstleisters über die Einhaltung der Dienstleisterpflichten nach § 11 Abs 1 DSG 2000.[206] Überlassungen oder Übermittlungen in Staaten außerhalb des EWR sind nur zulässig, wenn dabei ein angemessenes Datenschutzniveau gewahrt bleibt und sofern sie im Inland zulässig wären.[207] Die Wahrung eines angemessenen Datenschutzniveaus kann auf verschiedene Arten gewährleistet werden.

---

[199] Sehrschön 2010, 45 f. und Knyrim, Siegel und Autengruber 2004.
[200] § 7 Abs 2 Z 3 DSG 2000.
[201] Knyrim, Siegel und Autengruber 2004.
[202] § 8 Abs 1 Z 2 DSG 2000. Die Zustimmung muss in Kenntnis der Sachlage und für den konkreten Fall erfolgen (§ 4 Z 14 DSG 2000). Ein Widerruf ist jederzeit möglich (§ 8 Abs 1 Z 2 DSG 2000).
[203] § 8 Abs 2 DSG 2000.
[204] § 8 Abs 3 Z 4 DSG 2000 iVm § 8 Abs 1 Z 4 DSG 2000.
[205] § 12 Abs 1 DSG 2000. Die Formulierung der Bestimmung („an Empfänger in Vertragsstaaten“) lässt darauf schließen, dass es auf den Sitz des Empfängers und nicht auf den Ort der Datenspeicherung ankommt.
[206] § 12 Abs 5 DSG 2000.
[207] § 12 Abs 5 DSG 2000.

Zunächst kann durch Entscheidung der Europäischen Kommission und/oder Verordnung des Bundeskanzlers festgestellt werden, dass in einem Drittstaat ein angemessenes Datenschutzniveau herrscht.[208] Dies betrifft derzeit die Schweiz[209], Kanada[210], Argentinien[211], Guernsey[212], die Isle of Man[213] und die Färöer[214], sodass die Überlassung und die Übermittlungen von Daten in diese Staaten genehmigungsfrei zulässig sind[215] – wie gesagt, unter den oben dargelegten Voraussetzungen, die auch im Inland zu beachten sind und in allen nachfolgend beschriebenen Fällen ebenfalls gelten.

Für die USA besteht eine eigenständige Regelung, das Safe-Harbor-System.[216] US-Unternehmen können durch eine Erklärung gegenüber dem US-Department of Commerce dem „Safe Harbor" beitreten und verpflichten sich dadurch, die Safe Harbor Principles und die dazugehörenden Frequently Asked Questions (FAQ) zu beachten. An diese Unternehmen dürfen Daten aus der EU genehmigungsfrei überlassen oder übermittelt werden.[217]

In die übrigen Staaten ist eine Überlassung oder Übermittlung nur bei Zutreffen eines der in § 12 Abs 3 DSG 2000 aufgezählten Fälle ohne Genehmigung zulässig. Vier Fälle davon sind im gegebenen Zusammenhang bedeutsam. Besonders relevant ist der Fall, dass der Betroffene „ohne jeden Zweifel seine Zustimmung zur Übermittlung sei-

---

[208] § 12 Abs 2 DSG 2000.

[209] Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV), BGBl. II 521/1999.

[210] Entscheidung der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, ABl L 2, 13 vom 04.01.2002. Im Falle Kanadas besteht die Einschränkung, dass geprüft werden muss, ob der Datenempfänger unter das kanadische Datenschutzrecht fällt (Jahnel 2010, Rz. 4/139).

[211] Entscheidung der Kommission vom 30. Juni 2003 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Argentinien, ABl L 168, 19 vom 05.07.2003.

[212] Entscheidung der Kommission vom 21. November 2003 über die Angemessenheit des Schutzes personenbezogener Daten in Guernsey, ABl L 308, 28 vom 25.11.2003.

[213] Entscheidung der Kommission vom 28. April 2004 über die Angemessenheit des Schutzes personenbezogener Daten auf der Insel Man, ABl L 151, 48 vom 30.04.2004.

[214] Beschluss der Kommission vom 5. März 2010 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus, den das färöische Gesetz über die Verarbeitung personenbezogener Daten bietet, ABl L 58, 17 vom 09.03.2010.

[215] Eine aktuelle Übersicht dieser Entscheidungen/Beschlüsse ist auf der Website der Europäischen Kommission abrufbar (Europäische Kommission 2010b).

[216] Jahnel 2010, Rz. 4/140. Anzumerken ist, dass *Connolly* (2008) bei vielen US-Unternehmen deutliche Mängel in der praktischen Umsetzung des Save-Harbor-Systems feststellt, die insgesamt als systematische Schwächen des Systems betrachtet werden können.

[217] Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl L 215, 7 vom 25.08.2000.

ner Daten ins Ausland gegeben“[218] hat. Laut *Dohr et al.*[219] bedeutet dies, dass der Betroffene „in voller Kenntnis der Tragweite beweisbar zugestimmt haben“ muss.

Der zweite zu nennende Fall betrifft die indirekt personenbezogenen Daten.[220] Dies bedeutet im Ergebnis insbesondere, dass verschlüsselte Daten in beliebige Staaten genehmigungsfrei überlassen oder übermittelt werden dürfen.

Ein weiterer Fall, nämlich dass ein Vertrag mit dem Betroffenen nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann,[221] tritt im Zusammenhang mit Cloud Computing – wie zum analogen Fall unter Punkt 3.2.4 bereits erwähnt – wohl nur selten ein. Zu beachten ist allerdings, dass auch Verträge des Auftraggebers mit Dritten von dieser Ausnahme erfasst sind, sofern diese eindeutig im Sinne des Betroffen abgeschlossen wurden.[222]

Der vierte Fall ist die Erwähnung der Überlassung oder Übermittlung in einer Standardverordnung[223] oder Musterverordnung[224]. In der Praxis bedeutet dies, dass die Überlassung oder Übermittlung von Daten in Drittländer genehmigungsfrei zulässig ist, wenn die fragliche Datenanwendung einer in der Anlage zur Standard- und Muster-Verordnung 2004 (StMV 2004)[225] definierten Standard- oder Musteranwendung entspricht und der Empfängerkreis in der StMV 2004 mit einem Stern (*) gekennzeichnet ist.[226] Zu beachten ist, dass die fragliche Datenanwendung nicht über den in der StMV 2004 genau festgelegten Umfang der entsprechenden Standard- oder Musteranwendung hinausgehen darf.[227]

Liegt auch keiner der in § 12 Abs 3 DSG 2000 aufgezählten Fälle vor, so bedarf die Überlassung oder Übermittlung von Daten in Staaten ohne angemessenes Datenschutzniveau einer Genehmigung durch die Datenschutzkommission (DSK) nach § 13 DSG 2000. Eine solche wird erteilt, wenn der Auftraggeber glaubhaft macht, das entweder im konkreten Einzelfall ein angemessener Datenschutz besteht,[228] oder die schutzwürdigen Geheimhaltungsinteressen der Betroffenen ausreichend gewahrt wer-

---

[218] § 12 Abs 3 Z 5 DSG 2000.
[219] Dohr et al. 2009, Anmerkung 14 zu § 12 DSG 2000.
[220] § 12 Abs 3 Z 2 DSG 2000. Zum Begriff der indirekt personenbezogenen Daten siehe oben unter Punkt 3.2.2, S. 50.
[221] § 12 Abs 3 Z 6 DSG 2000.
[222] Jahnel 2010, Rz. 4/149.
[223] § 17 Abs 2 Z 6 DSG 2000.
[224] § 19 Abs 3.DSG 2000.
[225] Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 - StMV 2004), BGBl II 312/2004 idF BGBl II 255/2009.
[226] Jahnel 2010, Rz. 4/151.
[227] Jahnel 2010, Rz. 6/13.
[228] § 13 Abs 2 Z 1 DSG 2000. Dies trifft zu, wenn zwar nicht im gesamten Staat, aber etwa in einzelnen Bereichen ein angemessenes Datenschutzniveau besteht (Jahnel 2010, Rz. 4/158).

den.[229] Letzteres kann insbesondere mittels Vorlage eines Vertrages dargetan werden, worin sich der Empfänger zur Einhaltung bestimmter Datenschutzregeln verpflichtet.[230] Ein bedeutender Sonderfall hiervon sind die Standardvertragsklauseln der Europäischen Kommission.[231] Wenn diese einheitlichen Vorgaben im Vertrag zwischen Übermittler bzw. Überlasser und Empfänger der Daten unverändert verwendet werden, gilt der Nachweis des ausreichenden Datenschutzes als erbracht und die Überlassung oder Übermittlung wird genehmigt.[232]

Durch die Änderungen der DSG-Novelle 2010[233] sind nunmehr alternativ zu vertraglichen Zusicherungen auch einseitige Zusagen des Antragstellers geeignet, eine Genehmigung herbeizuführen.[234] Für Datenübermittlungen innerhalb von Konzernen kann dies insbesondere die Zusage sein, verbindliche unternehmensinterne Vorschriften über die Datenverarbeitung (Binding Corporate Rules, BCR) einzuführen.[235] Das Konzept der BCR sieht vor, dass für einen Konzern ein Datenschutzkonzept genehmigt und so die weltweite Datenübertragung innerhalb des Konzerns ermöglicht wird.[236] Dies hat sich aber in der Praxis in Europa noch nicht durchgesetzt.[237]

Zusammenfassend kann gesagt werden, dass die Weitergabe von Daten an einen Anbieter von Cloud-Services aufgrund der sehr spezifischen Anforderungen der Datenüberlassung in der Regel als Datenübermittlung zu qualifizieren sein wird. Eine solche ist auch im Inland nur unter bestimmten Voraussetzungen zulässig, wobei in der Praxis meist nur die Zustimmung des Betroffenen in Frage kommt. Sofern der jeweilige Anwendungsfall dies zulässt, bietet sich die Verschlüsselung der Daten als Alternative an, denn die Überlassung indirekt personenbezogener Daten unterliegt keinen Einschränkungen. Das Datenschutzrecht hat somit auf die Zulässigkeit der Nutzung von Cloud-Services im Zusammenhang mit personenbezogenen Daten sehr gravierende Auswirkungen.

3.2.6. Konsequenzen von Verstößen gegen Datenschutzbestimmungen

Nach § 32 DSG 2000 können Betroffene auf dem Zivilrechtsweg gegen Auftraggeber des privaten Bereichs wegen Verletzung ihrer Rechte auf Geheimhaltung, Richtigstellung oder Löschung ihrer Daten vorgehen und Unterlassung sowie Beseitigung eines

[229] § 13 Abs 2 Z 2 DSG 2000.
[230] Jahnel 2010, Rz. 4/159.
[231] Aktuelle Standardvertragsklauseln sind auf der Website der Europäischen Kommission abrufbar (Europäische Kommission 2010a).
[232] Jahnel 2010, Rz. 4/160.
[233] BGBl I 133/2009.
[234] § 13 Abs 2 Z 2 DSG 2000.
[235] Pollirer, Weiss und Knyrim 2010, Anmerkung 8 zu § 13 DSG 2000.
[236] Spies 2009, XII.
[237] Spies 2009, XII.

dem DSG 2000 widerstreitenden Zustands erwirken. In der Praxis kommt dies allerdings nur sehr selten vor.[238] Daraus auf eine geringe Zahl tatsächlicher Datenschutzverletzung zu schließen, wäre allerdings kurzsichtig. Häufig wird den Betroffenen die Verwendung ihrer Daten wohl nicht bekannt, oder es ist ihnen nicht bewusst, dass diese rechtswidrig erfolgt und sie dagegen vorgehen könnten. In vielen Fällen könnte den Betroffenen auch schlicht das Bedürfnis fehlen, ihre subjektiven Datenschutzrechte durchzusetzen, nicht zuletzt weil ein materieller Schaden häufig nicht vorliegt und ein Anspruch auf Ersatz immateriellen Schadens nur in sehr eingeschränkten Fällen besteht.[239]

Laut *Jahnel*[240] ist auch die praktische Bedeutung der im DSG 2000 vorgesehenen Strafbestimmung gering. *Jahnel* und *Thiele*[241] zeigen allerdings auf, dass auch ein wettbewerbsrechtliches Vorgehen durch Mitbewerber möglich ist, wenn ein Unternehmen schuldhaft gegen Datenschutzrecht verstößt um sich dadurch einen Vorsprung gegenüber Mitbewerbern zu verschaffen.

3.3. Branchenspezifische Bestimmungen

Wie sich gezeigt hat, ist es für österreichische Unternehmen unumgänglich, sich im Zusammenhang mit Cloud Computing mit dem Datenschutzrecht auseinanderzusetzen. Insbesondere Unternehmen, die branchenspezifischen Vorschriften unterliegen, müssen aber im Hinblick auf die Zulässigkeit der Nutzung von Cloud Computing noch weitere Bestimmungen beachten. Dieser Abschnitt gibt einen Überblick über solche Bestimmungen.

3.3.1. Banken und Cloud Computing

Die speziell für Banken geltenden aufsichtsrechtlichen Vorschriften sind im Bankwesengesetz (BWG)[242] geregelt. Die nachfolgend besprochenen Bestimmungen des BWG gelten für Kreditinstitute[243] mit österreichischer Lizenz[244] und für in einem Mitgliedstaat des EWR zugelassene Kreditinstitute.[245] Das BWG sieht zwar keine ausdrücklichen Regelungen bzgl. Outsourcing vor, dieses ist für Banken jedoch nicht etwa gene-

[238] OGH in 6 Ob 236/08m, 17.12.2008 ist laut *Jahnel* (2009) der erste derartige Fall, obwohl § 32 DSG 2000 seit 2000 in Kraft ist.
[239] Jahnel 2010, Rz. 9/63.
[240] Jahnel 2010, Rz. 9/79 ff.
[241] Jahnel und Thiele 2004.
[242] Bundesgesetz über das Bankwesen (Bankwesengesetz - BWG) [...], BGBl 532/199s3 idF BGBl I 152/2009. Zu Wertpapierdienstleistungen und den Bestimmungen des Wertpapieraufsichtsgesetzes 2007 siehe Punkt 3.3.2, S. 62.
[243] Zur Definition siehe § 1 Abs 1 BWG.
[244] Karas, Träxler und Waldherr in Dellinger, Rz. 1 zu § 1 BWG, vgl. Laurer et al. 2007, Rz. 1 zu § 9 BWG.
[245] § 15 Abs 1 BWG iVm § 9 Abs 1 BWG.

rell unzulässig, denn wie *Jergitsch* und *Siegl*[246] darlegen, enthält das BWG mehrere Bestimmungen, aus denen auf die Zulässigkeit der Auslagerung bestimmter Tätigkeiten auf Dritte zu schließen ist.[247] So werden in § 2 Z 27 BWG Anbieter von Nebendienstleistungen definiert und darunter auch ausdrücklich Betreiber von Rechenzentren genannt.[248] Aus der Formulierung des § 60 Abs 3 BWG, der dem Bankprüfer den Zugriff auf Unterlagen und Datenträger sichern soll, wenn diese von Dritten oder im Ausland geführt und/oder verwahrt werden, kann geschlossen werden, dass genau dies grundsätzlich zulässig ist. Jedoch hat das Kreditinstitut im Fall der Verwahrung von zu prüfenden Unterlagen im Ausland für die jederzeitige Verfügbarkeit der Unterlagen des laufenden und der drei vorangegangenen Geschäftsjahre im Inland zu sorgen.[249] *Höllerer* und *Puhm*[250] leiten aus den Bestimmungen zu den Auskunfts-, Vorlage- und Einschaurechten ab, dass eine Auslagerung, insbesondere ins Ausland, unzulässig ist, wenn dadurch die Durchsetzbarkeit der Aufsichtsrechte eingeschränkt wird.

Auch die Formulierung des Bankgeheimnisses nach § 38 BWG – eine zentrale Bestimmung des Gesetzes – schließt „sonstige für Kreditinstitute tätige Personen“ mit ein und gewährleistet damit, dass das Bankgeheimnis auch im Falle der Auslagerung von Tätigkeiten gewahrt bleibt.[251] Denn diese Formulierung umfasst alle (natürlichen oder juristischen)[252] Personen, die im Zusammenhang mit der Ausübung des Bankgeschäfts vom Kreditinstitut für Tätigkeiten herangezogen werden, unabhängig davon, auf welcher rechtlichen Grundlage dies erfolgt.[253] Dies schließt nach der Rechtsprechung auch Tätigkeiten eines Rechenzentrums mit ein.[254] Damit ist auch ein Anbieter von Cloud-Services, dem im Zuge seiner Tätigkeit für ein Kreditinstitut von diesem Kundendaten übermittelt werden, kraft Gesetzes an das Bankgeheimnis gebunden. Vom Bankgeheimnis erfasst sind alle einen Kunden betreffenden Tatsachen, die nur einer beschränkten Personenzahl bekannt sind und durch deren Offenbarung der Kunde einen Nachteil hätte.[255] Trotz dieser ohnehin bestehenden gesetzlichen Verpflichtung empfehlen *Jergitsch* und *Siegl*[256], die Einhaltung des Bankgeheimnisses vertrag-

[246] Jergitsch und Siegl 2010, 19.
[247] Dafür spricht auch § 15 iVm § 25 WAG. Siehe dazu Punkt 3.3.2, S. 62.
[248] § 2 Z 27 lit b BWG.
[249] § 60 Abs 3 BWG. Diese Bestimmung ist auch auf die Auskunfts-, Vorlage- und Einschaurechte der Finanzmarktaufsichtsbehörde (FMA) und der Oesterreichischen Nationalbank (OeNB) anzuwenden (§ 70 Abs 1 Z 1 bzw. 71 Abs 2 BWG).
[250] Höllerer und Puhm in Dellinger, Rz. 88 zu § 39 BWG.
[251] Jergitsch und Siegl 2010, 20 f.
[252] Schütz und Waldherr 2007, 142 f.
[253] Sommer und Hirsch in Dellinger, Rz. 115 zu § 38 BWG.
[254] OGH in 4 Ob 114/91, 25.02.1992.
[255] Sommer und Hirsch in Dellinger, Rz. 29 ff. zu § 38 BWG.
[256] Jergitsch und Siegl 2010, 28.

lich mit dem Dienstleister zu regeln. *Schütz* und *Waldherr*[257] erkennen sogar eine Pflicht des Kreditinstituts zu dieser vertraglichen Bindung des Dienstleisters an die Einhaltung das Bankgeheimnisses (und anderer Verschwiegenheitspflichten[258]), denn die Kenntnis des BWG könne nicht bei jedem Dienstleister a priori vorausgesetzt werden. Folgt man dieser – überzeugenden – Argumentation, so bedeutet dies, dass im Zusammenhang mit Daten, die dem Bankgeheimnis unterliegen, Cloud-Services nicht genutzt werden können, weil über deren Nutzung kein individuell ausgehandelter Vertrag abgeschlossen wird, der eine Verpflichtung des Anbieters zur Einhaltung des Bankgeheimnisses beinhalten könnte.[259]

Zusammenfassend kann somit gesagt werden, dass die Nutzung von Cloud-Services für Kreditinstitute zwar nicht generell unzulässig, aber auf bankwirtschaftlich unwesentliche Anwendungsfälle beschränkt ist. Insbesondere alle mit Kundendaten zusammenhängenden Anwendungsfälle – und dieses Kriterium erfüllen wohl die meisten der Kernbankprozesse eins Kreditinstituts – eignen sich wegen des Datenschutzgesetzes und des Bankgeheimnisses nicht für die Nutzung von Cloud-Services. Mit dieser Erkenntnis erübrigt sich die Betrachtung weiterer bankenspezifischer Bestimmungen, wie insbesondere von Basel II[260] und dessen Umsetzung im BWG.

3.3.2. Wertpapierdienstleistungen und Cloud Computing

Das Wertpapieraufsichtsgesetz 2007 (WAG 2007)[261] ist die österreichische Umsetzung der Markets in Financial Instruments Directive (MiFID)[262]. Es enthält in den §§ 25 f WAG ein allgemeines Regelwerk für das Outsourcing („Auslagerung“) im Bereich der Wertpapierdienstleistungen. Dieses gilt gemäß § 15 Abs 1 WAG für Kreditinstitute, Wertpapierfirmen, Wertpapierdienstleistungsunternehmen und bestimmte Versicherungsunternehmen,[263] nicht jedoch für in einem anderen EWR-Mitgliedstaat zugelassene Wertpapierfirmen und Kreditinstitute, die ihre Tätigkeit in Österreich über

---

[257] Schütz und Waldherr 2007, 143.
[258] Siehe dazu auch Punkt 3.2.3, S. 53.
[259] Siehe Charakteristikum „on-demand self-service“ in Tabelle 1, S. 28.
[260] Eigenkapitalvorschriften des Basler Ausschusses für Bankenaufsicht, umgesetzt in Richtlinie 2006/48/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (Neufassung), ABl L 177, 1 vom 30.06.2006 und Richtlinie 2006/49/EG des Europäischen Parlaments und des Rates vom 14. Juni 2006 über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten (Neufassung), ABl L 177, 201 vom 30.06.2006.
[261] Bundesgesetz über die Beaufsichtigung von Wertpapierdienstleistungen (Wertpapieraufsichtsgesetz 2007 – WAG 2007), BGBl I 60/2007 idF BGBl I 152/2009.
[262] Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates vom 21. April 2004 über Märkte für Finanzinstrumente […], ABl L 145, 1 vom 30.04.2004 samt Richtlinie 2006/73/EG der Kommission vom 10. August 2006 zur Durchführung der Richtlinie 2004/39/EG […], Abl L 241, 26 vom 02.09.2006.
[263] Zu Letzteren siehe § 2 Abs 2 WAG. Zu den Definitionen der Begriffe siehe § 2 ff WAG.

eine Zweigstelle ausüben.[264] § 25 WAG gilt nur für die Auslagerung wesentlicher betrieblicher Aufgaben. Eine wesentliche betriebliche Aufgabe liegt insbesondere vor, wenn deren unzureichende oder unterlassene Wahrnehmung die Einhaltung der Bestimmungen des WAG oder die Solidität oder Kontinuität der Wertpapierdienstleistungen und Anlagetätigkeiten wesentlich beeinträchtigen würde.[265] Wenn dies auf den jeweiligen Anwendungsfall zutrifft, kann daher die Nutzung von Cloud-Services unter den Begriff der wesentlichen betrieblichen Aufgaben fallen. *Harrer*[266] führt dazu aus, dass die Auslagerung von EDV-Dienstleistungen zumeist als wesentliche betriebliche Aufgabe zu qualifizieren, dies aber im Einzelfall zu prüfen sei. Wenn die Weitergabe von kundenspezifischen Daten damit verbunden sei, handle es sich jedenfalls um eine wesentliche betriebliche Aufgabe.

Die Auslagerung wesentlicher betrieblicher Aufgaben ist unzulässig, wenn dadurch die Qualität der internen Kontrolle und der Kontrolle durch die FMA wesentlich beeinträchtigt wird.[267] Zulässigkeitsvoraussetzung einer solchen Auslagerung ist auch, dass angemessene Vorkehrungen gemäß Anlage 1 zu § 25 WAG getroffen werden, um unnötige Geschäftsrisiken zu vermeiden.[268] Da die Dienstleister nicht selbst Normadressaten der §§ 25 f WAG sind, müssen die in Anlage 1 zu § 25 WAG festgelegten Auslagerungsbedingungen, insbesondere die Pflichten des Dienstleisters schriftlich zwischen den Vertragsparteien vereinbart werden.[269] An dieser Vorschrift wird, ähnlich wie oben im Zusammenhang mit dem Bankgeheimnis, die Nutzung von Cloud-Services für wesentliche betriebliche Aufgaben scheitern und somit insbesondere für Aufgaben, welche die Weitergabe von kundenspezifischen Daten erfordern. Z 9 der in Anlage 1 zu § 25 WAG festgelegten Auslagerungsbedingungen fordert beispielsweise den Zugang zu den Geschäftsräumen des Dienstleisters für Abschlussprüfer und die FMA, was – wenn überhaupt möglich – nur individuell vereinbart werden kann und nicht Teil der Standardvertragsbedingungen eines Anbieters von Cloud-Services sein wird. Zudem gilt auch für Wertpapierfirmen und Wertpapierdienstleistungsunternehmen eine Verschwiegenheitspflicht,[270] der – analog zum Bankgeheimnis – „für sie tätige Personen" ebenfalls unterliegen. Das oben zum Bankgeheimnis Gesagte gilt daher entsprechend auch für die Verschwiegenheitspflicht, weshalb Daten, die davon erfasst sind, mangels

[264] § 12 Abs 4 WAG und § 9 Abs 7 BWG, Harrer in Gruber und Raschauer 2009, Rz. 9 zu § 25 WAG.
[265] § 25 Abs 2 WAG.
[266] Harrer in Gruber und Raschauer 2009, Rz. 14 zu § 25 WAG.
[267] § 25 Abs 1 WAG.
[268] § 25 Abs 1 WAG.
[269] Harrer in Gruber und Raschauer 2009, Rz. 6 zu § 25 WAG.
[270] § 7 Abs 1 WAG.

eines individuellen Vertrages nicht im Rahmen von standardisierten Cloud-Services verwendet werden dürfen.

Die Zulässigkeit der Nutzung von Cloud Computing ist also auch im Zusammenhang mit Wertpapierdienstleistungen auf betrieblich unbedeutende Anwendungen beschränkt. Nur für solche, die nicht wesentliche betriebliche Aufgaben erfüllen und keine der Verschwiegenheitspflicht unterliegenden Daten beinhalten, kommt die Nutzung von Cloud-Services in Frage.

3.3.3. Versicherungsunternehmen und Cloud Computing

Für Versicherungsunternehmen sind die spezifischen aufsichtsrechtlichen Vorschriften im Versicherungsaufsichtsgesetz (VAG)[271] geregelt. Versicherungsunternehmen mit österreichischer Konzession[272] dürfen einem anderen Unternehmen, das seinerseits nicht Versicherungsunternehmen ist, wesentliche Teile ihrer Geschäftsgebarung zur Gänze oder in wesentlichem Umfang nur mit Genehmigung der FMA übertragen.[273] Aus dieser Bestimmung kann zunächst – analog zu den oben besprochenen Bestimmungen – geschlossen werden, dass Outsourcing für Versicherungsunternehmen nicht grundsätzlich unzulässig ist. Die Genehmigung ist jedoch zu versagen, wenn die Ausgliederung geeignet ist, die Interessen der Versicherten zu gefährden.[274] Für Korinek[275] ist die – nicht erschöpfende – Aufzählung der „wesentlichen Teile der Geschäftsgebarung“ im Gesetz um „den Bereich EDV“ zu ergänzen. Ob der Einsatz eines Cloud-Service für eine bestimmte Aufgabe tatsächlich als Auslagerung wesentlicher Teile der Geschäftsgebarung zu werten und damit genehmigungspflichtig ist, muss im Einzelfall geprüft werden. Dabei ist der Zweck der Genehmigungspflicht, die Gewährleistung einer effektiven Aufsicht,[276] zu berücksichtigen. Ist das Maß der Ausgliederung so gering, dass die Effektivität der Aufsicht nicht gefährdet ist oder sind nur unwesentliche Bereiche davon betroffen, muss die Ausgliederung weder genehmigt noch angezeigt werden.[277] Damit ist die – genehmigungsfreie – Nutzung von Cloud-Services auch im Zusammenhang mit Versicherungsunternehmen auf unwesentliche Anwendungen beschränkt.

---

[271] Bundesgesetz vom 18. Oktober 1978 über den Betrieb und die Beaufsichtigung der Vertragsversicherung (Versicherungsaufsichtsgesetz - VAG), BGBl 569/1978 idF BGBl I 28/2010.
[272] Arg. „innerhalb der gemäß § 4 Abs. 1 erteilten Konzession“ (§17a Abs 1 VAG).
[273] § 17a Abs 1 VAG.
[274] § 17a Abs 2 VAG.
[275] Korinek 2007, 41.
[276] Korinek 2007, 42. Dieser Hintergrund ist auch für die Ausgliederung ins Ausland relevant, die grundsätzlich zulässig ist: Die Nichtgenehmigung für eine Ausgliederung ins Ausland wird wahrscheinlicher sein, weil dadurch die Aufsicht erschwert wird (Korinek 2007, 42).
[277] Korinek 2007, 42.

3.4. Sonstige Bestimmungen

In diesem Abschnitt sind nachfolgend weitere Bestimmungen und Normen dargestellt, die im Zusammenhang mit Cloud Computing relevant sind.

3.4.1. Pflichten der Geschäftsleitung

Seit dem Jahr 2002 ist in den USA der Sarbanes-Oxley Act (SOX)[278] in Kraft, dessen Ziel es ist, die Unternehmensberichterstattung zu verbessern. In Section 404 verpflichtet er Unternehmen, ein internes Kontrollsystem (IKS) der Finanzberichterstattung einzurichten.[279] „Mit dem IKS soll die Effektivität und Effizienz der betrieblichen Tätigkeit, die Zuverlässigkeit der Finanzberichterstattung und die Einhaltung der für das Unternehmen maßgeblichen gesetzlichen Vorschriften überwacht werden."[280] Laut *Milla*, *Vcelouch-Kimeswenger* und *Weber* ist das IKS als Bestandteil eines unternehmensweiten Risikomanagementsystems (RMS) zu verstehen. Dieses „umfasst alle Tätigkeiten, die dazu dienen, Risiken zu identifizieren, zu analysieren, zu bewerten und Maßnahmen zu ergreifen, die verhindern, dass das Erreichen der Unternehmensziele durch den Eintritt von Risiken beeinträchtigt wird."[281] SOX ist für Unternehmen aus Österreich nur dann verbindlich, wenn diese an einer US-amerikanischen Börse notieren.[282] Zudem hat SOX auch deswegen eine gewisse Bedeutung, weil manche an sich nicht davon erfasste Unternehmen die SOX-Vorgaben einhalten, um diesbezüglichen Forderungen von Vertragspartnern nachzukommen.[283]

In Österreich besteht für Geschäftsführer von GmbH und Vorstände einer AG ebenfalls die Verpflichtung, ein IKS zu führen, das den Anforderungen des Unternehmens entspricht.[284] Die genannten Bestimmungen wurden im Zuge des Unternehmensrechts-Änderungsgesetzes 2008 (URÄG 2008)[285] für Gesellschaften, deren Wertpapiere auf einem geregelten Markt gehandelt werden, um die Pflicht ergänzt, im Lagebericht die wichtigsten Merkmale des IKS und des RMS im Hinblick auf den Rech-

[278] Public Law 107 - 204 - Sarbanes-Oxley Act of 2002, 30.07.2002.
[279] Menzies 2006, 15 f.
[280] Milla, Vcelouch-Kimeswenger und Weber 2008, 52.
[281] Milla, Vcelouch-Kimeswenger und Weber 2008, 52.
[282] Keller 2007, 166.
[283] Rath 2009, 153.
[284] § 82 AktG (Bundesgesetz über Aktiengesellschaften (Aktiengesetz – AktG), BGBl 98/1965 idF BGBl I 58/2010) bzw. § 22 Abs 1 GmbHG (Gesetz vom 6. März 1906, über Gesellschaften mit beschränkter Haftung (GmbH-Gesetz - GmbHG), RGBl 58/1906 idF BGBl I 58/2010).
[285] Bundesgesetz, mit dem das Unternehmensgesetzbuch, das Aktiengesetz 1965, das GmbH-Gesetz, das SE-Gesetz, das Genossenschaftsgesetz, das Genossenschaftsrevisionsgesetz, das Spaltungsgesetz, das Luftfahrtgesetz, das Bankwesengesetz und das Versicherungsaufsichtsgesetz geändert werden (Unternehmensrechts-Änderungsgesetz 2008 – URÄG 2008), BGBl I 70/2008.

nungslegungsprozess zu beschreiben.[286] Auch der Bestätigungsvermerk des Abschlussprüfers muss sich nunmehr auf die Richtigkeit dieser Beschreibung beziehen.[287] Das URÄG 2008 wurde zur Umsetzung der – umgangssprachlich als EuroSOX bezeichneten – Abschlussprüfungs-Richtline[288] beschlossen.[289]

Die genannten österreichischen und europäischen Bestimmungen sind mit den umfangreichen Berichts- und Prüfpflichten des SOX in ihrer Tragweite nicht vergleichbar.[290] Überdies lassen sich keine konkreten Vorgaben für die inhaltliche Ausgestaltung des IKS und des RMS aus diesen Bestimmungen ableiten, vielmehr liegt diese weiterhin in der Verantwortung der Geschäftsleitung.[291] Somit bestehen auch keine spezifischen Vorgaben für die IT. Die Geschäftsleitung ist aber aufgrund der potenziellen Auswirkungen von IT-Risiken auf den Unternehmenserfolg auch für die IT verantwortlich und muss diese daher in das IKS und das RMS einbeziehen.[292]

Im Zusammenhang mit Cloud Computing ist deshalb zu prüfen, ob die beschriebenen Kontrollpflichten der Geschäftsleitung eingehalten werden können, wenn Cloud-Services für wesentliche Geschäftsprozesse verwendet werden, also solche, die Einfluss auf den Unternehmenserfolg und/oder auf die Rechnungslegung haben. Wenn nicht ausreichende Zusicherungen seitens des Anbieters eines Cloud-Service hinsichtlich Informationssicherheit und Zuverlässigkeit vorliegen, wird dies zu verneinen sein.

3.4.2. SAS 70

Das Statement on Auditing Standards No. 70: Service Organizations (SAS 70) ist ein Standard zur Prüfung von Outsourcing-Dienstleistern und deren Zusammenwirken mit ihren Kunden, der aus den USA stammt.[293] Ein SAS-70-Report bescheinigt in der Variante „Type I“ die Angemessenheit und in der Variante „Type II“ die Wirksamkeit des internen Kontrollsystems eines Dienstleisters.[294] Für Unternehmen, die dem SOX unterliegen, bestätigt der Type-II-Report eines in Anspruch genommenen Dienstleisters die Compliance mit Section 404 des SOX. Aufgrund der Einschränkung der vorliegen-

[286] § 243a Abs 2 UGB (Bundesgesetz über besondere zivilrechtliche Vorschriften für Unternehmen (Unternehmensgesetzbuch - UGB), dRGBl S 219/1897 idF BGBl I 58/2010).
[287] Weber 2008, 432 f.
[288] Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates, ABl L 157, 87 vom 09.06.2007.
[289] Milla, Vcelouch-Kimeswenger und Weber 2008, 17.
[290] Weber 2008, 432 f. *Weber* kritisiert in diesem Zusammenhang die Bezeichnung „EuroSOX“, für die Abschlussprüfungs-RL, da vom europäischen Gesetzgeber niemals geplant gewesen sei, den Unternehmen ähnliche Belastungen wie jene des SOX aufzuerlegen.
[291] Milla, Vcelouch-Kimeswenger und Weber 2008, 51 f.
[292] § 274 Abs 5 UGB, siehe dazu Schober 2009, 41.
[293] Siehe im Volltext unter Auditing Standards Board 1992.
[294] Menzies 2006, 114.

den Arbeit auf österreichische Unternehmen als Nutzer von Cloud-Services ist die unmittelbare Relevanz der SAS-70-Zertifizierung eines Anbieters von Cloud-Service daher gering, denn österreichische Unternehmen unterliegen – wie oben angesprochen – nur in Ausnahmefällen dem SOX. Die größere Bedeutung der SAS-70-Zertifizierung liegt aus der Sicht österreichischer Nutzer in der Professionalität, die sie einem zertifizierten Anbieter von Cloud-Services grundsätzlich bescheinigt. Zu beachten ist allerdings, dass SAS 70 das interne Kontrollsystem und nicht etwa die Informationssicherheit betrifft.

3.4.3. ISO/IEC 27001

Im Gegensatz zu SAS 70 ist ISO/IEC 27001 ein solcher Informationssicherheits-Standard, der den englischen Titel „Information technology -- Security techniques -- Information security management systems -- Requirements“ trägt.[295] ISO/IEC 27001 spezifiziert Konzeption, Einführung und Betrieb eines Informationssicherheits-Managementsystems (ISMS). Dieses definiert der Standard als „Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.“[296] Die ISO/IEC-27001-Zertifizierung des Anbieters eines Cloud-Service spricht zwar deutlicher als eine Zertifizierung nach SAS 70 für die Professionalität des Anbieters, insbesondere in Bezug auf Informationssicherheit, sollte aber nicht als Freibrief betrachtet werden, den Cloud-Service ohne weitere Prüfung im Zusammenhang mit unternehmenskritischen Daten und Prozessen einzusetzen.[297] Entscheidend ist, dass neben einer Zertifizierung auch entsprechende vertragliche Zusicherungen hinsichtlich Informationssicherheit und Verfügbarkeit bestehen.

[295] ISO o.J. Der Standard kann dort kostenpflichtig heruntergeladen werden.
[296] ISO/ICE 27001 zitiert nach Kersten, Reuter und Schröder 2009, 37.
[297] Tucci 2009.

4. IT-strategische Aspekte des Cloud Computing

"One reason you should not use web applications to do your computing is that you lose control".[298]

Neben den rechtlichen Gesichtspunkten des Cloud Computing sind als Grundlage der Entscheidung über die Nutzung von Cloud-Services noch viele weitere Aspekte zu beachten, insbesondere organisatorische und monetäre. Sie werden hier unter dem Überbegriff IT-strategische Aspekte des Cloud Computing zusammengefasst. Da diese von den rechtlichen Überlegungen des vorigen Kapitels nicht unabhängig sind, fließen diese Überlegungen auch hier mit ein.

Die IT-strategischen Aspekte werden im Folgenden getrennt nach Stärken des Cloud Computing bzw. Chancen, die sich daraus für Unternehmen ergeben, und Schwächen bzw. Risiken des Cloud Computing behandelt. Dabei werden möglichst viele verschiedene Gesichtspunkte aufgezeigt. Diese werden allerdings jeweils nur knapp erläutert und zum Teil mit Verweisen auf ausführlichere Literatur versehen. Auf diese Weise werden auch Aspekte angesprochen, die nicht auf den ersten Blick zu erkennen und ohnehin jeder beliebigen Abhandlung über Cloud Computing zu entnehmen sind.

4.1. Stärken des Cloud Computing

Die offensichtlichsten und in der Literatur wohl am häufigsten erwähnte Argumente für die Nutzung von Cloud-Services sind Flexibilität und Kostenersparnis. Weitere positive Aspekte sind – wie nachfolgend erläutert – die Fokussierung auf das Kerngeschäft und die potenziell erhöhte Sicherheit, insbesondere für kleine und mittlere Unternehmen (KMU). Sehr großes Potenzial steckt nicht zuletzt in den neuen Möglichkeiten, die Cloud Computing für Unternehmen eröffnet, insbesondere in neuen Geschäftsmodellen.

4.1.1. Flexibilität

Eine wesentliche Eigenschaft des Cloud Computing ist die „rapid elasticity",[299] die auch als Bedarfsorientierung bezeichnet werden kann. Sie ist eine Folge des Geschäftsmodells Utility Computing. „Elastizität beschreibt die Eigenschaft, Ressourcen feingranular und in sehr kurzen Zeitspannen von Minuten (und nicht Wochen oder Monaten) hinzuzufügen bzw. zu entfernen, und somit den tatsächlichen Bedürfnissen einer An-

[298] *Richard Stallman*, Gründer der Free Software Foundation, über Cloud Computing, zitiert nach Johnson 2008.
[299] Siehe Tabelle 1, S. 28.

wendung besser gerecht zu werden."[300] Dies bedeutet, dass stets exakt die benötigte Menge an Ressourcen zur Verfügung steht. Schätzungen der durchschnittlichen Auslastung der Server in konventionellen Rechenzentren reichen von fünf bis 20 Prozent. Dies erscheint plausibel, da die Auslastung vieler Services zu Spitzenzeiten zwei- bis zehnmal so hoch ist als die durchschnittliche. Durch die Verteilung der Last verschiedener Nutzer in den Rechenzentren der Anbieter von Cloud-Services kann die Auslastung erheblich gesteigert werden. Dies führt nicht nur zu Energie- und Kostenersparnis, jedem einzelnen Nutzer stehen so potenziell auch mehr Ressourcen zur Verfügung, wenn diese kurzfristig benötigt werden. *Armbrust et al.* machen deutlich, wie hoch der potenzielle Schaden durch den Verlust von Kunden bei Überlastung wegen unterdimensionierter Ressourcen sein kann. Durch den Einsatz von Cloud-Services kann dies verhindert werden.[301]

Die Flexibilität des Cloud Computing hat noch viele weitere Gesichtspunkte. IaaS- und PaaS-Plattformen vereinfachen es, neue Anwendungen einzuführen oder bestehende um neue Funktionen zu erweitern.[302] Insbesondere muss dafür keine Hardware beschafft werden. Innovation wird dadurch beschleunigt und die Time-to-Market gesenkt.[303] Erhöhte Flexibilität besteht auch im Hinblick auf Expansionen, Reorganisationen und Akquisitionen, auf die durch den Einsatz von Cloud-Services einfacher reagiert werden kann.[304]

Flexibilität bietet die Nutzung von Cloud-Services auch hinsichtlich des Lizenz-Managements. Viele Unternehmen sind überlizenziert, d.h. sie besitzen mehr Lizenzen für konventionelle Software, als sie nutzen, was zu unnötigen Kosten führt.[305] Unterlizenzierung kann wegen der rechtlichen Konsequenzen ein noch größeres Problem sein. SaaS-Applikationen werden zwar meist auch nach der Anzahl der Nutzer bezahlt,[306] doch diese kann abhängig vom konkreten Bezahlmodell des Anbieters monatlich oder jährlich variiert werden.

Bei den meisten Cloud-Services gestaltet sich der Ein- und Ausstieg ebenfalls flexibel. Häufig ist es möglich einen Service für einen beschränkten Zeitraum kostenlos zu testen.[307] Manche Services bieten kostenlose Versionen mit eingeschränktem Funktionsumfang oder eingeschränkter Nutzungsintensität. Diese Angebote eignen sich gut, einen Cloud-Service anhand der eigenen Anforderungen ausgiebig zu testen, bevor man

[300] Baun et al. 2009, 90.
[301] Armbrust et al. 2009, 10, mit weiteren Nachweisen.
[302] Rittinghouse und Ransome 2009, 36.
[303] Velte, Velte und Elsenpeter 2009, 78 f. und BITKOM 2009, 16.
[304] Mather, Kumaraswamy und Latif 2009, 227 und Velte, Velte und Elsenpeter 2009, 80.
[305] Gerick 2009, 260, mit weiteren Nachweisen.
[306] Rittinghouse und Ransome 2009, 92.
[307] Velte, Velte und Elsenpeter 2009, 78 f.

sich für die kommerzielle Nutzung entscheidet. Und selbst wenn diese Entscheidung gefallen ist, besteht bei vielen Services keine Bindung, sodass man die Nutzung ohne finanziellen Verlust umgehend wieder einstellen kann.[308]

4.1.2. Fokussierung

Fokussierung beschreibt die Konzentration auf das Kerngeschäft, die Unternehmen durch die Nutzung von Cloud-Services ermöglicht wird.[309] Durch den Einsatz von PaaS und SaaS braucht sich das IT-Personal nicht um Bereitstellung der Infrastruktur, Updates, Skalierbarkeit, und bestimmte Aspekte der Sicherheit zu kümmern,[310] sondern kann sich – im Fall von PaaS – auf die Entwicklung der eigentlichen Anwendung konzentrieren. Bei der Verwendung von IaaS fallen zwar weniger dieser Tätigkeiten weg, allerdings sind IaaS-Angebote vielseitiger einsetzbar.

Die Fokussierung kann zudem dazu führen, dass die genannten, auf den Anbieter ausgelagerten Tätigkeiten professioneller ausgeführt werden, da diese zum Kerngeschäft und damit zu den Kernkompetenzen des Anbieters gehören, dessen Mitarbeiter auf diese Tätigkeiten spezialisiert sind.

4.1.3. Sicherheit

Ein wesentlicher Gesichtspunkt der eben angesprochenen Professionalisierung bestimmter Tätigkeiten durch Auslagerung auf die Anbieter von Cloud-Services ist die gesteigerte Sicherheit. Trotz berechtigter Sicherheitsbedenken im Zusammenhang mit Cloud Computing, [311] kann durch den Einsatz von Cloud-Services die Sicherheit auch positiv beeinflusst werden. Dies umso deutlicher, je weniger professionell das Thema Sicherheit im Unternehmen zuvor gehandhabt wurde. Insbesondere viele KMU haben begrenzte Ressourcen und Expertise in diesem Bereich.[312] Anbieter von Cloud-Services investieren hingegen in der Regel viel in die Sicherheit ihrer Services und können dabei Economies of Scale nützen.[313] Für die Anbieter ist dies eine betriebliche Notwendigkeit, ihr Geschäft steht und fällt mit ihrem guten Ruf in Sachen Sicherheit.[314]

---

[308] Sobald man einen Cloud-Service allerdings tatsächlich für betrieblich relevante Zwecke nutzt, kann es auch dazu kommen, dass die Nutzung nicht ohne Probleme wieder eingestellt werden kann. Siehe dazu die Ausführungen zum Thema Vendor-Lock-in unter Punkt 4.2.2, S. 76

[309] BITKOM 2009, 16.

[310] Velte, Velte und Elsenpeter 2009, 15 und 78.

[311] Siehe dazu Punkt 4.2.1, S. 74.

[312] Mather, Kumaraswamy und Latif 2009, 145.

[313] Velte, Velte und Elsenpeter 2009, 94.

[314] Velte, Velte und Elsenpeter 2009, 36. Damit soll keineswegs pauschal ausgesagt werden, alle Anbieter von Cloud-Services böten hohe Sicherheit. Vielmehr sollten bei der Auswahl des Anbieters dessen Angaben über Sicherheitsmaßnahmen und deren Glaubwürdigkeit (Zertifizierungen etc.) sehr genau geprüft werden.

Neben diesem Professionalisierungsaspekt gibt es noch weitere Gründe, warum der Einsatz von Cloud-Services die Sicherheit steigern kann. In der Cloud stehen sofort gleichartige Ressourcen zur Verfügung, auf denen die betreffenden Anwendung bei Auftreten eines Defekts – im Idealfall nahtlos – weiterbetrieben werden kann.[315] Dieses Niveau der Ausfallsicherheit ist ohne den Einsatz von Cloud Computing nur mit hohem Kapitaleinsatz zu erreichen, während bei Verwendung eines Cloud-Service aufgrund der Flexibilität nur im tatsächlichen Fehlerfall Mehrkosten entstehen.

Durch die Datenspeicherung beim jeweiligen Anbieter kann sich durch die Nutzung von SaaS die Datensicherheit auch dadurch erhöhen, dass in der Folge keine geschäftsrelevanten Daten mehr auf den Endgeräten der Anwender gespeichert sind. Wird ein mobiles Endgerät gestohlen, können diese Daten nicht in fremde Hände gelangen, da sie sich ausschließlich auf den Servern befinden.[316] Ein weiterer Aspekt der Datensicherheit ist, dass Cloud-Services auch zur Datensicherung außerhalb des Unternehmensstandorts verwendet werden können. [317]

4.1.4. Monetäre Aspekte

Cloud Computing verspricht wesentliche Kostenvorteile im Vergleich zu konventionellem Hosting und dem Betrieb eigener Infrastruktur. Diese ergeben sich zum Teil aus Eigenschaften des Cloud Computing, die in diesem Abschnitt bereits angesprochen wurden, insbesondere aus der Flexibilität. Viele Cloud-Services werden entsprechend des Utility-Computing-Prinzips nutzungsabhängig abgerechnet, andere – insbesondere SaaS-Angebote – in Form von Abonnement-Modellen.[318] Auf Seiten des Nutzers werden somit Investitionskosten für eigene Hardware und Software-Lizenzen durch Betriebsaufwand in Form von (in der Regel) monatlichen Zahlungen entsprechend der tatsächlichen Nutzung – und damit entsprechend des tatsächlichen Nutzens – ersetzt.[319] Dadurch ist wesentlich weniger Kapital notwendig um neue Serviceangebote, Projekte, Expansionen oder ganze Unternehmen zu starten. Das damit verbundene unternehmerische Risiko sinkt.

Allerdings könnte der Fall eintreten, dass die Gesamtkosten für Cloud-Services im Laufe der Jahre die Investitions- und Betriebskostenkosten für eigene Infrastruktur übersteigen. Daher ist Cloud Computing nicht für jede Anwendung zwangsläufig kostengünstiger. Jedoch sind in solche Kostenüberlegungen zwei unter Punkt 4.1.1 bereits

---

[315] Velte, Velte und Elsenpeter 2009, 38.
[316] Velte, Velte und Elsenpeter 2009, 38 und 94.
[317] Rittinghouse und Ransome 2009, 156. Durch Verschlüsselung der zu sicherenden Daten können Datenschutzprobleme in diesem Zusammenhang vermieden werden.
[318] Rittinghouse und Ransome 2009, xxxii.
[319] Rittinghouse und Ransome 2009, xxxii und 35, Mather, Kumaraswamy und Latif 2009, 26 und BITKOM 2009, 16.

angesprochene Aspekte mit einzubeziehen: Einerseits der potenziell hohe Schaden durch Unterdimensionierung der Infrastruktur und andererseits die Kostenersparnis durch die meist höhere durchschnittliche Auslastung der Server in Cloud-Rechenzentren. Hinzu kommt, dass Schätzungen zufolge die Kosten pro Einheit für Aufbau und Betrieb sehr großer Rechenzentren nur ein Fünftel bis eine Siebtel der Kosten mittelgroßer Rechenzentren betragen.[320] Sofern Konkurrenz unter den Anbietern angenommen werden kann, ist davon auszugehen, dass diese enormen Kostenvorteile durch Economies of Scale an die Nutzer weitergegeben werden.

