Universität Zürich
Rechtswissenschaftliche Fakultät

Cloud Computing – Eine rechtliche Gewitterwolke?

Masterarbeit

bei

Prof. Dr. Andreas Kellerhals

vorgelegt von

Eric P. Neuenschwander
[redacted]

[redacted]
Studiengang: Master of Law
11. Semester
HS 14

Inhaltsverzeichnis

Literaturverzeichnis

BARRELET DENIS/EGLOFF WILLI, Kommentar zum Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, 3. Auflage, Bern 2008.

BAUMGARTNER ANDREAS C., Cloud Computing – Vertragsgestaltung als Teil des Risikomanagements, in: Daniel Lengauer/Giordano Rezzonico (Hrsg.), Chancen und Risiken rechtlicher Neuerungen 2011/2012, Zürich 2012, S. 104 ff.

BEGLINGER JACQUES/BURGWINKEL DANIEL/LEHMANN BEAT/NEUENSCHWANDER PETER/WILDHABER BRUNO, Records Management – Leitfaden zur Compliance bei der Aufbewahrung von elektronischen Dokumenten in Wirtschaft und Verwaltung mit Checklisten, Mustern und Vorlagen, 2. Auflage, Zollikon 2008.

BERANEK ZANON NICOLE/DE LA CRUZ BÖHRINGER CARMEN, Urheberrechtliche Beurteilung von IaaS- (und XaaS)-Cloud-Diensten für die betriebliche Nutzung gemäss Art. 19 URG, in: sic! – Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht 2013, S. 663 ff.

BHEND JULIA, Safe Harbor: Globaler Datenumschlagplatz?, in: digma – Zeitschrift für Datenrecht und Informationssicherheit 3/2011, S. 122 ff.

BÜHLER LUKAS, Schweizerisches und internationales Urheberrecht im Internet, Diss. Fribourg 1999.

„Contracting Cloud Services: A Guide to Best Practices“, Cloud Industry Forum – Cloud UK, Paper 3 2011, online verfügbar unter <http://cloudindustryforum.org/downloads/whitepapers/cif-white-paper-3-2011.pdf> (zuletzt besucht am 29. Oktober 2014).

DE LA CRUZ CARMEN, Cloud Computing: Alter Wein in neuen Schläuchen?, in: Jusletter IT, 15. Mai 2013.

EGLI URS, Outsourcing und IT-Governance, in: Jusletter IT 6. Juni 2012.

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER EDÖB, Erläuterungen zu Cloud Computing, Oktober 2011, online verfügbar unter <http://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=de> (zuletzt besucht am 24. September 2014).

FUCHS PHILIPPE, Cloud Computing – eine datenschutzrechtliche Betrachtung, in: Jusletter IT, 6. Juni 2012.

GAUCH PETER/SCHLUEP WALTER R./SCHMID JÖRG/EMMENEGGER SUSAN, Schweizerisches Obligationenrecht Allgemeiner Teil, 10. Auflage, Zürich 2014.

GUROVITS KOHLI ANDRÀS A., Service Level Agreements in der Outsourcing-Praxis, in: Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich (ZIK) Band/Nr. 23 2003, S. 97 ff.

HECK UWE/MÜLLER WILLY, Vorstudie zu Cloud Computing in Schweizer Behörden, Version 1.0, 21. Oktober 2010, online verfügbar unter <http://www.isb.admin.ch/themen/architektur/00183/01368/01372/index.html?lanl=de> (zuletzt besucht am 17. September 2014).

HERMANN WOLFGANG, Cloud Computing – das Buzzword des Jahres?, in: Computerwoche, 09.04.2008, online verfügbar unter http://www.computerwoche.de/knowledge_center/software_infrastruktur/1860108 (zuletzt besucht am 18. September 2014).

HILBER MARC (Hrsg.), Handbuch Cloud Computing, Köln 2014 (zitiert: BEARBEITERIN, Handbuch Cloud Computing, Teil X).

HILTY RETO M., Urheberrecht, Bern 2010.

HOFFMANN RAUNO, Cloud Computing: Die Nutzung von Cloud-Computing – Services und deren datenschutzrechtliche Voraussetzungen, in: Der Schweizer Treuhänder, Zürich, Bd. 86 (2012), Nr. 6/7, S. 465–469.

HON KUAN W./MILLARD CHRISTOPHER/WALDEN IAN, Negotiating Cloud Contracts: Looking at Clouds from both Sides now, in: Stanford Technology Law Review, Volume 16, Number 1 Fall 2012, online verfügbar unter <http://stlr.stanford.edu/pdf/cloudcontracts.pdf> (zuletzt besucht am 24. September 2014).

HONSELL HEINRICH/VOGT NEDIM PETER/WIEGAND WOLFGANG (Hrsg.), Basler Kommentar zum Schweizerischen Privatrecht, Bd. I, 5. Auflage, Basel 2011 (zitiert: BSK OR I-BEARBEITERIN).

HONSELL HEINRICH/VOGT NEDIM PETER/WIEGAND WOLFGANG (Hrsg.), Basler Kommentar zum Schweizerischen Privatrecht, Bd. II, 4. Auflage, Basel 2012 (zitiert: BSK OR II-BEARBEITERIN).

MAURER-LAMBROU URS/VOGT NEDIM PETER, Basler Kommentar zum Datenschutzgesetz, 2. Auflage, Zürich 2006 (zitiert: BSK DSG-BEARBEITERIN).

MEIR-HUBER MARIO, Cloud Computing: Praxisratgeber und Einstiegsstrategien, 2. Auflage, Frankfurt am Main 2011.

MELL PETER/GRANCE TIMOTHY, The NIST definition of Cloud Computing, Special Publication 800-145, 2011, online verfügbar unter <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> (zuletzt besucht am 23. September 2014).

METZGER CHRISTIAN/REITZ THORSTEN/VILLAR JUAN, Cloud computing: Chancen und Risiken aus technischer und unternehmerischer Sicht, München 2011.

MEYER LEONZ, Source Code-Escrow, in: HANS RUDOLF TRÜEB (Hrsg.), Softwareverträge, Zürich 2004, S. 176 ff.

MORROW SUSAN, The Challenge of Securing Data in a Cloud, in: digma – Zeitschrift für Datenrecht und Informationssicherheit, 2009 S. 16 ff.

MÜLLER WILLY, Studie „Cloud Labeling“, erstellt im Auftrag des Informatiksteuerungsorgans des Bundes ISB, Oktober 2013, online verfügbar unter < http://www.s-i.ch/fileadmin/daten/si/PDF_Dokumente/Projekt_GovCloud.CH_Studie_Labeling_final01.pdf> (zuletzt besucht am 20. November 2014).

REHBINDER MANFRED/VIGANÒ ADRIANO, Kommentar zum Urheberrechtsgesetz, 3. Auflage, Zürich 2008.

ROHRLICH MICHAEL, Cloud Computing: Rechtliche Grundlagen, Frankfurt am Main 2014.

ROSENTHAL DAVID/JÖHRI YVONNE, Handkommentar zum Datenschutzgesetz sowie weiteren ausgewählten Bestimmungen, Zürich 2008 (zitiert: BEARBEITERIN, Handkommentar DSG).

ROSENTHAL DAVID, Haftungsfragen nicht vernachlässigen, in: digma – Zeitschrift für Datenrecht und Informationssicherheit, 4/2001 S. 171 ff.

RUDIN BEAT, Über den Wolken muss die Freiheit ... Löst Cloud Computing die Fesseln des irdischen Informatikdaseins und bringt uns endlich die Freiheit?, in: digma – Zeitschrift für Datenrecht und Informationssicherheit 2009, S. 4 ff.

SCHUSTER FABIAN/REICHL WOLFGANG, Cloud Computing & SaaS: Was sind die wirklich neuen Fragen?, in: Computer und Recht – Zeitschrift für die Praxis des Rechts der Informationstechnologien, Heft 1, 15. Januar 2010, S. 38 ff.

SCHWANINGER DAVID/LATTMANN STEPHANIE S., Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, in: Jusletter, 11. März 2013.

„Public-Cloud-Markt wächst jährlich knapp 23 Prozent“, IT Reseller vom 5. November 2014, online verfügbar unter <http://www.itreseller.ch/Artikel/78721/Public-Cloud-Markt_waechst_jaehrlich_knapp_23_Prozent.html> (zuletzt besucht am 5. November 2014).

STAFFELBACH OLIVER, Cloud-Computing-Verträge, in: Computerworld 11/2012, S. 38 ff., online verfügbar unter <http://www.wengervieli.ch/Weitere-Seiten/Weitere-Publikationen.aspx?anwalt=252> (zuletzt besucht am 19. November 2014).

STAEHELIN ADRIAN/BAUER THOMAS/STAEHELIN DANIEL (Hrsg.), Basler Kommentar zum Bundesgesetz über Schuldbetreibung und Konkurs, Bd. I, 2. Auflage, Basel 2010 (zitiert: BSK SchKG I-BEARBEITERIN).

STRAUB WOLFGANG, Cloud Computing – Checkliste zum vertraglichen Regelungsbedarf, in: Jusletter 14. Juli 2014 (zitiert: STRAUB, Cloud Computing – Checkliste).

DERSELBE, Cloud Verträge – Regelungsbedarf und Vorgehensweise, in: AJP 7/2014, S. 905 ff. (zitiert: STRAUB, Cloud Verträge)

SURY URSULA, Informatikrecht, Bern 2013.

SÖBBING THOMAS, Cloud Computing, die Zukunftsvisionen von Amazon, Google und Microsoft rechtlich betrachtet, in: Jusletter 10. August 2009.

VAN HOBOKEN JORIS/ARNBAK AXEL/VAN EIJK NICO, Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act, Institute for Information Law University of Amsterdam (Hrsg.), Amsterdam 2012, online verfügbar unter <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534> (zuletzt besucht am 4. Oktober 2014).

VEHLOW MARKUS/GOLKOWSKY CORDULA, Cloud Computing – Navigation in der Wolke, PricewaterhouseCoopers AG (Hrsg.), 2011, online verfügbar unter <http://www.pwc.de/de_de/de/prozessoptimierung/assets/cloud_computing_deutsch.pdf> (zuletzt besucht am 29. Oktober 2014).

WEBER ROLF H./STAIGER DOMINIC N., Spannungsfelder von Datenschutz und Datenüberwachung in der Schweiz und in den USA, in: Jusletter IT, 15. Mai 2014.

WELLENS VINCENT, Proposal for a right to claim back data from bankrupt cloud computing providers, NautaDutilh Avocats Luxembourg, November 2012, online verfügbar unter <http://www.newsletter-nautadutilh.com/EN/xzine/information_-_communication_technology/proposal_for_a_right_to_claim_back_data_from_bankrupt_cloud_computing_providers/projet_de_loi_instaurant_un_droit_de_revindiquer_ses_données_auprès_dun_fournisseur_de_solutions_cloud_failli.html?cid=4&xzine_id=4834> (zuletzt besucht am 21. November 2014).

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
AJP	Aktuelle Juristische Praxis
Art.	Artikel
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
BG	Bundesgesetz
BGE	Amtliche Sammlung der Bundesgerichtsentscheide
BGFA	BG über die Freizügigkeit der Anwältinnen und Anwälte vom 23. Juni 2000 (SR 935.61)
BSK	Basler Kommentar
bspw.	beispielsweise
BÜPF	BG betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1)
CID	Client Identifying Data
DBG	BG über die direkte Bundessteuer vom 14. Dezember 1990 (SR 642.11)
d.h.	das heisst
Diss.	Dissertation
DSB	Datenschutzbeauftragter des Kantons Zürich
DSG	BG über den Datenschutz vom 19. Juni 1992 (SR 235.1)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
e.g.	exempli gratia (zum Beispiel)
etc.	et cetera (und so weiter)
EWR	Europäischer Wirtschaftraum
f./ff.	und folgende (Seite/Seiten)
FINMA	Eidgenössische Finanzmarktaufsicht
GeBüV	Verordnung über die Führung und Aufbewahrung der Geschäftsbücher vom 24. April 2002 (SR 221.431)
gem.	gemäss
h.L.	herrschende Lehre
Hrsg.	Herausgeber
IaaS	Infrastructure as a Service
i.S.v.	im Sinne von
IT	Informationstechnologie
i.V.m.	in Verbindung mit
lit.	litera
m.E.	meines Erachtens
m.w.H.	mit weiteren Hinweisen
MWSTG	BG über die Mehrwertsteuer vom 12. Juni 2009 (SR 641.20)
MWSTGV	Verordnung zum BG über die Mehrwertsteuer vom 29. März 2000 (SR 641.201)
N	Note, Randnote
NIST	National Institute of Standards and Technology
Nr.	Nummer
OR	BG betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (SR 220)
PaaS	Platform as a Service
Rz.	Randzeile

S.	Seite
SaaS	Software as a Service
SAV	Schweizerischer Anwaltsverband
SchKG	BG über Schuldbetreibung und Konkurs vom 11. April 1889 (SR 281.1)
SECO	Staatssekretariat für Wirtschaft
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht
SLA	Service Level Agreement
sog.	sogenannt
SR	Systematische Rechtssammlung
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0)
u.a.	unter anderem
URG	BG über das Urheberrecht und verwandte Schutzrechte vom 9. Oktober 1992 (SR 231.1)
usw.	und so weiter
v.a.	vor allem
VDSG	Verordnung zum BG über den Datenschutz vom 14. Juni 1993 (SR 235.11)
vgl.	vergleiche
ZAV	Zürcher Anwaltsverband
z.B.	zum Beispiel

Materialienverzeichnis

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 27. Februar 2013, BBl 2013 2683 ff.

Botschaft zur Änderung des Obligationenrechts (Aktienrecht und Rechnungslegungsrecht sowie Anpassungen im Recht der Kollektiv- und der Kommanditgesellschaft, im GmbH-Recht, Genossenschafts-, Handelsregister- sowie Firmenrecht) vom 21. Dezember 2007, BBl 2008 1589 ff.

Botschaft zum Bundesbeschluss über die Genehmigung von zwei Abkommen der Weltorganisation für geistiges Eigentum und zur Änderung des Urheberrechtsgesetzes vom 10. März 2006, BBl 2006 3389 ff.

A. Einleitung

1 Der Technologie des „Cloud Computing“ wird heute viel zugetraut und wohl die meisten Nutzer von IT haben bereits mit einer der vielfältigen Einsatzformen der Cloud zu tun gehabt (sei es als Nutzer von E-Mail-Diensten wie Gmail oder beim Speichern von Fotos in einem Onlinespeicher wie Dropbox). Die Einsatzmöglichkeiten von Cloud-Lösungen sind sehr vielfältig und reichen von einfachen Lösungen für Privatkunden über standardisierte Massenangebote bis hin zu individuellen Grosstransaktionen. Betrachtet man die prognostizierten Marktchancen von Cloud Computing, stellt man fest, dass Cloud Computing den Technologiemarkt in den kommenden Jahren wohl erobern und nachhaltig verändern wird. Man könnte leicht dazu verleitet werden, zu glauben, den vielen Chancen und Vorteilen stünden keine Risiken gegenüber. Dem ist jedoch nicht so und eine vertiefte Prüfung ist empfehlenswert. Dabei stellt man fest, dass sich beim Umgang mit Cloud Computing diverse Probleme ergeben, und diese sollen in der vorliegenden Masterarbeit aufgezeigt werden.

2 Diese Arbeit soll dem interessierten Leser einen Einstieg in die Thematik des Cloud Computing bieten und die elementaren Grundlagen vermitteln. Sie soll aber auch ein Problembewusstsein schaffen und die mannigfaltigen rechtlichen Aspekte der Nutzung einer Cloud beleuchten. Ziel meiner Masterarbeit ist, dass der Leser nach der Lektüre die Risiken, welche den Chancen des Cloud Computing gegenüberstehen, erkennt und besser abwägen kann. Natürlich kann dem Leser die Beantwortung der Frage, ob eine Cloud-Lösung für ihn oder für sein Unternehmen lohnenswert ist, nicht abgenommen werden. Im Idealfall sollte die Arbeit es jedoch ermöglichen, die rechtlichen Fallstricke im Zusammenhang mit der Nutzung einer Cloud zu erkennen und so zu vermeiden, dass am IT-Himmel rechtliche Gewitterwolken aufziehen.

3 Mein Dank geht an Herrn Prof. Dr. Andreas Kellerhals, für sein Interesse, welches er dieser Problematik entgegengebracht hat, und seine Bereitschaft, meine Arbeit zu betreuen. Besonderer Dank gilt meinem Vater, Dr. Peter Neuenschwander, welcher mich stets mit seinem Fachwissen hinterfragt und in meiner Arbeit ermuntert hat.

B. Begrifflichkeiten

4 In einem ersten Teil sollen zuerst die wesentlichen Begrifflichkeiten erläutert werden. Zudem werden die verschiedenen Aspekte und Erscheinungsformen von Cloud Computing aufgezeigt und erläutert.

