EuroCloud AUSTRIA

EuroCloud Österreich

Leitfaden

Cloud Computing

Herausforderungen, Qualitätssicherung, Standards und Zertifizierung

ÖSTERREICH

08

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































Impressum

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

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

Copyright: EuroCloud.Austria

Inhaltsverzeichnis

Impressum		2
1.	Vorwort	4
2.	Einleitung	5
3.	Cloud Computing – Die größten Herausforderungen	5
4.	Der Empfehlungskatalog „Cloud-Verträge“	14
5.	Cloud-Standards und Zertifizierungen im Überblick	16
6.	Cloud-Standards in der EU	21
7.	EuroCloud Star Audit	22
8.	Glossar Cloud Computing	26
9.	Rechtlicher Hinweis	32
10.	Autoren	34



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

1 Vorwort

Liebe Leserinnen und Leser!

Die Grundidee des Cloud Computings hat bereits einen älteren Ursprung, ist in Ihrer Ausprägung und den damit verbundenen Herausforderungen und Möglichkeiten aber noch sehr jung.

Bisher traf ein vielfältiges Angebot seitens der Bieter auf die vorsichtige Zurückhaltung seitens der Kunden. Jedoch wird insbesondere bei größeren Unternehmen der Wunsch, sich mit neuen Optionen und den damit verbundenen Fragestellungen zu beschäftigen, deutlich spürbar.

EuroCloud hat sich mit dem gesamten Veranstaltungs- und Leitfadenprogramm darauf verschrieben, eine tiefgehende und umfangreiche Informationsplattform zu liefern und es somit Kunden und Anbietern leichter zu machen, sich auf die Themen zu einigen, die abgestimmt werden müssen.

Im aktuellen Leitfaden soll ein Bogen gespannt werden, der von einer überblicksartigen Beschreibung der Herausforderungen zu möglichen Lösungswegen, empfohlenen vertraglichen Komponenten, Standards, Qualitätssicherungsmöglichkeiten und Zertifizierungen führt.

Herzlichen Dank an alle Autoren (siehe Kap. 10. Autoren), die sich in diesem Leitfaden engagiert haben, insbesondere Herrn Mag. Árpád Geréd, der die umfänglichste inhaltliche Verantwortung trug.

Wien, Juni 2013



Dr. Tobias Höllwarth
Vorstand EuroCloud.Austria

2. Einleitung

Obwohl Cloud Computing im Allgemeinen als etwas Neues wahrgenommen wird, stellt es aus technischer Sicht nichts grundsätzlich Neues dar. Neu ist lediglich, dass beispielsweise Software, Datenspeicher oder auch Rechenkapazität statt wie bisher lokal und statisch nunmehr über ein Netzwerk und dynamisch an den Bedarf der Nutzer angepasst als Dienste zur Verfügung gestellt werden. Neu ist auch das Ausmaß, in dem die Bereitstellung dieser Dienste erfolgt. Anbieter zielen nicht mehr auf die Bereitstellung möglichst individualisierter Lösungen ab, sondern auf die massentaugliche Standardisierung der Angebote. Aus diesem Grund wird Cloud Computing vollkommen zu Recht auch als die Industrialisierung der IT angesehen.

Doch wie schon die Industrialisierung in der analogen Welt schafft auch die Industrialisierung in der IT neue Herausforderungen, die man nur zum Teil mit bewährten Methoden aus vorindustrieller Zeit meistern kann. Ehemalige Randthemen wie beispielsweise Interoperabilität, Portabilität oder auch Datenschutz sind nunmehr wesentlich und, zumindest teilweise, durch mediale Verbreitung in den Fokus der Öffentlichkeit gerückt. Zeitgleich verursacht die Industrialisierung, heute wie damals, Unsicherheit. Allen voran in den Bereichen Datensicherheit und Datenschutz wird Cloud Computing von vielen als unsicher oder zumindest problematisch wahrgenommen. Dadurch steigt aber das Bedürfnis nach technischen wie auch rechtlichen Standards im Bereich Cloud Computing, durch welche man sich die Lösung zumindest einiger der neuen Herausforderungen verspricht.

Im internationalen Umfeld existieren bereits, vor allem aufgrund entsprechender Initiativen bei der International Organization for Standardization (ISO), Standards für einzelne Aspekte des Cloud Computings. [1]

In Europa hat die EuroCloud aufgrund der Nachfrage durch ihre Mitglieder bereits früh in Deutschland mit der Arbeit an Auditierungsstandards begonnen, die speziell auf Software-as-a-Service-Lösungen abgestimmt waren. Diese Standards wurden erstmals im Jänner 2011 als „Euro-Cloud Star Audit“ vorgestellt. Doch auch die Europäische Union hat dieses Bedürfnis bereits erkannt, weshalb die Europäische Kommission im Herbst 2012 das European Telecommunications Standards Institute (ETSI), das sich unter anderem auch für den GSM-Standard verantwortlich zeigte, mit der Koordinierung der Erstellung von Standards für Cloud Computing beauftragte.[2]

Vor diesem Hintergrund hat sich dieser Leitfaden die Aufgabe gesetzt, einen Überblick über die Herausforderungen sowie Lösungsansätze im Bereich Cloud Computing zu bieten und speziell auf Cloud Computing zugeschnittene Empfehlungen hinsichtlich Vertrag und Qualitätssicherung darzustellen.

Abgerundet wird der Leitfaden durch ein übersichtliches Cloud-Glossar und eine Checkliste für Cloud-Vertragselemente.

---

1 Einen guten Überblick bietet die Seite http://cloud-standards.org

2 Siehe dazu auch die Pressemeldung der ETSI:
http://www.etsi.org/news-events/news/600-2012-11-cloud-standards-coordination-launch

3 Cloud Computing – Die größten Herausforderungen

3.1 Überblick

Bevor man sich die Frage stellt, zu welchen Themenbereichen im Rahmen von Cloud Computing Standards oder zumindest Empfehlungen erforderlich sind, muss man zuerst analysieren, welche Fragen sich im Zusammenhang mit Cloud Computing überhaupt stellen. Der nächste Schritt ist, festzustellen, welche dieser Fragen sich nicht oder nur unzureichend mit bestehenden Regelungen beantworten lassen oder wo trotz bestehender Regelungen eigene Standards oder Empfehlungen im Bereich Cloud Computing sinnvoll wären.

Die EuroCloud.Austria hat sich im Rahmen mehrerer, teils multinationaler Leitfäden zu den verschiedensten Themen intensiv mit den Fragen auseinandergesetzt, die sich für Nutzer und Anbieter im Zusammenhang mit Cloud-Diensten stellen. Die Autoren haben dabei auch stets versucht, sofern dies möglich war, praxisnahe Lösungen oder zumindest Empfehlungen anzubieten.

Im Folgenden werden die wichtigsten Ergebnisse der Leitfäden kurz zusammengefasst, einerseits als Überblick über die Leitfäden selbst, andererseits aber auch als kurze Einführung in die Komplexität der Themen und Herausforderungen, welche durch die Industrialisierung der IT entstehen.

3.2 Lizenzen[3]

Aus Sicht des Urheberrechts stellen sich beim Cloud Computing verschiedenste Fragen. Kern dieser Fragestellungen ist, welche Nutzungsrechte benötigt werden, um den Cloud-Dienst nutzen oder anbieten zu können, ohne dadurch Urheberrechte Dritter zu verletzen.
Dazu ist zunächst zu klären, welches Recht anwendbar ist, zumal es in der Praxis eine seltene Ausnahme ist, dass alle Beteiligten (also Anbieter, Nutzer, aber auch sonstige Beteiligte, deren Rechte durch die Cloud-Dienste berührt sein können, wie etwa Software-Rechteinhaber) im selben Staat ihren Sitz haben. Vom Recht hängt es wiederum ab, ob und welche Zustimmungen des Rechteinhabers überhaupt erforderlich sind.

Die naheliegendste Lösung wäre eine vertragliche Rechtswahlklausel. Allerdings hat im Urheberrecht eine derartige Rechtswahl nur sehr eingeschränkte Wirkung. Vielmehr gelangt in diesem Zusammenhang das in internationalen Verträgen festgelegte Schutzlandprinzip zur Anwendung. Dieses bedeutet, dass das Recht jenes Staates zur Anwendung kommt, für den der Schutz beansprucht werden soll, somit des Staates, in dem das urheberrechtlich geschützte Werk benützt oder verletzt wurde.

Auch wenn im Internet und somit auch beim Cloud Computing Dienste an sich weltweit nutzbar sind und damit auch theoretisch urheberrechtlich geschützte Werke über einen Cloud-Dienst weltweit benützt oder verletzt werden können, so vertritt zumindest die Rechtsprechung in Österreich die Auffassung, dass neben der reinen Abrufbarkeit eines internetbasierten Dienstes weitere Kriterien hinzutreten müssen, um einen hinreichenden Inlandsbezug herzustellen und damit eine Anwendbarkeit des inländischen Rechts zu bewirken. Somit besteht, zumindest nach dieser Rechtsansicht, für Anbieter und Nutzer beispielsweise die Möglichkeit, über technische Maßnahmen oder vertragliche Bestimmungen die Cloud-Dienste territorial abzugrenzen oder sie zu fokussieren.

---

[3] Näheres zu diesem Thema findet sich im EuroCloud.Austria-Leitfaden Nr. 3 „Cloud Services – Lizenzen im Cloudvertrag“, zu beziehen über www.eurocloud.at

Im Zweifel gilt auch hier, dass allein eine Einigung mit dem Rechteinhaber jegliche Zweifel beseitigen kann, wobei ein von einem großen Cloud-Anbieter mit entsprechender Marktpräsenz initiierter Dialog im Allgemeinen erfolgversprechender ist als ein von einem kleinen Anbieter eingeleiteter. Unbefriedigend ist diese Lösung in jenen Fällen, in denen der Rechteinhaber nicht gewillt ist, für die Verwendung im Cloud-Umfeld wirtschaftlich sinnvolle Konditionen anzubieten. Wiewohl es auch dann noch mitunter rechtliche Möglichkeiten gäbe, ein für Cloud-Anbieter und Nutzer verträglicheres Ergebnis zu finden, wäre es wohl einzig über Standards möglich, rasch eine wirtschaftliche Lösung zu finden.