Damit in Zusammenhang steht auch der zweite oben bereits angesprochene Punkt, der sich kostensenkend auswirkt, die Fokussierung. Die Auslagerung von Tätigkeiten, die nicht zum Kerngeschäft und zu den Kernkompetenzen gehören, auf Anbieter von Cloud-Services kann nicht nur zur oben angesprochenen Professionalisierung, sondern auch zu Kostenersparnis führen. Insbesondere Personalkosten für Betrieb und Wartung können eingespart werden.[321]

4.1.5. Neue Möglichkeiten

Die bisher genannten positiven Aspekte der Nutzung von Cloud-Services ergeben sich aus dem Vergleich mit dem herkömmlichen Betrieb eigener Infrastruktur. Cloud Computing bietet Unternehmen jedoch in vielerlei Hinsicht auch völlig neue Möglichkeiten, die zuvor schlicht undenkbar waren, ähnlich wie in den vergangenen Jahrzehnten die Einführung von IT-Systemen in Unternehmen nicht nur zu Erleichterungen und Effizienzsteigerungen in bestehenden Geschäftsprozessen geführt, sondern vor allem auch völlig neue Geschäftsmodelle ermöglicht hat.

Unternehmen aller Größenordnungen haben durch Cloud Computing Zugriff auf eine Menge von Ressourcen, die bisher nicht vorstellbar bzw. nicht finanzierbar war. Manche Geschäftsmodelle werden dadurch erst möglich[322] oder wirtschaftlich umsetzbar, etwa solche, die auf der kurzfristigen Lösung komplexer Aufgaben durch extreme Parallelisierung aufbauen.[323] Ohne Cloud Computing wäre dafür eine große Anzahl eigener Server notwendig, die insgesamt schlecht ausgelastet wären und den angebotenen Service stark verteuerten, sodass dieser möglicherweise nicht nachgefragt würde. Diese Entwicklung führt auch zu einer Verringerung der Markteintrittsbarrieren und

[320] Armbrust et al. 2009, 4 f. Ohne konkrete Zahlen zu nennen so auch Velte, Velte und Elsenpeter 2009, 78.
[321] Velte, Velte und Elsenpeter 2009, 13, 78 und 174 und Mather, Kumaraswamy und Latif 2009, 18.
[322] BITKOM 2009, 25 und Armbrust et al. 2009, 7 f.
[323] Siehe dazu die Ausführungen über „parallel batch processing“ in Armbrust et al. 2009, 7.

somit zu neuen Möglichkeiten für Unternehmen.[324] Doch nicht nur die Quantität, auch die Qualität der Ressourcen, die in Form von Cloud-Services nunmehr insbesondere auch kleineren Unternehmen zur Verfügung stehen, bietet diesen neue Möglichkeiten.[325]

Eine weitere Stärke des Cloud Computing ist die systemimmanente weltweite Verfügbarkeit der Services.[326] Voraussetzung für den Zugriff auf Cloud-Services ist lediglich ein Internetzugang. Insbesondere SaaS-Angebote können dadurch sehr einfach auch von Außendienstmitarbeitern oder Heimarbeitern genutzt werden,[327] häufig auch mittels mobiler Endgeräte.[328]

Systemimmanent ist bei Cloud-Services auch die zentrale Wartung und Aktualisierung.[329] Dies hat neben Vereinfachung und Kostenersparnis für den Nutzer den Vorteil, dass all seine Mitarbeiter stets dieselbe Version einer Software benutzen.[330] Zudem kommen dadurch Innovationen rascher beim Nutzer an.[331] Letzteres betrifft sowohl die Aktualität der Software (SaaS, PaaS) als auch die Aktualität der Hardware (SaaS, PaaS und IaaS).[332]

Cloud Computing bietet darüber hinaus neue Möglichkeiten der Online-Zusammenarbeit. Dies betrifft einerseits die Zusammenarbeit von Entwicklerteams in PaaS-Entwicklungsumgebungen[333] und andererseits das gemeinsame Arbeiten in SaaS-Anwendungen. Beispielsweise können an einem Textdokument oder einer Tabelle in *Google Apps* bis zu 50 Personen gleichzeitig arbeiten.[334]

Positiv ist noch zu erwähnen, dass große PaaS- und IaaS-Anbieter die Möglichkeit bieten, (Web-)Anwendungen geografisch auf mehrere Rechenzentren zu verteilen, um so durch die Nähe zum Endbenutzer kurze Latenzzeiten zu erzielen.[335] Dies kann zwar auch ohne die Nutzung von Cloud-Services erreicht werden, jedoch nur mit ungleich höherem Aufwand.

---

[324] Rittinghouse und Ransome 2009, xxxiv und Mather, Kumaraswamy und Latif 2009, 26.
[325] BITKOM 2009, 16 f.
[326] Rittinghouse und Ransome 2009, 54.
[327] Velte, Velte und Elsenpeter 2009, 78.
[328] Rittinghouse und Ransome 2009, 257. Siehe dazu Abschnitt 4.3, S. 79.
[329] Velte, Velte und Elsenpeter 2009, 78.
[330] Rittinghouse und Ransome 2009, 54.
[331] Rittinghouse und Ransome 2009, 67. Dies muss allerdings nicht zwangsläufig ein Vorteil sein. Auf die Nutzung der jeweils aktuellsten Softwareversion zugunsten der Stabilität zu verzichten, ist bei Cloud-Services in der Regel nicht möglich.
[332] Rittinghouse und Ransome 2009, 35.
[333] Velte, Velte und Elsenpeter 2009, 15.
[334] Google o.J. Zu *Google Apps* siehe Abschnitt 5.7, S. 111.
[335] Velte, Velte und Elsenpeter 2009, 17.

4.2. Schwächen und Risiken des Cloud Computing

Die eben dargelegten Chancen, die Cloud Computing bietet, sollen nicht darüber hinwegtäuschen, dass es auch berechtigte Bedenken bezüglich der Nutzung von Cloud-Services gibt. Auch diese sind zum Teil den Bereichen Sicherheit und Kosten zuzuordnen. Darüber hinaus birgt Cloud Computing Risiken strategischer Natur.

4.2.1. Sicherheitsrisiken

Die negative Seite der mit der Nutzung von Cloud-Services einhergehenden Auslagerung bestimmter Tätigkeiten auf den Anbieter ist der Verlust der Kontrolle über diese Tätigkeiten. Dies betrifft insbesondere Sicherheitsmaßnahmen einschließlich der Ausfallsicherheit. Wie unter dem Stichwort Fokussierung oben bereits angesprochen, kann dies abhängig von der Professionalität der unternehmenseigenen IT-Abteilung auch ein positiver Aspekt sein. Allerdings verlangt Cloud Computing damit vom Nutzer nicht weniger, als sich auf die Zuverlässigkeit des Anbieters zu verlassen, denn die von diesem übernommene Gewährleistung und Haftung ist meist nicht sehr weitreichend.[336] Und selbst wenn der Anbieter haftet, kann der entstandene Schaden oftmals nicht ungeschehen gemacht und nur unzureichend finanziell kompensiert werden, etwa wenn Informationen über Sicherheitsprobleme an die Öffentlichkeit gelangt sind und den guten Ruf des Nutzers beeinträchtigen. Noch wesentlich schwerwiegender ist der Kontrollverlust, wenn der Anbieter berechtigt ist, zur Erbringung des Cloud-Service Sub-Dienstleister heranzuziehen.

Über das potenzielle Problem des Kontrollverlusts hinaus tun sich bei der Nutzung von Cloud-Services systembedingt im Vergleich zum Betrieb unternehmenseigener Server weitere Sicherheitsrisiken auf.[337] Zu nennen sind hier zunächst die Angriffsmöglichkeiten aufgrund der Tatsache, dass der Administrator-Zugriff remote erfolgt, man also in öffentlichen und nicht in privaten Netzwerken agiert. Ebenso ist die Nutzung ein und derselben Hardware durch mehrere Nutzer (multi-tenancy) ein zusätzliches Risiko. Denkbar sind hier einerseits die ungewollte gegenseitige Beeinflussung der Anwendungen verschiedener Nutzer und andererseits gezielte Angriffe zwischen virtuellen Maschinen oder Anwendungen innerhalb ein und desselben Servers.[338] Durch geeignete Maßnahmen muss daher gewährleistet werden, dass die Anwendungen verschiedener Nutzer vollständig voneinander isoliert sind, und nur jener Nutzer

---

[336] *Christopher Crowhurst*, VP of Strategic Technology bei *Thomson Reuters*, zitiert nach Velte, Velte und Elsenpeter 2009, 87 f. Näheres dazu siehe in Kapitel 5 (S. 81), wo die Haftung einzelner Anbieter im Detail beleuchtet wird.

[337] Zu Sicherheitsrisiken und -maßnahmen siehe ausführlich Mather, Kumaraswamy und Latif 2009, 35 ff.

[338] Rittinghouse und Ransome 2009, 161.

Zugriff auf die involvierten Daten hat, von dem diese jeweils stammen. Sicherheitslücken können hier nie gänzlich ausgeschlossen werden. Ein Spezialfall der gegenseitigen Beeinträchtigung von Nutzern kann dann eintreten, wenn einer der Nutzer illegal handelt und die von Behörden oder Dritten gegen dieses Verhalten ergriffenen Maßnahmen Auswirkungen auf andere Nutzer haben, deren virtuelle Maschinen oder Anwendungen auf demselben Server laufen.[339] Solche Maßnahmen können die Beschlagnahme von Datenträgern[340] oder das Blockieren von IP-Adressen durch Anti-Spam-Services sein.[341]

Nicht nur die Kontrolle über bestimmte Tätigkeiten wird im Zuge der Nutzung von Cloud-Services aus der Hand gegeben, sondern vor allem auch Daten, die in den Rechenzentren des Anbieters gespeichert werden. Sofern es sich um unverschlüsselte Daten handelt, die aus betrieblichen, rechtlichen oder anderen Gründen nicht in fremde Hände gelangen dürfen, entstehen dadurch zusätzliche Risiken. Zu denken ist hier einerseits an Fehler oder gezielte Angriffe, die zu unbefugtem Zugriff auf die Daten führen, andererseits auch an die absichtliche Herausgabe von Daten durch den Service-Anbieter an Sub-Dienstleister, Marketing-Unternehmen oder Behörden.[342] Zu einer Herausgabepflicht an Letztere kann es bei Daten, die in den USA gespeichert sind, insbesondere aufgrund des USA PATRIOT Act[343] kommen. Darüber hinaus kann man nie die Gewissheit haben, dass Daten, die man aus der Hand gegeben hat, jemals wieder gelöscht werden, wenn man diese zur Nutzung des jeweiligen Cloud-Service nicht mehr benötigt, dessen Nutzung einstellt oder die Festplatten, auf denen die Daten gespeichert waren, entsorgt werden.[344] Keiner der in Kapitel 5 untersuchten Cloud-Services sichert dies in den Vertragsbedingungen zu. Das Datensicherheitsrisiko ist damit eines der wesentlichen zusätzlichen Risiken im Zuge der Nutzung von Cloud-Services.

All diese Risiken können durch geeignete Maßnahmen des Anbieters wie auch des Nutzers verringert, nie aber gänzlich ausgeschlossen werden. *Armbrust et al*[345] gehen zwar davon aus, dass Cloud Computing technisch genau so sicher gemacht werden könne wie die meisten unternehmensinternen Systeme, die gängigen Anbieter von Cloud-Services geben dafür aber keinerlei rechtlich verbindliche Zusagen ab, wie im nachfolgenden Kapitel 5 gezeigt werden wird. Allerdings sollte dabei nicht vergessen

339 Armbrust et al (2009, 18) bezeichnen dieses Problem als „reputation fate sharing".
340 Rittinghouse und Ransome 2009, 158.
341 Armbrust et al. 2009, 18.
342 Velte, Velte und Elsenpeter 2009, 31 f.
343 PUBLIC LAW 107 - 56 - UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001, 26.10.2001. Siehe dazu Mather, Kumaraswamy und Latif 2009, 156 ff. und Velte, Velte und Elsenpeter 2009, 26.
344 Velte, Velte und Elsenpeter 2009, 99.
345 Armbrust et al. 2009, 15.

werden, dass – wie oben dargelegt – für Anbieter von Cloud-Services auch ohne rechtliche Verpflichtung ein Anreiz besteht, professionelle Sicherheitsmaßnahmen zu ergreifen, und dass insbesondere für KMU der Zugewinn an Sicherheit durch den Einsatz von Cloud-Services häufig deutlich größer ist als die zusätzlichen Risiken.

4.2.2. Strategische Risiken

Aufgrund der verbreiteten Verwendung proprietärer Architekturen, Technologien und Schnittstellen durch Anbieter von Cloud-Services besteht das Risiko der Abhängigkeit vom jeweiligen Anbieter (Vendor-Lock-in).[346] Dieses Problem ist am größten bei SaaS und PaaS.[347] Der Nutzer kann seine Daten und Programme oftmals nicht einfach aus einem Cloud-Service portieren und nahtlos in einem Cloud-Service eines anderen Anbieters weiter verwenden.[348] Es sollte allerdings nicht übersehen werden, dass auch beim lokalen Betrieb Abhängigkeiten von Herstellern, Plattformen und Technologien bestehen können.[349] Diese können hier sogar größer sein, etwa wenn teure Lizenzen erworben wurden. Während aber in diesem Fall zumindest die Daten lokal vorliegen, ist man beim Wechsel von Cloud-Services auf die jeweils angebotenen Exportmöglichkeiten beschränkt. Denkbar ist auch, dass der Anbieter den Datenexport künstlich erschwert, indem er dafür eine unangemessen hohe Gebühr verlangt.[350]

Vendor-Lock-in kann dazu führen, dass der jeweilige Anbieter für bestehende Kunden die Preise erhöht bzw. Verringerungen der ihm entstehenden Kosten nicht an diese weitergibt, während er neue Kunden mit extrem günstigen Angeboten ebenfalls in die Abhängigkeit lockt.[351] Es gibt allerdings Entwicklungen, die der Gefahr des Vendor-Lock-in entgegenwirken, insbesondere sind dies Open-Source-Software und Standardisierung. Beispielsweise gibt es mit *Eucalyptus*[352] ein Open-Source-Private-Cloud-Framework, dessen Schnittstellen mit *Amazon EC2* und *S3*[353] kompatibel sind, und mit *AppScale*[354] eine Open-Source-Implementierung von *Google App Engine*[355], die in der Lage ist, für *Google App Engine* entwickelte Webanwendungen auszuführen. Ein anderes Beispiel ist die jüngst erfolgte Veröffentlichung des Quellcodes seiner intern ver-

346 Baun et al. 2009, 69 und Armbrust et al. 2009, 15. Eine technische Erläuterung des Vendor-Lock-in im Zusammenhang mit IaaS siehe in Bias 2010.*Richard Stallman*, Gründer der Free Software Foundation, warnte 2008 eindringlich vor diesem Problem und bezeichnete Cloud Computing als eine Kampagne zur Schaffung solcher Abhängigkeiten (Johnson 2008).
347 Baun et al. 2009, 69.
348 Armbrust et al. 2009, 15.
349 Baun et al. 2009, 69.
350 Velte, Velte und Elsenpeter 2009, 13.
351 Mather, Kumaraswamy und Latif 2009, 229.
352 Nurmi et al. 2009 und Eucalyptus Systems 2010. Zum praktischen Einsatz siehe Baun et al. 2009, 99 ff.
353 Siehe dazu Abschnitt 5.1, S. 83.
354 AppScale o.J.
355 Siehe dazu Abschnitt 5.4, S. 96.

wendeten Cloud-Infrastruktur-Software durch *Rackspace*[356], um dadurch einen Standard zu schaffen.[357] Diese Beispiele stützen die folgende Hypothese bzgl. der Standardisierung: Es ist anzunehmen, dass proprietäre Technologien und Schnittstellen großer Anbieter von Cloud-Services im Laufe der Zeit auch von anderen, zum Teil später in den Markt eingestiegenen Anbietern verwendet werden und sich auf diese Weise zu Standards entwickeln.

Ein weiteres Risiko des Cloud Computing, das mit der Thematik des Vendor-Lock-in zusammenhängt, ist der Konkurs des Anbieters[358]. Nicht nur die Konsequenzen der Verwendung proprietärer Technologien und Schnittstellen werden in diesem Fall spürbar, weil man gezwungen ist, zu einem anderen Anbieter zu wechseln. Im schlimmsten Fall könnte der Betrieb der Server ohne Vorwarnung eingestellt werden, sodass man keine Gelegenheit mehr hat, Daten zu exportieren. Das Risiko des Konkurses des Anbieters besteht allerdings bei allen Formen des Outsourcings gleichermaßen.[359]

Neben der Abhängigkeit von einem bestimmten Anbieter kann es durch den Einsatz von Cloud-Services auch zur generellen Abhängigkeit von Cloud-Services bzw. externen Dienstleistungen kommen, weil dadurch unternehmensinternes Know-how verloren geht oder gar nicht aufgebaut wird. Dies soll hier in Anlehnung an den Begriff Vendor-Lock-in als Cloud-Lock-in bezeichnet werden.

Weitere Schwächen des Cloud Computing können sich daraus ergeben, dass die Nutzung von Cloud-Services notwendigerweise auch die Nutzung einer Internetverbindung erfordert. Diese weist eine gewisse Latenzzeit und einen begrenzten Datendurchsatz auf, was Cloud Computing für manche Anwendungen ungeeignet macht, bei denen es auf diese Leistungsparameter besonders ankommt.[360] Wenn sehr große Datenmengen übertragen werden müssen, ist das physische Versenden von Festplatten, wie es beispielsweise *Amazon Web Services* ermöglicht, ein Weg, dies zu umgehen.[361] Zudem kann die Internetverbindung ausfallen, wodurch der Zugriff auf alle Cloud-Services unterbrochen wird.[362] Dies ist eine klare Schwäche von SaaS gegenüber konventioneller, lokal betriebener Software. Die Nutzung von IaaS und insbesondere PaaS offenbart in diesem Zusammenhang allerdings auch eine Stärke. Lokal betriebene (Web-)Server wären in diesem Fall im Gegensatz zu in der Cloud betriebenen von außen ebenfalls nicht mehr erreichbar.

---

[356] Siehe dazu Abschnitt 5.2, S. 90.
[357] Bias 2010.
[358] Rittinghouse und Ransome 2009, 164.
[359] Baun et al. 2009, 69.
[360] Velte, Velte und Elsenpeter 2009, 28 f.
[361] Armbrust et al. 2009, 16. Zu *Amazon Web Services* (*AWS*) siehe Abschnitt 5.1, S. 83.
[362] Velte, Velte und Elsenpeter 2009, 5 f.

Auch die Suche und Behebung von Fehlern und Performanceproblemen kann durch die Verwendung von Cloud-Services erschwert werden, einerseits ebenfalls wegen der Verwendung einer Internetverbindung und andererseits aufgrund der generell gesteigerten technischen und organisatorischen Komplexität, die Cloud Computing mit sich bringt. [363]

Neben den bisher genannten Aspekten, können auch die in der zweiten Hälfte von Kapitel 3 beschriebenen rechtlichen Einschränkungen der Nutzung von Cloud-Services als Schwäche des Cloud Computing betrachtet werden. Sie führen dazu, dass in bestimmten Fällen sehr genau geprüft werden muss, ob ein Cloud-Service für das jeweilige Szenario eingesetzt werden darf. Fällt diese Prüfung negativ aus, ergibt sich dadurch eine Einschränkung.

Zwar keine Schwäche von Cloud-Services, aber ein Aspekt, der in die Entscheidungsfindung über die Umstellung eines bestehenden Systems auf die Nutzung von Cloud-Services einfließen sollte, ist die Tatsache, dass es sich dabei um eine Veränderung handelt und eine solche immer mit Risiken verbunden ist.[364] Nicht weil sich Cloud Computing derzeit als Trend abzeichnet, sondern nur aufgrund des Überwiegens der Stärken über die Schwächen im Einzelfall sollte daher ein System auf die Nutzung von Cloud-Services umgestellt werden.

4.2.3. Monetäre Aspekte

Die potenziellen finanziellen Vorteile des Cloud Computing wurden bereits behandelt.[365] Dabei wurde erwähnt, dass der Einsatz von Cloud Computing insgesamt auch höhere Kosten verursachen kann als Anschaffung und Betrieb eigener Infrastruktur, der Flexibilitätsvorteil des Cloud Computing allerdings in solche Überlegungen mit einfließen sollte. Je größer ein Unternehmen ist, desto eher ist es allerdings in der Lage, selbst direkt von Economies of Scale zu profitieren und damit Flexibilität und Effizienz auch in Private Clouds bzw. eigenen Rechenzentren zu erzielen. Dies kann in diesem Fall wirtschaftlicher sein, als die Nutzung von Public Clouds.

Ein Faktor, der bei der Kostenkalkulation ebenfalls bedacht werden muss, sind die gesteigerten Zuverlässigkeits- und Bandbreitenerfordernisse der Internetverbindung, die zuvor bereits angesprochen wurden. Zu berücksichtigen sind in diesem Zusammenhang auch jene Kosten, die vom Anbieter eines Cloud-Service für die Datenübertragung und das Speichern von Daten verrechnet werden.

---

[363] Velte, Velte und Elsenpeter 2009, 249 f.
[364] Velte, Velte und Elsenpeter 2009, 27 f.
[365] Siehe Punkt 4.1.4, S. 71.

Wie bereits in Abschnitt 1.3 erwähnt, muss eine detaillierte Kostenkalkulation als Teil der Entscheidungsfindung über den Einsatz von Cloud-Services stets im Einzelfall durchgeführt werden. Im Rahmen dieses Kapitels wurden lediglich die dabei zu berücksichtigenden Aspekte angesprochen. Letztlich können wohl die meisten der genannten Stärken und Schwächen des Cloud Computing monetär bewertet werden.

4.3. Exkurs: Cloud Computing und mobile Endgeräte

In diesem Abschnitt soll ein kurzer Überblick über einen spezifischen Aspekt des Cloud Computing gegeben werden, der sich als Trend der Zukunft abzeichnet:[366] Die Nutzung von Cloud Computing mittels mobiler Endgeräte, insbesondere Smartphones.[367] Dabei können zwei grundlegende Konzepte unterschieden werden, einerseits die Nutzung Smartphone-spezifischer Komponenten von (unternehmensweit eingesetzten) SaaS-Anwendungen mittels mobiler Endgeräte und andererseits die Erweiterung der Kapazitäten von Smartphones durch Cloud-Ressourcen. Ersteres wurde bereits unter den Stärken des Cloud Computing (Punkt 4.1.5, S. 72) angesprochen und wird darüber hinaus in der explorativen Marktanalyse im nächsten Kapitel behandelt: Die beiden untersuchten SaaS-Angebote *Salesforce CRM*[368] und *Google Apps*[369] bieten auch die Möglichkeit der Nutzung mittels Smartphone und enthalten eigens für diesen Zweck konzipierte Lösungen.

Eine besondere Stärke dieser mobilen Komponenten von SaaS-Anwendungen, die im Unternehmen eingesetzt werden, ist die systeminterne Kommunikation, die dadurch ermöglicht wird. Dies bedeutet, die Mitarbeiter können auch unterwegs direkt Aktionen in den unternehmensweit verwendeten Systemen setzen. Dies reicht vom mobilen Zugriff auf E-Mails, Adressen etc. und der gemeinsamen Bearbeitung von Dokumenten im Fall von *Google Apps* bis hin zur Nutzung der gesamten Funktionalität von *Salesforce Sales Cloud* mittels Smartphone, beispielsweise während eines Kunden-Meetings oder unmittelbar danach.

Währen bei diesem Ansatz die Integration von Smartphones in bestehende – und primär mittels Desktop-Systemen genutzte – SaaS-Anwendungen im Mittelpunkt steht, rückt das zweite eingangs genannte Konzept das Smartphone selbst in den Mittelpunkt. Es geht dabei um die Möglichkeit, technisch bedingte Einschränkungen von Smartphones – geringe Prozessorleistung im Vergleich zu Desktop-Systemen, beschränkte Akku-

366 Siehe dazu z.B. Perez 2010, Schmidt 2010.
367 Zum Begriff „Smartphone“ und den verschiedenen Plattformen siehe ausführlich Rittinghouse und Ransome 2009, 236 ff.
368 Siehe dazu Abschnitt 5.6, S. 105.
369 Siehe dazu Abschnitt 5.7, S. 111. *Google Mail* konnte bereits bisher mittels Smartphone genutzt werden, für *Google Text & Tabellen* wurde diese Möglichkeit jüngst ebenfalls angekündigt (Girouard 2010).

laufzeit[370] – durch den Einsatz von Cloud-Ressourcen zu umgehen. *Rittinghouse* und *Ransome* sprechen in diesem Zusammenhang davon, dass Cloud Computing wahrscheinlich die Zukunft des Mobile Computing sein wird.[371] Typische Anwendungen, für welche die Rechenleistung von Smartphones nicht ausreicht, und die daher erst durch Heranziehung von Cloud-Infrastruktur ermöglicht werden, sind die Text- und Spracherkennung und Übersetzung in Echtzeit.[372] Es stellt sich allerdings die Frage, ob dieses Konzept nicht vom technischen Fortschritt in der Entwicklung von Smartphone-Prozessoren überholt werden wird. Wenn sich das Konzept hingegen durchsetzt, könnte der umgekehrte Fall eintreten und die Entwicklung schnellerer Prozessoren mangels Bedarf verlangsamt werden.

Die Nutzung von Cloud Computing mittels mobiler Endgeräte und damit beide beschriebenen Konzepte weisen eine Schwäche auf: Die Internetverbindung von Smartphones ist nicht so zuverlässig wie jene von Desktop-Systemen und kann von Zeit zu Zeit ausfallen. Software, die von Cloud-Infrastruktur abhängig ist, funktioniert dann grundsätzlich nicht mehr. *Armbrust et al.*[373] weisen allerdings darauf hin, dass die Herausforderung des Offline-Betriebs auch in anderen Anwendungsgebieten bereits erfolgreich gelöst werden konnte und sich daher auch in diesem Fall Lösungen für dieses Problem entwickeln werden. Eine davon ist das kommende HTML5, das Features für den Umgang mit Verbindungsunterbrechungen beinhalten wird.[374]

[370] Die Prozessorleistung ist die primäre Einschränkung. Allerdings kann unter bestimmten Voraussetzungen durch Auslagerung von rechenintensiven Aufgaben in die Cloud tatsächlich auch Energie gespart werden (Kumar und Lu 2010).
[371] Rittinghouse und Ransome 2009, 257.
[372] Schmidt 2010.
[373] Armbrust et al. 2009, 7.
[374] Perez 2010.

5. Explorative Marktanalyse

"Using Amazon Web Services, Hadoop and our own code, we ingested 405,000 very large TIFF images, 3.3 million articles in SGML and 405,000 xml files mapping articles to rectangular regions in the TIFF's. This data was converted to a more web-friendly 810,000 PNG images (thumbnails and full images) and 405,000 JavaScript files — all of it ready to be assembled into a TimesMachine. By leveraging the power of AWS and Hadoop, we were able to utilize hundreds of machines concurrently and process all the data in less than 36 hours."[375]

In diesem Kapitel werden die Ergebnisse einer explorativen Marktanalyse bedeutender kommerzieller Cloud-Services präsentiert. Die Auswahl der untersuchten Services erhebt weder Anspruch auf Vollständigkeit, noch darauf, ein repräsentativer Querschnitt des gesamten Angebots zu sein.[376] Die Services wurden Aufgrund der Häufigkeit des Auftretens während der Recherchen zur vorliegenden Diplomarbeit sowie aufgrund erwähnenswerter Besonderheiten ausgewählt. Dabei wurde darauf geachtet, Anbieter aller drei Service-Modelle (SaaS, PaaS und IaaS) ausgewogen zu berücksichtigen. Auf diese Weise wird ein Überblick über einige derzeit in der Praxis meistverwendeten Services gegeben.

Da die einzelnen Angebote rasch verändert und erweitert werden, veraltet Literatur über konkrete Cloud-Services sehr schnell. Aus diesem Grund entstammt ein Großteil der Informationen dieses Kapitels bewusst nicht der Literatur sondern eigenen Recherchen, die nach Möglichkeit direkt auf der Website des jeweils untersuchten Anbieters durchgeführt wurden.[377]

---

375 *Derek Gottfrid*, Senior Software Architect and Product Technologist at *The New York Times*, über das Projekt „*TimesMachine*" (Gottfrid 2008). *TimesMachine* ist abrufbar unter http://timesmachine.nytimes.com/browser (Zugriff am 24. September 2010). Zu *Amazon Web Services* siehe Abschnitt 5.1, S. 83. *Hadoop* ist ein Open-Source-Framework zur Verarbeitung großer Datenmengen, das die Ansätze des Programmiermodells *Google MapReduce* (Dean und Ghemawat 2008) und des *Google File System* (Ghemawat, Gobioff und Leung 2003) implementiert (Fischer 2010).

376 Dieser Anspruch ist aufgrund der Dimensionen, die der Cloud-Computing-Markt bereits angenommen hat, im Rahmen einer Diplomarbeit nicht erfüllbar. Dies illustriert etwa das Beispiel einer regelmäßig aktualisierten Liste relevanter Unternehmen und Organisationen im Bereich Cloud Computing („The Top 250 Players in the Cloud Computing Ecosystem"), die im Jänner 2010 noch 150 Nennungen umfasste und bis September 2010 auf 250 angewachsen ist (Geelan 2010).

377 Alle anbieterspezifischen Informationen in diesem Kapitel ohne gesonderte Quellenangabe stammen von der Website des jeweiligen Anbieters. Die entsprechende URL ist den Angaben am Beginn des entsprechenden Abschnitts dieses Kapitels zu entnehmen. Primärquellen, d.h. URLs zu vorgestellten Anbietern, Initiativen, Projekten, Software etc. und den dort zu findenden Angaben, werden in diesem Kapitel aus Gründen der Übersichtlichkeit direkt als URL und nicht im Rahmen des Literaturverzeichnisses angegeben.

Aktiv getestet – im Sinne der praktischen Verwendung des jeweiligen Service – wurden nicht alle untersuchten Services. Dies war zur Erlangung der benötigten Informationen nicht erforderlich. Dennoch wurden die Services *Amazon EC2* und *S3* und *Google App Engine* im Rahmen eines eigens konzipierten Testprojekts eingesetzt, um einen Eindruck von der praktischen Nutzung von Cloud-Services zu erhalten. Als Testprojekt wurde die in einer – aus 15 Knoten bestehenden – Hybrid Cloud verteilte Kompilierung einer *Linux*-Distribution für eine spezielle Hardware-Plattform gewählt. Gesteuert wurde diese durch ein Webservice, welches in *Google Apps Engine* lief. Näheres zu diesem Projekt siehe in Kapitel 7. Zusätzlich wurde von den in diesem Kapitel untersuchten SaaS-Angeboten *Google Apps* aktiv getestet.

Im Folgenden sind zu den einzelnen Cloud-Services zunächst grundsätzliche Angaben wie Service-Modell, Anbieter und URL angeführt. Es folgt jeweils eine Beschreibung des/der angebotenen Service(s). Anschließend wird jeweils auf die Vertragsbedingungen eingegangen. Wichtige Bestimmungen werden in eigenen Worten zusammengefasst wiedergegeben. Sofern die untersuchten AGB und sonstigen Vertragsbestandteile durch Nummerierungen gegliedert sind, wird bei jeder Erwähnung einer Bestimmung angegeben, unter welcher Nummer diese im Originaldokument zu finden ist. Aufgrund ihres Umfangs konnten die Vertragsbedingungen aller untersuchten Cloud-Services nicht im Volltext in die vorliegende Arbeit aufgenommen werden. Um allerdings einen Eindruck solcher Vertragsbedingungen zu vermitteln, wurden die AGB und sonstigen untersuchten Vertragsbestandteile eines Anbieters (*Amazon Web Services*), im Volltext in Anhang C aufgenommen.

Zur Untersuchung solcher Vertragsbedingungen ist anzumerken, dass diese nicht unabhängig vom geltenden Recht existieren. Es ist durchaus möglich, dass einzelne Vertragsklauseln dem Gesetz widersprechen und daher im Streitfall letztlich nicht anzuwenden wären.[378] Um solche Widersprüche erkennen zu können, ist die Kenntnis des geltenden Rechts erforderlich. Da die Verträge der untersuchten Anbieter von Cloud-Services nicht österreichischem Recht unterliegen, sondern Rechtsordnungen, über die der Autor keine Kenntnis hat, kann über dieses Zusammenwirken der Vertragsbedingungen mit dem Gesetz nichts ausgesagt werden. Es ist daher nicht ausgeschlossen, dass im Folgenden einzelne Vertragsklauseln besprochen werden, die letztlich keine Wirkung entfalten würden, da ihnen das geltende Recht vorgeht. Dies müsste vom Nutzer allerdings erst gerichtlich durchgesetzt werden, was aufwändig und erst im Nach-

[378] Unter den Punkten 11.5 und 11.8 des „Amazon Web Services Customer Agreements“ (siehe Anhang B) ist dies beispielsweise ausdrücklich angesprochen: Die dort geregelten Garantie-, Gewährleistungs- bzw. Haftungsausschlüsse gelten nur, soweit dies gesetzlich zulässig ist.

hinein möglich ist. Daher haben auch solche dem Gesetz widersprechende Klauseln eine faktische Wirkung und die Auseinandersetzung mit ihnen eine Berechtigung.

5.1. Amazon Web Services (AWS)

Service-Modell	*IaaS (Ressourcen-Sets, Infrastruktur-Services)*
Service-Anbieter (für Nutzer in Österreich)	*Amazon Web Services LLC* *P.O. Box 81226* *Seattle, WA 98108-1226* *USA*
Service-URL	*http://aws.amazon.com*

Amazon kann wohl als der führende Anbieter von IaaS bezeichnet werden.[379] Kern des Angebots ist die *Amazon Elastic Compute Cloud* (*EC2*), die Ressourcen-Sets – d.h. virtuelle Server – on-demand zur Verfügung stellt. Daneben wird eine große Zahl von Infrastruktur- und sonstigen Services angeboten, darunter insbesondere Datenspeicherungs- und Monitoring-Services, die ergänzend zu *EC2* und zum Teil auch eigenständig eingesetzt werden können. Neben *EC2* werden im Folgenden auch einige dieser Services näher betrachtet.[380] Aufgrund dieses umfangreichen Angebots von *AWS* und weil *Amazon EC2* und *Amazon S3*[381] im Zuge der vorliegenden Diplomarbeit aktiv getestet wurden,[382] fällt dieser Abschnitt im Vergleich zur Behandlung anderer Anbieter sehr ausführlich aus. Dies erscheint dem Autor aufgrund der großen Bedeutung von *AWS* angemessen.

Vor der Beschreibung der einzelnen Webservices folgt eine kurze Einführung in die Organisation und einige Gemeinsamkeiten der Services. Die Rechenzentren von *AWS* sind auf vier voneinander isolierte Regionen verteilt, „US East“ (Virginia), „US West“ (Kalifornien), „EU“ (Irland) und „Asia Pacific“ (Singapur). In jeder der vier Region gibt es Server in mindestens zwei so genannten „Availability Zones“, die technisch unabhängig und physisch getrennt betrieben werden, sodass keine gemeinsamen Fehlerquellen bestehen und Naturkatastrophen nicht mehrere Availability Zones gleichzeitig beeinträchtigen können. Vor der Nutzung eines Service, etwa beim Starten eines

[379] Diese Ansicht stützend Bias 2010, Urquhart 2010 und Rosen 2010. Zur Entwicklung von *Amazon* vom Web-Buchhändler zu einem der ersten Anbieter von Cloud-Services siehe Rhoton 2010.

[380] Eine ausführliche Beschreibung von *AWS* siehe auch in Rittinghouse und Ransome 2009, 37 ff.

[381] Siehe dazu Punkt 5.1.2, S. 85.

[382] Eine Zusammenfassung des Testprojekts, das unter anderem Einblicke in die praktische Verwendung von *Amazon EC2* und *S3* gibt, befindet sich in Kapitel 7.

virtuellen Servers, kann angegeben werden, in welcher Availability Zone dies erfolgen soll.

Die Datenübertragungskosten sind für alle Services gemeinsam geregelt. Eingehender Datentransfer kostet 0,10 USD, ausgehender 0,15 USD pro GB.[383] Ab einem Transfervolumen von 10 TB sinken die Kosten pro GB in mehreren Stufen. Auch für Datentransfer zwischen Services in unterschiedlichen Regionen fallen die angegebenen Kosten an, Datentransfer zwischen Availability Zones in derselben Region kostet 0,01 USD pro GB. Die Kosten der verschiedenen Services sind meist in den vier Regionen unterschiedlich hoch und in der Regel in der Region „US East" am geringsten.[384]

Die Gefahr des Vendor-Lock-in wird bei *AWS* durch die Existenz des Open-Source-Private-Cloud-Frameworks *Eucalyptus*[385] etwas entschärft, dessen Schnittstellen mit *Amazon EC2* und *S3* kompatibel sind. Somit kann mittels *Eucalyptus* bei Bedarf die Nutzung von *EC2* und *S3* durch eine Private Cloud ersetzt werden, ohne Änderungen in der Systemarchitektur und den Schnittstellen vornehmen zu müssen.

5.1.1. Amazon Elastic Compute Cloud (EC2)

Auf *Amazon EC2* können virtuelle Server (genannt Instanzen) verschiedener Leistungsklassen und mit verschiedenen Betriebssystemen betrieben werden. Eine beliebige Anzahl von Instanzen kann innerhalb weniger Minuten gestartet werden, die Abrechnung erfolgt pro angefangener Stunde. Die günstigste verfügbare Instanz bietet etwa die Leistung eines Büro-PC und kostet 0,085 USD pro Stunde. Bei höherem Leistungsbedarf sind verschiedene virtuelle Konfigurationen bis hin zum Leistungsäquivalent zweier aktueller Vierkern-Prozessoren und 68,4 GB Hauptspeicher verfügbar. Diese Konfiguration kostet beispielsweise 2,40 USD pro Stunde. Als Betriebssysteme können *Linux*, *OpenSolaris* und *Microsoft Windows* verwendet werden, wobei die stündlichen Kosten für *Windows*-Server deutlich höher sind, als für Server mit den anderen Betriebssystemen. Es können beliebige *Linux*-Distributionen eingesetzt werden,[386] da neben vorgefertigten auch vom Nutzer selbst erstellte *Linux*-Images verwendet werden können. Zudem besteht die Möglichkeit, solche Images anderen Nutzern kostenpflichtig zur Verfügung zu stellen. Dies nutzen etwa Unternehmen wie *IBM* oder *Microsoft*, um Server mit ihrer Software auf *EC2* verfügbar zu machen.

---

[383] Bis 1. November 2010 ist allerdings der gesamte eingehende Datentransfer gebührenfrei.

[384] Alle Kostenangaben in diesem Abschnitt beziehen sich auf diese Region. Die regionalen Kostenunterschiede betragen bis zu ca. 20%. Wie bereits an anderer Stelle erwähnt, dienen die Kostenangaben primär dazu, die Größenordnung der Kosten zu vermitteln, wozu bereits die Angaben zu einer Region ausreichen.

[385] Nurmi et al. 2009 und Eucalyptus Systems 2010. Zum praktischen Einsatz siehe Baun et al. 2009, 99 ff.

[386] Es muss allerdings einer der vorgegebenen Linux-Kernels verwendet werden, jedoch ist eine große Zahl verschiedener Kernels verfügbar.

EC2-Instanzen können mittels eines Low-Level-Web-Service-Interfaces oder eines Web-Interfaces oder mit dem Plug-in *Elasticfox*[387] für *Mozilla Firefox* gestartet, gestoppt und verwaltet werden. Aufgrund der Steuerungsmöglichkeit mittels Web-Service-Interface können diese Vorgänge einerseits auch durch Konsolenbefehle und andererseits automatisiert und mittels selbst entwickelter Software ausgeführt werden. Der Zugriff auf die laufenden Instanzen erfolgt wie bei einem privaten Remote-Server mittels SSH (*Linux*) bzw. RDP (*Windows*) und ermöglicht root- bzw. Administratorrechte.

Amazon EC2 bietet neben dem bedarfsabhängigen Starten von Instanzen durch den Nutzer noch zwei weitere Abrechnungsmodelle. Einerseits gibt es eine laufende Auktion für ansonsten ungenutzte Ressourcen. Der Nutzer kann einen Maximalpreis für eine bestimmte Instanz angeben. Liegt der nachfrageabhängige aktuelle Preis unter diesem Maximalpreis, wird die Instanz gestartet. Dies kann genutzt werden, um zeitlich unkritische Aufgaben sehr kostengünstig zu erledigen. Während der Tests durch den Autor lag der Preis einer solchen „Spot Instance" stets bei weniger als der Hälfte des Preises einer herkömmlichen Instanz. Darüber hinaus wird andererseits auch ein konventionelles, langfristiges Abrechnungsmodell angeboten. Beliebige Instanzen können gegen eine einmalige Zahlung als so genannte „Reserved Instances" für ein Jahr oder drei Jahre durchgehend gemietet werden. Falls ohnehin der Dauerbetrieb einer Instanz geplant ist, ergibt sich dadurch – zulasten der Flexibilität – ein deutlicher Kostenvorteil gegenüber einer herkömmlichen on-demand-Instanz.[388]

5.1.2. Amazon Simple Storage Service (S3)

Amazon S3 dient dem Speichern beliebiger Dateien und kann sowohl als eigenständiger Service als auch in Verbindung mit *Amazon EC2* verwendet werden.[389] Beispielsweise werden auch die vom Nutzer selbst erstellten *Linux*-Images in *S3* gespeichert. Das Speichern, Abrufen und Verwalten der Daten erfolgt mittels eines einfachen Low-Level-Web-Service-Interfaces. Alternativ zu den Konsolenbefehlen kann auch hier ein Web-Interface oder ein Plug-in für *Mozilla Firefox* namens *S3Fox Organizer*[390] verwendet werden. Jede in *S3* gespeicherte Datei kann direkt unter einer individuellen URL im Web-Browser abgerufen werden, sodass sie – je nach den vom Nutzer vergebenen Zugriffsrechten – von jedermann heruntergeladen werden kann.

---

[387] Siehe dazu http://developer.amazonwebservices.com/connect/entry.jspa?externalID=609.
[388] Genau genommen handelt es sich dabei allerdings nicht mehr um Cloud Computing, da das Kriterium der „rapid elasticity" fehlt (siehe Tabelle 1, S. 28).
[389] Einen kurzen Überblick über die Funktionsweise geben Velte, Velte und Elsenpeter 2009, 142 ff.
[390] Siehe unter http://developer.amazonwebservices.com/connect/entry.jspa?externalID=366.

Das Speichern von einem GB Daten für einen Monat kostet 0,15 USD bei einer angegebenen Verfügbarkeit von 99.999999999% und 0,10 USD bei reduzierter Verfügbarkeit (99,99%). Die *Angaben* von Amazon deuten darauf hin, dass eine Replikation der Daten an drei – bzw. bei der Variante mit reduzierter Verfügbarkeit an zwei – unabhängigen Orten vorgenommen wird.[391]

5.1.3. Amazon Elastic Block Storage (EBS)

Im Gegensatz zur dateibezogenen Speicherlösung *Amazon S3*, bei welcher der (weltweite) Zugriff auf einzelne Dateien im Vordergrund steht, stellt *Amazon EBS* virtuelle Datenträger für die Verwendung mit *EC2*-Instanzen zur Verfügung. Diese virtuellen Datenträger – mit einer Größe zwischen einem GB und einem TB – können jeweils einer bestimmten *EC2*-Instanz zugewiesen und von dieser wie ein herkömmliches Laufwerk verwendet werden. Einer Instanz können gleichzeitig auch mehrere virtuelle Datenträger zugewiesen werden, ein Datenträger aber nicht mehreren Instanzen gleichzeitig. Zusätzlich ist es möglich, *EBS*-Datenträger als Boot-Partitionen für Instanzen zu verwenden. Auf diese Weise gehen Änderungen der Boot-Partition nicht verloren, wenn eine Instanz gestoppt wird.

Datensicherheit wird bei *EBS* ebenfalls durch Replikation erreicht, sowie durch die Möglichkeit, zu einem beliebigen Zeitpunkt Snapshots eines *EBS*-Datenträgers in *Amazon S3* abzulegen. Die Nutzung von *EBS* kostet pro GB und Monat 0,10 USD zuzüglich 0,10 USD pro einer Million Eingabe-/Ausgabe-Anfragen.

5.1.4. Amazon CloudFront

Amazon CloudFront ist ein Service zur Leistungssteigerung bei der Bereitstellung von Daten aus *Amazon S3*. Durch die Verteilung der Daten über weltweit 16 so genannte „Edge-Standorte“ – davon neun in den USA, vier in Europa und drei in Asien – und bedarfsorientierte Spiegelung können Zugriffszeiten verkürzt und Datenübertragungen beschleunigt werden. Der Zugriff erfolgt mittels HTTP (Download) oder mittels RTMP (Streaming). Die Gesamtkosten sind zwar höher als bei herkömmlicher Datenübertragung, es entstehen allerdings nur dann Kosten, wenn tatsächlich Daten übertragen werden. Für das bloße Vorhalten von Daten mittels *Amazon CloudFront* fallen daher – abgesehen von der monatlichen Gebühr für die Speicherung der Originaldatei(en) in *S3* – keine Kosten an.

[391] Amazon Web Services o.J.

5.1.5. Amazon Simple Queue Service (SQS)

Mit *Amazon SQS* können über eine Web-Service-Schnittstelle Queues zum Speichern von Nachrichten erzeugt werden, die der asynchronen Kommunikation zwischen verteilten Komponenten dienen. *SQS* ist besonders auf Skalierbarkeit und Zuverlässigkeit ausgelegt und bietet Mechanismen zur Authentifizierung. Die Abrechnung erfolgt mittels einer sehr geringen Gebühr pro Anfrage. Hinzu kommen die üblichen Datentransferkosten.

5.1.6. Vertragsbedingungen

Wie in Abbildung 6 ersichtlich muss der Nutzer dem „Amazon Web Services Customer Agreement“ zustimmen, um einen Account bei *AWS* zu erstellen. Dieses enthält die wesentlichen Vertragsbedingungen und verweist zudem auf fünf weitere Dokumente, die dadurch ebenfalls Vertragsbestandteil werden. Für zwei der vier oben beschriebenen Services – *EC2* und *S3* – existiert darüber hinaus ein SLA. Im Folgenden wird auf die wichtigsten Vertragsbestimmungen aus diesen Dokumenten näher eingegangen. Die behandelten Dokumente befinden sich im Volltext in Anhang C.

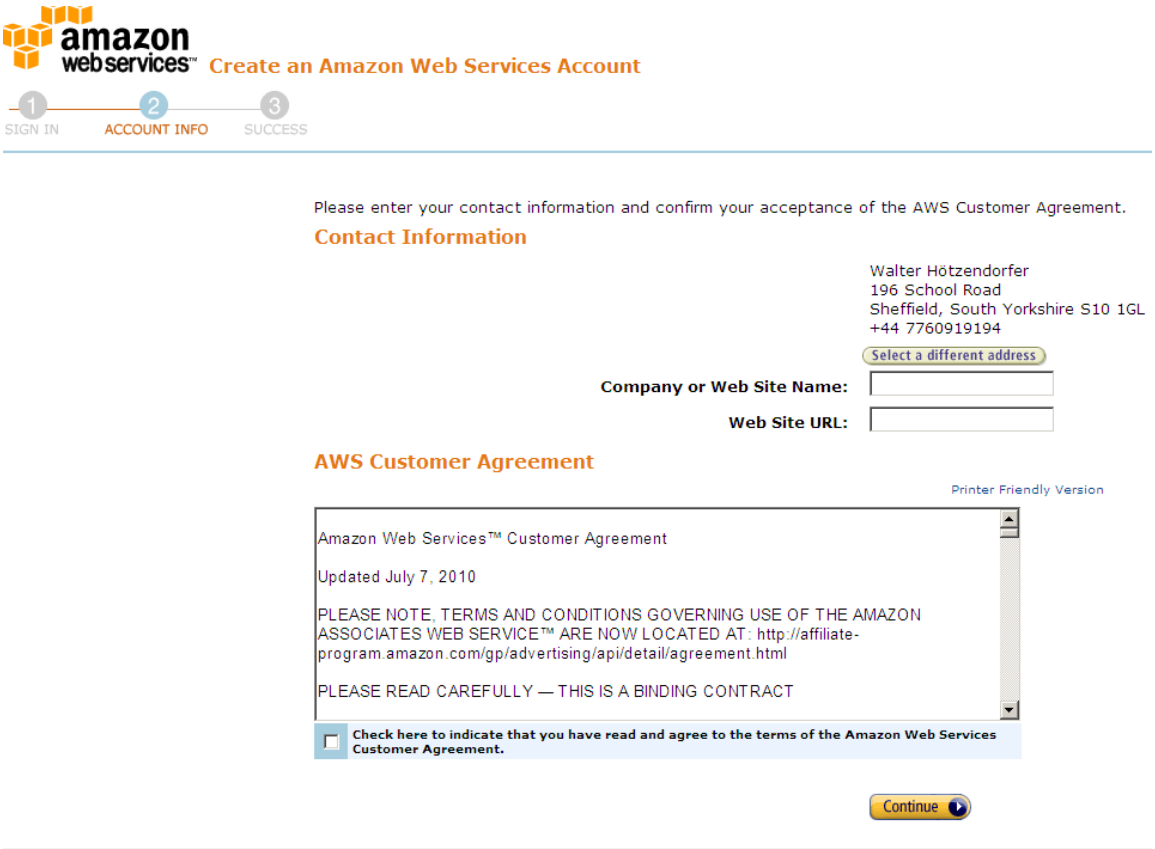


Abbildung 6 – Erstellung eines Accounts bei *AWS*[392]

[392] Quelle: Screenshot von http://aws.amazon.com (erstellt am 16. August 2010).

