Leitfaden

# Cloud Computing

## Risk & Compliance

## Schweiz

Leitfaden
Cloud Computing
Risk & Compliance

www.eurocloudswiss.ch

**Impressum**

Dieser Leitfaden wird herausgegeben von:

EuroCloud Swiss
Verein zur Förderung von Cloud Computing
8000 Zürich

E-Mail: info@eurocloudswiss.ch
Web: www.eurocloudswiss.ch

# Inhalt

## Vorwort

Liebe Leserinnen und Leser,

Cloud Computing beschreibt einen Ansatz zur Erbringung von IT-Dienstleistungen, der viele Hürden der IT-Planung überwindet. Während anderswo der Begriff „Lean Production“ geprägt wurde, führt Cloud Computing im Unternehmen zu einer „Lean IT“. Das Nutzungspotential ist gross und Kostenvorteile von Cloud Computing können positiv hervorgehoben werden. Gleichzeitig bestehen jedoch gelegentlich Bedenken in Bezug auf Sicherheits- und Datenschutzbedürfnisse.

Der vorliegende Leitfaden informiert über Sicherheits- und Complianceaspekte im Cloud Computing Umfeld. Er soll für Anbieter und Anwender gleichermassen hilfreich sein.

Die erstmalige Umstellung auf einen Cloud-Service stellt ein Migrationsprojekt dar. Die Umsetzung solcher Projekte und die Nutzung von Cloud Services sind für jedes Unternehmen individuell zu betrachten. Das Nutzungs- und Einsparungspotential sowie die Angebote am Markt sind vielfältig. Jedes Unternehmen wird sich also mit der Frage beschäftigen müssen, ob Teile der erforderlichen IT-Services nicht besser aus der Cloud bezogen werden sollten. Spätestens dann sind die in diesem Leitfaden angesprochenen Fragen zu klären.

EuroCloud Swiss ist der schweizerische Fachverband zur Förderung des Cloud Computing in der Schweiz. Gleichzeitig repräsentiert EuroCloud Swiss das paneuropäische EuroCloud-Netzwerk in der Schweiz. Wie zuvor die EuroCloud Deutschland_eco e.V. und die EuroCloud Austria präsentiert nun auch die EuroCloud Swiss einen Leitfaden zum Cloud Computing.

EuroCloud Swiss bietet eine Auditierung von Cloud-Anbietern im Bereich „Software as a Service" (SaaS) an. Im Rahmen der Auditierung lässt EuroCloud Swiss neben den rechtlichen Aspekten auch die betriebliche Bereitstellung und die Serviceerbringung durch unabhängige Experten prüfen. Von EuroCloud zertifizierte Cloud Service-Anbieter weisen mit diesem Gütesiegel nach, dass sie ihren Service nach höchsten Qualitätsansprüchen abwickeln. Gerade mittelständische Unternehmen, welche die eigene Wettbewerbsfähigkeit durch Einbindung von externen Serviceangeboten erhalten und ausbauen wollen, verfügen oftmals nicht über die Ressourcen zur individuellen Prüfung von externen Anbietern. Das EuroCloud Gütesiegel unterstützt den Kunden in der Auswahl des Dienstleisters.

Als Präsident der EuroCloud Swiss bedanke ich mich bei den Autoren, die bei der Erstellung des vorliegenden Leitfadens mitgewirkt haben.

Zürich, März 2012

Heinz Dill, Präsident EuroCloud Swiss

# 1 Einleitung

Wie bei jedem IT Projekt ist es auch für Cloud Projekte zentral, dass Anbieter auf Bedürfnisse der Kunden eingehen. Heute ist der Informationsschutz wichtiger denn je, entsprechend haben die Kundenbedürfnisse betreffend Informationsschutz und Sicherheit einen hohen Stellenwert. Gleich verhält es sich mit Compliance-Vorgaben für den Kunden.

Entscheidend ist die Erkenntnis, dass Cloud Projekte, unter Berücksichtigung der genannten Kundenbedürfnisse sich ohne weiteres realisieren lassen. Freilich sind entsprechend unterschiedliche Massnahmen vorzukehren.

Dieser Leitfaden „Cloud Computing: Risk & Compliance“ gibt Empfehlungen für die Realisierung von Cloud Projekten, namentlich hinsichtlich:

- Vertragsgestaltung (siehe Ziffer 5) und
- Sicherheit (siehe Ziffer 6).

Damit bekommen sowohl Anbieter als auch Anwender ein Hilfsmittel für die Umsetzung eines Cloud Projektes. Der Leitfaden soll auch als Basis für Gespräche zwischen Anbieter und Kunden bilden. Eine Detailprüfung seitens Anwender und Anbieter kann der Leitfaden nicht ersetzen.

Ergänzend und als Grundlage für die oben genannten praktischen Umsetzungshilfen (Vertragsgestaltung, technische und organisatorische Massnahmen) beschreibt der Leitfaden „Cloud Computing, Risk & Compliance“ folgende Aspekte:

- Ausführungen zum Paradigmenwechsel, der Cloud Computing überhaupt erst ausmacht (Ziffer 2);
- Ausführungen zu den Chancen sowie den Themen, die aus Risikoüberlegungen wohl bedacht und vertraglich geregelt sein müssen (Ziffer 3);
- Ausführungen zu den sich stellenden Compliance Themen (Ziffer 4);
- Weitere hilfreiche Dokumentation, namentlich das Glossar (Ziffer 7) sowie Quellennachweise (Ziffer 8) runden den Leitfaden ab.

Die im Leitfaden beschriebenen Themen sind aus den Prüfkriterien des EuroCloud SaaS-Gütesiegels abgeleitet. Das Gütesiegel bildet einen Rahmen für „Software as a Service“-Angebote und definiert Beurteilungskriterien für SaaS-Angebote unter Berücksichtigung von Serviceerbringung, rechtlichen Aspekten, Datensicherheit, Datenschutz, Vertragsgestaltung und Interoperabilität.

Dieser Leitfaden beschränkt sich nicht allein auf Software as a Service (SaaS), sondern beschreibt auch die Grundlagen und Empfehlungen, die im Umfeld von Infrastructure as a Service (IaaS) sowie Platform as a Service Angeboten (PaaS) massgeblich werden.

# 2 Der Weg in die Cloud

Der Weg in die Cloud führt meistens über ein Migrationsprojekt, das sowohl für den Anbieter wie auch den Nutzer Herausforderungen bietet.

Der Nutzer muss seine Nutzungsbedürfnisse sowie das im Markt verfügbare Angebot, das seine Abläufe verbessert und Mehrwert generiert kennen (lernen).

Der Anbieter muss entsprechend seiner strategischen Ziele neue Produkte und Dienstleistungen definieren. Gleichzeitig muss der Anbieter abklären, welche Produkte und Dienstleistungen die Erwartungen und die Bedürfnisse der Nutzer am besten abdecken.

## 2.1 Die „Cloud“

### 2.1.1 Paradigmenwechsel

Die Innovationszyklen werden immer schneller. Technologische Entwicklungen in den Bereichen Endgeräte, Netzwerke, Kommunikation, Server- und Speicherinfrastrukturen sowie Anwendungen gehen rasant einher.