Open Source Software, die besonders im Serverbereich stark verbreitet ist, stellt einen Sonderfall dar. Sie beruht auf dem Grundprinzip, dass die Software beliebig verbreitet, vervielfältigt und genutzt werden kann. Ebenso darf sie beliebig verändert und weitergegeben werden. Open Source Software ist jedoch keine lizenzfreie Software. Die dargelegten Grundprinzipien werden vielmehr verwirklicht, indem sie als Nutzungsbeschränkungen Bestandteil der Lizenzvereinbarung und damit auch gerichtlich durchsetzbar sind. Verstößt der Nutzer gegen die in der Open-Source-Lizenzvereinbarung festgelegten Bedingungen, so stellt dies ebenso wie bei klassischen, proprietären Softwarelizenzvereinbarungen eine Rechteverletzung dar.

Im Bereich der Open Source Software existieren verschiedene Lizenzbedingungen, welche sich in ihren rechtlichen Auswirkungen voneinander unterscheiden, sodass allgemeingültige rechtliche Aussagen zu Open Source Software nicht möglich sind.

Für den Bereich des Cloud Computings sind aber vor allem die Unterschiede im Bereich des Copyleft-Prinzips von Relevanz. Dieses besagt, dass die Software vom Nutzer zwar verändert werden darf, die Verbreitung der geänderten Software jedoch nur unter denselben Lizenzbedingungen zulässig ist wie die ursprüngliche Software. Im Falle der Verbreitung besteht auch die Pflicht, den (geänderten) Quellcode der Software offenzulegen. Manche Open-Source-Lizenzen, wie etwa die BSD-Lizenz, enthalten kein Copyleft-Prinzip. Wo es jedoch enthalten ist und an eine Verbreitungshandlung anknüpft, bleibt es bei Cloud-Diensten wie etwa SaaS oder PaaS (Näheres zu diesen Begriffen siehe Glossar) wirkungslos, da es an einer Verbreitungshandlung fehlt. Dies berührt aber nicht die Gültigkeit der Lizenz an sich, sodass auch solche Software im Rahmen von Cloud-Diensten genutzt werden kann.

3.3 Datenschutz und Compliance[4]

Eingangs muss betont werden, dass das Datenschutzgesetz nicht auf alle Daten Anwendung findet, sondern nur auf sogenannte personenbezogene Daten. Das sind im Allgemeinen solche, über welche die Identität einer natürlichen (in Österreich auch einer juristischen) Person bestimmt oder bestimmbar ist. Doch auch wenn das Gesetz selbst nicht auf alle Arten von Daten anwendbar ist, die im Rahmen von Cloud-Diensten verarbeitet werden, so stellen sich die nachfolgend dargestellten Probleme auch für sonstige, nicht personenbezogene, jedoch für den Cloud-Nutzer relevante Daten.

---

[4] Näheres zu diesem Thema findet sich im EuroCloud.Austria-Leitfaden Nr. 1 „Cloud Computing – Recht, Datenschutz & Compliance“, zu beziehen über www.eurocloud.at

Der Nutzer von Cloud-Diensten verfügt regelmäßig nicht mehr vollständig über die bei Erbringung dieser Dienste verarbeiteten (personenbezogenen) Daten. Dennoch bleibt er für gewöhnlich auch bei der Nutzung von Cloud Computing im Rahmen der anwendbaren Gesetze für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er darf also auch mittels des Cloud-Dienstes nur solche datenschutzrelevanten Verarbeitungen vornehmen lassen, die er auch selbst vornehmen dürfte.

Dabei ist der Abschluss eines Vertrags über die Dienstleistung als datenschutzrechtliche Grundlage auch dann erforderlich, wenn der Einsatz des Cloud-Dienstes nur getestet werden soll. Um den Aufwand für den Abschluss eines solchen Vertrags zu vermeiden, bietet es sich an, Testzugänge ohne Echtdaten oder zumindest ohne personenbezogene Daten zu nutzen. In Österreich kann der Nutzer zudem auf von der Datenschutzkommission (DSK) herausgegebene Musterverträge und Mustervertragsklauseln zurückgreifen.

Grundsätzlich hat der Nutzer (datenschutzrechtlich: Auftraggeber) sich zudem vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Cloud-Anbieter (datenschutzrechtlich: Auftragnehmer) getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, welche eine ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten müssen. Diese Kontrollpflicht ist auch innerhalb der Europäischen Union in den einzelnen Mitgliedstaaten in der Intensität unterschiedlich ausgeprägt.

In der Praxis bedeutet dies, dass der Nutzer den Anbieter in erster Linie sorgfältig auswählen und sich schon vor Vertragsabschluss von der Eignung des Anbieters ein Bild machen muss, um seiner gesetzlichen Pflicht Rechnung zu tragen. In der praktischen Durchführung wird diese Auswahl für den Nutzer erleichtert, wenn der Anbieter Standards eines Gütesiegels oder einer Auditierung erfüllt oder zumindest über eine entsprechende Reputation verfügt.

Eine derartige Kontrolle durch den Nutzer genügt dem Gesetz zumeist ohne weiteres jedoch nur bei einem Cloud-Dienstleister (oder sonstigem Aufragnehmer), der seinen Sitz in der EU oder dem Europäischen Wirtschaftsraum (EWR) hat. Bei einer Beauftragung von Anbietern mit Sitz in einem Drittstaat – also außerhalb der EU und/oder des EWR – oder einer tatsächlichen Datenverarbeitung in einem solchen Drittstaat müssen zusätzliche Anforderungen erfüllt werden, damit eine Übertragung von Daten in einen solchen Drittstaat überhaupt erst erfolgen darf. Dafür empfiehlt es sich, in einem solchen Fall auf den von der Europäischen Union abgesegneten Standardvertrag zur „Auftragsdatenverarbeitung“ zurückzugreifen (sog. „Standard Contract Clauses“ für „Data Processing“). Darüber hinaus bedarf die Überlassung von Daten an einen Empfänger in einem Drittstaat oder zur Verarbeitung in einem Drittstaat im Regelfall einer Genehmigung, in Österreich etwa durch die DSK. Zwar befreit der Abschluss des vorgenannten Standardvertrags nicht vom Erfordernis der Genehmigung des Datentransfers durch die DSK, doch kann er diese in der Praxis durchaus erleichtern.

Ein weiteres heißes Thema im Bereich Datenschutz ist die Heranziehung von Subdienstleistern. Das Gesetz fordert für gewöhnlich, im Dienstleistervertrag die Beiziehung weiterer Dienstleister („Subdienstleister“) zu regeln, wobei als Regel die Heranziehung von Subdienstleistern nur mit Bewilligung des Auftraggebers, also des Nutzers, möglich ist und deshalb der Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen ist, dass er dies allenfalls untersagen kann. Das Gesetz geht dabei oft bereits dann von einem Subdienstleister aus, wenn der Zugriff des Subunternehmers (etwa über einen Remote-Zugang) auf die für den Nutzer verarbeiteten Daten nicht ausgeschlossen werden kann. Der bloße Zugriff genügt dabei; eine Verarbeitung der Daten durch den Subdienstleister ist nicht erforderlich. Ebenso wenig ist die Übermittlung an den Subdienstleister nötig.

Als praxistaugliche Regelung kann sich in diesem Zusammenhang eine Gestaltung erweisen, die zwischen Kategorien von Subunternehmern differenziert. Damit können bestimmte Kategorien unter einen Zustimmungsvorbehalt des Nutzers gestellt werden, während in anderen Kategorien die Einschaltung von Subunternehmern ohne gesonderte Einwilligung zulässig ist, sofern bestimmte definierte Anforderungen eingehalten sind. In jedem Fall sollte der Auftraggeber über die Subunternehmer und deren Tätigkeit informiert werden. Manche größere Anbieter umgehen diese Problematik jedoch so einfach wie radikal, indem sie zusichern, die Dienste ausschließlich selbst zu erbringen und keine Subdienstleister hinzuzuziehen.

Einen der wesentlichsten Punkte in Bezug auf Daten bei Cloud-Diensten stellt die Rückgabe selbiger bei Vertragsbeendigung dar. Zumindest für personenbezogene Daten muss die Rückgabe oft aufgrund gesetzlicher Vorgabe jedenfalls vertraglich geregelt werden. Das Gesetz verlangt, dass nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber, also dem Cloud-Nutzer, zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten sind.

Die drei Grundszenarien sind daher die (in der Praxis am weitesten verbreitete) Rückübertragung der Daten plus Löschung in den Systemen des Anbieters oder die weitere Aufbewahrung der Daten oder die bloße Löschung der Daten in den Systemen des Anbieters. Auch wenn der Dienstleistervertrag beendet ist, sollte die datenschutzrechtliche Dienstleistung aber so ausgestaltet sein, dass die Pflichten aus dem Dienstleistervertrag bis zur eindeutigen Bestätigung der Löschung durch den Anbieter fortgelten.
Der Nutzer sollte sich bereits bei Vertragsschluss entscheiden, welche technischen Anforderungen an die Rückgabe – Übertragungsweg (z. B. per SFTP) und in welchem Dateiformat oder ob Erläuterungen zur Dateistruktur erforderlich werden – zu stellen sind, damit er zu einem anderen Anbieter wechseln oder die weitere Verarbeitung wieder selbst wahrnehmen kann. Dies kann höchstens dann entfallen, wenn die technischen Aspekte bereits durch die Art und Weise der Speicherung bzw. Verarbeitung eindeutig geklärt sind.

Für den Anbieter ist zudem entscheidend, wann er die Daten löschen kann, falls der Nutzer die Vergütung nicht (mehr) zahlt oder insolvent wird. Auch dies sollte bereits im Vertrag geregelt werden.

In jedem Fall muss vor allem der Nutzer bedenken, dass gesetzliche Regelungen zumeist nicht alle für ihn relevanten Daten, insbesondere Geschäftsdaten, abdecken. Daher ist eine vertragliche Definition der Rechte und Pflichten bezüglich aller Daten, nicht nur personenbezogener, sinnvoll und empfehlenswert.

3.4 Öffentliche Auftragsvergabe[5]

Cloud Computing ist für öffentliche Auftraggeber aufgrund der Vielfalt der möglichen Einsatzgebiete eine ebenso attraktive und valide Option wie für private Unternehmen. Wie bei anderen IT-Outsourcing-Projekten stellt aber auch die Ausschreibung und Vergabe von Cloud-Computing-Leistungen eine Herausforderung für den öffentlichen Auftraggeber dar, da sich zur Komplexität der auszuschreibenden Leistungen die Komplexität der einzuhaltenden vergaberechtlichen Normen gesellt.