Wichtige Bestimmungen des AWS Customer Agreements:

- 2.: Das Customer Agreement kann durch *AWS* jederzeit einseitig geändert werden.
- 3.3.2.: Die Kündigung des Service durch *AWS* ist ohne Angabe von Gründen innerhalb von 60 Tagen nach Mitteilung möglich. In diesem Fall:
  - 3.7.2.: Recht des Nutzers auf weitere 30 Tage Speicherung der Daten
  - 3.7.2.: Recht des Nutzers, die Daten zurückzubekommen
- 3.7.3.: Im Fall der Kündigung durch *AWS* wegen Verfehlungen des Nutzers besteht kein Recht auf Rückerhalt der Daten.
- 4.3.: *AWS* ist nicht verantwortlich für Datenverlust und unautorisierten Datenzugriff.
- 7.1.: Nichtverfügbarkeit des Service kann jederzeit auftreten, und der Service kann planmäßig oder in Reaktion auf bestimmte Ereignisse jederzeit ausgesetzt werden, jeweils ohne dass *AWS* dafür eine Haftung übernimmt.
- 7.2.: Sicherheit wird nicht garantiert, keine Haftung für unautorisierten Datenzugriff, Datenverlust etc.
- 8.1.: Die Kosten können jederzeit erhöht werden, sofern dies 30 Tage vorher angekündigt wurde.
- 10.2.: Alle Arten von Nutzerdaten können durch *AWS* herausgegeben werden, wenn dies von einer Regierungs- oder Regulierungsbehörde, oder durch gerichtliche Anordnung gefordert wird.
- 11.5.: Gewährleistungsausschluss. *AWS* übernimmt keine Verantwortung oder Gewährleistung jeglicher Art, insbesondere keine Gewährleistung für die beschriebene Funktionalität, jeweils soweit dies nach dem anwendbaren Recht zulässig ist.
- 11.8.: Haftungsausschluss. *AWS* übernimmt keine Haftung und leistet keinen Schadenersatz, wenn Services nicht benutzt werden können, oder wenn auf die Nutzerdaten unautorisiert zugegriffen wurde. Zusätzlich wird allfälliger Schadenersatz mit der Höhe aller vom Nutzer jemals geleisteten Servicegebühren limitiert. Dies alles gilt ebenfalls soweit es nach anwendbarem Recht zulässig ist.
- 14.1.: Gerichtszuständigkeit. Rechtstreitigkeiten mit einem Streitwert von mehr als mehr als 7.500 USD sind vor den Gerichten in King County, Washington auszutragen.
- 14.2.: Rechtswahl. Der Vertrag und alle zwischen den Vertragspartnern auftretenden Rechtstreitigkeiten unterliegen ausschließlich dem Recht des Staates Washington.

Von den fünf weiteren Dokumenten, auf welche das *AWS* Customer Agreement verweist, ist hier nur die „Amazon.com Privacy Notice“ wesentlich. In dieser behält sich *Amazon* das Recht vor, Subdienstleister einzusetzen und diesen Nutzerdaten zu übertragen, soweit dies notwendig ist. Darüber hinaus ist der Privacy Notice zu entnehmen, dass *Amazon* am Safe-Harbor-Programm teilnimmt.[393] Die übrigen vier Dokumente enthalten keine im Rahmen dieser Untersuchung relevanten Bestimmungen. Einer Übersichtsseite zu den Sicherheitsmaßnahmen ist zu entnehmen, dass *AWS* SAS-70-zertifiziert ist.

Wichtige Bestimmungen des Service Level Agreements von EC2:

- *AWS* verpflichtet sich dazu, wirtschaftlich sinnvolle Anstrengungen unternehmen, um eine jährliche Verfügbarkeit von mindestens 99,95% zu erreichen.[394]
- Wird dies nicht erreicht, erhält der Nutzer eine Gutschrift in Höhe von 10% seiner Monatsrechnung, anrechenbar auf zukünftige Rechnungen.
- Der Service gilt nur dann als nicht verfügbar, wenn innerhalb einer Region mindestens zwei Availability Zones, in denen der Nutzer Instanzen betreibt, für über fünf Minuten keine Verbindung zum Internet haben.[395]
- Die geplante oder ungeplante Aussetzung des Service nach Abschnitt 7.1 des *AWS* Customer Agreements (siehe oben) ist von dieser Regelung ausgenommen, ebenso wie Nichtverfügbarkeit, deren Ursache außerhalb der Kontrolle von *AWS* liegt.
- Zusätzlich behält sich *AWS* vor, für bestimmte Gründe der Nichtverfügbarkeit nach eigenem Ermessen keine Gutschrift zu geben.

Wichtige Bestimmungen des Service Level Agreements von S3:

- *AWS* wird wirtschaftlich sinnvolle Anstrengungen unternehmen, um eine monatliche Verfügbarkeit von mindestens 99,9% zu erreichen.
- Wird dies nicht erreicht, erhält der Nutzer eine Gutschrift in Höhe 10% – bzw. bei einer Verfügbarkeit von weniger als 99% in Höhe von 25% – seiner Monatsrechnung, anrechenbar auf zukünftige Rechnungen.
- Die Verfügbarkeit wird aus dem Verhältnis von erfolgreichen zu fehlerhaften Server-Anfragen in Zeiträumen von jeweils fünf Minuten berechnet.

---

393 Zum Safe-Harbor-Programm siehe Punkt 3.2.5, S. 56.

394 Anmerkung: Die jährliche Verfügbarkeit ist (im Vergleich zu einer monatsbezogenen Angabe) ein sehr grobes Maß. Ein einmaliger großer Ausfall von über vier Stunden entspricht noch immer weniger als 0,05% eines Jahres und wäre somit kein Verstoß gegen die Verfügbarkeitszusage.

395 Ausfälle, die nur vier Minuten dauern, werden folglich nicht berücksichtigt, selbst dann nicht, wenn sie häufig auftreten.

- Es bestehen die gleichen Ausnahmen von dieser Regelung wie im Service Level Agreement von *EC2*.

Die besprochenen Vertragsbedingungen von *AWS* offenbaren, dass die Rechtsposition des Nutzers sehr schwach ist. Wie gezeigt wurde, ist jegliche Haftung und Gewährleistung ausgeschlossen, soweit dies gesetzlich zulässig ist. Lediglich eine Verfügbarkeitszusage wird abgegeben, bei deren Nichterfüllung der Nutzer in der Praxis aber nur einen sehr geringen Ersatz erhält. Der Nutzer muss sich daher darauf verlassen, dass *AWS* – im Sinne der diesbezüglichen Überlegungen unter Punkt 4.1.3 (S. 70) – trotz der unzureichenden vertraglichen Verpflichtung für Sicherheit und Zuverlässigkeit sorgt, um hohe Kundenzufriedenheit zu schaffen und einen guten Ruf aufzubauen und zu behalten.

Eine Zusicherung der Erfüllung der Dienstleisterpflichten nach § 11 DSG 2000 kann den Vertragsbedingungen nicht entnommen werden. Insbesondere wird nichts über das Heranziehen von Subdienstleistern und das Löschen aller Daten des Nutzers nach Vertragsbeendigung ausgesagt.

5.2. Rackspace Cloud

Service-Modell	*IaaS (Ressourcen-Sets, Infrastruktur-Services), PaaS*
Service-Anbieter (für Nutzer in Österreich)	*Rackspace* *5000 Walzem Road* *San Antonio, TX 78218* *USA*
Service-URL	*http://www.rackspacecloud.com*

Ein eigenes Cloud-Angebot von *Rackspace* für den europäischen Markt ist derzeit im Aufbau und soll noch im Laufe des Jahres 2010 verfügbar sein.[396] Generell scheint sich das Unternehmen derzeit in einer Umstellungs- bzw. Expansionsphase zu befinden. Als der Autor einem Mitarbeiter von *Rackspace* in einem Telefonat mitteilte, dass seine Anmeldung bei *Rackspace* ausschließlich der Untersuchung der Funktionalität diene, erwähnte dieser, eine solche Untersuchung würde bereits in einigen Monaten zu ganz anderen Ergebnissen führen, weil die von *Rackspace* gebotenen „Möglichkeiten“ dann viel umfangreicher sein würden.

[396] Siehe Ankündigung unter http://www.rackspace.co.uk/cloud-hosting/public-cloud/register-interest.

Diese Expansionspläne, die Erwähnungen in der Literatur und die – allerdings nur beschränkt aussagekräftigen – Erhebungen von *Rosen*[397] lassen allerdings darauf schließen, dass *Rackspace* einer der bedeutendsten Konkurrenten von *Amazon Web Services* auf dem IaaS-Markt ist. Zusätzliche Bedeutung kommt *Rackspace* auch durch die vor kurzem erfolgte Veröffentlichung des Quellcodes seiner intern verwendeten Cloud-Infrastruktur-Software im Rahmen der *OpenStack*-Initiative zu.[398]

Aufgrund der beschriebenen Umbruchphase, in dem sich die Angebote des Unternehmens derzeit befinden, wird allerdings auf eine Servicebeschreibung und eine Untersuchung der Vertragsbedingungen verzichtet.

5.3. FlexiScale

Service-Modell	*IaaS (Ressourcen-Sets)*
Service-Anbieter	*Flexiant Limited*
(für Nutzer in Österreich)	*Geddes House*
	Kirkton North
	Livingston
	EH54 6GU
	United Kingdom
Service-URL	*http://www.flexiant.com/products/flexiscale*

FlexiScale wurde in diese Marktanalyse aufgenommen, da es ein europäisches IaaS-Angebot ist. Unternehmenssitz und Standort des einzigen Rechenzentrums ist England.

5.3.1. Servicebeschreibung

Flexiant bietet unter der Marke *FlexiScale* virtuelle Server an, die stundenweise auf Basis von so genannten „Units“ abgerechnet werden. Diese Units müssen vom Nutzer im Vorhinein erworben werden, wobei der Preis pro Unit mit der Anzahl der gleichzeitig erworbenen Units sinkt. Bei Abnahme von 10.000 Units entspricht eine Unit etwa 0,01 GBP. Die Konfiguration der virtuellen Server kann aus verschiedenen Kombinationen von eins bis vier virtuellen CPUs und 0,5 bis acht GB Speicher gewählt werden. Beispielsweise kostet ein Server mit einem GB Speicher und einer virtuellen CPU drei Units, die Maximalvariante (acht GB, vier CPUs) 20 Units pro Stunde. Hinzu kommen die Kosten für die Nutzung von virtuellen Datenträgern, von denen jeder Server min-

[397] Rosen 2010. *Rosen* erhebt monatlich, wie viele der 500.000 in den USA meistbesuchten Websites auf Webservern in einer IaaS-Cloud betrieben werden und bei welchen Anbietern dies erfolgt. Da Webhosting nur eine von vielen möglichen Anwendungen von IaaS ist, können die Ergebnisse dieser Erhebung nur als Indiz für die gesamte Nutzung der jeweiligen Services herangezogen werden. Die Daten sind allerdings verhältnismäßig leicht zu erheben.

[398] Bias 2010.

destens einen benötigt, denn auf diese Weise werden die Server persistiert, wenn sie nicht laufen. Zur Laufzeit werden zwei Units pro GB für Lese- und Schreiboperationen auf diesen Datenträgern fällig, und unabhängig davon, ob der Server läuft, sind für die gesamte Größe eines virtuellen Datenträgers fünf Units pro Monat und GB zu bezahlen. Von den virtuellen Datenträgern können Snapshots erstellt werden, und diese können auch geklont werden, um mehrere identische Server zu betreiben. CPU- oder Speicherkonfiguration eines Servers können verändert werden, nicht allerdings zur Laufzeit. Netzwerktransfer kostet fünf Units pro GB.

Als Betriebssysteme stehen verschiedene *Linux*-Distributionen und *Microsoft Windows* zur Verfügung, letzteres für drei Units mehr pro Stunde. Auch die Verwendung eigener Betriebssysteme ist möglich. Zur Verwaltung der virtuellen Server steht einerseits ein Web-Service-Interface zur Verfügung, sodass diese auch automatisiert werden kann, und anderseits ein Web-Interface für den Browser.

5.3.2. Vertragsbedingungen

Bei der Erstellung eines Accounts muss der Nutzer den „Terms and Conditions“ zustimmen (siehe Abbildung 7). Dieses Dokument verweist auf die „Acceptable Use Policy“ und die „Privacy Policy“, die ebenfalls Vertragsbestandteil werden. Die Acceptable Use Policy verbietet die Verwendung von *FlexiScale* für illegale und sonstige verpönte Aktivitäten, wobei die Konsequenzen bis hin zur Kündigung des Vertrages gehen können. Terms and Conditions und Privacy Policy werden im Folgenden näher behandelt.

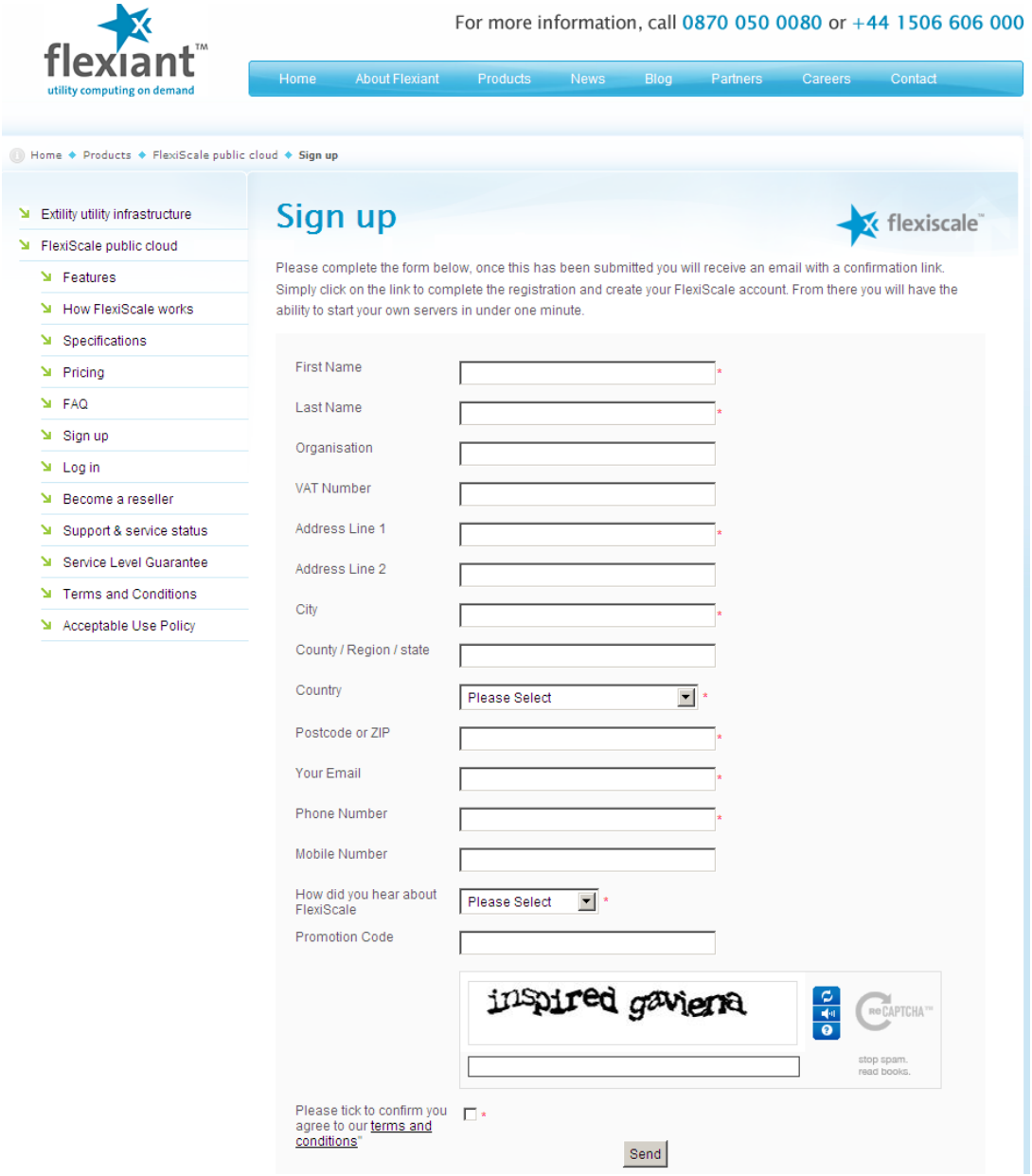


Abbildung 7 – Erstellung eines Accounts bei *FlexiScale*[399]

Wichtige Bestimmungen der FlexiScale Terms and Conditions of Business:[400]

- *Flexiant* kann die Terms and Conditions jederzeit einseitig ändern.
- 4.2.: Die angebotenen Services können von Zeit zu Zeit geändert werden.

---

399 Quelle: Screenshot von http://www.flexiant.com/products/flexiscale (erstellt am 07. September 2010).

400 Quelle: http://www.flexiant.com/products/flexiscale/terms/?__utma=1.154146841.1283871402.1283871402.1283871402.1&__utmb=1.1.10.1283871402&__utmc=1&__utmx=-&__utmz=1.1283871402.1.1.utmcsr=flexiant.com|utmccn=%28referral%29|utmcmd=referral|utmcct=/products/flexiscale/faq/&__utmv=-&__utmk=266091151 (Zugriff am 08. September 2010)

- 4.3.: Der Service kann fehlerhaft sein, und daher wird jegliche Gewährleistung der Eignung des Service für Aktivitäten, die mit hohem Risiko verbunden sind, ausgeschlossen.
- 6.14.: Wird der Account eines Nutzers drei Monate lang nicht genutzt, kann ihn *Flexiant* jederzeit löschen, wodurch damit verknüpfte „Services" – also offenbar auch Daten – gelöscht werden und alle gekauften Units verfallen.
- 9.4.: Angekündigte Wartung oder Nichtverfügbarkeit kann vorkommen, wobei der Nutzer rechtzeitig davon verständigt wird.
- 9.5.: Unangekündigte Wartung oder Nichtverfügbarkeit kann ebenfalls vorkommen, wenn dies notwendig ist.
- 13.1.2.: *Flexiant* ist nicht für Datensicherung und daher nicht für Datenverlust verantwortlich, den der Nutzer durch die Nutzung des Service bzw. durch dessen Fehler erleidet.
- 13.1.3.: Der Nutzer muss seine Daten regelmäßig sichern.
- 13.2.: Unabhängig davon muss sich der Nutzer ausreichend gegen Datenverlust versichern.
- 14.2.: Gewährleistungsausschluss. Soweit gesetzlich zulässig, übernimmt *Flexiant* keine Gewährleistung jeglicher Art, insbesondere keine Gewährleistung für die beschriebene Funktionalität und gespeicherte Daten, sowie keine Verantwortung für Service-Unterbrechungen.
- 15.1.: Haftungsbeschränkung. Soweit dies gesetzlich möglich ist (14.3), ist die Haftungssumme beider Vertragspartner auf die Summe der drei dem Ereignis vorhergehenden Monatsrechnungen des Nutzers beschränkt, beträgt jedoch mindestens 15.000 GBP. Keine Haftung besteht für entgangenen Gewinn, Folgeschäden etc.
- 17.2.: *Flexiant* kann den Vertrag jederzeit kündigen. Die Kündigungsfrist beträgt 30 Tage.
- 17.5.1.: Bei Vertragsende wird die Serviceerbringung umgehend eingestellt und der Account des Nutzers gelöscht.
- 21.11.: Rechtswahl und Gerichtszuständigkeit. Die Terms and Conditions unterliegen englischem Recht. Für Rechtsstreitigkeiten in Verbindung mit den Terms and Conditions sind ausschließlich die englischen Gerichte zuständig

Die Privacy Policy[401] enthält unter anderem Bestimmungen über die Weitergabe von Nutzerdaten. Account-Daten des Nutzers werden weitergegeben, wenn *Flexiant* Gründe hat, zu glauben, dass dies notwendig ist, um gegen den Nutzer wegen Verfehlungen

[401] Quelle: http://www.flexiant.com/about/privacy (Zugriff am 08. September 2010).

vorzugehen, oder gesetzlich gefordert ist. Kommunikationsdaten des Nutzers können insbesondere weitergegeben werden, um die Interessen von *Flexiant* oder seiner Kunden zu schützen oder wenn dies durch gerichtliche Anordnung gefordert wird. Über die Inhaltsdaten der Servicenutzung wird damit aber offenbar nichts ausgesagt.

Wichtige Bestimmungen der FlexiScale Service Level Guarantee:[402]

- *Flexiant* gibt eine 100%-Verfügbarkeitsgarantie ab.
- Ausgenommen ist die – ebenfalls garantierte – Zeitspanne von maximal 15 Minuten, nach der ein virtueller Server automatisch ohne Zutun des Nutzers spätestens wieder verfügbar ist, wenn die zugrundeliegende Hardware defekt ist („Live Recovery").
- Ausgenommen sind auch geplante Wartung, die mindestens 72 Stunden im Vorhinein angekündigt wird, sowie hacking, Viren, etc., höhere Gewalt und sonstige Fälle, deren Ursache außerhalb der Kontrolle von *Flexiant* liegt.
- Hält sich *Flexiant* nicht an diese Garantiezusagen, bekommt der Nutzer für jede halbe Stunde Nichtverfügbarkeit 5% der in den letzten 30 Tagen ausgegebenen Units gutgeschrieben, maximal jedoch 100%.

Da in den Terms and Conditions die Service Level Guarantee nicht erwähnt wird und *Flexiant* darin jede Garantie für die auf der Website gemachten Angaben ausschließt, ist streng genommen nicht klar, ob und wodurch sich *Flexiant* an die Service Level Guarantee gebunden fühlt, welche sich – leicht auffindbar – auf der Website befindet. Geht man allerdings davon aus, dass sie verbindlich ist, muss die als „Live Recovery" bezeichnete garantierte Wiederverfügbarkeit innerhalb von 15 Minuten positiv erwähnt werden. Die als Entschädigung bei Nichteinhaltung angebotenen Gutschriften werden aber auch hier in der Praxis ein nur unzureichender Ersatz sein, wenngleich sie deutlich höher ausfallen können, als bei *Amazon Web Services*.

Insgesamt ist die Rechtsposition des Nutzers auch bei *FlexiScale* als schwach zu bezeichnen. Es wird keinerlei Funktionalität garantiert, und die Haftung ist zwar nicht gänzlich ausgeschlossen, aber ebenfalls sehr beschränkt. Ob man auch einem kleineren Anbieter wie *Flexiant* zutraut, für ausreichend Sicherheit und Zuverlässigkeit zu sorgen, ohne rechtlich dazu verpflichtet zu sein, muss jeder Nutzer selbst entscheiden. Aber auch und gerade kleine Anbieter können nur überleben, wenn sie sich einen guten Ruf schaffen.

[402] Quelle: http://www.flexiant.com/products/flexiscale/slg (Zugriff am 08. September 2010).

Die Vertragsbedingungen von *FlexiScale* enthalten wie jene von *Amazon Web Services* keine Angaben über die Heranziehung von Subdienstleistern und das Löschen aller Daten des Nutzers nach Vertragsbeendigung. Die Erfüllung der Dienstleisterpflichten nach § 11 DSG 2000 wird daher nicht vollständig zugesichert. Positiv hervorzuheben ist allerdings, dass es sich um einen Anbieter aus einem Mitgliedstaat des EWR handelt.

5.4. Google App Engine

Service-Modell	*PaaS (Laufzeitumgebung)*
Service-Anbieter (für Nutzer in Österreich)	*Google Inc.* *1600 Amphitheatre Parkway* *Mountain View, CA 94043* *USA*
Service-URL	*http://code.google.com/appengine/*

Google App Engine ist einer jener Cloud-Services, die im Rahmen des in Kapitel 7 vorgestellten Testprojekts verwendet wurden. Die Zusammenfassung des Testprojekts vermittelt einen Eindruck des praktischen Einsatzes von *Google App Engine*.

5.4.1. Servicebeschreibung

Google App Engine bietet eine Java-Laufzeitumgebung sowie eine Python-Laufzeitumgebung für Webanwendungen. Die Datenspeicherung erfolgt in einer proprietären nichtrelationalen Datenbank,[403] auf die einerseits direkt auf Objekt-Basis und andererseits mittels einer SQL-ähnlichen Abfragesprache namens GQL zugegriffen werden kann. Sowohl diese Datenbank als auch die gesamte Laufzeitumgebung sind auf hohe Skalierbarkeit ausgelegt. Darüber, wo sich die Rechenzentren befinden, in denen die Anwendung des Nutzers letztlich läuft, konnten keine Angaben gefunden werden. Der Nutzer hat somit keine Kontrolle darüber, in welchem Land seine mit der Anwendung zusammenhängenden Daten gespeichert werden.

Eine eigene Entwicklungsumgebung wird nicht angeboten, jedoch ist zu Entwicklungszwecken eine lokale Laufzeitumgebung verfügbar, die *Google App Engine* emuliert. Insbesondere wegen der proprietären Lösung zur Datenspeicherung können wohl die meisten existierenden Webanwendungen nicht ohne Modifikationen auf *Google App Engine* portiert werden. Die Portierung in die entgegengesetzte Richtung – also das Betreiben von Webanwendungen, die für *Google App Engine* entwickelt wurden,

[403] Die Technologie heißt *Google BigTable*. Einen kurzen Überblick über die Funktionsweise geben Velte, Velte und Elsenpeter 2009, 147 ff.

unabhängig von *Googles* Infrastruktur – wird durch *AppScale* ermöglicht. Dies ist eine Open-Source-Implementierung von *Google App Engine*, die sich auch für den Betrieb auf Cluster- und Cloud-Infrastruktur wie etwa *AWS* eignet.[404] *AppScale* entschärft somit die Problematik des Vendor-Lock-in bei *Google App Engine*.

Google App Engine ist grundsätzlich kostenlos. Kosten entstehen erst, wenn der Nutzer die kostenpflichtige Nutzung aktiviert hat und die Intensität der Nutzung einer Anwendung bestimmte Freigrenzen überschreitet. Die Kosten betragen dann für die über die Freigrenzen hinausgehende Nutzung 0,12 USD pro GB für ausgehenden und 0,10 USD pro GB für eingehenden Datentransfer, 0,10 USD pro CPU-Stunde und 0,15 USD pro GB gespeicherte Daten. Der Nutzer hat die Möglichkeit, für die verschiedenen Posten eine Obergrenze der täglich anfallenden Kosten zu setzen. Wird diese Obergrenze erreicht, ist die Anwendung nicht mehr verfügbar und eine Fehlermeldung erscheint, wenn versucht wird, die Anwendung aufzurufen. Dies ist auch die Folge des Erreichens einer der oben erwähnten Freigrenzen, wenn die kostenpflichtige Nutzung nicht aktiviert ist. Diese Freigrenzen liegen bei 43.200.000 Aufrufen, einem GB eigehenden und einem GB ausgehenden Datentransfer und 6,5 CPU-Stunden jeweils pro Tag sowie einem GB gespeicherten Daten. Dies wird selbst für viele kommerziell betriebene Anwendungen ausreichen.

5.4.2. Vertragsbedingungen

Bei der Erstellung einer Anwendung in *Google App Engine* muss der Nutzer den „Google App Engine Terms of Service“ zustimmen (siehe Abbildung 8). Diese verweisen in Abschnitt 3 auf drei weitere Dokumente, die somit ebenfalls Vertragsinhalt werden.

[404] AppScale o.J.

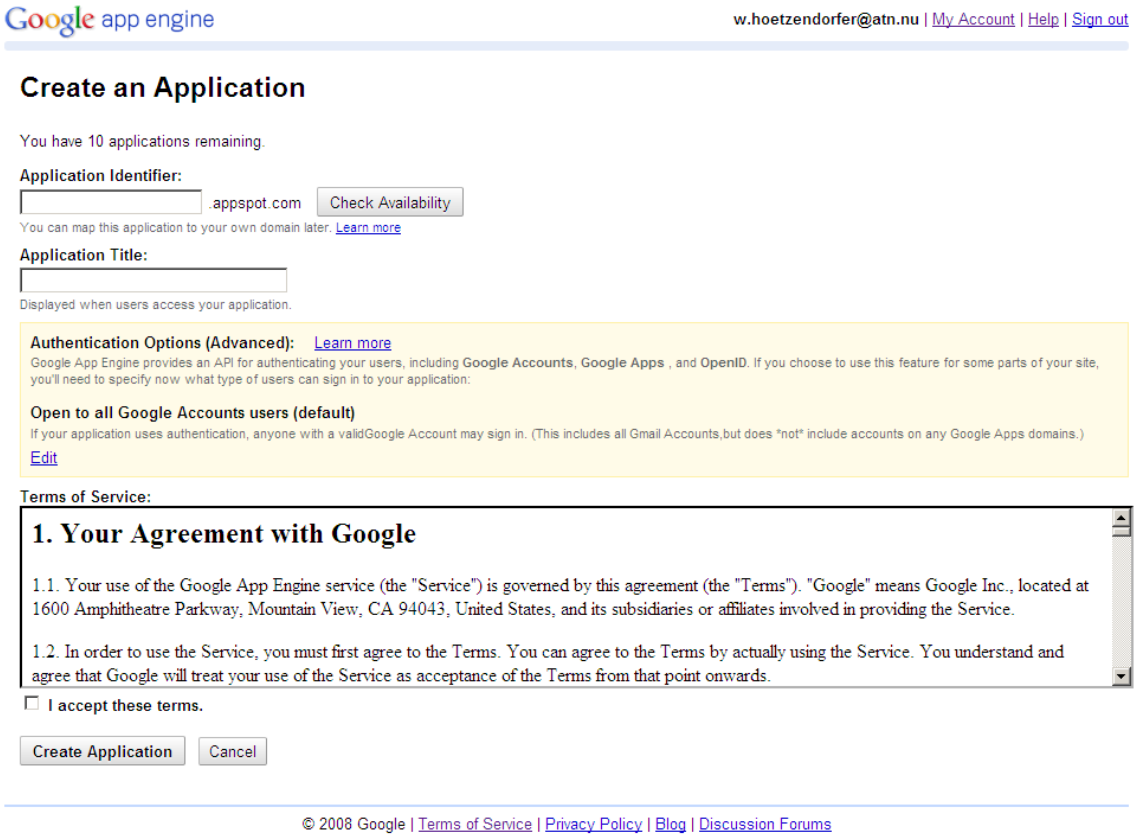


Abbildung 8 – Erstellung einer Applikation in *Google Apps*[405]

Wichtige Bestimmungen der Google App Engine Terms of Service:[406]

- 4.2.: *Google* gibt Informationen heraus, wenn dies durch gerichtliche Anordnung oder sonstige rechtliche Verfahren gefordert wird, und behält sich das Recht vor, die Serviceerbringung bei Zahlungsverspätung einzustellen.
- 4.3.: Die Freigrenzen können jederzeit geändert werden und die Preise dann, wenn dies 90 Tage vorher angekündigt wurde.
- 5.2.: *Google* behält sich die Kontrolle über die Inhalte der Anwendungen vor, einschließlich des Rechts zur Änderung oder Löschung.
- 5.3.: *Google* behält sich das Recht vor, Anwendungen bei (mutmaßlichen) Verstößen gegen die „Program Policies“[407] zu deaktivieren.
- 5.5.: *Google* übernimmt keine Verantwortung oder Haftung für Datenverluste. Der Nutzer ist für die Sicherheit der Anwendung verantwortlich.

---

[405] Quelle: Screenshot von http://code.google.com/intl/de-DE/appengine (erstellt am 16. August 2010).

[406] Quelle: http://code.google.com/intl/de-DE/appengine/terms.html (Zugriff am 02. September 2010)

[407] Beispielsweise verstößt neben illegalen Aktivitäten auch das Anbieten von Glücksspiel gegen diese Bestimmungen. Quelle: http://code.google.com/intl/de-DE/appengine/program_policies.html (Zugriff am 03. September 2010).

- 8.2.: *Google* darf Logos und Marken etc. des Kunden zu Marketingzwecken verwenden.
- 10.2.: Wenn ein Service offiziell eingestellt oder aktualisiert wird, wird *Google* wirtschaftlich sinnvolle Anstrengungen unternehmen, die bisherige Version für drei Jahre weiterhin in Betrieb zu belassen.
- 10.3.: Der Betrieb eines Service oder einer älteren Version eines Service (siehe unter 10.2) kann aber jederzeit eingestellt werden, wenn *Google* entscheidet, dass dieser zur wesentlichen wirtschaftlichen oder technischen Belastung wird.
- 10.4.: In diesem Fall oder wenn der Nutzer die Verwendung des Service einstellt oder diese von *Google* aus wichtigem Grund gekündigt wird, hat der Nutzer für 90 Tage die Möglichkeit, Daten zu exportieren.
- 11.3.: Gewährleistungsausschluss. *Google* schließt jegliche Garantie, insbesondere für Sicherheit und Zuverlässigkeit des Service aus.
- 12.1.: Haftungsausschluss. *Google* übernimmt keine Haftung für allfällige Schäden jeglicher Art, die der Nutzer erleidet, oder entgangenen Gewinn.
- 16.1.: Google kann die Vertragsbedingungen jederzeit einseitig ändern.
- 17.7.: Rechtswahl und Gerichtszuständigkeit. Das Rechtsverhältnis zwischen dem Nutzer und *Google* unterliegt dem Recht des Staates Kalifornien. Für alle daraus entstehenden Rechtsstreitigkeiten sind ausschließlich die Gerichte des County of Santa Clara, Kalifornien zuständig. *Google* behält sich allerdings vor, einstweilige Rechtsmittel auch in jeder anderen Rechtsordnung zu ergreifen.

Die Terms of Service verweisen auf die „Privacy Notice".[408] In dieser wird der Umgang mit Nutzerdaten erläutert, und sie enthält den Hinweis, dass *Google* die Safe Harbor Principles beachtet.[409]

Bei näherer Betrachtung der Vertragsbedingungen von *Google App Engine* wird deutlich, dass hier die Rechtsposition des Nutzers noch schlechter ist, als bei anderen Services, da es für *Google App Engine* kein SLA gibt, bzw. konnte im Zuge der Recherchen kein solches gefunden werden. Jedoch ergaben die Recherchen, dass *Google* ein Angebot namens *App Engine for Business* plant, das – neben neuen Features wie beispielsweise SQL-Datenbank-Support – auch ein SLA bietet, dessen Entwurf bereits verfügbar

[408] Quelle: http://code.google.com/intl/de-DE/appengine/privacy.html (Zugriff am 03. September 2010).
[409] Zum Safe-Harbor-Programm siehe Punkt 3.2.5, S. 56.

ist.[410] Die Grundprinzipien dieses SLA-Entwurfs – Verfügbarkeitszusage 99,9% auf Basis von Server-Anfragen, Gutschrift in Höhe eines (gestuften) Prozentanteils der Monatsrechnung – ähneln jenen des *Amazon-S3*-SLA. Bis *App Engine for Business* verfügbar ist, oder für Nutzer, die dieses aus Gründen, die möglicherweise jetzt noch nicht absehbar sind, nicht verwenden möchten, lautet die Conclusio auch im Fall der *Google App Engine*, dass sie sich auf das Bemühen des Anbieters verlassen und diesem Vertrauen müssen. Eine vertragliche Verpflichtung, Sicherheit und Zuverlässigkeit zu gewährleisten, besteht für *Google* nicht.

Hinsichtlich des Datenschutzrechts ist zu sagen, dass auch die Vertragsbedingungen von *Google App Engine* keine vollständige Zusicherung der Erfüllung der Dienstleisterpflichten nach § 11 DSG 2000 enthalten. Insbesondere fehlen Angaben über das Heranziehen von Subdienstleistern und das Löschen der Nutzerdaten nach Vertragsbeendigung.

5.5. Microsoft Windows Azure

Service-Modell	*PaaS, (IaaS)*
Service-Anbieter (für Nutzer in Österreich)	*Microsoft Ireland Operations Limited* *70 Sir John Rogerson's Quay* *Dublin 2* *Irland*
Service-URL	*http://www.microsoft.com/windowsazure*

5.5.1. Servicebeschreibung

Die beiden wesentlichen Bestandteile der *Microsoft Windows Azure Platform* sind *Windows Azure* und *SQL Azure*. *Windows Azure* ist eine Laufzeitumgebung, die primär für *Microsoft .Net*-Webanwendungen konzipiert ist. Diese Webanwendungen sind in Komponenten, so genannten „Web Roles", organisiert. Für Hintergrunddienste von Webanwendungen und für andere Anwendungen existiert das Konzept der „Worker Roles". Eine vom Nutzer erstellte Anwendung kann sich aus mehreren Web Roles und Worker Roles zusammensetzen. Von diesen Web Roles und Worker Roles können wiederum beliebig viele Instanzen gestartet werden, denen jeweils ein virtueller Server zugrunde liegt. Diese virtuellen Server basieren auf dem Betriebssystem *Microsoft Windows Server 2008 SP2* und sind hinsichtlich Größenklassen und Verrechnung mit

[410] Siehe unter http://code.google.com/intl/de-DE/appengine/business/sla.html (Zugriff am 03. September 2010).

jenen von IaaS-Angeboten zu vergleichen, mit dem wesentlichen Unterschied, dass der Nutzer darüber keine volle Kontrolle im Sinne eines Administratorzugriffs besitzt.[411]

Zur Datenspeicherung aus den Anwendungen wird einerseits ein Service für Binärdateien und andererseits ein Service für strukturierte Daten auf Tabellenbasis angeboten, auf die jeweils auch per HTTP zugegriffen werden kann. Als relationale Datenbank steht – als wesentlicher Bestandteil der gesamten Plattform – *SQL Azure* zur Verfügung. Dies ist im Wesentlichen eine Implementierung des *Microsoft SQL Servers*, die als Cloud-Service betrieben wird. Hinzu kommt *AppFabric*, ein Cloud-Service, das einerseits Service-Bus- und andererseits Zugriffskontrollfunktionalität zur Verfügung stellt. Zur Entwicklung von Anwendungen für *Windows Azure* besteht eine komfortable Integration in die Entwicklungsumgebung *Microsoft Visual Studio*, die auch das Deployment und die Verwaltung der Anwendungen unterstützt. Eine Stärke der *Windows Azure Platform* ist, dass Anwendungen, die für lokalen oder herkömmlich gehosteten Betrieb entwickelt wurden, ohne Änderungen in *Windows Azure* betrieben werden können, sofern sie neben der SQL-Datenbank keine persistente Datenspeicherung beinhalten.[412]

Die Abrechnung erfolgt grundsätzlich nach benutzten Ressourcen, ähnlich wie bei den bisher besprochenen Services. Die kleinste von vier verfügbaren Serverinstanzen kostet 0,0852 EUR, die größte 0,6809 EUR pro Stunde. Auch die Tarife für Datenspeicherung und Datenübertragung sind mit jenen von *Amazon Web Services* vergleichbar. *SQL-Azure*-Datenbanken sind in zwei Ausführungen und insgesamt sieben Größenklassen erhältlich. Sie kosten zwischen 7,085 EUR (ein GB) und 354,565 EUR (50 GB) pro Monat. Neben der nutzungsabhängigen Verrechnung besteht die Möglichkeit, Ressourcen in Paketen für die monatliche Nutzung in verschiedenem Umfang, zum Teil inkl. *SQL-Azure*-Datenbank zu abonnieren. Die Verträge über diese Pakete haben eine Laufzeit von mindestens sechs Monaten. Vorausgesetzt man braucht die im Paket erworbenen Ressourcen jeden Monat auf, ergibt sich eine Ersparnis gegenüber der rein nutzungsabhängigen Verrechnung. Für die über die erworbenen Paket-Ressourcen hinausgehende Nutzung innerhalb eines Monats gelten die oben beschriebenen nutzungsabhängigen Tarife. Derzeit (September 2009) bietet *Microsoft* als Einstiegsangebot ein solches Ressourcen-Paket kostenlos an.

[411] Wolf 2010.
[412] Wolf 2010.

5.5.2. Vertragsbedingungen

Die Nutzung der Produktivversionen von *Microsoft Windows Azure* erfordert zunächst eine Anmeldung bei *Microsoft Online Services*, die grundsätzlich nur Unternehmen möglich ist. Wie in Abbildung 9 ersichtlich, können dann die verschiedenen Paketvarianten der *Windows Azure Platform* bestellt werden. Zu diesem Zweck werden sie zunächst in den Einkaufswagen (Abbildung 10) gelegt. Dort kann mit dem Link „Vertrag anzeigen“ der „Online-Abonnement-Vertrag“ aufgerufen werden, welcher der Benützung zugrunde liegt.

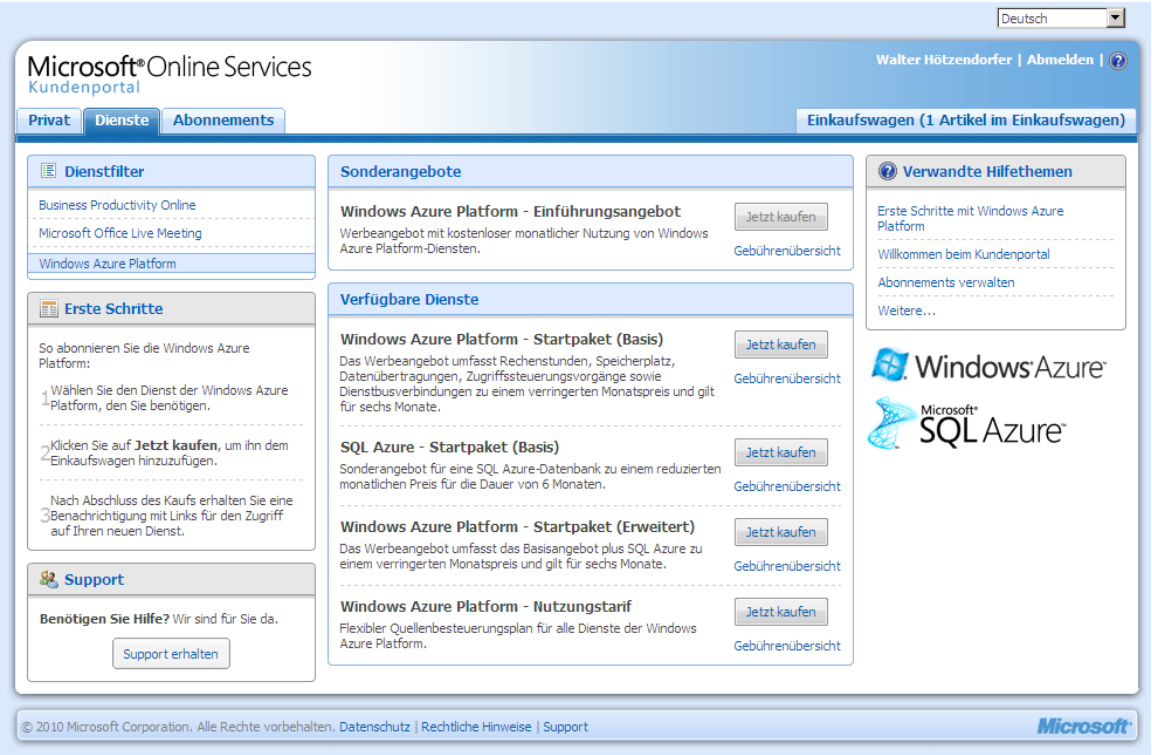


Abbildung 9 – Verfügbare Varianten der *Windows Azure Platform* und *SQL Azure*[413]

[413] Quelle: Screenshot von https://mocp.microsoftonline.com (erstellt am 23. September 2010).

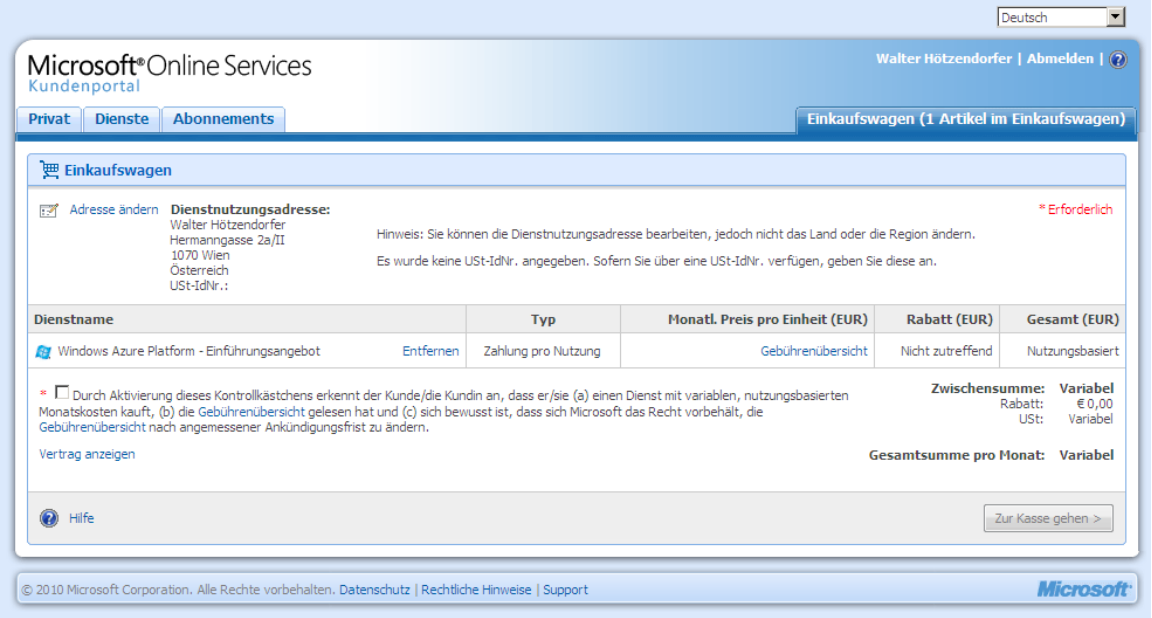


Abbildung 10 – Einkaufswagen mit *Windows-Azure*-Paket und Link zum zugrundeliegenden Vertrag[414]

Wichtige Bestimmungen des Online-Abonnement-Vertrags:[415]

- 3.d.: *Microsoft* kann den Vertrag jederzeit ändern, für abonnierte Pakete gilt ein geänderter Vertrag aber nur ab Verlängerung/Neubestellung.
- 4.: Mit Ausnahme von Vertragsbindungen besteht eine Kündigungsfrist von 30 Tagen.
- 6.a.: Gewährleistung. *Microsoft* gewährleistet, dass die Funktionalität „im Wesentlichen" den Beschreibungen entspricht. Davon ausgenommen sind Probleme, die durch Ereignisse außerhalb des Einflussbereichs von *Microsoft* verursacht werden, und Ausfallzeiten, die in einem SLA geregelt sind.
- 6.b.: Bei Nichterfüllung der Gewährleistung kann *Microsoft* entweder den Fehler beheben oder der Nutzer erhält den für die Vertragslaufzeit bzw. maximal zwölf Monate bezahlten Betrag zurück. Darüber hinausgehende Ansprüche sind ausgeschlossen.
- 6.c.: Soweit gesetzlich zulässig, sind alle anderen Gewährleistungsansprüche und Garantien ausgeschlossen.
- 8.b.: Haftungsbeschränkung. Die Haftung von *Microsoft* ist auf die vom Nutzer für die Vertragslaufzeit bzw. maximal zwölf Monate bezahlte Summe beschränkt. Für indirekte Schäden wird – ausgenommen bzgl. Vertraulichkeitsverpflichtungen – jede Haftung ausgeschlossen.

414 Quelle: Screenshot von https://mocp.microsoftonline.com (erstellt am 23. September 2010).
415 Quelle: https://mocp.microsoftonline.com/Site/Mocp_Eagreement.aspx?country=AUT&lang=de (Zugriff am 23. September 2010).

- 10.e.: Rechtswahl. Der Vertrag unterliegt irischem Recht.
- 10.f.: Gerichtszuständigkeit. Klagen gegen *Microsoft* sind in Irland zu erheben. (Klagen gegen den Kunden würde *Microsoft* am Gerichtsstand von dessen Hauptsitz einbringen.)