Mit der zunehmend globalisierten Wirtschaft und den Bedürfnissen zu immer schnelleren und umfangreicheren Informationen sind die Anforderungen auch seitens der Unternehmen als zukünftige potentielle Nutzer stark gestiegen.

Ein Paradigmenwechsel ist notwendig. Für die Nutzer soll die verfügbaren Angebote einfacher und kostengünstiger werden, was auf Seiten der Anbieter zu mehr Komplexität führt, Investitionen erfordert und neue Businessmodelle eröffnet.

Von einem systemzentrischen Ansatz wechselt man in einen informationszentrischen Ansatz.

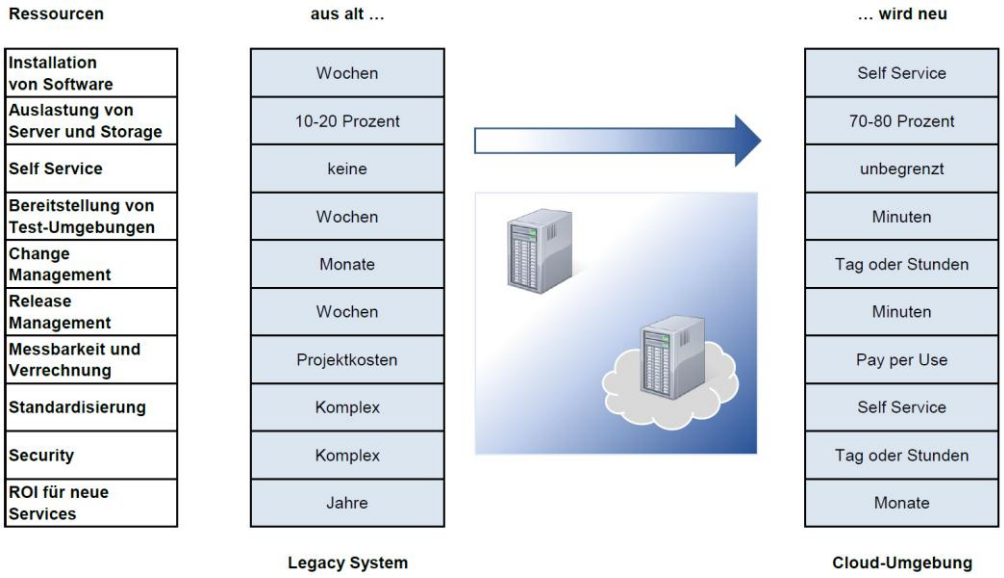
Beim systemzentrischen Ansatz standen die IT Infrastruktur, Transaktionen und Daten im eigenen Netz im Vordergrund. Beim informationszentrischen Ansatz stehen im Zentrum Workloads, Prozesse, Daten und Services, die von überall erreichbar sind.

Der Wechsel von der althergebrachten IT-Nutzung zu den neuen und innovativen Cloud Services verändert die Nutzung, das Software-Lizenz Modell und das Geschäft der IT Anbieter erheblich.

Im Zusammenhang mit dem Paradigmenwechsel stellen sich namentlich die folgenden Fragen:

- Wo sind die Daten, wohin gehen sie, wer nutzt sie und wie werden sie genutzt?
- Wie kann die Einhaltung von Policies sichergestellt und wie Verletzungen verhindert werden?
- Wer hat Zugriff und wie kann die Authentizität sichergestellt werden?
- Insbesondere der Data Loss Prevention (DLP) muss in diesem Zusammenhang grosse Beachtung beigemessen werden.

Die nachfolgende Graphik zeigt im Einzelnen, auf welchen Ebenen sich der Paradigmenwechsel niederschlägt:




Cloud Services sind shared Services und bedeuten eine Konsolidierung der ICT auf allen Ebenen. Gleichzeitig bedeutet Cloud Computing einen Wechsel von der Investitionskostenrechnung (Capital Expenditure, Capex) zur Betriebskostenrechnungen (Operational Expenditure, Opex).

### 2.1.2 Cloud Services oder Outsourcing?

„Outsourcing“ und „Cloud Computing“ werden teilweise als Gegensätze dargestellt.

Innerhalb des IT-Bereiches erscheint jedoch Cloud Computing als Weiterentwicklung von Outsourcing, die dadurch begünstigt wird, dass einerseits die Anforderungen an den Ausbau der IT in allen Bereichen (z.B. Internet-Infrastruktur, Bandbreiten, Server-, Speicherkapazitäten. Softwareentwicklung, Sicherheit, betriebliche Aufwände etc.) und andererseits die Anforderung an die Business Flexibilität gestiegen sind.

Wesentliche Unterschiede sind:

- Der Begriff „Outsourcing“ ist älter und etabliert. Der Markt kann sich etwas darunter vorstellen.
- Cloud Computing ist anders als Outsourcing auf den IT Bereich beschränkt. Outsourcing ist dem gegenüber ein umfassenderer Denkansatz, der auch Bereiche ausserhalb der IT Infrastrukturen einbeziehen kann.

## 2.2 Charakteristiken von Cloud Computing

### 2.2.1 Standardisierung

Kostenüberlegungen veranlassen Anbieter zu einem hohen Grad an Standardisierung, Automatisierung und Skalierbarkeit. Dies wirkt sich sehr häufig auf die Standardisierung der Serviceerbringung aus, was gleichzeitig positiv wie auch negativ gewürdigt werden kann:

- Kunden können von den Spezialkenntnissen der Anbieter profitieren und sich so auf ihr Kerngeschäft konzentrieren;
- der Spielraum für den Kunden, vom Anbieter individuelle technische Lösungen zu beziehen, ist sehr oft eingeschränkt.

### 2.2.2 Kernbedürfnisse der Nutzer

Für den Erfolg und die Akzeptanz von Cloud Computing sind die folgenden Themen aus Kundensicht zentral, und zwar branchenübergreifend:

- Datensicherheit bzw. Kontrollverlust über die Daten (Zugriffsschutz und Kontrolle über Speicherort etc.)
- Portabilität von Daten und Softwarecode (vom Kunden definierte Makros oder dergleichen, die der Kunde in der Cloud-Anwendung vorgenommen hat)