---

[5] Näheres zu diesem Thema findet sich im EuroCloud.Austria-Leitfaden Nr. 2 „Cloud Services – Öffentliche Auftragsvergabe“, zu beziehen über www.eurocloud.at

Grundsätzlich sind Cloud-Computing-Leistungen auszuschreiben, da sie in den meisten Fällen als Dienstleistungen unter den Begriff „Datenverarbeitung und verbundene Tätigkeiten" fallen und damit, etwa in Österreich, prioritäre Dienstleistungen im Sinne des Gesetzes darstellen. Damit fällt die Vergabe dieser Leistungen in den gesetzlichen Vollanwendungsbereich, was bedeutet, dass öffentliche Auftraggeber bei ihrer Vergabe alle einschlägigen vergaberechtlichen Regelungen zu beachten haben.

Nur in bestimmten Fällen können Cloud-Computing-Leistungen als Lieferleistungen zu qualifizieren sein, und zwar vor allem dann, wenn sie als Miete von Cloud-Diensten ausgestaltet sind.

In Einzelfällen kann die Vergabe von Cloud-Computing-Leistungen aber unter eine gesetzliche Ausnahmebestimmung fallen, was zur Folge hat, dass bestimmte Regelungen nicht beachtet werden müssen. Dies kann z. B. bei geheimen oder sicherheitskritischen Beschaffungsvorgängen oder Inhouse-Vergaben der Fall sein. Nach dem Gesetz ausschreibungsfrei kann eine Beschaffung weiters dann sein, wenn der öffentliche Auftraggeber bei einer zentralen Beschaffungsstelle einkauft – diese kann sich auch im Ausland befinden –, sofern die zentrale Beschaffungsstelle selbst in Übereinstimmung mit den EU-Vergaberichtlinien ausschreibt. Generell ist zu diesen Ausnahmebestimmungen anzumerken, dass sie eng zu interpretieren sind und die Beweislast für ihr Vorliegen beim öffentlichen Auftraggeber liegt.

Wesentlich für ein erfolgreiches Ausschreibungsprojekt ist jedenfalls die Kenntnis des Marktes. Ohne Kenntnis der Möglichkeiten und Grenzen der IT-Dienstleister geht eine Ausschreibung am Markt vorbei und bietet keine Grundlage für gute Angebote. In der Praxis lässt sich dieses Wissen, sofern es nicht bereits beim öffentlichen Auftraggeber vorhanden ist, durch die Hinzuziehung externer Berater beschaffen.

Für die Vergabe komplexer Cloud-Computing-Leistungen bietet sich, beispielsweise in der österreichischen Praxis, an erster Stelle das Verhandlungsverfahren mit Bekanntmachung an. Dieses Verfahren ist insbesondere immer dann zulässig, wenn es die Komplexität der zu vergebenden Leistungen nicht erlaubt, das Leistungsbild vorab so abschließend zu definieren, dass ein offenes oder nicht offenes Vergabeverfahren durchgeführt werden kann.

Steht der konkrete Bedarf des öffentlichen Auftraggebers an Cloud-Computing-Leistungen noch nicht fest, kommt der Abschluss von Rahmenvereinbarungen in Betracht. Das sind Vereinbarungen ohne Abnahmeverpflichtung für den Auftraggeber, die grundsätzlich auf maximal drei Jahre abgeschlossen werden dürfen. Der Vertragspartner ist dennoch durch Ausschreibung zu ermitteln.

3.5 Vertragsrecht in der Praxis[6]

All die oben beschriebenen Rechtsbereiche müssen bei der Erstellung von Verträgen zwischen Cloud-Anbietern und Kunden bzw. im Rahmen der Vertragsanbahnung berücksichtigt werden. Darüber hinaus stellen Verträge im Bereich Cloud Computing eine besondere Herausforderung dar, da Bedürfnisse der Vertragsparteien und Szenarien antizipiert werden müssen, welche erst im Laufe der Vertragsabwicklung auftreten würden (wenn überhaupt), allerdings bereits zuvor im Vertrag geregelt werden sollten.

---

6 Näheres zu diesem Thema findet sich im EuroCloud.Austria-Leitfaden Nr. 6 „Cloud Computing – Der gelebte Vertrag – Leistungsstörungen und Vertragshaftung in der Vertragsabwicklung", zu beziehen über www.eurocloud.at

Dies verlangt neben dem juristischen auch ein technisches Verständnis der Materie, das von Juristen ansonsten allenfalls im Zusammenhang mit kurzfristigen Softwareverträgen, kaum jedoch bei längerfristigen Dienstleistungsverträgen abverlangt wird. Gerade diese Längerfristigkeit gilt es jedoch bei Cloud-Verträgen zu berücksichtigen.
So sollte beispielsweise klar geregelt sein, ob die Hinzuziehung von Subdienstleistern zulässig ist und falls ja, auf welche Art und in welchem Ausmaß. Dies ist umso wichtiger, je kritischer die ausgelagerten Dienste oder Daten für den Kunden (und sei es auch nur nach dessen subjektiver Wahrnehmung) sind. Eine entsprechend detaillierte Regelung gewährt dem Anbieter die notwendige Flexibilität und schafft zugleich für beide Parteien Rechtssicherheit.

Auch das Recht und die Modalitäten der Kontrolle der Vertragseinhaltung sollten definiert werden. Derartige Regelungen sind bei sonstigen IT-Verträgen im Allgemeinen unüblich, insbesondere im Zusammenhang mit der Auslagerung von Daten kann sich der Kunde aber bisweilen mit einer, etwa von Gesetz oder Rechtsprechung herausgebildeten, Pflicht zur Durchführung von Kontrollmaßnahmen konfrontiert sehen.

Ein weiterer Aspekt von Verträgen im Bereich Cloud Computing, der sich in der Praxis als wesentlich erweisen kann, ist die Definition von Informations- und Meldepflichten. Insbesondere dem Kunden ermöglicht oftmals allein die detaillierte Festlegung derartiger Pflichten die Einhaltung eigener gesetzlicher oder vertraglicher Obliegenheiten. Das Kontrollrecht allein bietet keinen ausreichenden Ersatz, da der Kunde die Dienste des Anbieters weder ständig (oder auch nur kurzfristig) regelmäßig überwachen kann noch will. Daher ist es essenziell, dem Anbieter bereits bei der Vertragserrichtung die eigenen Anforderungen im Hinblick auf Informationen und Meldungen zu kommunizieren und mit einer entsprechenden Verpflichtung zu festigen.

Sollte dennoch ein Streitfall eintreten, so ist es von unschätzbarem Vorteil, wenn bereits der Vertrag einem Rahmen vorgibt, innerhalb dessen die Vertragsparteien Konflikte austragen können, der aber gleichzeitig die fortlaufende Erbringung der Dienste bestmöglich gewährleistet. Für den Kunden ist es nämlich essenziell, dass die von ihm genutzten Dienste und Daten zumindest so lange verfügbar sind, bis er auf einen alternativen Anbieter ausweichen kann. Gleichzeitig ist der Anbieter daran interessiert, seine Dienste nur gegen entsprechende Vergütung zu erbringen. Je nach Art und Ausgestaltung der maßgeblichen Cloud-Dienste kommen verschiedene Absicherungsmechanismen infrage, beispielsweise Treuhänderregelungen.

Aus der praxisnahen Auseinandersetzung mit den zuvor beschriebenen rechtlichen Themen entstand die Erkenntnis, dass sich viele potenzielle rechtliche wie auch tatsächliche Probleme und Unsicherheiten im Bereich Cloud Computing vermeiden ließen, wenn der Nutzer, der derartige Verträge nicht regelmäßig abschließt, bereits im Zuge der Vertragsanbahnung sich und dem Anbieter die erforderlichen Fragen stellen würde. Daraus entstand die Idee, potenziellen Cloud-Nutzern einen Empfehlungskatalog zur Verfügung zu stellen, welcher die wesentlichsten Fragen auflistet. Umgesetzt wurde diese Idee schließlich in Form des Empfehlungskatalogs „Cloud-Verträge“ (siehe Punkt 4).

Neben diesen Themen, die unmittelbar für die zwischen Cloud-Anbieter und Nutzer abgeschlossenen Verträge relevant sind, entstanden auf Initiative der EuroCloud.Austria weitere Leitfäden zu anderen, auch nicht-juristischen Bereichen, die Aspekte beleuchten, die über den bloßen Vertrag hinaus bedeutsam sind.

3.6 Steuerrecht[7]

Wie auch in allen anderen Bereichen seiner Geschäftstätigkeit sollte sich ein Unternehmer beim Anbieten bzw. der Nutzung von Cloud Computing mit unternehmens- (handels-) und steuerrechtlichen Themen auseinandersetzen. Denn die Nichtbeachtung der entsprechenden Vorschriften kann schnell zu erheblichen (auch finanziellen) Risiken führen.

Prinzipiell sind zwei Bereiche des Steuerrechts vordergründig für den Unternehmer wichtig und abklärungsbedürftig. Einerseits der Bereich des Ertragsteuerrechts und andererseits der Bereich des Umsatzsteuerrechts.
Ertragsteuerrecht:

Nachdem sich Cloud Computing in seiner finalen Ausprägung über mehrere Länder erstrecken kann, gilt es hier zu klären, wie die Besteuerung im Hinblick auf die potentielle Vielzahl an beteiligten Staaten geregelt ist. Grundsätzlich gilt in Österreich für natürlichen oder juristischen Personen mit Wohnsitz, gewöhnlichen Aufenthalt oder Sitz im Inland das sogenannte Welteinkommensprinzip. Das bedeutet, dass diese Steuerpflichtigen in Österreich mit ihrem gesamten Welteinkommen der Besteuerung unterliegen.

Die internationalen Steuerrechtsnormen, die die Zuteilung der Besteuerungsrechte an die einzelnen Staaten regeln, finden sich üblicher Weise in von Österreich mit anderen Staaten (jedoch nicht mit allen Staaten) abgeschlossenen Staatsverträgen, sogenannten Doppelbesteuerungsabkommen (DBA). Vielen dieser DBA liegt das sogenannte OECD-Musterabkommen (OECD-MA) zugrunde, welches (wie auch das österreichische Steuerrecht) das Besteuerungsrecht primär an das Vorhandensein einer ertragsteuerlichen Betriebsstätte knüpft.