Wichtige Bestimmungen der Microsoft Windows Azure Platform-Datenschutzerklärung:[416]

- *Microsoft* behält sich die Heranziehung von Subdienstleistern vor.
- Die Daten des Nutzers können in den USA oder in anderen Ländern gespeichert und verarbeitet werden.
- *Microsoft* hält sich an die Safe-Harbor-Bestimmungen.[417]
- *Microsoft* kann die Datenschutzbestimmungen jederzeit einseitig ändern.

Es gelten jeweils eigene SLA für die Services *Windows Azure*[418], *SQL Azure*[419] und *AppFabric*[420]. Diese werden aus Platzgründen hier nicht im Detail beschrieben, zumal sie jenen von *Amazon Web Services* sehr ähnlich sind. Dies betrifft die Berechnung der prozentualen Nichtverfügbarkeit mittels Zeitintervallen, den Ausschluss geplanter, vorangekündigter Nichtverfügbarkeit und die Vergütung in Form einer Gutschrift (maximal 25% der Monatsrechnung).

In einzelnen Punkten sind die Vertragsbedingungen von *Microsoft Windows Azure* nutzerfreundlicher als jene anderer Cloud-Services. Der Schluss liegt nahe, dass den (deutschsprachigen) Vertragsbedingungen die umfassende und bereits lange zurückreichende Marktpräsenz von *Microsoft* im kontinentaleuropäischen Rechtskreis anzumerken ist. Letztlich verhindern allerdings die Beschränkung der Gewährleistung und Haftung und die Ausgestaltung der SLA wie bei den anderen untersuchten Cloud-Services, dass der Nutzer im Fall des Verlustes unternehmenskritischer Daten oder des Ausfalles unternehmenskritischer Anwendungen angemessen entschädigt wird. Der

---

416 Quelle: http://www.microsoft.com/online/legal/?langid=de-de&docid=1 (Zugriff am 23. September 2010).
417 Zum Safe-Harbor-Programm siehe Punkt 3.2.5, S. 56.
418 Quelle: http://download.microsoft.com/download/0/E/E/0EE244BF-22CA-4180-ACF0-F2F40CAEE3D6/Windows%20Azure%20Compute%20SLA-German.doc (Zugriff am 23. September 2010).
419 Quelle: http://download.microsoft.com/download/B/0/9/B09851E2-6177-4A62-83AB-3B591659CE1E/SQL%20Azure%20SLA-German.doc (Zugriff am 23. September 2010).
420 Quelle: http://download.microsoft.com/download/7/5/C/75CFE293-88FD-43EC-B5C7-3F418078AC89/Windows%20Azure%20platform%20AppFabric%20Access%20Control%20SLA-German.docx (Zugriff am 23. September 2010).

Einsatz solcher Anwendungen bzw. Daten setzt daher auch im Zusammenhang mit der *Windows Azure Platform* das Vertrauen in das Bemühen des Anbieters voraus.

Im Hinblick auf das Datenschutzrecht ist zunächst zu betonen, dass (gegenüber österreichischen Nutzern) mit der irischen Tochtergesellschaft von *Microsoft* – wie im Falle von *FlexiScale* – ein Unternehmen aus dem EWR als Anbieter auftritt. Allerdings behält sich *Microsoft* vor, die Daten in beliebigen Staaten zu speichern und Subdienstleister heranzuziehen. Die Einhaltung der Dienstleisterpflichten nach § 11 DSG 2000 wird in den Vertragsbedingungen somit nicht vollständig zugesagt.

5.6. Salesforce CRM

Service-Modell	*SaaS, PaaS*
Service-Anbieter (für Nutzer in Österreich)	*salesforce.com Sàrl,* *Rue St-Louis 2* *Morges, 1110* *Schweiz*
Service-URL	*https://www.salesforce.com*

5.6.1. Servicebeschreibung

Salesforce ist ein umfangreiches SaaS-Angebot rund um Customer-Relationship-Management (CRM). Die beiden wichtigsten Anwendungen sind die Vertriebssoftware *Sales Cloud* und die Kundenservicesoftware *Service Cloud*. Zu den Features von *Sales Cloud* gehören eine Kundendatenbank, die mit der mit den einzelnen Kunden bisher geführten Kommunikation verknüpft ist, eine Lead-Verwaltung, die unter anderem Schnittstellen zum Keyword-Advertising-Service *Google AdWords* und zum Mikroblogging-Service *Twitter* bietet, eine direkte Verknüpfung von Materialien wie etwa Präsentationsfolien und ein umfassendes Berichtswesen. *Sales Cloud* besitzt darüber hinaus Schnittstellen zu *Microsoft Outlook*, *Lotus Notes* und *Google Apps*[421], sodass Termine, Aufgaben und E-Mail-Verkehr direkt aus *Sales Cloud* verwaltet werden können. Auch mittels mobiler Endgeräte – unterstützt werden *iPhone*, *BlackBerry* und *Windows Mobile* – kann auf *Sales Cloud* zugegriffen werden.

[421] Siehe dazu Abschnitt 5.7, S.111.

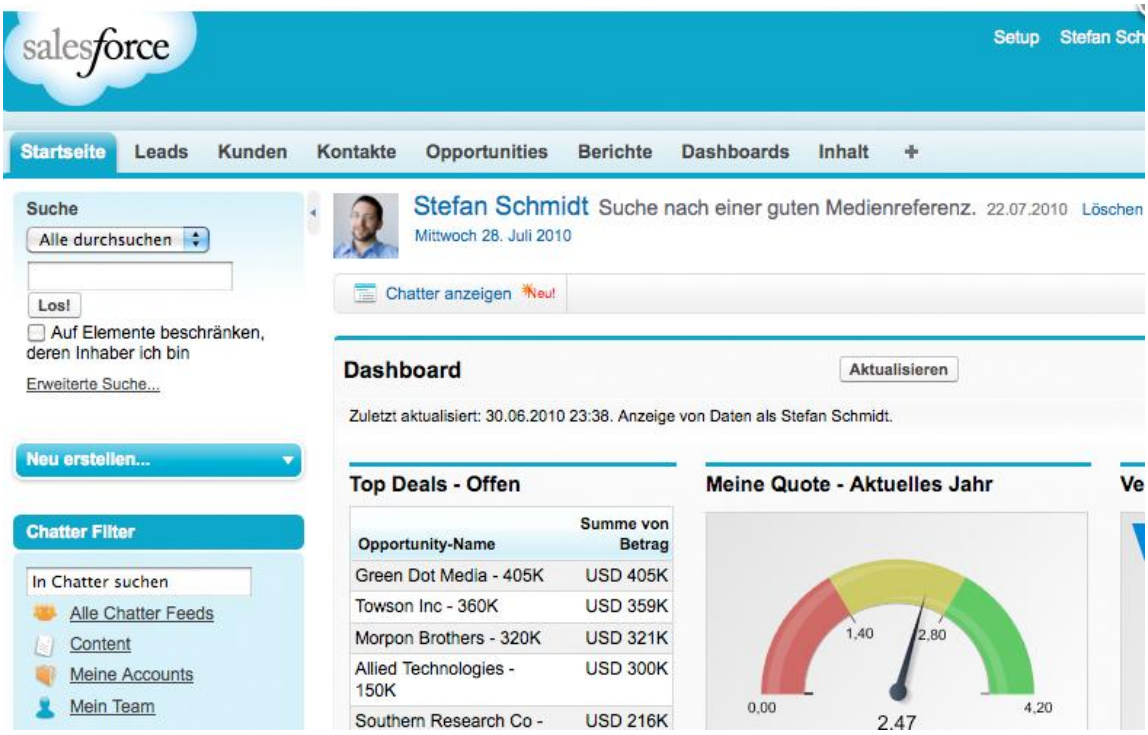


Abbildung 11 – Startseite von *Salesforce Sales Cloud*[422]

Zum Teil ähnliche Funktionen wie *Sales Cloud* bietet *Service Cloud* im Kontext des Kundenservice. Auch hier steht eine Vielzahl von Schnittstellen zur Verfügung. Kundenanfragen, die über diverse Kanäle eintreffen können, werden direkt mit der Kundendatenbank verknüpft, sowie mit relevanten, den jeweiligen Kunden und dessen Produkte betreffenden Informationen. Auf diese Weise können etwa vorhandene Anleitungen zur Behandlung der jeweiligen Kundenanfrage rasch gefunden werden. *Sales Cloud* kann auch in die Website des Nutzers integriert werden, sodass dessen Kunden unter anderem auf solche Anleitungen zur Problemlösung und sonstige Produktdokumentation auch selbständig zugreifen können.

In *Sales Cloud* und *Service Cloud* integriert ist die Anwendung *Chatter*. Diese dient der team- bzw. unternehmensinternen Kommunikation. Bezüglich Erscheinungsbild und Funktionalität von *Chatter* drängt sich der Vergleich mit der populären Social-Networking-Plattform *Facebook* auf. Diese „Social-Networking-Funktionalität" ist mit den einzelnen Bereichen von *Sales Cloud* und *Service Cloud* sinnvoll verknüpft, sodass etwa Kommentare oder Nachrichtenaustausch direkt auf einen Kunden bezogen werden können und diese dann auf der Übersichtsseite zu diesem Kunden sichtbar sind.

Die Abrechnung erfolgt jeweils auf Basis einer monatlichen Gebühr pro Benutzer. *Sales Cloud* gibt es in fünf Varianten, von einer einfachen Version zur Kontaktverwal-

[422] Quelle: Screenshot einer interaktiven Demo auf http://www.salesforce.com/de/crm/salesforce-automation (erstellt am 04. September 2010).

tung für vier EUR bis zur Version „Unlimited“ für 270 EUR, jeweils pro Benutzer und Monat. *Sales Cloud* ist in drei Varianten erhältlich, deren monatliche Kosten zwischen 70 und 285 EUR pro Benutzer liegen. *Chatter* kostet 15 EUR pro Benutzer und Monat.

Neben dem SaaS-Angebot betreibt *Salesforce* auch das PaaS- Angebot *Force.com*, das hier nur kurz erwähnt werden soll. Es handelt sich dabei um eine Entwicklungsumgebung mit einer eigenen Programmiersprache namens Apex und Funktionen zum vereinfachten Entwerfen von Datenbanken, Geschäftslogik, Workflows und Benutzeroberflächen sowie um eine Laufzeitumgebung für die erstellen (Geschäfts-)Anwendungen.

In diesem Zusammenhang ebenfalls zu erwähnen ist *AppExchange*, der von *Salesforce* betriebene Online-Marktplatz für Software von Drittherstellern zur Erweiterung des eigenen SaaS-Angebots von *Salesforce*. Diese Software wird in der Regel ebenfalls gegen eine monatliche Gebühr, zum Teil aber auch kostenlos angeboten. Damit schließt sich der Kreis zur Servicebeschreibung des SaaS-Angebots wieder, denn die Möglichkeit zur Erweiterung von dessen Funktionalität mittels Software von *AppExchange* zählt zu dessen bedeutendsten Stärken.

5.6.2. Vertragsbedingungen

Für den Einstieg in *Sales Cloud* und/oder *Service Cloud* bietet *Salesforce* eine kostenlose Testversion an, die je nach gewählter Variante nach sieben bis 30 Tagen automatisch ausläuft, sofern sich der Nutzer nicht in der Zwischenzeit für die – kostenpflichtige – reguläre Nutzung entscheidet. Bei der Anmeldung muss der Nutzer dem „Master Subscription Agreement“ zustimmen, das sowohl für die kostenlose Testversion als auch für die kostenpflichtigen Varianten gilt.

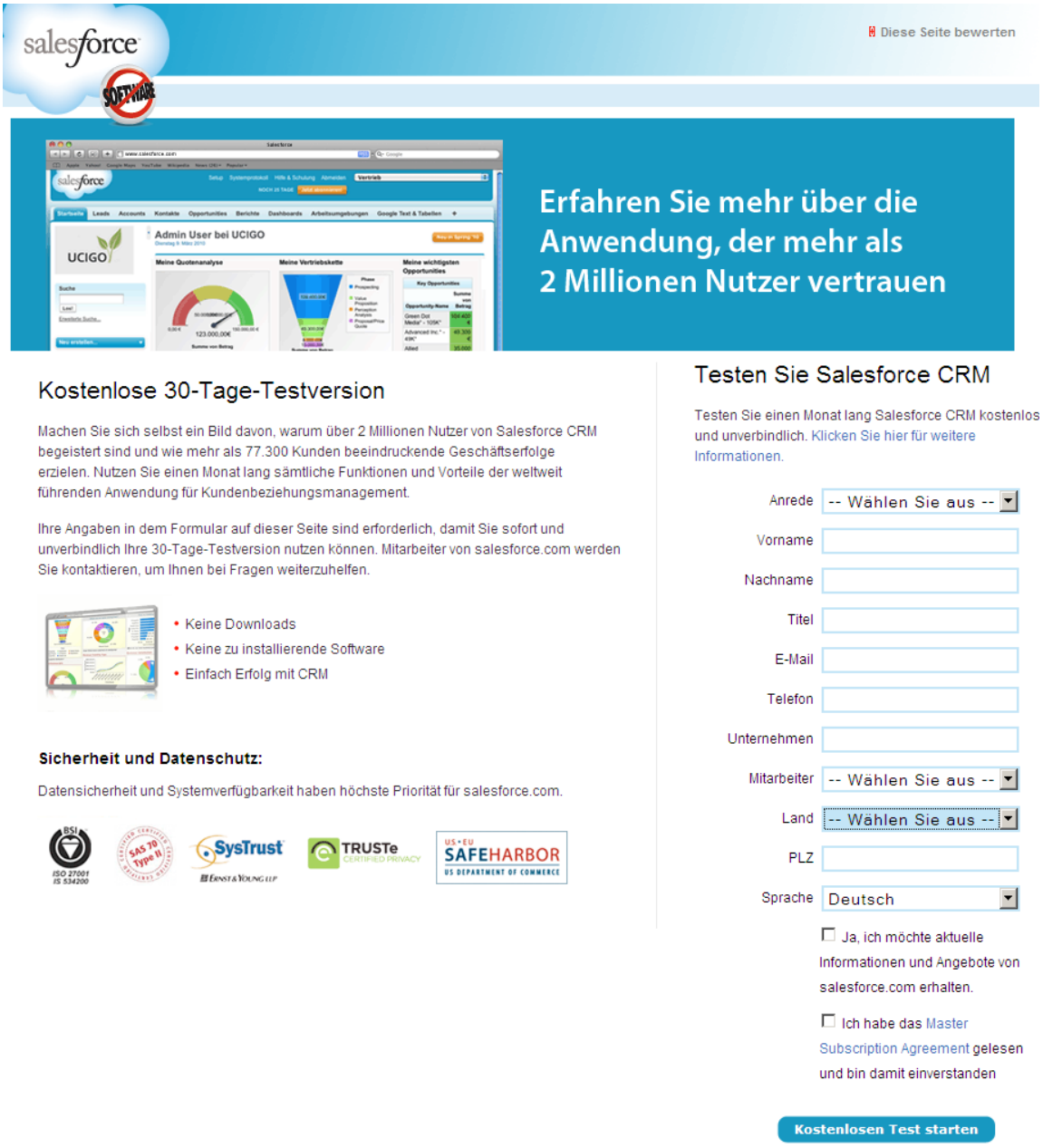


Abbildung 12 – Anmeldung zu *Salesforce Sales Cloud*[423]

Wichtige Bestimmungen des Master Subscription Agreements:[424]

- 4.1.: *Salesforce* sichert kostenlosen grundlegenden Support zu, sowie wirtschaftlich sinnvolle Anstrengungen, um permanente Verfügbarkeit des Service zu gewährleisten. Davon ausgenommen ist geplante Nichtverfügbarkeit, die soweit möglich nur am Wochenende vorkommt und mindestens acht Stunden vorher angekündigt wird, und Nichtverfügbarkeit, deren Ursache außerhalb der Kontrolle von *Salesforce* liegt.

[423] Quelle: Screenshot von https://www.salesforce.com/de (erstellt am 04. September 2010).
[424] Quelle: http://www.salesforce.com/company/msa.jsp (Zugriff am 03. September 2010).

- 5.2.: Installiert der Nutzer eine Anwendung eines Drittherstellers, erhält dieser Zugriff auf die Daten des Nutzers, soweit dies zur Zusammenarbeit der Anwendungen erforderlich ist.
- 8.2.: Nur jene Mitarbeiter und Vertragspartner von *Salesforce* haben Zugriff auf Nutzerdaten, die Geheimhaltungsvereinbarungen unterschrieben haben und bei denen dies für Zwecke erforderlich ist, die mit dem Master Service Agreement vereinbar sind. (Dies schließt die Datenweitergabe an andere Unternehmen ohne Zustimmung des Nutzers wohl nicht aus, sofern diese Unternehmen als Subdienstleister tätig sind.)
- 8.3.: *Salesforce* setzt angemessene Datenschutz- und Datensicherheitsmaßnahmen.
- 8.4.: *Salesforce* gibt Nutzerdaten heraus, wenn es dazu gesetzlich verpflichtet ist.
- 9.1.: *Salesforce* garantiert die Funktionalität der Services entsprechend dem Benutzerhandbuch. Konsequenz eines Verstoßes durch *Salesforce* ist aber ausschließlich ein außerordentliches Kündigungsrecht des Nutzers nach Punkt 12.3.
- 9.3.: Alle darüber hinausgehenden Garantien werden ausgeschlossen.
- 11.1.: Einschränkung der gesamten Haftungssumme auf die Summe aller durch den Nutzer jemals bezahlten Gebühren und der Haftungssumme für ein einzelnes Ereignis auf die Summe aller durch den Nutzer in den diesem vorhergehenden zwölf Monaten bezahlten Gebühren (absolute Höchstgrenze 500.000 USD). Dies gilt jeweils für beide Vertragsparteien.
- 11.2.: Ausschluss der Haftung für Folgeschäden und entgangenen Gewinn.
- 12.2.: Der Vertrag verlängert sich automatisch um die Dauer der bisherigen Vertragslaufzeit, maximal jedoch ein Jahr, wenn nicht eine Partei mindestens 30 Tage vor Ende der Vertragslaufzeit kündigt. Allfällige Preiserhöhungen, die *Salesforce* vor Ablauf dieser Frist bekannt gibt, werden bei Vertragsverlängerung wirksam, wobei der bisherige Preis um maximal 7% erhöht werden darf.
- 12.5.: Der Nutzer kann seine Daten innerhalb eines Zeitraums von 30 Tagen nach Vertragsende in Form einer csv-Datei bzw. in ihrem ursprünglichen Dateiformat herunterladen. Danach löscht *Salesforce* die Daten. Dies ist nicht als bloßes Recht zur Löschung formuliert, sondern offenbar als Verpflichtung dies zu tun.
- 13.1.: Für Nutzer aus europäischen Ländern wird der Vertrag mit der *Salesforce*-Tochtergesellschaft *salesforce.com Sàrl*, einer GmbH nach schweizerischem Recht mit Sitz in der Schweiz, geschlossen. Es gilt schweizerisches Recht und schweizerische Gerichtsbarkeit.

Punkt 12.2 des Master Subscription Agreements deutet darauf hin, dass der Nutzer eine bestimmte Mindestvertragsdauer eingehen muss, sobald er sich für eine kostenpflichtige Variante entscheidet.[425] Dies scheint zwar auf den ersten Blick die für Cloud Computing typische Flexibilität zu beschränken, wird jedoch relativiert durch die kostenlose Testmöglichkeit am Beginn sowie durch die Tatsache, dass der Wechsel der CRM-Lösung eins Unternehmens ohnehin ein seltenes und langfristig geplantes Ereignis sein sollte. In der Datenschutzerklärung[426] findet sich der Hinweis, dass *Salesforce* die Safe-Harbor-Richtlinien einhält.[427]

Die vertraglichen Verpflichtungen, die sich *Salesforce* auferlegt, sind gering, die Rechtsposition des Nutzers daher auch hier entsprechend schwach. Die Garantie der beschriebenen Funktionalität wird dadurch abgeschwächt, dass dem Nutzer als Sanktion lediglich die Kündigung des Vertrages zur Verfügung steht. Allerdings schließt *Salesforce* nicht jegliche Haftung aus, sondern legt nur eine Haftungsobergrenze festlegt. In diesem Rahmen richtet sich die Haftung somit nach dem Gesetz, für österreichische Nutzer daher nach schweizerischem Recht. Diese Konstruktion der Wahl schweizerischen Rechts und schweizerischer Gerichtszuständigkeit sowie einer eigenen europäische Tochtergesellschaft für europäische Nutzer, ist generell beachtenswert. Allerdings wurde mit der Schweiz ein Staat ausgewählt, welcher nicht dem EWR angehört. Vollständige und aktuelle Angaben über die Standorte der Rechenzentren von *Salesforce* konnten nicht gefunden werden. Nichts deutet daher darauf hin, dass der Nutzer den Ort der Datenspeicherung beeinflussen kann, insbesondere um diesen auf Europa zu beschränken.

Salesforce ist nach eigenen Angaben nach SAS 70 und ISO 27001 zertifiziert. Wie in Abschnitt 3.4 (S. 65) erläutert, spricht dies zwar für die Professionalität des Anbieters, ist aber keinerlei Garantie für die Sicherheit und Zuverlässigkeit des Service. Insbesondere sollte berücksichtigt werden, dass die ISO-27001-Zertifizierung zwar die Existenz eines angemessenen Informationssicherheits-Managementsystems bescheinigt, die von *Salesforce* vertraglich zugesicherte Haftung allerdings sehr gering ausfällt.

Bezüglich des Datenschutzes ist zu erwähnen, dass sich *Salesforce* zwar offenbar[428] zum Löschen der Nutzerdaten nach Vertragsende verpflichtet, allerdings die Heranziehung von Subdienstleitern nicht beschränkt, sodass die Vertragsbedingungen

[425] Diese liegt wohl zwischen einem Monat und einem Jahr. Näheres konnte im Zuge der Recherchen nicht ermittelt werden.
[426] Quelle: https://www.salesforce.com/de/company/updated_privacy.jsp (Zugriff am 23. September 2010).
[427] Zum Safe-Harbor-Programm siehe Punkt 3.2.5, S. 56.
[428] Siehe dazu Punkt 12.5 des Master Subscription Agreements.

nicht als vollständige Zusage der Erfüllung der Dienstleisterpflichten nach § 11 DSG 2000 gelten können.

5.7. Google Apps

Service-Modell	*SaaS*
Service-Anbieter (für Nutzer in Österreich)	*Google Ireland Limited* *Gordon House* *Barrowe Street* *Dublin 4* *Irland*
Service-URL	*http://www.google.com/apps*

5.7.1. Servicebeschreibung

Google Apps ist ein SaaS-Angebot, das im Wesentlichen die Funktionen eines Office-Pakets bietet. Kern des Angebots sind einerseits *Google Mail* und *Google Kalender* und andererseits *Google Text & Tabellen*[429]. Letzteres umfasst einfache Programme zur Textverarbeitung und Tabellenkalkulation sowie zum Erstellen von Präsentationen, Web-Formularen und Zeichnungen (siehe Abbildung 13). Zu *Google Apps* gehören zudem *Google Groups* – zur Gruppenkommunikation und Freigabe von Inhalten –, *Google Sites* – zur einfachen Erstellung von Intranet-Websites – und *Google Video* – zum unternehmensinternen Streaming von Videos. Diese Aufzählung illustriert bereits, dass ein Schwerpunkt von *Google Apps* auf der Online-Zusammenarbeit liegt. Dies zeigt sich auch in den Funktionen von *Text & Tabellen*: Dokumente können für andere Benutzer freigegeben und von bis zu 50 Benutzern gleichzeitig bearbeitet oder bei Bedarf im Web öffentlich gemacht werden.

[429] *Google Text & Tabellen* heißt in der englischen Version *Google Docs*.

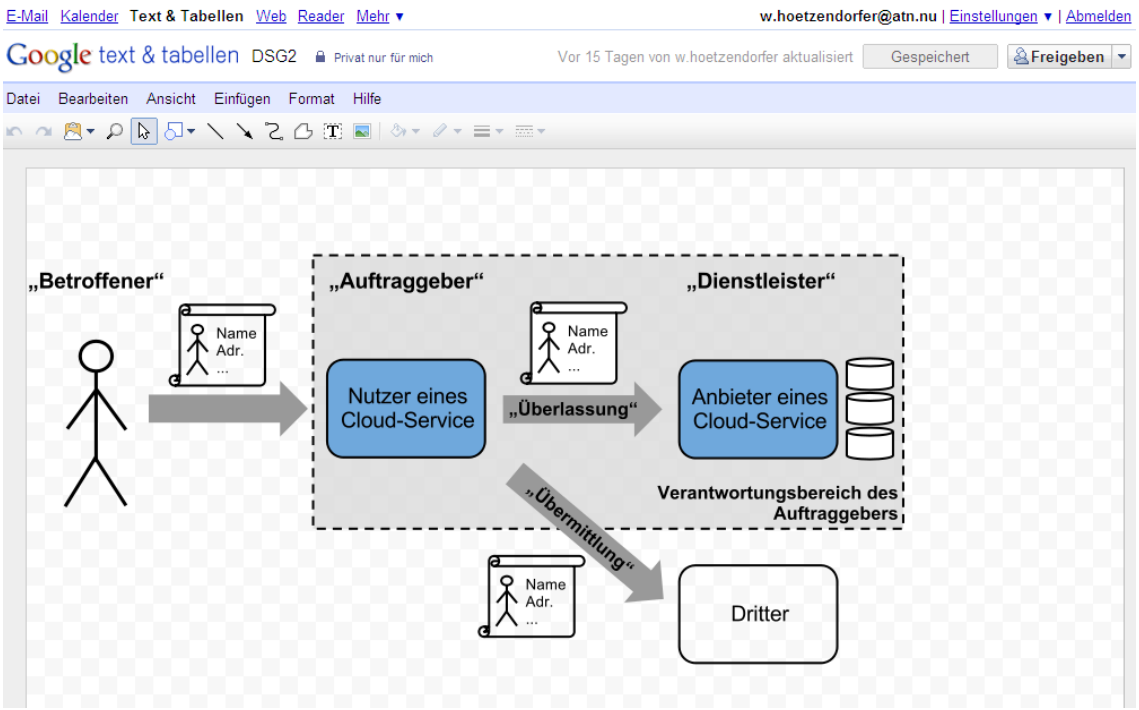


Abbildung 13 – Erstellung einer Abbildung für die vorliegende Diplomarbeit in *Google Text & Tabellen*[430]

Google Apps wird in zwei Varianten angeboten: *Google Apps Standard Edition* ist kostenlos, *Google Apps Premier Edition* kostet 40 EUR pro Nutzer und Jahr (siehe Abbildung 14) und bietet erweiterten Funktionsumfang und Service. Dazu zählen mobiler Zugriff auf E-Mails und Kalender für alle gängigen mobilen Plattformen, Kompatibilität mit *Microsoft Outlook* und Synchronisation mit dem *BlackBerry Enterprise Server*, erweiterte Sicherheitsfunktionen, Support rund um die Uhr und ein SLA mit 99,9%-Verfügbarkeitsgarantie. Zudem kann die *Premier Edition* durch eine Reihe von professionellen Funktionen in die IT-Infrastruktur eines Unternehmens eingebunden werden. Nachfolgend werden die Vertragsbedingungen der *Premier Edition* untersucht.

[430] Quelle: Screenshot von http://docs.google.com (erstellt am 08. September 2010).

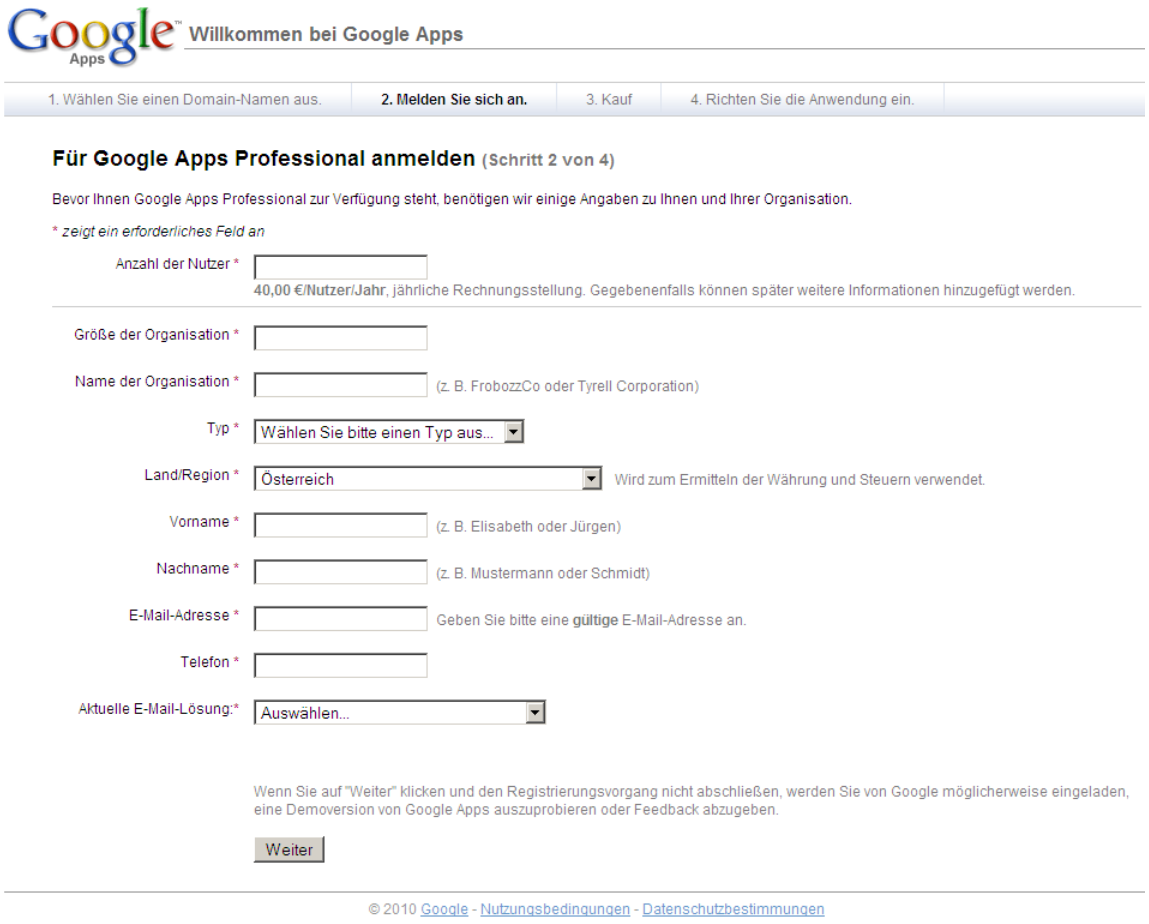


Abbildung 14 – Anmeldung für *Google Apps Premier Edition*[431]

5.7.2. Vertragsbedingungen

Wichtige Bestimmungen der Google Apps Professional-Vereinbarung:[432]

- 2.8.: Von *Google* erfasste Informationen können in den USA oder in beliebigen anderen Ländern gespeichert werden.
- 8.1.3.: *Google* legt vertrauliche Informationen offen, wenn dies gesetzlich vorgeschrieben ist.
- 9.3.: Es ist nicht erlaubt, den Service für risikoreiche Tätigkeiten (13.4.) zu nutzen.
- 13.1.: Gewährleistungsausschluss. *Google* schließt jegliche Gewährleistung im gesetzlich zulässigen Rahmen aus.
- 13.2.: Garantieausschluss. *Google* schließt jegliche Garantie aus, insbesondere die Garantie für fehlerfreien und ununterbrochenen Betrieb der Services.

---

[431] Quelle: Screenshot von https://www.google.com/a/cpanel/premier/new?hl=de (erstellt am 08. September 2010).

[432] Quelle: http://www.google.com/apps/intl/de/terms/premier_terms_ie.html (Zugriff am 08. September 2010)

- 15.1.4.: Im Hinblick auf vertrauliche Informationen wird die Haftung weder beschränkt noch ausgeschlossen.
- 15.3.: Haftungsausschluss für wirtschaftliche Schäden und sonstige Folgeschäden.
- 15.4.: *Google* beschränkt seine Haftungssumme auf 400 EUR.
- 16.1.: Der Vertrag gilt für den Zeitraum von einem Jahr und kann vom Nutzer um ein weiteres Jahr verlängert werden (16.2.). Wird der Vertrag nicht verlängert, wird der Service auf die (kostenlose) *Google Apps Standard Edition* zurückgestuft.
- 16.3.: *Google* darf den Vertrag jederzeit kündigen. Die Kündigungsfrist beträgt sechs Monate.
- 16.7.: *Google* behält sich das Recht vor, die Services jederzeit nach Benachrichtigung innerhalb angemessener Frist zu ändern, auszusetzen oder einzustellen.
- 17.1.: *Google* verpflichtet sich zur Einhaltung aller „anwendbaren" Datenschutzbestimmungen, einschließlich der europäischen Datenschutzrichtlinie und zur Implementierung aller erforderlichen Maßnahmen zur Gewährleistung von Sicherheit und Vertraulichkeit persönlicher Daten.
- 18.3.: Rechtswahl und Gerichtszuständigkeit. Der Vertrag unterliegt den Gesetzen von England und Wales. Für alle daraus entstehenden Rechtsstreitigkeiten sind ausschließlich die englischen Gerichte zuständig. *Google* behält sich allerdings vor, einstweilige Rechtsmittel auch in jeder anderen Rechtsordnung zu ergreifen.
- 18.8.: Keiner der Vertragspartner ist für Umstände haftbar, die außerhalb seiner Kontrolle liegen.
- 18.12.: Im Falle der Abweichung der Übersetzung von der Originalvereinbarung ist die Originalvereinbarung maßgeblich.

Die Google Apps Professional-Vereinbarung verweist auf die „Google Apps Professional und Google Apps Education - Programmrichtlinien für Administratoren"[433], die somit ebenfalls Vertragsinhalt werden. Dieses Dokument enthält einerseits eine Auflistung der im Rahmen der Nutzung von *Google Apps* verbotenen Maßnahmen und andererseits Verweise auf Bedingungen für die Endnutzer – das sind in der Regel die Dienstnehmer des Nutzers –, an welche diese gebunden werden müssen. Die Google Apps Professional-Vereinbarung verweist zudem auf ein SLA, das allerdings nur für *Google Mail*, nicht für das gesamte Angebot von *Google Apps* gilt.

[433] Quelle: http://www.google.com/apps/intl/de/terms/use_policy.html (Zugriff am 08. September 2010).

Wichtige Bestimmungen des Service Level Agreement für Google Mail:[434]

- *Google* garantiert eine monatliche Verfügbarkeit der Google Mail-Webbenutzeroberfläche von 99,9%.
- Bei Nichteinhaltung dieser Zusage kann der Nutzer Service-Gutschriften beantragen, die den Vertrag um eine bestimmte Anzahl von Tagen – gestaffelt nach dem Prozentsatz der tatsächlichen Verfügbarkeit – kostenlos verlängern. Maximal 15 Tage können auf diese Weise pro Monat gutgeschrieben werden.
- Eine mehr als fünfprozentige serverseitige „Benutzerfehlerrate" gilt als Ausfallzeit.
- Ausfallzeiten von weniger als zehn aufeinanderfolgenden Minuten werden nicht berücksichtigt.
- Geplante Ausfallzeit – das sind pro Kalenderjahr maximal zwölf Stunden Ausfallzeit, die fünf Tage im Voraus angekündigt werden – gilt nicht als Ausfallzeit.
- Die Verfügbarkeitszusage gilt nicht für Probleme, die sich außerhalb der Kontrolle von *Google* befinden.

Auch die Rechtsposition des Nutzers von *Google Apps Premier Edition* unterscheidet sich nicht wesentlich von jener der Nutzer anderer betrachteter Services. *Google* ist berechtigt, die Services jederzeit einzustellen und die maximale Haftungssumme ist mit 400 EUR sehr niedrig. Das SLA ist auf den Teil-Service *Google Mail* beschränkt und verlängert im schlimmsten Fall nur die Erbringung eines fehlerhaften Service. Soweit die Einschätzung der rein rechtlichen Situation des Nutzers. Jedoch kann insbesondere von einem Anbieter wie *Google* aufgrund seiner Größe und Bedeutung erwartet werden, dass er seinen Ruf verteidigen und daher mit all seinen Möglichkeiten unabhängig von einer vertraglichen Verpflichtung für Sicherheit, Verfügbarkeit und Kundenzufriedenheit sorgen will. Daher ist es sehr unwahrscheinlich, dass *Google* insbesondere von Rechten wie etwa dem zur jederzeitigen Einstellung des Service Gebrauch machen wird, sofern genug Kundenachfrage besteht. Zum Datenschutz ist zu sagen, dass der Vertrag zwar mit einer europäischen Tochtergesellschaft von *Google* geschlossen wird, *Google* sich allerdings vorbehält, die Daten in seinen Rechenzentren weltweit zu speichern und dies vom Nutzer nicht nachvollzogen werden kann.

[434] Quelle: http://www.google.com/apps/intl/de/terms/sla.html (Zugriff am 08. September 2010).

6. Ergebnis: Vorgehensmodell und Einsatzgebiete für den betrieblichen Einsatz von Cloud Computing

"With the cloud comes unconstrained thinking and willingness to tinker and experiment without worrying too much about cost".[435]

In diesem Kapitel werden die Schlussfolgerungen aus den bisher gewonnenen Erkenntnissen gezogen. Die Frage nach geeigneten Anwendungsfällen für den Einsatz von Cloud-Services im Unternehmen wird beantwortet. Dazu wird ein Vorgehensmodell zur Entscheidungsfindung über den betrieblichen Einsatz von Cloud Computing vorgestellt, welches aus den Ergebnissen der vorhergehenden Kapitel abgeleitet wurde. Dieses besteht aus einer Reihe von Fragen, mit denen sich ein Unternehmen auseinandersetzen kann, um zu einer Entscheidung über den Einsatz von Cloud-Services zu kommen. Kernstück des Vorgehensmodells ist ein Kriterienkatalog zur Klärung Frage nach dem Nutzen bzw. den Nachteilen und Risiken des Einsatzes eines Cloud-Service für ein bestimmtes Aufgabengebiet im Unternehmen.

Um einerseits geeignete Anwendungsfälle von Cloud-Services aufzuzeigen und andererseits das Vorgehensmodell praktisch zu demonstrieren werden im zweiten Teil dieses Kapitels zunächst sechs prototypische Klassen von Unternehmen definiert. Anschließend werden basierend auf den in der vorliegenden Diplomarbeit gewonnenen Erkenntnissen unter Einbeziehung des Vorgehensmodells typische Anwendungsfälle von Cloud-Services für jede der sechs Klassen von Unternehmen herausgearbeitet.

Anzumerken ist, dass das Vorgehensmodell über die eben genannte prototypische Verwendung hinaus nicht validiert wurde. Das Vorgehensmodell bildet als Form der Aufbereitung der Ergebnisse einen zusammenfassenden Schlusspunkt der vorliegenden Diplomarbeit. Es könnte ebenso als Ausgangspunkt einer weiteren Arbeit dienen, die es mit empirischen Mitteln und/oder durch praktische Anwendung zu validieren versucht. Dies würde einer eigenen Arbeit mit ähnlichem Aufwand bedürfen und daher den Rahmen der vorliegenden Diplomarbeit sprengen.

6.1. Vorgehensmodell zur Entscheidungsfindung über den betrieblichen Einsatz von Cloud Computing

In Verbindung mit den detaillierten Ausarbeitungen zu den verschiedene Aspekten des Cloud Computing in den vorhergehenden Kapiteln kann das in diesem Abschnitt vorgestellte Vorgehensmodell von österreichischen Unternehmen als Unterstützung bei der Entscheidungsfindung über die Nutzung von Cloud Computing eingesetzt werden. Mit

[435] *Werner Vogels*, Chief Technology Officer and Vice President, World-wide Architecture, *Amazon.com*, zitiert nach Malik 2010.

anderen Worten, das Vorgehensmodell dient der praktischen Umsetzung der Erkenntnisse der vorhergehenden Kapitel. Diese können somit für ausführlichere Erläuterungen und zur Vertiefung der im Vorgehensmodell angesprochen Punkte herangezogen werden.

Das Vorgehensmodell ist aus einzelnen Fragen aufgebaut, die nachfolgend einzeln erläutert werden, wobei auf die Kapitel 4 und 5 verwiesen wird. Die ausführliche Frage 3 (Punkt 6.1.3) nach dem Nutzen sowie den Nachteilen und Risiken des Einsatzes eines Cloud-Service für ein konkretes Aufgabengebiet ist der Kern des Vorgehensmodells. Dieser gliedert sich in 15 weitere Fragen, die zum Teil wieder Subfragen enthalten und gemeinsam einen Kriterienkatalog bilden, der zur Entscheidung darüber dient, ob Cloud Computing für ein bestimmtes Aufgabengebiet im Unternehmen eingesetzt werden soll. Die 15 Fragen des Kriterienkatalogs haben alle grundsätzlich denselben Stellenwert, stehen also in keiner Rangordnung, und die Reihenfolge ihrer Beantwortung spielt ebenfalls nur eine untergeordnete Rolle. Vielmehr richtet sich die Bedeutung, die einer einzelnen Frage jeweils beigemessen werden sollte, nach den Anforderungen des Einzelfalls. Manche der Fragen sind nur für bestimmte Cloud-Service-Modelle relevant. Wenn dies der Fall ist, sind die jeweiligen Cloud-Service-Modelle bei der Frage angegeben.

Die Antworten auf die Fragen sprechen jeweils für sich genommen entweder tendenziell für – symbolisiert durch eine Wolke – oder tendenziell gegen – symbolisiert durch ein „x“ – den Einsatz eines Cloud-Service, oder führen zu weiteren Fragen. Die einzelnen Fragen aber keineswegs als trennscharfe Ausschlusskriterien zu sehen. Vielmehr soll sich aus den Antworten auf alle Fragen des Kriterienkatalogs für den jeweiligen Fall ein Trend pro oder contra Cloud Computing ergeben. Dabei werden wohl in den meisten Fällen manche Kriterien für und manche gegen den Einsatz eines Cloud-Service sprechen. Welche davon letztlich schwerer wiegen, muss im Einzelfall entschieden werden.

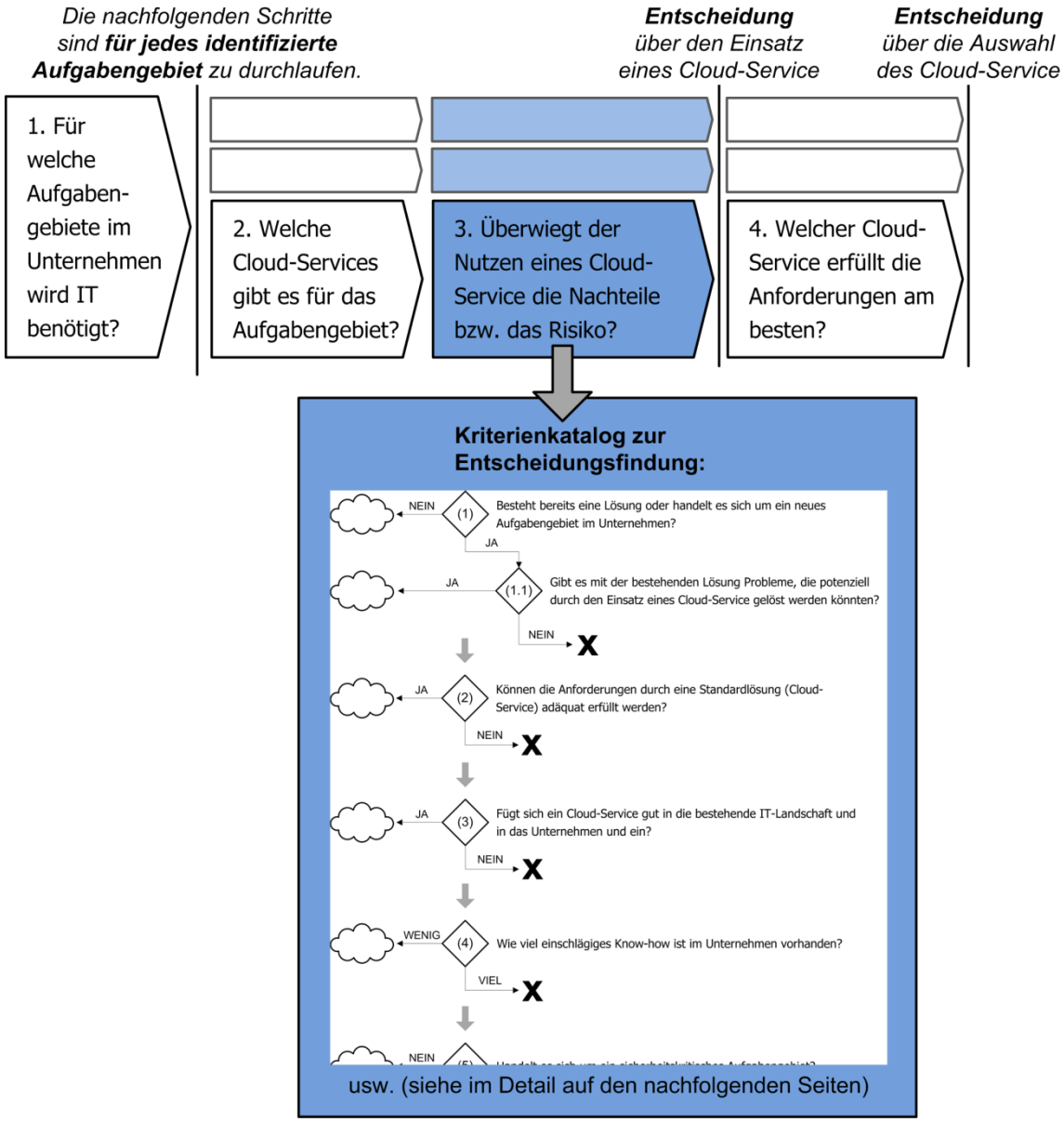
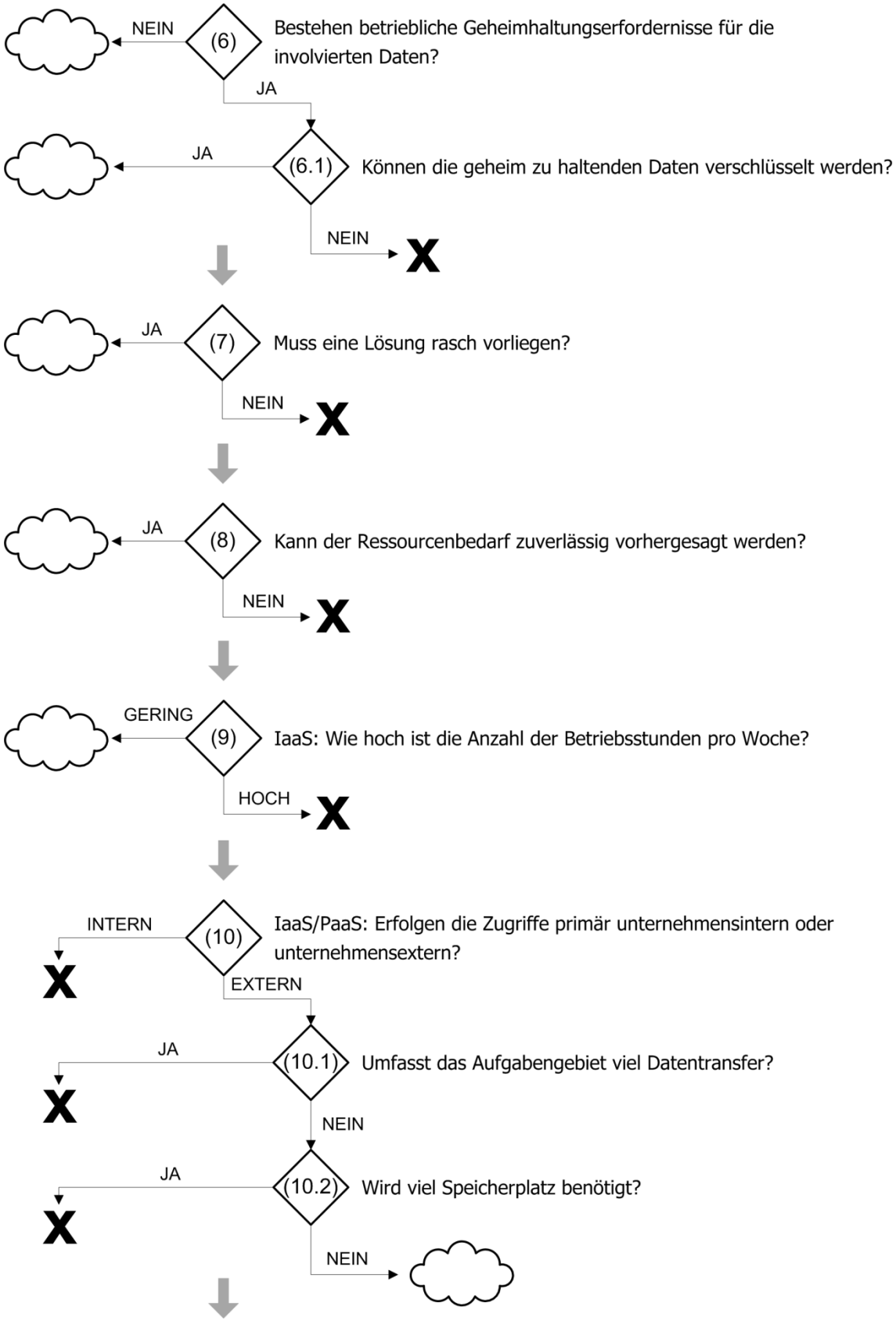


Abbildung 15 – Vorgehensmodell zur Entscheidungsfindung über den Einsatz von Cloud Computing[436]

Auf den folgenden drei Seiten ist der in Abbildung 15 nur schematisch eingefügte Kriterienkatalog zur Entscheidungsfindung im Detail dargestellt. Um die Fragen, aus denen der Kriterienkatalog aufgebaut ist, richtig interpretieren zu können, ist es notwendig, die ausführlichen Erläuterungen unter Punkt 6.1.3 (S. 123) nachzuvollziehen.