### 2.2.3 Herausforderungen

| **Herausforderungen der Nutzer** | **Herausforderungen der Anbieter** |
|---|---|
| <u>Strategie</u><br><br>• Analyse der Leistungserwartungen (geschäftliche und sicherheitsbezogene)<br>• Analyse der Ausgangslage (aktuelle Kosten des IT Betriebs)<br>• Analyse der Möglichkeiten (Make or Buy, Full-, Teil-, Hybrid-Sourcing) | <u>Strategie</u><br><br>• Wie sieht die interne und die kommunizierte Cloud Strategie aus?<br>• Ist meine Positionierung im Markt noch richtig und richtig kommuniziert?<br>• Welches Marktsegment soll bedient werden? |
| <u>Produktauswahl</u><br><br>• Customizing nötig und, wenn ja, möglich?<br>• Chancen und Risiken?<br>• Anforderungen an Sicherheit und Vertraulichkeit erfüllt?<br>• Kann der Cloud Service in meine bestehende IT integriert werden? Welche Einflüsse hat der Cloud Service auf meine Prozesse?<br>• Welchen Implementierungs und Schulungsaufwand habe ich? | <u>Produktentwicklung</u><br><br>• Welche Angebote sind möglich und sinnvoll?<br>• Chancen und Risiken?<br>• Ergibt sich Investitionsbedarf? |

| Herausforderungen der Nutzer | Herausforderungen der Anbieter |
|---|---|
| Auswahl des Anbieters<br><br>• Finanzielle und organisatorische Verlässlichkeit des Anbieters?<br>• Entspricht der Servicevertrag meinen Bedürfnissen? | Aufstellung im Markt<br><br>• Können Cloud Services mit der heutigen Organisation entwickelt und vertrieben werden?<br>• Sind Partnerschaften einzugehen, um das Produkt anbieten zu können?<br>• Ist in andere Unternehmen zu investieren? |

## 2.3 Kompetenzen des Kunden sind gefragt

Die Standardisierung führt gleichzeitig zu einer hohen Spezialisierung, Modularisierung und Segmentierung der Anbieter.

Dadurch benötigt der Kunde ein hohes Mass an Kompetenz in IT-Angelegenheiten und Marktkenntnis. Die interne IT übernimmt damit die Rolle eines Brokers und Managers von parallel laufenden ausgelagerten Workflows.

Andernfalls besteht die Gefahr, dass die genutzten Dienstleistungen die Bedürfnisse des Nutzers nicht befriedigen oder das Potential nicht optimal ausgeschöpft wird.

# 3 Chancen & Risiken

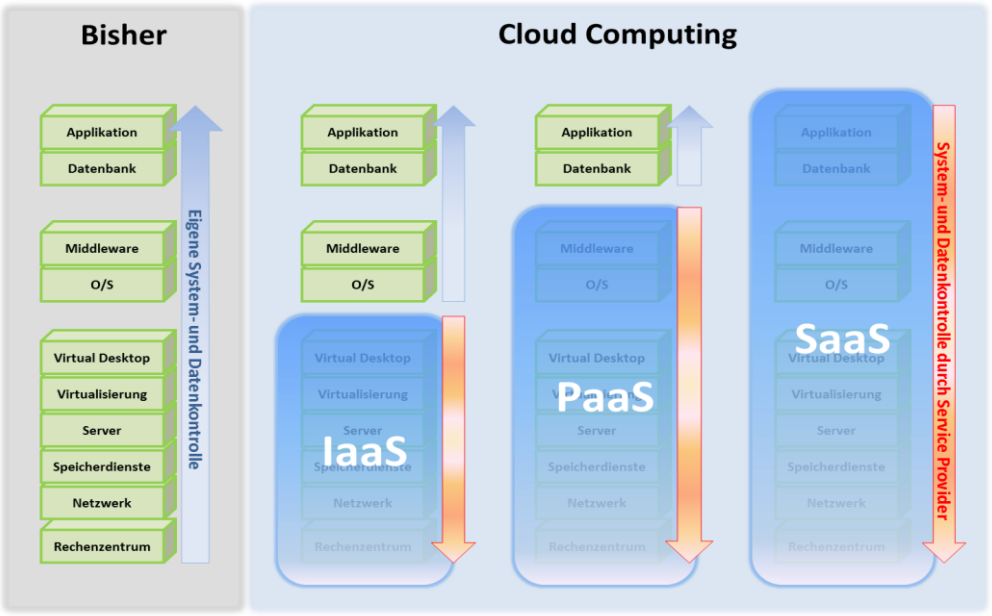
Cloud Computing bietet erhebliche Chancen, die Effizienz im Umgang mit IT-Mitteln, Flexibilität sowie Informationssicherheit zu verbessern.

Bei der Nutzung von Cloud Computing gibt jedoch der Nutzer immer auch die Kontrolle über die in der Cloud bearbeiteten Daten an den Cloud Provider ab. Bei bisherigen Modellen der IT-Nutzung hielt der Nutzer die Kontrolle über Systeme und Daten weitgehend in der eigenen Hand.

Durch den Wechsel hin zum Cloud Computing lässt die Kontrolle mit jedem weiteren, vom Cloud Anbieter bezogenen Service Layer ab. Die Infrastruktur muss der Nutzer nun zwar nicht mehr selbst verwalten, dafür verliert der Kunde die Kontrolle über die Infrastruktur.

Da im Cloud Computing die weiteren Layer jeweils auf den darunterliegenden Schichten aufbauen, nimmt der Verlust der Kontrolle über Systeme und Daten mit jeder zusätzlichen Schicht zu.

Dies zeigt die nachstehende Grafik:




Wer ein Cloud Projekt realisieren will, sollte die Chancen zusammen mit den Risiken würdigen, um seine Ziele ausgewogen umzusetzen.

Die folgenden Unterkapitel beschreiben die Chancen und Risiken pro Service Layer. Zudem werden Massnahmen erläutert, welche der Risikominimierung dienen.

## 3.1 Infrastructure as a Service (IaaS)

Der Cloud Service beinhaltet über das Internet, auf Subskriptionsbasis (On Demand) genutzte IT-Infrastruktur wie Platz, Klima, Netzwerk, Server, Speicher bis zum Betriebssystem und dem zugehörigen Betriebs-Monitoring. Kunden können jeweils individuelle Middleware- und/oder Anwendungsumgebungen frei implementieren oder über das Internet nutzen.

| Chancen | Risiken |
|---|---|
| • Hohe Skalierbarkeit der benötigten Systeme, je nach Bedarf<br>• Redundante Datenspeicherung<br>• Physisch getrennte Aufbewahrung und Nutzung von Daten<br>• Keine Maintenance für Einrichtung und Betrieb der Infrastruktur<br>• Opex statt Capex<br>• Pay-as-you-Go | • Standort der Daten bei Public- wie auch bei Private Clouds nicht immer erkennbar<br>• Stark abhängig von Verfügbarkeit der Infrastruktur und Netzwerke<br>• Fehlende oder mangelnde Abgrenzung / Isolierung der diversen Daten-Bearbeitungen<br>• Unberechtigter Datenzugriff auf Grund von Fehlkonfiguration<br>• Gewährleistung der Vertraulichkeit, Sicherheit und Integrität der Daten |

## 3.2 Platform as a Service (PaaS)

PaaS baut auf IaaS auf. Diese Dienstleistung ermöglicht es dem Kunden, seine benötigte Middleware (Tools, Datenbanken etc.) On Demand zusammenzustellen. Die Nutzer können auf der Plattform für Ihre Kunden oder ihre eigene Bedürfnisse Anwendungssoftware entwickeln, betreiben und über das Internet nutzen.