I. Der Begriff des Cloud Computing

5 Der Begriff des Cloud Computing ist in der IT-Welt derzeit in aller Munde. Dennoch sucht man vergeblich eine einheitliche Definition dieses Begriffs. Denn die verschiedenen Software-, Service- oder Infrastrukturanbieter betonen je nach Interessenlage unterschiedliche Aspekte des Begriffs.[1]

6 Gartner[2] beschreibt Cloud Computing kurz als „Bereitstellen skalierbarer IT-Services über das Internet für eine potentiell grosse Zahl externer Kunden". Im Bestreben, eine Definition zu erarbeiten, befragte das US-Unternehmen Forrester Research diverse Unternehmen, die sich in diesem neuen Marktumfeld bewegen, und kam zum Schluss, dass Cloud Computing für einen „Pool aus abstrahierter, hoch skalierbarer und verwalteter IT-Infrastruktur, welche Kundenanwendung vorhält und nach Verbrauch abgerechnet wird", steht.[3]

7 Das US-amerikanische National Institute of Standards and Technology (NIST) wiederum definiert Cloud Computing in seiner Spezialpublikation mit dem Titel „The NIST Definition of Cloud Computing" folgendermassen: „*Cloud computing is a model for enabling ubiquitous, 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*."[4]

8 Obwohl es also keine einheitliche Definition des Cloud Computing gibt, weisen die diversen Begriffsdefinitionen doch gewisse Gemeinsamkeiten auf und ermöglichen den ansatzweisen Versuch einer standardisierten Definition. Cloud Computing kann demnach als die Bereitstellung und Nutzung von IT-Infrastruktur, von Plattformen und von Anwendungen aller Art als im Internet elektronisch verfügbare Dienste bezeichnet werden. Die genutzten Ressourcen sind also nicht mehr physisch beim Kunden vorhanden, vielmehr bezieht dieser die benötigten Anwendun-

1 Vgl. HERMANN, S. 1.
2 Gartner Inc., www.gartner.com
3 Siehe dazu HECK/MÜLLER, S. 6.
4 MELL/GRANCE, S. 1 ff.

gen, Rechen- und Speicherkapazitäten aus einem Pool von Angeboten – metaphorisch als „Cloud“ oder eben „Wolke“ bezeichnet – bedarfsorientiert über das Internet. Der Begriff der Wolke soll dabei diese Ansammlung von Ressourcen versinnbildlichen, die sich – frei wie eine Wolke – überall befinden können.[5] Der Begriff der Wolke beinhaltet m.E. aber auch eine Komponente der Flüchtigkeit und Unbestimmtheit.

II. Ausprägungen

9 Cloud Computing weist eine mehrdimensionale Ausprägung auf und wird einerseits hinsichtlich des Serviceangebots und andererseits in Bezug auf die verschiedenen Organisationsformen differenziert. Im Folgenden soll die allgemein gebräuchliche Unterteilung kurz aufgezeigt und erläutert werden.

1. Organisationsformen

10 Cloud-Computing-Lösungen können in verschiedenen Formen organisiert werden, man spricht dabei von sog. Deployment-Modellen. Das wesentliche Unterscheidungsmerkmal zwischen den einzelnen Modellen ist die Offenheit bzw. Zugriffsbeschränkung hinsichtlich der enthaltenen Daten. Entscheidend ist also, wer Zugriff auf die Services hat.[6] Allgemein differenziert man zwischen den folgenden Betriebsmodellen.[7]

a) Private Cloud

11 Eine Private Cloud zeichnet sich dadurch aus, dass einem Kunden dedizierte Services bereitgestellt werden, unter Verwendung von abgrenzbaren Hardware-Ressourcen (physische oder virtuelle Server) und Netzwerkbereichen, die nicht von Dritten genutzt werden.[8] Die Nutzung einer Private Cloud ist auf einen bestimmten Personenkreis (z.B. nur Mitarbeiter einer bestimmten Unternehmenseinheit) beschränkt, was die Möglichkeiten bezüglich Datensicherheit und Kontrolle wesentlich vergrössert.[9] Die Private Cloud ist somit mit dem altbekannten Modell eines „eigenen“, durch einen Dritten betriebenen Netzwerks vergleichbar.

---

5 HOFFMANN, S. 465.
6 WEISS, Handbuch Cloud Computing, Teil 1 A, Rz. 14 ff.
7 Gem. Institute of Standards and Technology (NIST), siehe dazu: MELL/ GRANCE, S. 2.
8 WEISS, Handbuch Cloud Computing, Teil 1 A, Rz. 14.
9 Es ist jedoch auch möglich, den Zugriff auf die Private Cloud mittels spezieller Schnittstellen auf Aussenstehende zu erweitern, was bspw. im Umgang mit Kunden oder Lieferanten sinnvoll sein kann; m.w.H. ZANON BERANEK/DE LA CRUZ BÖHRINGER, S. 668.

b) Public Cloud

12 Wie es der Name bereits sagt, steht die Public Cloud einer unbegrenzten Anzahl von potentiellen Nutzern offen. Es handelt sich somit nicht um einen dedizierten Server, sondern die Hardware-Ressourcen werden gemeinschaftlich genutzt.[10] Dabei wissen die Kunden aber nicht, welche anderen Aufgaben und Dienste auf derselben Infrastruktur, d.h. auf dem gleichen physischen Server, bearbeitet werden. Anders als bei einer Private Cloud haben die Nutzer einer Public Cloud typischerweise weder Einfluss auf den Standort des Datenspeichers noch auf die Sicherungskomponenten, welche der Cloud-Anbieter zur Sicherung der Daten einsetzt.[11]

c) Community Cloud

13 Eine Community Cloud stellt eine Kombination mehrerer Cloud-Services dar. Der Zugang zur Cloud ist nicht öffentlich und wird durch den Betreiber der Cloud geregelt. Eine Community Cloud eignet sich für bestimmte Anwendergruppen, welche meist ähnliche Anforderungen an Verfügbarkeit, Compliance, Betriebsprozesse und Sicherheit der bereitgestellten Ressourcen stellen. Dies kann z.B. bei Branchenvereinigungen oder Regierungsstellen der Fall sein.[12]

d) Hybrid Cloud

14 Die Hybrid Cloud stellt eine Mischform zwischen Private Cloud und Public Cloud dar und ist der Versuch, die Vorteile beider Modelle zu vereinen und die Nachteile zu substituieren.[13] Hybride Clouds sind komplexer Natur und lassen sich am besten anhand eines Beispiels erläutern. Ein Unternehmen betreibt bspw. eine Private Cloud, also ein dediziertes Netzwerk, als Basis für die unternehmenseigene Infrastruktur. Zusätzlich kann das Unternehmen bei Belastungsspitzen oder Kapazitätsengpässen einen Public-Cloud-Dienst in Anspruch nehmen. In diesem Fall liegt dann eine sog. hybride Cloud vor.[14]

---

10 Dennoch findet mittels einer Mandantenzuordnung eine Separierung der Cloud-Leistungen statt, siehe dazu unten Rz. 30 (Multi-Tenancy-Architektur).
11 ZANON BERANEK/DE LA CRUZ BÖHRINGER, S. 668.
12 WEISS, Teil 1A, Rz. 17.
13 MEIR-HUBER, S. 41.
14 METZGER/REITZ/VILLAR, S. 20.

2. Servicemodelle

15 Wie bereits erwähnt, gibt es verschiedene Ebenen des Cloud Computing. Die einzelnen Ebenen bauen aufeinander auf, wobei das Zur-Verfügung-Stellen von Hardware (Server usw.) die unterste Ebene darstellt. Auf der darüber liegenden Ebene stellt der Cloud-Anbieter bereits eine gänzlich verwaltete Umgebung zur Verfügung (der Anwender muss sich dabei nur noch um seine Applikationen kümmern) und auf der höchsten Ebene gibt es vollständige Anwendungen, die der Endanwender direkt verwenden kann.[15] Die einzelnen Serviceebenen werden im Folgenden etwas genauer betrachtet.

a) Infrastructure as a Service (IaaS)

16 Infrastructure as a Service bildet die unterste Stufe der verschiedenen Cloud-Servicemodelle und beinhaltet Angebote wie grosse Mengen an Speicherplatz, hohe Rechenleistung oder Backup im Netz. Im Wesentlichen handelt es sich also um eine Infrastruktur, welche der Cloud-Anbieter über virtuelle und physische Server nutzbar macht. Dem Cloud-Nutzer steht es sodann frei, eine eigene Software auf diese Infrastruktur aufzusetzen.[16]

17 Für den Cloud-Nutzer entfallen somit hohe Investitionskosten für die physische Hardware, und auch die Verantwortung für den Betrieb hat nicht er zu tragen. Diese liegt allein beim Cloud-Anbieter, welcher auch die Kosten des sog. „Housing" (Kosten für Kühlung, unterbruchsfreie Stromversorgung, physische Sicherheit und weitere Aufwendungen) zu tragen hat.[17] Hingegen trägt der Konsument einer IaaS-Lösung die Kosten für die zusätzlich installierte Software, und auch die Verwaltung der Plattform obliegt ihm.[18] Die IaaS-Plattform ist der Cloud-Computing-Dienst mit dem geringsten Abstraktionsgrad, dafür aber mit der grössten Flexibilität.[19]

b) Platform as a Service (PaaS)

18 Während es auf der Ebene des IaaS v.a. um Hardware geht, geht es auf der zweiten Ebene, Platform as a Service, zusätzlich um Middleware. PaaS ist hauptsächlich für die Entwickler von Systemen und Anwendungen gedacht. Der Anbieter

---

15 Siehe zu den einzelnen Ebenen MEIR-HUBER, S. 42; METZGER/REITZ/VILLARS, S. 34.
16 MEIR-HUBER, S. 42.
17 ZANON BERANEK/DE LA CRUZ BÖHRINGER, S. 667.
18 Hinsichtlich der Lizenzierungskosten für die verwendete Software bestehen hier einige Parallelen zum klassischen On-Premise Hosting, da der IaaS-Nutzer ebenfalls die Kosten für die zusätzlich installierte Software trägt. Siehe dazu m.w.H. MEIR-HUBER, S. 44.
19 MEIR-HUBER, S. 44.

stellt eine Plattform zur Verfügung, welche der Konsument dazu nutzen kann, eigene Anwendungen zu entwickeln, ohne dass er gezwungen ist, hohe Investitionen in Hardware oder Entwicklungssoftware zu tätigen.[20] Kunden von PaaS können also eine geeignete Entwicklungsplattform nutzen und müssen sich nicht um Hardware- oder Softwareabhängigkeiten kümmern.[21]

19 Obwohl die Entwicklungsumgebung nicht dem Kunden gehört, behält er dennoch die Kontrolle über die selbstentwickelte Software. Dank der vorkonfigurierten Plattform kann er sich somit auf die Entwicklung seiner Software konzentrieren und er benötigt kein Know-how, um die Plattform zu betreiben. Typische PaaS-Dienstleistungen sind bspw. die Google App Engine von Google, die Windows-Azure-Plattform von Microsoft oder die Plattform Force.com von Salesforce.com.[22]

c) Software as a Service (SaaS)

20 Software as a Service ist die letzte und womöglich abstrakteste Form des Cloud Computing. Bei SaaS bezieht der Kunde eine bereits komplett entwickelte, funktionsfähige und auf dem neusten Stand befindliche Software über das Internet. Sofern also ein Internetzugang vorhanden ist, kann die Anwendung von jedem Ort aus verwendet werden. Für den Kunden bietet diese Lösung den Vorteil, dass einerseits anders als bei klassischen Anwendungen kein Problem mit der Verteilung besteht und er andererseits jederzeit über die aktuellste Version der Software verfügt. Denn im Gegensatz zu lokal installierter Software werden SaaS-Anwendungen direkt vom Provider am Webserver aktualisiert.

21 Trotz aller Vorteile verstärkt eine solche Lösung natürlich die Abhängigkeit vom Internet. Zudem bietet die fertige SaaS-Plattform für den Kunden meist keine Möglichkeit, Anpassungen vorzunehmen. Dennoch stellen gem. METZGER/REITZ/VILLAR SaaS-Anwendungen den grössten Bereich der Cloud-Lösungsangebote im B2B-Bereich dar.[23] Bekannte SaaS-Dienstleistungen sind bspw. Windows Life Services oder Windows 365 von Microsoft, iWork.com von Apple oder das Customer Relationship Management (CRM) von Salesforce.com.[24]

---

20 ROHRLICH, S. 15.
21 MEIR-HUBER, S. 44.
22 ZANON BERANEK/DE LA CRUZ BÖHRINGER, S. 667.
23 „B2B“ steht für „business to business“ und bezeichnet eine Geschäftsbeziehung zwischen min. zwei Unternehmen; siehe METZGER/REITZ/VILLAR, S. 36.
24 Siehe dazu MEIR-HUBER, S. 46; ZANON BERANEK/DE LA CRUZ BÖHRINGER, S. 667.

III. Vertragsgestaltung

22 Die Ausgestaltung der vertraglichen Regelungen ist sehr vielfältig und reicht von Allgemeinen Geschäftsbedingungen bei Providern von Standard-Cloud-Lösungen oder Gratisservices bis hin zu komplexen, massgeschneiderten Vertragswerken bei Grossprojekten. Da Cloud-Computing-Dienstleistungen sehr unterschiedlich sein können, ist eine abstrakte Qualifikation von Cloud-Verträgen weder möglich noch sinnvoll. Je nach Dienstleistung handelt es sich um einen Innominatvertrag mit u.a. mietvertraglichen, auftragsrechtlichen oder auch werkvertragsähnlichen Komponenten. Der einzelne Vertrag ist somit in concreto zu qualifizieren.[25] Bei Rechtsfragen, welche sich durch die Auslagerung von IT-Ressourcen an einen externen Dienstleister ergeben können, kann man auch auf die durch die Lehre entwickelten Grundsätze zum IT-Outsourcing zurückgreifen. Beim Cloud Computing sind in etwa die gleichen Fragestellungen (z.B. Service Levels, Sicherheitsaspekte, Haftungsfragen) zu regeln wie bei klassischen Outsourcing-Verträgen.[26]

23 In einem ersten Schritt sollte man zwischen Grossprojekten und kleineren Cloud-Projekten unterscheiden. Als Faustregel gilt: Je höher die Serviceebene (IaaS, PaaS, SaaS) und die Exklusivität (Public, Community oder Private Cloud), desto individueller ist die vertragliche Regelung.[27] Laut einer Studie des Cloud Industry Forum aus dem Jahre 2011 wurde rund die Hälfte der Cloud-Service-Verträge von Unternehmenskunden individuell verhandelt.[28]

1. Standard-Cloud-Services

24 Ausgangspunkt für kleinere Cloud-Services sind oft die Allgemeinen Geschäftsbedingungen der Cloud-Anbieter. Diese sind naturgemäss zu deren Vorteil ausgestaltet und eignen sich für voll standardisierte Cloud-Leistungen. Bei solchen Leistungen sind die Verhandlungsspielräume für den Kunden, wenn sie denn überhaupt existieren, gering. Ob solche „click-through"-Verträge der Cloud-Anbieter verhandelt werden können, hängt natürlich von der Verhandlungsmacht ab. Grosse Anbieter verweigern häufig jegliche Änderungen ihrer AGB und bieten ihre Services auf einer „take it or leave it"-Basis an. Wie die Untersuchung von HON/MILLARD/WALDEN zeigte, versuchen v.a. grosse, nachfragemächtige Kunden

---

25 Siehe auch DE LA CRUZ, Rz. 15.
26 STRAUB, Cloud Verträge, S. 906. Zur Abgrenzung Cloud Computing – IT-Outsourcing siehe unten Rz. 28 ff.
27 STRAUB, Cloud Verträge, S. 906.
28 Siehe dazu auch HON/MILLARD/WALDEN, S. 84 ff.

wie Behörden oder Banken zu verhandeln oder bestehen sogar darauf, dass ihre eigenen AGB dem Vertragsverhältnis zugrunde gelegt werden.[29] Doch selbst bei diesen Kunden, die teils grosse Volumen zu vergeben haben, sind den Anbietern standardisierter Cloud-Dienstleistungen von ihrem Geschäftsmodell her Grenzen gesetzt.[30]

25 Für die Cloud-Anbieter ist die Verwendung ihrer eigenen AGB natürlich ökonomisch sinnvoll, da Verhandlungskosten wegfallen. Gem. HON/MILLARD/WALDEN monierten einige Cloud-Nutzer, dass sogar grosse Cloud-Anbieter nicht genügend Kapazitäten in der internen Rechtsabteilung hätten, um die Cloud-Verträge mit den Kunden individuell auszuhandeln, was die Weigerung, Verträge zu verhandeln, natürlich auch erklären kann.[31] Dies führt wohl zum oben erwähnten Untersuchungsergebnis, wonach nur rund die Hälfte aller Cloud-Service-Verträge individuell verhandelt wurde.