[436] Quelle: Eigene Darstellung.


NEIN
(1)
Besteht bereits eine Lösung oder handelt es sich um ein neues Aufgabengebiet im Unternehmen?
JA
JA
(1.1)
Gibt es mit der bestehenden Lösung Probleme, die potenziell durch den Einsatz eines Cloud-Service gelöst werden könnten?
NEIN
X
JA
(2)
Können die Anforderungen durch eine Standardlösung (Cloud-Service) adäquat erfüllt werden?
NEIN
X
JA
(3)
Fügt sich ein Cloud-Service gut in die bestehende IT-Landschaft und in das Unternehmen ein?
NEIN
X
WENIG
(4)
Wie viel einschlägiges Know-how ist im Unternehmen vorhanden?
VIEL
X
NEIN
(5)
Handelt es sich um ein sicherheitskritisches Aufgabengebiet?
JA
ERHÖHEN
(5.1)
Würde sich die Sicherheit durch Einsatz eines Cloud-Service erhöhen oder verringern?
VERRINGERN
X


NEIN
(6)
Bestehen betriebliche Geheimhaltungserfordernisse für die involvierten Daten?
JA
JA
(6.1)
Können die geheim zu haltenden Daten verschlüsselt werden?
NEIN
X
JA
(7)
Muss eine Lösung rasch vorliegen?
NEIN
X
JA
(8)
Kann der Ressourcenbedarf zuverlässig vorhergesagt werden?
NEIN
X
GERING
(9)
IaaS: Wie hoch ist die Anzahl der Betriebsstunden pro Woche?
HOCH
X
INTERN
(10)
IaaS/PaaS: Erfolgen die Zugriffe primär unternehmensintern oder unternehmensextern?
X
EXTERN
JA
(10.1)
Umfasst das Aufgabengebiet viel Datentransfer?
X
NEIN
JA
(10.2)
Wird viel Speicherplatz benötigt?
X
NEIN

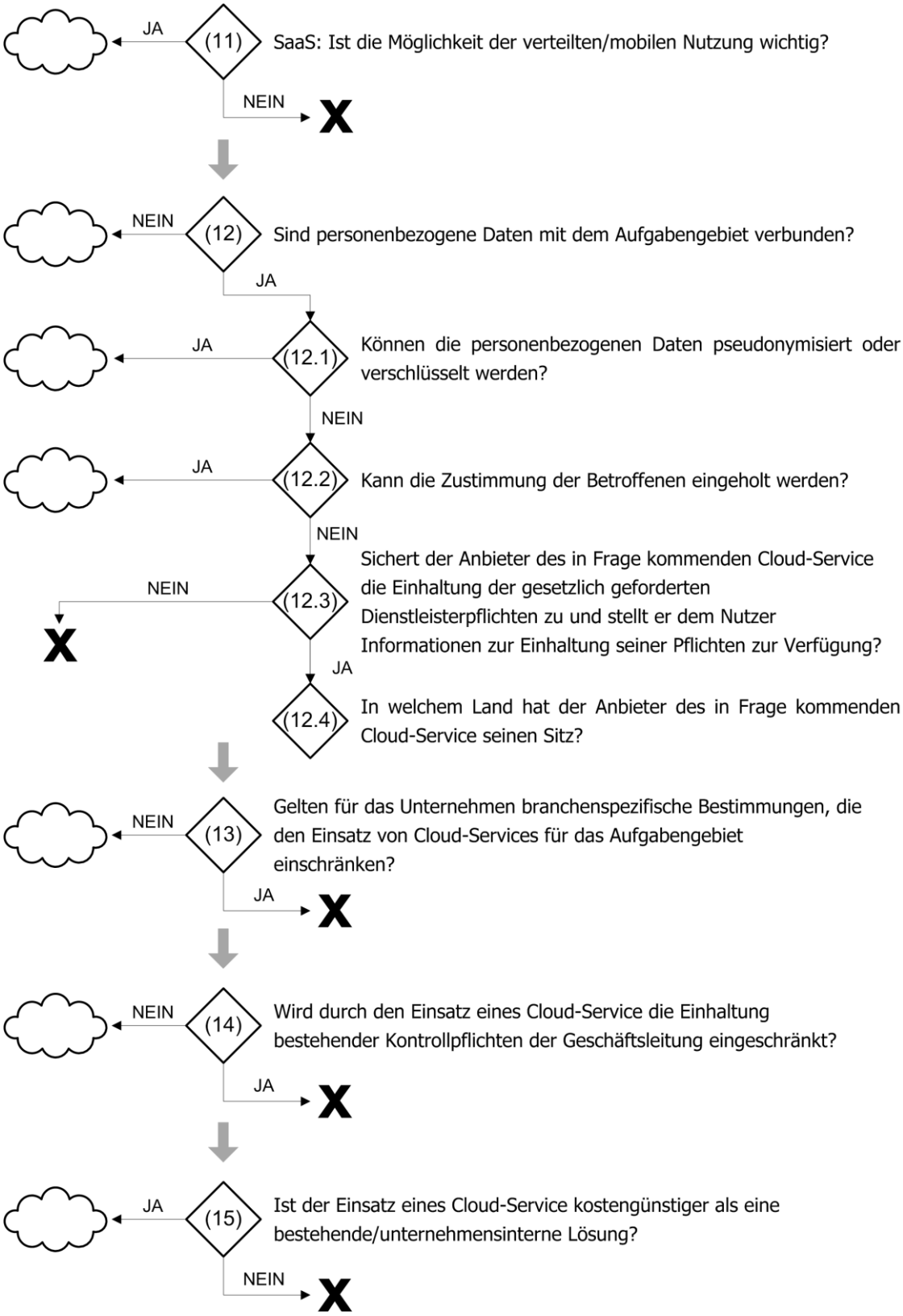


Abbildung 16 – Kriterienkatalog zur Entscheidungsfindung über den Einsatz von Cloud-Services[437]

[437] Quelle: Eigene Darstellung.

6.1.1. Für welche Aufgabengebiete im Unternehmen wird IT benötigt?

Die systematische Analyse der Einsatzmöglichkeiten von Cloud-Services im Unternehmen beginnt mit der Frage, für welche Aufgabengebiete des Unternehmens gegenwärtig IT eingesetzt wird. Dies sind potenzielle Einsatzgebiete von Cloud-Services, für welche die Umstellung auf die Nutzung von Cloud-Services anhand dieses Vorgehensmodells geprüft werden kann.

Doch nicht nur in bereits bestehenden Aufgabengebieten kann Cloud Computing eingesetzt werden. Gerade der Bedarf nach IT in neu gegründeten Unternehmen oder Geschäftsbereichen ist ein Einsatzgebiet, in dem Cloud Computing seine Stärken wie Flexibilität und Fokussierung des Nutzers auf das Kerngeschäft ausspielen kann.[438] Selbst der umgekehrte Ansatz kann gewählt werden: Im Sinne der diesbezüglichen Ausführungen unter Punkt 4.1.5 (S. 72) kann analysiert werden, welche neuen Möglichkeiten bzw. Aufgabengebiete im Unternehmen durch den Einsatz von Cloud Computing geschaffen werden können.

Für jedes der in diesem Punkt ermittelten Aufgabengebiete, für die der Einsatz von Cloud-Services grundsätzlich in Erwägung gezogen wird, können die nachfolgenden Fragen des Vorgehensmodells durchlaufen werden, um zu einer Entscheidung zu gelangen.

6.1.2. Welche Cloud-Services gibt es für das Aufgabengebiet?

Zur Klärung dieser Frage kann die vorliegende Arbeit nur bedingt herangezogen werden. Die in Kapitel 5 vorgestellten Cloud-Services decken zwar eine breite Palette von Anwendungsgebieten ab, eine eigene Recherche ist jedoch unerlässlich, um alle aktuell für ein konkretes Aufgabengebiet verfügbaren Cloud-Services zu finden. Literatur wie die vorliegende Arbeit und die in Anhang B befindliche Liste von Cloud-Services kann dabei nur ein Ausgangspunkt, nicht aber alleinige Quelle sein, weil der Markt sehr dynamisch ist und laufend neue Services hinzukommen, bestehende Angebote verändert und erweitert werden. Web-Quellen wie die Liste von *Geelan*[439], die offenbar von Zeit zu Zeit aktualisiert wird, können ebenfalls als Einstieg in die Recherche dienen. Generell ist die Web-Community in Sachen Analyse des Cloud-Computing-Markts sehr aktiv.[440] Details zu den einzelnen Services können schließlich direkt auf der Website des jeweiligen Anbieters ermittelt werden.

---

[438] Siehe dazu Abschnitt 4.1, S. 68.
[439] Geelan 2010,
[440] Beispiele dafür sind neben Geelan 2010, Bias 2010, Rosen 2010, Urquhart 2010 und Warfield 2010.

6.1.3. Überwiegt der Nutzen eines Cloud-Service die Nachteile bzw. das Risiko? (Kriterienkatalog zur Entscheidungsfindung)

IT-STRATEGISCHE KRITERIEN:

(1) Besteht bereits eine Lösung oder handelt es sich um ein neues Aufgabengebiet?

Es versteht sich fast von selbst, dass in die Überlegungen über den Einsatz einer neuen IT-Lösung die bestehende Lösung mit einbezogen werden sollte, wenn eine solche bereits existiert. Muss hingegen eine IT-Lösung für ein neues Aufgabengebiet von Grund auf entwickelt werden, können die mittels der nachfolgenden Fragen und anhand von Kapitel 4 erarbeiteten Stärken und Schwächen des Einsatzes eines Cloud-Service unmittelbar abgewogen werden. Kommt aber die Beibehaltung einer bereits bestehenden IT-Lösung ebenfalls in Frage, müssen die Stärken der Nutzung eines Cloud-Service zusätzlich mit den Stärken einer Beibehaltung der bestehenden Lösung abgewogen werden.

(1.1) Gibt es mit der bestehenden Lösung Probleme, die potenziell durch den Einsatz eines Cloud-Service gelöst werden könnten?

Solche Probleme, seien es vergleichsweise hohe Kosten oder zeitweilige Überlastung, wären selbstredend ein Argument für den Einsatz eines Cloud-Service.

(2) Können die Anforderungen durch eine Standardlösung (Cloud-Service) adäquat erfüllt werden?

Die Entscheidung über den Einsatz von SaaS kann auch als Entscheidung zwischen Standard- und Individualsoftware betrachtet werden, sofern letztere für das betreffende Aufgabengebiet grundsätzlich in Frage kommt.[441] Auch für potenzielle Einsatzgebiete von IaaS und PaaS stellt sich die Frage, ob die von den Cloud-Services gebotenen standardisierten Möglichkeiten für den jeweiligen Fall ausreichen. Insbesondere bei IaaS tritt dies aber möglicherweise in den Hintergrund, weil mit der (virtuellen) Infrastruktur ohnehin nur ein kleiner Teil des Gesamtsystems nicht vom Nutzer stammt. Wenn allerdings die physische Kontrolle über die Hardware nötig ist oder Software eingesetzt werden soll, die sehr spezifische Hardwareanforderungen hat, ist die Verwendung eigener Hardware meist die einzig mögliche Lösung.

(3) Fügt sich ein Cloud-Service gut in die bestehende IT-Landschaft und in das Unternehmen und ein?

Dies ist eine sehr umfassende Thematik, die hier nur gestreift werden kann, da die technischen und organisatorischen Schnittstellen und Auswirkungen einer IT-Lösung

[441] Siehe dazu BITKOM 2009, 44 f.

im Unternehmen sehr weit reichend sein können. Auf technischer Ebene seien als Beispiel die Schnittstellen eines neu einzuführenden SaaS-CRM-Systems zum bestehenden unternehmensinternen E-Mail- und Terminverwaltungssystem genannt, die in diesem Fall ein wesentliches Kriterium bei der Auswahl des CRM-Systems sein werden. Auf organisatorischer Ebene sind die Kenntnisse und Gewohnheiten der bestehenden Mitarbeiter ein wesentlicher Faktor bei der Auswahl neu einzuführender Systeme. Sowohl aus technischer als auch aus organisatorischer Sicht ist dieses Kriterium aber nicht nur für SaaS, sondern gleichermaßen für PaaS und IaaS wesentlich. Neben den Schnittstellen sind hier vor allem auch die verwendeten Technologien und die entsprechenden Kenntnisse der Mitarbeiter entscheidend.

(4) Wie viel einschlägiges Know-how ist im Unternehmen vorhanden?

Im Zuge des Einsatzes eines Cloud-Service werden Tätigkeiten – wie z.B. Betrieb und Wartung von Server-Hardware – durch den Anbieter des Cloud-Service erbracht, die theoretisch auch unternehmensintern erbracht werden könnten. Falls im Unternehmen Mitarbeiter vorhanden sind, welche diese Tätigkeiten bisher erbracht haben, verliert das Unternehmen deren einschlägiges Know-how, wenn diese Mitarbeiter das Unternehmen verlassen oder langfristig für andere Tätigkeiten eingesetzt werden. Der neuerliche Aufbau einer unternehmensinternen IT-Lösung für das Aufgabengebiet – etwa weil sich der Einsatz eines Cloud-Service als Fehlentscheidung erwiesen hat – wird dadurch erheblich erschwert. Dadurch besteht eine Abhängigkeit von Cloud-Services bzw. unternehmensexternen Anbietern, für die unter Punkt 4.2.2 (S. 76) die Bezeichnung „Cloud-Lock-in“ eingeführt wurde. Dies sollte in die Überlegungen mit einbezogen werden.

Wenn kein Verlust von Know-how droht, weil die einschlägigen Tätigkeiten trotz Nutzung eines Cloud-Service für ein bestimmtes Aufgabengebiet im Unternehmen ohnehin für andere Aufgabengebiete weiterhin erbracht werden, sollte allerdings die Wirtschaftlichkeit der Nutzung des Cloud-Service sehr genau geprüft werden. Möglicherweise könnten in dieser Konstellation die an den Anbieter des Cloud-Service ausgelagerten Tätigkeiten im Unternehmen insgesamt kostengünstiger erbracht werden, weil die entsprechenden Mitarbeiter und Strukturen ohnehin vorhanden sind. Mit anderen Worten, in dieser Situation tritt die unter Punkt 4.1.2 (S. 70) beschriebene Fokussierung nicht ein, ein Vorteil der Lösung mittels Cloud-Service fällt weg.

Ist jedoch das Gegenteil der Fall und kein oder nur geringes einschlägiges Know-how für eine unternehmensinterne Lösung vorhanden, kann dies durch den Einsatz eines Cloud-Service kompensiert werden. Wenig vorhandenes Know-how ist somit ein Argument für den Einsatz von Cloud-Services.

(5) Handelt es sich um ein sicherheitskritisches Aufgabengebiet?

Es gibt Aufgabengebiete, die keine hohen Anforderungen an die Sicherheit und Verfügbarkeit der eingesetzten IT-Anwendungen stellen. Beispiele hierfür sind massiv parallelisierte Konvertierungs- oder sonstige Berechnungsaufgaben mit einer großen Menge von – unkritischen – Daten, wie dies etwa im Zitat am Beginn von Kapitel 5 beschrieben wird. Für solche Anwendungsgebiete können Cloud-Services bedenkenlos genutzt werden, ansonsten ist eine weitere Prüfung nötig:

(5.1) Würde sich die Sicherheit durch Einsatz eines Cloud-Service erhöhen oder verringern?

In Kapitel 4 wurde deutlich, dass die Auswirkungen der Nutzung von Cloud-Services auf die Sicherheit differenziert betrachtet werden müssen: Der Einsatz von Cloud-Services kann die Sicherheit sowohl verringern als auch erhöhen. Dies hängt vom Verhältnis der unternehmensintern gebotenen Sicherheit zu jener Sicherheit ab, die der jeweilige Cloud-Service bieten würde. Formell betrachtet ist letztere meist nicht sehr hoch, denn die Gewährleistung und Haftung der Anbieter von Cloud-Services ist in der Regel in Sicherheitsfragen wie auch generell sehr begrenzt, vorausgesetzt die Ergebnisse der explorativen Marktanalyse in Kapitel 5 können verallgemeinert werden. Wie bereits mehrfach angesprochen, ist aber die formale, vertragsrechtliche Sichtweise nicht die einzige, die in diesem Zusammenhang relevant ist. Faktisch kann die gebotene Sicherheit und Verfügbarkeit eines Cloud-Service um ein vielfaches höher sein, als vertraglich zugesichert, weil der Anbieter einen Anreiz hat, für Sicherheit, Verfügbarkeit und Kundenzufriedenheit zu sorgen, um einen guten Ruf zu erlangen und zu verteidigen.

Ob dies im konkreten Fall so einzuschätzen ist und welche vertraglichen Zusicherungen bestehen, muss bei sicherheitskritischen Aufgabengebieten für jeden in Frage kommenden Cloud-Service analysiert werden. Das Ergebnis dieser Analyse muss anschließend mit jenem Sicherheitsniveau verglichen werden, das bei unternehmensinterner Leistungserbringung – wirtschaftlich sinnvoll – erreichbar ist. Für Details zu den Stärken und Schwächen des Cloud Computing im Sicherheitsbereich sei auf die Punkte 4.1.3 (S. 70) und 4.2.1 (S. 74) verwiesen.

(6) Bestehen betriebliche Geheimhaltungserfordernisse für die involvierten Daten?

Unabhängig vom Datenschutzrecht, das im letzten Teil dieses Kriterienkatalogs behandelt wird, kann die Geheimhaltung von Daten aus unternehmensinternen Gründen erforderlich sein. Dies ist beispielsweise dann der Fall, wenn die Daten Wettbewerbern einen Vorteil verschaffen könnten.

(6.1) Können die geheim zu haltenden Daten verschlüsselt werden?

Bedeutende, geheim zu haltende Unternehmensdaten im Rahmen der Nutzung eines Cloud-Service zu verwenden, kann nur dann empfohlen werden, wenn diese vorher verschlüsselt werden können und damit ausschließlich in verschlüsselter Form das Unternehmen verlassen. Die Nutzung eines Cloud-Service ist nämlich immer mit dem Verlust der Kontrolle über die involvierten Daten verbunden. Selbst wenn der Anbieter diesbezüglich verbindliche Zusicherungen abgibt, was angesichts der Ergebnisse der explorativen Marktanalyse in Kapitel 5 ohnehin nicht zu erwarten ist, besteht das Risiko, dass die Daten – z.B. aufgrund von Sicherheitslücken – in fremde Hände gelangen. Wie bereits unter Punkt 4.2.1 (S. 74) angesprochen, kann es sein, dass in diesem Fall ein allfälliger Schadenersatzanspruch den tatsächlichen Schaden nicht mehr ausgleichen kann.

Das Risiko sollte im Einzelfall anhand des Werts der Daten und der vom Anbieter des jeweiligen Cloud-Service einerseits vertraglich zugesicherten und andererseits tatsächlich zu erwartenden Datensicherheit abgeschätzt werden. Eine entsprechende Empfehlung für den Einsatz von Cloud Computing kann in diesem Zusammenhang aber wie gesagt nur bei Verwendung entsprechender Datenverschlüsselung abgegeben werden.

(7) Muss eine Lösung rasch vorliegen?

Große Stärken des Cloud Computing sind – als Ausprägung von dessen Flexibilität[442] – die unmittelbare Verfügbarkeit und der rasche Einstig. Dies spricht dafür, im Fall der Entwicklung einer neuen Lösung für ein Aufgabengebiet, die möglichst rasch fertig sein soll, Cloud-Services einzusetzen.

(8) Kann der Ressourcenbedarf zuverlässig vorhergesagt werden?

Ebenfalls aufgrund der Flexibilität des Cloud Computing eignet sich dieses besonders für Aufgabengebiete, deren Nutzungsintensität und damit Ressourcenbedarf nicht zuverlässig vorhergesagt werden kann. Zwei Aspekte der Nutzungsintensität sind dabei zu beachten: Die kurzfristige, welche nicht zuverlässig vorhergesagt werden kann, wenn die Nutzung starken Schwankungen unterliegt, und die langfristige, welche z.B. aufgrund des Wachstums des Unternehmens zunehmen kann. Für beide Aspekte kann eine Anwendung durch den richtigen Einsatz eines Cloud-Service im Vorhinein so ausgelegt werden, dass die Kosten mit der tatsächlichen Nutzung – nach oben und unten – skalieren.

[442] Siehe Punkt 4.1.1, S. 68.

(9) IaaS: Wie hoch ist die Anzahl der Betriebsstunden pro Woche?

Bei der Entscheidungsfindung über die Nutzung von Cloud-Services, die nach der Anzahl der Betriebsstunden abgerechnet werden, wie insbesondere IaaS, sollte versucht werden, die Anzahl der durchschnittlichen wöchentlichen Betriebsstunden abzuschätzen. Wenn ein Server sehr häufig oder permanent laufen soll, ist der Betrieb eines eigenen Servers oder das konventionelle Anmieten eines Servers – nach derzeitigem Stand des IaaS-Marktes – in der Regel billiger, als der Einsatz von IaaS. Lässt sich die Anzahl der Betriebsstunden nicht abschätzen, spricht dies – wie soeben unter Punkt 6 erläutert – für den Einsatz eines Cloud-Service.

(10) IaaS/PaaS: Erfolgen die Zugriffe primär unternehmensintern oder unternehmensextern?

Wird der Einsatz von IaaS oder PaaS für ein Aufgabengebiet erwogen, sollte überlegt werden, von wo aus das System primär genutzt wird. Die Kosten für die Datenübertragung, der begrenzte Datendurchsatz und die höheren Latenzzeiten, die ein Cloud-Service im Vergleich zu einer unternehmensinternen Lösung mit sich bringt, sprechen bei überwiegend unternehmensinterner Nutzung an einem einzigen Standort für eine unternehmensinterne Lösung, insbesondere wenn die Nutzung intensiv ist und es auf diese Faktoren besonders ankommt. Wenn dies nicht der Fall ist, kann es durchaus sein, dass andere Aspekte die hier genannten Schwächen einer Lösung mittels Cloud-Service überwiegen. Überwiegend unternehmensexterne Zugriffe und Zugriffe von mehreren Unternehmensstandorten aus sprechen eher für den Einsatz eines Cloud-Service, allerdings bestehen bestimmte Einschränkungen:

(10.1) Umfasst das Aufgabengebiet viel Datentransfer?

Datentransfer wird bei IaaS und PaaS in der Regel nach Volumen abgerechnet. Wenn im Rahmen einer Anwendung häufig große Datenmengen übertragen werden müssen, kann es kostengünstiger sein, die Anwendung nicht auf einem Cloud-Service zu betreiben, sondern in einem Umfeld, bei dem die Internetverbindung pauschal nach zur Verfügung stehender Bandbreite abgerechnet wird. Dies kann konventionelles Hosting oder unternehmensinterner Betrieb sein.

(10.2) Wird viel Speicherplatz benötigt?

Ähnliches wie das eben Gesagte gilt für Anwendungen, die viel Speicherplatz beanspruchen, der in der Regel bei IaaS und PaaS ebenfalls nach Volumen abgerechnet wird. Konventionelles Hosting oder unternehmensinterner Betrieb kann daher im Vergleich dazu die kostengünstigere Lösung sein.

(11) SaaS: Ist die Möglichkeit der verteilten/mobilen Nutzung wichtig?

Wie unter Punkt 4.1.5 (S. 72) angesprochen, ist die systemimmanente weltweite Verfügbarkeit eine wesentliche Stärke von SaaS. Dieses bietet sich daher besonders an, wenn eine Software von verschiedenen Standorten aus genutzt werden soll, sei es in verschiedenen Filialen, an Heimarbeitsplätzen oder durch Außendienstmitarbeiter.

RECHTLICHE KRITERIEN:

(12) Sind personenbezogene Daten mit dem Aufgabengebiet verbunden?

Wie in Kapitel 3 gezeigt wurde, ist das Datenschutzrecht ein wesentlicher Faktor bei der Entscheidungsfindung über den Einsatz eines Cloud-Service. Dieses ist zu beachten, wenn das Aufgabengebiet, für das die Nutzung eines Cloud-Service in Betracht gezogen wird, mit personenbezogenen Daten[443] in Zusammenhang steht.

(12.1) Können die personenbezogenen Daten pseudonymisiert oder verschlüsselt werden?

Falls die personenbezogenen Daten vor ihrer Verwendung im Rahmen eines Cloud-Service verschlüsselt oder pseudonymisiert werden können, ist diese Verwendung unbedenklich, wird also durch das Datenschutzrecht nicht beschränkt. Unter Pseudonymisierung versteht man das Ersetzen der Namen der betroffenen Personen in den Datensätzen durch eindeutige Nummern, Buchstabenkombinationen o.Ä., die nur vom Ersteller, nicht aber von unberechtigten Dritten, wieder den betroffenen Personen zugeordnet werden können. Verschlüsselung und Pseudonymisierung werden allerdings in vielen Fällen nicht möglich sein, insbesondere bei der Nutzung im Rahmen von SaaS, bei der die Daten nicht nur im Web gespeichert sondern auch im Web be- und verarbeitet werden.[444]

(12.2) Kann die Zustimmung der Betroffenen eingeholt werden?

Die Zustimmung der betroffenen Personen entspricht einem datenschutzrechtliche „Freibrief", denn der Gesetzgeber schützt Personen im Rahmen des Datenschutzrechts nur, soweit sie dies selbst wollen: Willigt ein Betroffener ohne Zwang in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten ein, ist diese Verwendung zulässig. Die Zustimmung muss also sehr spezifisch sein und von jeder einzelnen Person vorliegen, deren Daten verwendet werden sollen. Auch eine Überlassung von Daten in das Ausland wird durch eine solche Zustimmung des Betroffenen zulässig, sofern sie sich auf alle spezifischen Umstände, also auch auf das betreffende Land bezieht.

---

443 Zur Definition von personenbezogenen Daten siehe Punkt 3.2.2, S.50.
444 Velte, Velte und Elsenpeter 2009, 32 f.

(12.3) Sichert der Anbieter des in Frage kommenden Cloud-Service die Einhaltung der gesetzlich geforderten Dienstleisterpflichten zu und stellt er dem Nutzer Informationen zur Einhaltung seiner Pflichten zur Verfügung?

Die Datenüberlassung in das Ausland – und von dieser ist im Zusammenhang mit Cloud Computing auszugehen, da es nach Wissensstand des Autors keinen nennenswerten Anbieter von Cloud-Services in Österreich gibt – setzt eine schriftliche Zusicherung der Einhaltung der Dienstleisterpflichten nach § 11 Abs 1 DSG 2000 und damit auch der Datensicherheitsmaßnahmen nach § 14 DSG 2000 durch den Dienstleister voraus.[445] Aufgrund des Kriteriums des „on-demand self-serivce"[446] müsste sich eine solche Zusicherung direkt in den Standard-Vertragsbedingungen des Anbieters befinden. Bei den in Kapitel 5 untersuchten Cloud-Services ist dies nicht der Fall. Insbesondere behalten sich einige der untersuchten Anbieter entweder vor, zur Erfüllung des Vertrages mit dem Nutzer Subdienstleister heranzuziehen, oder es geht aus den Vertragsbedingungen nicht klar hervor, ob dazu die Zustimmung des Nutzers erforderlich ist.[447] Zudem ist die Pflicht des Dienstleisters (also des Anbieters), alle Daten des Auftraggebers (also des Nutzers) nach der Beendigung der Dienstleistung diesem zu übergeben oder zu vernichten[448] von allen untersuchten Vertragsbedingungen nur in jenen von *Salesforce CRM* zu finden.

Auch eine uneingeschränkte Zusicherung der Einhaltung der Datensicherheitsmaßnahmen nach § 14 DSG 2000 ergibt sich bei keinem der untersuchten Services eindeutig aus den Vertragsbedingungen. Bestimmungen wie etwa die Nichtübernahme der Verantwortung für unautorisierten Datenzugriff durch Dritte und weitgehende Garantie- und Haftungsausschlüsse stehen dem entgegen. Hinzuzufügen ist, dass es nicht genügen würde, wenn es sich aus den Vertragsbestimmungen in ihrer Gesamtheit möglicherweise doch herauslesen ließe, dass sich der Anbieter die erforderlichen Pflichten auferlegt. Nötig wäre eine explizite, eindeutige Zusicherung der Einhaltung aller Dienstleisterpflichten, wie sie bei den untersuchten Cloud-Services offensichtlich nicht vorliegt.

Wenn der Anbieter die Einhaltung der Dienstleisterpflichten zusichert, umfasst dies auch die Pflicht, dem Nutzer jene Informationen zur Verfügung zu stel-

---

445 Diese Bestimmungen befinden sich im Volltext in Anhang A.
446 Siehe dazu Tabelle 1, S. 28.
447 Dienstleisterpflicht nach § 11 Abs 1 Z 3 DSG 2000 (siehe in Anhang A).
448 Dienstleisterpflicht nach § 11 Abs 1 Z 5 DSG 2000 (siehe in Anhang A).

len, die zur Kontrolle der Einhaltung dieser Pflichten erforderlich sind.[449] Der Nutzer hat seinerseits die Pflicht diese Kontrolle auch tatsächlich durchzuführen. Wie unter Punkt 3.2.3 (S. 53) erläutert, ist es allerdings juristisch fraglich, ob diese Kontrolle im Fall eines Cloud-Service, dessen Nutzung ohne zwischenmenschliche Interaktion erfolgt, überhaupt ausreichend ausgeübt werden kann. Daher bleibt es für den – angesichts der Ergebnisse von Kapitel 5 wohl unwahrscheinlichen – Fall, dass ein Anbieter eines Cloud-Service alle genannten Verpflichtungen in den Vertragsbedingungen eingeht und laufend Informationen über deren Einhaltung zur Verfügung stellt, dennoch datenschutzrechtlich riskant, diesem im Zuge der Nutzung personenbezogene Daten anzuvertrauen.

(12.4) In welchem Land hat der Anbieter des in Frage kommenden Cloud-Service seinen Sitz?

Wird dieses Risiko der rechtlichen Ungewissheit dennoch eingegangen, muss letztlich noch darauf geachtet werden, in welchem Land der Anbieter des in Frage kommenden Cloud-Service seinen Sitz hat. Für Anbieter in Mitgliedstaaten des EWR sowie in der Schweiz, in Argentinien, Guernsey, auf der Isle of Man, den Färöer und mit Einschränkungen auch in Kanada bestehen keine weitere Einschränkung. Datenübertragungen an Anbieter von Cloud-Services in anderen Ländern sind nur bei Vorliegen zusätzlicher Voraussetzungen zulässig. Näheres dazu siehe unter Punkt 3.2.5 (S. 56).

Abschließend muss an dieser Stelle noch auf die tatsächlichen Risiken eines Verstoßes gegen Datenschutzbestimmungen eingegangen werden. Wie in Abschnitt 3.2.6 (S. 59) erläutert, sind diese Risiken gering, da primär die Betroffenen selbst gegen Verstöße vorgehen müssten, was in der Praxis selten vorkommt. Möglicherweise droht allerdings ein größeres Risiko vonseiten der Mitbewerber des Nutzers, die wettbewerbsrechtlich gegen dessen Nichteinhaltung von Datenschutzbestimmungen vorgehen können. Auch wenn damit insgesamt das Risiko einer Verurteilung wegen Verstoßes gegen Datenschutzbestimmungen nicht sehr hoch ist, sollte beachtet werden, dass eine solche Verurteilung die Reputation eines Unternehmens beträchtlich schädigen kann.

(13) Gelten für das Unternehmen branchenspezifische Bestimmungen, die den Einsatz von Cloud-Services für das Aufgabengebiet einschränken?

Die in Abschnitt 3.3 (S. 60) besprochenen Vorschriften für Banken, Wertpapierdienstleistungsunternehmen und Versicherungen sind bedeutende Beispiele für branchenspezifische Bestimmungen, die die Einsatzmöglichkeiten von Cloud-Services in den

[449] Dienstleisterpflicht nach § 11 Abs 1 Z 6 DSG 2000 (siehe in Anhang A).

betroffenen Unternehmen einschränken. Ist ein Aufgabengebiet von solchen Bestimmungen betroffen, kann der Einsatz von Cloud-Services für dieses Aufgabengebiet unzulässig sein. Die Einzelheiten sind für die genannten Branchen Abschnitt 3.3 (S. 60) zu entnehmen, für andere Branchen den jeweils einschlägigen Bestimmungen.

(14) Wird durch den Einsatz eines Cloud-Service die Einhaltung bestehender Kontrollpflichten der Geschäftsleitung eingeschränkt?

Wie unter Punkt 3.4.1 (S. 65) dargelegt, hat die Geschäftsleitung von Kapitalgesellschaften ein angemessenes internes Kontrollsystem (IKS) zu implementieren. Für bestimmte Gesellschaften ist zudem ein Risikomanagementsystem verpflichtend. Wenn die Nutzung eines Cloud-Service für ein Aufgabengebiet erwogen wird, das Einfluss auf den Unternehmenserfolg und/oder auf die Rechnungslegung hat, müssen die betroffenen Unternehmen daher prüfen, ob dadurch die Ausübung von Kontrollpflichten eingeschränkt wird. Für die in Kapitel 5 untersuchten Cloud-Services würde sich eine solche Einschränkung und damit ein rechtliches Risiko ergeben, denn in den Vertragsbedingungen werden keine ausreichenden Zusicherungen hinsichtlich Informationssicherheit und Zuverlässigkeit gemacht.

KOSTENKALKULATION:

(15) Ist der Einsatz eines Cloud-Service kostengünstiger als eine bestehende/unternehmensinterne Lösung?

Selbstverständlich sind auch die Kosten ein wesentliches Kriterium, das in die Entscheidung über den Einsatz von Cloud Computing einfließt. In der Praxis werden dessen geringere und nutzungsadäquatere Kosten einer der wichtigsten Gründe für die grundsätzliche Erwägung der Nutzung von Cloud Computing sein. Bewusst wurden die Kosten allerdings auch in die Reihe der übrigen hier gesammelten Kriterien eingeordnet. Damit soll verdeutlicht werden, dass die Kosten nur ein Kriterium unter mehreren sind, die in die Entscheidung über den Einsatz von Cloud Computing einfließen sollen.

Die Kosten müssen für den jeweiligen Einzelfall kalkuliert werden, wobei viel mehr Faktoren einfließen, als bloß die Kosten des Cloud-Service an sich. An dieser Stelle sei noch einmal auf das gesamte Kapitel 4 verwiesen, da wohl die meisten der dort behandelten Stärken und Schwächen des Cloud Computing Einfluss auf die Kostenkalkulation haben.

Nach dem Durchlaufen aller Fragen muss gewichtet werden: Welche der Kriterien sind für das Aufgabengebiet besonders bedeutend und sprechen diese überwiegend für oder gegen den Einsatz eines Cloud-Service? Dies kann nur im Einzelfall beurteilt werden. Wie in der Fragestellung dieses dritten Schritts des Vorgehensmodells betont,

ist entscheidend, dass der Nutzen des Einsatzes eines Cloud-Service gegenüber den Nachteile bzw. Risiken *überwiegt*. Cloud Computing sollte aufgrund dieses Überwiegens verwendet werden, nicht etwa nur deswegen, weil es ein aktueller Trend ist.[450] Insbesondere wenn bestehende Lösungen durch Cloud-Services ersetzt werden sollen, ist zu beachten, dass Änderungen wie diese stets Ungewissheit, Risiken und Aufwand mit sich bringen, die durch zu erlangenden Nutzen gerechtfertigt sein müssen.

6.1.4. Welcher Cloud-Service erfüllt die Anforderungen am besten?

Der Kriterienkatalog in Schritt drei des Vorgehensmodells sollte bereits mit Blick auf die in Schritt zwei ermittelten potenziell geeigneten Cloud-Services auf dem Markt durchlaufen werden. Während manche Fragen des Kriterienkatalogs unabhängig vom letztlich ausgewählten Cloud-Service beantwortet werden können, hängen die Antworten auf viele der Fragen bereits davon ab, welchen Cloud-Service man betrachtet. Die generelle Entscheidung pro oder kontra Cloud Computing lässt sich somit nicht scharf von der Entscheidung über die Verwendung eines konkreten Cloud-Service trennen. Auch hier kommt es darauf an, welche Kriterien besonders wichtig sind. Jener der in Schritt zwei ermittelten Cloud-Services, für den die meisten dieser Kriterien sprechen, sollte letztlich ausgewählt werden.

Zu beachten sind dabei noch einige anbieterspezifische Kriterien. So sollte stets darauf geachtet werden, welches Lock-in-Risiko ein bestimmter Cloud-Service mit sich bringt.[451] Ein weiteres anbieterspezifisches Kriterium ist dessen Wahl des anwendbaren Rechts und des Gerichtsstands in den Vertragsbedingungen. Eine europäische Rechtsordnung bzw. ein europäischer Gerichtsstand erleichtern für österreichische Nutzer die Rechtsdurchsetzung. Aufgrund der vielfach angesprochenen Notwendigkeit, dem Anbieter eines Cloud-Service in Sachen Sicherheit und Zuverlässigkeit vertrauen zu müssen, sind dessen Ruf und dessen Bedeutung in der Branche letztlich wesentliche Entscheidungskriterien.

[450] Velte, Velte und Elsenpeter 2009, 27 f.
[451] Siehe dazu Punkt 4.2.2, S. 76.

6.2. Einsatzgebiete für Cloud-Services in verschiedenen Klassen von Unternehmen

Anhand des soeben erläuterten Vorgehensmodells können Unternehmen die Frage nach geeigneten Einsatzgebieten für Cloud-Services individuell für ihre spezifische Situation beantworten. Das Vorgehensmodell ist somit das wesentliche Ergebnis der vorliegenden Arbeit. Als Ergänzung dazu werden in diesem Abschnitt auf abstrakter Ebene typische Einsatzgebiete für Cloud-Services in verschiedenen Klassen von Unternehmen aufgezeigt.[452] Diese Klassen wurden anhand von zwei Dimensionen so definiert, dass sich zwischen den Klassen Unterschiede in den typischen Einsatzmöglichkeiten von Cloud-Services ergeben. Zu diesem Zweck erwiesen sich die Dimensionen Unternehmensgröße und IKT/Nicht-IKT als geeignet. Letzteres ist keine strikte Brancheneinteilung. IKT steht für Unternehmen, deren Kerngeschäft die Informations- und/oder Kommunikationstechnologie ist oder umfassenden Einsatz dieser Technologien erfordert[453], Nicht-IKT für alle übrigen Unternehmen.

Die Dimension Unternehmensgröße steht streng genommen nicht nur für die Größe an sich, denn sie gliedert sich in die drei Kategorien Startup-Unternehmen[454], kleine und mittlere Unternehmen (KMU) und große Unternehmen. Startup-Unternehmen sind Unternehmen in der Gründungsphase, also notwendigerweise kleine Unternehmen, die alle Unternehmensstrukturen einschließlich der IT völlig neu aufbauen müssen. KMU sind Unternehmen, die weniger als 250 Mitarbeiter beschäftigen und entweder einen Jahresumsatz von höchstens 50 Millionen EUR oder eine Jahresbilanzsumme von höchstens 43 Millionen EUR aufweisen.[455] Großunternehmen sind alle Unternehmen, die nicht in die Kategorie KMU fallen.

Nachfolgend spielen die Begriffe „Kernprozess“ und „Supportprozess“ eine wichtige Rolle. Dabei wird folgende Begriffsdefinition zugrundgelegt:

---

[452] Wie die Formulierung „typische Einsatzgebiete“ bereits deutlich macht, erhebt diese Zuordnung keinen Anspruch auf Vollständigkeit und Allgemeingültigkeit. Ziel ist es, geeignete Einsatzgebiete von Cloud-Services herauszuarbeiten, die sich in Unternehmen der jeweiligen Klasse typischerweise ergeben können.

[453] Dies sind primär Unternehmen der Klassen J 61 (Telekommunikation), J 62 (Erbringung von Dienstleistungen der Informationstechnologie) und J 63.1 (Datenverarbeitung, Hosting und damit verbundene Tätigkeiten; Webportale) der Klassifikation nach ÖNACE 2008 (siehe dazu Statistik Austria 2008), aber auch Unternehmen wie beispielsweise Betreiber von Online-Shops und Online-Wettanbieter, wenn die entsprechenden IT-Leistungen grundsätzlich unternehmensintern erbracht werden.

[454] Die Kategorie Startup wurde gewählt, weil sich Cloud Computing für diese Unternehmen besonders anbietet, wie nachfolgend gezeigt wird, wobei allerdings auch beträchtliche Einschränkungen deutlich gemacht werden.

[455] Dies entspricht der Definition der Europäischen Kommission (Empfehlung 2003/361/EG der Europäischen Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl L 124/36 vom 20.5.2003).

„Ein Kernprozess ist [...] ein Prozess, dessen Aktivitäten direkten Bezug zum Produkt eines Unternehmens besitzen und damit einen Beitrag zur Wertschöpfung im Unternehmen leisten.

Ein Supportprozess ist demgegenüber ein Prozess, dessen Aktivitäten aus Kundensicht zwar nicht wertschöpfend, jedoch notwendig sind, um einen Kernprozess ausführen zu können. Die Trennung zwischen Kern- und Supportprozessen ist fließend, da in unterschiedlichen Kontexten und für unterschiedliche Unternehmen derselbe Prozess Kern- oder Supportprozess sein kann."[456]

Zu beachten ist, dass neben den an der Herstellung von Produkten bzw. der Erbringung von Dienstleistungen unmittelbar beteiligten Prozessen auch Tätigkeiten in den Bereichen Marketing, Vertrieb und Kundendienst zu den Kernprozessen zählen, weil diese das Kriterium erfüllen, zur Wertschöpfung beizutragen.[457]

In der nachfolgenden Tabelle sind geeignete Einsatzgebiete für Cloud-Services in den verschiedenen Unternehmensklassen zusammengefasst. Die Tabelle ist nach den zwei genannten Dimensionen aufgebaut und enthält für jede der sechs Klassen von Unternehmen vier Arten von Angaben. Zunächst ist eine Bewertung für das generelle Potenzial von Cloud Computing für die jeweilige Klasse angegeben, die sich aus der Gesamtheit der übrigen Angaben ergibt, von „––" (sehr gering) bis „++" (sehr groß). Danach ist angegeben, für welche Art von Prozessen (Kernprozesse, Supportprozesse) sich der Einsatz von Cloud-Services in der betreffenden Unternehmensklasse besonders eignet. Eingeklammerte Angaben sollen dabei eine bedingte Eignung andeuten. Dies gilt auch für den übrigen Teil der Tabelle. Die dritte Gruppe von Angaben ist eine Aufzählung der positiven Auswirkungen, die der Einsatz von Cloud-Services speziell in Unternehmen der jeweiligen Klasse nach sich ziehen kann. Den Abschluss bilden Angaben zur besonderen Eignung und zu konkreten Anwendungsfällen jedes der drei Cloud-Service-Modelle IaaS, PaaS und SaaS.

Die Angaben in der Tabelle wurden aus den Erkenntnissen der gesamten Diplomarbeit abgeleitet. Dabei wurden Annahmen bzw. Verallgemeinerungen zu den Eigenschaften der einzelnen Unternehmensklassen getroffen, z.B. dass IKT-Unternehmen mehr internes Know-how im IT-Bereich haben als andere Unternehmen, oder dass Prognosen der Kundennachfrage für Startup-Unternehmen besonders schwierig sind. Diese Annahmen treffen nicht notwendigerweise auf jedes einzelne Unternehmen der jeweiligen Klasse zu. Es sei daher noch einmal darauf hingewiesen, dass dieser Abschnitt eine individuelle Prüfung der Potenziale des Cloud Computing für jedes konkrete Unternehmen anhand des oben vorgestellten Vorgehensmodells nicht ersetzen kann.

[456] Becker und Kahn 2005, 7.
[457] Becker und Kahn 2005, 7.

	Nicht-IKT-Unternehmen (primäres Ziel: Fokussierung)	**IKT-Unternehmen** (primäres Ziel: neue Möglichkeiten)
Startups	[+] *Supportprozesse, (Kernprozesse)* • geringe Einschränkungen („grüne Wiese“) • Fokussierung • (Kosten-)Flexibilität **IaaS:** *(Supportprozesse)* Datensicherung **SaaS:** *Kern- u. Supportprozesse* Anwendungen nach Bedarf [aber: DSG 2000 beachten!]	[++] *Kernprozesse, Supportprozesse* • neue Möglichkeiten • geringe Einschränkungen („grüne Wiese“) • Fokussierung • (Kosten-)Flexibilität **IaaS:** *Kernprozesse, (Supportprozesse)* Content-Delivery, parallelisierbare Berechnungsaufgaben, Datensicherung **PaaS:** *Kernprozesse, (Supportprozesse)* Webanwendungen **SaaS:** *Kern- u. Supportprozesse* Anwendungen nach Bedarf [aber: DSG 2000 beachten!]
KMU	[–] *Supportprozesse, (Kernprozesse)* • Fokussierung • (Kosten-)Flexibilität **IaaS:** *(Supportprozesse)* Datensicherung **SaaS:** *Supportprozesse, (Kernprozesse)* Anwendungen nach Bedarf [aber: DSG 2000 beachten!]	[+] *Supportprozesse, Kernprozesse* • neue Möglichkeiten • Fokussierung • (Kosten-)Flexibilität **IaaS:** *Kernprozesse, (Supportprozesse)* Software-Entwicklung, Lastspitzen, Content-Delivery, parallelisierbare Berechnungsaufgaben, Datensicherung **PaaS:** *Kernprozesse, (Supportprozesse)* Software-Entwicklung, Lastspitzen, Webanwendungen **SaaS:** *Supportprozesse, (Kernprozesse)* Online-Zusammenarbeit Anwendungen nach Bedarf [aber: DSG 2000 beachten!]
Groß-unternehmen	[– –] *(Supportprozesse)* • (Kosten-)Flexibilität **IaaS:** *(Supportprozesse)* Business Intelligence [aber: DSG 2000 zu beachten!] **PaaS:** *(Supportprozesse)* (Business Intelligence) [aber: DSG 2000 beachten!]	[–] *(Supportprozesse, Kernprozesse)* • neue Möglichkeiten • (Kosten-)Flexibilität **IaaS:** *(Kernprozesse)* Software-Entwicklung, Lastspitzen **PaaS:** *(Kernprozesse, Supportprozesse)* Software-Entwicklung, Lastspitzen **SaaS:** *(Supportprozesse)* Online-Zusammenarbeit [aber: DSG 2000 beachten!]

Tabelle 3 – Geeignete Einsatzgebiete für Cloud-Services in verschiedenen Klassen von Unternehmen (Zusammenfassung der Ergebnisse dieses Abschnitts)[458]

[458] Quelle: Eigene Darstellung.

In der Tabelle zeigt sich, dass IKT-Unternehmen Cloud-Services meist in gleicher Weise nutzen können wie andere Unternehmen derselben Größenkategorie, zusätzlich aber noch besondere Nutzungsmöglichkeiten haben, die sich daraus ergeben, dass die IT in diesen Unternehmen zum Kerngeschäft gehört. Die übrigen Ergebnisse in der Tabelle sind nachfolgend – gegliedert nach den sechs Unternehmensklassen – im Detail erläutert.

6.2.1. Nicht-IKT-Startups

Startup-Unternehmen unterliegen den geringsten Einschränkungen im Hinblick auf den Einsatz von Cloud-Services. Ein wesentlicher Faktor, der andere Unternehmen vom Einsatz von Cloud-Services abhalten könnte, fällt bei Startups per definitionem weg: Sie haben keine bestehenden IT-Systeme und Mitarbeiter, die durch den Einsatz von Cloud-Services obsolet werden können (Kriterium 1 und 4). Somit kann nicht die Situation eintreten, dass der Weiterbetrieb bestehender – und bereits bezahlter – IT-Systeme wirtschaftlicher sein könnte, als der Einsatz von Cloud-Services. Ebenso spielt die Kompatibilität mit bestehenden IT-Systemen (Kriterium 3) keine Rolle. Sofern sie nicht als GmbH (oder AG) gegründet wurden, bestehen für Startups auch keine gesetzlichen Kontrollpflichten der Geschäftsleitung (Kriterium 14), sodass sich auch für Kernprozesse keine diesbezügliche Einschränkung ergibt. Startups haben darüber hinaus am ehesten die Möglichkeit, beim Aufbau von Datenbanken, die personenbezogene Daten beinhalten, – primär ist hier an Kundendatenbanken zu denken – von vorn herein die Zustimmung jedes einzelnen Betroffenen zur Verarbeitung seiner Daten im Rahmen eines Cloud-Service einzuholen (Kriterium 12.2). Dies kann beispielsweise im Zuge von Anmeldeformularen o.ä. erfolgen. Allerdings eignen sich bei Weitem nicht alle Datensammlungen für ein solches Vorgehen, man denke nur an Einträge zukünftiger Kunden, mit denen man noch keinen Vertrag abgeschlossen hat.