Ein oder mehrere Server oder ein Rechenzentrum begründet allerdings nach dem OECD-MA nur dann eine Betriebsstätte, wenn der Unternehmer über eine solche (nicht nur vorübergehend) die Verfügungsmacht hat. Dies ist sicher beim Anbieter der Fall, im Bereich des Cloud Computing jedoch kaum beim Nutzer, der typischer Weise nur über die Daten auf dem Server verfügen kann, nicht aber über das Gerät selbst. Im Falle des Anbieters ist es z.B. hingegen nicht relevant, dass die Server de facto von anderen Unternehmen genutzt werden, dienen sie doch letztendlich dem unternehmerischen Zweck des Anbieters, nämlich der Bereitstellung von Cloud-Diensten.

Umsatzsteuerrecht:

Auch hier ist primär zu untersuchen, ob eine Betriebsstätte im umsatzsteuerlichem Sinne vorliegt (z.B. auf Seiten des Anbieters), da nur eine solche geeignet ist einen Ort, von dem aus der Unternehmer sein Unternehmen betreibt, neu zu definieren. Diesfalls würde der Ort, von dem aus der Unternehmer sein Unternehmen betreibt, für jene Leistungen, die an bzw. von der umsatzsteuerlichen Betriebsstätte erbracht werden, eben an den Ort der umsatzsteuerlichen Betriebsstätte wechseln.

---

7 Näheres zu diesem Thema findet sich im EuroCloud.Austria-Leitfaden Nr. 5 „Cloud Computing – Steuerliche Aspekte in der DACH-Region“, zu beziehen über www.eurocloud.at

Die Anforderungen an die, im Unionsrecht als feste Niederlassung bezeichnete umsatzsteuerliche Betriebsstätte, sind jedoch inhaltlich wesentlich enger gefasst, als jene, an die ertragsteuerliche Betriebsstätte nach dem OECD-MA. Prinzipiell kommt die Annahme einer festen Niederlassung nur dann in Frage, wenn eine Einrichtung für eine gewerbliche Betätigung ein ständiges Zusammenwirken von persönlichen und Sachmitteln voraussetzt, die für die Erbringung der betreffenden Cloud-Dienstleistungen erforderlich sind.

3.7 Prozesse und Organisation[8]

Doch nicht nur im rechtlichen Bereich entstehen durch Cloud Computing neue Möglichkeiten und Herausforderungen. Einer Beschaffung und dem Einsatz von Cloud-Diensten muss nämlich die Analyse der unternehmerischen Anforderungen in funktionaler, aber auch insbesondere organisatorischer und betriebswirtschaftlicher Hinsicht vorangehen.

Selbst wenn bereits eine Cloud-Strategie existiert und es nun um deren Umsetzung geht, muss jedes Unternehmen für sich klären, ob es tatsächlich schon ausreichend vorbereitet ist. Die Integration von Cloud-Diensten hat unter anderem Auswirkungen auf Prozesse im Unternehmen und auf die Aufgabenstellungen und Verantwortungen von Mitarbeitern. Diese Auswirkungen müssen im Vorfeld erkannt und bei der Implementierung von Cloud-Diensten entsprechend berücksichtigt werden. Vor allem Vorbehalte gegen die Nutzung von Cloud-Diensten, sei es infolge fehlender Verankerung in einer bestehenden IT-Strategie, wegen Bedenken bzgl. der Risiken oder auch Ängsten bzgl. eines Verlusts des Aufgaben- und Verantwortungsspektrums, müssen identifiziert und adressiert werden.

Diese notwendigen Vorbereitungen sind weder übermäßig komplex noch teuer, allerdings erfordern sie eine durchdachte und gut organisierte Herangehensweise und eine Ableitung aus einer Cloud-Strategie, damit die Ergebnisse rechtzeitig zur Verfügung stehen und verwertet werden können. Denn erst anhand der identifizierten Auswirkungen und Barrieren können die Prozesse wirksam für die Migration in die Cloud angepasst werden.

Ein wesentlicher Faktor, der über den Erfolg der Implementierung von Cloud-Diensten entscheiden kann, ist die Mitarbeiterkommunikation. Letztendlich muss die Akzeptanz der Nutzer für die Cloud-Migration hergestellt werden. Die Kommunikation sollte vorbereitend zum geplanten Umstieg erfolgen.

Schließlich ist es nach Umsetzung des Cloud-Dienstes und dessen Übernahme in einen produktiven Betrieb wesentlich, die vertraglichen Vereinbarung zu monitoren, Performance und Verfügbarkeit zu überwachen und insbesondere die Verbesserung des Cloud-Dienstes, beispielsweise durch regelmäßige Evaluierung, voranzutreiben

---

[8] Näheres zu diesem Thema findet sich im EuroCloud.Austria-Leitfaden Nr. 4 „Cloud Computing – Auswahl und Einführung von Cloud Services – Prozesse und Organisation“, zu beziehen über www.eurocloud.at

4 Der Empfehlungskatalog „Cloud-Verträge“

Auf Initiative der EuroCloud.Austria fand sich am 03.02.2012 beim Austrian Standards Institute die Arbeitsgruppe 001.38 zusammen, eine Expertengruppe mit Beteiligung von unter anderem der Wirtschaftskammer Wien – Fachverband UBIT und dem IT-Cluster Wien, um die Erstellung eines Katalogs von Empfehlungen für Verträge über Cloud-Dienste zu besprechen.

Ziel dieses Katalogs sollte es sein, vor allem kleinen und mittelständischen Unternehmen eine komprimierte Zusammenstellung wesentlicher Qualitätskriterien zur Verfügung zu stellen, die als Vertragsbestandteil in Allgemeine Geschäftsbedingungen oder Servicelevel Agreements übernommen werden können. Gleichzeitig sollte dieser Katalog Nutzer dabei unterstützen, herauszufinden, ob ein von ihnen in Aussicht genommener Vertrag über Cloud-Dienste alle für sie relevanten Informationen enthält. Grundlage dieses Katalogs waren in erster Linie die von der EuroCloud für den „EuroCloud Star Audit“ entwickelten Qualitätskriterien.

Die Arbeitsgruppe einigte sich darauf, dass die Empfehlungen allgemein gehalten sein sollten, damit sie an die konkreten Dienste angepasst werden können. Dementsprechend sollte auch keine Sammlung an Musterklauseln geschaffen werden, welche mitunter nur für wenige Cloud-Dienste zur Gänze übernommen werden könnten.

Das Ergebnis dieser Arbeitsgruppe wurde schließlich in Form der Publikation „Cloud-Verträge – Was Anbieter und Kunden besprechen sollten“ publiziert und im Rahmen des CLOUDkongresses am 05.11.2012 in Wien erstmals der Öffentlichkeit vorgestellt.[9]

4.1 Der Katalog im Detail

Der Katalog befasst sich mit vier für das Vertragsverhältnis und die Leistungserbringung wesentlichen Bereichen: den Rahmenbedingungen, der Leistungserbringung, der Verrechnung sowie der Sicherheit.

4.1.1 Rahmenbedingungen

Hier geht es in erster Linie darum, jene Informationen aufzulisten, welche dem Nutzer mitgeteilt werden sollen, um ihn ausreichend über seinen potenziellen zukünftigen Vertragspartner und die vertraglichen Grundlagen zu informieren.

So wird beispielsweise empfohlen, sämtliche an der Leistungserbringung beteiligten Unternehmen anzuführen. Weiters wird die detaillierte Regelung der möglichen Änderung von Vertragsbedingungen sowie vor allem auch der Vertragsbeendigung nahegelegt.

---

[9] Zu beziehen beispielsweise über www.eurocloud.at

Besonders Letzteres ist bei Cloud-Diensten bereits bei Vertragsabschluss von größter Relevanz, zumal der Nutzer bereits im Vorfeld darüber Bescheid wissen sollte, in welcher Form und in welchem Zeitrahmen er im Falle einer Vertragsauflösung seine Daten wieder erlangen kann, und vor allem in welchem Ausmaß den Anbieter eine Mitwirkungspflicht trifft.

4.1.2 Leistungserbringung

Dieser Teil befasst sich vor allem mit den technischen Aspekten des Cloud-Dienstes. So werden Regelungen über die eingesetzte Infrastruktur, den Inhalt und Betrieb und vor allem über die Erreichbarkeit des Diensteanbieters empfohlen, um dem Nutzer besonders in Problemfällen die rasche Kontaktaufnahme mit kompetenten Ansprechpartnern zu ermöglichen.

4.1.3 Verrechnung

Die Empfehlungen in diesem Abschnitt laufen im Wesentlichen darauf hinaus, die Verrechnung möglichst transparent und für den Nutzer nach Möglichkeit im Voraus kalkulierbar zu gestalten. Was banal klingt, kann sich besonders bei Cloud-Diensten als Herausforderung erweisen. Aufgrund verschiedenster Verrechnungsmodelle besteht zwar grundsätzlich ein großes Maß an Flexibilität. Diese birgt aber auch die Gefahr der Intransparenz und einer mitunter beachtlichen Kostensteigerung im Falle der unbedarften Nutzung der Flexibilität in sich.

4.1.4 Sicherheit

Schließlich wird der Themenbereich behandelt, der nach der Wahrnehmung vieler Nutzer das größte Risikopotenzial enthält. Die Empfehlungen befassen sich mit Datenschutz, IT-Sicherheit und vor allem der Datensicherung sowie der Datenlöschung.

4.2 Zukünftige Entwicklungen

Die an der Arbeitsgruppe 001.38 beteiligten Institutionen sahen den Empfehlungskatalog einhellig nur als ersten Schritt. Bereits im Vorfeld wurde wiederholt das Interesse an der Erstellung von Musterklauseln für Allgemeine Geschäftsbedingungen und Servicelevel Agreements geäußert. Aufgrund der Komplexität und Verschiedenartigkeit von Cloud-Diensten stellt dies jedoch alles andere als ein triviales Unterfangen dar. Der veröffentlichte Katalog hat aufgrund seiner allgemein gehaltenen Empfehlungen nicht nur den Vorteil der großflächigen Anwendbarkeit, er war zudem Kompromissen leicht zugänglich, weshalb er auch in relativ kurzer Zeit fertiggestellt werden konnte. All diese Vorteile wären bei der Erstellung von Musterklauseln jedoch nicht mehr gegeben. Derzeit ist daher noch nicht absehbar, in welchem Ausmaß und vor allem in welchem Zeitrahmen die Erstellung von Musterklauseln tatsächlich umgesetzt werden kann. Auch die Europäische Kommission ist in mehreren Arbeitsgruppen (SLA, Code of Conduct, Fair and Safe Contract Terms) aktiv in diesen Bereichen tätig.