2. Premium-Cloud-Services

26 Natürlich gibt es auch Cloud-Anbieter, welche ihren Kunden Lösungen anbieten, die auf ihre individuellen Bedürfnisse zugeschnitten sind. Diese Anbieter verfolgen ein Geschäftsmodell, welches es ihnen erlaubt, auf die Kundenwünsche sowohl bei der Leistungserbringung als auch bei der Vertragsgestaltung einzugehen. Solche Cloud-Lösungen sind aber dementsprechend für den Kunden mit wesentlich höheren Kosten verbunden als Standardleistungen.[32]

27 In der Praxis bedient man sich in diesem Fall häufig eines Vertragsmodells, bei dem zwischen den Parteien ein Rahmenvertrag als Basis dient, welcher die grundlegenden Rechte und Pflichten der Parteien festhält. Sodann wird als gesonderter Teil des Vertrags ein sog. Service Level Agreement (SLA) abgeschlossen, welches die Leistungskriterien konkretisiert.[33] Ein SLA kann als eine Vereinbarung definiert werden, mit welcher die Vertragsparteien messbare Leistungskriterien für die in einem zwischen diesen Parteien abgeschlossenen Dienstleistungsvertrag vorgesehenen Leistungen festlegen und die Folgen der Nichteinhaltung dieser Leistungskriterien regeln.[34] Die wesentlichen Punkte, die einem SLA geregelt wer-

---

29 HON/MILLARD/WALDEN, S. 89.
30 INTVEEN/HILBER/RABUS, Handbuch Cloud Computing, Teil 2, Rz. 7.
31 HON/MILLARD/WALDEN, S. 89.
32 INTVEEN/HILBER/RABUS, Handbuch Cloud Computing, Teil 2, Rz. 8.
33 GUROVITS KOHLI, S. 99.
34 GUROVITS KOHLI, S. 100.

den sollten, sind insbesondere die Spezifikation der Leistungskriterien, das Messverfahren und die Folgen der Nichteinhaltung der Leistungskriterien.[35]

IV. Abgrenzung zu IT-Outsourcing

28 Der Begriff des Outsourcings (zu deutsch „Auslagerung“) ist bereits seit Jahrzehnten etabliert. Im Kern geht es dabei um die Frage, ob IT-Ressourcen selber vorgehalten und betrieben werden sollen oder ob es sich lohnt, die benötigten Ressourcen von aussen zuzukaufen.[36] Die Idee, Software und Speicherkapazitäten von einem externen Server zu beziehen, ist also keinesfalls neu.[37]

29 Es wird sogar gesagt, „Cloud Computing“ sei bloss ein Modewort, welches von Marketingfachleuten verwendet werde, um eine bereits bestehende Technologie neu anzupreisen.[38] So meinte bspw. Larry Ellison an einer Analystenkonferenz im September 2008: „*The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. The computer industry is the only industry that is more fashion-driven than women's fashion.*“[39]

1. Multi-Tenancy-Architektur

30 Doch Cloud Computing unterscheidet sich in wesentlichen Punkten vom klassischen Outsourcing. Vor dem Zeitalter des Cloud Computing hielten Unternehmen ihre Daten entweder auf einem eigenen, im internen Netzwerk eingebundenen Server oder auf einem Server eines Outsourcing-Partners. Der Partner und sein(e) Standort(e) waren bekannt sowie auch die für die Anbindung gewählte, meist dedizierte Telekommunikationsinfrastruktur.[40] Auch bei einer Cloud-Computing-Lösung werden Daten, Anwendungen und Rechenvorgänge an einen Cloud-Anbieter ausgelagert. Anders als beim ursprünglichen Outsourcing wird die physische Infrastruktur des Cloud-Anbieters jedoch nicht nur von einem Kunden genutzt, sondern mehrere Kunden teilen sich diese.[41] Es erfolgt ein Ressourcen-Pooling und mehrere Kunden werden nebeneinander mittels derselben physi-

---

35 INTVEEN/HILBER/RABUS, Handbuch Cloud Computing, Teil 2, Rz. 200 ff.

36 Eine Fragestellung, die sich in der betriebswirtschaftlichen Forschung unter dem Stichwort „make or buy“ etabliert hat.

37 Eine gute Übersicht zur Abgrenzung Cloud Computing – Outsourcing bietet das Werk von SCHUSTER/REICHL, S. 38 ff.

38 MORROW, S. 16.

39 <http://www.businessinsider.com/best-larry-ellison-quotes-2013-4?op=1#ixzz3Der34Ybp> (zuletzt besucht am 18. September 2014).

40 ZANON BERANEK/DE LA CRUZ BÖHRINGER, S. 665.

41 Ausser bei der reinen Private Cloud.

schen oder virtuellen Infrastruktur (d.h. Hard- oder Software) bedient.[42] Cloud-Anbieter verwenden dazu eine sog. Multi-Tenancy-Architektur (Mehrmandantenfähigkeit). Dabei handelt es sich um eine Software, bei welcher nicht für jeden einzelnen Kunden eine dedizierte Infrastruktur zur Verfügung gestellt wird, sondern alle Nutzer auf der gleichen Plattform arbeiten.[43] Dennoch erfolgt eine virtuelle Trennung der Daten mittels sog. Partitions und jede Client-Gruppe arbeitet mit einer kundenspezifischen virtuellen Anwendungsinstanz.[44]

2. Pay Per Usage

31 Eine weitere Besonderheit des Cloud Computing ist die Art der Bezahlung. Dadurch, dass der Kunde den Dienst des Cloud-Anbieters als „Service aus dem Netz“ nutzt, entfallen hohe Anschaffungskosten für die benötigte IT-Infrastruktur sowie die Kosten für teure Lizenzen, Betrieb, Wartung und Pflege der Plattformen. Der Kunde bezieht den Service vom Cloud-Anbieter und muss lediglich für die Nutzung zahlen, welche nach dem tatsächlichen Gebrauch verrechnet wird.[45] Aus Investitionen werden somit variable Kosten und der Kunde spart dadurch nicht nur Geld, er gewinnt auch grössere Flexibilität. Er kann seinen Verbrauch an die aktuellen Erfordernisse anpassen und diesen beliebig nach unten oder oben skalieren.[46]

V. Weshalb Cloud Computing?

32 „Über den Wolken muss die Freiheit wohl grenzenlos sein“, heisst es in einem bekannten Lied von Reinhard Mey.[47] Doch lohnt es sich für ein Unternehmen tatsächlich, Cloud-Computing-Dienstleistungen in Anspruch zu nehmen? Was sind die Vorteile gegenüber herkömmlichen IT-Lösungen? Und ist Cloud Computing tatsächlich das Betriebssystem der Zukunft oder nur ein vorübergehendes Phänomen?[48] Im vorliegenden Kapitel sollen die Marktchancen des Cloud Computing,

---

42 ZANON BERANEK/DE LA CRUZ BÖHRINGER, S. 665.

43 Im Gegensatz zum klassischen Outsourcing, wo die gemietete Infrastruktur klassischerweise exklusiv von einem Kunden genutzt wird (sog. Single-Tenant-Architektur), siehe dazu: <https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html>, <http://www.itwissen.info/definition/lexikon/Multi-Tenancy-Architektur-multitenancy-architecture.html> (beide zuletzt besucht am 18. September 2014).

44 Siehe dazu <http://www.itwissen.info/definition/lexikon/Multi-Tenancy-Architektur-multitenancy-architecture.html> (zuletzt besucht am 18. September 2014).

45 Auch bekannt als „pay as you go“, siehe dazu HOFFMANN, S. 466; MEIR-HUBER, S. 51 ff.

46 Siehe dazu HECK/MÜLLER, S. 6,

47 Vgl. RUDIN, S.4.

48 So sagte bspw. auch der CEO von Microsoft, Steve Ballmer, dass Cloud Computing ein IT Thema der Zukunft sei; siehe dazu: SÖBBING, S. 1 ff.

die möglichen Einsatzgebiete und die Vorteile, welche das Cloud Computing bietet, analysiert werden.

1. Marktchancen

33 Experten prophezeien dem Cloud Computing eine blühende Zukunft. So soll der Schweizer Markt für Public Cloud Computing gem. einer Studie der Experton Group bis ins Jahr 2018 jährlich um 33 Prozent wachsen und schliesslich ein Volumen von 1.2 Milliarden Franken erreichen. Der restliche Schweizer IT-Markt soll dagegen nur gerade um 4 Prozent pro Jahr wachsen.[49]

34 Weltweit sollen gem. neusten Zahlen des Marktforschungsunternehmens International Data Corporation (IDC) die Ausgaben für Public-Cloud-IT-Services für das laufende Jahr rund 56.6 Milliarden Dollar erreichen.[50] Bis ins Jahr 2018 soll der globale Markt für Cloud Computing jährlich um 23 Prozent wachsen und er wird sodann rund 127 Milliarden US Dollar umfassen. Diese Wachstumsrate ist sechsmal höher als die Wachstumsrate des gesamten übrigen IT-Marktes.[51]

35 Verglichen mit den Wachstumsprognosen für den übrigen IT-Markt wird der Cloud-Computing-Markt in den kommenden Jahren also gewaltig zulegen und so noch zunehmend an Bedeutung gewinnen.

2. Einsatzgebiet

36 Unternehmen, die Cloud-Services in Anspruch nehmen wollen, müssen sich über die Anwendungsbereiche im Klaren sein, in welchen Cloud Computing gegenüber traditionellen IT-Plattformen Vorteile bietet. Es gibt drei wesentliche Einsatzgebiete, in welchen eine Cloud-Lösung sinnvoll ist. Diese sollen nachfolgend kurz umrissen werden.

a) Variable Auslastung mit Belastungsspitzen

37 Die Auslastung von Plattformen kann stark variieren und Belastungsspitzen kommen regelmässig dann zustande, wenn eine Plattform nur während einer gewissen Zeit genutzt wird. Herkömmliche Plattformen stossen bei hohen Anforderun-

---

49 Experton Group, Cloud Vendor Benchmark 2014, <http://www.experton-group.de/research/studien/cloud-vendor-benchmark-2014/projekt.html>, (zuletzt besucht am 25. September 2014); m.w.H. IT Reseller.

50 Vgl. Pressemitteilung IDC vom 3. November 2014, online verfügbar unter <http://www.idc.com/getdoc.jsp?containerId=prUS25219014> (zuletzt besucht am 5. November 2014).

51 IT Reseller vom 5. November 2014.

gen möglicherweise an ihre Kapazitätsgrenzen und sind bspw. in der Nacht hingegen wenig bis gar nicht ausgelastet.[52] Bei einem solchen Szenario bietet eine Cloud-Plattform für den Kunden Vorteile, da er während der Nacht die bezogene Leistung an den Bedarf anpassen und somit Kosten sparen kann.[53]

b) Zeitlich begrenzte Plattform

38 Wird eine Plattform oder eine Anwendung erstellt, welche nur vorübergehend nutzbar sein soll, so bietet Cloud Computing wesentliche Vorteile gegenüber einer klassischen Vor-Ort-Lösung („On-premise“). Früher musste man auch für eine Plattform, die nur für eine begrenzte Zeit verfügbar sein sollte, die benötigte Hardware kaufen und für die Inbetriebnahme fielen zusätzlich noch Servicekosten an. Mit einer Cloud-Computing-Lösung fallen diese Kosten weg und die Ausgaben werden auf ein Minimum reduziert.[54]

c) Kontinuierliches Wachstum

39 Ein weiteres Einsatzgebiet, in welchem sich Cloud Computing lohnen kann, ist eine ständig wachsende Plattform oder Anwendung. Dank Cloud Computing muss nicht mehr laufend neue Hardware gekauft werden, wenn der Bedarf steigt. Dank der Skalierbarkeit von Cloud-Computing-Lösungen kann der Cloud-Service mit dem Unternehmen mitwachsen, was gerade für Start-ups besonders interessant sein kann.[55]

3. Vorteile

40 Nach diesem ersten Überblick sollen die Vorteile, die Cloud Computing bietet, nochmals zusammenfassend aufgeführt werden.

a) Kostenreduktion

41 Durch die Nutzung von Cloud-Services fallen für den Cloud-Nutzer hohe Investitionskosten für Hard- und Software weg. Er muss die kostenintensive IT-Infrastruktur nicht mehr selber betreiben und auch die Aufwendungen für Lizenzen, Wartung und Pflege fallen weg.[56] Die Abrechnung der Cloud-Services erfolgt

---

52 Bspw. die Plattform einer Behörde, welche Onlineformulare zur Verfügung stellt. Diese werden wohl primär während des Tages verwendet und in der Nacht ist die Auslastung sodann nur gering.

53 MEIR-HUBER, S. 63.

54 MEIR-HUBER, S. 65.

55 MEIR-HUBER, S. 66.

56 HOFFMANN, S. 466.

mittels einer nutzungsabhängigen Gebühr und der Kunde bezahlt nur das, was er auch tatsächlich konsumiert hat (sog. „pay as you go"-Vergütungsmodell).[57] Dadurch verschieben sich die Kosten im IT-Bereich von Fixkosten zu variablen Kosten und das Unternehmen kann die finanziellen Mittel effizienter einsetzen und somit Kosten sparen.[58]

42 Der Cloud-Anbieter wiederum nutzt durch die Multi-Tenancy-Architektur die „Economies of Scale"[59] und kann somit viel effizienter arbeiten und die Services dementsprechend kostengünstiger anbieten. Auch die Kosten für die Sicherheit und den Betrieb der IT-Architektur kann der Anbieter auf die verschiedenen Parteien aufteilen.[60] Gegenüber herkömmlichen Lösungen hat Cloud Computing durchaus das Potential, die Kosten sowohl für den Nutzer als auch für den Anbieter zu senken, und dies ist sicher ein wichtiger Faktor für den Erfolg des Cloud Computing.

b) Effizienzsteigerung

43 Herkömmliche On-Premise-, d.h. firmeninterne IT-Lösungen können nur selten so genutzt werden, dass sie dem tatsächlichen Bedarf im Unternehmen entsprechen. Eine effiziente Auslastung ist sehr schwierig, da bspw. schwer abschätzbar ist, wie viele Lizenzen für die Mitarbeiter nun bezogen werden müssen oder wie lange es geht, bis die notwendigen Programme gekauft und installiert sind. Dank der Skalierbarkeit der Cloud-Services wird eine effiziente Nutzung der Ressourcen möglich, der Kunde verfügt über eine sehr hohe Rechenleistung und er kann dank Cloud Computing auch ortsunabhängig agieren.[61]

44 Für kleine und mittelgrosse Unternehmen werden durch Cloud Computing hervorragende und professionelle IT-Lösungen erschwinglich, welche ihnen bislang aufgrund zu hoher Kosten verwehrt blieben.[62]

c) Datensicherheit

45 Dadurch, dass dank Cloud Computing auch kleinere und mittlere Unternehmen in den Genuss von hochprofessionellen IT-Lösungen kommen, erhöht sich für diese

---

57 Siehe dazu STRAUB, Cloud Verträge, S. 907; METZGER/REITZ/VILLAR, S. 65; MEIR-HUBER, S. 61.
58 METZGER/REITZ/VILLAR, S. 65.
59 Zu deutsch „Skaleneffekt"; beschreibt in der Produktionstheorie der Betriebswirtschaftslehre die Abhängigkeit der Produktionsmenge von der Menge der eingesetzten Produktionsfaktoren, <http://de.wikipedia.org/wiki/Skaleneffekt> (zuletzt besucht am 25. September 2014).
60 METZGER/REITZ/VILLAR, S. 62.
61 HOFFMANN, S. 466.
62 METZGER/REITZ/VILLAR, S. 64.

Kunden grundsätzlich auch die Sicherheit ihrer Daten. Ein Cloud-Anbieter kann dank besseren Sicherheitsprogrammen eine viel bessere Datensicherheit bieten als Unternehmen, die bislang keinen starken IT-Bezug aufweisen. Auch bzgl. Back-Up-Technologien ist ein Cloud-Anbieter diesen Nutzern überlegen und sie erhalten durch die Nutzung eines Cloud-Services eine wesentlich sicherere Back-Up-Lösung.[63]

VI. Übersicht über die rechtlichen Probleme

46 Cloud Computing wird als das Betriebsmodell der Zukunft bezeichnet.[64] Doch zukünftige Nutzer von Cloud-Services dürfen sich nicht einfach von den erhofften Effizienzgewinnen blenden lassen, sondern sind gut beraten, die Risiken, welche Cloud Computing mit sich bringt, genau zu analysieren und abzuwägen. Im nun folgenden Teil dieser Arbeit sollen die wesentlichen Risiken erläutert werden, welche bei Cloud-Services auftauchen können und welche den bereits aufgezeigten Vorteilen gegenüber stehen.

47 Dabei sollen Themen beleuchtet werden, über deren Tragweite sich potentielle Cloud-Nutzer im Klaren sein sollten. So etwa das Thema des Datenschutzes und unter welchen Umständen Personendaten ins Ausland übermittelt werden dürfen, wenn beispielsweise ein Cloud-Anbieter seine Server im Ausland stationiert hat. Ausserdem soll die Frage geklärt werden, was mit Daten im Falle des Konkurses eines Cloud-Anbieters passiert. Auch Fragen der Haftung und des Urheberrechts sollen beleuchtet werden, ebenso die Frage nach der Erfüllung von gesetzlichen Aufbewahrungsvorschriften bei Cloud-Lösungen und dem Schicksal der Daten im Falle einer Vertragsbeendigung.

48 Ein abschliessendes Fazit soll dem Leser die Beantwortung der Frage ermöglichen, ob sich der Einstieg in eine Cloud-Computing-Lösung allenfalls lohnt oder nicht. Ausserdem soll eine kurze und prägnante Checkliste dem Leser und potentiellen Cloud-Nutzer eine möglichst strukturierte Herangehensweise an das Projekt Cloud-Nutzung erleichtern.