Bei Startup-Unternehmen kommen auch die wesentlichen Stärken des Cloud Computing am deutlichsten zum Tragen. Zu nennen sind hier zunächst die Flexibilität und die damit verbundene Vermeidung von Fixkosten. Dies ist besonders wichtig, wenn der Erfolg des Unternehmens, dessen Wachstum und damit der Bedarf an IT-Ressourcen in der Gründungsphase nicht vorhergesagt werden können (Kriterium 8). Für den Einsatz von Cloud-Services spricht gerade bei Startups auch die dadurch bewirkte Fokussierung auf das Kerngeschäft. Nicht zuletzt kann sich dabei der in Kriterium 5.1 beschriebene Effekt einstellen, dass die Informationssicherheit und Zuverlässigkeit durch den Einsatz von Cloud-Services erhöht wird, denn Nicht-IKT-Startups sind wohl von allen Unternehmensklassen am meisten gefährdet, die Informationssicherheit aus Mangel an finanziellen Mitteln, Zeit und Verständnis zu vernachlässigen.

Zuletzt ist auf die unter dem Titel „Neue Möglichkeiten“ (Punkt 4.1.5, S. 72) erwähnten Gesichtspunkte hinzuweisen, die für Startups besonders relevant sind. Beispielsweise können Nicht-IKT-Startups mittels Cloud Computing IT-Systeme einsetzen, deren Professionalitätsniveau bisher größeren Unternehmen vorbehalten war.

Nach so viel Positivem müssen allerdings an dieser Stelle die in Abschnitt 4.2 (S. 74) beschriebenen potenziellen negativen Konsequenzen der Nutzung von Cloud-Services – Abhängigkeit von einzelnen Anbietern oder von externer Leistungserbringung (im Allgemeinen), Kontrollverlust (über Systeme und Daten) etc. – auch noch einmal in Erinnerung gerufen werden.

Für Nicht-IKT-Startups sind zwei Gruppen von Cloud-Services besonders geeignet, SaaS im Allgemeinen[459] sowie IaaS für das spezifische Aufgabengebiet der Datensicherung. Andere Anwendungsfälle für IaaS wird es in dieser Unternehmensklasse hingegen in der Regel nicht geben, weil sowohl der Bedarf als auch das dazu benötigte Know-how fehlt. PaaS kann zusätzlich – abhängig vom Unternehmensgegenstand – zum Hosting von Webanwendungen in Frage kommen, sofern deren Entwicklung und Betrieb nicht insgesamt an externe Dienstleister ausgelagert ist. Der Bedarf nach SaaS hängt zum Teil von der Branche ab, zum Teil ist dieser branchenübergreifend. Ein Office-Paket wie z.B. *Google Apps*[460] benötigen die meisten Unternehmen, viele auch eine Art von Kundenverwaltung für die Kernprozesse Vertrieb und Marketing, wenngleich es insbesondere bei kleinen Unternehmen nicht immer eines umfassenden CRM-Systems wie *Salesforce CRM*[461] bedarf. Doch insbesondere bei SaaS tritt für österreichische Unternehmen die Datenschutzproblematik zutage, sobald personenbezogene Daten involviert sind (Kriterium 12). Letzteres ist bei einer Kundenverwaltung definitiv der Fall und auch die Nutzung eines Office-Pakets kann personenbezogene Daten umfassen. Es liegt allerdings in der Natur der Sache, dass die Daten vor der Verwendung im Rahmen eines solchen Cloud-Service nicht verschlüsselt oder pseudonymisiert werden können (Kriterium 12.1). Die Daten werden vielmehr im Klartext, in der Regel im Webbrowser eingegeben oder aus bestehenden Dateien hochgeladen und auf den Servern des Anbieters verarbeitet und gespeichert.

Für die datenschutzrechtskonforme Nutzung der beiden untersuchten SaaS-Angebote – und wahrscheinlich aller SaaS-Angebote, die nicht spezifisch auf das österreichische Datenschutzrecht ausgerichtet sind (Kriterium 12.3) – ist daher die Zustimmung aller Betroffenen erforderlich (Kriterium 12.2), wenn personenbezogene Daten involviert sind. Diese Zustimmung wird zwar – wie oben erwähnt – am ehesten noch

[459] BITKOM 2009, 57.
[460] Siehe dazu Abschnitt 5.7, S. 111.
[461] Siehe dazu Abschnitt 5.6, S. 105.

von Startups systematisch eingeholt werden können, weil diese am Beginn keine bestehenden Daten besitzen, vielfach wird dies aber nicht möglich sein.

Anders verhält es sich mit dem zweiten für Nicht-IKT-Startups besonders geeigneten Anwendungsgebiet, der Datensicherung mittels IaaS, denn diese ist problemlos mit Verschlüsselung kombinierbar. Datenschutzprobleme und der Verlust der Kontrolle über die Daten spielen keine Rolle, wenn diese mit ausreichend sicheren Verfahren verschlüsselt wurden. Die Datensicherung kann entweder direkt mittels IaaS-Angeboten wie *Amazon S3*[462] durchgeführt werden, oder mittels Lösungen von Drittanbietern, die auf IaaS aufsetzen.[463] IaaS eignet sich für Startups auch deswegen so gut zur Datensicherung, weil diese meist nur einen einzigen Standort haben und die Daten dadurch an einem unabhängigen Ort gesichert sind.

6.2.2. IKT-Startups

Für IKT-Startup-Unternehmen trifft das im vorhergehenden Punkt allgemein über Startups Gesagte ebenfalls zu. Auch die dort genannten geeigneten Anwendungsgebiete für Cloud Computing – einerseits SaaS für Kern- und Supportprozesse, vorbehaltlich der Datenschutzproblematik, und andererseits Datensicherung mittels IaaS – gelten ebenso für diese Unternehmensklasse. Da in dieser Klasse die IT zu den Kernprozessen gehört, wird es darüber hinaus viele Aufgabengebiete geben, in denen PaaS und IaaS eingesetzt werden können, um die unternehmensinternen Ressourcen für die Entwicklung des eigentlichen Produkts bzw. der eigentlichen Dienstleistung zu bündeln (Fokussierung). In Unternehmen der IKT-Branche wird auch das zur Nutzung von IaaS benötigte Know-how vorhanden sein.

Gerade IKT-Startups können sich die nahezu unbegrenzten Ressourcen zunutze machen, die mittels IaaS zu perfekt skalierenden, nutzungsabhängigen Kosten zur Verfügung stehen. Konkrete Einsatzgebiete von IaaS können etwa Content-Delivery oder komplexe, zeitkritische Berechnungsaufgaben[464] sein, sofern sich diese zur Parallelisierung eignen. In diesen Gebieten existieren auch viele Einsatzgebiete, die keine personenbezogenen Daten umfassen. Für Content-Delivery – insbesondere Audio- und Videostreaming – bieten Cloud-Services wie *Amazon S3*[465] spezifische Funktionalität, allerdings muss hier auf die Kosten für Datenspeicherung und -transfer besonders geachtet werden (Kriterium 10). Im günstigsten Fall werden diese ebenfalls in Form von nutzungsabhängigen Kosten an den Kunden überwälzt.

---

462 Siehe dazu Punkt 5.1.2, S. 85.
463 Siehe dazu etwa Velte, Velte und Elsenpeter 2009, 19.
464 Armbrust et al. 2009, 7.
465 Siehe dazu Punkt 5.1.2, S. 85.

Wenn Webanwendungen zu den Kernprozessen eines IKT-Startups gehören, eignet sich für diese der Einsatz von PaaS. Besondere Stärken solcher Lösungen sind primär ebenfalls die rasche Verfügbarkeit, die tendenziell höhere Professionalität im Vergleich zu interner Leistungserbringung in Startups und die Vermeidung von Fixkosten, was Startups aufgrund der schlechten Vorhersehbarkeit des Kundeninteresses und damit der Nutzungsintensität ihrer Webanwendungen besonders entgegenkommt. Bei Webanwendungen von IKT-Startups besteht zudem eine besonders gute Möglichkeit, im Rahmen von Web-Formularen die datenschutzrechtlich notwendige Zustimmung der Betroffenen einzuholen, wenn diese personenbezogene Daten im Rahmen der Nutzung der Webanwendung angeben.

Oben wurde bereits auf die „neuen Möglichkeiten" hingewiesen, die Cloud Computing insbesondere für Startups bietet. „Neue Möglichkeiten" ergeben sich speziell für IKT-Startups durch Cloud Computing auch insofern, als dieses neue Geschäftsideen und -modelle eröffnet, welche die Neugründung von Unternehmen erst auslösen bzw. ermöglichen.

6.2.3. Nicht-IKT-KMU

In bestehenden Unternehmen fallen viele der Faktoren weg, die den Einsatz von Cloud-Services für Startups so attraktiv machen. Insbesondere bestehen einerseits bereits IT-Systeme und andererseits meist auch Datenbanken, die personenbezogene Daten beinhalten, für welche die Zustimmung der Betroffenen zur Verarbeitung im Rahmen eines Cloud-Service nicht vorliegt und nur schwer nachträglich eingeholt werden kann. Werden allerdings neue Geschäftsfelder eröffnet, können Bedingungen vorliegen, die jenen eines Startups gleichkommen.

Allerdings unterliegen auch viele KMU aufgrund ihrer Größe ähnlichen Einschränkungen wie Startups – hinsichtlich der Ressourcen, der internen Möglichkeiten und des internen Know-hows (Kriterium 4). Die Fokussierung auf das Kerngeschäft, die durch SaaS ermöglicht wird, macht solche Cloud-Services daher auch in dieser Unternehmensklasse attraktiv. Bezüglich des Datenschutzes gilt das bereits bei den Startup-Unternehmen Gesagte, mit der Einschränkung, dass es bestehenden Unternehmen in der Regel besonders schwer fallen wird, die Zustimmung aller Betroffenen einzuholen, also etwa aller Kunden bei Verlagerung der Kundendatenbank in ein System wie *Salesforce CRM*[466].

[466] Siehe dazu Abschnitt 5.6, S. 105.

6.2.4. IKT-KMU

IKT-KMU können IaaS und PaaS grundsätzlich für ähnliche Aufgabengebiete einsetzen wie IKT-Startups. Für SaaS gilt in dieser Klasse das soeben über Nicht-IKT-KMU Gesagte. Im Vergleich zu Startups haben IKT-KMU allerdings in der Regel mehr Möglichkeiten (Ressourcen, Know-how) zur unternehmensinternen Leistungserbringung (Kriterium 4). Für Unternehmen dieser Klasse ist daher die Abwägung, in welchem Ausmaß für die IT-Kernprozesse IaaS und PaaS herangezogen werden sollen, besonders schwierig. Vielfach werden IKT-KMU bei interner Leistungserbringung ein höheres Informationssicherheits- und Zuverlässigkeitsniveau gewährleisten können als (die untersuchten) Cloud-Services. Auch die beschrieben Datenschutzprobleme können bei interner Leistungserbringung nicht auftreten. Hingegen bieten Cloud-Services im Vergleich dazu mehr Flexibilität und können kostengünstiger sein. Welche Aspekte überwiegen, muss anhand der Gegebenheiten des Einzelfalls entschieden werden.

Fällt die Entscheidung in einem Aufgabengebiet für unternehmensinternen Betrieb der Infrastruktur, können Cloud-Services als Ergänzung zum Zwecke der bedarfsgerechten Abfederung von Lastspitzen eingesetzt werden. Zu denken ist dabei insbesondere an Webanwendungen, bei deren drohender Überlastung zusätzliche Server in einem Cloud-Service gestartet werden. Je nach Aufgabengebiet kann dies entweder mittels IaaS oder mittels PaaS erfolgen. Dieses Vorgehen ist selbstverständlich nur möglich, wenn die ursprüngliche Entscheidung gegen den Einsatz eines Cloud-Service nicht aus Gründen des Datenschutzes oder der Informationssicherheit gefallen ist (Kriterien 5 und 12).

Ein Einsatzgebiet von IaaS und PaaS, das mit zunehmender Komplexität der Produkte und Dienstleistungen von IKT-Unternehmen besonders zum Tragen kommt ist die Software-Entwicklung. Um rasch einen Prototypen einer bestimmten Idee zu Demonstrationszwecken zu implementieren, eignen sich Cloud-Services hervorragend, unabhängig davon, ob die fertige Lösung letztlich auf internen Ressourcen oder in der Cloud betrieben werden wird.

Im Bereich der Supportprozesse bietet sich ab einer gewissen Unternehmensgröße der Einsatz von SaaS zur Online-Zusammenarbeit an. Dies schließt auch die mobilen bzw. standortübergreifenden Verwendungsmöglichkeiten vieler SaaS-Angebote mit ein (Kriterium 11). Auch hier muss allerdings wieder auf das Datenschutzrecht hingewiesen werden.

6.2.5. Nicht-IKT-Großunternehmen

Die meisten Banken und Versicherungen sowie ein Teil der Wertpapierdienstleistungsunternehmen fallen in die Kategorie der Nicht-IKT-Großunternehmen. Diese Unternehmen unterliegen branchenspezifischen Bestimmungen, die in Abschnitt 3.3 (S. 60) behandelt wurden (Kriterium 13). Dort wurde bereits der Schluss gezogen, dass Cloud-Services in diesen Unternehmen aufgrund dieser Bestimmungen nur für betrieblich unwesentliche Einsatzgebiete verwendet werden können. Für die Kernprozesse dieser Unternehmen, die aufgrund der Spezifika der Branchen wohl ausnahmslos personenbezogene Daten beinhalten, ist Cloud Computing somit nicht geeignet.

Auch für alle übrigen Unternehmen dieser Klasse eignet sich der Einsatz von Cloud-Services für betrieblich bedeutende Aufgabengebiete in der Regel nicht. Ein wichtiger Grund dafür sind neben dem bereits ausführlich besprochenen Datenschutzrecht, welches insbesondere – aber nicht ausschließlich – im Zusammenhang mit SaaS relevant ist, in großen Unternehmen die Kontrollpflichten der Geschäftsleitung (Kriterium 14). Dies betrifft auch die Datensicherung, da diese eine betrieblich sehr wichtige Aufgabe ist. Zudem kann in großen Unternehmen – abhängig vom zu sichernden Datenvolumen – die Datensicherung mittels IaaS im Vergleich zur unternehmensinternen Datensicherung ohnehin unwirtschaftlich sein.

Überdies ist zu berücksichtigen, dass Cloud-Services per definitionem Standardlösungen sind. Insbesondere Großunternehmen bedürfen aber möglicherweise individueller Lösungen, welche die Anforderungen besser erfüllen als Cloud-Services, und haben auch am ehesten die Ressourcen dafür.

Ein Aufgabengebiet, das für den Einsatz von Cloud-Services gut geeignet ist, gibt es aber auch in dieser Unternehmensklasse: Business Intelligence, also die – oftmals sehr ressourcenintensive – Analyse von gesammelten Daten aller Art zum Zwecke der Entscheidungsunterstützung.[467] Diese kann durch den Einsatz von IaaS (oder Paas) einerseits beschleunigt werden und andererseits können aufgrund der Flexibilität des Cloud Computing die damit verbundenen Kosten gesenkt werden. Es bestehen aber Einschränkungen, insbesondere aufgrund des Datenschutzrechts. Business Intelligence ist allerdings ein Aufgabengebiet, das in vielen Fällen auch mit pseudonymisierten Daten durchgeführt werden kann, womit dem Datenschutz Genüge getan ist. Unter Pseudonymisierung versteht man das Ersetzen der Namen der betroffenen Personen in den Datensätzen durch eindeutige Nummern, Buchstabenkombinationen o.Ä. (Kriterium 12.1). Eine weitere Einschränkung ist grundsätzlicher Natur und betrifft die Ent-

[467] Armbrust et al. 2009, 7

scheidung, ob die zu analysierenden Daten nicht zu wertvoll sind, um sie aus der Hand zu geben (Kriterium 6).

6.2.6. IKT-Großunternehmen

Das soeben allgemein über Großunternehmen Gesagte lässt sich auch auf diese Unternehmensklasse übertragen. Hinzu kommt, dass sich IKT-Großunternehmen in der Regel durch hohen Bedarf an IT-Ressourcen, umfangreiche bestehende IT-Systeme und ein hohes Maß an unternehmensintern verfügbarem Know-how auszeichnen. Diese Voraussetzungen sprechen grundsätzlich gegen die Einführung von Cloud-Services als Ersatz für bestehende Systeme, denn ein hoher Ressourcenbedarf, dem das Potenzial gegenübersteht, diesen unternehmensintern zu decken, lässt den Einsatz von Cloud-Services im Allgemeinen unwirtschaftlich erscheinen. IKT-Großunternehmen haben von allen Klassen auch die besten Voraussetzungen, Private Clouds zu betreiben und somit einige der Stärken des Cloud Computing zu nutzen, ohne dessen größten Schwächen – Kontrollverlust, Einschränkungen wegen des Datenschutzrechts etc. – ausgesetzt zu sein.

Es gibt allerdings auch in dieser Unternehmensklasse Aufgabengebiete, in denen sich die Nutzung von Cloud-Services besonders eignet. Zu nennen ist zunächst der bereits im Zusammenhang mit IKT-KMU erwähnte Einsatz von Cloud-Services als Ergänzung zu unternehmensinternen Systemen zur Abfederung von Lastspitzen. Ebenso wurde für die Klasse der IKT-KMU das Potenzial von IaaS und PaaS für rasche Test-Entwicklungen und Prototypen zu Demonstrationszwecken bereits angesprochen. In IKT-Großunternehmen mit starren Strukturen kommt dies noch stärker zum Tragen. Es ist sogar denkbar, dass sich aus Experimenten mit Cloud-Services durch einzelne Mitarbeiter neue innovative Lösungen oder Geschäftsfelder entwickeln, die ohne die anfänglichen Experimente nie entstanden wären. Diese Leichtigkeit, mit Cloud-Services zu experimentieren, ist es, die im Zitat am Anfang dieses Kapitels angesprochen wurde.

7. Testprojekt zum praktischen Einsatz von Cloud-Services

Um Erfahrungen im praktischen Einsatz von Cloud-Services zu gewinnen und dem Leser vermitteln zu können, führte der Autor im Zuge der vorliegenden Diplomarbeit gemeinsam mit Roman Fenkhuber, Student der technischen Informatik, ein Testprojekt durch. Nachfolgend werden Konzept und Umsetzung dieses Projekts beschrieben.

7.1. Aufgabenstellung

Die primären Ziele des Projekts waren, Erfahrung im praktischen Einsatz von Cloud Computing zu sammeln, mehrere Cloud-Services zu testen und Verständnis für die technischen Hintergründe des Cloud Computing, insbesondere für die Virtualisierung zu gewinnen. Letzteres sollte dadurch erreicht werden, dass in Ansätzen auch eine Private Cloud aufgesetzt werden und das Gesamtprojekt letztlich in einer Hybrid Cloud ablaufen sollte.[468] Der Inhalt des Projekts war somit nur insofern von Bedeutung, als er für die Umsetzung dieser Anforderungen geeignet sein musste. Die Suche nach einem geeigneten Projektinhalt erwies sich allerdings als schwierige Aufgabe.

Schließlich wurde die verteilte Kompilierung von *Optware*[469], einem *Linux*-Erweiterungs- und -Paketverwaltungssystem, für eine spezielle Hardware-Plattform als Testprojekt ausgewählt. *Optware* dient der Erweiterung der *Linux*-Distribution *NSLU2-Linux*[470], die ursprünglich von der Open-Source-Community als alternatives Betriebssystem für das Network-Attached-Storage-Gerät *NSLU2* des Herstellers *Linksys* bzw. *Cisco Systems* konzipiert wurde, um dieses Gerät zu einem vollwertigen Server zu machen. Mittels *Optware* ist es möglich, *NSLU2-Linux* eine große Auswahl von Softwarepaketen hinzuzufügen, sodass es für nahezu jeden beliebigen Zweck einsetzbar ist. Mittlerweile wurden *NSLU2-Linux* und *Optware* für viele weitere schlanke Nicht-x86-Plattformen portiert. Im Zuge des Projekts sollte diesen Plattformen eine weitere hinzugefügt werden, indem alle verfügbaren *Optware*-Pakete für die Plattform *WD TV Live HD Media Player*[471] (im Folgenden *WD-TV*-Plattform) kompiliert werden sollten. Nach Wissensstand des Autors wurde *Optware* bisher noch nicht für diese Plattform portiert, sondern lediglich für das Vorgängermodell *WD TV HD Media Player*.[472]

---

[468] Zu den Begriffen Private Cloud und Hybrid Cloud siehe Tabelle 2, S. 32.
[469] Siehe dazu http://www.nslu2-linux.org/wiki/Optware/HomePage (Zugriff am 19. September 2010).
[470] Siehe dazu http://www.nslu2-linux.org (Zugriff am 25. September 2010).
[471] Siehe dazu http://www.wdc.com/en/products/Products.asp?DriveID=734 (Zugriff am 19. September 2010).
[472] Siehe dazu http://b-rad.cc/optware-for-wdtv (Zugriff am 25. September 2010).

Selbstverständlich erfordert diese Aufgabe nicht zwingend die Nutzung von Cloud-Services, sondern kann auch auf einem einzelnen Rechner durchgeführt werden. Allerdings kann IaaS für diese Aufgabe sehr gut eingesetzt werden, denn sie eignet sich zur Parallelisierung, da die verschiedenen *Optware*-Pakete weitgehend unabhängig voneinander kompiliert werden können. Genau genommen bestehen bei der Kompilierung zwar zum Teil Abhängigkeiten zwischen den einzelnen Paketen, die Aufgabe wurde allerdings so gelöst, dass diese Abhängigkeiten nur geringfügen Einfluss auf die Gesamtdauer der Kompilierung hatten, das Endergebnis aber nicht beeinflussen konnten.

Da der Prozessor der *WD-TV*-Plattform nicht wie die Prozessoren der kompilierenden Systeme auf der x86-Architektur basiert, musste ein Cross-Compiler verwendet werden – ein Compiler, der selbst auf der x86-Architektur läuft, aber Programme erstellt, die auf der Zielplattform laufen. Dadurch wurde das Konfigurieren der Kompilierungsumgebung und des Kompiliervorgangs sehr aufwändig. Da hier jedoch die Verwendung von Cloud-Services im Vordergrund steht, wird auf die Details der Kompilierung nicht näher eingegangen.

7.2. Projektablauf

Die Kompilierung sollte im Detail folgendermaßen ablaufen: Virtuelle Server (im Folgenden als „Workernodes“ bezeichnet) fragen bei einer zentralen Instanz (im Folgenden als „Jobdispatcher“ bezeichnet) nacheinander jeweils den Namen eines Paktes ab, das noch nicht kompiliert wurde. Daraufhin laden sie sich den Quellcode dieses Pakets von der *Optware*-Projekt-Website[473] auf einen gemeinsam genutzten Fileserver herunter und beginnen, das Paket zu kompilieren. Bestehen für die Kompilierung Abhängigkeiten in der Form, dass andere Pakete vor dem aktuellen Paket kompiliert werden müssen, und liegen diese Pakete noch nicht auf dem von allen Workernodes gemeinsam genutzten Fileserver, werden die benötigten Pakte automatisch vorher kompiliert. Durch die Verwendung eines gemeinsam genutzten Fileservers wird verhindert, dass im Falle solcher Abhängigkeiten von verschiedenen Workernodes dasselbe Paket mehrfach kompiliert wird. Hat ein Workernode ein Paket fertig kompiliert, kopiert er das Ergebnis auf einen lokal betriebenen (physischen) Server, sodass sich nach der Beendigung des Projekts und dem Stoppen aller virtuellen Server alle kompilierten *Optware*-Pakete auf dem lokalen Server befinden.

[473] http://ipkg2.nslu2-linux.org/sources (Zugriff am 22. September 2010).

7.3. Projektkonfiguration

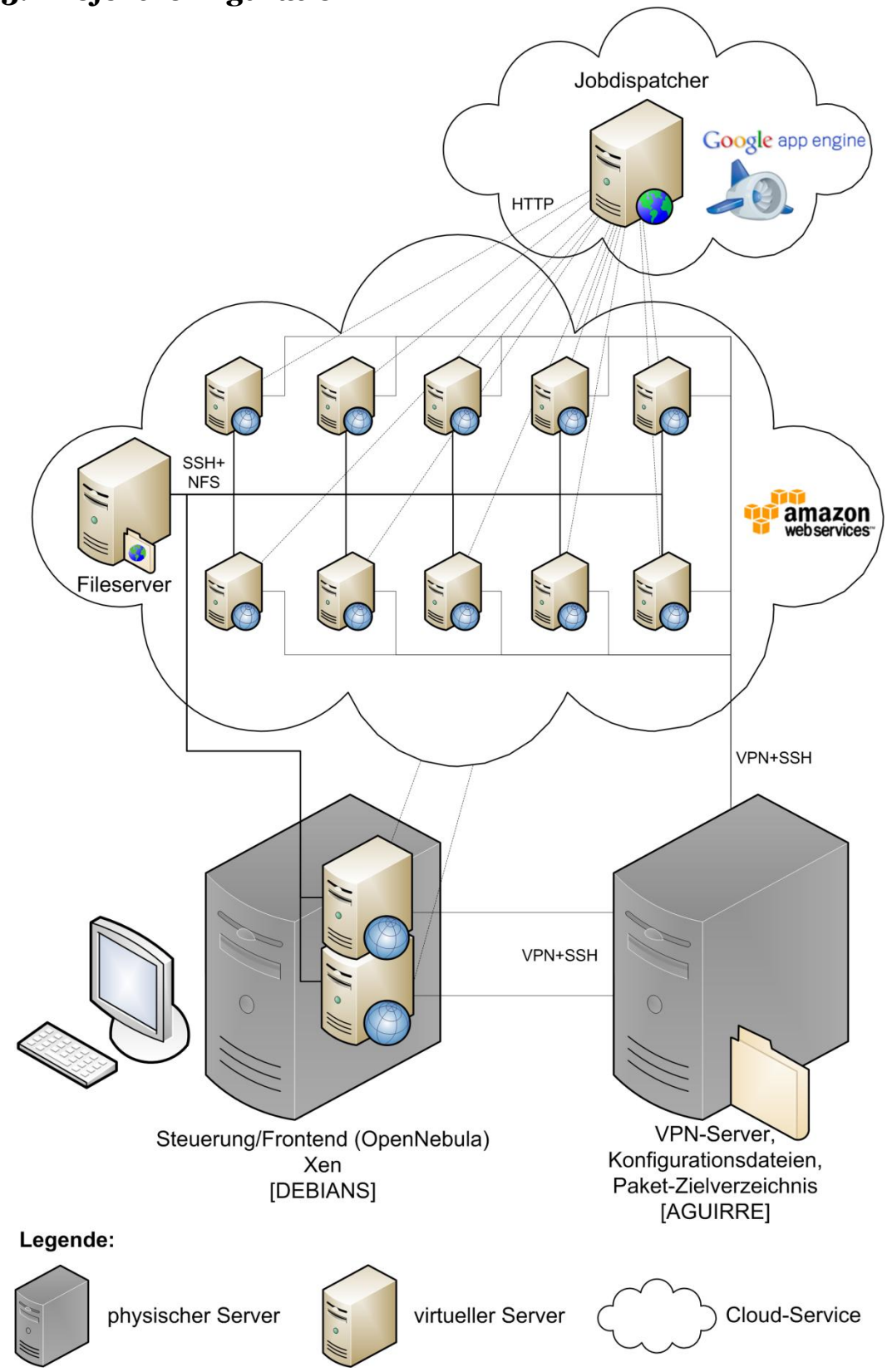


Abbildung 17 – Schematische Darstellung der Projektkonfiguration[474]

[474] Quelle: Eigene Darstellung.

Vorausgeschickt werden muss, dass die Aufgabe bewusst aufwändig gelöst wurde, da die Nutzung von Cloud-Services und Virtualisierung – nicht die effiziente Zielerreichung – im Vordergrund standen. Die resultierende Projektkonfiguration ist in Abbildung 17 dargestellt.

Als lokale und persistente „Basis" der Projektinfrastruktur dienten zwei (physische) Server, mit den Hostnamen „AGUIRRE" und „DEBIANS". AGUIRRE besaß als einziger involvierter Server eine öffentliche, fixe IP-Adresse und diente als VPN-Server und persistenter Fileserver, mit dem alle Workernodes unmittelbar nach dem Starten eine VPN-Verbindung aufbauten. Über diese Verbindung luden sie dann ein in Python programmiertes Client-Programm herunter, führten dieses aus und begannen damit als Workernodes zu arbeiten. Auf AGUIRRE wurden zudem die fertig kompilierten *Optware*-Pakete gesammelt.

DEBIANS verfügte als einziger involvierter Server über Bildschirm und Tastatur und diente somit einerseits der Steuerung des gesamten Projekts. Andererseits wurde auf DEBIANS die Virtualisierungslösung *Xen*[475] aufgesetzt, die übrigens auch von *Amazon* für *EC2* eingesetzt wird. Mittels *Xen* wurden auf DEBIANS zwei virtuelle Server als Workernodes zur Kompilierung betrieben. Zur Steuerung des Projekts war auf DEBIANS das Cloud-Computing-Framework *OpenNebula*[476] installiert. Durch Konsolen-Befehle können mittels *OpenNebula* virtuelle Server sowohl lokal als auch in *EC2* sehr einfach gestartet und verwaltet werden.

Im Rahmen des Projekts wurden drei der in Kapitel 5 untersuchten Cloud-Services verwendet, *Amazon EC2*, *Amazon S3* und *Google App Engine*. In *Amazon EC2* wurden insgesamt elf virtuelle Server gestartet. Zehn davon übernahmen in der Rolle als Workernodes neben den lokalen virtuellen Servern auf DEBIANS den Großteil der Kompilierung. Für diese *EC2*-Workernodes wurden Instanzen des Typs „Small" verwendet. Der elfte virtuelle Server diente allen Workernodes als Fileserver zum Speichern des heruntergeladenen Quellcodes und der aufgrund der beschriebenen Abhängigkeiten von anderen Workernodes benötigten Daten. Aufgrund der erhöhten Bandbreitenanforderungen wurde für den Fileserver der Instanzentyp „Large" verwendet. Abbildung 18 zeigt die elf Instanzen während der Startphase im Web-Interface von *EC2*. In Abbildung 19 sind die laufenden Instanzen im Plug-in *Elasticfox*[477] für *Mozilla Firefox* zu sehen.

---

475 Siehe dazu http://www.xen.org (Zugriff am 22. September 2010).
476 Siehe dazu http://www.opennebula.org (Zugriff am 22. September 2010).
477 Siehe dazu http://developer.amazonwebservices.com/connect/entry.jspa?externalID=609 (Zugriff am 22. September 2010).

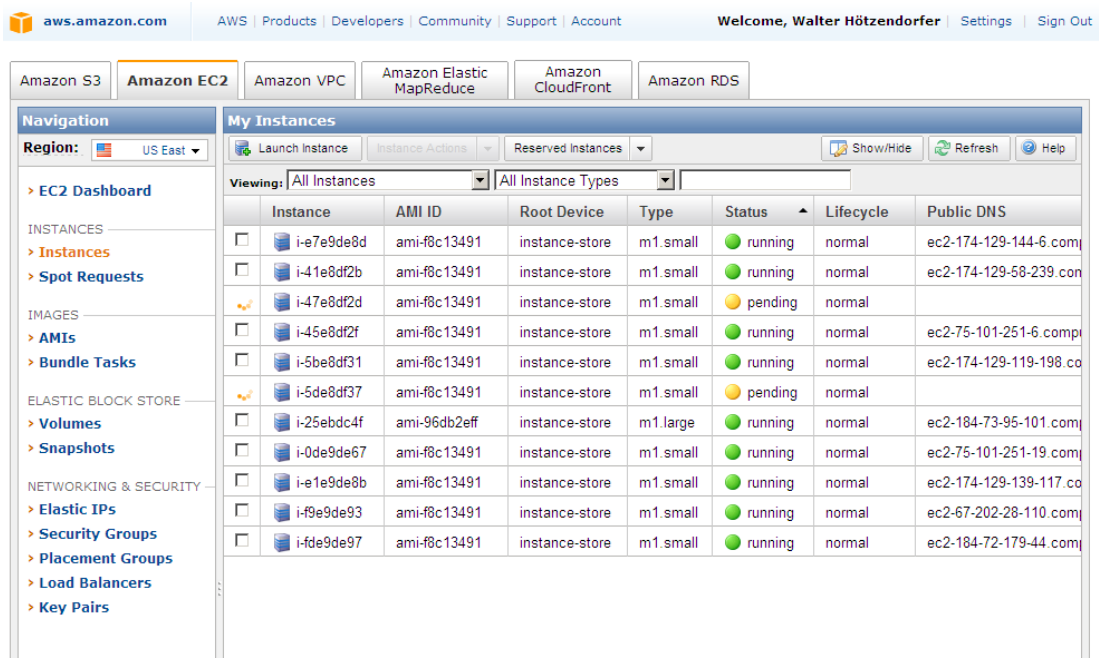


Abbildung 18 – Web-Interface von *Amazon EC2* mit neun laufenden und zwei startenden Instanzen[478]

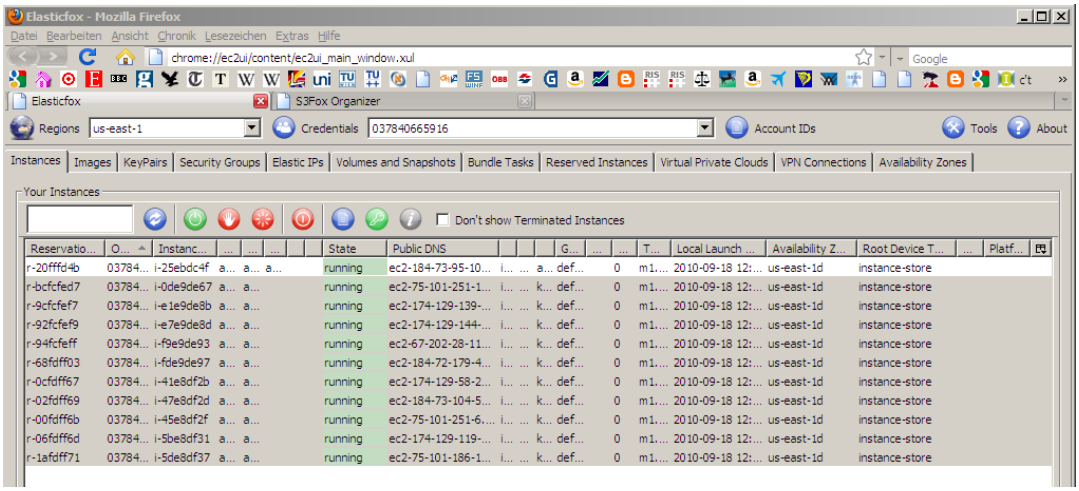


Abbildung 19 – *Mozilla-Firefox*-Plug-in *Elasticfox* mit elf laufenden *Amazon-EC2*-Instanzen[479]

Als Betriebssystem aller verwendeten realen wie auch virtuellen Server mit Ausnahme des Jobdispatchers wurde *Debian GNU/Linux 5.0* („*Lenny*“) eingesetzt. Für den Fileserver wurde ein fertiges, bei *EC2* verfügbares Image verwendet, für die Workernodes wurde hingegen ein eigenes Image zusammengestellt, das so konfiguriert war, dass nach dem Starten automatisch – wie oben beschrieben – die VPN-Verbindung zu AGUIRRE hergestellt und mittels des heruntergeladenen Client-Programms die Tätigkeit als Workernode aufgenommen wurde. Für die *EC2*-Workernodes wurde dieses

[478] Quelle: Screenshot von http://aws.amazon.com (erstellt am 18. September 2010).
[479] Quelle: Screenshot von *Elasticfox* (erstellt am 18. September 2010).

Image mit Hilfe der so genannten *EC2-AMI-Tools* für *Amazon EC2* vorbereitet[480] und in *Amazon S3* hochgeladen. Dies war Voraussetzung, um das Image für *EC2*-Instanzen einsetzen zu können. Abbildung 20 zeigt das Image im Web-Interface von *S3*. In *S3* war darüber hinaus die Kompilierungsumgebung („Toolchain“) gespeichert, die vor Beginn des Kompilierens von jedem Workernode heruntergeladen wurde.

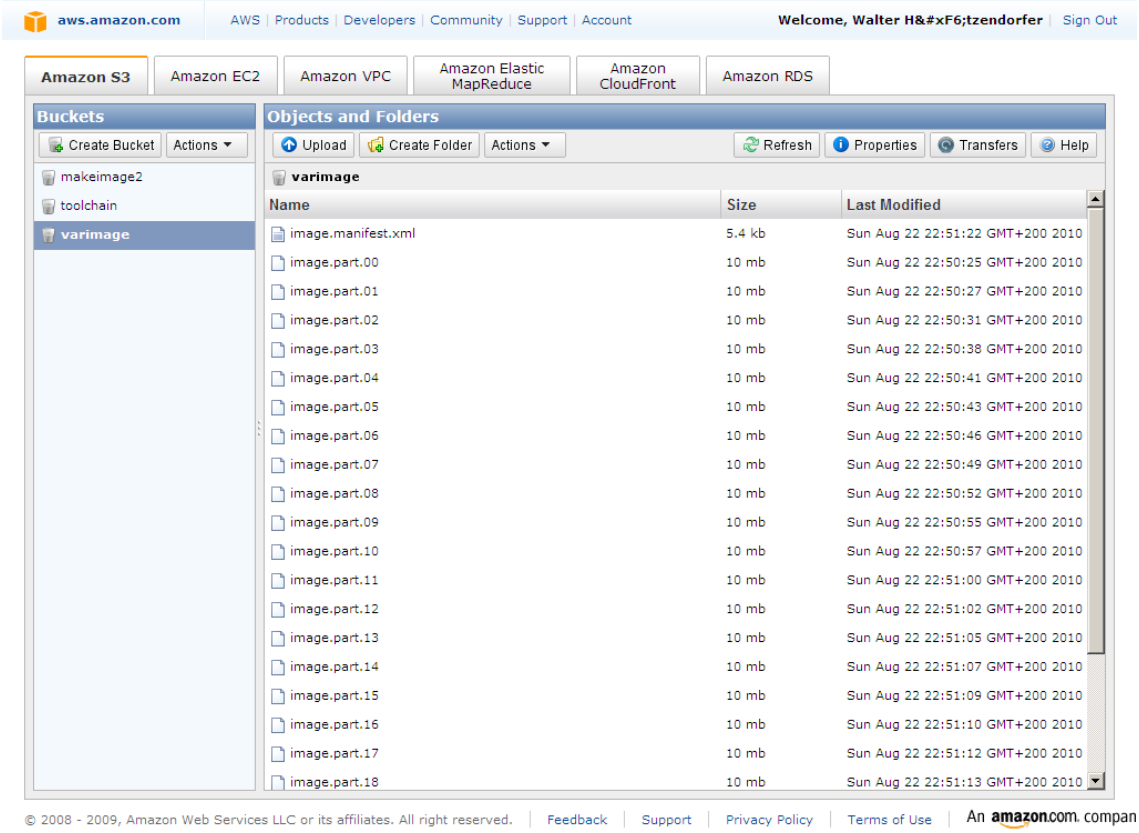


Abbildung 20 – Web-Interface von *Amazon S3* mit gespeichertem Image für *EC2*[481]

Wie bereits erwähnt, wurde die Kompilierung von einem Jobdispatcher koordiniert, der entsprechende HTTP-Anfragen eines Workernodes mit der Rückgabe des Namens eines noch nicht kompilierten Pakets beantwortete, das der Workernode kompilieren sollte. Dieser Jobdispatcher wurde in Python programmiert und in *Google App Engine* betrieben. Seine Funktionalität umfasste das Hochladen einer Liste der Namen von zu kompilierenden Paketen, das erwähnte Abrufen von Paketnamen, ein Fehlermanagement und ein Logging-System. Letzteres empfing und verarbeitete Statusmeldungen der Workernodes. In Abbildung 21 ist die Jobdispatcher-Webanwendung namens „wdtv-live-optware“ im *Google-App-Engine*-Account des Autors zu sehen. Darunter ist in Abbildung 22 der „Datastore Viewer“ der Anwendung abgebildet, welcher die Tabelle

[480] Aus dem *Linux*-Image wurde ein so genanntes „Amazon Machine Image“ erzeugt. Siehe dazu http://docs.amazonwebservices.com/AWSEC2/latest/DeveloperGuide/index.html?creating-an-ami-s3-linux.html (Zugriff am 22. September 2010).

[481] Quelle: Screenshot von http://aws.amazon.com (erstellt am 22. September 2010).

der zu diesem Zeitpunkt zur Kompilierung vergebenen Pakete zeigt. In Abbildung 23 ist die Nutzungsstatistik des Jobdispatchers während des Projektdurchlaufs im so genannten „Dashboard“ der Anwendung dargestellt.

Abbildung 21 – *Google-App-Engine*-Account des Autors mit der Jobdispatcher-Webanwendung[482]

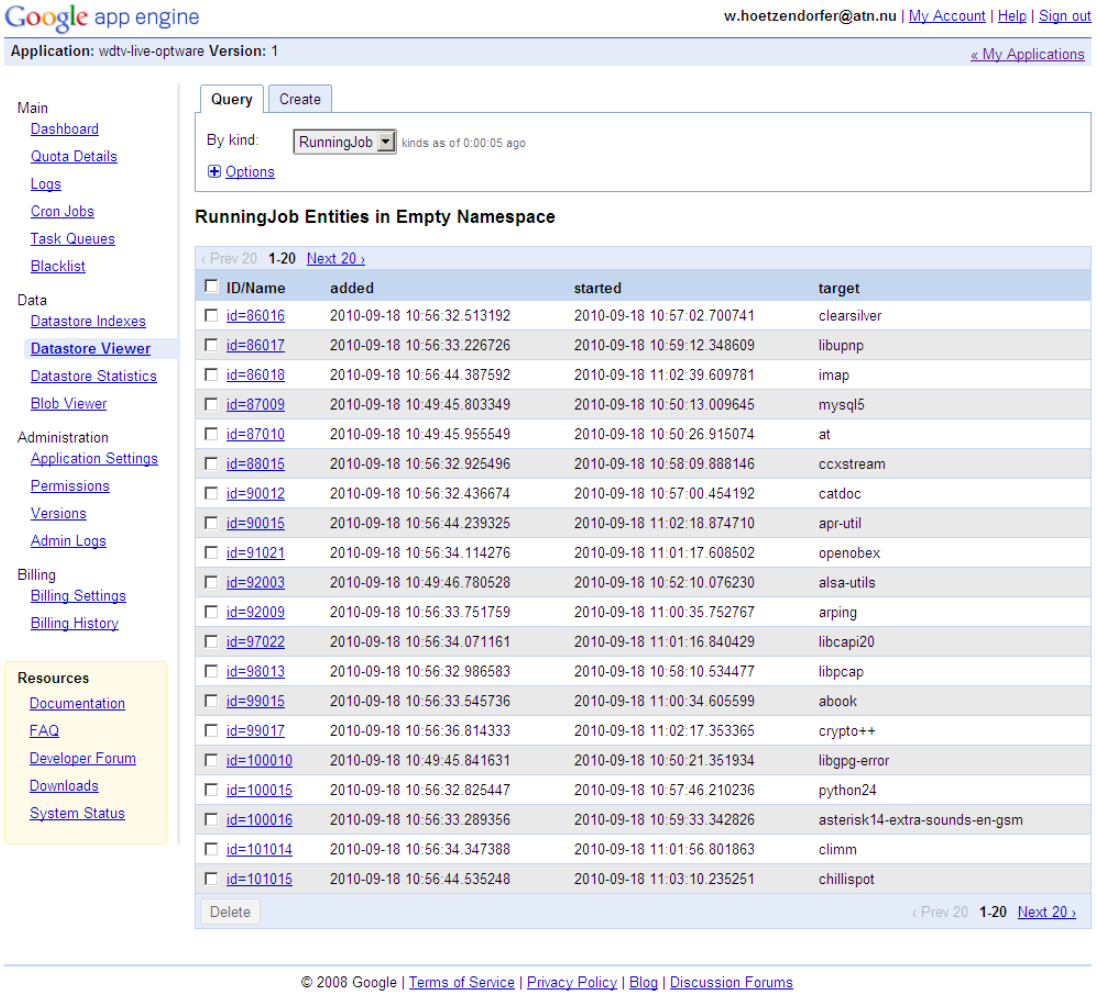


Abbildung 22 – „Datastore Viewer“ mit Tabelle der zu diesem Zeitpunkt zur Kompilierung vergebenen Pakete[483]

[482] Quelle: Screenshot von https://appengine.google.com (erstellt am 16. August 2010).
[483] Quelle: Screenshot von https://appengine.google.com (erstellt am 18. September 2010).

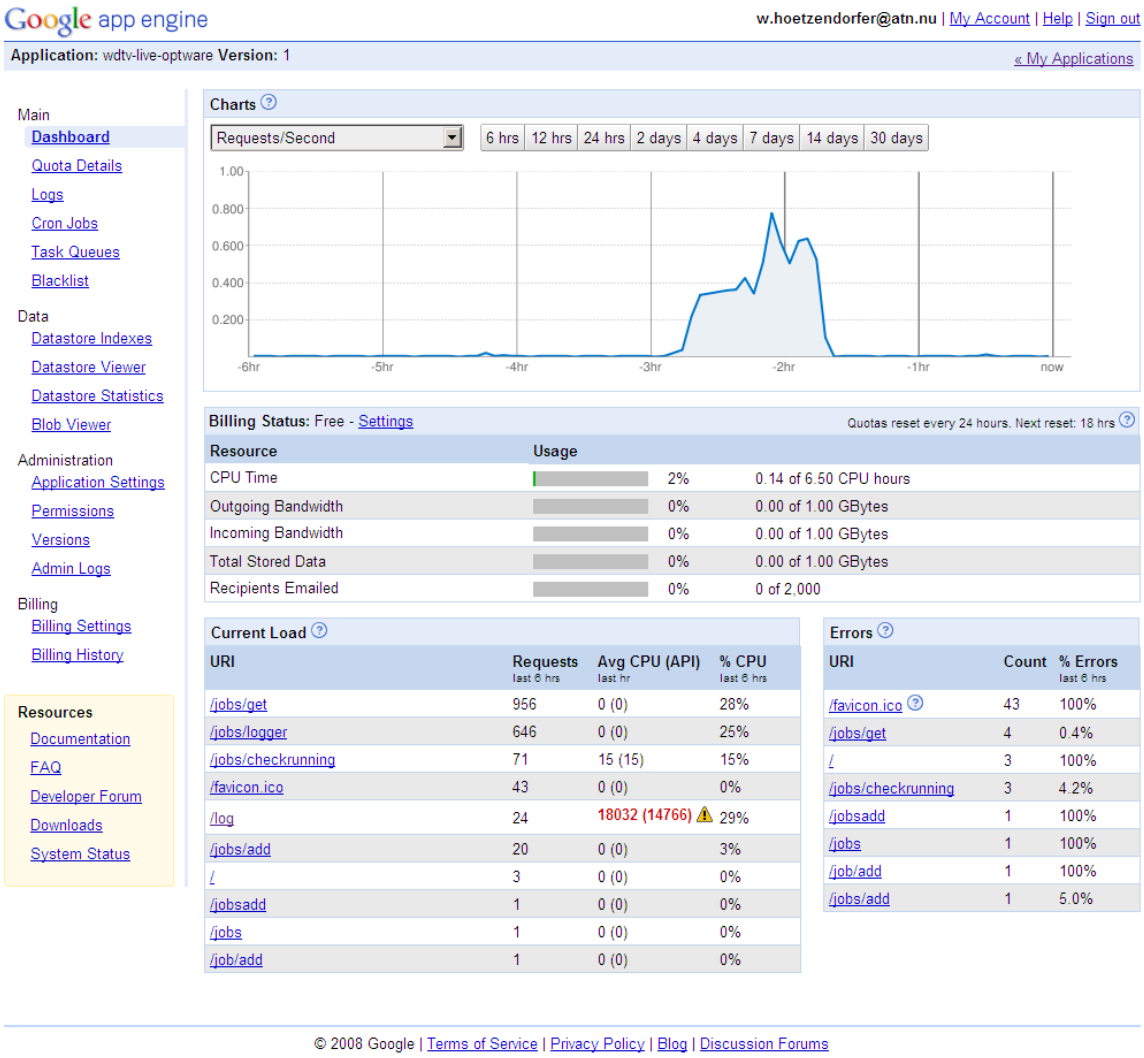


Abbildung 23 – „Dashboard“ der Jobdispatcher-Webanwendung mit Nutzungsstatistik für den Zeitraum des Projektdurchlaufs[484]

7.4. Fazit

Das Projekt wurde im August und September 2010 konzipiert, implementiert und getestet. Der finale Projektdurchlauf und somit die Kompilierung erfolgte am 18. September 2010 in Anwesenheit von DDr. Alexander Hampel. In etwas mehr als einer Stunde wurde die in den Jobdispatcher geladene Paket-Liste abgearbeitet, die entsprechenden Pakete wurden kompiliert und auf dem Server AGUIRRE abgelegt. Danach wurden die gestarteten *EC2*-Instanzen wieder beendet.