5 Cloud-Standards und Zertifizierungen im Überblick

Im folgenden Kapitel soll nun ein Bogen von den ursächlichen Herausforderungen (siehe Kapitel 3) und empfehlenswerten Vertragselementen hin zu Standards gespannt werden, die als allgemeingültig und von allen Beteiligten akzeptiert werden können, ohne dass aufwendige Verhandlungen zu führen sind.

Standards und Cloud, passt das überhaupt zusammen? Cloud Computing ist einer der entscheidenden Innovationstreiber bei der zukünftigen Gestaltung der Informationstechnologie. Da ist meist wenig Platz für Standards, weil neue Konzepte, Architekturen und Technologien entwickelt werden, die sich zum Teil noch bestätigen müssen und kontinuierlich verändert und optimiert werden. Auf der anderen Seite verlangen Kunden Verlässlichkeit und wollen Investitionssicherheit für eigene Entwicklungen, um Cloud-Services optimal in die eigene IT-Infrastruktur zu integrieren.

Die folgenden Grundanforderungen werden in zahlreichen Studien genannt:

- Sind die Sicherheitsanforderungen ausreichend erfüllt?
- Kann ein Wechsel zu einem anderen Anbieter mit überschaubarem Aufwand erfolgen?
- Sind die rechtlichen und regulatorischen Anforderungen zu erfüllen?
- Besteht eine ausreichende Transparenz zur Überwachung der Services durch den Kunden?

Bei der Menge und Vielfalt der Cloud-Serviceangebote ist es auf Dauer ökonomisch nicht vertretbar, alle diese Grundanforderungen anhand individueller Analysen zu bewerten und sich mit den jeweiligen Technologien und Architekturen vertraut zu machen. Daher besteht auch in diesem Bereich die Notwendigkeit, Standards zu etablieren und deren Einhaltung zu prüfen.

	Standards	Beispiele
Technologie	Datei & Austauschformate	OVF, EC2, USDL, CIM SVM, EDI...
	Programmierungsmodelle	MapReduce, JAQL; PIG, HIVE
	Protokolle & Schnittstellen	OCCI. CDMI, Cloud Audit, Google DLF, ...
	Standardkomponenten & Referenzarchitekturen	OpenStack, OSGI, NIST RM, IBM RM, DMTF, CTP, ...
	Benchmark & Tests	Benchmarking Suits, Security Assessment, ...
Management	Geschäftsmodelle	IaaS, PaaS, SaaS operating models, Hybrid, Community
	Service-Level-Vereinbarungen	WS-Vereinbarungen (W3C), Business SLAs, ...
	Vertragsbedingungen	EVB-IT, EU SVK, Komponenten von T&C, EULA
	Management-Modelle & Prozesse	ISO 27001/27002, ITIL, COBIT, ...
	Controlling-Modelle & Prozesse	SSAE, SAS 70, ...
	Richtlinien	BSI-Anforderungen, NIST UC, EuroCloud LDP&C
Recht	Gesetzliche Anforderungen	EU Datenschutz Vorschriften, nationale Vorschriften, Safe Harbor
	Freiwillige Verpflichtung	Open Cloud Manifesto, ...
	Unternehmensleitlinien	Interne Leitlinien, ...

Abbildung 1 Quelle: Quelle Booz & Company und FZI (2012) - http://www.trusted-cloud.de/documents/BMWi_Cloud_Standards_Studie_d_web(4).pdf

5.1 Standards

Daran anknüpfend stellt sich die Frage, was ein Standard ist und in welchen Bereichen Standards schon zum Einsatz kommen. Im Kontext Cloud Computing sind es die Bereiche Technologie, Management und Recht, zu denen allgemeine Vorgaben zu erfüllen sind, die zumeist nicht cloudspezifisch sind, sondern generell in den Bereichen IT-Outsourcing und Interoperabilität zu berücksichtigen sind:

Zumindest auf dieser Ebene existiert eine Vielzahl von Standardisierungsinitiativen, die bei der zukünftigen Gestaltung von Cloud-Services zu berücksichtigen sind. Zur Vermeidung von „Lock In"-Situationen – also der Inkompatibilität von kundenspezifischen Daten bei einer möglichen Migration auf einen anderen Cloud-Service oder der Rücküberführung in die selbstgeführte IT-Verarbeitung – ist besonders der Bereich Interoperabilität zu beachten. Ein valider Ansatz ist der Einsatz von Open-Source-Technologien, die schon vom Grundkonzept her darauf ausgelegt sind, eine breite Integration zu unterstützen.
Eine weitere Möglichkeit ergibt sich durch den Einsatz von „Cloud-Brokern", die den Zugriff auf unterschiedliche Cloud-Services vereinheitlichen. Dabei werden proprietäre Schnittstellen auf eine einheitliche Schnittstelle zusammengeführt. Wir kennen diese Konzepte aus dem Bereich der Enterprise Application Integration (EAI). Generell entwickelt sich ein Markt „Migration as a Service", bei dem Daten zwischen unterschiedlichen Anwendungen überführt werden können. Solche Services können zum Beispiel gesamte E-Mail-Konten von Unternehmen in die Cloud oder von einem Cloud-Service zum nächsten überführen.

5.2 Qualität

Die besondere Herausforderung für den Anwender besteht nun in der qualitativen Bewertung eines Cloud-Services und des Anbieters, über den der Service bezogen wird. Der Begriff Qualität lässt sich gemäß ISO 9000 beschreiben als „ein Grad, in dem ein Satz objektiv messbarer Merkmale definierte Anforderungen erfüllt". Das hört sich etwas sperrig an, sagt aber letztendlich aus, ob die Eignung anhand vorher festgelegter Anforderungen gegeben ist.

Bei der Vielzahl der angebotenen Cloud-Services ist es eine enorme Herausforderung, den geeigneten Anbieter zu wählen. Für das klassische IT-Outsourcing konnte man entweder eine langjährige Reputation, den direkten Kontakt zum Anbieter oder in vielen Fällen auch die regionale Erreichbarkeit der IT-Standorte des Anbieters berücksichtigen. All diese Kriterien sind bei Cloud Computing zunächst nicht gegeben. Es wird in erster Linie ein Service gemietet, und die Art und Weise der Serviceerbringung durch den Anbieter kann sehr komplex und völlig losgelöst von regionalen Betrachtungen sein.

So ist zum Beispiel zu prüfen, ob ein Softwaredienst eines nationalen Anbieters Teile der Erbringung (zum Beispiel die Rechner und Speicherkapazitäten) aus dem Ausland bezieht und sich somit besondere Anforderungen aus dem Datenschutz- und Steuerrecht ergeben. Eine Vielzahl von Services wird mittlerweile auch über Marktplätze und Portale angeboten, zum Teil auch als Eigenmarke. Auch hier ist zu hinterfragen, wer der eigentliche Leistungserbringer ist.

5.3 Compliance

Unter dem Begriff Compliance wird die Einhaltung von Gesetzen und Richtlinien des Unternehmens für eine ordnungsgemäße Betriebsführung verstanden. Für den Bereich Cloud Computing erreicht man die Prüfbarkeit der Compliance-Anforderungen nur durch eine ausreichende Transparenz der externen Serviceerbringung – die konkrete Bestimmung der Datenorte, der Leistungserbringer und ihrer Funktionen sowie die vertragliche Prüfung aller notwendigen Leistungsgarantien. Hinzu kommt die Anzeigepflicht eventueller Änderungen in der Leistungserbringung, die dann auch zu einem außerordentlichen Kündigungsrecht führen muss und bei der im Vorfeld auch eine ordnungsgemäße Rückführung der Daten an den Anwender vorgesehen wird.

5.4 Prüfanforderungen

Es gibt schon eine Reihe von Auditierungsschemen für IT-Outsourcing, die sich allerdings sehr auf die Themen Sicherheit und korrekte Transaktionsdurchführung beziehen. Für den komplexen Bereich des Cloud Computings müssen aber alle kritischen Bereiche im Sinne der Compliance-Anforderungen geprüft werden.

Es ist sehr hilfreich, zunächst die eigenen Anforderungen zu klassifizieren und je nach Service eine Gewichtung bezüglich des notwendigen Erfüllungsgrades zu erstellen. Dies sind in erster Linie die Bereiche

- Sicherheit
- Transparenz
- Skalierbarkeit
- Kontrollmöglichkeiten
- Integrationsfähigkeit und -aufwand
- Flexibilität
- Wirtschaftlichkeit
- Compliance

Die Anforderungen können je nach fachlicher Nutzung und Risikoeinschätzung der zu verwaltenden Daten unterschiedlich gesehen werden. Es ist zu empfehlen, für jeden geeigneten IT-Service, der aus der Cloud bezogen wird, eine Scorecard zu entwickeln, in der neben den jeweiligen Anforderungen auch eine Problemeinschätzung durchgeführt wird. Dabei sind die Fachanforderungen sehr unterschiedlich und können sehr stark variieren, je nach Cloud-Service.

Die Prüfung darf sich auch nicht monolithisch in diesen Bereichen bewegen, sondern muss auch die Zusammenhänge untersuchen. So ist zum Beispiel die Zusage einer Verfügbarkeit von 99,9 % einer SaaS-Anwendung nicht viel wert, wenn der Infrastrukturlieferant im Innenverhältnis nur eine Verfügbarkeit von 99,5 % zusichert und keine geeigneten Redundanzverfahren eingerichtet sind.

Die Anforderung der Kontrolle eines externen IT-Anbieters wird im Bereich Cloud Computing zunehmend zu Problemen führen. Gerade in manchen Datenschutzbestimmungen wird die Vor-Ort-Prüfung des Anbieters eingefordert. Es stellt sich aber die Frage, wo ist denn „vor Ort“? Beim Vertragsgeber, beim Rechenzentrumdienstleister oder beim Betreiber des Softwareangebotes? Und wenn man einmal vom Standort der Daten ausgeht, muss man sich auch die Frage stellen, welche Informationen man aus einem persönlichen Besuch eines Rechenzentrums erhalten kann.