---

63 HOFFMANN, S. 466.
64 Z.B. bei WEISS, Handbuch Cloud Computing, Teil 1 A, Rz. 48.

C. Datenschutz

49 Lagert ein Unternehmen seine Daten in die Cloud aus, nimmt es zwangsläufig einen Kontrollverlust in Kauf. Cloud-Lösungen implizieren diverse datenschutzrechtliche Probleme, weshalb es für zukünftige Cloud-Computing-Nutzer essentiell ist, dass den Vorschriften zum Datenschutz Rechnung getragen wird. Dieses Kapitel soll deshalb die verschiedenen datenschutzrechtlichen Themen beleuchten, welche bei der Nutzung von Cloud-Lösungen zu beachten sind. Dabei wird aber nur die schweizerische Gesetzgebung als Grundlage herangezogen.[65]

I. Datenschutzrechtliche Anforderungen an Cloud Computing

1. Anwendungsbereich des Datenschutzgesetzes

50 Werden Daten einer bestimmten bzw. bestimmbaren natürlichen oder juristischen Person bearbeitet, so findet das Datenschutzgesetz (DSG) Anwendung.[66] Das Gesetz umschreibt den Begriff des „Bearbeitens“ in Art. 3 lit. e so, dass darunter jeder Umgang mit Personendaten fällt, unabhängig von den angewandten Mitteln und Verfahren. Insbesondere sind darunter das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder das Vernichten von Daten zu verstehen. Werden in einer Cloud also Daten von natürlichen oder juristischen Personen bearbeitet (z.B. wenn Kundendaten gespeichert werden), so ist das schweizerische Datenschutzgesetz grundsätzlich anwendbar.[67]

51 Das DSG macht keine Angaben zu seinem örtlichen Geltungsbereich. Aufgrund seines öffentlich-rechtlichen Charakters gilt deshalb das Territorialitätsprinzip.[68] Es erfasst demnach nur Sachverhalte, die sich in der Schweiz zutragen. Das Bundesverwaltungsgericht führte jedoch aus, dass unter die Bearbeitung von Personendaten auch die Bekanntgabe von Daten ins Ausland sowie die Sammlung von persönlichen Daten aus einem Standort im Ausland in der Schweiz fällt.[69]

---

65 Innerhalb der EU sind die wichtigsten Regelungen zum Datenschutz in der Richtlinie 95/46 EG enthalten. Diese Richtlinie findet zwar auf Cloud Computing Anwendung, sie sieht aber – anders als das schweizerische Datenschutzgesetz – als Mindeststandard lediglich den Schutz von Daten für natürliche Personen vor.

66 Vgl. Art. 2 DSG.

67 SCHWANINGER/LATTMANN, S. 2.

68 Vgl. dazu Urteil des Bundesverwaltungsgerichts A-7040/2009 vom 30.03.2011 E 5.4.1.

69 Urteil des Bundesverwaltungsgerichts A-7040/2009 vom 30.03.2011 E 5.4.1, sowie das Urteil A-3144/2008 vom 27.05.2009 E 4.2.

2. Auftragsbearbeitung gemäss Art. 10a DSG

52 Werden Personendaten eines Cloud-Nutzers in der Cloud gespeichert, und nicht wie bisher auf seinem eigenen Server, so liegt aus datenschutzrechtlicher Sicht eine Datenbearbeitung durch Dritte i.S.v. Art. 10a DSG vor (auch Auftragsbearbeitung genannt).[70] Damit eine solche Bearbeitung der Daten zulässig ist, müssen die Voraussetzungen von Art. 10a Abs. 1 DSG erfüllt sein: Die Daten dürfen vom Cloud-Anbieter nur so bearbeitet werden, wie der Cloud-Nutzer es selbst tun dürfte (lit. a), und die Bearbeitung durch einen Dritten darf durch keine gesetzliche oder vertragliche Geheimhaltungspflicht verboten sein (lit. b). Zudem muss der Cloud-Nutzer als Auftraggeber sicherstellen, dass der Cloud-Provider die Datensicherheit gewährleistet (Art. 10a Abs. 2 DSG).[71] Liegt eine rechtmässige Auftragsbearbeitung vor, so wird der Cloud-Anbieter im Verhältnis zum Cloud-Nutzer nicht mehr als Dritter betrachtet und die Bekanntgabe von Personendaten durch den Cloud-Nutzer an den Cloud-Anbieter zieht nicht die Rechtsfolgen einer unrechtmässigen Datenbekanntgabe an Dritte nach sich.[72]

53 Für den Cloud-Nutzer stellt die letzte Voraussetzung eine praktische Herausforderung dar. Er muss potentielle Cloud-Anbieter und deren Sicherheitsstandards untersuchen und eine umfassende Risikoeinschätzung der Cloud-Anbieter in organisatorischer, rechtlicher und technischer Hinsicht vornehmen. Eine sorgfältige Auswahl ist deshalb sehr zu empfehlen und es sollte genau geprüft werden, ob der Cloud-Anbieter die notwendigen Voraussetzungen für eine datenschutzkonforme Datenbearbeitung erfüllt und die gewünschte bzw. gesetzlich vorgeschriebene Datensicherheit gewährleisten kann. Dabei gilt der Grundsatz des EDÖB: „*Je vertraulicher, geheimer, wichtiger (weil geschäftskritisch) oder sensitiver (weil besonders schützenswert) die Daten sind, umso eher ist von einer Auslagerung der Daten in die Cloud abzusehen, und desto strikter und umfassender müssen die (Datenschutz-)Sicherheitsvorkehrungen und deren Kontrolle sein*“[73].

54 Aus vertraglicher Sicht muss sich der Cloud-Nutzer gegenüber dem Cloud-Anbieter deswegen ein Weisungsrecht in Bezug auf die Datenbearbeitung ausbe-

---

70 EDÖB, Erläuterungen zu Cloud Computing, S. 2.
71 FUCHS, S. 3 ff.
72 SCHWANINGER/LATTMAN, Rz. 11.
73 EDÖB, Erläuterungen zu Cloud Computing, S. 3.

dingen, um ihn auch entsprechend instruieren zu können.[74] Falls der Cloud-Anbieter einen Sub-Provider beiziehen möchte, so muss der Cloud-Nutzer sicherstellen, dass für den Sub-Provider dieselben Pflichten gelten wie für den Cloud-Anbieter.[75]

55 Es ist jedoch wichtig, zu wissen, dass letztlich dennoch der Cloud-Nutzer als Auftraggeber gegenüber den betroffenen Personen für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich ist.[76] Trotz aller organisatorischer Massnahmen, die ein Cloud-Anbieter treffen kann, um die Datensicherheit zu gewährleisten, sollte der Cloud-Nutzer im Vorfeld sorgfältig abwägen, welche Daten er in die Cloud auslagern will.

II. Cloud-Services mit Auslandberührung

56 Die Nutzung von Cloud Computing weist häufig einen Auslandbezug auf, da die Datenbearbeitung durch grosse Cloud-Anbieter meist auf weltweit verteilten Servern stattfindet. Anders als beim klassischen Outsourcing ist für den Nutzer einer Cloud-Lösung nicht immer erkennbar, wo die Server stehen, auf denen seine Daten gespeichert werden.[77] Um zu beurteilen, ob eine Datenbearbeitung im Ausland erfolgt, ist auf den tatsächlichen Ort der Datenbearbeitung abzustellen und nicht auf den Sitz des Cloud-Anbieters.[78] Falls sich ein Server im Ausland befindet, so ist dies aus gesetzlicher Sicht von Relevanz. Denn obwohl eine Auftragsbearbeitung i.S.v. Art. 10a DSG vorliegt, muss ebenso Art. 6 DSG eingehalten werden.

1. Datentransfer ins Ausland

57 Art. 6 DSG schliesst eine grenzüberschreitende Datenbekanntgabe aus, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet würde, namentlich weil im Zielland eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.[79] Um zu prüfen, ob aus Schweizer Sicht ein angemessenes Schutzniveau besteht, kann auf eine vom EDÖB publizierte Liste zurückgegriffen

---

74 BSK DSG-CORRADO RAMPINI, Art. 14 N 11; ROSENTHAL, Handkommentar zum DSG, Art. 10a N 52 ff.
75 SCHWANINGER/LATTMAN, Rz. 13.
76 EDÖB, Erläuterungen zu Cloud Computing, S. 4.
77 So kann es z.B. sein, dass ein weiterer Server unbestimmten Standorts hinzugezogen wird, falls der ursprünglich zugeteilte Server nicht mehr ausreicht; m.w.H.: FUCHS, Rz. 16.
78 FUCHS, Rz. 18.
79 Art. 6 Abs. 1 DSG.

werden, auf der alle Länder aufgeführt sind, welche diese Anforderung erfüllen.[80] Auf der Liste sind alle EU-Mitgliedsstaaten sowie die Staaten des EWR zu finden. Besteht im Zielland kein angemessenes Datenschutzniveau und es erfolgt ein Datenexport gestützt auf vertragliche Pflichten, so muss der EDÖB vor der Übermittlung der Daten über die mit dem Cloud-Anbieter vereinbarten Datenschutzregeln informiert werden.[81] Der EDÖB bewilligt eine Datenübermittlung, wenn die Voraussetzungen von Art. 6 Abs. 2 DSG erfüllt sind, d.h. wenn eine Einwilligung der betroffenen Person im Einzelfall vorliegt oder „hinreichende Garantien" einen angemessenen Schutz gewährleisten können.[82]

58 Über kein angemessenes Datenschutzniveau verfügen die Vereinigten Staaten von Amerika. Wegen der Relevanz der diversen grossen US-amerikanischen Cloud-Anbieter (IBM, Google, Amazon etc.) soll kurz auf den Spezialfall des Datentransfers in die USA eingegangen werden.

2. Datentransfer in die USA

59 Wegen des nicht angemessenen Datenschutzniveaus in den Vereinigten Staaten von Amerika dürfen Personendaten an ein Unternehmen in den USA nur übermittelt werden, wenn dafür spezielle Garantien vereinbart wurden. Der EDÖB hat dafür gemeinsam mit dem Staatssekretariat für Wirtschaft (SECO) mit dem U.S. Department of Commerce das U.S.-Swiss Safe Harbor Framework ausgehandelt.[83]

60 US-Unternehmen haben die Möglichkeit, dem U.S.-Swiss Safe Harbor Framework beizutreten und sich so zu einem bestimmtem Schutzniveau für den Umgang mit Personendaten zu verpflichten.[84] Werden Daten an US-Unternehmen bekanntgegeben, die nach dem U.S.-Swiss Safe Harbor Framework zertifiziert sind, so fällt

---

80 Die Liste erstellt der EDÖB aufgrund von Art. 31 Abs. 1 lit. d DSG i.V.m. Art. 7 VDSG und sie ist online verfügbar unter <http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html> (zuletzt besucht am 3. Oktober 2014).

81 Gem. Art. 6 Abs. 5 VDSG hat der EDÖB dazu 30 Tage Zeit. Vgl. dazu STRAUB, Cloud Verträge, S. 917.

82 Als „hinreichende Garantie" gilt bspw. der vom EDÖB publizierte „Mustervertrag für das Outsourcing von Datenbearbeitungen ins Ausland"; online verfügbar unter <http://www.edoeb.admin.ch/datenschutz/00626/00743/00858/00859/index.html> (zuletzt besucht am 20. Oktober 2014).

83 Bilaterales Datenschutzrahmenwerk zwischen der Schweiz und den USA unterzeichnet, Medienmitteilung EDÖB, Bern 09.12.2008, online verfügbar unter <https://www.news.admin.ch/message/index.html?lang=de&msg-id=23809> (zuletzt besucht am 3. Oktober 2014).

84 Die Liste der von der International Trade Administration (ITA) zertifizierten Unternehmen ist online verfügbar unter <https://safeharbor.export.gov/swisslist.aspx> (zuletzt besucht am 3. Oktober 2014).

eine solche Datenbekanntgabe nach Ansicht des EDÖB nicht unter Art. 6 Abs. 2 DSG.[85]

III. Gesetzliche Spezialfälle

61 Zusätzlich zum Datenschutzgesetz gibt es noch weitere gesetzliche Vorschriften, die gewisse Daten unter einen besonderen Schutz stellen. Nachfolgend wird auf die Spezialfälle der Klientendaten von Anwälten, Patientendaten von Ärzten sowie Bankkundendaten eingegangen und aufgezeigt, unter welchen Voraussetzungen solche Daten in eine Cloud ausgelagert werden können.

1. Bankkundendaten

62 Aufgrund der hohen Sensibilität von Bankkundendaten gelten für Banken spezielle Voraussetzungen, wenn sie Cloud-Dienstleistungen in Anspruch nehmen wollen. Die eidgenössische Finanzmarktaufsicht (FINMA) erliess 2008 ein Rundschreiben, welches den Banken Vorschriften zur Auslagerung von Geschäftsbereichen macht. Die Grundsätze in diesem Rundschreiben sind von Banken zu beachten, wenn sie Bankkundendaten in eine Cloud auslagern.[86] So sind Banken gem. Grundsatz 6 des erwähnten Rundschreibens dazu verpflichtet, Kunden, deren Daten durch eine Outsourcing-Lösung an einen externen Dienstleister gelangen, über die Auslagerung ihrer Daten zu informieren. Für den Umgang mit elektronischen Kundendaten ist ausserdem Anhang 3 des Rundschreibens betr. operationelle Risiken von Bedeutung, welcher im Rahmen einer Teilrevision des Rundschreibens eingefügt wurde und auf den 1. Januar 2015 in Kraft tritt.[87] In diesem Anhang formuliert die FINMA Grundsätze für das sachgerechte Management von Risiken im Zusammenhang mit der Vertraulichkeit elektronischer Personendaten natürlicher Personen.[88]

---

85 BHEND, S. 122 ff.

86 Eidg. Finanzmarktaufsicht FINMA, Rundschreiben 2008/7 – Outsourcing Banken; Auslagerung von Geschäftsbereichen bei Banken, 20. November 2008, online verfügbar unter <https://www.finma.ch/d/regulierung/Documents/finma-rs-2008-07.pdf> (zuletzt besucht am 23. Oktober 2014).

87 Vgl. Medienmitteilung: FINMA veröffentlicht Rundschreiben „Operationelle Risiken Banken“ vom 1.10.2013, online verfügbar unter <http://www.finma.ch/d/aktuell/seiten/mm-rs-opr-risiken-banken-20130110.aspx> (zuletzt besucht am 23. Oktober 2014).

88 Eidg. Finanzmarktaufsicht FINMA, Rundschreiben 2008/21 – Operationelle Risiken Banken; Eigenmittelanforderungen und qualitative Anforderungen für operationelle Risiken bei Banken, 20. November 2008, online verfügbar unter <https://www.finma.ch/d/regulierung/Documents/finma-rs-2008-21.pdf> (zuletzt besucht am 23. Oktober 2014).

63 Grundsatz 2 schreibt vor, dass eine Bank alle Kundendaten, die sie verarbeitet, kategorisieren muss. Dies bedeutet, dass zunächst jene Daten festzulegen sind, die es ermöglichen, einen Kunden zweifelsfrei zu identifizieren (Client Identifying Data, CID).[89] Gem. Grundsatz 3 muss die Bank stets wissen, wo CID gespeichert sind, von welchen Anwendungen und IT-Systemen CID verarbeitet werden und wo elektronisch auf sie zugegriffen werden kann. Zudem müssen CID, falls sie ausserhalb der Schweiz gespeichert werden, angemessen geschützt sein (z.B. mittels Anonymisierung oder Verschlüsselung).[90] Die Banken sind also für die CID, welche sie in die Cloud auslagern, zu einem höheren Schutzniveau verpflichtet.

2. Klientendaten von Anwälten

64 Rechtsanwälte und deren Hilfspersonen sind dem Anwaltsgeheimnis unterstellt. Dieses Berufsgeheimnis wird durch Art. 321 StGB (Schweizerisches Strafgesetzbuch) und Art. 13 BGFA (Anwaltsgesetz) geschützt. Lagert ein Anwalt seine Daten in die Cloud aus, so ist der Cloud-Anbieter als Hilfsperson i.S.v. Art. 321 StGB zu qualifizieren, sofern es sich um einen Schweizer Anbieter handelt und seine Server in der Schweiz stehen. In diesem Fall ist eine Auslagerung der Klientendaten in die Cloud zulässig, da der Anbieter als Hilfsperson der berufsspezifischen Geheimhaltungspflicht untersteht.[91]

65 Handelt es sich jedoch nicht um einen schweizerischen Cloud-Anbieter oder stehen die Server nicht in der Schweiz, so gilt der Anbieter nicht als Hilfsperson im Sinne des Gesetzes, da er diesem auch nicht untersteht. In diesem Fall können die Daten nur in die Cloud ausgelagert werden, sofern der betr. Klient seine Einwilligung dazu abgibt (er muss dabei auf alle möglichen Risiken hingewiesen werden, wie z.B. den Zugriff durch die ausländischen Behörden). Gem. SCHWANINGER/LATTMAN wäre die Auslagerung der Daten in die Cloud ohne eine Einwilligung strafbar und würde eine Verletzung des Anwaltsgeheimnisses darstellen.[92] Noch fehlt aber eine offizielle Stellungnahme oder Empfehlung einer Aufsichtsbehörde. Der Schweizerische Anwaltsverband (SAV) ist der Meinung, dass Klienten nicht vorgängig über die Cloud-Nutzung informiert werden müssen. Nach Ansicht des

---

89 Kundendaten besser schützen, Neue Zürcher Zeitung vom 24.5.2013, online verfügbar unter <http://www.nzz.ch/aktuell/wirtschaft/wirtschaftsnachrichten/kundendaten-besser-schuetzen-1.18086186> (zuletzt besucht am 23. Oktober 2014).

90 FINMA, Anhang 3, Rundschreiben „Operationelle Risiken Banken“, Rz. 9 ff.

91 SCHWANINGER/LATTMAN, Rz. 35.

92 SCHWANINGER/LATTMAN, Rz. 35.

SAV ist also die Pflicht zur Kundenorientierung, wie sie sich für Banken aus dem Rundschreiben 2008/7 der FINMA ergibt, für Anwaltskanzleien nicht analog anwendbar.[93] Doch insbesondere wenn es um die Bestimmung der erforderlichen Sorgfalt im Umgang mit Kundendaten geht, können die Grundsätze dieses Rundschreibens durchaus als „best practice" herangezogen werden.[94]

66 Auf europäischer Ebene setzt sich der Rechtsanwaltsdachverband CCBE einerseits bei der Europäischen Kommission für einheitliche Vorgaben zum Thema Cloud Computing ein und andererseits hat er selbst allgemein gehaltene Empfehlungen für Anwälte erlassen, welche bei der Nutzung von Cloud-Lösungen zu beachten sind.[95]

3. Patientendaten von Ärzten

67 Da Ärzte ebenfalls dem Berufsgeheimnis gem. Art. 321 StGB unterstellt sind, gelten für die Auslagerung von Patientendaten die gleichen Grundsätze wie bei der Auslagerung von Klientendaten bei Anwälten. Für weiterführende Fragen muss indes aus Platzgründen auf die einschlägige Spezialliteratur verwiesen werden.[96]

---

93 So zumindest zum heutigen Stand, wie Herr Adrian Rufener (Vorstandsmitglied SAV) in einer Veranstaltung des Zürcher Anwaltsverbandes zum Thema Cloud Computing in Anwaltskanzleien vom 13. November 2014 ausführte.