| Chancen | Risiken |
|---|---|
| • Kein Administrationsaufwand, da die notwendige Infrastruktur nicht selbst implementiert und bereitgestellt werden muss<br>• Entwicklung im Team (auch geographisch verteilt)<br>• Eine einzige Plattform mit minimalen Kosten<br>• Keine Maintenance für Einrichtung und Betrieb der Plattform und deren Tools<br>• Opex statt Capex<br>• Pay-as-you-Go | • Vendor Lock-in<br>• Fehlende Portabilität<br>• Fehlende Interoperabilität<br>• Keine standardisierten Technologien<br>• Mangelnde Flexibilität<br>• Anforderungen von proprietären Anwendungen oder Entwicklungsumgebungen |

## 3.3 Software as a Service (SaaS)

SaaS baut auf PaaS und IaaS auf und ist die angebotene Dienstleistung, die dem Anwender den grössten Nutzen bringt. Die Anwendungssoftware ist On Demand abrufbar und kann von verschiedenen Standorten und von mehreren Usern gleichzeitig über das Internet genutzt werden.

| Chancen | Risiken |
|---|---|
| • Trennbarkeit / Mandantenfähigkeit der Applikationen<br>• Schnell einsatzfähig / Schnellere Projekteinführung<br>• Keine Maintenance für den Betrieb der Business-Funktionalitäten<br>• Opex statt Capex<br>• Pay-as-you-Go<br>• Niedriger Gesamtkosten (TCO)<br>• Mobilität / Standortunabhängigkeit | • Fehlende Portabilität<br>• Geringere Integrierbarkeit in bestehende Applikationslandschaften<br>• Geringere Anpassungsmöglichkeiten, da vorgegebene Standardisierung<br>• Evtl. höhere Antwortzeiten<br>• Auswahl des richtigen Providers<br>• Sicherheitslücken<br>• Keine Nutzung ohne Internetzugang |

# 4 Compliance

Cloud Computing ist neben der organisatorisch-technischen Herausforderung eine Compliance Aufgabe.

Da der Cloud Anbieter meist nicht gleich eng wie ein Outsourcing Dienstleister kontrolliert werden kann, fragt sich, ob die Bearbeitung und Speicherung von Daten bei externen Cloud Anbietern überhaupt möglich ist. Dies umso mehr, wenn sich der Dienstleister im Ausland befindet oder zumindest der Zugriff auf die Daten aus dem Ausland geschehen kann.

Dieses Kapitel behandelt die wesentlichen Compliance Themen, die für Cloud Projekte zu beachten sind.

## 4.1 Vorbemerkungen

### 4.1.1 Wer hat für Compliance zu sorgen?

Wer Cloud Services einsetzen und nutzen will, hat die ihn geltenden Gesetze und Branchenregulierungen einzuhalten. Der Eidgenössische Datenschutz- und Öffentlichkeits-beauftragte (EDÖB) bringt es in den Erläuterungen zu Cloud Compution vom Oktober 2011 auf den Punkt:

„*Unternehmen und Behörden, die solche Dienste in Anspruch nehmen, sind sich oft zu wenig bewusst, dass die primäre Pflicht zur Einhaltung der Datenschutzregeln zunächst einmal bei ihnen selbst liegt und nicht beim Anbieter, der die Daten auf einem Cloud-Server speichert oder in der Cloud bearbeitet*."

Demgegenüber ist der Cloud Anbieter primär für die Sicherheit der Daten hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit sowie für die Besorgung der nötigen Softwarelizenzen sowie für die Einhaltung weiterer vertraglicher Vereinbarungen zuständig. Vor diesem Hintergrund sind die folgenden Ausführungen zu beachten.

### 4.1.2 Strukturierung der Fragestellung

Dem Nichtjuristen kann der Entscheid, ob er Daten in die Cloud auslagern darf, schwerfallen. Der nachstehende Checkliste soll helfen, die Datenauslagerung in die Cloud vorzubereiten und die notwendigen Fragen zu stellen:

- Welche für Daten werden ausgelagert? (dazu Ziffer 4.3)
- Dürfen die Daten ausgelagert werden? (dazu Ziffer 4.4)
- Dürfen die Daten ins Ausland ausgelagert werden? (dazu Ziffer 4.5)
- Welche zusätzlichen Compliance Anforderungen sollen berücksichtigt werden? (dazu Ziffer 4.6)

Da Personendaten oft eine besondere Hürde für Cloud Vorhaben darstellen, ist den Personendaten ein eigenes Kapitel zu widmen (dazu Ziffer 4.2).

Anzumerken ist freilich bereits hier, dass behörden- und/oder branchenspezifische Anforderungen für den Nutzer weit gewichtigere Einflüsse, respektive Sanktionen zur Folge haben können als etwa das (schweizerische) Datenschutzrecht.

Namentlich zu nennen sind beispielsweise die Vorschriften, denen Finanzdienstleister (Bankkundengeheimnis), Telekommunikationsanbieter oder Unternehmen der Versicherungswirtschaft unterstehen.

### 4.1.3 Relevante Themen

Aus Compliance-Sicht sind die folgenden Themen abzudecken:

- Datenschutz
- Branchenspezifika
- Steuerrecht Geschäftsbücherverordnung
- Vertragsrecht

Die rechtlichen Herausforderungen des Cloud Computing sind ähnlich gelagert wie jene bei anderen Outsourcing-Projekten. Rechtliche Rahmenbedingungen können jedoch ein Cloud Projekt stark beeinflussen, obwohl der Nutzen einer Auslagerung in die Cloud gross wäre.

Nachfolgend einige Beispiele:

- Ausland: Die Auslagerung ins Ausland kommt häufig vor. Gelangen die Daten ins Ausland, ist der Kontrollverlust grösser als im Inland. Gemäss Schweizerischem Recht müssen Länder in welche Personendaten ausgelagert werden, das gleiche datenschutzrechtliche Niveau bieten wie die Schweiz (in EU-Ländern wie Deutschland gewährleistet). Ein prominentes Beispiel eines Landes, welche das datenschutzrechtliche Niveau der Schweiz nicht erreicht, sind die USA.

- Datenbearbeitung durch Dritte: Ausgelagerte Daten können evtl. durch Drittpersonen bearbeitet werden. Das Schweizerische Recht ermöglicht natürlichen sowie juristischen Personen zu bestimmen, von wem, ob und wie ihre Daten verarbeitet werden. Handelt es sich bei den zu migrierenden Daten um Personendaten, können besondere Geheimnispflichten bestehen (z.B. Bankgeheimnis).

- Andere Drittrechte: Sind die zu migrierenden Daten beispielsweise durch Immaterialgüterrechte geschützt, kann eine Auslagerung verboten sein.

- Besondere Regulierung: Regulierungen verlangen unter Umständen besondere Massnahmen (bspw. bei Finanzdienstleistern, Dienstleistern des Gesundheitswesens, Versicherungsdienstleister etc.).

## 4.2 Personendaten insbesondere

### 4.2.1 Definition von Personendaten

Das Schweizerische Datenschutzgesetz (DSG) **definiert Personendaten** als jene Angaben, die sich auf eine bestimmte oder bestimmbare (natürliche oder juristische) Person beziehen.