Ohne eine intensive Überprüfung durch geschulte Personen aus dem Bereich Datenschutz, Datensicherheit, Betriebsführung und gegebenenfalls Softwareentwicklung erhält man im besten Fall einen subjektiven Eindruck, ob das Gesehene einen ordentlichen Eindruck macht, allerdings ohne qualitative Aussage zur Umsetzung der technischen und organisatorischen Maßnahmen.

Daher wird die Anwendung von Zertifizierungen durch anerkannte Prüfstellen eine immer wichtiger werdende Funktion für den Nachweis der Erfüllung von Kontrollpflichten sein.

Im Bereich Cloud Computing wird diese Eignung zunächst an den fachlichen Anforderungen validiert und erst im Weiteren die Bereiche Sicherheit, Datenschutz, Integrationsfähigkeit und Compliance als fachübergreifende Anforderungen geprüft. Um eine solche Prüfung durchzuführen, bedarf es allerdings Kriterien und Prüfanforderungen, und zwar besonders in Bereichen, die nicht bei der fachlichen Betrachtung erkennbar sind. Da solche Prüfungen in der Regel aufwendig sind und besondere Expertise dabei benötigen, gibt es Zertifizierungen.

5.5 Zertifizierung

Hier werden generelle Anforderungen im Rahmen eines standardisierten Prüfverfahrens formuliert und durch qualifizierte Auditoren validiert. Die ISO Norm 27001 (IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen) ist das bekannteste Prüfverfahren im Bereich der IT-Sicherheit.

Standard	Geltungsbereich	Kern- Prüfbereiche	Cloud spezifisch?	Kommentare
ISO 27001	Informations-Sicherheits-Management System	Sicherheit, Compliance	begrenzt	Sehr allgemein. Man muss genau verstehen, welche Einheit und was geprüft wurde
COBIT	Informations-Technologie	IT Management	Nein	Allgemeines Qualitäts-Rahmenwerk
SAS 70/SSAE16/ ESAE3402	Transaktionen und Rechnungswesen	Buchhaltung Compliance	begrenzt	Sinvolle Erweiterung, z.B. für ERP Cloud Services
EuroCloud Star Audit	Cloud Service (SaaS, PaaS, IaaS)	EU und nationales Recht, Sicherheit, Compliance, EU und nationaler Datenschutz, Interoperabiliät	Ja	Umfassender Anwendungsbereich, für KMUs einfach zu verstehen
FedRamp	Cloud Service Provider	Sicherheit, US Compliance, ständige Überwachung	Ja	Hohe Bürokratie, teilweise nur Selbsteinschätzung, Kontrolle gegenüber NIST SP 800-53 R3
CSA	Cloud Sicherheit	Sicherheit, Interoperabilität	Ja	Exzellente Risikobewertung
PCI DSS	CC Payment Services	Sicherheit	begrenzt	Sehr begrenzter Anwendungsbereich

Abbildung 2 Quelle: EuroCloud Deutschland

In Bezug auf Cloud Computing ist Sicherheit aber nur ein Aspekt der Prüfungsanforderungen. Gerade die Spezifikation von Service Level Agreements (SLA) und die vertragliche Formulierung von Datenschutzanforderungen sind ebenfalls in hohem Maße relevant. Da Cloud-Services oftmals über mehrere Beteiligte erbracht werden, ist auch zu prüfen, ob die Anforderungen über die gesamte Lieferkette erfüllt sind. Wenn der Anbieter einer SaaS-Lösung eine ISO 27001 Zertifizierung hat, sagt dies noch lange nichts über die Sicherheitssysteme der Vorlieferanten, z. B. eines eingebundenen Plattform- oder Infrastrukturanbieters aus.

In der folgenden Übersicht werden einige der typischen Zertifizierungssysteme dargestellt:

Die EuroCloud-Organisation hat schon 2010 mit der Definition eines cloudspezifischen Zertifizierungsverfahrens begonnen und es im Frühjahr 2011 unter der Bezeichnung „EuroCloud Star Audit“ veröffentlicht. Mit einem einheitlichen Prüfverfahren für alle Cloud-Services und mit einem abgestuften Bewertungsverfahren ist die Umsetzung der Qualitätsanforderungen für die Kunden nachvollziehbar dokumentiert und durch qualifizierte Auditoren validiert.

Weiterführende Informationen unter www.eurocloud.de und www.star-audit.de.

Genereller Einstieg: http://www.cloud-migration.eu/

6 Cloud-Standards in der EU

Auf europäischer Ebene befasst sich derzeit nach Betrauung durch die Europäische Kommission die ETSI mit der Schaffung von Standards für Cloud Computing. Als erster Schritt fand Anfang Dezember 2012 in Cannes ein zweitägiger Koordinierungs-Workshop statt, zu dem 125 Experten als Vertreter staatlicher und nichtstaatlicher Organisationen sowie aus der Privatwirtschaft, darunter, aufgrund ihrer Mitwirkung am EuroCloud Star Audit, Vertreter der EuroCloud Austria und Deutschland, eingeladen waren.

Ziel dieser Veranstaltung war es, zunächst bestehende Standards und deren Anwendbarkeit im Cloud-Umfeld sowie fehlende Regelungen zu analysieren und auf dieser Grundlage den weiteren Fahrplan festzulegen. Dazu fanden in fünf Arbeitskreisen, je einer zu den Themen Sicherheit und Datenschutz, Interoperabilität, Übertragbarkeit von Daten, Servicelevel Agreements sowie Wiedererlangbarkeit von Daten, teils hitzige Diskussionen statt.

Als erstes Ergebnis dürften aller Voraussicht nach die Arbeitskreise zur Übertragbarkeit und zur Wiedererlangbarkeit von Daten zusammengelegt werden, da sie sich thematisch stark überschneiden. Insbesondere das im Cloud-Umfeld brisante Thema, auf welche Art sichergestellt werden kann, dass ein Nutzer im Falle der Beendigung des Vertragsverhältnisses mit seinem bisherigen Cloud-Anbieter, sei es infolge Kündigung oder Insolvenz des Anbieters, seine Daten wiedererlangen und mit möglichst geringem Aufwand zu einem anderen Anbieter oder in das eigene Rechenzentrum übertragen kann, wird von beiden Arbeitskreisen behandelt.
Im Übrigen wird die ETSI nun die Ergebnisse des Treffens analysieren. Danach wird voraussichtlich im Februar 2014 ein weiteres Treffen stattfinden, nach dem ein erster Zwischenbericht an die Europäische Kommission ergehen soll.

Der Koordinierungs- und Standardisierungsprozess bei der ETSI steht somit noch am Anfang. Aufgrund des vor allem auch politischen Interesses an Standards für Cloud Computing ist aber davon auszugehen, dass er früher oder später zu verwertbaren Ergebnissen führen wird. Fraglich ist natürlich der zeitliche Horizont, zumal bei diesem Thema, wie man auch in Cannes beobachten konnte, verschiedene Interessen teils heftig aufeinanderprallen. Dies ist aber eine Herausforderung, vor der die ETSI bereits früher stand und sie auch gemeistert hat.

Im Rahmen der European Cloud Partnership hat die EU-Kommission weitere Arbeitsgruppen mit ausgewählten Industrievertretern gebildet, die praxisorientierte Empfehlungen für die Themen

- Certification
- Service Level Agreements
- Code of Conduct

erarbeiten, die die weitere Basis für die Umsetzung der Anforderungen in der Europäischen Union sind.

7 EuroCloud Star Audit

Die Organisation EuroCloud bietet erstmals eine Cloud-Zertifizierung unter dem Namen „EuroCloud Star Audit“ an. Die Zertifizierung ist spezifisch auf die Bereiche IaaS, PaaS und SaaS ausgelegt und hat definierte Aussagen zu Kontrollelementen, die abgestuft zu erfüllen sind, um als vertrauenswürdiger Cloud-Anbieter zertifiziert zu werden.

Zur qualitativen Prüfung der Leistungserbringung hinsichtlich der Datensicherheit, des technischen Betriebes und der organisatorischen Abläufe bedarf es einer weitreichenden Expertise, um die jeweiligen Anforderungen, die sich aus den Servicegarantien ergeben, zu prüfen. Aus diesem Grund werden zumeist Zertifikate herangezogen, die eine kompakte Aussage zu den Sicherheitsaspekten und der Zuverlässigkeit des Serviceanbieters geben.

Für die vorgenannten vertraglichen, technischen und organisatorischen Anforderungen hat EuroCloud ein spezielles Gütesiegel entworfen, dessen Nutzung voraussetzt, dass die für die Bereitstellung von Cloud-Services grundlegenden Anforderungen durch geschulte Auditoren geprüft und durch ein Zertifikat bestätigt werden. Für die Prüfanforderungen wurde in enger Abstimmung mit öffentlichen Institutionen, Forschungseinrichtungen, Cloud-Anbietern, Rechtsexperten und Wirtschaftsprüfungsgesellschaften ein Kriterienkatalog erstellt.
Konkret werden im EuroCloud Star Audit folgende Kategorien erfasst:

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

Durch ein Punktesystem und die Vorgabe von Mindestkriterien kann ein Anbieter verschiedene Gütestufen (ein Stern bis fünf Sterne) erreichen.

Im Kern geht es um rechtliche Aspekte, zuverlässige Bereitstellung von technischen Dienstleistungen sowie Datenschutz, Datensicherheit und Einhaltung grundlegender Qualitätsstandards für Betriebsprozesse und Anwendungsgestaltung. Für seine Angaben im Audit muss der Anbieter konkrete Nachweise vorlegen; zudem verpflichtet er sich, signifikante Änderungen der Rahmenbedingungen (zum Beispiel Ort der Leistungserbringung, Änderung der Subunternehmervereinbarungen) und kritische Vorfälle unverzüglich zu melden.

Im Ergebnis werden je nach Umsetzungsgrad die drei folgenden Gütestufen vergeben:

- Trusted Cloud-Service – drei Sterne
- Trusted Cloud-Service Advanced – vier Sterne
- Trusted Cloud-Service Advanced HA (High Availability) – fünf Sterne

7.1 Ein-Stern-Zertifizierung

Der Anbieter hat folgende Pflichtkriterien erfüllt:

- Es handelt sich um ein im EU-Handelsregister eingetragenes Unternehmen.
- Der technische Betrieb der Anwendung erfolgt in einer für die Bereitstellung von webbasierten Diensten geeigneten Infrastruktur.