94 So gem. Peter Neuenschwander und Wolfgang Straub, wie sie im Rahmen einer Veranstaltung zum Thema Cloud Computing der Fachgruppe ICT – Recht und Praxis des EIZ vom 5. September 2013 ausführten.

95 Siehe dazu: „CCBE Response regarding the European Commission Public Consultation on Cloud Computing", online verfügbar unter <http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_090911_CCBE_Respo1_1316068571.pdf>, sowie „CCBE Guidelines on the Use of Cloud Computing Services by Lawyers", online verfügbar unter <http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/07092012_EN_CCBE_gui1_1347539443.pdf>, beide zuletzt besucht am 19. November 2014.

96 Siehe zum Ganzen: URSULA WIDMER, Gesundheitsdaten in der Cloud, in: P. SCHARTER/J. TAEGER (Hrsg.), D•A•CH Security 2011, syssec 2011, S. 166–177.

D. Datensicherheit

I. Technische und organisatorische Massnahmen

68 Die schweizerische Datenschutzgesetzgebung schreibt vor, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen.[97] Der Cloud-Nutzer muss sicherstellen, dass sein Cloud-Provider die Daten gegen unbefugtes Bearbeiten schützt (Art. 7 Abs. 1 DSG) sowie die Verfügbarkeit und die Integrität der Daten sichergestellt ist (Art. 8 Abs. 1 VDSG). Insbesondere die folgenden Risiken müssen abgesichert werden: unbefugte oder zufällige Vernichtung oder zufälliger Verlust; technische Fehler; Fälschung; Diebstahl oder widerrechtliche Verwendung; unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitung.[98]

1. Vor-Ort-Kontrollen

69 Ein potentieller Cloud-Nutzer ist bei der Auswahl eines Cloud-Anbieters aufgrund der Sorgfaltspflicht aus Art. 10a DSG verpflichtet, darauf zu achten, dass die oben genannten Voraussetzungen von Art. 7 Abs. 1 DSG sowie Art. 8 VDSG durch den Cloud-Anbieter eingehalten werden. Diese Verpflichtung kann einen potentiellen Cloud-Nutzer jedoch vor Schwierigkeiten stellen. Wie soll er sich in der Praxis vergewissern, dass der Cloud-Anbieter die Voraussetzungen erfüllt?

70 Der EDÖB empfiehlt in seinen Erläuterungen zum Cloud Computing, die Massnahmen des Cloud-Anbieters gegen unbefugtes Bearbeiten periodisch vor Ort zu überprüfen.[99] Eine solche Vor-Ort-Kontrolle ist aber wohl nur selten möglich oder praktikabel. Der Nutzer einer standardisierten Cloud-Lösung hat meistens nur wenig Einfluss auf die datensicherheitstechnische Ausgestaltung des Providers. Überdies wäre es der Sicherheit in einem Datencenter nicht förderlich, wenn etwa alle Nutzer einer Public Cloud, was viele Tausend bis Hunderttausend Kunden sein können, Audits in den Rechenzentren des Anbieters vornehmen würden. Lediglich grossen Nutzern einer Public Cloud wird wohl ein Inspektionsrecht gewährt.

71 Das Gesetz beantwortet die Frage, wie der Cloud-Nutzer seinen Provider tatsächlich überprüfen soll, nicht. In der Lehre wird deshalb davon ausgegangen, dass es ausreicht, wenn sich der Cloud-Nutzer auf eine äquivalente Weise ein Bild von der

---

97 Art. 7 DSG.
98 Art. 8 Abs. 1 VDSG; siehe dazu SCHWANINGER/LATTMAN, Rz. 21; FUCHS, Rz. 21.
99 EDÖB, Erläuterungen zu Cloud Computing, S. 3.

Einhaltung der Datensicherheit machen kann.[100] Regelmässige Reportings des Cloud-Anbieters wären ein möglicher Kompromiss, oder der Cloud-Nutzer kann bspw. nur mit zertifizierten Providern zusammenarbeiten.[101]

2. Verfügbarkeit, Ausfallsicherheit und Datenwiederherstellung

72 Anhand eines konkreten Beispiels soll aufgezeigt werden, wie der Cloud-Nutzer sicherstellen kann, dass sein Cloud-Provider die gesetzlichen Datenschutzbestimmungen erfüllt. Gem. Art. 8 Abs. 1 VDSG muss der Bearbeiter von Personendaten die Verfügbarkeit der Daten gewährleisten. In der Praxis wird dies durch ein Service Level Agreement (SLA) sichergestellt.[102]

73 Die Verfügbarkeit definiert den Zeitraum, in welchem das Cloud-Computing-System dem Kunden zur Nutzung zur Verfügung stehen muss, wann er also auf seine Daten zugreifen kann. Die Betriebszeiten können den Bedürfnissen des jeweiligen Kunden angepasst werden und sollten von den Parteien mit grosser Sorgfalt festgelegt werden. Ein Unternehmen, das bspw. nur während der üblichen Geschäftszeiten Aufträge entgegennimmt, kann möglicherweise auf eine jederzeitige Verfügbarkeit verzichten.[103] Eine solche Klausel könnte folgendermassen ausformuliert werden: „*Der Dienstleistungserbringer sichert dem Kunden eine Verfügbarkeit des Systems jeweils von Montag bis Freitag von 08:00 Uhr bis 17:30 Uhr, ausgenommen gesetzliche Feiertage in [Kanton/Land], zu.*“[104]

74 Gemeinsam mit der Verfügbarkeit sollte die Ausfallsicherheit vertraglich vereinbart werden, d.h. ob und wie lange das System während der Betriebszeiten nicht zur Verfügung stehen darf, ohne dass den Provider die festgelegten Folgen treffen. Die gewünschte Ausfallsicherheit hängt ebenfalls von den Wünschen des Kunden ab, so bedürfen zeitkritische Anwendungen (z.B. die Auftragserfassung eines Grossunternehmens) einer möglichst hohen Ausfallsicherheit, dafür können weniger zeitkritische Abläufe (z.B. Zugriff auf Archivdaten) mit einer geringeren Ausfallsicherheit auskommen. Eine entsprechende Klausel in einem SLA könnte folgendermassen lauten: „*Der Dienstleistungserbringer sichert eine durchschnittliche*

---

100 HOFFMANN, S. 468; FUCHS, Rz. 24.
101 Cloud-Anbieter können sich bspw. nach ISO/IEC 20000 oder EuroCloud zertifizieren lassen; siehe dazu MÜLLER, S. 1 ff.
102 Siehe dazu Kapitel B III 2.
103 Siehe zum Ganzen GUROVITS KOHLI, S. 97 ff.
104 Diese Klausel soll lediglich ein Vorschlag darstellen und erhebt keinen Anspruch auf Vollständigkeit. Für weitere Vorschläge siehe GUROVITS KOHLI, S. 103 ff.

Mindest-Verfügbarkeit von 99% pro jeweils drei Monate zu. Diese Mindestverfügbarkeit berechnet sich als Mittelwert während jeweils eines Quartals.“[105]

75 Des Weiteren sollten es potentielle Cloud-Nutzer nicht unterlassen, sich mit ihrem Cloud-Anbieter über eine allfällige Notfallwiederherstellung von Daten zu einigen. Das sog. Disaster Recovery bezeichnet Massnahmen, welche nach einem Zusammenbruch des IT-Systems eingeleitet werden. Unterschieden werden dabei RPO (Recovery Point Objective) und RTO (Recovery Time Objective). Der RPO ist der Wiederanlauf-Zeitpunkt nach dem Ausfall des betr. Systems. Wird bspw. alle 24 Stunden ein Back-Up erstellt, so beträgt der RPO 24 Stunden. Daten, die sich innerhalb dieser Zeitspanne geändert haben, sind nach einem Ausfall des Systems schlimmstenfalls verloren.[106]

76 Damit zusammenhängend steht RTO für die Wiederanlauf-Dauer, d.h. die Zeitspanne, bis der Cloud-Nutzer nach dem Zusammenbruch der Cloud wieder Zugriff auf seine Daten hat.[107] Natürlich sind RPO und RTO Kostenfaktoren, denn je umfangreicher der Schutz der Daten bei einem möglichen Systemausfall sein soll, desto teurer wird es für den Kunden.[108]

II. Rechtliche Risiken

1. Kontrollverlust über die Daten

77 Ein grosser Vorteil des Cloud Computing, nämlich die Skalierbarkeit der Cloud-Services, ist im Hinblick auf den Datenschutz auch gleichzeitig ein grosser Nachteil. Dadurch, dass der Cloud-Nutzer seine Daten auf die Server seines Cloud-Anbieters auslagert, hat er automatisch nicht mehr die volle Kontrolle über seine Daten. Der Cloud-Anbieter hat seine Server möglicherweise auf der ganzen Welt verteilt oder lässt sie teilweise durch Sub-Provider betreiben, welche dem Cloud-Nutzer schlimmstenfalls gar nicht bekannt sind.[109]

78 Public-Cloud-Nutzer sind dieser Gefahr am ehesten ausgesetzt, da sie, wie bereits erwähnt, oftmals die AGB ihres Providers akzeptieren müssen, ohne dabei Ände-

---

105 GUROVITS KOHLI, S. 103.

106 Siehe dazu <http://www.itwissen.info/definition/lexikon/recovery-point-objective-RPO.html> (zuletzt besucht am 20. Oktober 2014).

107 Siehe dazu <http://www.itwissen.info/definition/lexikon/recovery-time-objective-RTO.html> (zuletzt besucht am 20. Oktober 2014).

108 Einen umfangreichen Schutz bietet eine sog. CDP-Lösung (continuous data protection), doch diese ist mit entsprechend hohen Kosten verbunden.

109 FUCHS, Rz. 26.

rungen bzgl. technischer oder organisatorischer Massnahmen anbringen zu können.[110]

79 Anhand der AGB eines Cloud-Providers soll aufgezeigt werden, wie ein Nutzer die Kontrolle über seine Daten verlieren kann. Die Amazon Web Services Inc. (AWS) schreibt in ihrem Customer Agreement zum Thema Datenschutz Folgendes: „*We participate in the safe harbor programs described in the Privacy Policy. You may specify the […] regions in which Your Content will be stored and accessible by End Users.*" Dies mag vielversprechend klingen, doch die Aussage wird durch den folgenden Absatz relativiert: *„We will not move Your Content from your selected […] regions without notifying you, unless required to comply with the law or requests of governmental entities."*[111]

80 Diese geschickt formulierte Klausel ermöglicht es Amazon also durchaus, die Daten in andere als die vom Kunden gewünschten Regionen zu verschieben. Sie muss den Kunden lediglich davon in Kenntnis setzen. Selbst diese Informationspflicht kann jedoch entfallen, falls es rechtlich oder aufgrund einer behördlichen Anfrage notwendig ist.

2. Datentrennung

81 Das Konzept der gemeinsamen Nutzung der Server eines Cloud-Anbieters durch verschiedene Kunden wurde bereits erläutert. Aus datenschutzrechtlicher Sicht ist die konsequente Trennung der Daten der einzelnen Kunden von grosser Relevanz. Gerade bei Public Clouds besteht für die Nutzer das Risiko, durch Hackerattacken auf einen Mitnutzer in Mitleidenschaft gezogen zu werden.[112] So kann es bei einer ungenügenden Trennung zwischen den Daten der Cloud-Nutzer dazu kommen, dass ein Nutzer wegen eines Hackerangriffs nicht mehr auf seine Daten zugreifen kann, obwohl er selber nicht das Ziel des Angriffs war. Eine klare Trennung bei der Datenbearbeitung durch den Cloud-Provider (sog. „Chinese Wall") ist deshalb äusserst wichtig. Da das Risiko, Opfer eines solchen Angriffs zu werden, leider nie ganz ausgeschlossen werden kann, empfiehlt es sich, sensitive Daten nur in eine Private Cloud auszulagern.[113]

---

110 FUCHS, Rz. 27.

111 Ziffer 3.2. Data Privacy des Customer Agreement von Amazon Web Services Inc., online verfügbar unter <http://aws.amazon.com/de/agreement/> (zuletzt besucht am 20. Oktober 2014).

112 So geschehen beim Online-Speicherdienst Dropbox, siehe dazu <http://www.20min.ch/digital/webpage/story/26286778> (zuletzt besucht am 4. Oktober 2014).

113 FUCHS, Rz. 29.

3. Zugriff durch Behörden

82 Wegen der weltweiten Vernetzung lässt es sich in vielen Fällen nicht vermeiden, dass Daten auf einem Server im Ausland gespeichert werden. Eine nicht zu unterschätzende Gefahr für die Daten liegt deshalb in den Zugriffsrechten in- und ausländischer Behörden gegenüber dem Cloud-Provider.[114]

a) Zugriff durch schweizerische Behörden

83 In der Schweiz können Behörden Personendaten abfragen und auswerten, dies gestützt auf das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)[115] und Art. 273 der Strafprozessordnung (StPO).[116] Im Vergleich zu den Möglichkeiten ausländischer Behörden bieten diese beiden gesetzlichen Ermächtigungen dem Schweizer Nachrichtendienst jedoch nur sehr beschränkte Überwachungskompetenzen.[117] Dies liegt hauptsächlich am hohen Aufwand, da für jede Abfrage eine Genehmigung beim Zwangsmassnahmengericht eingeholt werden muss.[118] Zudem ist es in der Schweiz Behörden nicht möglich, Zugang zu Unternehmensservern zu bekommen (bzw. Massenabfragen zu formulieren), da für jede Abfrage eine spezifische Person zu benennen ist.[119]

b) Spezialfall USA

84 Wegen der besonderen Relevanz soll wiederum der Spezialfall USA etwas näher erläutert werden. US-amerikanische Behörden, insbesondere die National Security Agency (NSA), haben gestützt auf den US Patriot Act, den Foreign Intelligence Surveillance Act (FISA) sowie den 50 US Code 1881a weitreichende Kompetenzen, Überwachungsmassnahmen durchzuführen.[120]

85 Es würde den Rahmen dieser Arbeit sprengen, auf alle erwähnten gesetzlichen Grundlagen genauer einzugehen. Entscheidend ist, dass die gesetzlichen Grundlagen es den US-amerikanischen Behörden ermöglichen, auf Daten ausserhalb

---

114 STRAUB, Cloud Verträge, S. 917.
115 Das BÜPF befindet sich zurzeit in Totalrevision, vgl. BBl 2013 2683 ff.
116 STRAUB, Cloud Verträge, S. 917.
117 WEBER/STAIGER, Rz. 54 ff.
118 Art. 272 Abs. 1 StPO i.V.m. Art. 13 Abs. 1 lit. a BÜPF.
119 Art. 270 StPO; m.w.H. WEBER/STAIGER, Rz. 54.
120 Daneben gibt es noch diverse weitere gesetzliche Grundlagen wie z.B. den FISA Amendments Act of 2008, den Electronic Communications Privacy Act (ECPA) und die Cyber Intelligence Sharing and Protection Bill (CISPA) sowie die Rechtsprechung des U.S. Supreme Court (z.B. *Katz v. United States, 389 U.S. 347, 361 (1967)*). Siehe zum Ganzen VAN HOBOKEN/ARNBAK/VAN EIJK, S. 16 ff.

der USA und von nicht-amerikanischen Personen zuzugreifen.[121] Voraussetzung dafür ist, dass diese Daten bei Gesellschaften gelagert sind, welche a) in den USA ihren Sitz haben, b) dort börsenkotiert sind, c) zu einem Konzern gehören, welcher US-Gesellschaften umfasst, oder auch d) lediglich eine dauerhafte Tätigkeit in den USA ausüben.[122] Ein Entscheid des Southern District Court of New York sorgte vor kurzem für Aufsehen. Das Gericht entschied, dass das US-Technologieunternehmen Microsoft Daten von einem Server, der in Irland steht, herausgeben muss. Konkret geht es um Daten von einem E-Mail-Konto eines Nutzers, welche aber ausserhalb der USA gespeichert sind und auf die deshalb, so argumentierte Microsoft, die US-Regierung keinen Zugriff hätte. Die zuständige Richterin betonte allerdings, dass es eine Frage der Kontrolle und nicht des Speicherorts sei.[123] Microsoft legte gegen den Entscheid Berufung ein und wurde dabei von diversen anderen Firmen wie AT&T, Apple und Cisco unterstützt. Wohl zu Recht fürchten diese Unternehmen einen solch weitreichenden Zugriff der US-Behörden auf Daten, da dies die vorherrschende Stellung von US-Unternehmen im Cloud-Computing-Markt schwächen würde.[124]

86 Aus schweizerischer Sicht kann man sich gegen diese extra-territoriale Anwendung von US-Recht nicht vertraglich absichern. Es kann somit nur empfohlen werden, die Angebote ausländischer Cloud-Anbieter nur dann zu verwenden, wenn man keine sensiblen Daten in die Cloud auslagern will. Des Weiteren empfiehlt sich eine Verschlüsselung der Daten durch entsprechende technische Massnahmen (sodass z.B. der Schlüssel in der Schweiz bleibt).[125]

4. Konkurs eines Cloud-Anbieters

87 Natürlich ist auch ein Cloud-Nutzer nicht davor gefeit, dass gegen seinen Cloud-Anbieter (oder dessen Sub-Provider) ein Insolvenzverfahren eröffnet wird. Wenn der Nutzer geschäftskritische Daten in die Cloud zu seinem Provider ausgelagert hat, kann dessen Insolvenz für den Nutzer möglicherweise zu unangenehmen

---

121 VAN HOBOKEN/ARNBAK/VAN EIJK, S. 16.

122 Siehe dazu STRAUB, Cloud Verträge, S. 917; WEBER/STAIGER, Rz. 85 ff.

123 Entscheid des Southern District Court of New York, 2014 U.S. Dist. LEXIS 59296 (S.D.N.Y. April 25, 2014), online verfügbar unter <http://www.nysd.uscourts.gov/show.php?db=special&id=398> (zuletzt besucht am 6. Oktober 2014).