Wer selber Kunden hat, bearbeitet wohl immer auch deren Personendaten. Beispiele für Personendaten sind die Daten aus dem CRM des Cloud Nutzers, Bankkundendaten, Transaktionsdaten wie z.B. Verkaufstransaktionen mit bestimmten Personen etc.

Zu beachten sind zudem besonders schützenswerte Personendaten, bei welchen zusätzliche, höhere Anforderungen an die Bearbeitung, insbesondere durch Dritte gestellt werden. Besonders schützenswerte Personendaten sind beispielsweise Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative oder strafrechtliche Verfolgungen und Sanktionen.

### 4.2.2 Verschlüsselung und Anonymisierung

Der Personenbezug von Daten lässt sich jedoch entfernen. Gelingt dies vollständig, spricht man von **anonymisierten** Daten. Das DSG kommt bei anonymisierten Daten nicht zur Anwendung, da wie beschrieben der Personenbezug fehlt. Mit der Anonymisierung ist dem Datenschutzinteresse Genüge getan; aufgrund der Anonymisierung können die Daten keiner Person mehr zugewiesen werden, und der Nutzer hat seine Pflichten damit erfüllt.

In der Praxis wird auch die **Verschlüsselung** von Daten als genügende Massnahme angesehen, um den Personenbezug zu entfernen und die betroffene Person zu schützen. Ob diese Massnahme wirklich ausreichend ist, kann hier nicht abschliessend behandelt werden. Denkbar ist, dass die heute genügende Verschlüsselung morgen aufgrund des Fortschritts der Technik bereits nicht mehr genügt und ohne weiteres entschlüsselbar ist.

Kann die Anonymisierung der Personendaten nicht vollständig sichergestellt werden, resultiert der Anonymisierungsversuch oft nur in einer **Pseudonymisierung**. Pseudonymisierung bedeutet, dass der Personenbezug nicht ohne weiteres erkennbar ist, jedoch leicht wieder hergestellt werden kann. Statistische Daten sind meistens anonymisierte Daten, ausser die Datenmenge lässt wegen geringer Zahl Rückschlüsse auf Personen zu.

### 4.2.3 Einschaltung von Subunternehmern und deren Kontrolle

Das Schweizerische Datenschutzrecht gilt als auslagerungsfreundlich. Der Cloud Nutzer muss dennoch gewisse gesetzliche Anforderungen einhalten, bevor die Daten Bearbeitung an Dritte ausgelagert werden kann. Die Auslagerung ist teilweise nicht ohne die vorgängige Zustimmung der Kunden oder anderer Geheimhaltungsberechtigten zulässig; bei besonders schützenswerten Personendaten ist die explizite Zustimmung des Kunden notwendig.

Aus Perspektive des Nutzers ist zu empfehlen, dass der Cloud Vertrag eine Verpflichtung des Anbieters aufstellt, welche sicherstellt, dass der Nutzer über allfällige Datenschutzverstösse umgehend informiert wird. Der Nutzer sollte zudem sicherstellen, dass er den Vertrag seinen Kunden offenlegen darf.

## 4.3 Auslagerung von Daten im Allgemeinen

Die Rechtsordnung als solche stellt kein generelles Auslagerungsverbot auf und steht der arbeitsteiligen Wirtschaft grundsätzlich offen gegenüber. Die Auslagerung von Daten und die anschliessende Bearbeitung kann durch Vereinbarung oder Gesetz übertragen werden, wenn:

- die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte und
- keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

Der Auftraggeber muss sich insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet.

Es bestehen nur wenige Fälle, wo eine Auslagerung ins Inland oder Ausland absolut verweigert wird. In den meisten Fällen können die berechtigten Personen ihre Zustimmung zur Datenmigration geben (Consent); es kommen Rechtsfolgen zum Tragen, wenn die Zustimmung ausbleibt. Manchmal verlangt das Recht nur, dass informiert wird (Notice).

Bei gewissen Sektoren können Ausnahmefälle bestehen, bei welchen die Auslagerung als solche nicht erlaubt ist (z.B. gewisse Bereiche der öffentlichen Behörden). Auch aufgrund von

Rechtsunsicherheit (z.B. wegen zu wenig klarer Regelung) kann sich der Schluss ergeben, dass von einer Auslagerung als solcher besser abzusehen ist (z.B. Berufsgeheimnisse).

### 4.3.1 Auslagerung durch Behörden

Gewisse kantonale Gesetze stellen rechtliche Hindernisse für die Auslagerung von Daten dar, insbesondere bei der Auslagerung von Daten öffentlicher Einrichtungen.

Beispiele hierfür sind:

- Formale Vorbedingungen: Allgemeine Verbote zur Nutzung von Informatikmitteln, an denen dem Kanton keine Eigentums- oder Nutzungsrechte zustehen (z.B. § 9 Abs. 1 des Reglements über den Einsatz der Informatik des Regierungsrates des Kantons Thurgau). Auch dann, wenn die Möglichkeit von Ausnahmen im Einzelfall besteht, stellt das Erfordernis zur Einholung einer vorgängigen Genehmigung ein Hindernis bei der Auslagerung von Daten dar.

- Formale Anforderungen an den Vertrag: Generelles Erfordernis der Schriftlichkeit für Verträge bei der Auslagerung von Informatikdienstleistungen (z.B. § 8 der Verordnung über die Informatiksicherheit (VIS) des Kantons Basel-Landschaft). Falls bei solchen Regelungen Schriftlichkeit analog dem Obligationenrecht im Sinne der handschriftlichen Unterzeichnung zu verstehen ist, werden dadurch der Abschluss von Online Vereinbarungen oder durch E-Mail ausgeschlossen (zumal der Einsatz von digitalen Signaturen noch nicht üblich ist).

- Inhaltliche Anforderungen an den Vertrag: Verbindliche Vorgaben in Bezug auf den Inhalt des mit externen Anbietern abzuschliessenden Vertrages, z.B. aufgrund der Pflicht zur Verwendung der „Allgemeine Geschäftsbedingungen (AGB) Sicherheit“ des Kantons Zürich oder der AGB des Kantons Bern über die Informationssicherheit und den Datenschutz (ISDS) bei der Erbringung von Informatikdienstleistungen, welche umfangreiche Pflichten des Anbieters in Bezug auf Information, Datensicherheit, Beizug von Subunternehmern, Verpflichtung des Personals zur Vertraulichkeit, einschliesslich Datenschutz-Revers, Durchführung von Datenschutz- und Sicherheits-Audits sowie Unterstellung unter die Aufsicht und Kontrolle der zuständigen kantonalen Aufsichtsbehörden vorsehen.

- Kontrollmechanismen: Verpflichtung des externen Anbieters zur Gewährung des Zutrittsrechts zu seinen Räumen (§ 15 Abs. 2 Informatikgesetz des Kantons Luzern). Dies ist bei den heutigen Cloud-Infrastrukturen bzw. Datenzentren nur schwer umsetzbar.

Der Anwendungsbereich derartiger Vorschriften ist differenziert festzulegen. Die Anforderungen bezüglich Datensicherheit und Datenschutz sind abzustufen, je nachdem ob es sich z.B. um Daten mit oder ohne Personenbezug, um besonders schützenswerte Personendaten, um geheime Daten, um Anwendungen mit strategischer Bedeutung etc. handelt.