Wie in Abbildung 24 ersichtlich, kostete der gesamte Projektdurchlauf ca. 4 USD. Kosten fielen ausschließlich für die Nutzung von *Amazon Web Services* an, denn die Nutzungsintensität des Jobdispatchers überstieg die kostenlosen Freigrenzen von

[484] Quelle: Screenshot von https://appengine.google.com (erstellt am 18. September 2010).

Google App Engine nicht.[485] Für die Nutzung von *Amazon Web Services* während der Entwicklungsphase entstanden zusätzlich Kosten in der Höhe von ca. 5 USD.

This Month's Activity as of September 21, 2010

The billing cycle for this report is September 1 - September 30, 2010. The AWS service usage charges on this page currently show activity through approximately 09/21/2010 16:59 GMT.

Expand All Services | Collapse All Services — Printer Friendly Version

		Totals
Amazon Elastic Compute Cloud View/Edit Service		
US East (Northern Virginia) Region		
Amazon EC2 running Linux/UNIX		
$0.085 per Small Instance (m1.small) instance-hour (or partial hour)	21 Hrs	1.79
$0.34 per Large Instance (m1.large) instance-hour (or partial hour)	3 Hrs	1.02
Amazon EC2 running Linux/UNIX Spot Instances		
Large Spot Instance (m1.large) instance-hour (View Details)	3 Hrs	0.42
	Download Usage Report »	**3.23**
Amazon Simple Storage Service View/Edit Service		
US Standard Region		
$0.150 per GB - first 50 TB / month of storage used	0.404 GB-Mo	0.06
$0.01 per 1,000 PUT, COPY, POST, or LIST requests	59 Requests	0.01
$0.01 per 10,000 GET and all other requests	201 Requests	0.01
	Download Usage Report »	**0.08**
Amazon Virtual Private Cloud View/Edit Service		
	Download Usage Report »	**0.00**
AWS Data Transfer (excluding Amazon CloudFront) View/Edit Service		
$0.000 per GB - data transfer in (Until October 31st, 2010)	0.758 GB	0.00
$0.000 per GB - first 1 GB / month data transfer out	1 GB	0.00
$0.150 per GB - up to 10 TB / month data transfer out	0.241 GB	0.04
$0.010 per GB - regional data transfer - in/out/between EC2 Avail Zones or when using public/elastic IP addresses or ELB	0.000181 GB	0.01
		0.05
Taxes Estimated Taxes | VAT Registration (Due October 1, 2010)		**0.66**
Total Charges due on October 1, 2010†		**$4.02**

Abbildung 24 – Abrechnung von *AWS* für den Projektdurchlauf[486]

[485] Näheres zur Kostenstruktur von *Google App Engine* siehe unter Punkt 5.4.1, S. 96.
[486] Quelle: Screenshot von http://aws.amazon.com (erstellt am 22. September 2010).

Das Projekt führte auf sehr eindrucksvolle Weise die Stärken von Cloud Computing vor Augen: Obwohl insgesamt ca. 15 (physische und virtuelle) Server eingesetzt wurden, beliefen sich die Gesamtkosten – abgesehen von den Kosten der ohnehin vorhandenen lokalen Server – auf weniger als umgerechnet zehn EUR. Die Flexibilität des Cloud Computing ermöglichte es, eine Aufgabe in weniger als zwei Stunden zu lösen, für die ein einzelner Rechner wohl mindestens zwölf Stunden gebraucht hätte. Eine weitere Stärke von Cloud Computing, die Fokussierung, wird deutlich, wenn man rückblickend versucht, die aufwändigen Teile des Projekts zu ermitteln. Dabei ergibt sich, dass diese im Grunde mit Cloud Computing nichts zu tun haben. Die aufwändigsten Tätigkeiten waren die Programmierung der Jobdispatcher- und der Workernode-Software, die Vorbereitungsarbeiten der Kompilierung und die lokale Einrichtung von *Xen* und *OpenNebula*. All jene Probleme, die durch den Einsatz von Cloud-Services gelöst wurden – Einrichtung und Betrieb des Jobdispatchers, des Fileservers und der Workernodes – nahmen hingegen wenig Zeit in Anspruch. Lediglich die Vorbereitung eines eigenen *Linux*-Images für die Verwendung in *EC2* war ein vergleichsweise aufwändiges Unterfangen.

Insgesamt verlief das Projekt sehr erfolgreich. Die gewählte Aufgabenstellung erwies sich als sehr gut geeignet, und die Ziele des Projekts – Erfahrung im praktischen Einsatz von Cloud Computing und Virtualisierung zu gewinnen und mehrere Cloud-Services zu testen – wurden erreicht.

8. Schlussfolgerungen

In diesem Kapitel werden die Ergebnisse der vorliegenden Diplomarbeit noch einmal zusammengefasst und kritisch diskutiert. Darüber hinaus werden Schlussfolgerungen aus dem Prozess der Erstellung der Diplomarbeit gezogen, die als interdisziplinäres Projekt betrachtet werden kann.

8.1. Anmerkungen zum Vorgehensmodell

Die vorliegende Arbeit ist so aufgebaut, dass ihre Ergebnisse bereits ausführlich in Kapitel 6 aufbereitet wurden, insbesondere in dem dort vorgestellten Vorgehensmodell. Dieses bildet das wesentliche Ergebnis der Diplomarbeit. Es kann von Unternehmen unter Einbeziehung der übrigen Kapitel zur Entscheidungsfindung über den Einsatz von Cloud-Services herangezogen werden und dient darüber hinaus dem Leser dazu, einen Überblick über die Ergebnisse der gesamten Arbeit zu erhalten.

Dies ist auch der entscheidende Mehrwert, den das Vorgehensmodell bietet: Es stellt die komplexen Rahmenbedingungen des Einsatzes von Cloud-Services übersichtlich und leicht verständlich in aggregierter Form dar und dient somit dem Praktiker zur Entscheidungsunterstützung. Für nähere Informationen kann darüber hinaus in den übrigen Teilen der vorliegenden Arbeit nachgeschlagen und die darin zitierte Literatur herangezogen werden. Durch diesen zweistufigen Ansatz wurde eine fundierte und ausführliche Behandlung des Themas mit einer übersichtlichen Präsentation der Ergebnisse verknüpft. Eine weitere Besonderheit des Vorgehensmodells besteht darin, dass es auch die juristischen Rahmenbedingungen nach österreichischem Recht berücksichtigt, zu denen es derzeit (September 2010) nach Wissensstand des Autors keine Publikationen gibt. Die Erkenntnisse der Diplomarbeit zeigen, wie wichtig die Einbeziehung der rechtlichen Rahmenbedingung bei der Entscheidungsfindung über den Einsatz von Cloud Computing ist.

Anzumerken ist, dass das Vorgehensmodell als unterstützender Leitfaden betrachtet werden sollte, der individuelle Überlegungen in Bezug auf die Gegebenheiten eines konkreten Unternehmens und die dafür erforderliche Auseinandersetzung mit der Materie nicht ersetzen kann. Für letztere können – wie mehrfach betont – u.a. die übrigen Kapitel der Arbeit herangezogen werden. An dieser Stellte ist darüber hinaus noch einmal darauf hinzuweisen, dass das Vorgehensmodell nicht in der Praxis validiert wurde. Es ist aus theoretischen Erkenntnissen deduktiv abgeleitet und stellt einen zusammenfassenden Schlusspunkt der Arbeit dar. Wie am Beginn von Kapitel 6 bereits erläutert, bedürfte die Validierung eines eigenen Projekts mit ähnlich hohem Aufwand.

8.2. Zusammenfassung und Ausblick

Da – wie eben noch einmal erläutert – die Zusammenfassung der Ergebnisse der vorliegenden Diplomarbeit bereits ausführlich in Kapitel 6 erfolgte, werden an dieser Stelle abschließend lediglich einige besonders wichtige Erkenntnisse der Arbeit hervorgehoben.

In Kapitel 5 wurde gezeigt, dass die Vertragsbedingungen gängiger Anbieter von Cloud-Services den Nutzer in eine schwache Rechtsposition drängen. Mit anderen Worten, die vertraglichen Verpflichtungen und Haftungen, die sich die Anbieter auferlegen, sind tendenziell gering. Aus diesem Grund spielt das Vertrauen des Nutzers in die Bereitschaft und Fähigkeit eines Anbieters, auch ohne vertragliche Verpflichtung für Sicherheit und Zuverlässigkeit der angebotenen Services zu sorgen, bei der Entscheidungsfindung über die Nutzung eines Cloud-Service eine wesentliche Rolle. Wie unter Punkt 4.1.3 angesprochen, besteht für Anbieter allerdings ein Anreiz, dies tatsächlich zu tun, um sich einen guten Ruf aufzubauen und zu erhalten.

Hingegen ist Vertrauen keine Lösung für das Problem, dass die Vertragsbedingungen der untersuchten Anbieter nicht auf das österreichische bzw. europäische Datenschutzrecht ausgerichtet sind. In diesem Zusammenhang zählt ausschließlich, was vertraglich zugesichert ist, und dies reicht in den untersuchten Fällen nicht aus, um im Rahmen der Cloud-Services personenbezogene Daten ohne Zustimmung der Betroffenen zu verwenden. Dies bedeutet eine wesentliche Einschränkung der Nutzungsmöglichkeiten von Cloud-Services für österreichische Unternehmen.

In diesem Zusammenhang sollte allerdings nicht übersehen werden, dass die vorliegende Arbeit bewusst auf jene Cloud-Services eingeschränkt ist, die ohne Vorlaufzeit und zwischenmenschliche Interaktion gebucht und verwendet werden können. Daher mag das Ergebnis möglicherweise ohnehin wenig überraschend erscheinen, dass diese Cloud-Services vorwiegend für betrieblich unwesentliche Aufgaben und kleinere Unternehmen geeignet sind. Andere, auf dem Markt ebenfalls als Cloud-Service bezeichnete Angebote, die einen individuell ausgehandelten Vertrag und damit ein engeres Verhältnis zwischen Nutzer und Anbieter, umfassendere Gewährleistung und besseren Datenschutz mit sich bringen, eignen sich möglicherweise besser für unternehmenskritischere Aufgaben. Solche Services sind aber nach dem Verständnis der vorliegenden Arbeit keine Cloud-Services und haben mit diesen auch wenig gemein. Sie bedürfen einer längeren Vorlaufzeit, werden längerfristiger abgeschlossen und sind – aufgrund der verringerten Standardisierung – wohl mit wesentlich höheren Kosten verbunden.

Es bleibt daher zu hoffen, dass die Zukunft eine Professionalisierung der (eigentlichen) Cloud-Services mit sich bringen wird, sodass diese insbesondere im Hinblick

auf das Datenschutzrecht auch für österreichische Unternehmen besser einsetzbar sind. Möglicherweise können europäische oder gar österreichische Anbieter diese Nische erfolgreich besetzen. Fraglich ist allerdings, ob dem geltenden Datenschutzrecht durch Anpassungen der Anbieter überhaupt vollständig entsprochen werden kann. Möglicherweise ist daher eine Anpassung der Datenschutzbestimmungen – insbesondere des Dienstleisterbegriffs – an die neuen Gegebenheiten sinnvoll, was nicht zwangsläufig eine wesentliche Aufweichung des Datenschutzes bedeuten würde.

8.3. Anmerkungen zur Interdisziplinarität des Projekts

Wie in Abschnitt 1.3 (S. 21) dargelegt, kann das Vorbereiten und Verfassen der vorliegenden Diplomarbeit als interdisziplinäres Projekt an der Schnittstelle von Informatik, Betriebswirtschaftslehre und Rechtswissenschaft betrachtet werden. In diesem Abschnitt wurde auch erwähnt, dass der Autor im Rahmen dieses Projekts mit Experten dieser Fachgebiete zusammengearbeitet hat. Ohne deren Unterstützung und Erfahrung wäre die Erstellung der vorliegenden interdisziplinären Arbeit nicht möglich gewesen. Für den Autor war es eine interessante Erfahrung die Rolle des „Bindeglieds“ zwischen diesen zum Teil sehr verschiedenen, aber doch zusammenhängenden „Welten“ einzunehmen.

Das Zusammenführen dieser „Welten“ erwies sich im Rahmen des Verfassens der Diplomarbeit als große Herausforderung. Dies wird besonders in Kapitel 3 deutlich, das die umfangreichen juristischen Grundlagen der Arbeit enthält. Dieses soll einerseits die rechtlichen Rahmenbedingungen des Cloud Computing in der nötigen Tiefe behandeln, andererseits aber für juristische Laien verständlich sein. Es wäre möglich gewesen, nur die entscheidungsrelevanten Ergebnisse der juristischen Recherchen und Analysen darzustellen und auf ausführliche rechtswissenschaftliche Begründungen zu verzichten. Dies hätte jedoch den Wert des juristischen Teils der vorliegenden Arbeit erheblich geschmälert, der beträchtlich ist, zumal es in Österreich nach Wissensstand des Autors noch keine rechtswissenschaftlichen Veröffentlichungen zum Thema Cloud Computing gibt. Diese Tatsache wiederum liegt wohl ebenfalls in der Interdisziplinarität des Themas begründet, welche eine Auseinandersetzung damit für Juristen mit ausschließlich rechtswissenschaftlichem Hintergrund sehr schwierig macht. Auch der beträchtliche Umfang der Arbeit ist ihrer Interdisziplinarität geschuldet.

Die Erkenntnisse der Arbeit haben gezeigt, wie wichtig eine interdisziplinäre Herangehensweise an das Thema Cloud Computing ist: Nur unter Einbeziehung technischer, betriebswirtschaftlicher und rechtlicher Aspekte können Entscheidungen über den Einsatz von Cloud-Services sinnvoll getroffen werden.

Literaturverzeichnis

Publizierte Quellen

Baun, Christian, Marcel Kunze, Jens Nimis und Stefan Tai (2009). *Cloud Computing: Web-basierte dynamische IT-Services*. Berlin: Springer-Verlag, 2009.

Becker, Jörg und Dieter Kahn (2005). „Der Prozess im Fokus." In: *Prozessmanagement – Ein Leitfaden zur prozessorientierten Organisationsgestaltung*, Hrsg.: Jörg Becker, Martin Kugeler und Michael Rosemann. Berlin/Heidelberg/New York: Springer-Verlag, 2005: 3.

Berlich, Rüdiger (2010). „Was ist da im Anzug?" *Linux-Magazin*, Mai 2010: 36.

Burgstaller, Alfred, Matthias Neumayr (2010). *Internationales Zivilverfahrensrecht*. Wien: LexisNexis ARD Orac, 2010.

Buyya, Rajkumar, Chee Shin Yeo, Srikumar Venugopal, James Broberg und Ivona Brandic (2009). „Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility." *Future Generation Computer Systems*, 2009: 599.

Dean, Jeffrey und Sanjay Ghemawat (2008). „MapReduce: simplified data processing on large clusters." *Communications of the ACM*, Jänner 2008: 107.

Dellinger, Markus (Hrsg.) (2007-2010). *Bankwesengesetz – Kommentar*. Wien: LexisNexis ARD Orac, 2007-2010.

Dohr, Walter, Hans-Jürgen Pollirer, Ernst M. Weiss und Rainer Knyrim (2009). *Datenschutzrecht – DSG*. Wien: Manz, 2009.

Fallenböck, Markus und Michael Trappitsch (2002). „Application Service Providing (ASP) – rechtlich betrachtet." *Medien und Recht (MR) – Zeitschrift für Medien- und Kommunikationsrecht*, 2002: 3.

Foster, Ian, Yong Zhao, Ioan Raicu und Shiyong Lu (2008). „Cloud Computing and Grid Computing 360-Degree Compared." *Grid Computing Environments Workshop, 2008. GCE'08*, 2008.

Fucik, Robert, Alexander Klauser, Barbara Kloiber (2009). *ZPO – Österreichisches und Europäisches Zivilprozessrecht*. Wien: Manz, 2009.

Gerick, Thomas (2009). „Software-Lizenzmanagement: Risiken und Kosten minimieren." *CFOaktuell*, 2009: 260.

Ghemawat, Sanjay, Howard Gobioff und Shun-Tak Leung (2003). „The Google file system." *ACM SIGOPS Operating Systems Review*, Dezember 2003: 29.

Grapentin, Sabine (2009). „Rechtliche Einordnung von IT-Outsourcing-Leistungen." In: *IT-Outsourcing*, Hrsg.: Peter Bräutigam. Berlin: Erich Schmidt Verlag, 2009: 177.

Gruber, Michael und Nicolas Raschauer (Hrsg.) (2009). *Wertpapieraufsichtsgesetz (WAG) – Kommentar*. Wien: LexisNexis ARD Orac, 2009.

Hirschheim, Rudy und Jens Dibbern (2009). „Outsourcing in a Global Economy: Traditional Information Technolgy Outsourcing, Offshore Outsourcing, and Business Process Outsourcing.“ In: *Information Systems Outsourcing: Enduring Themes, Global Challenges, and Process Opportunities,* Third Edition, Hrsg.: Rudy Hirschheim, Armin Heinzl und Jens Dibbern. Berlin, Heidelberg: Springer-Verlag, 2009: 3

Jahnel, Dietmar (2010). *Handbuch Datenschutzrecht*. Wien: Jan Sramek Verlag, 2010.

Jahnel, Dietmar (2009). „OGH: Anspruch auf Beseitigung von Kreditkonten, die durch eine Bank unzulässig weitergeführt wurden.“ *jusIT – Zeitschrift für IT-Recht, Rechtsinformation und Datenschutz*, 2009: 64.

Jahnel, Dietmar (2005). „OGH: Kein Schutz von Unternehmensdaten nach dem DSG?“ *Österreichisches Recht der Wirtschaft (RdW)*, 2005: 200.

Jahnel, Dietmar und Clemens Thiele (2004). „Datenschutz durch Wettbewerbsrecht.“ *Österreichische Juristen-Zeitung (ÖJZ)*, 2004: 55.

Jahnel, Dietmar (2003). „Datenschutzrecht.“ In: *Informatikrecht*, von Dietmar Jahnel, Alfred Schramm und Elisabeth Staudegger. Wien/New York: Springer-Verlag, 2003: 241.

Jergitsch, Friedrich und Christine Siegl (2010). „Outsourcing von Bankgeschäften.“ In: *Outsourcing: Ein Leitfaden für Juristen und Praktiker*, Herausgeber: Bertram Burtscher. Wien: Linde, 2010: 19.

Keller, Wolfgang (2007). *IT-Unternehmensarchitektur*. Heidelberg: dpunt.verlag, 2007.

Kersten, Heinrich, Jürgen Reuter und Klaus-Werner Schröder (2009). *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz*. 2. Auflage. Wiesbaden: Vieweg+Teubner, 2009.

Knyrim, Rainer (2004). „Hosting von Websites (§ 16 ECG) ist Dienstleistung im datenschutzrechtlichen Sinn.“ *Medien und Recht (MR) – Zeitschrift für Medien- und Kommunikationsrecht*, 2004: 51.

Knyrim, Rainer, Volker Siegel und Stefan Autengruber (2004). „Datenschutz und Datenrettung beim Outsourcing.“ *ecolex – Fachzeitschrift für Wirtschaftsrecht*, 2004: 413.

Korinek, Stephan (2007). „Ausgliederungen bei Versicherungen und Pensionskassen.“ *Zeitschrift für Finanzmarktrecht (ZFR)*, 2007: 39.

Koziol, Helmut und Rudolf Welser (2007). *Bürgerliches Recht*. 13. Auflage. Bd. II. Wien: Manz, 2007.

Koziol, Helmut und Rudolf Welser (2006). *Bürgerliches Recht*. 13. Auflage. Bd. I. Wien: Manz, 2006.

Koziol, Helmut, Peter Bydlinski und Raimund Bollenberger (Hrsg.) (2007). *Kommentar zum ABGB*. 2. Auflage. Wien/New York: Springer-Verlag, 2007.

Krejci, Heinz (2008). *Unternehmensrecht*. 4. Auflage. Wien: Manz, 2008.

Kumar, Karthik und Yung-Hsiang Lu (2010). „Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?“ *Computer,* April 2010: 51.

Laga, Gerhard, Ulrike Sehrschön und Meinhard Ciresa (2007). *E-Commerce Gesetz*. Wien: LexisNexis ARD Orac, 2007.

Laurer, H. René, Rainer Borns, Johann Strobl, Melitta Schütz und Oliver Schütz (2007). *Bankwesengesetz – BWG*. 3. Auflage. Wien: Manz, 2007.

Lenk, Alexander, Markus Klems, Jens Nimis, Stefan Tai und Thomas Sandholm (2009). „What's Inside the Cloud? An Architectural Map of the Cloud Landscape.“ *ICSE 2009 Workshop on Software Engineering Challenges of Cloud Computing*, 2009.

Mankowski, Peter (2008). „Die Rom-I-Verordnung – Änderungen im europäischen IPR für Schuldverträge.“ *IHR – Internationales Handelsrecht,* 2008, 133.

Mather, Tim, Subra Kumaraswamy und Shahed Latif (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. Sebastopol: O'Reilly Media, 2009.

Mayer-Schönberger, Viktor und Ernst O. Brandl (2006). *Datenschutzgesetz*. 2. Auflage. Wien: Linde, 2006.

Menzies, Christof (Hrsg.) (2006). *Sarbanes-Oxley und Corporate Compliance*. Stuttgart: Schäffer-Poeschl, 2006.

Milla, Aslan, Ruth Vcelouch-Kimeswenger und Martin Weber (2008). *Unternehmensrechts-Änderungsgesetz 2008: Praxiskommentar*. Wien: Linde, 2008.

Nägele, Thomas und Sven Jacobs (2010). „Rechtsfragen des Cloud Computing.“ *Zeitschrift für Urheber- und Medienrecht (ZUM)*, 2010: 281.

Niemann, Fabian und Jörg-Alexander Paul (2009). „Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computings.“ *Kommunikation & Recht (K&R)*, 2009: 444.

Nordmeier, Carl Friedrich (2010). „Cloud Computing und Internationales Privatrecht: Anwendbares Recht bei der Schädigung von in Datenwolken gespeicherten Daten.“ *Multimedia und Recht (MMR) – Zeitschrift für Informations-, Telekommunikations- und Medienrecht*, 2010: 151.

Nurmi, Daniel, Rich Wolski, Chris Grzegorczyk, Graziano Obertelli, Sunil Soman, Lamia Youseff und Dimitrii Zagorodnov (2009). „The Eucalyptus Open-Source Cloud-Computing System.“ *Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid*, 2009: 124.

Pohl, Lorenz (2009). *IT-Outsourcing: Lizenzierung von Fremdsoftware*. Wien: LexisNexis ARD Orac, 2009.

Pohle, Jan und Thorsten Ammann (2009a). „Über den Wolken… – Chancen und Risiken des Cloud Computing.“ *Computer und Recht (CR) – Zeitschrift für die Praxis des Rechts der Informationstechnologien*, 2009a: 273.

Pohle, Jan und Thorsten Ammann (2009b). „Software as a Service – auch rechtlich eine Evolution?“ *Kommunikation & Recht (K&R)*, 2009b: 625.

Pollirer, Hans-Jürgen, Ernst M. Weiss und Rainer Knyrim (2010). *Datenschutzgesetz 2000 (DSG 2000) samt ausführlichen Erläuterungen*. Wien: Manz, 2010.

Rath, Michael (2009). „Rechtliche Aspekte von IT-Compliance.“ In: *Compliance in der Unternehmenspraxis*, Hrsg.: Gregor Wecker und Hendrik van Laak. Wiesbaden: Gabler, 2009: 149

Rechberger, Walter H., Daphne-Ariane Simotta (2009). *Zivilprozessrecht – Erkenntnisverfahren*. 7. Auflage. Wien: Manz, 2009.

Rechberger, Walter H. (2006). *Kommentar zur Zivilprozessordnung*. 3. Auflage. Wien: Springer-Verlag, 2006.

Rhoton, John (2010). *Cloud Computing Explained*. Second Edition. o.O.: Recursive Press, 2010.

Rittinghouse, John W. und James F. Ransome (2009). *Cloud Computing: Implementation, Management, and Security* . Boca Raton: CRC Press, 2009.

Rummel, Peter (Hrsg.) (2000-2007). *Kommentar zum Allgemeinen bürgerlichen Gesetzbuch*. 3. Auflage. Manz, 2000-2007.

Schober, Andreas (2009). *IT Governance und der Sarbanes-Oxley Act*. Saarbrücken: VDM Verlag Dr. Müller, 2009.

Schulz, Carsten und Timo Rosenkranz (2009). „Cloud Computing – Bedarfsorientierte Nutzung von IT-Ressourcen.“ *Der IT-Rechts-Berater (ITRB) – Informationsdienst für die EDV-, Multimedia- und TK-rechtliche Beratungspraxis*, 2009: 232.

Schumacher, Volker A. (2006). „Service Level Agreements: Schwerpunkt bei IT- und Telekommunikationsverträgen.“ *Multimedia und Recht (MMR) – Zeitschrift für Informations-, Telekommunikations- und Medienrecht*, 2006: 12.

Schuster, Fabian und Wolfgang Reichl (2010). „Cloud Computing & SaaS: Was sind die wirklich neuen Fragen?“ *Computer und Recht (CR) – Zeitschrift für die Praxis des Rechts der Informationstechnologien*, 2010: 38.

Schütz, Oliver und Markus Waldherr (2007). „Die Auslagerung bankgeschäftlicher Tätigkeiten aus bankaufsichtsrechtlicher Sicht (Outsourcing).“ *Österreichisches Bank-Archiv (ÖBA) – Zeitschrift für das gesamte Bank- und Börsenwesen*, 2007: 138.

Schwimann, Michael (Hrsg.) (2004-2007). *ABGB Praxiskommentar*. 3. Auflage. Wien: LexisNexis ARD Orac, 2004-2007.

Sehrschön, Ulrike (2010). „Datenschutz und Bankgeheimis.“ In: *Outsourcing: Ein Leitfaden für Juristen und Praktiker*, Hrsg.: Bertram Burtscher. Wien: Linde, 2010: 45.

Sonnenberger, Hans Jürgen (2009). *Münchener Kommentar zum BGB*. Bd. 10. München: C.H.Beck, 2009.

Spies, Axel (2009). „USA: Cloud Computing – Schwarze Löcher im Datenschutzrecht." *Multimedia und Recht (MMR) – Zeitschrift für Informations-, Telekommunikations- und Medienrecht*, 2009: Heft 5, XI.

The Economist (2010). „Clouds under the hammer." *The Economist,* 13. März 2010: 64.

Thiele, Clemens (2004). „Internet Provider auf Abwegen – Zur Rechtsnatur der Domainbeschaffung." *ecolex – Fachzeitschrift für Wirtschaftsrecht*, 2004: 777.

Velte, Toby, Anthony Velte und Robert C. Elsenpeter (2009). *Cloud Computing: A Practical Approach*. New York City: Mcgraw-Hill Professional, 2009.

Weber, Martin (2008). „Das Unternehmensrechts-Änderungsgesetz 2008 im Überblick." *Österreichische Juristen-Zeitung (ÖJZ)*, 2008: 45.

Wolf, Boris (2010). „Blaues Wunder: Mit Microsofts Azure in die Cloud – ein Erfahrungsbericht." *iX - Magazin für Informationstechnik*, September 2010: 78.

Zankl, Wolfgang (2005). „Qualifikation und Dauer von Mobilfunkverträgen." *ecolex – Fachzeitschrift für Wirtschaftsrecht*, 2005: 29.

Zankl, Wolfgang (2002). *E-Commerce-Gesetz*. Wien: Verlag Österreich, 2002.

Internet-Quellen

Amazon Web Services (o.J.). „Amazon Simple Storage Service (Amazon S3)." *Amazon Web Services*. http://aws.amazon.com/s3/ (Zugriff am 31. August 2010).

AppScale (o.J.). „About the Projekt." *AppScale*. http://appscale.cs.ucsb.edu/ (Zugriff am 04. September 2010).

Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica und Matei Zaharia (2009). „Above the Clouds: A Berkeley View of Cloud Computing." *UC Berkeley Reliable Adaptive Distributed Systems Laboratory*. 2009. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf (Zugriff am 27. September 2010).

Auditing Standards Board (1992). „Statement on Auditing Standards 70: Report on the Processing of Transactions by Service Organizations." *UMISS AICPA Accounting Database*. 1992. http://umiss.lib.olemiss.edu:82/articles/1038093.6672/1.DOC (Zugriff am 22. September 2010).

Bias, Randy (2010). „Does OpenStack Change the Cloud Game?" *cloudscaling.com Blog*. 20. Juli 2010. http://cloudscaling.com/blog/cloud-computing/does-openstack-change-the-cloud-game (Zugriff am 01. September 2010).

BITKOM (2009). „Cloud Computing – Evolution in der Technik, Revolution im Business." *BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.)*. 2009. http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf (Zugriff am 25. August 2010).

CA Technologies (2010). „Unleashing the Power of Virtualization 2010." *CA Technologies*. 2010. http://www.ca.com/files/supportingpieces/ca_virtualisatn_survey_report_228900.pdf (Zugriff am 18. September 2010).

Cloud Security Alliance (2009). „Security Guidance for Critical Areas of Focus in Cloud Computing V2.1." *Cloud Security Alliance*. 2009. http://www.cloudsecurityalliance.org/csaguide.pdf (Zugriff am 25. August 2010).

Connolly, Chris (2008). „The US Safe Harbor – Fact or Fiction? (2008)." *galexia*. 02. Dezember 2008. http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf (Zugriff am 01. September 2010).

Eucalyptus Systems (2010). „Introducing Eucalyptus 2.0." *open.eucalyptus.com*. 2010. http://open.eucalyptus.com/wiki/IntroducingEucalyptus_v2.0 (Zugriff am 08. September 2010).

Europäische Kommission (2010a). „Entscheidung der Kommission hinsichtlich Standardvertragsklauseln für die Übermittlung Personenbezogener Daten in Drittländer." *Europäische Kommission. 2010*. http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_de.htm (Zugriff am 07. Juni 2010).

Europäische Kommission (2010b). „Entscheidungen der Kommission zur Angemessenheit des Schutzes persönlicher Daten in Drittstaaten." *Europäische Kommission. 2010*. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm (Zugriff am 07. Juni 2010).

Farber, Dan (2008). „Defining cloud computing." *CNET News*. 07. Mai 2008. http://news.cnet.com/8301-13953_3-9938949-80.html (Zugriff am 02. Juli 2010).

Fischer, Oliver (2010). „Datenverarbeiter: Verarbeiten großer verteilter Datenmengen mit Hadoop." *heise Developer*. 01. April 2010. http://www.heise.de/developer/artikel/Verarbeiten-grosser-verteilter-Datenmengen-mit-Hadoop-964755.html (Zugriff am 30. August 2010).

Geelan, Jeremy (2010). „The Top 250 Players in the Cloud Computing Ecosystem." *Cloud Computing Journal*. 29. August 2010. http://cloudcomputing.sys-con.com/node/1386896 (Zugriff am 30. August 2010).

Geelan, Jeremy (2009). „Twenty-One Experts Define Cloud Computing." *Cloud Computing Journal*. 24. Jänner 2009. http://cloudcomputing.sys-con.com/node/612375/ (Zugriff am 02. Mai 2010).

Girouard, Dave (2010). „Three million businesses have gone Google: celebrating growth, innovation and security." *The Official Google Blog*. 20. September 2010. http://googleblog.blogspot.com/2010/09/three-million-businesses-have-gone.html (Zugriff am 26. September 2010).

Google (o.J.). „Zusammenarbeiten: Gleichzeitiges Bearbeiten und Betrachten." *Google*. http://docs.google.com/support/bin/answer.py?hl=de&answer=44680 (Zugriff am 09. August 2010).

Gottfrid, Derek (2008). „The New York Times Archives + Amazon Web Services = TimesMachine." *open.blogs.nytimes.com*. 21. Mai 2008. http://open.blogs.nytimes.com/2008/05/21/the-new-york-times-archives-amazon-web-services-timesmachine/ (Zugriff am 29. August 2010).

ISO (o.J.). „ISO/IEC 27001:2005." *International Organization for Standardization*. o.J. http://www.iso.org/iso/catalogue_detail?csnumber=42103 (Zugriff am 2010. September 20).

Johnson, Bobbie (2008). „Cloud computing is a trap, warns GNU founder Richard Stallman." *guardian.co.uk*. 29. September 2008. http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman (Zugriff am 29. September 2010).

Malik, Om (2010). „Amazon Web Services: Quietly Staking Out the Cloud." *Bloomberg Businessweek*. 02. Februar 2010. http://www.businessweek.com/technology/content/feb2010/tc2010022_692380.htm (Zugriff am 30. August 2010).

Marwan, Peter (2010). „Cloud Computing: Die meisten Anbieter sind noch nicht so weit." *ZDNet.de*. 14. April 2010. http://www.zdnet.de/it_business_hintergrund_cloud_computing_die_meisten_anbieter_sind_noch_nicht_so_weit_story-11000006-41530450-1.htm (Zugriff am 11. Mai 2010).

NIST (2009). „The NIST Definition of Cloud Computing (Version 15)." *NIST (National Institute of Standards and Technology)*. 2009. http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc (Zugriff am 25. August 2010).

Open Cloud Manifesto Discussion Group (2009). „Open Cloud Manifesto." 2009. http://opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf (Zugriff am 25. August 2010).

Perez, Sarah (2010). „Mobile Cloud Computing: $9.5 Billion by 2014." *ReadWriteWeb*. 23. Februar 2010. http://www.readwriteweb.com/archives/mobile_cloud_computing_95_billion_by_2014.php (Zugriff am 26. September 2010).

Rosen, Guy (2010). „State of the Cloud – August 2010." *Jack of all Clouds*. 06. August 2010. http://www.jackofallclouds.com/2010/08/state-of-the-cloud-august-2010/ (Zugriff am 30. August 2010).

Schmidt, Holger (2010). „Eric Schmidt: Googles Devise heißt jetzt ‚Mobile first'." *F.A.Z.-Blogs*. 17. Februar 2010. http://faz-community.faz.net/blogs/netzkonom/archive/2010/02/17/googles-devise-heisst-ab-jetzt-mobile-first.aspx (Zugriff am 26. September 2010).

Statistik Austria (2008). „Klassifikationsdatenbank." *Statistik Austria*. 2008. http://wko.at/statistik/oenace/oenace2008.pdf (Zugriff am 24. September 2010).

Tucci, Linda (2009). „ISO 27001 certification not enough for verifying SaaS, cloud security." *SearchCompliance.com*. 21. Oktober 2009. http://searchcompliance.techtarget.com/news/1372041/ISO-27001-certification-not-enough-for-verifying-SaaS-cloud-security (Zugriff am 21. September 2010).

Urquhart, James (2010). „Amazon APIs as cloud standards? Not so fast.“ *cnet news*. 09. Juli 2010. http://news.cnet.com/8301-19413_3-20010072-240.html?part=rss&tag=feed&subj=TheWisdomofClouds (Zugriff am 30. August 2010).

Warfield, Bob (2010). „Amazon Web Services: The De Facto Cloud API?“ *SmoothSpan Blog*. 12. Juli 2010. http://smoothspan.wordpress.com/2010/07/12/amazon-web-services-the-de-facto-cloud-api/ (Zugriff am 30. August 2010).

Verzeichnis der zitierten Entscheidungen

DSK in K120.819/006-DSK/2003, 14.11.2003.

BGH in XII ZR 120/04, MMR 2007, 243, 15.11.2006.

LG Klagenfurt in 1 R 171/08d, 19.06.2008.

OGH in 4 Ob 114/91, 25.02.1992.

OGH in 1 Ob 538/93, 01.05.1993.

OGH in 7 Ob 120/98t, 10.08.1998.

OGH in 3 Ob 146/99p, 24.05.2000.

OGH in 6 Ob 69/05y, 21.04.2005.

OGH in 9 Ob 15/05d, 04.05.2006.

OGH in 2 Ob 192/07k, 24.01.2008.

OGH in 6 Ob 236/08m, 17.12.2008.

OGH in 2 Ob 159/08h, 22.01.2009.

Anhang A: Ausgewählte Bestimmungen des DSG 2000

In diesen Anhang sind jene Bestimmungen des DSG 2000 enthalten, auf die im Vorgehensmodell in Kapitel 6 verwiesen wird.

Pflichten des Dienstleisters

§ 11. (1) Unabhängig von allfälligen vertraglichen Vereinbarungen haben Dienstleister bei der Verwendung von Daten für den Auftraggeber jedenfalls folgende Pflichten:

1. die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten;
2. alle gemäß § 14 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;
3. weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, daß er dies allenfalls untersagen kann;
4. - sofern dies nach der Art der Dienstleistung in Frage kommt - im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen;
5. nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten;
6. dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der unter Z 1 bis 5 genannten Verpflichtungen notwendig sind.

(2) Vereinbarungen zwischen dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung der in Abs. 1 genannten Pflichten sind zum Zweck der Beweissicherung schriftlich festzuhalten.

Datensicherheitsmaßnahmen

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

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

1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,

6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

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

(3) Nicht registrierte Übermittlungen aus Datenanwendungen, die einer Verpflichtung zur Auskunftserteilung gemäß § 26 unterliegen, sind so zu protokollieren, daß dem Betroffenen Auskunft gemäß § 26 gegeben werden kann. In der Standardverordnung (§ 17 Abs. 2 Z 6) oder in der Musterverordnung (§ 19 Abs. 2) vorgesehene Übermittlungen bedürfen keiner Protokollierung.

(4) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck - das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes - unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, daß es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, handelt.

(5) Sofern gesetzlich nicht ausdrücklich anderes angeordnet ist, sind Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren. Davon darf in jenem Ausmaß abgewichen werden, als der von der Protokollierung oder Dokumentation betroffene Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.

(6) Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, daß sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können.

Anhang B: Liste von Cloud-Services

Dieser Anhang enthält eine Liste aller während der Recherchen zur vorliegenden Arbeit aufgefundenen Cloud-Services, die prima facie das Kriterium des on-demand self-service[487] erfüllen. Die Zusammenstellung erhebt weder Anspruch auf Vollständigkeit, noch wurden alle genannten Cloud-Services näher untersucht. Die Liste basiert auf einer ähnlichen Zusammenstellung in *Baun et al.*[488] und wurde während der Recherchen laufend erweitert und präzisiert.

Anbieter	Service	Service-Modell[489]	Service-Typ
Amazon	EC2	IaaS (R)	Virtuelle Server
Amazon	S3	IaaS (I)	Massenspeicher
Amazon	Elastic Block Store (EBS)	IaaS (I)	Persistente Speicherung
Amazon	SimpleDB	IaaS (I)	Datenbank
Amazon	CloudFront	IaaS (I)	Content Distribution Network
Amazon	Simple Queue Service (SQS)	IaaS (I)	Nachrichten-Queues
AppNexus	AppNexus Cloud	IaaS (R)	Virtuelle Server
Bluelock	Virtual Cloud Computing	IaaS (R)	Virtuelle Server
Bluelock	Virtual Recovery	IaaS (I)	Wiederherstellung virtueller Server bei Störungen
Dropbox	Dropbox Cloud Storage	IaaS (I)	Massenspeicher
ElasticHosts	ElasticHosts	IaaS (I)	Virtuelle Server
ENKI	Virtual Private Data Centers	IaaS (R)	Bedarfsgerechte Bereitstellung virtueller Rechenzentren
FlexiScale	FlexiScale Cloud Computing	IaaS (R)	Virtuelle Server
GoGrid	Cloud Hosting	IaaS (R)	Virtuelle Server
GoGrid	Cloud Storage	IaaS (I)	Massenspeicher
Joynet	Accelerator	IaaS (R)	Virtuelle Server
Joynet	Connector	IaaS (R)	Vorkonfigurierte virtuelle Server
Joynet	BingoDisk	IaaS (I)	Massenspeicher
Microsoft	SQL Azure	IaaS (I)	Implementierung des Microsoft SQL-Servers
Nirvanix	Storage Delivery Network	IaaS (I)	Massenspeicher

[487] Zum Charakteristikum „on-demand self-service“ siehe Tabelle 1, S. 28.
[488] Baun et al. 2009, 31 ff.
[489] Einteilung nach Abschnitt 2.4 (S. 28). Legende:
A Anwendung
AS Anwendungsservice
E Entwicklungsumgebung
I Infrastruktur-Service
L Laufzeitumgebung
R Ressourcen-Set

Rackspace	Mosso Cloud Sites	IaaS (R)	Vorkonfigurierte virtuelle Server
Rackspace	Mosso Cloud Storage	IaaS (I)	Massenspeicher
Rackspace	Mosso Cloud Servers	IaaS (R)	Virtuelle Server
Terremark	Infinistructure	IaaS (R)	Virtuelle Server
Terremark	vCloud Express	IaaS (R)	Virtuelle Server
Zumodrive	Hybrid Cloud Storage	IaaS (I)	Massenspeicher
Bungee	Bungee Connect	PaaS (E+L)	Entwicklungs- u. Laufzeitumgebung für AJAX-Applikationen
Engine Yard	AppCloud	PaaS (E+L)	Entwicklungs- und Laufzeitumgebung für Ruby on Rails
Facebook	Facebook Platform	PaaS (L)	Werkzeuge und Laufzeitumgebung für Erweiterungen von Facebook
Google	Google App Engine	PaaS (L)	Skalierbare Laufzeitumgebung für Web-Applikationen
Microsoft	Windows Azure	PaaS (E+L)	Laufzeitumgebung für (Web-)Applikationen
Salesforce	Force.com	PaaS (E+L)	Entwicklungs- und Laufzeitumgebung für Erweiterungen von Salesforce CRM
Sun	Project Caroline	PaaS (E+L)	Entwicklungs- und Laufzeitumgebung für verteilte Web-Applikationen
Zoho	Zoho Creator	PaaS (E+L)	Entwicklungs- und Laufzeitumgebung für Web-Applikationen
Google	Google Apps	SaaS (A)	Office-Suite
IBM	LotusLive	SaaS (A)	Online-Zusammenarbeit
Intuit	QuickBooks Online	SaaS (A)	Buchhaltung (Quicken)
Microsoft	Office Live	SaaS (A)	Office-Suite
Microsoft	Office Live Small Business	SaaS (A)	Unternehmens-Website, Shop-Management, E-Mail-Marketing
Microsoft	Dynamics CRM	SaaS (A)	CRM
NetSuite	NetSuite	SaaS (A)	ERP, CRM
OpenID	OpenID	SaaS (AS)	Verteiltes System zur Verwaltung systemübergreifender Benutzeridentitäten
Oracle	Oracle CRM On Demand	SaaS (A)	CRM
Oracle	Oracle Beehive	SaaS (A)	Online-Zusammenarbeit
Salesforce	Salesforce CRM	SaaS (A)	Erweiterbares CRM-System
Workday	Workday 101	SaaS (A)	HR-, Payroll- und Financial Management
Zoho	Zoho Apps	SaaS (A)	Office-Suite und andere Anwendungen

Anhang C: Vertragsbedingungen von Amazon Web Services

Um dem Leser einen Eindruck der Vertragsbedingungen von Cloud-Services zu vermitteln und die Komplexität der Analyse solcher Vertragsbedingungen zu verdeutlichen, sind in diesem Anhang exemplarisch die in Kapitel 5 behandelten Vertragsbedingungen von *Amazon Web Services* im Volltext enthalten. Sie wurden direkt von der Website des Anbieters übernommen. Die genaue Quellenangabe befindet sich am Ende jedes Dokuments. Bedeutende Stellen in den Vertragsbedingungen, auf die zum Teil in Kapitel 5 verwiesen wird, sind farblich hinterlegt. Von einer Wiedergabe der Vertragsbedingungen aller untersuchten Cloud-Services wurde aufgrund ihres Umfangs abgesehen.

Amazon Web Services™ Customer Agreement

Updated July 7, 2010

PLEASE NOTE, TERMS AND CONDITIONS GOVERNING USE OF THE AMAZON ASSOCIATES WEB SERVICE™ ARE NOW LOCATED AT:
https://affiliate-program.amazon.com/gp/advertising/api/detail/agreement.html

PLEASE READ CAREFULLY – THIS IS A BINDING CONTRACT

THIS AWS CUSTOMER AGREEMENT ("AGREEMENT" OR "AMAZON WEB SERVICES CUSTOMER AGREEMENT") IS A BINDING AGREEMENT BETWEEN AMAZON WEB SERVICES LLC ("AWS") AND YOU AND, IF APPLICABLE, THE COMPANY OR OTHER LEGAL ENTITY YOU REPRESENT (COLLECTIVELY, "YOU"). THIS AGREEMENT INCORPORATES BY REFERENCE (1) THE PRIVACY NOTICE POSTED ON WWW.AMAZON.COM ("PRIVACY NOTICE"), (2) THE TERMS OF USE POSTED ON AWS.AMAZON.COM ("TERMS OF USE"), (3) THE ACCEPTABLE USE POLICY POSTED ON AWS.AMAZON.COM ("AUP"), (4) THE SERVICE TERMS POSTED ON AWS.AMAZON.COM ("SERVICE TERMS"), AND (5) THE TRADEMARK GUIDELINES POSTED ON AWS.AMAZON.COM, AS THESE POLICIES AND TERMS MAY BE MODIFIED BY AWS OR ITS AFFILIATES FROM TIME TO TIME.
BY CLICKING THE "ACCEPT" BUTTON FOR THIS AGREEMENT OR ACCEPTING ANY MODIFICATION TO THIS AGREEMENT IN ACCORDANCE WITH SECTION 2 BELOW, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND THE LEGAL ENTITY TO THIS AGREEMENT, IN WHICH CASE "YOU" SHALL MEAN SUCH ENTITY. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT, YOU MUST SELECT THE "DECLINE" BUTTON AND YOU MAY NOT USE THE SERVICES.

Welcome

This Agreement includes the following Sections:

1. The Services

The services covered by this Agreement include both free services that AWS and its affiliates (referred to together herein as "we" or "us") make available for no fee (the "Free Services"), and services that we make available for a fee (the "Paid Services"). The Free Services and the Paid Services are referred to collectively in this Agreement as the "Services." Each Free Service and Paid Service is referred to individually as a "Service."

1.1. Free Services. The Free Services include the Alexa® Site Widgets, Amazon FWS and all other web services that we make available to you free of charge on the Amazon Web Services-branded or Alexa®-branded web sites accessible from aws.amazon.com (collectively, the "AWS Website"), except those web services for which we specifically provide a separate customer agreement.

1.2. Paid Services. The Paid Services include all web services and any related support services that we make available to you for a fee on the AWS Website, except those web services for which we specifically provide a separate customer agreement. Our Paid Services include, but are not limited to:

- Amazon Simple Storage Service (Amazon S3)
- Amazon CloudFront
- Amazon Simple Queue Service (Amazon SQS)
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Alexa® Web Information Service (AWIS)
- Alexa® Web Search
- Alexa® Top Sites
- Amazon Flexible Payments Service (Amazon FPS)
- Amazon DevPay Service (Amazon DevPay)
- Amazon SimpleDB Service (Amazon SimpleDB)
- Amazon Elastic MapReduce
- Amazon Virtual Private Cloud (Amazon VPC)
- Amazon Multi-Factor Authentication (Amazon MFA)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Web Services Premium Support (AWS Premium Support)

If you use Amazon FPS, you may incur fees for transactions that you submit through the Payment Service provided by Amazon Payments, which is described in Section 8, below. We may,

in our sole discretion, (i) begin charging fees for a Free Service, in which case such Service will thereafter be deemed a Paid Service, or (ii) cease charging fees for a Paid Service, in which case such Service will thereafter be deemed a Free Service.

2. Modifications to this Agreement

You agree that we may modify this Agreement or any policy or other terms referenced in this Agreement (collectively, "Additional Policies") at any time by posting a revised version of the Agreement or such Additional Policy on the AWS Website or our "Developer Connection" pages accessible at http://developer.amazonwebservices.com/connect/index.jspa. The revised terms shall be effective as follows:

- if the revised terms are for (a) any Paid Services which we are adding at the time of the revision, (b) Amazon FPS and Amazon DevPay, (c) the Privacy Notice, (d) the Terms of Use, (e) any Service Terms or the AUP, (f) any other general terms and conditions applicable to our services, web sites or other properties, or (g) any Free Service, then the revised terms shall be effective upon posting (unless we expressly state otherwise at the time of posting); and
- if the revised terms are otherwise for any then-existing Paid Services, then the revised terms shall be effective upon the earlier to occur of (a) fifteen (15) days after posting and (b) if we provide a mechanism for your immediate acceptance of the revised terms, such as a click-through confirmation or acceptance button, your acceptance.

By continuing to use or receive the Services after the effective date of any revisions to this Agreement or any Additional Policies, you agree to be bound by the revised Agreement or any revised Additional Policies. It is your responsibility to check the AWS Website and the Developer Connection pages regularly for changes to this Agreement or the Additional Policies, as applicable. We last modified this Agreement on the date set forth at the top of this Agreement.