124 Siehe dazu STEVE LOHR, Microsoft protests order to disclose email stored abroad, New York Times 10.06.2014, online verfügbar unter <http://www.nytimes.com/2014/06/11/technology/microsoft-protests-order-for-email-stored-abroad.html?_r=0> (zuletzt besucht am 4. Oktober 2014).

125 STRAUB, Cloud Verträge, S. 917.

Überraschungen führen. Auch wenn der Cloud-Nutzer Massnahmen zur frühzeitigen Erkennung von wirtschaftlichen Problemen seines Providers ergreift[126], sollte er sich dennoch über die Folgen eines möglichen Insolvenzverfahrens im Klaren sein.

88 Als Erstes stellt sich die Frage nach dem anwendbaren Insolvenzrecht. Dieses bestimmt sich nach dem Sitz des Cloud-Anbieters.[127] Aber gerade in internationalen Verhältnissen kann die Bestimmung des anwendbaren Rechts mit Schwierigkeiten verbunden sein, wenn z.B. ein Cloud-Anbieter seine Server auf der ganzen Welt verteilt hat und von Tochterunternehmen betreiben lässt.[128] Aus diesem Grund soll im Folgenden nur der Fall untersucht werden, dass der Cloud-Anbieter sowohl seinen Sitz als auch seine Rechenzentren in der Schweiz hat.

a) Aussonderungsansprüche

89 Geht ein Cloud-Anbieter in Konkurs, so haben seine Kunden ein Interesse daran, ihre Daten zurückzubekommen, denn sie wollen möglichst verhindern, dass diese in die Konkursmasse gelangen und sodann nicht mehr kontrolliert werden kann, an wen die Daten gelangen. Das schweizerische Schuldbetreibungs- und Konkursrecht (SchKG, SR 281.1) gibt einem Gläubiger die Möglichkeit, die konkursrechtliche Aussonderung für Sachen, die in seinem Eigentum stehen, zu verlangen.[129] Gem. der herrschenden Lehre und der konstanten Rechtsprechung des Bundesgerichts können Aussonderungsansprüche allerdings nur für körperliche Gegenstände geltend gemacht werden.[130] Für elektronische Daten, die auf den Servern des Cloud-Anbieters gespeichert sind, besteht kein Herausgabeanspruch, da sie nicht unter die gesetzliche Definition einer körperlichen Sache fallen.[131] Der Kunde kann lediglich die Aussonderung der Datenträger verlangen, welche in seinem Eigentum stehen.[132] Cloud-Nutzern kann deshalb empfohlen werden, dass Datenträger, welche sich beim Provider befinden, aber im Eigentum des Nutzers

---

126 So z.B. eine periodische Überprüfung der Kreditwürdigkeit des Cloud-Anbieters oder eine Verpflichtung desselben zur regelmässigen Information über Kennzahlen. Siehe dazu STRAUB, Cloud Verträge, S. 922.

127 BSK SchKG I-ERNST F. SCHMID, Art. 46 N 63 ff.

128 SCHWANINGER/LATTMAN, Rz. 51 ff.; STRAUB, Cloud Verträge, S. 922.

129 Art. 242 SchKG.

130 BSK SchKG II-MARC RUSSENBERGER, Art. 242 N 10.

131 SCHWANINGER/LATTMAN, Rz. 55.

132 Wenn ein Cloud-Nutzer bspw. seine Daten auf einer Festplatte dem Cloud-Anbieter übergeben hat, sodass dieser die Daten in die Cloud übertragen kann, siehe dazu SCHWANINGER/LATTMAN, Rz. 55; STRAUB, Cloud Verträge, S. 922.

stehen, auch als solche gekennzeichnet werden.[133] So erkennt die Konkursverwaltung sofort, wer daran berechtigt ist, und die Aussonderung kann vereinfacht werden.

90 Eine gesetzliche Lösung, wie sie in Luxemburg existiert, wäre jedoch auch für die Schweiz wünschenswert. In Luxemburg anerkannte der Gesetzgeber vor kurzem ein Aussonderungsrecht für Daten im Falle eines Konkurses, sofern die betr. Daten von den Daten der anderen Cloud-Nutzer getrennt werden können.[134]

b) Verwertung von Daten

91 Im Rahmen eines Konkurses gehört es zu den Aufgaben der Konkursverwaltung, die bestehenden Aktiven zu verwerten.[135] In diesem Zusammenhang stellt sich die Frage, ob Daten auf den Servern des Cloud-Anbieters einen Wert haben können und, falls ja, ob diese verwertet werden können, indem sie an einen Dritten verkauft werden.[136]

92 Antwort auf diese Frage gibt ein Positionspapier des Datenschutzbeauftragten des Kanton Zürichs (DSB). Der DSB ist der Ansicht, dass das Konkursamt im Rahmen seiner Aufgabenerfüllung Kundendateien verwerten darf. Zuvor sei jedoch in jedem Fall eine Interessenabwägung vorzunehmen. Im Rahmen einer solchen muss untersucht werden, von was für einem Vertrauensverhältnis die Vertragsbeziehung zwischen dem konkursiten Unternehmen und dem Kunden geprägt war. Je grösser das Vertrauensverhältnis war, desto eher ist eine Datenbekanntgabe einzuschränken. Bei einem qualifizierten Vertragsverhältnis sei grundsätzlich die Zustimmung der betroffenen Personen notwendig.[137]

93 Dies führt zum unbefriedigenden Ergebnis, dass der Cloud-Nutzer seine ausgelagerten Daten im Konkursfall seines Anbieters schlimmstenfalls nicht zurückerhält und dass sogar das Risiko besteht, dass seine Daten im Rahmen des Konkursverfahrens verwertet werden. Es ist aus diesem Grund jedem Cloud-Nutzer anzura-

---

133 Dies setzt jedoch voraus, dass der Kunde Eigentum am betr. Datenträger erworben hat und dass nur eine individuelle Speicherung seiner Daten auf dem Träger erfolgt (und der Träger nicht mit anderen Kunden geteilt wird).

134 Siehe dazu WELLENS, S. 1.

135 Art. 252 ff. SchKG.

136 SCHWANINGER/LATTMAN, Rz. 59.

137 Siehe zum Ganzen: Datenschutzbeauftragter des Kantons Zürich DSB, Kundendaten im Konkursverfahren, Oktober 2011, online verfügbar unter <https://dsb.zh.ch/internet/datenschutzbeauftragter/de/themen/gemeinden/betreibungen.html> (zuletzt besucht am 7. Oktober 2014).

ten, sicherzustellen, dass im Vertrag mit dem Cloud-Anbieter festgehalten wird, dass sämtliche Daten als vertraulich gelten und nicht ohne schriftliche Zustimmung an Dritte übergeben werden dürfen.[138] Eine solche Geheimhaltungsklausel kann jedoch eine Verwertung der Daten nicht vollends verhindern. Empfehlenswert ist aus diesem Grund, vertraglich festzuhalten, dass der Cloud-Anbieter auf allfällige Retentionsrechte an den Daten verzichtet.[139]

94 Um jegliche Restrisiken[140] auszuschliessen, sollten Cloud-Nutzer zusätzlich sämtliche Daten durch eine wirksame und zeitgemässe Verschlüsselung oder durch Anonymisierung der Datensätze schützen.[141]

c) Spezialfall Softwareentwicklung

95 Wurde im Rahmen des Cloud-Servicevertrags zwischen dem Nutzer und dem Provider Software entwickelt, so stellen sich im Rahmen eines Insolvenzfalls gewisse Detailfragen. So sollte vorvertraglich geregelt werden, welche Entwicklungsergebnisse wem gehören. Empfehlenswert ist auch, individualisierte Softwarekomponenten allenfalls bei einem Escrow-Agenten zu hinterlegen.[142]

III. Aufbewahrungsvorschriften

96 Heute verwenden wohl die meisten bilanzierungspflichtigen Unternehmen elektronische Buchführungssysteme, doch in Bezug auf die Datensicherheit dürfen Nutzer von Cloud-basierten Aufbewahrungssystemen für Geschäftsbücher und Belege gesetzliche Aufbewahrungspflichten nicht ausser Acht lassen. Die wesentlichen zu beachtenden Aufbewahrungsvorschriften finden sich im Obligationenrecht (OR) und in der Geschäftsbücherverordnung (GeBüV). Aufgrund der aufkommenden elektronischen Kommunikation und der digitalen Dokumentenaufbewahrung wurde die digitale Dokumentation im Rahmen einer Revision des OR den entsprechenden Dokumenten aus Papier gesetzlich gleichgestellt, somit wurde das papierlose

---

138 SCHWANINGER/LATTMAN, Rz. 61.

139 An Sachen, deren Natur eine Verwertung nicht zulässt, kann das Retentionsrecht jedoch nicht ausgeübt werden (Art. 896 Abs. 1 ZGB). Sind die Daten also nicht wirtschaftlich verwertbar, so fällt ein Retentionsrecht nach der h.L. weg. Siehe dazu STRAUB, Cloud Verträge, S. 922 (Fn. 142), sowie BGE 122 IV 322 E. 3a.

140 Falls Datenträger z.B. unvollständig gelöscht und sodann weiterverkauft werden.

141 SCHWANINGER/LATTMAN, Rz. 61; STRAUB, Cloud Verträge, S. 922.

142 Der Source Code beinhaltet die Gesetzmässigkeiten einer Software und stellt somit den Kern der schöpferischen Leistung des Software-Entwicklers dar. Für den Fall eines Konflikts empfiehlt es sich, eine Kopie des Source Code bei einem Dritten, dem sog. Escrow-Agenten (z.B. bei der Software Escrow AG, siehe <www.escrow.ch>), zu hinterlegen, welcher in klar definierten Fällen wie bspw. Konkurs oder Liquidation den Source Code dem Abnehmer herausgeben darf. Siehe zum Ganzen MEYER, S. 176 ff.

Führen von wichtigen Geschäftsunterlagen zulässig.[143] Die Einhaltung von Aufbewahrungsvorschriften ist ein wichtiger Teil der Compliance[144] und aus diesem Grund sollen die wichtigsten handelsrechtlichen und auch steuerrechtlichen Anforderungen erläutert werden, welche bei einer Auslagerung von Daten in die Cloud zu beachten sind.

1. Handelsrechtliche Anforderungen

97 Die Pflicht zur Buchführung ergibt sich aus Art. 957 OR und trifft alle Einzelunternehmen, Personengesellschaften und juristischen Gesellschaften, die verpflichtet sind, sich in das Handelsregister einzutragen.[145] Gem. Art. 957a Abs. 1 OR bildet die Buchführung die Grundlage der Rechnungslegung und beinhaltet sowohl die Führung eines Hauptbuches (sachlogische Gliederung aller verbuchten Geschäftsvorfälle) sowie eines Hilfsbuches (Angaben, die zur Feststellung der Vermögenslage sowie Schuld- und Forderungsverhältnisse des Geschäftsbetriebs notwendig sind).[146] Die Buchführung kann sowohl schriftlich als auch elektronisch erfolgen und auch elektronische Aufzeichnungen können als aufbewahrungspflichtiger Buchungsbeleg gelten.[147]

98 Die Aufbewahrungspflicht für Geschäftsbücher dient in erster Linie der Beweisführung im Falle einer späteren Auseinandersetzung.[148] Die Geschäftsbücher sowie Buchungsbelege sind deshalb während zehn Jahren aufzubewahren.[149] Werden Cloud-basierte elektronische Buchführungssysteme genutzt, so sind dabei die Grundsätze der ordnungsgemässen Datenverarbeitung einzuhalten.[150] Dazu gehört insbesondere, dass die aufbewahrten Bücher, Belege und Korrespondenz sorgfältig, geordnet und vor schädlichen Einwirkungen geschützt aufzubewahren

---

143 BSK OR II-MARKUS NEUHAUS/ERIK STEIGER, Art. 957 N 1.

144 Unter Compliance versteht man die Gesamtheit aller organisatorischen Massnahmen zur Verhinderung von Gesetzesverletzungen in Unternehmen. Aus Platzgründen kann in dieser Arbeit leider keine abschliessende Übersicht über diesen Themenkomplex geboten werden. Siehe zur IT-Governance generell EGLI, Rz. 1 ff.

145 BBl 2008 1696. Gem. Art. 934 OR ist verpflichtet, sich ins Handelsregister eintragen zu lassen, wer ein Handels-, Fabrikations- oder ein anderes nach kaufmännischer Art geführtes Gewerbe betreibt. Siehe dazu BSK OR II-MARTIN K. ECKERT, Art. 934 N 1 ff.

146 Art. 1 GeBüV.

147 Art. 957a Abs. 3 und 5 OR. Darunter können also auch E-Mails fallen, was z.B. bei der Umstellung von einer intern betriebenen E-Mail-Software auf einen E-Mail-Cloud-Service zu beachten wäre.

148 BEGLINGER/BURGWINKEL/LEHMANN/NEUENSCHWANDER/WILDHABER, S. 47.

149 Art. 958f OR. Die Aufbewahrungsfrist beginnt mit dem Ablauf des Geschäftsjahres.

150 Art. 2 Abs. 2-3 GeBüV.

sind.[151] Bei der permanenten Umschichtung von Daten, welche den Cloud-Services ja immanent ist, muss also sichergestellt sein, dass die aufbewahrten Daten gegen jegliche Veränderung geschützt sind.[152] Werden die im Original aufzubewahrenden Geschäftsbücher und Buchungsbelege elektronisch aufbewahrt, sind sie sogar mit einer qualifizierten elektronischen Signatur zu versehen.[153] Des Weiteren muss sichergestellt sein, dass die Daten innert angemessener Frist aufgefunden, eingesehen und geprüft werden können.[154]

2. Steuerrechtliche Anforderungen

99 Im Steuerrecht finden sich an unterschiedlichen Stellen Vorschriften, welche von Nutzern Cloud-basierter elektronischer Aufbewahrungsmöglichkeiten zu beachten sind. Aufgrund von Art. 126 Abs. 2 des Bundesgesetzes über die direkte Bundessteuer (DBG, SR 642.11) muss der Cloud-Nutzer z.B. sicherstellen, dass er auf Verlangen der Veranlagungsbehörde mündlich oder schriftlich Auskunft erteilen und seine Geschäftsbücher, Belege und weitere Bescheinigungen sowie Urkunden vorlegen kann.[155]

100 Steuerpflichtige Personen, die für den Vorsteuerabzug, die Steuererhebung oder den Steuerbezug relevante Daten und Informationen elektronisch übermitteln, empfangen und aufbewahren, müssen sicherstellen, dass diese während der ganzen gesetzlichen Aufbewahrungsfrist jederzeit lesbar gemacht werden können.[156] Erwähnenswert in diesem Zusammenhang ist zudem Art. 58 Abs. 2 Satz 3 MWSTG (Bundesgesetz über die Mehrwertsteuer, SR 641.20), wonach sich die gesetzliche Aufbewahrungspflicht unter Umständen bis zum Ende der Verjährung der Steuerforderung, auf welche sich die Geschäftsbücher, Belege, Geschäftspapiere und sonstigen Aufzeichnungen beziehen, verlängern kann.[157]

101 Abschliessend kann festgehalten werden, dass die gesetzlichen Aufbewahrungspflichten einer Nutzung von Cloud-Services bei der elektronischen Buchführung nicht im Wege stehen. Jedoch sollten die Nutzer die sich daraus ergebenden Anforderungen (jederzeitiger Zugriff, Unveränderbarkeit der Daten) genauestens ab-

---

151 Art. 5 GeBüV.
152 KNORR, Handbuch Cloud Computing, Teil 6 Rz. 79.
153 BBl 2008 1704.
154 Art. 6 Abs. 1 GeBüV.
155 BEGLINGER/BURGWINKEL/LEHMANN/NEUENSCHWANDER/WILDHABER, S. 72.
156 Art. 44 Abs. 1 MWSTGV.
157 Siehe dazu BEGLINGER/BURGWINKEL/LEHMANN/NEUENSCHWANDER/WILDHABER, S. 78.

klären und wenn möglich die entsprechenden Massnahmen für ihre Cloud-Nutzung mit dem Provider besprechen und ergreifen.