Für anonymisierte Daten oder Anwendungen erscheinen Anforderungen im Sinne der oben erwähnten Vorschriften jedenfalls als zu weitgehend.

### 4.3.2 Träger von Berufsgeheimnissen (Ärzte, Anwälte, Treuhänder, etc.)

Es ist umstritten, ob Geheimnisträger ohne individuelle Zustimmung der Geheimnisberechtigten Daten in die Cloud auslagern dürfen.

Die Praxis tendiert dahin, die Auslagerung zuzulassen. Der Cloud Anbieter wird als Gehilfe, d.h. als Teil der Organisationsinfrastruktur des Geheimnisträgers angesehen. Hier ist jedoch insofern zu differenzieren, dass z.B. die Zahnarztgehilfin unter viel engerer Kontrolle des Zahnarztes steht als ein Cloud Anbieter, welcher dem Zahnarzt möglicherweise nicht einmal persönlich bekannt ist.

Der Berufsgeheimnisträger wird demnach Bestimmungen in den Vertrag aufnehmen müssen, die den Anbieter einer Kontrolle unterwerfen. Der Anbieter muss als Gehilfe (und Auftragsdatenbearbeiter) in den „informationellen Schutzbereich“ des Geheimnisträgers integriert werden. Geschützte Informationen müssen abgekapselt gehalten werden. Abgekapselt heisst mit Blick auf Cloud-Angebote mit verteilter Server- und Speicherinfrastruktur nicht „einheitlicher Server- und Speicherort“ oder „physisch getrennte Datenhaltung“. Im Resultat muss jedoch sichergestellt sein, dass der Cloud Anbieter den Zugriff individuell kontrollieren kann.

Der Anbieter muss diese vertragliche Kapselung von Information technisch-organisatorisch umsetzen können. Cloud Anbieter, die für diese Probleme Lösungen anbieten (PET, privacy enhancing technology), werden im Markt einen erheblichen Wettbewerbsvorsprung erreichen können.

Auch Banken, Versicherungen und Telekommunikationsdienstanbieter müssen besondere Vertraulichkeitsvorschriften einhalten. Für sie kommen entsprechende Anforderungen zum Tragen.

Am einfachsten kann den besonderen Datenschutzvorschriften der oben genannten Dienstleister dadurch Folge getragen werden, dass im Cloudvertrag oder auch in einem zusätzlichen Vertrag der Anbieter denselben datenschutzrechtlichen Vorschriften unterworfen wird wie der Nutzer der Cloud.

## 4.4 Auslagerung von Daten ins Ausland

Unter der Voraussetzung, dass die Auslagerung von Daten an Dritte zulässig ist, kann in einem nächsten Schritt geprüft werden, ob die Daten auch ins Ausland ausgelagert werden können.

Das Datenschutzgesetz stellt besondere Anforderungen an die Auslagerung von Daten ins Ausland auf, welche zwingend einzuhalten sind. Grundsätzlich gilt, dass Personendaten nicht ins Ausland bekannt gegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

Auslagerungen ins europäische Ausland oder andere Rechtsordnungen mit einem angemessenen Datenschutzniveau sind grundsätzlich möglich, da die Datenschutzbestimmungen den schweizerischen grösstenteils entsprechen.

Findet die Auslagerung jedoch in andere Länder  statt (oder haben Personen aus einem Land ohne angemessenes Schutzniveau Zugriff auf Personendaten), ist diese nur zulässig, wenn:

- hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten;
- die betroffene Person im Einzelfall eingewilligt hat;
- die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt;
- die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;
- die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen;
- die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat;
- die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.

Weitere Anforderungen an die Auslagerung ins Ausland können sich aus besonderen Regulierungen ergeben, auf die im Rahmen dieses Leitfadens jedoch nicht eingegangen werden kann.

**Achtung:** Ist der geschäftliche Sitz des Cloud Anbieters im Ausland, untersteht er ausländischem Recht. Ausländische Behörden oder Private können dann auf Inhalte in der Cloud zugreifen. Der Kunde kann also auch dann Compliance Pflichten haben, wenn ein (ausländischer) Anbieter die Serverinfrastruktur ausschliesslich in der Schweiz betreibt.

## 4.5 Weitere Compliance Anforderungen

### 4.5.1 Steuerrecht, Buchführung und Archivierung

Bevor ein Unternehmen Cloud Dienstleistungen als Nutzer in Anspruch nimmt, muss es abklären, welche Risiken in seinem Nutzungsbereich bestehen und welche Sicherheitsstandards es einhalten muss resp. mindestens einhalten will. Vor der Auslagerung von Daten in die Cloud muss ein Unternehmen seine Anforderungen in Bezug auf Risiken und Sicherheit festlegen.

So muss der Kunde z.B. in Steuerverfahren oder in Rechtsstreitigkeiten (Zivil- oder Strafprozess) gewisse Nachweise erbringen können (bspw. Offenlegung der Buchführung etc.). Diese Nachweispflichten werden jedoch nicht durch die Tatsache der Auslagerung als solches beeinträchtigt bzw. beeinflusst. Die Frage stellt sich umgekehrt:

Zunächst geht es darum festzustellen, welche Anforderungen der Nutzer generell einhalten muss resp. welche Daten er bereithalten muss.

Anschliessend ist zu bestimmen, welche Leistungen der Dienstleister zu erbringen hat, damit er dem Nutzer helfen kann, den an ihn gestellten Nachweispflichten nachzukommen.

Dies kann bedeuten, dass der Cloud Vertrag durch gewisse Mindestinhalte zu ergänzen ist.

### 4.5.2 Ausländische Regulierungen

Neben nationalen Regulierungen können auch ausländische Regulierungen einen Einfluss auf Kunden oder Anbieter in der Schweiz haben. Unternehmen mit Gruppengesellschaften z.B. in den USA können verpflichtet sein, die US-amerikanischen Bestimmungen gruppenweit einzuhalten. So kann eine ausländische Regelung eine Reflexwirkung in die Schweiz entfalten.

Nach den Terroranschlägen vom 11. September 2001 haben etwa die USA den „Patriot Act“ erlassen (Gesetz zur Terrorismusbekämpfung), aufgrund dessen das FBI Internetprovider und somit auch Cloud Anbieter überwachen und ggf. zwingen kann, Daten herauszugeben.

Es ist nicht ausdrücklich vorgesehen, dass Daten, die ausserhalb der USA gespeichert sind und die nicht der Kontrolle einer US-amerikanischen Niederlassung unterliegen, von den USA überwacht werden können. Sollte jedoch begründeter Verdacht auf Terrorismus bestehen, müssten die amerikanischen Behörden bei den zuständigen Schweizer Behörden Zugriff auf die Daten verlangen.

Die Handhabung des Gesetzes ist noch nicht gefestigt. Fest steht, dass verschlüsselte Daten keinen Schutz vor dem Zugriff im Rahmen des Patriot Act bieten.