- Hierzu gehört:
  - ein abgeschlossener Bereich für die verwendeten Hardwarekomponenten
  - redundante Stromversorgung mit USV-Betrieb für mindestens 20 Minuten
  - redundante Internetanbindung
  - Zutrittskontrolle
  - grundlegende Arealsicherheit

- Die vertraglichen Vereinbarungen sind konform mit den Datenschutzanforderungen im Sinne des Bundesdatenschutzgesetzes.
- Es bestehen nachvollziehbare Kündigungsvereinbarungen.
- Es bestehen eindeutige Vereinbarungen bezüglich der Kundendaten ohne Zurückbehaltungsrecht durch den Auftragnehmer.
- Es bestehen vertraglich vereinbarte Regelungen mit dokumentierten Datenexportschnittstellen zur Rückgabe und Löschung von Kundendaten bei Beendigung des Vertragsverhältnisses.

7.2 Zwei-Sterne-Zertifizierung

Ergänzend zu den vorgenannten Anforderungen sind folgende Pflichtkriterien erfüllt:

- Der Anbieter macht nachvollziehbare Angaben zu den zugesicherten Serviceleistungen in Bezug auf Verfügbarkeit und Geschwindigkeit der Anwendung. Diesbezüglich stehen auch Berichtsfunktionen zum Nachweis der Servicezusagen zur Verfügung.
- Der technische Betrieb entspricht den Minimalanforderungen eines Rechenzentrums hinsichtlich der redundanten Auslegung der technischen Grundversorgung. Arealrisiken und Gebäudesicherheit sind durch Dokumentation des Anbieters ausgewiesen.
- Die Exportformate der Kundendaten sind durchgängig dokumentiert und für die Migration in andere Umgebungen verfügbar.

7.3 Drei-Sterne-Zertifizierung

Ergänzend zu den vorgenannten Anforderungen sind folgende Pflichtkriterien erfüllt:

- Der Anbieter ermöglicht die Wahl des nationalen Gerichtsstandes durch den Anwender oder bietet direkt den Vertrag nach Recht des Anwenders an.
- Der Anbieter bietet eine umfangreiche Dokumentation sowie Schulungsmaterial zur Einführung in die Nutzung des Services an. Eine Hotline steht zu üblichen Arbeitszeiten des Anwenders zur Verfügung. Probleme können durch ein elektronisches Ticketsystem übermittelt werden.
  Der Anbieter hat Prozesse mit garantierten Bearbeitungsabläufen und den dazu notwendigen internen Anwendungen auch mit möglichen Vorlieferanten etabliert.
- Die jeweiligen Zusagen im Service-Management und bezüglich der technischen Bereitstellung wurden durch geschulte Auditoren vor Ort geprüft.

7.4 Vier-Sterne-Zertifizierung

Ergänzend zu den vorgenannten Anforderungen sind folgende Pflichtkriterien erfüllt:

- Die technische Bereitstellung entspricht den Anforderungen an einen professionellen Rechenzentrumsanbieter. Die Kommunikationsanbindung erfolgt über einen direkten und redundant ausgelegten Internet-Exchange-Knoten (IX).
- Die Serviceprozesse entsprechen den Anforderungen gemäß ITIL und ISO 27001 im Sinne eines ISMS (Information Security Management System).
- Die Sicherheitsfunktionen und Anwendungen von Verschlüsselungstechniken sind nachvollziehbar dokumentiert und entsprechen den normalen IT-Sicherheitsanforderungen. Schutzmaßnahmen gegen externe Angriffe sind vorhanden und entsprechen zum Zeitpunkt der Auditierung den Anforderungen der ISO 27001.
- Die direkten Zugriffe durch Administratoren sind eingeschränkt, und für Einzelzugriffe erfolgt eine Anonymisierung von Transaktionsdaten gegenüber den Benutzerprofilen. Hierzu bestehen auch entsprechende Verfahrensdokumentationen, die dem Kunden bei Bedarf zur Verfügung gestellt werden.
- Sofern nicht durch andere Maßnahmen die Langzeitarchivierung von Kundendaten im Sinne der Grundsätze zum Datenzugriff und der Prüfbarkeit digitaler Unterlagen umgesetzt wird, werden durch den Anbieter die Archivierungs- und Bereitstellungsfunktionen von Kundendaten im Umfang der gesetzlichen Anforderungen erfüllt.

7.5 Fünf-Sterne-Zertifizierung

Ergänzend zu den vorgenannten Anforderungen sind folgende Pflichtkriterien erfüllt:

- Der Anbieter verfügt über eine redundante Bereitstellung des Serviceangebotes über mindestens zwei Rechenzentren mit einer Verfügbarkeit von 99,99 Prozent und einer hochausfallsicheren Infrastruktur.
- Es werden regelmäßig (mindestens einmal pro Jahr) Notfallübungen durchgeführt und dokumentiert gemäß BS 25999.
- Es werden regelmäßig (mindestens einmal pro Jahr) Penetrationstests zum Nachweis der Sicherheitsfunktionen durchgeführt und dokumentiert.
- Der Anbieter verfügt über ein variables Preismodell und erlaubt auch im laufenden Vertrag den Wechsel in ein allgemein angebotenes, günstigeres Vertragsmodell zu den jeweiligen Laufzeitkonditionen (Best-Price-Option).

7.6 EuroCloud Star Audit

Die vorgenannte Zertifizierung ist ein Best-Practice-Ansatz, um die wichtigen Managementfragen bei der Auswahl eines geeigneten Cloud-Anbieters zu beantworten. In Abgrenzung zu reinen Sicherheits- oder Datenschutzzertifizierungen wird hier der gesamte Bereich berücksichtigt und in einer verständlichen Aussage attestiert. Es werden sich klassische Zertifizierungssysteme weiter in Richtung Cloud-Prüfung entwickeln; dies kann aber zum Teil mehrere Jahre dauern. In den Kernfragen und besonders für den Mittelstand sind jetzt Hilfestellungen notwendig.

Anbieter mit dem folgenden Siegel haben die Kriterienerfüllung durch EuroCloud bestätigt bekommen:

Abbildung 3 Quelle: EuroCloud Deutschland



8 Glossar Cloud Computing

8.1 Was ist unter Cloud Computing zu verstehen?[10]

„Cloud Computing ist ein Modell, das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."

Folgende fünf Eigenschaften charakterisieren gemäß der NIST-Definition einen Cloud-Service:

- On-demand Self Service: Die Provisionierung der Ressourcen (z. B. Rechenleistung, Storage) läuft automatisch ohne Interaktion mit dem Service-Provider ab.
- Broad Network Access: Die Services sind mit Standard-Mechanismen über das Netz verfügbar und nicht an einen bestimmten Client gebunden.
- Resource Pooling: Die Ressourcen des Anbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können (Multi-Tenant-Modell). Dabei wissen die Anwender nicht, wo die Ressourcen sich befinden, sie können aber vertraglich den Speicherort, also z. B. Region, Land oder Rechenzentrum, festlegen.
- Rapid Elasticity: Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unendlich zu sein.
- Measured Services: Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt werden.

8.2 Bereitstellungs- und Bezugsfunktionen von Cloud-Services

Es existieren vielfältige Möglichkeiten der Bereitstellung und des Bezugs von Cloud-Computing-Leistungen. Daher ist zwischen den folgenden Rollen zu differenzieren:

---

0 https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html

(a) Bereitstellung

- Cloud-Serviceanbieter – Unternehmen, das die Cloudleistungen gegenüber dem Kunden als Vertragsgeber anbietet.
- Cloud-Service-Subunternehmer – Vorlieferant von Cloud-Services,die vom Cloud-Serviceanbieter als Teilfunktion integriert werden.
- Cloud (Managed) Hosting Provider – Cloud-Services-Subunternehmer, der technische IT-Leistungen, die dem klassischen IT-Outsourcing entsprechen (Rechner, Speicher, Netzwerk), erbringt, die nicht als vollwertige Cloud-Serviceleistung bezogen werden.
- Co-Location Provider – Vorlieferant von Infrastrukturkomponenten, der Gebäude, Strom, Klima, Kommunikation etc. als Grundversorgung bereitstellt.
- Cloud-Servicevermittler – Unternehmen, das für den Cloud-Serviceanbieter Kunden wirbt (und rechtlich die Stellung eines Handelsvertreters einnimmt).
- Cloud Service Reseller – Wiederverkäufer von Cloud-Services, der selbst keine Anpassung des Cloud-Services erbringt, sondern sämtliche Leistungen der Serviceerbringung vom Cloud-Serviceanbieter bezieht (und rechtlich als Vertragshändler zu qualifizieren ist).
- Cloud-Lösungsanbieter – Cloud Service Reseller, der mehrere Cloud-Services bündelt und als integriertes Paket weiterverkauft.

Der Begriff „Broker“ wird hier bewusst nicht verwendet, da dieser im Markt in unterschiedlichen Bedeutungen verwendet wird, d.h. sowohl im Sinne von Vermittler als auch im Sinne von Lösungsanbieter.
Auch der Begriff „Marktplatz“ wird im Markt in unterschiedlichen Bedeutungen verwendet, d.h. im Sinne von „Vermittler“ oder „Reseller“.

(b) Bezug

- Cloud-Serviceabnehmer – Vertragspartner des Cloud-Serviceanbieters, der als Unternehmen den Service nutzen will.
- Cloud-Servicenutzer – Einzelner Benutzer eines Cloud-Services, in der Regel ein Arbeitnehmer des Cloud-Serviceabnehmers.
- Cloud-Serviceadministrator – Fachbereich des Cloud-Serviceabnehmers, der mit der Verwaltung von Identitäten und Nutzungsoptionen des Cloud-Services betraut ist.

Im Markt wird teilweise der Begriff „Broker“ auch verwendet als Bezeichnung einer internen Funktion im IT-Bereich des Cloud-Serviceabnehmers, die den Cloud-Servicenutzern cloudbasierte Lösungen bereitstellt.

Nachfolgend werden die Beteiligten in den inhaltlichen Beiträgen gemäß diesen Definitionen bezeichnet, sofern es der Kontext nicht anders erfordert, allerdings jeweils ohne den Zusatz „Cloud-Service-...“.