E. Haftung

102 In Bezug auf die Haftung ergeben sich gegenüber den bereits bekannten Grundsätzen von Outsourcing-Verträgen keine grossen Abweichungen. Cloud-Nutzer wünschen sich natürlich, dass Betriebsausfallsrisiken umfassend durch den Cloud-Anbieter abgesichert werden. Die Praxis zeigt jedoch, dass dieser Wunsch nur selten Realität wird. Ein Provider wird, sofern er überhaupt gewillt ist, über die Haftung zu verhandeln, nur selten dem Wunsch des Kunden nach umfassender Haftung nachkommen. Hält man sich vor Augen, dass ein einziger Vorfall bei einem Cloud-Anbieter allenfalls Tausende von Kunden betreffen kann, ist diese Abneigung gegen allzu umfassende Haftung nachvollziehbar. Ansonsten könnte bereits ein minimaler Ausfall ein existentielles Risiko für den Provider darstellen.[158]

I. Haftung des Cloud-Providers

103 Ausgangspunkt für die Haftung eines Cloud-Providers ist oftmals jener Teil der gesetzlichen Haftung, welcher nicht wegbedungen werden kann.[159] Gem. Art. 100 Abs. 1 OR sind Freizeichnungsklauseln nichtig, wenn sie die Haftung für rechtswidrige Absicht oder grobe Fahrlässigkeit ausschliessen, nicht aber, wenn die Freizeichnung leichte oder mittlere Fahrlässigkeit betrifft.[160] Eine weitergehende Haftung als für Vorsatz und Grobfahrlässigkeit wird oft in den AGB durch den Anbieter wegbedungen. Ein Beispiel für einen umfassenden Haftungsausschluss findet sich z.B. im bereits zitierten Customer Agreement von AWS.[161]

104 Eine etwas weniger weitreichende Variante findet man im Master Subscription Agreement von Salesforce.[162] Dieser Anbieter schliesst die Haftung nicht pauschal aus, sondern garantiert eine Haftung in der maximalen Höhe des Betrags, wel-

---

158 STAFFELBACH, S. 39.

159 Vgl. GAUCH/SCHLUEP/SCHMID/EMMENEGGER, Rz. 3076 ff.

160 BSK OR I-WIEGAND, Art. 100 N 1 ff.

161 Vgl. Ziffer 11 AWS Customer Agreement: „**Limitation of Liability.** NEITHER PARTY'S LIABILITY WITH RESPECT TO ANY SINGLE INCIDENT ARISING OUT OF OR RELATED TO THIS AGREEMENT WILL EXCEED THE AMOUNT PAID BY CUSTOMER HEREUNDER IN THE 12 MONTHS PRECEDING THE INCIDENT, PROVIDED THAT IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER HEREUNDER. THE ABOVE LIMITATIONS WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY. HOWEVER, THE ABOVE LIMITATIONS WILL NOT LIMIT CUSTOMER'S PAYMENT OBLIGATIONS UNDER SECTION 6 (FEES AND PAYMENT FOR PURCHASED SERVICES)", online verfügbar unter <http://aws.amazon.com/de/agreement/> (zuletzt besucht am 25. Oktober 2014).

162 Salesforce Master Subscription Agreement, online verfügbar unter <http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf> (zuletzt besucht am 25. Oktober 2014).

chen der Kunde in den letzten zwölf Monaten vor Eintritt des Schadensfalls einbezahlt hat. Salesforce nennt allerdings einige Ausnahmen von diesem Grundsatz, insbesondere besteht keine Haftung für mittelbare Schäden wie entgangene Gewinne.[163]

105 Sofern ein Kunde die Möglichkeit hat, allfällige Haftungsansprüche mit seinem Cloud-Anbieter zu verhandeln, sollte er in der Vertragsverhandlung auf die folgenden Punkte achten.[164] Im Cloud-Vertrag sollte klar geregelt werden, wie allfällige Schäden bewiesen und berechnet werden, denn die gesetzliche Beweislast ist in komplexen IT-Umgebungen nicht zwingend zielführend (wenn z.B. nur eine Partei Einblick in die betr. Systeme hat).[165] Ausserdem sollte das Verhältnis zu allfälligen Konventionalstrafen geklärt werden, denn gem. ROSENTHAL zeigen Vertragsstrafen (z.B. für nicht erreichte Service-Levels gem. SLA) oft mehr Wirkung als ein (meist) diffuses Haftungsrisiko.[166]

II. Haftung für Hilfspersonen

106 Oft ist es in der Realität so, dass der Cloud-Provider für seine Services auch die Hilfe von Subunternehmen (sog. Sub-Providern) in Anspruch nimmt. Im Grundsatz haftet der Geschäftsherr für den Schaden, den eine von ihm zur Erfüllung einer Schuldpflicht eingesetzte Hilfsperson bei der Ausübung dieser Tätigkeit verursacht, so Art. 101 OR.[167] Der Provider hat die Möglichkeit, seine Haftung für Subunternehmer in grösserem Ausmasse wegzubedingen als seine eigene Haftung gem. Art. 100 OR.[168] So kann er gem. Art. 101 Abs. 2 OR die Haftung des Geschäftsherrn durch eine im Voraus getroffene Verabredung beschränken oder aufheben.[169] Eine solche Wegbedingung muss aber unmissverständlich im Vertrag festgehalten sein.[170] In der Praxis wird aber regelmässig der Massstab der eigenüblichen Sorgfalt (die „diligentia quam in suis“) zur Geschäftsherrenhaftung vereinbart.

---

163 STAFFELBACH, S. 39.
164 Siehe dazu STRAUB, Cloud Computing – Checkliste, S. 3 ff.
165 Vgl. dazu ROSENTHAL, Haftungsfragen, S. 171 ff.
166 ROSENTHAL, Haftungsfragen, S. 174.
167 Siehe zum Ganzen BSK OR I-WIEGAND, Art. 101 N 1 ff.
168 BSK OR I-WIEGAND, Art. 101 N 16.
169 Die Wegbedingung erstreckt sich aber nur auf die vertragliche Haftung des Geschäftsherrn für die Hilfsperson, nicht jedoch auf die ausservertragliche Haftung der Hilfsperson selbst; siehe BSK OR I-WIEGAND, Art. 101 N 16.
170 BSK OR I-WIEGAND, Art. 101 N 16.

107 Der Anbieter kann auch, anstatt die Leistungen seiner Sub- und Mitunternehmer als eigene Leistungen mitanzubieten, auf gesonderte Verträge verweisen. So könnte er es vermeiden, für das Verschulden seiner Subunternehmer einstehen zu müssen. Dies wiederum bedeutet aber für den Kunden, dass er bei einem Leistungspaket überprüfen muss, ob er die einzelnen Leistungen von nur einem Provider erhält oder allenfalls (unbemerkt) mit verschiedenen Anbietern Verträge abschliesst.[171] Gem. SÖBBING kann es aber auch sein, dass sich für den Anbieter eine Haftung für seine Subunternehmer aufgrund des Auftragsrechts aus Art. 398 Abs. 3 und Art. 399 OR ergibt.[172]

[171] Solche Fragen stellen sich natürlich bei standardisierten Cloud-Lösungen nicht. Siehe dazu INTVEEN/HILBER/RABUS, Handbuch Cloud Computing, Teil 2 Rz. 18.

[172] Dies setzt jedoch voraus, dass der Subunternehmer als Substitut für den Generalunternehmer (sprich Hauptanbieter der Cloud-Lösung) tätig ist, so SÖBBING, S. 4.

F. Urheberrechte

108 In diesem Kapitel soll die Frage erläutert werden, inwiefern die verschiedenen Abläufe im Cloud Computing urheberrechtlich relevant sein können. Denn Cloud Computing hat einen wesentlichen urheberrechtlichen Aspekt. Die Cloud ermöglicht es, dass digitalisierte Werke vereinfacht weltweit angeboten und genutzt werden können. Urheberrechtlich relevante Fragen können sich somit sowohl für den Anbieter als auch für den Nutzer von Cloud-Lösungen stellen. So setzt bspw. jeder Anbieter von Cloud-Services Software ein, sei es Software, die der Anbieter für die von ihm angebotenen Services selber nutzt (z.B. E-Mail- oder Anti-Spam-Software), oder Software, die der Anbieter im Rahmen eines SaaS-Lösung dem Nutzer zur Verfügung stellt. Aber auch der Nutzer einer Cloud-Lösung muss sich darüber im Klaren sein, ob er urheberrechtlich geschützte Werke in der Cloud abspeichern oder mittels der Cloud Dritten zum Download verfügbar machen darf.[173]

I. Urheberrechtlich geschützte Werke

109 In Art. 2–5 des Bundesgesetzes über das Urheberrecht und verwandte Schutzrechte (URG, SR 231.1) umschreibt der Gesetzgeber, welche Werke urheberrechtlich geschützt sind. Auch Daten können als urheberrechtlich geschützte Werke gelten. Dies hängt von drei Voraussetzungen ab: Es muss sich um (1) eine geistige Schöpfung der (2) Literatur und Kunst mit (3) individuellem Charakter handeln.[174]

110 In Art. 2 Abs. 3 URG stellt der Gesetzgeber klar, dass Computerprogramme zwar keine Werke sind, aber wie Werke geschützt werden. Voraussetzung ist aber auch hier, dass das Computerprogramm einen individuellen Charakter aufweist.[175]

II. Urheberrechtlich relevante Handlung

111 Ob nun ein urheberrechtlich relevanter Vorgang vollzogen wird, lässt sich am besten beurteilen, indem man zuerst den Schutzbereich des Urhebers abgrenzt. In Art. 10 URG listet der Gesetzgeber nicht abschliessend auf, welche Rechte ausschliesslich dem Urheber eines Werkes zustehen. Die Normen des URG sind technikneutral, d.h. die verschiedenen Formen der Nutzung können sich sowohl auf die analoge als auch auf die technische Verwendung eines Werkes bezie-

[173] PAUL/NIEMANN, Handbuch Cloud Computing, Teil 3, Rz. 3 ff.
[174] M.w.H. zu den Begriffsmerkmalen BARRELET/ EGLOFF, Art. 2 N 4 ff..
[175] BARRELET/EGLOFF, Art. 2 N 23 f.

hen.[176] Diese Normen können daher grundsätzlich auch auf Cloud-Computing-Dienstleistungen angewandt werden.[177] Relevant für Cloud-Sachverhalte sind insbesondere die zwei im Folgenden erläuterten Normen des URG.

1. Vervielfältigungsrecht (Art. 10 Abs. 2 lit. a URG)

112 Gem. Art. 10 Abs. 2 lit. a URG hat der Urheber das ausschliessliche Recht, sein Werk auf beliebigen Trägermaterialien festzuhalten und entsprechende Werkexemplare herzustellen. Somit stellen nicht nur der Download, sondern auch der Upload sowie das Speichern von Werken auf die Server eines IaaS-Cloud-Providers bzw. des Cloud-Nutzers Vervielfältigungshandlungen dar und bedürfen der Zustimmung des Urhebers.[178]

113 Gerade im Bereich der elektronischen Nutzung von Werken führte die gesetzliche Regelung des Art. 10 Abs. lit. a URG zu praxisfremden Ergebnissen: Es konnte nicht dem gesetzgeberischen Willen entsprechen, dass jeder technische Reproduktionsvorgang, welcher praktisch bei jeder Übermittlung eines Werkes via Internet erfolgt, als urheberrechtlich relevante Vervielfältigung gilt.[179] Dies führte dazu, dass solche Vorgänge, die sich ausserhalb des privaten Kreises gem. Art. 19 Abs. 1 lit. a URG abspielten, eigentlich unzulässig waren. Da aber keinerlei Interesse an einer Durchsetzung dieses Verbot bestand, blieb das Vervielfältigungsrecht für vorübergehende Kopien toter Buchstabe. Mit dem im Rahmen der Teilrevision von 2007 eingefügten Art. 24a URG hat der Gesetzgeber diesen Umstand korrigiert und die vorübergehende Vervielfältigung unter bestimmten Voraussetzungen vom Urheberrechtsschutz ausgenommen.[180]

2. Recht auf Zugänglichmachung (Art. 10 Abs. 2 lit. c URG)

114 Unter dem Recht auf Zugänglichmachung versteht man das ausschliessliche Recht des Urhebers „das Werk direkt oder mit irgendwelchen Mitteln (…) anderswo wahrnehmbar oder so zugänglich zu machen, dass Personen von Orten und Zeiten ihrer Wahl dazu Zugang haben“. Die herrschende Lehre versteht darunter auch die Bereitstellung eines Werkes in einer Datenbank oder auf einer Website

176 BARRELET/EGLOFF, Art. 10 N 7a.
177 ZANON BERANEK /DE LA CRUZ BÖHRINGER, S. 672.
178 ZANON BERANEK /DE LA CRUZ BÖHRINGER, S. 672; m.w.H. BÜHLER, S. 156 ff.
179 BÜHLER, S. 161.
180 BARRELET/EGLOFF, Art. 24 a N 1 ff.

und die Möglichkeit zum Abrufs des Werkes auf den eigenen Bildschirm.[181] Aber auch die Software, welche ein SaaS-Provider seinen Nutzern zur Verfügung stellt, ist urheberrechtlich geschützt. Deshalb bedarf es hierzu der Zustimmung des Urhebers, da es sich um eine urheberrechtlich relevante Zugänglichmachung durch den SaaS-Provider handelt.[182]

III. Schranken des Urheberrechts

115 Diese Ausschliesslichkeitsrechte des Urhebers schränkt das Gesetz aber an verschiedenen Stellen ein. Der Denkansatz liegt bei den gesetzlichen Schranken darin, dass nicht verboten sein soll, was nicht verboten werden kann. Gewisse Werknutzungen lassen sich faktisch gar nicht unterbinden, da der Rechteinhaber unter Umständen gar nicht die Möglichkeit hat, sie zu kontrollieren.[183] Insbesondere die zwei nachfolgenden Ausnahmen sind für Cloud-Computing-Sachverhalte relevant.

1. Geschäftlicher Eigengebrauch

116 Nutzt ein Unternehmen eine IaaS-Cloud-Lösung und lädt seine eigenen Daten sowie Daten, die Werke Dritter und somit urheberrechtlich geschützt sind, in die Cloud, so liegt ein Fall des geschäftlichen Eigengebrauchs gem. Art. 19 Abs. 1 lit. c URG vor. Dieser Bestimmung zufolge ist die Vervielfältigung von Werken in Betrieben (sowie in der öffentlichen Verwaltung und weiteren Einrichtungen) für die interne Information und Dokumentation erlaubt.[184] Macht sich also ein Unternehmen, das eine Cloud-Lösung nutzt, strafbar, wenn es urheberrechtlich geschützte Daten in das Intranet zur betriebsinternen Verbreitung lädt?

117 Obwohl das Gesetz dabei eigentlich nur das „Vervielfältigen“ als erlaubte Handlung erwähnt, wird auch die betriebsinterne Verbreitung der Vervielfältigungen als vom Gesetzeszweck erfasst verstanden.[185] Die h.L. geht entgegen dem Wortlaut von Art. 19 Abs. 1 lit. c URG davon aus, dass die Speicherung und Verbreitung in einem betriebsinternen Netzwerk einen zulässigen Fall des geschäftlichen Eigengebrauchs darstellt.[186]

---

181 M.w.H. BARRELET/EGLOFF, Art. 10 N 22.
182 NIEMANN/PAUL/SCHÄFER, Handbuch Cloud Computing, Rz. 20 ff.
183 HILTY, § 17 N 218.
184 Art. 19 Abs. 1 lit. c URG.
185 BARRELET/EGLOFF, Art. 19 N 16.
186 ZANON BERANEK /DE LA CRUZ BÖHRINGER, S. 675, sowie BGE 133 III 473 E. 3.1. Zur Frage nach der geschuldeten Vergütung muss aus Platzgründen auf die einschlägige Literatur verwiesen werden, z.B. BARRELET/EGLOFF, Art. 20, ZANON BERANEK /DE LA CRUZ BÖHRINGER, S. 678.

118 Nicht unter diesen gesetzlichen Ausnahmetatbestand fällt jedoch die im Rahmen einer SaaS-Dienstleistung genutzte Software. In Art. 19 Abs. 4 URG nimmt der Gesetzgeber die Nutzung von Software bewusst vom geschäftlichen Eigengebrauch aus. Dies bedeutet für die Praxis, dass der Anbieter, welcher seinen Kunden im Rahmen einer Cloud-Lösung Software verfügbar macht, sicherstellen muss, dass er über die nötigen Lizenzrechte verfügt.[187] Der Cloud-Nutzer seinerseits muss darauf vertrauen, dass sein Provider auch tatsächlich über das Recht verfügt, die Lizenz einzuräumen.[188] Im Übrigen kann aber der Cloud-Nutzer hinsichtlich der Anwendungssoftware wohl keine urheberrechtlich relevante Handlung vornehmen, da er (meistens) technisch nicht in der Lage dazu ist, die Software zu vervielfältigen.[189] Der Nutzer muss lediglich sicherstellen, dass er über die notwendigen Nutzungsrechte verfügt, falls er auf der Plattform seines Cloud-Providers eigene Software betreiben will.[190]

2. Vorübergehende Speicherung

119 Die zunehmende Digitalisierung erforderte eine weitere Ausnahmebestimmung im Bereich der vorübergehenden Vervielfältigung von Werken. Diese kommt dann zum Tragen, wenn Daten über das Internet übertragen werden und bei diesem Vorgang technisch bedingte Vervielfältigungen vorgenommen werden.[191] Würden solche Vervielfältigungen unter das Verbot von Art. 10 Abs. 2 lit. a URG fallen, so könnte sich der Rechtsinhaber dagegen wehren, womit die rechtskonforme Nutzung des Internets praktisch verunmöglicht würde.[192]

120 Der Gesetzgeber hat deshalb eine Ausnahmeregelung für Vervielfältigungen formuliert, welche nur flüchtiger (sog. ephemerer) Natur sind und danach wieder gelöscht werden und somit keine eigenständige wirtschaftliche Bedeutung haben.[193] Eine Vervielfältigung fällt unter den gesetzlichen Ausnahmetatbestand von Art. 24a URG, wenn die unter lit. a–d genannten Voraussetzungen kumulativ erfüllt sind.