### 4.5.3 Import/ Export Regulatorien

Bei der Erbringung oder dem Bezug von Dienstleistungen sind sowohl Anbieter als auch Nutzer verpflichtet, die gesetzlichen Regelungen betreffend Export und Import einzuhalten.

In der Schweiz werden diese Vorgaben durch das Staatssekretariat für Wirtschaft SECO geregelt. Andere relevante Autoritäten sind die EFTA, OECD und die WTO. Dienstleister müssen sicherstellen, keine Leistungen in Länder zu liefern, gegen welche die Schweiz Embargos oder Sanktionen etabliert hat.

US-Amerikanische Anbieter dürfen keine Leistungen in Länder wie z.B. Kuba, Burma, Nordkorea, Iran, Nordsudan oder Syrien liefern.

## 4.6 Beispiele

Bevor ein Kunde den Entscheid zur Auslagerung von Daten fällt, sollte er sich bewusst werden, welche Daten von der Auslagerung betroffen sind. Für jede Kategorie der zu migrierenden Daten sollte eine separate Analyse vorgenommen und ein separater Entscheid gefällt werden. In den nächsten Tabellen haben wir einige Beispiele aufgeführt, welche die Entscheidungsfindung für ausgewählte Branchen illustrieren.

### 4.6.1 Banken

| | Bankenkundendaten (Bearbeitung, Speicherung) | Anonymisierte Daten (z.B. in Testumgebung) | Software (z.B. Zur-Verfügung-Stellung einer Entwicklungsumgebung) |
|---|---|---|---|
| **Auslagerung erlaubt?** | Zulässig | Keine Einschränkung | Soll eine Software durch einen externen Dienstleister betrieben werden, braucht es dazu die Zustimmung des Inhabers der Urheberrechte an der Software. |
| **Auslagerung ins Ausland erlaubt?** | Nicht erlaubt ohne Zustimmung der betroffenen Kunden. | Keine Einschränkung, solange genügend Vorkehrungen getroffen sind | Nach Massgabe des Lizenzvertrages mit Rechtsinhaber. |
| **Zusätzliche Compliance Anforderungen?** | FINMA RS 2008/07 „Outsourcing“<br><br>Datenschutzgesetz | Keine | Keine |
| **Vertragliche Massnahmen** | Namentlich:<br>• Auswahl des Anbieters<br>• Sicherheitsmassnahmen<br>• Kontrollrechte<br>• Information über Datenschutzverstösse | Keine | ev. Lizenzvertrag zur Nutzung der Software |

### 4.6.2 Industrieunternehmung

| | Kundendaten (CRM) | Daten in ERP (z.B. Einkaufs- und Verkaufsdaten) | Forschungs- und Entwicklungsdaten |
|---|---|---|---|
| **Auslagerung erlaubt?** | Zulässig. Vorbehalten sind besondere Geheim-haltungspflichten. | Keine Einschränkung. | Urheber- und Patent-rechte (eigene sowie solche von Zulieferern)<br><br>Interne Richtlinien des Kunden. |
| **Ausland erlaubt?** | Ja falls:<br><br>• Angemessenes Schutzniveau,<br>• Safe Harbor, oder<br>• Zustimmung der betroffenen Kunden | Siehe Kundendaten<br><br>Pflicht zur Archivierung in der Schweiz (Mehr-wertsteuergesetz) | Gemäss Lizenzver-trägen mit Dritten. |
| **Zusätzlich Compliance Anforderungen?** | Unterscheidung ob ein-fache oder besonders schützenswerte Perso-nendaten involviert sind<br><br>Datenschutzgesetz | Steuerrecht (Mehrwertsteuer)<br><br>Buchführung und Archivierung | Keine |
| **Vertragliche und sonstige Massnahmen** | Sicherheitsmassnahmen<br><br>Kontrollrecht<br><br>Information über Datenschutzverstösse | grundsätzlich keine<br><br>Ev. Geheimhaltungs-vereinbarung etc. | grundsätzlich keine<br><br>Ev. Geheimhaltungs-vereinbarung etc. |

# 5 Vertragsgestaltung

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

## 5.1 Orientierung am Gütesiegel „EuroCloud SaaS“

Es gibt schon heute eine Vielzahl von professionellen und sicheren Lösungen. Das Gütesiegel soll Anbietern eine Hilfestellung sein, das Vertrauen der Nutzern betreffend sicherer Anwendungen zu gewinnen.

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

Konkret werden im Gütesiegel folgende Kategorien erfasst:

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

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

Im Unterschied zu anderen Initiativen, bei denen entweder nur Teilbereiche berücksichtigt werden oder die Angaben ohne Gegenkontrolle als freiwillige Selbstverpflichtung zu sehen sind, wird beim SaaS Gütesiegel eine Validierung der Angaben durchgeführt und in vereinbarten Zeiträumen wiederholt, damit ein konkreter Nachweis der Angaben sichergestellt werden kann.

Zudem verpflichtet sich der Anbieter, signifikante Änderungen der Rahmenbedingungen (z.B. Ort, Datenhaltung und/oder Ressourcen für die Leistungserbringung, Änderung der Subunternehmervereinbarungen) und kritische Vorfälle unverzüglich zu melden.

Das SaaS-Gütesiegel wird seit Anfang 2011 offiziell vergeben.

## 5.2 Vertragsabschluss und Vertragsgestaltung

Die folgenden Punkte sollten bei der Vertragsgestaltung entsprechend umgesetzt und im Rahmen der EuroCloud SaaS-Gütesiegel-Zertifizierung geprüft werden:

- ☐ Wie wird der Vertrag geschlossen?
  - ☐ online
  - ☐ schriftlich
- ☐ Kann der Nutzer auf einen schriftlichen Vertrag bestehen?

## 5.3 Vertragliche Massnahmen

### 5.3.1 Vergütungsregelung

- ☐ Wird die Nutzung des Services pauschal oder zeitabhängig berechnet?
- ☐ Wird die Nutzung des Services nach Verbrauch berechnet?
  - ☐ Existieren Mengenrabatte/unterschiedliche Tarife in Abhängigkeit von der abgenommenen Servicemenge?
  - ☐ Kann der Anbieter seinen Tarif bei signifikanter Änderung des Nutzungsumfangs ändern?
  - ☐ Gibt es eine Best-Price-Option?
- ☐ Wird optional eine Flatrate (Fixpreis) oder per User-Preis angeboten?
- ☐ Gibt es zusätzlich zu verrechnende Sonderleistungen?
- ☐ Wenn ja, welche?

### 5.3.2 Leistungsstörung

- ☐ Leistungsstörung beim Anbieter oder dessen Unterauftragnehmern
  - ☐ Bestehen Regelungen zum Schadensersatz bei Leistungsstörungen?
- ☐ Streit über Leistungserbringung/Zahlungsverzug
  - ☐ Ist ein Zurückbehaltungsrecht an Daten des Nutzers oder ihm gegenüber zu erbringenden Leistungen vertraglich ausgeschlossen?
  - ☐ Ist auch im Fall von Streitigkeiten zur Leistungserbringung oder Zahlungsverzug ausgeschlossen, dass der Anbieter die Daten zurückbehält?