8.3 Cloud-Services und deren Eigenschaften

Als weitere typische Eigenschaften für einen Cloud-Service treten häufig die folgenden Merkmale auf:

1. Selbstverwaltung des Services und der damit verbundenen Leistungen durch den Anwender.
2. Technisch uneingeschränkter Netzwerkzugriff mit Standardanwendungen (z. B. Web-Browser) des Anwendergerätes (z. B. Notebook, Smart Phone).
3. Multimandantennutzung der technischen Ressourcen, zumeist über ganze Rechenzentrumsbereiche oder mehrere verteilte Rechenzentren als Ressourcenpool.
4. Unmittelbare Elastizität, das heißt die automatische Bereitstellung von technischen Ressourcen aus dem Ressourcenpool bei Spitzenanforderungen oder Erweiterung der Zahl der Benutzer.
5. Kontinuierliche Messung der tatsächlichen Nutzung pro Mandant und leistungsgerechte Abrechnung.

8.4 Cloud-Services und Betriebsmodelle

Bei der Bereitstellung von Cloud-Services gibt es zwei Unterscheidungsebenen: die Art der Cloud-Services und die verschiedenen Betriebsmodelle, die in freier Kombination verwendet werden können.

(a) Cloud-Services

Bei der Bereitstellung von Cloud-Services unterscheidet man in erster Linie drei Ebenen:

- SaaS – Software as a Service
  Sämtliche Angebote von Anwendungssoftware, die den Kriterien des Cloud Computings entsprechen, fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. Als Beispiele seien Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen genannt.

- PaaS – Platform as a Service
  Ein PaaS-Anbieter stellt eine komplette Infrastruktur bereit und bietet dem Kunden auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So kann die Plattform z. B. Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe, etc. als Service zur Verfügung stellen. Der Kunde hat keinen Zugriff auf die darunterliegenden Schichten (Betriebssystem, Hardware), er kann aber auf der Plattform eigene Anwendungen laufen lassen, für deren Entwicklung der PaaS-Anbieter in der Regel eigene Werkzeuge anbietet. Als Beispiel kann force.com der Firma Salesforce oder Azure der Firma Microsoft genannt werden.
- IaaS – Infrastructure as a Service
  Bei IaaS werden IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze als Service angeboten. Ein Cloud-Serviceabnehmer kauft diese virtualisierten und in hohem Maß standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Cloud-Serviceabnehmer z. B. Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.

Daneben gibt es weitere Ausprägungen als Sonderform, wie zum Beispiel Security, Business Process, Storage, Monitoring oder Communication as a Service, die zusammenfassend oftmals auch als XaaS benannt werden.

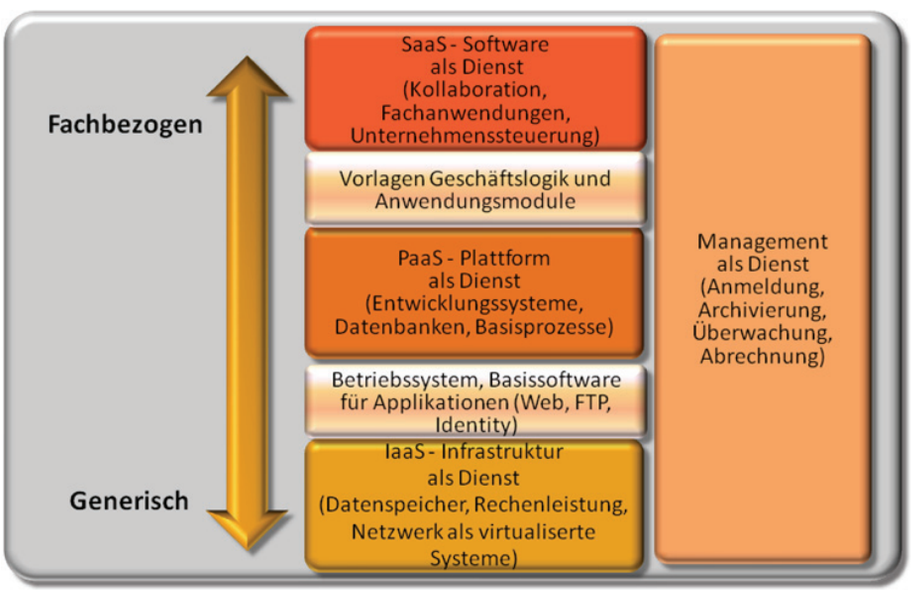


Abbildung 4 Quelle: EuroCloud Deutschland

(b) Cloud-Betriebsmodelle

Bei den Betriebsmodellen ist zu unterscheiden, wer der Betreiber ist und wer generell Zugriff auf die Services hat:

Private Cloud: Dedizierte Bereitstellung der Services für einen definierten Kunden unter Verwendung von abgrenzbaren Hardware-Ressourcen (also in der Regel Rechenzentren, abgeschlossene Bereiche innerhalb des Rechenzentrums) und Netzwerkbereiche, die nicht von Dritten genutzt werden.

Virtual Private Cloud: Im Gegensatz zur Private Cloud erfolgt die Mandantenabgrenzung lediglich auf der logischen Netzwerkebene, bei gleichzeitiger Nutzung der Hardware über mehrere Kunden.



Abbildung 5 Quelle: EuroCloud Deutschland

Public (öffentliche) Cloud: Generelle Bereitstellung der Services für einen unbeschränkten Kundenkreis, der Hardware-Ressourcen gemeinschaftlich nutzt. Die von den Kunden in Anspruch genommenen Cloud-leistungen werden mittels logischer Mandantenzuordnung separiert.



Abbildung 6 Quelle: EuroCloud Deutschland

Daneben existieren noch Sonderformen wie

- Community Cloud: Kombination mehrerer Cloud-Services für bestimmte Anwendergruppen. Dies kann zum Beispiel im Bereich Logistik, Fertigung, Forschung oder Branchenvereinigungen definiert werden. Der Zugang ist nicht öffentlich, sondern erfordert zusätzliche Authorisierung durch die Betreiber der Community Cloud. Die an einer Community Cloud teilnehmenden Unternehmen haben meist ähnliche Anforderungen an Verfügbarkeit, Compliance und Sicherheit der bereitgestellten Ressourcen. Als Beispiel seien hier Banken oder Regierungsstellen genannt.

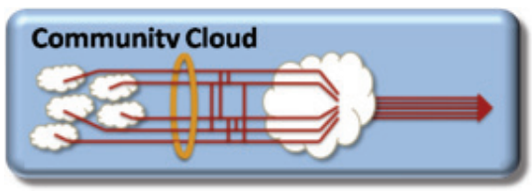


Abbildung 7 Quelle: EuroCloud Deutschland

- Hybrid Cloud: Kombination von Private und Public Cloud. Hierbei erfolgt ein kombinierter Betrieb von Cloud-Services, bei denen ein Teil in einer privaten Umgebung (zum Beispiel ein ERP-System) und ein Teil aus einem öffentlichen Bereich (z. B. CRM) technisch und logisch zusammengeführt wird. Ein Beispiel für die Entstehung einer Hybrid Cloud ist die Verlagerung einer öffentlichen

Firmenwebseite aus der Private Cloud in die Public Cloud. Da die Firmenwebseite ohnehin aus dem Internet erreichbar sein muss, kann einer Verlagerung in die Public Cloud unter Umständen sogar für höhere Sicherheit sorgen.

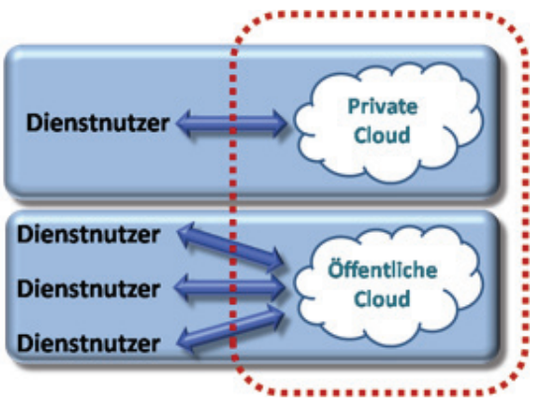


Abbildung 8 Quelle: EuroCloud Deutschland

8.5 Cloud-Service-Marktplatz

Unterschiedliche Institutionen bieten ihre Leistungen über einen gemeinsamen Marktplatz und gegebenenfalls auch über eine gemeinsame Ausführungsplattform in der Cloud an. Diese Dienste können wiederum zur Unterstützung von Geschäftsprozessen zu komplexeren Mehrwert-Dienstleistungen gebündelt werden. Neben den Anbietern und Abnehmern dieser Dienste sowie den Entwicklern der Dienste und den Prozessdesignern, die die Mehrwert-Dienstleistungen zusammenstellen, kommt dem Betreiber des Marktplatzes als Lösungsanbieter oder Reseller eine zentrale Rolle zu.

Quellen:

https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html

http://www.fokus.fraunhofer.de/de/elan/_docs/isprat_cloud_studie_20110106.pdf

http://csrc.nist.gov/groups/SNS/cloud-computing/

http://www.isst.fraunhofer.de/Images/Fraunhofer-ISST_CSMP-Whitepaper_www_tcm81-98065.pdf

9 Rechtlicher Hinweis

9.1 Allgemeines

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

9.2 Inhalt des Leitfadens

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

9.3 Verweise und Links

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

9.4 Urheberrecht

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

9.5 Vergütung

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

10 Autoren

Die Autoren dieses Leitfadens sind:



Mag. Árpád Geréd
Maybach Görg Lenneis & Partner Rechtsanwälte
a.gered@mglp.eu
www.eurocloud.at



Andreas Weiss
Direktor EuroCloud Deutschland_eco e.V.
andreas.weiss@eurocloud.de
www.eurocloud.de
Managing Director EuroCloud Europe s.a.r.l.
www.eurocloud.org



DI Bernd Becker
Vorstand EuroCloud Deutschland_eco e.V.
Präsident EuroCloud Europe s.a.r.l.
bernd.becker@eurocloud.de
www.eurocloud.de



DI Ulrike Huber
Geschäftsführerin
ulrike.huber@42virtual.com
www.42virtual.com



Mag. Christian Zeidler
office1@zeidler-pinkel.com
www.zeidler-pinkel.com

Notizen

EuroCloud Österreich

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

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

Copyright: EuroCloud.Austria

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