---

187 SCHUSTER/REICHL, S. 40.
188 SURY, S. 35.
189 Siehe dazu auch SCHUSTER/REICHL, S. 40 f.
190 STRAUB, Cloud Verträge, S. 908.
191 So z.B. bei der Speicherung auf den Servern eines Access-Providers, wenn Werke über das Internet abgerufen werden, oder bei Speicherungen im Arbeitsspeichers eines Computers. Siehe dazu BBl 2006 3430.
192 HILTY, § 18 N 229. Vgl. auch Kap. F II 1.
193 BBl 2006 3430; HILTY, § 18 N 229, BARRELET/EGLOFF, Art. 24a N 3.

121 Für Cloud-Provider ist dieser Artikel von grundlegender Bedeutung, da der Gesetzgeber die Datenübertragung in einem Netz zwischen Dritten durch einen Vermittler privilegiert.[194] Die Verantwortlichkeit des Providers gegenüber den Inhabern von Urheberrechten wird durch diese Ausnahme geschützt.[195] Denn der Provider soll in der Grauzone der (Mit-)Haftung nicht als Gehilfe oder Mittäter unrechtmässiger Vervielfältigung zur Verantwortung gezogen werden können. Die h.M. geht deshalb davon aus, dass diese Schranke nur den Provider schützt, nicht aber die Nutzer, welche über seine Dienste Werke zugänglich machen oder abrufen.[196] Die Nutzer einer Cloud fallen von vornherein nicht unter diesen Tatbestand, da sie nicht als Dritte gelten und somit die gesetzlichen Voraussetzungen nicht erfüllen.[197]

194 REHBINDER/VIGANÒ, Art. 24a N 7.
195 BBl 2006 3431.
196 REHBINDER/VIGANÒ, Art. 24a N 7.
197 Art. 24a lit. b URG spricht nur von der Übertragung in einem Netz zwischen Dritten. Siehe dazu BARRELET/EGLOFF, Art. 24a N 6.

G. Vertragsbeendigung

122 Bevor ein Nutzer einen Vertrag mit einem Cloud-Provider eingeht, sollte er sich Gedanken über die Beendigung der Zusammenarbeit machen. Die Vertragsbeendigung beschlägt im Rahmen einer Cloud-Computing-Zusammenarbeit mehrere wichtige Aspekte. Für den Nutzer ist es grundlegend, dass er bei Nichterfüllung der vereinbarten Leistung schnellstmöglich einen Wechsel zu einem anderen Anbieter vornehmen kann. Gem. der Untersuchung von HON/MILLARD/WALDEN ist der sog. „Lock-in-Effekt" eine der grössten Sorgen von Cloud-Nutzern.[198] STRAUB empfiehlt sogar, Themen wie die Portierbarkeit von Applikationen oder die Migrationsmöglichkeiten von Daten bereits im Rahmen einer vorvertraglichen Due Diligence zu prüfen.[199] Im Folgenden soll erläutert werden, wieso und über welche Themen sich potentielle Cloud-Nutzer Gedanken machen sollten, bevor sie sich vertraglich binden.

I. Vertragsauflösungsgründe

123 Neben der ordentlichen Kündigung, für welche je nach Vertrag unterschiedliche Fristen gelten, können sowohl der Cloud-Anbieter als auch der Cloud-Nutzer das Vertragsverhältnis vorzeitig ausserordentlich kündigen. Die Gründe, welche eine ausserordentliche Kündigung ermöglichen, können vielfältig sein und sollten möglichst genau im Vertrag festgehalten werden.

1. Vertragsdauer und ordentliche Kündigung

124 Die Flexibilität von Cloud Computing wird oftmals als grosser Vorteil angepriesen, doch bei der Kündigung von Cloud-Verträgen hat sich Flexibilität noch nicht wirklich durchgesetzt. Gem. einer Studie von PricewaterhouseCoopers, welche 51 Cloud-Anbieter in Deutschland befragte, sah rund die Hälfte dieser Anbieter in ihren Standardverträgen eine ordentliche Kündigungsfrist von einem Monat vor. Ein Anbieter ermöglicht seinen Kunden sogar eine ordentliche Vertragsbeendigung innerhalb von 24 Stunden.[200]

---

198 HON/MILLARD/WALDEN, S. 115.
199 STRAUB, Cloud Verträge, S. 923.
200 Vgl. VEHLOW/ GOLKOWSKY, S. 30.

125 Die meisten Standardverträge von Cloud-Anbietern haben eine Laufzeit von einem Jahr bis zu drei Jahren und oftmals verlängern sich diese Verträge automatisch.[201] Falls ein Cloud-Vertrag eine solche Erneuerungsklausel enthält, sollte der Nutzer zumindest versuchen, die Dauer, in welcher der Vertrag noch ordentlich gekündigt werden kann, zu verlängern.[202] Gerade bei grösseren und aufwändigeren Projekten sehen Cloud-Anbieter oftmals eine Mindestvertragsdauer und damit zusammenhängend auch Strafzahlungen für vorzeitige Beendigung vor.[203] Wie lang die Laufzeit eines Cloud-Vertrags und die ordentliche Kündigungsfrist schlussendlich sind, bestimmt sich im Einzelfall sowohl nach Anbieter als auch nach Art der Leistung.

2. Ausserordentliche Vertragsauflösungsgründe

a) Verstösse gegen Service-Levels

126 Ein Cloud-Nutzer hat wohl meistens ein Interesse daran, den Vertrag mit seinem Cloud-Anbieter zu kündigen, wenn dieser die vereinbarten Leistungsstandards nicht einhält oder in einer anderen Art und Weise schwerwiegend den Vertrag verletzt.[204] Die ausserordentliche Kündigung sollte jedoch stets eine ultima ratio darstellen, da in diesem Fall auch der Cloud-Nutzer sich nach einem neuen Anbieter umsehen muss. Die Voraussetzungen der ausserordentlichen Kündigung sollten deshalb stets mit den übrigen Vertragsstrafen im Rahmen des SLA abgestimmt werden.[205]

b) Change of Control

127 Wird ein Cloud-Anbieter übernommen, so können die Kunden dieses Anbieters ein Interesse haben, den Vertrag zu kündigen. Gerade in Konstellationen, in denen der neue Eigentümer ein direkter oder indirekter Wettbewerber des Cloud-Nutzers ist, der somit faktisch Zugriff auf dessen Daten erlangen würde, kann ein ausserordentliches Kündigungsrecht angebracht sein.[206] Es ist ratsam, dass die Parteien

---

201 Z.B. werden rund 46% der Verträge von britischen Cloud-Anbietern automatisch verlängert (insbesondere bei Verträgen mit kleineren Kunden), siehe dazu: Cloud Industry Forum – Cloud UK.

202 Bspw. von 30 Tagen auf 60 Tage. Vgl. dazu HON/MILLARD/WALDEN, S. 120.

203 HON/MILLARD/WALDEN, S. 120.

204 Gem. STRAUB können z.B. Datenschutzverletzungen vertraglich als generell schwerwiegende Vertragsverletzungen definiert werden; STRAUB, Cloud Verträge, S. 923.

205 INTVEEN/HILBER/RABUS, Handbuch Cloud Computing, Teil 2, Rz. 366.

206 INTVEEN/HILBER/RABUS, Handbuch Cloud Computing, Teil 2, Rz. 369.

in jedem Fall vertraglich vereinbaren, sich gegenseitig unverzüglich über geänderte Mehrheitsverhältnisse zu informieren.

c) Zahlungsverzug

128 Befindet sich der Cloud-Nutzer mit der Bezahlung der Servicegebühr im Verzug, so sollte dies nicht direkt zur Vertragsauflösung führen. Da es für den Cloud-Nutzer unter Umständen schwerwiegende Folgen haben kann, wenn die Leistung vom Anbieter sehr kurzfristig beendet wird, könnte bspw. die Hinterlegung einer bestimmten Summe auf einem Sperrkonto vereinbart werden. Sollte es sodann zu einer Auseinandersetzung bzgl. der Höhe gewisser Vergütungen kommen, könnte die Zahlung vom Sperrkonto mit befreiender Wirkung geleistet werden.[207] Befindet sich der Cloud-Nutzer indes unberechtigterweise im Zahlungsverzug, wird dies regelmässig zur Beendigung des Vertrags berechtigen.

d) Insolvenz

129 Ist ein Provider in wirtschaftlichen Schwierigkeiten, so ist es für die Nutzer seiner Services wichtig, dies möglichst frühzeitig zu erkennen. Droht einer der beiden Vertragsparteien eine Insolvenz, wird dies ebenfalls zur Kündigung berechtigen. Im Falle einer Insolvenz sollte dies jedoch nicht direkt zur automatischen Vertragsauflösung führen, da insbesondere der Cloud-Nutzer allenfalls ein Interesse an der Weiternutzung seiner Daten hat. Als Beispiel sei die Gründung einer Auffanggesellschaft genannt.[208]

II. Lock-in-Effekt und Portabilität

130 Wie bereits erwähnt, ist gem. der Studie von HON/MILLARD/WALDEN eine der Hauptsorgen von Cloud-Nutzern die zu grosse Abhängigkeit von den Services des Cloud-Anbieters (sog. „Lock-in-Effekt“).[209] Wird die Zusammenarbeit, aus welchen Gründen auch immer, beendet, so hat der Nutzer ein Interesse daran, dass er seine Daten selber weiternutzen oder bei einem neuen Provider zur Nutzung unterbringen kann. Man spricht in diesem Zusammenhang auch von der Portierbarkeit der Daten. Um ihre eigene Handlungsfähigkeit zu bewahren, sollten Cloud-Nutzer im Vertrag folgende Möglichkeiten vorsehen.

---

[207] STRAUB, Cloud Verträge, S. 923.
[208] STRAUB, Cloud Verträge, S. 923.
[209] HON/MILLARD/WALDEN, S. 116.

131 Um die Daten, welche der Provider verarbeitet hat, weiter nutzen zu können, müssen diese in ein Format migriert werden, welches einfach zugänglich und lesbar ist und in andere Applikation importiert werden kann. Der Cloud-Nutzer sollte also sicherstellen, dass sein Provider verpflichtet ist, die Daten in einem standardisierten Format an ihn zu übergeben. Der Cloud-Provider ist jedoch nicht verpflichtet, auf Besonderheiten des neuen Systems Rücksicht zu nehmen; es genügt, wenn er die Daten in einem gängigen Format herausgibt.[210] Sicherstellen sollte der Cloud-Nutzer jedoch, dass sein Provider bestimmte Schnittstellen nutzt, welche die Datenmigration ebenfalls auf einfache Weise ermöglichen.[211]

132 Im Idealfall, d.h. wenn der Cloud-Anbieter die Daten im vertraglich vereinbarten Format und in der entsprechenden Qualität zum richtigen Zeitpunkt zur Verfügung stellt, kann der Cloud-Nutzer, allenfalls sogar mit seinem neuen Provider, die Migration so durchführen, dass ein nahtloser Umstieg möglich ist.

III. Vergütungsfragen

133 Ebenfalls bereits vorvertraglich sollte die allfällige Vergütung des Cloud-Providers für beendigungsunterstützende Massnahmen festgelegt werden. Wird der Cloud-Provider zur Beendigungsunterstützung verpflichtet (z.B. Erstellen eines Migrationskonzepts) oder ist der Nutzer auf die Zusammenarbeit zwischen seinem alten und seinem neuen Provider angewiesen, so wird der Provider diese Pflichten sicherlich nicht kostenlos erfüllen.[212]

134 Gem. der Studie von VEHLOW/GOLKOWSKY stellen rund 25% der befragten Cloud-Provider ihren Kunden auch nach der Beendigung des Vertrags noch Zusatzkosten in Rechnung. Rund 40% dieser Provider, bei welchen für die Kunden Zusatzkosten entstehen, rechtfertigen diese Kosten mit gesetzlichen Datenaufbewahrungspflichten.[213]

---

210 INTVEEN/HILBER/RABUS, Handbuch Cloud Computing, Teil 2, Rz. 389.

211 Schnittstellen (sog. Interfaces) sind definierte Übergänge zwischen Datenübertragungseinrichtungen, Hardwarekomponenten oder logischen Softwareeinheiten, siehe dazu: <http://www.itwissen.info/definition/lexikon/Schnittstelle-IF-interface.html> (zuletzt besucht am 30. Oktober 2014).

212 INTVEEN/HILBER/RABUS, Handbuch Cloud Computing, Teil 2, Rz. 395.

213 VEHLOW/GOLKOWSKY, S. 30.

H. Fazit und Checkliste

135 Die Idee des Cloud Computing mag zwar nicht neu sein, doch setzt man sich mit der Thematik näher auseinander, so stellt man fest, dass man sich in diversen Bereichen noch auf juristischem Neuland bewegt. Die Vorteile, welche eine Cloud mit sich bringt, liegen auf der Hand und deshalb kann allen zukünftigen Nutzern einer Cloud-Lösung geraten werden, einerseits mit einer gesunden Neugier an das Thema heranzugehen und andererseits stets die notwendige Sorgfalt walten zu lassen. Die nachfolgende Checkliste soll interessierten Kreisen helfen, die in dieser Arbeit aufgeworfenen Rechtsfragen übersichtlich vertraglich zu regeln. Sie soll einen Denkanstoss geben, erhebt aber keinesfalls Anspruch auf Vollständigkeit.[214] Sie kann ebenso wenig die individuelle Rechtsberatung durch einen Experten ersetzen, weshalb in Zweifelsfällen der Gang zum spezialisierten Anwalt empfohlen wird.

136 Ausgangspunkt eines Einstiegs in eine Cloud-Lösung sollte stets die Erstellung einer Cloud-Strategie sein:

- Welches Servicemodell passt am besten zur beabsichtigten Nutzung?
- Welche Daten sollen ausgelagert werden (bei höchst sensitiven Daten wird eine Auslagerung nicht empfohlen)?
- Ist der mögliche Provider zertifiziert, wo hat er seinen Sitz/Rechenzentren (Welche nationalen Rechtsvorschriften könnten anwendbar sein?), zieht er Sub-Provider bei?
- Wie werden die Daten in die Cloud migriert (welche Formate werden vom Provider unterstützt?)
- Können die technischen und organisatorischen Massnahmen gegen das unbefugte Bearbeiten der Daten (vgl. Art. 10a DSG) durch den Provider überprüft werden?
- Was sind die Folgen bei einer Vertragsbeendigung? (Besteht die Gefahr eines „lock-in“?)

137 Hat sich der Nutzer für einen Anbieter entschieden, so sollten die folgenden Punkte wenn möglich im Vertrag schriftlich festgehalten werden (dies gilt natürlich nur

[214] Eine übersichtliche und ausführliche Checkliste findet sich bei STRAUB, Cloud Computing – Checkliste, S. 3 ff; eine weitere Checkliste findet man im Leitfaden „Cloud Computing – Risk & Compliance“ von EuroCloud Swiss, online verfügbar unter <http://www.eurocloudswiss.ch/index.php/publikationen/leitfaden/79-cloud-computing-risk-compliance> (zuletzt besucht am 21. November 2014).

für jene Nutzer, die überhaupt die Möglichkeit haben, den Vertrag mit ihrem Cloud-Anbieter zu verhandeln):

- vertragliches Weisungsrecht (um in einem gewissen Mass auf den Provider Einfluss nehmen zu können)
- Festlegung von Service-Levels (Mindestverfügbarkeiten, Support-Levels, Definition von RTO und RPO)
- Urheberrecht: wer darf welche Daten bearbeiten bzw. über die Cloud weiterverbreiten?
- Nutzungsrechte bzgl. der verwendeten Software klären (nutzt der Anbieter Drittsoftware und stellt diese seinen Cloud-Nutzern zur Verfügung, so sind dazu entsprechende Lizenzen erforderlich)
- Der Cloud-Anbieter sollte sich den geltenden Geheimhaltungs- und Datenschutzvorschriften (angemessene technische und organisatorische Massnahmen gem. Art. 7 DSG) unterstellen.
- Sicherheitskonzept des Anbieters genau analysieren („Chinese Walls“, Trennung der Kundendaten, Verschlüsselungsmethoden oder auch die Risiko- und Katastrophenvorsorge)
- Haftungsfragen klären (insbesondere Haftungsausschlüsse und das Verhältnis zu allfälligen Konventionalstrafen).

138 Ein grosses Risiko für jeden Cloud-Nutzer sind die Folgen eines Konkurses des Cloud-Anbieters und für einen solchen Fall sollten zwingend:

- ein Retentionsrecht sowie
- ein Verwertungsverbot der Daten vertraglich ausgeschlossen werden und
- ein Verfahren für die Löschung der Daten festgelegt werden.

139 Auch mit entsprechenden Vorkehrungen besteht in diesem Fall für den Nutzer ein gewisses Risiko, da es der schweizerische Gesetzgeber bis anhin unterlassen hat, das gesetzliche Aussonderungsrecht im Konkurs auf Daten auszuweiten. Eine Erweiterung des gesetzlichen Aussonderungsrechts auf Daten würde grössere Rechtssicherheit schaffen und ein Tätigwerden des Gesetzgebers in dieser Richtung wäre für die betroffenen Parteien wünschenswert.

140 Natürlich bleibt beim Gang in die Cloud immer ein gewisses Restrisiko, doch wählt man einen rein schweizerischen Cloud-Anbieter aus, dessen Rechenzentren in der Schweiz stehen, so kann man eher ausschliessen, dass am Horizont Gewitterwolken aufziehen.