3. Term, Termination and Suspension

3.1. Term. The term of this Agreement ("Term") will commence, and you may begin using the Services, once you agree to the terms and conditions of this Agreement by clicking the "Accept" button below and complete the registration process for your Amazon Web Services account. The Agreement will remain in effect until terminated by you or us in accordance with this Section 3.

3.2. Termination by You for Convenience. You may terminate this Agreement for any reason or no reason at all, at your convenience, by (i) providing us written notice of termination in accordance with Section 15 and (ii) closing your account for any Service for which we provide an account closing mechanism.

3.3. Termination or Suspension by Us Other Than for Cause.

3.3.1. Free Services. We may suspend your right and license to use any or all Free Services and any associated Amazon Properties (as defined in Section 6.1 below), or, if you are only using Free Services, terminate this Agreement in its entirety (and, accordingly, cease providing all Services to you), for any reason or for no reason, at our discretion at any time, immediately upon notice to you in accordance with the notice provisions set forth in Section 15 below.

3.3.2. Paid Services (other than Amazon FPS and Amazon DevPay). We may suspend your right and license to use any or all Paid Services (and any associated Amazon Properties) other than Amazon FPS and Amazon DevPay, or terminate this Agreement in its entirety (and, accordingly, cease providing all Services to you), for any reason or for no reason, at our discretion at any time by providing you sixty (60) days' advance notice in accordance with the notice provisions set forth in Section 15 below.

3.3.3. Amazon FPS and Amazon DevPay. We may suspend your right and license to use Amazon FPS or Amazon DevPay and any associated Amazon Properties, or, if you are only using Amazon FPS, terminate this Agreement in its entirety (and, accordingly, cease providing all

Services to you), for any reason or for no reason, at our discretion at any time, immediately upon notice to you in accordance with the notice provisions set forth in Section 15 below.

3.4. Termination or Suspension by Us for Cause. We may suspend your right and license to use any individual Service or any set of Services, or terminate this Agreement in its entirety (and, accordingly, your right to use all Services), for cause effective as set forth below:

3.4.1. Immediately upon our notice to you in accordance with the notice provisions set forth in Section 15 below if: (i) you attempt a denial of service attack on any of the Services; (ii) you seek to hack or break any security mechanism on any of the Services or we otherwise determine that your use of the Services or the Amazon Properties poses a security or service risk to us, to any user of services offered by us, to any third party sellers on any of our websites, or to any of our or their respective customers or may subject us or any third party to liability, damages or danger; (iii) you otherwise use the Services in a way that disrupts or threatens the Services; (iv) you are in default of your payment obligations hereunder and there is an unusual spike or increase in your use of the Services; (v) we determine, in our sole discretion, there is evidence of fraud with respect to your account; (vi) you use any of the AWS Content (as defined in Section 6.1) or Marks (as defined in Section 6.2) other than as expressly permitted herein; (vii) we receive notice or we otherwise determine, in our sole discretion, that you may be using AWS Services for any illegal purpose or in a way that violates the law or violates, infringes, or misappropriates the rights of any third party; (viii) we determine, in our sole discretion, that our provision of any of the Services to you is prohibited by applicable law, or has become impractical or unfeasible for any legal or regulatory reason; or (ix) subject to applicable law, upon your liquidation, commencement of dissolution proceedings, disposal of your assets, failure to continue your business, assignment for the benefit of creditors, or if you become the subject of a voluntary or involuntary bankruptcy or similar proceeding.

3.4.2. Fifteen (15) days following our provision of notice to you in accordance with the notice provisions set forth in Section 15 below if you are in default of any payment obligation with respect to any of the Services or if any payment mechanism you have provided to us is invalid or charges are refused for such payment mechanism, and you fail to cure such payment obligation default or correct such payment mechanism problem within such 15 day period.

3.4.3. Five (5) days following our provision of notice to you in accordance with the notice provisions set forth in Section 15 below if you breach any other provision of this Agreement and fail, as determined by us, in our sole discretion, to cure such breach within such 5 day period.

3.5. Effect of Suspension or Termination.

3.5.1. Suspension. Upon our suspension of your use of any Services, in whole or in part, for any reason, (i) fees will continue to accrue for any Services that are still in use by you (including Premium Support), notwithstanding the suspension (including your continued storage of data on the Amazon S3 or Amazon SimpleDB service during the period of suspension); (ii) you remain liable for all fees, charges and any other obligations you have incurred through the date of suspension with respect to the Services; and (iii) all of your rights with respect to the applicable Services shall be terminated during the period of the suspension.

3.5.2. Termination. Upon termination of this Agreement for any reason: (i) you remain liable for all fees, charges and any other obligations you have incurred through the date of termination with respect to the Services; (ii) all of your rights under this Agreement shall immediately terminate; and (iii) you shall immediately return, or if instructed by us, destroy all AWS Confidential Information (as defined in Section 9 below) and any Amazon Properties then in your possession.

3.6. Survival. In the event this Agreement is terminated for any reason, Sections 3.5, 3.6, 3.7, 3.8, 4.2, 6, 8 (with respect to payments that are accrued but unpaid at the time of termination), and 9 through 16 will survive any such termination.

3.7. Data Preservation in the Event of Suspension or Termination.

3.7.1. In the Event of Suspension Other Than for Cause. In the event of a suspension by us of your access to any Service for any reason other than a for cause suspension under Section 3.4.1, during the period of suspension, (i) we will not take any action to intentionally erase any of your data stored on the Services and (ii) applicable Service data storage charges will continue to accrue.

3.7.2. In the Event of Termination Other Than for Cause. In the event of any termination by us of any Service or any set of Services, or termination of this Agreement in its entirety, other than a for cause termination under Section 3.4.1, (i) we will not take any action to intentionally erase any of your data stored on the Services for a period of thirty (30) days after the effective date of termination; and (ii) your post termination retrieval of data stored on the Services will be conditioned on your payment of Service data storage charges for the period following termination, payment in full of any other amounts due us, and your compliance with terms and conditions we may establish with respect to such data retrieval.

3.7.3. In the Event of Other Suspension or Termination. Except as provided in Sections 3.7.1 and 3.7.2 above, we shall have no obligation to continue to store your data during any period of suspension or termination or to permit you to retrieve the same.

3.8. Post-Termination Assistance. Following the suspension or termination of your right to use the Services by us or by you for any reason other than a for cause termination (i.e., a termination under Section 3.2 or under Section 3.3), you shall be entitled to take advantage of any post-termination assistance we may generally make available with respect to the Services, such as data retrieval arrangements we may elect to make available. We may also endeavor to provide you unique post-suspension or post-termination assistance, but we shall be under no obligation to do so. Your right to take advantage of any such assistance, whether generally made available with respect to the Services or made available uniquely to you, shall be conditioned upon your acceptance of and compliance with any fees and terms we specify for such assistance.

4. Authorization and License to Use the Services

Subject to your acceptance of and compliance with this Agreement and with the payment requirements for the Services that are set forth on the applicable Service detail page on the AWS Website (as such payment terms may be updated from time to time), we hereby grant you a limited, non-exclusive, non-transferable, non-sublicenseable right and license, in and under our intellectual property rights, to access and use the Services, solely in accordance with the terms and conditions of this Agreement.

4.1. Permitted Uses Generally.

4.1.1. You may write or develop software, web sites, or other online services or technology that you store in, or that interface with, the Services (collectively "Applications"). Applications include machine images containing software applications, libraries, data and associated configuration settings ("AMIs"). You acknowledge that we may change, deprecate or republish APIs (as defined in Section 6.1 below) for any Service or feature of a Service from time to time, and that it is your responsibility to ensure that calls you make to any Service are compatible with then-current APIs for the Service. You further acknowledge that we may change or remove features or functionality of the Services at any time.

4.1.2. You may enable access and use of Your Content by your end users in accordance with the terms of this Agreement. "Your Content" means any Application, data or other content that you may (a) provide to us pursuant to this Agreement, (b) make available to any end users in conjunction with the Services, or (c) develop, or use in connection with the Services. Your Content includes, but is not limited to, software, data, and content that you or your end users upload to ours systems as a part of an Application. You are responsible for all terms and conditions applicable to Your Content.

4.1.3. You may make network calls or requests to the Services at any time that the Services are available, provided that, unless otherwise set forth in the Service Terms applicable to any Service, you (or if you build and release an Application, each installed copy of your Application)

may not exceed the maximum file size or maximum calls per second limit (if any) set forth in the Service Terms for any particular Service (or, in the event the Service Terms for a Service do not indicate a maximum file size, greater than 40K).

4.2. Restricted Uses Generally.

4.2.1. You may not interfere or attempt to interfere in any manner with the functionality or proper working of the Services.

4.2.2. You may not compile or use the Amazon Properties or any other information obtained through the Services for the purpose of direct marketing, spamming, unsolicited contacting of sellers or customers, or other impermissible advertising, marketing or other activities, including, without limitation, any activities that violate anti-spamming laws and regulations.

4.2.3. You may not remove, obscure, or alter any notice of any Mark, or other intellectual property or proprietary right designation appearing on or contained within the Services or on any Amazon Properties.

4.2.4. Subject to the terms and conditions of this Agreement, you may generally publicize your use of the Services; however, you may not issue any press release with respect to the Services or this Agreement without our prior written consent.

4.3. Accounts and Keys. Unless otherwise stated in the applicable Service Terms, you may only create one account per email address. AWS accounts are associated with one or more public key/private key pairs, which are used to access the service. Examples include an Amazon-issued Access Key ID string (as a public key) and an Amazon-issued Secret Access Key string (as a private key), or an X.509 certificate (as a public key) and its corresponding private key. When you complete the account creation process, you will be issued unique account identifiers ("Account Identifiers"), and may add a public key to your account. Account Identifiers (i) identify your account and (ii) allow you to make requests to AWS. The Account Identifier is immutable and will always uniquely identify your AWS account. Public key/private key pairs are unique to your account and are subject to change. Private keys are for your personal use only, and you may not sell, transfer, sublicense or otherwise disclose your private key to any other party. You may use your public key in the open in requests to AWS; your public key is therefore not secret. However, you are responsible for maintaining the secrecy and security of your private key. You are fully responsible for all activities that occur under your Account Identifiers, regardless of whether such activities are undertaken by you or a third party. Therefore, you should contact us immediately if you believe a third party may be using your private key, or if your private key is otherwise lost or stolen. You are responsible for maintaining up-to-date and accurate information (including contact information) for your AWS account. We are not responsible for any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of Your Content or other data which you submit or use in connection with your account or the Services.

5. Acceptable Use Policy and Service Terms

You may only use the Services in accordance with the AUP and the applicable Service Terms.

6. License to Use the Amazon Properties

6.1. Amazon Properties. We may make available to you, for your installation, copying and/or use in connection with the Services, from time to time, a variety of software, data and other content and printed and electronic documentation (all such materials except those specifically made available by us under separate license terms, the "Amazon Properties"). Subject to your acceptance of this Agreement, ongoing compliance with its terms and conditions with respect to the subject Service, and payment if and as required for your right to use the subject Service, we hereby grant to you, without the right to sublicense, a limited, non-exclusive, non-transferable license during the Term, under our intellectual property or proprietary rights in the Amazon Properties, only to install, copy and use the Amazon Properties solely in connection with and as necessary for your use of such Services and solely to the extent in compliance with

all the terms and conditions of this Agreement. The Amazon Properties may include, without limitation:

- Proprietary application programming interfaces ("APIs");
- Developer tools for use in connection with the APIs;
- Articles and documentation for use in connection with the use and implementation of the APIs (collectively, "Documentation");
- Specifications describing the operational and functional capabilities, use limitations, technical and engineering requirements, and testing and performance criteria relevant to the proper use of a Service and its related APIs and other technology;
- Textual materials made available as part of the Service ("Text Materials"); and
- Other forms of digital content, data, text, images, logos, user interface designs and other creative designs, audio and video (with the Text Materials, collectively, "AWS Content").

Sample source code which we may make available from time to time for use in connection with the Services ("Sample Source Code") and libraries which we may make available from time to time for use in connection with the Services ("Libraries") will be made available to you under separate license that accompanies each Sample Source Code or Library and the term "Amazon Properties," as used herein, specifically excludes any Sample Source Code or Libraries made available to you under separate license.

Except as may be expressly authorized under this Agreement:

- You may not, and may not attempt to, modify, alter, tamper with, repair, or otherwise create derivative works of any software included in or accessed via the Amazon Properties.
- You may not, and may not attempt to, reverse engineer, disassemble, or decompile the Amazon Properties or the Services or apply any other process or procedure to derive the source code of any software included in or accessed via the Amazon Properties.
- You may edit Text Materials only by deleting text from and reducing the length of the Text Materials and only if, in doing so, you do not materially alter the meaning of the Text Materials or cause the Text Materials to become factually incorrect or misleading. You may not add additional information to the Text Materials (e.g., you may not insert words into a customer review or supplement a wish list or Listmania® list with new items). You hereby irrevocably assign to us any and all intellectual property or proprietary rights in such edited Text Material.

6.2. Restrictions with Respect to Use of Marks. Your use of any trademarks, service marks, service or trade names, logos, and other designations of AWS and its affiliates or licensors ("Marks") shall strictly comply with the Trademark Guidelines and the following provisions. You may use the Marks in conjunction with the display of the AWS Content and for the purpose of indicating that your Application was created using the Services. You must immediately discontinue use of any Mark as specified by us at any time in writing. We may modify any Marks provided to you at any time, and upon notice, you will use only the modified Marks and not the old Marks. Other than as specified in this Agreement, you may not use any trademark, service mark, trade name or other business identifier of Amazon or its affiliates unless you obtain Amazon's or its affiliates' prior written consent. In addition, you agree not to misrepresent or embellish the relationship between us and you, for example by implying that we support, sponsor, endorse, or contribute money to you or your business endeavors.

6.3. Nonexclusive Rights. The rights granted by Amazon in this Agreement with respect to the Amazon Properties, the Marks and the Services are nonexclusive, and Amazon reserves the right to: (i) itself act as a developer of products or services related to any of the products that you may develop in connection with the Amazon Properties or via your use of the Services; and

(ii) appoint third parties as developers or systems integrators who may offer products or services which compete with Amazon or your Application.

7. Downtime and Service Suspensions; Security

7.1. Downtime and Service Suspensions. In addition to our rights to terminate or suspend Services to you as described in Section 3 above, you acknowledge that: (i) your access to and use of the Services may be suspended for the duration of any unanticipated or unscheduled downtime or unavailability of any portion or all of the Services for any reason, including as a result of power outages, system failures or other interruptions; and (ii) we shall also be entitled, without any liability to you, to suspend access to any portion or all of the Services at any time, on a Service-wide basis: (a) for scheduled downtime to permit us to conduct maintenance or make modifications to any Service; (b) in the event of a denial of service attack or other attack on the Service or other event that we determine, in our sole discretion, may create a risk to the applicable Service, to you or to any of our other customers if the Service were not suspended; or (c) in the event that we determine that any Service is prohibited by law or we otherwise determine that it is necessary or prudent to do so for legal or regulatory reasons (collectively, "Service Suspensions"). Without limitation to Section 11.5, we shall have no liability whatsoever for any damage, liabilities, losses (including any loss of data or profits) or any other consequences that you may incur as a result of any Service Suspension. To the extent we are able, we will endeavor to provide you email notice of any Service Suspension in accordance with the notice provisions set forth in Section 15 below and to post updates on the AWS Websites regarding resumption of Services following any such suspension, but shall have no liability for the manner in which we may do so or if we fail to do so.

7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, without limitation to Section 4.3 above and Section 11.5 below, you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications. We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.

8. Fees

8.1. Service Fees. In consideration of your use of any of the Paid Services, you agree to pay applicable fees for Paid Services in the amounts set forth on the respective Service detail pages on the AWS Website (including any minimum subscription fees). You are responsible for any fees assessed by Amazon Payments for transactions that you submit to the Payment Service using Amazon FPS. Fees for any new Service or new Service feature will be effective upon posting by us on the AWS Website for the applicable Service. We may increase or add new fees for any existing Service or Service feature, or implement a fee for any previously Free Service or Free Service feature, by giving you 30 days' advance notice. Such notice will be posted on the AWS Website on the Service detail page for the affected Service. You agree that you are responsible for checking the AWS Website each month to confirm whether there are any new fees and their effective date(s). All fees payable by you are exclusive of applicable taxes and duties, including, without limitation, VAT and applicable sales tax. You will provide such information to us as reasonably required to determine whether we are obligated to collect VAT from you, including without limitation your VAT identification number.

8.2. Payment. We may specify the manner in which you will pay any fees, and any such payment shall be subject to our general accounts receivable policies from time to time in effect. All amounts payable by you under this Agreement will be made without setoff or counterclaim and without deduction or withholding. If any deduction or withholding is required by applicable law, you shall notify us and shall pay such additional amounts to us as necessary to ensure that the net amount that we receive, after such deduction and withholding, equals the amount we would have received if no such deduction or withholding had been required. Additionally, you

shall provide us with documentation that the withholding and deducted amounts have been paid to the relevant taxing authority.

8.3. Special Pricing Programs. From time to time, we may offer free or discounted pricing for compute capacity, data transfer, data storage, and other usage of certain Services (each a "Special Pricing Program"). After a Special Pricing Program ends, normal charges will apply. You must comply with any additional terms, restrictions, or limitations (e.g., limitations on the total amount of usage) we impose in connection with the Special Pricing Program as described on the Service-specific detail pages on the AWS Website. You may not sign-up for multiple AWS accounts in order to receive additional benefits under a Special Pricing Program. We may immediately terminate any account that we determine, in our sole discretion, is established or used to avoid the terms, restrictions, or limitations applicable to a Special Pricing Program. Any data stored as part of a Special Pricing Program must be actively used.

9. Confidentiality

9.1. Use and Disclosure. You shall not disclose AWS Confidential Information during the Term or at any time during the three (3) year period following the end of the Term. As used in this Agreement, "AWS Confidential Information" means all nonpublic information disclosed by us, our business partners or our or their respective agents or contractors that is designated as confidential or that, given the nature of the information or circumstances surrounding its disclosure, reasonably should be understood to be confidential. AWS Confidential Information includes, without limitation, (i) nonpublic information relating to our or our business partners' technology, customers, business plans, promotional and marketing activities, finances and other business affairs (including, but not limited to, any information about or involving one of our so-called beta tests or a beta test product that you obtain as a result of your participation in such beta test), (ii) third-party information that we are obligated to keep confidential, and (iii) the nature, content and existence of any discussions or negotiations between you and us. Confidential Information does not include any information described in Section 9.2 or any information that you are required to disclose by law.

9.2. Excluded Information. Notwithstanding any other provision in this Agreement, you shall not have any confidentiality obligation to us under Section 9.1 above, with respect to any information provided or made available by us hereunder, and we shall not have any confidentiality or non-use obligation to you hereunder with respect to any information, software application, data or content provided or made available by you hereunder that: (i) is or becomes publicly available without breach of this Agreement; (ii) can be shown by documentation to have been known to the receiving party at the time of its receipt from the disclosing party; (iii) is received from a third party who did not acquire or disclose the same by a wrongful or tortious act; or (iv) can be shown by documentation to have been independently developed by the receiving party.

9.3. Conflict with Separate Non-Disclosure Agreement. If you and we are parties to a separate non-disclosure agreement ("Stand-Alone NDA") and there is a conflict between the terms of the Stand-Alone NDA and the terms of this Section 9, the terms of the Stand-Alone NDA shall control.

10. Intellectual Property

10.1. Our Services and the Amazon Properties. Other than the limited use and access rights and licenses expressly set forth in this Agreement, we reserve all right, title and interest (including all intellectual property and proprietary rights) in and to: (i) the Services; (ii) the Amazon Properties; (iii) the Marks; and (iv) any other technology and software that we provide or use to provide the Services and the Amazon Properties. You do not, by virtue of this Agreement or otherwise, acquire any ownership interest or rights in the Services, the Amazon Properties, the Marks, or other technology and software (including third party technology and software), except for the limited use and access rights described in this Agreement.

10.2. Your Applications, Data and Content. Other than the rights and interests expressly set forth in this Agreement, and excluding Amazon Properties and works derived from Amazon Properties, you reserve all right, title and interest (including all intellectual property and proprie-

tary rights) in and to Your Content. We will not disclose Your Content, except: (i) if you expressly authorize us to do in connection with your use of the Services; or (ii) as necessary to provide the Services to you, or to comply with the Agreement or the request of a governmental or regulatory body, subpoenas or court orders.

10.3. Feedback. In the event you elect, in connection with any of the Services, to communicate to us suggestions for improvements to the Services, the Amazon Properties or the Marks (collectively, "Feedback"), we shall own all right, title, and interest in and to the same, even if you have designated the Feedback as confidential, and we shall be entitled to use the Feedback without restriction. You hereby irrevocably assign all right, title and interest in and to the Feedback to us and agree to provide us such assistance as we may require to document, perfect, and maintain our rights to the Feedback.

10.4. Non-Assertion. During and after the term of the Agreement, with respect to any of the Services that you elect to use, you will not assert, nor will you authorize, assist, or encourage any third party to assert, against us or any of our customers, end users, vendors, business partners (including third party sellers on websites operated by or on behalf of us), licensors, sublicensees or transferees, any patent infringement or other intellectual property infringement claim with respect to such Services.

11. Representations and Warranties; Disclaimers; Limitations of Liability

11.1. Use of the Services. You represent and warrant that you will not use the Services, Amazon Properties and/or your Application and Your Content: (i) in a manner that infringes, violates or misappropriates any rights of us or any third party; (ii) to engage in spamming or other impermissible advertising, marketing or other activities, including, without limitation, any activities that violate anti-spamming laws and regulations, including, without limitation, the CAN SPAM Act of 2003; (iii) in any manner that constitutes or facilitates the illegal export of any controlled or otherwise restricted items, including, without limitation, software, algorithms or other data that is subject to export laws; and/or (iv) in a way that is otherwise illegal or promotes illegal activities, including, without limitation, in a manner that might be libelous or defamatory or otherwise malicious or harmful to any person or entity, or discriminatory based on race, sex, religion, nationality, disability, sexual orientation, or age.

11.2. Applications and Content. You represent and warrant: (i) that you are solely responsible for the development, operation, and maintenance of Your Content, including without limitation, the accuracy, security, appropriateness and completeness of Your Content and all product-related materials and descriptions; (ii) that you have the necessary rights and licenses, consents, permissions, waivers and releases to use and display Your Content; (iii) that Your Content (a) does not violate, misappropriates or infringes any rights of us or any third party, (b) does not constitutes defamation, invasion of privacy or publicity, or otherwise violates any rights of any third party, or (c) is not designed for use in any illegal activity or to promote illegal activities, including, without limitation, use in a manner that might be libelous or defamatory or otherwise malicious, illegal or harmful to any person or entity, or discriminatory based on race, sex, religion, nationality, disability, sexual orientation, or age; (iv) that Your Content does not contain any unauthorized data, malware, viruses, Trojan horses, spyware, worms, or other malicious or harmful code (collectively "Harmful Components"); and (v) to the extent to which you use any of the Marks, that you will conduct your business in a professional manner and in a way that reflects favorably on the goodwill and reputation of Amazon.

11.3. Public Software and Feedback. You represent and warrant that you will not use, and will not authorize any third party to use, any Public Software in connection with the Services in any manner that requires, pursuant to the license applicable to such Public Software, that any Amazon Properties or Services be (a) disclosed or distributed in source code form, (b) made available free of charge to recipients, or (c) modifiable without restriction by recipients. With respect to any Feedback, you represent and warrant that such Feedback, in whole or in part, contributed by or through you, (i) contains no third party software or any software that may be considered Public Software and (ii) does not violate, misappropriate or infringe any intellectual property rights of any third party. "Public Software" means any software, documentation or

other material that contains, or is derived (in whole or in part) from, any software, documentation or other material that is distributed as free software, open source software (e.g., Linux) or similar licensing or distribution models, including, but not limited to software, documentation or other material licensed or distributed under any of the following licenses or distribution models, or licenses or distribution models similar to any of the following: (i) GNU's General Public License (GPL), Lesser/Library GPL (LGPL), or Free Documentation License, (ii) The Artistic License (e.g., PERL), (iii) the Mozilla Public License, (iv) the Netscape Public License, (v) the Sun Community Source License (SCSL), (vi) the Sun Industry Standards License (SISL), (vii) the BSD License and (viii) the Apache License.

11.4. Authorization and Account Information. You represent and warrant that: (i) the information you provide in connection with your registration for the Services is accurate and complete; (ii) if you are registering for the Services as an individual, that you are at least 18 years of age and have the legal capacity to enter into this Agreement; and (iii) if you are registering for the Services as an entity or organization, (a) you are duly authorized to do business in the country or countries where you operate, (b) the individual clicking "Accept" on this Agreement and completing the registration for the Services meets the requirements of subsection (ii) above and is an authorized representative of your entity, and (c) your employees, officers, representatives and other agents accessing the Services are duly authorized to access the Services and to legally bind you to this Agreement and all transactions conducted under your account.

11.5. Disclaimers. AMAZON PROPERTIES, THE MARKS, THE SERVICES AND ALL TECHNOLOGY, SOFTWARE, FUNCTIONS, CONTENT, IMAGES, MATERIALS AND OTHER DATA OR INFORMATION PROVIDED BY US OR OUR LICENSORS IN CONNECTION THEREWITH (COLLECTIVELY THE "SERVICE OFFERINGS") ARE PROVIDED "AS IS". WE AND OUR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE WITH RESPECT TO THE SERVICE OFFERINGS. EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, WE AND OUR LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE. 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.

11.6. Your Applications are Your Responsibility. In addition to the foregoing, we specifically disclaim all liability, and you shall be solely responsible for the development, operation, and maintenance of your Application (including any Bundled Application) and for all materials that appear on or within your Application and you agree that you shall, without limitation, be solely responsible for:

11.6.1. the technical operation of your Application and all related equipment;

11.6.2. the accuracy and appropriateness of any materials posted on or within your Application (including, among other things, any product-related materials);

11.6.3. ensuring that any materials posted on your site or within your Application are not illegal and do not promote illegal activities, including without limitation any activities that might be libelous or defamatory or otherwise malicious, illegal or harmful to any person or entity, or discriminatory based on race, sex, religion, nationality, disability, sexual orientation, or age;

11.6.4. ensuring that your Application accurately and adequately discloses, either through a privacy policy or otherwise, how you collect, use, store, and disclose data collected from visitors, including, where applicable, that third parties (including advertisers) may serve content and/or advertisements and collect information directly from visitors and may place or recognize cookies on visitors' browsers;

11.6.5. any of your users' or customers' claims relating to your Application or any Services utilized in connection with your Application; and

11.6.6. your election to utilize AMIs, sample code and libraries that may be made available on the AWS Website, many of which may be provided by third parties and many of which we have not tested or screened in any way.

11.7. Links. The AWS Website and/or the Services may contain links to websites that are not under our control ("Third Party Sites"). We are not responsible for the contents or functionality of any Third Party Sites or any website that can be accessed via links on any Third Party Site. We provide these links to you as a convenience and the inclusion of any such links does not constitute or imply our endorsement or validation of any Third Party Site.

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.

12. Indemnification

12.1. General. You agree to indemnify, defend and hold us, our affiliates and licensors, each of our and their business partners (including third party sellers on websites operated by or on behalf of us) and each of our and their respective employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses (including reasonable attorneys fees), arising out of or in connection with any claim arising out of (i) your use of the Services and/or Amazon Properties in a manner not authorized by this Agreement, and/or in violation of the applicable restrictions, Additional Policies, and/or applicable law, (ii) Your Content, or the combination of either with other applications, content or processes, including but not limited to any claim involving infringement or misappropriation of third-party rights and/or the use, development, design, manufacture, production, advertising, promotion and/or marketing of Your Content, (iii) your violation of any term or condition of this Agreement or any applicable Additional Policies, including without limitation, your representations and warranties, or (iv) you or your employees' or personnel's negligence or willful misconduct.

12.2. Notification. We agree to promptly notify you of any claim subject to indemnification; provided that our failure to promptly notify you shall not affect your obligations hereunder except to the extent that our failure to promptly notify you delays or prejudices your ability to defend the claim. At our option, you will have the right to defend against any such claim with counsel of your own choosing (subject to our written consent) and to settle such claim as you deem appropriate, provided that you shall not enter into any settlement without our prior written consent and provided that we may, at any time, elect to take over control of the defense and settlement of the claim.

13. US Government License Rights; Import and Export Compliance

13.1. U.S. Government License Rights. All Services provided to the U.S. Government are provided under the commercial license rights and restrictions generally applicable under this Agreement.

13.2. Import and Export Compliance and Restrictions. You shall, in connection with your use of the Services or the Amazon Properties, comply with all applicable import, export and re-export control laws and regulations of any country, including the U.S. Export Administration Regulations, the U.S. International Traffic in Arms Regulations, Council Regulation (EC) No 428/2009 on the control of exports of dual-use items and technology, and country-specific economic sanctions programs or embargoes adopted against countries or individuals under any applicable national or international legislation, including any measures implemented by the U.S. Office of Foreign Assets Control.

14. Disputes

14.1. Notwithstanding anything to the contrary, we may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of Amazon's or any third party's intellectual property and/or proprietary rights. Any dispute relating in any way to your visit to the AWS Website or to products or services sold or distributed by AWS or its affiliates in which the aggregate total claim for relief sought on behalf of one or more parties exceeds $7,500 shall be adjudicated in any state or federal court in King County, Washington, and you consent to exclusive jurisdiction and venue in such courts. You further acknowledge that our rights in the Amazon Properties are of a special, unique, extraordinary character, giving them peculiar value, the loss of which cannot be readily estimated and may not be adequately compensated for in monetary damages.

14.2. Governing Law. By using the Services, you agree that the laws of the State of Washington, without regard to principles of conflicts of laws, will govern this Agreement and any dispute of any sort that might arise between you and us. The parties expressly exclude application of the United Nations Convention for the International Sale of Goods to this Agreement.

15. Notices

15.1. To You. Except as otherwise set forth herein, notices made by us to you under this Agreement that affect our customers generally (e.g., notices of updated fees, etc.) will be posted on the AWS Website. Notices made by us under this Agreement for you or your account specifically (e.g., notices of breach and/or suspension) will be provided to you via the email address provided to us in your registration for the Services or in any updated email address you provide to us in accordance with standard account information update procedures we may provide from time to time. It is your responsibility to keep your email address current and you will be deemed to have received any email sent to any such email address, upon our sending of the email, whether or not you actually receive the email.

15.2. To Us. For notices made by you to us under this Agreement and for questions regarding this Agreement or the Services, you may contact Amazon as follows:

aws@amazon.com

and/or

Amazon Web Services LLC
410 Terry Ave. North
Seattle, WA 98109

15.3. Language. All communications and notices to be made or given pursuant to this Agreement shall be in the English language.

16. Miscellaneous Provisions

16.1. Third Party Activities. If you authorize, assist, encourage or facilitate another person or entity to take any action related to the subject matter of this Agreement, you shall be deemed to have taken the action yourself.

16.2. Severability. If any portion of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remaining portions of this Agreement will remain in full force and effect, and any invalid or unenforceable portions shall be construed in a manner that most closely reflects the effect and intent of the original language. If such construction is not possible, the provision will be severed from this Agreement, and the rest of the Agreement shall remain in full force and effect.

16.3. Waivers. The failure by us to enforce any provision of this Agreement shall in no way be construed to be a present or future waiver of such provision nor in any way affect our right to enforce such provision thereafter. All waivers by us must be in writing to be effective.

16.4. Successors and Assigns. This Agreement will be binding upon, and inure to the benefit of the parties and their respective successors and assigns.

16.5. Entire Agreement. This Agreement incorporates by reference all policies and guidelines posted on the AWS Website, including all Additional Policies, and constitutes the entire agreement between you and us regarding the subject matter hereof and supersedes any and all prior or contemporaneous representation, understanding, agreement, or communication between you and us, whether written or oral, regarding such subject matter.

16.6. No Endorsement. You understand and acknowledge that we are not certifying nor endorsing, and have no obligation to certify or endorse, any of your Applications or Your Content.

16.7. Relationship. Nothing in this Agreement is intended to or does create any type of joint venture, creditor-debtor, escrow, partnership or any employer/employee or fiduciary or franchise relationship between you and us (or any of our affiliates).

Quelle: http://aws.amazon.com/agreement/ (Zugriff am 01. September 2010).

Amazon.com Privacy Notice

Last updated: October 1, 2008. To see what has changed, click here.

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. **By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.**

What Personal Information About Customers Does Amazon.com Gather?

The information we learn from customers helps us personalize and continually improve your shopping experience at Amazon.com. Here are the types of information we gather.

- **Information You Give Us:** We receive and store any information you enter on our Web site or give us in any other way. Click here to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you.
- **Automatic Information:** We receive and store certain types of information whenever you interact with us. For example, like many Web sites, we use "cookies," and we obtain certain types of information when your Web browser accesses Amazon.com or advertisements and other content served by or on behalf of Amazon.com on other Web sites. Click here to see examples of the information we receive.
- **E-mail Communications:** To help us make e-mails more useful and interesting, we often receive a confirmation when you open e-mail from Amazon.com if your computer supports such capabilities. We also compare our customer list to lists received from other companies, in an effort to avoid sending unnecessary messages to our customers. If you do not want to receive e-mail or other mail from us, please adjust your Customer Communication Preferences.
- **Information from Other Sources:** We might receive information about you from other sources and add it to our account information. Click here to see examples of the information we receive.

What About Cookies?

- Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your Web browser to enable our systems to recognize your browser and to provide features such as 1-Click purchasing, Recommended for You, personalized advertisements on other Web sites (e.g., Amazon Associates with content served by Amazon.com and Web sites using Checkout by Amazon payment service), and storage of items in your Shopping Cart between visits.
- The Help portion of the toolbar on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash cookies, by changing the add-on's settings or visiting the Web site of its manufacturer. However, because cookies allow you to take advantage of some of Amazon.com's essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Amazon.com products and services that require you to Sign in.

Does Amazon.com Share the Information It Receives?

Information about our customers is an important part of our business, and we are not in the business of selling it to others. We share customer information only as described below and with subsidiaries Amazon.com, Inc. controls that either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice.

- **Affiliated Businesses We Do Not Control:** We work closely with affiliated businesses. In some cases, such as Marketplace sellers, these businesses operate stores at Amazon.com or sell offerings to you at Amazon.com. In other cases, we operate stores, provide services, or sell product lines jointly with these businesses. Click here for some examples of co-branded and joint offerings. You can tell when a third party is involved in your transactions, and we share customer information related to those transactions with that third party.

- **Third-Party Service Providers:** We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service. They have access to personal information needed to perform their functions, but may not use it for other purposes.
- **Promotional Offers:** Sometimes we send offers to selected groups of Amazon.com customers on behalf of other businesses. When we do this, we do not give that business your name and address. If you do not want to receive such offers, please adjust your Customer Communication Preferences.
- **Business Transfers:** As we continue to develop our business, we might sell or buy stores, subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise). Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.
- **Protection of Amazon.com and Others:** We release account and other personal information when we believe release is appropriate to comply with the law; enforce or apply our Conditions of Use and other agreements; or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction. Obviously, however, this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for commercial purposes in violation of the commitments set forth in this Privacy Notice.
- **With Your Consent:** Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information.

How Secure Is Information About Me?

- We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input.
- We reveal only the last four digits of your credit card numbers when confirming an order. Of course, we transmit the entire credit card number to the appropriate credit card company during order processing.
- It is important for you to protect against unauthorized access to your password and to your computer. Be sure to sign off when finished using a shared computer. Click here for more information on how to sign off.

What About Third-Party Advertisers and Links to Other Websites?

Our site includes third-party advertising and links to other Web sites. We do not provide any personally identifiable customer information to these advertisers or third-party Web sites. Click here for more information about our Advertising Policies and Specifications.

These third-party Web sites and advertisers, or Internet advertising companies working on their behalf, sometimes use technology to send (or "serve") the advertisements that appear on our Web site directly to your browser. They automatically receive your IP address when this happens. They may also use cookies, JavaScript, web beacons (also known as action tags or single-pixel gifs), and other technologies to measure the effectiveness of their ads and to personalize advertising content. We do not have access to or control over cookies or other features that they may use, and the information practices of these advertisers and third-party Web sites are not covered by this Privacy Notice. Please contact them directly for more information about their privacy practices. In addition, the Network Advertising Initiative offers useful information about Internet advertising companies (also called "ad networks" or "network advertisers"), including information about how to opt-out of their information collection.

Amazon.com also displays personalized third-party advertising based on personal information about customers, such as purchases on Amazon.com, visits to Amazon Associate Web sites, or use of payment services like Checkout by Amazon on other Web sites. Click here for more information about the personal information that we gather. Although Amazon.com does not provide any personal information to advertisers, advertisers (including ad-serving companies) may assume that users who interact with or click on a personalized advertisement meet their criteria to personalize the ad (for example, users in the northwestern United States who bought or browsed for classical music). If you do not want us to use personal information that we gather to allow third parties to personalize advertisements we display to you, please adjust your Advertising Preferences.

Which Information Can I Access?

Amazon.com gives you access to a broad range of information about your account and your interactions with Amazon.com for the limited purpose of viewing and, in certain cases, updating that information. Click here to see some examples, the list of which will change as our Web site evolves.

What Choices Do I Have?

- As discussed above, you can always choose not to provide information, even though it might be needed to make a purchase or to take advantage of such Amazon.com features as Your Profile, Wish Lists, Customer Reviews, and Amazon Prime.
- You can add or update certain information on pages such as those referenced in the "Which Information Can I Access?" section. When you update information, we usually keep a copy of the prior version for our records.
- If you do not want to receive e-mail or other mail from us, please adjust your Customer Communication Preferences. (If you do not want to receive Conditions of Use and other legal notices from us, such as this Privacy Notice, those notices will still govern your use of Amazon.com, and it is your responsibility to review them for changes.)
- If you do not want us to use personal information that we gather to allow third parties to personalize advertisements we display to you, please adjust your Advertising Preferences.
- The Help portion of the toolbar on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash cookies, by changing the add-on's settings or visiting the Web site of its manufacturer. However, because cookies allow you to take advantage of some of Amazon.com's essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Amazon.com products and services that require you to Sign in.

Are Children Allowed to Use Amazon.com?

Amazon.com does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian.

Does Amazon.com Participate in the Safe Harbor Program?

Amazon.com is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union. We have certified that we adhere to the Safe Harbor Privacy Principles agreed upon by the U.S. and the E.U. For more information about the Safe Harbor and to view our certification, visit the U.S. Department of Commerce's Safe Harbor Web site. If you would like to contact Amazon.com directly about the Safe Harbor program, please send an e-mail to safeharbor@amazon.com.

Conditions of Use, Notices, and Revisions

If you choose to visit Amazon.com, your visit and any dispute over privacy is subject to this Notice and our Conditions of Use, including limitations on damages, resolution of disputes, and application of the law of the state of Washington. If you have any concern about privacy at Amazon.com, please contact us with a thorough description, and we will try to resolve it. Our business changes constantly, and our Privacy Notice and the Conditions of Use will change also. We may e-mail periodic reminders of our notices and conditions, unless you have instructed us not to, but you should check our Web site frequently to see recent changes. Unless stated otherwise, our current Privacy Notice applies to all information that we have about you and your account. We stand behind the promises we make, however, and will never materially change our policies and practices to make them less protective of customer information collected in the past without the consent of affected customers.

Related Practices and Information

- Conditions of Use
- Discussion Boards
- Community Rules
- Help department
- Most Recent Purchases
- Your Profile and Community Guidelines

Examples of Information Collected

Information You Give Us

You provide most such information when you search, buy, bid, post, participate in a contest or questionnaire, or communicate with customer service. For example, you provide information when you search for a product; place an order through Amazon.com or one of our third-party sellers; provide information in Your Account (and you might have more than one if you have used more than one e-mail address when shopping with us) or Your Profile; communicate with us by phone, e-mail, or otherwise; complete a questionnaire or a contest entry form; compile Wish Lists or other gift registries; provide employer information when opening a corporate account; participate in Discussion Boards or other community features; provide and rate Reviews; specify a Special Occasion Reminder; share information with Amazon Friends; and employ other Personal Notification Services, such as Available to Order Notifications. As a result of those actions, you might supply us with such information as your name, address, and phone numbers; credit card information; people to whom purchases have been shipped, including addresses and phone number; people (with addresses and phone numbers) listed in 1-Click settings; e-mail addresses of Amazon Friends and other people; content of reviews and e-mails to us; personal description and photograph in Your Profile; and financial information, including Social Security and driver's license numbers.

Automatic Information

Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information such as browser type, version, and time zone setting, browser plug-in types and versions, operating system, and platform; purchase history, which we sometimes aggregate with similar information from other customers to create features such as Purchase Circles and Top Sellers; the full Uniform Resource Locator (URL) clickstream to, through, and from our Web site, including date and time; cookie number; products you viewed or searched for; and the phone number you used to call our 800 number. We may also use browser data such as cookies, Flash cookies (also known as Flash Local Shared Objects), or similar data on certain parts of our Web site for fraud prevention and other purposes. During some visits we may use software tools such as JavaScript to measure and collect session information, including page response times, download errors, length of visits to certain pages, page interaction infor-

mation (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.

Information from Other Sources

Examples of information we receive from other sources include updated delivery and address information from our carriers or other third parties, which we use to correct our records and deliver your next purchase or communication more easily; account information, purchase or redemption information, and page-view information from some merchants with which we operate co-branded businesses or for which we provide technical, fulfillment, advertising, or other services (such as Target.com); search term and search result information from some searches conducted through the Web search features offered by our subsidiaries, Alexa Internet and A9.com; search results and links, including paid listings (such as Sponsored Links); and credit history information from credit bureaus, which we use to help prevent and detect fraud and to offer certain credit or financial services to some customers.

Co-branded and Joint Offerings

Examples of businesses with which we offer joint or co-branded products and other offerings include Target, CD Now, Verizon Wireless, Sprint, T-Mobile, AT&T, Shutterfly, J&R, Godiva, Avon, Macy's, PacSun, Eddie Bauer and Northern Tool + Equipment.

Information You Can Access

Examples of information you can access easily at Amazon.com include up-to-date information regarding recent orders; personally identifiable information (including name, e-mail, password, communications and personalized advertising preferences, address book, and 1-Click settings); payment settings (including credit card information and gift certificate, gift card, and check balances); e-mail notification settings (including Alerts, Available to Order notifications, Delivers, Recommended for You, Special Occasion Reminders, Weekly Movie Showtimes, and newsletters); recommendations (including recent product view history, prior order history, and Favorites); shopping lists and gift registries (including Wish Lists and Baby and Wedding Registries); Marketplace seller accounts; and Your Profile (including your product Reviews, Requests, and Recommendations, Listmania lists, "So You'd Like to..." guides, personal profile, people you tagged as interesting, and Amazon Friends).

Quelle:

http://www.amazon.com/gp/help/customer/display.html/?ie=UTF8&nodeId=468496 (Zugriff am 01. September 2010).

Amazon EC2 Service Level Agreement

Effective Date: October 23, 2008

This Amazon EC2 Service Level Agreement ("SLA") is a policy governing the use of the Amazon Elastic Compute Cloud ("Amazon EC2") under the terms of the Amazon Web Services Customer Agreement (the "AWS Agreement") between Amazon Web Services, LLC ("AWS", "us" or "we") and users of AWS' services ("you"). This SLA applies separately to each account using Amazon EC2. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Amazon EC2 available with an Annual Uptime Percentage (defined below) of at least 99.95% during the Service Year. In the event Amazon EC2 does not meet the Annual Uptime Percentage commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- "Service Year" is the preceding 365 days from the date of an SLA claim.
- "Annual Uptime Percentage" is calculated by subtracting from 100% the percentage of 5 minute periods during the Service Year in which Amazon EC2 was in the state of "Region Unavailable." If you have been using Amazon EC2 for less than 365 days, your Service Year is still the preceding 365 days but any days prior to your use of the service will be deemed to have had 100% Region Availability. Any downtime occurring prior to a successful Service Credit claim cannot be used for future claims. Annual Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Amazon EC2 SLA Exclusion (defined below).
- "Region Unavailable" and "Region Unavailability" means that more than one Availability Zone in which you are running an instance, within the same Region, is "Unavailable" to you.
- "Unavailable" means that all of your running instances have no external connectivity during a five minute period and you are unable to launch replacement instances.
- The "Eligible Credit Period" is a single month, and refers to the monthly billing cycle in which the most recent Region Unavailable event included in the SLA claim occurred.
- A "Service Credit" is a dollar credit, calculated as set forth below, that we may credit back to an eligible Amazon EC2 account.

Service Commitments and Service Credits

If the Annual Uptime Percentage for a customer drops below 99.95% for the Service Year, that customer is eligible to receive a Service Credit equal to 10% of their bill (excluding one-time payments made for Reserved Instances) for the Eligible Credit Period. To file a claim, a customer does not have to have wait 365 days from the day they started using the service or 365 days from their last successful claim. A customer can file a claim any time their Annual Uptime Percentage over the trailing 365 days drops below 99.95%.

We will apply any Service Credits only against future Amazon EC2 payments otherwise due from you; provided that, we may issue the Service Credit to the credit card that you used to pay for Amazon EC2 for the billing cycle in which the error occurred. Service Credits shall not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability or non-performance of Amazon EC2 or other failure by us to provide Amazon EC2 is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA or termination of your use of Amazon EC2.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a request by sending an e-mail message to aws-sla-request @ amazon.com. To be eligible, the credit request must (i) include your account number in the subject of the e-mail message (the account number can be found at the top of the AWS Account Activity page); (ii) include, in the body of the e-mail, the dates and times of each incident of Region Unavailable that you claim to have experienced including instance ids of the instances that were running and affected during the time of each incident; (iii) include your server request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks); and

(iv) be received by us within thirty (30) business days of the last reported incident in the SLA claim. If the Annual Uptime Percentage of such request is confirmed by us and is less than 99.95% for the Service Year, then we will issue the Service Credit to you within one billing cycle following the month in which the request occurred. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon EC2 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon EC2, or any other Amazon EC2 performance issues: (i) that result from Service Suspensions described in Section 7.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon EC2; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) that result from failures of individual instances not attributable to Region Unavailability; or (vi) arising from our suspension and termination of your right to use Amazon EC2 in accordance with the AWS Agreement (collectively, the "Amazon EC2 SLA Exclusions"). If availability is impacted by factors other than those explicitly listed in this agreement, we may issue a Service Credit considering such factors in our sole discretion.

Quelle: http://aws.amazon.com/ec2-sla/ (Zugriff am 01. September 2010).

Amazon S3 Service Level Agreement

Effective Date: October 1, 2007

This Amazon S3 Service Level Agreement ("SLA") is a policy governing the use of the Amazon Simple Storage Service ("Amazon S3") under the terms of the Amazon Web Services Customer Agreement (the "AWS Agreement") between Amazon Web Services, LLC ("AWS", "us" or "we") and users of AWS' services ("you"). This SLA applies separately to each account using Amazon S3. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Amazon S3 available with a Monthly Uptime Percentage (defined below) of at least 99.9% during any monthly billing cycle (the "Service Commitment"). In the event Amazon S3 does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- "Error Rate" means: (i) the total number of internal server errors returned by Amazon S3 as error status "InternalError" or "ServiceUnavailable" divided by (ii) the total number of requests during that five minute period. We will calculate the Error Rate for each Amazon S3 account as a percentage for each five minute period in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the Amazon S3 SLA Exclusions (as defined below).
- "Monthly Uptime Percentage" is calculated by subtracting from 100% the average of the Error Rates from each five minute period in the monthly billing cycle.

- A "Service Credit" is a dollar credit, calculated as set forth below, that we may credit back to an eligible Amazon S3 account.

Service Credits

Service Credits are calculated as a percentage of the total charges paid by you for Amazon S3 for the billing cycle in which the error occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Equal to or greater than 99% but less than 99.9%	10%
less than 99%	25%

We will apply any Service Credits only against future Amazon S3 payments otherwise due from you; provided that, we may issue the Service Credit to the credit card that you used to pay for Amazon S3 for the billing cycle in which the error occurred. Service Credits shall not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability or non-performance of Amazon S3 or other failure by us to provide Amazon S3 is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA or termination of your use of Amazon S3.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a request by sending an e-mail message to aws-sla-request @ amazon.com. To be eligible, the credit request must (i) include your account number in the subject of the e-mail message (the account number can be found at the top of the AWS Account Activity page); (ii) include, in the body of the e-mail, the dates and times of each incident of non-zero Error Rates that you claim to have experienced; (iii) include your server request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks); and (iv) be received by us within ten (10) business days after the end of the billing cycle in which the errors occurred. If the Monthly Uptime Percentage applicable to the month of such request is confirmed by us and is less than 99.9%, then we will issue the Service Credit to you within one billing cycle following the month in which the error occurred. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon S3 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon S3, or any other Amazon S3 performance issues: (i) that result from Service Suspensions described in Section 7.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon S3; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (v) arising from our suspension and termination of your right to use Amazon S3 in accordance with the AWS Agreement (collectively, the "Amazon S3 SLA Exclusions"). If availability is impacted by factors other than those used in our calculation of the Error Rate, we may issue a Service Credit considering such factors in our sole discretion.

Quelle: http://aws.amazon.com/s3-sla/ (Zugriff am 01. September 2010).