### 5.3.3 Vertragskündigung

- ☐ Welche Kündigungsfristen sind für den Nutzer und den Anbieter definiert?
- ☐ Gibt es eine demonstrative Liste der möglichen (ausserordentlichen) Kündigungsgründe?
- ☐ Wenn ja, für wen?
  - ☐ Nutzer
  - ☐ Anbieter
- ☐ Ist eine Vorankündigung von Änderungen bei der Diensterbringung von Subunternehmern vertraglich geregelt?
- ☐ Existieren Regelungen zur Mitwirkung des Anbieters bei der Datenbereitstellung nach einer Vertragskündigung?

### 5.3.4 Datenlöschung bei Vertragsende

- ☐ Existieren Regelungen zur Löschung der Daten und zur Rückgabe von Datenträgern nach Beendigung des Vertrags?
- ☐ Gewährleistet der Anbieter, dass die Daten auf Wunsch des Nutzers tatsächlich gelöscht werden?

### 5.3.5 Insolvenz des Anbieters

- ☐ Existieren Regelungen zum Schutz der Daten des Nutzers und der Verfügbarkeit der Anwendung bei Insolvenz des Anbieters?
- ☐ Existiert ein Source Code Escrow?
- ☐ Ist die Software an eine bestimmte Plattform gebunden?
- ☐ Wird dem Auftraggeber ein Recht auf Herausgabe der letzten Datensicherung und Dokumentation eingeräumt?

## 5.4 Abbildung der Compliance Massnahmen

### 5.4.1 Datenschutz

Ist das Vorhaben aus datenschutzrechtlicher Sicht relevant? Werden innerhalb der Anwendung personenbezogene Daten im Sinne des DSG verwendet?

Anmerkung: Zu beachten ist, dass der Begriff der „personenbezogenen Daten“ im Sinne des DSG sehr weit gefasst ist. Alle Angaben, die einen Personenbezug haben oder bei denen der Nutzer, der Anbieter oder ein Dritter einen Personenbezug herstellen könnte, gelten aus Sicht des Datenschutzgesetzes als „personenbezogene Daten“, und zwar sowohl bezüglich natürlicher als auch juristischer Personen. In der Praxis wird es nur sehr wenige IT- und Cloud-Anwendungen geben, bei denen Daten verarbeitet werden, die nicht zumindest teilweise personenbezogen sind.

- ☐ Organisation
  - ☐ Ist die Datensammlung – soweit erforderlich – beim EDÖB registriert?
  - ☐ Sind die Mitarbeiter des Anbieters nachweislich zur Einhaltung von Geheimhaltungspflichten und Verwertungsverboten verpflichtet?
  - ☐ Ist geregelt, wer gegenüber dem Kunden seitens des Anbieters, Ansprechpartner in datenschutzrechtlichen Angelegenheiten ist?
  - ☐ Sind Regeln für die Berichtigung, Löschung und Sperrung von Daten auf Antrag eines Betroffenen definiert?
- ☐ Auswahl Anbieter und Subunternehmer
  - ☐ Bietet der Anbieter genügend Informationen zu seinem Unternehmen und seinen Unterauftragnehmern, um dem Nutzer eine gut begründete Auswahl gemäss Art. 10a DSG zu ermöglichen?
  - ☐ Werden die Unterauftragnehmer bekanntgegeben?
- ☐ Datenschutzniveau
  - ☐ Ist auch ausserhalb der EU (auch bei beteiligten Unterauftragnehmern) ein angemessenes Datenschutzniveau (z.B. über EU-Standardvertrag, Safe-Harbour-Regelung etc.) hergestellt?
  - ☐ Besteht die Möglichkeit, wenn aufgrund von gesetzlichen oder behördlichen Auflagen an den Auftraggeber erforderlich, die Orte der Datenhaltung auf die Schweiz oder die EU einzugrenzen?

### 5.4.2 Datenarchivierung

Es bestehen eine Reihe von Sondernormen zu unternehmens- und steuerrechtlichen Aufbewahrungspflichten bei der Verwendung von elektronischen Datenträgern, so beträgt etwa die Aufbewahrungsfrist der Geschäftsbücher grundsätzlich 10 Jahre.

Zu beachten ist, dass der Nutzer ein Interesse daran haben kann, Unterlagen für eine längere Dauer aufzubewahren, und zwar namentlich, um in zivil- und verwaltungsrechtlichen Verfahren die eigenen Rechte besser wahrnehmen zu können.

Im Fall von SaaS muss somit bei elektronischer Bearbeitung und Archivierung beim SaaS-Anbieter sichergestellt sein, dass die betroffenen Daten (etwa elektronische Rechnungen, Bücher, Aufzeichnungen und sonstige Unterlagen) während der gesetzlichen Aufbewahrungsfristen sicher aufbewahrt werden und deren vollständige, geordnete und inhaltsgetreue Wiedergabe, auch an die Behörden möglich ist.

Weiter muss ein Prozess einer kontinuierlichen Rückübermittlung solcher Daten an den Auftraggeber gewährleistet sein.

Folgende Punkte sind zu beachten:

- ☐ Sind für die als SaaS betriebene Anwendung besondere Vorschriften betreffend Archivierung und Datenhaltung zu beachten?
- ☐ Werden im Rahmen der Anwendung elektronische Rechnungen verarbeitet?
- ☐ Werden im Rahmen der Anwendung Daten verarbeitet, die direkt in die Buchführung des Nutzers einfliessen?
- ☐ Falls besondere Vorschriften (bspw. ElDI-V) anzuwenden sind: Werden die Verpflichtungen des Nutzers gegenüber der Finanzbehörde durch den Anbieter unterstützt?
- ☐ Falls besondere Vorschriften (ElDI-V) anzuwenden sind: Werden die Verpflichtungen des Nutzers gegenüber der Finanzbehörde durch den Anbieter unterstützt?
- ☐ Weitere

### 5.4.3 Beauftragung und Weisungsrecht

- ☐ Sind die Verantwortlichkeiten zwischen Nutzer (grundsätzliche datenschutzrechtliche Verantwortlichkeit) und Anbieter (Umsetzung von Weisungen, technischen Schutzmassnahmen etc.) sauber definiert?
- ☐ Ist der Umfang des Auftrags zur Daten-Bearbeitung hinreichend klar spezifiziert, insbesondere:
  - ☐ Ist der Dienst beschrieben? Sind in der Beschreibung der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Bearbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen dokumentiert?
  - ☐ Ist die Dauer der Bearbeitung exakt definiert?
  - ☐ Ist dokumentiert, ob und wenn ja wie sensible Daten erhoben, verarbeitet oder genutzt werden?
- ☐ Ist die Löschung der Daten geregelt?

- ☐ Ist ein Entscheidungsspielraum des Dienstleisters zur Bearbeitung der Daten ausgeschlossen?
- ☐ Ist das Weisungsrecht des Nutzers eindeutig definiert?

### 5.4.4 Kommunikation

- ☐ Ist eine Kommunikationsregel etabliert für den Fall, dass Weisungen des Nutzers nach Meinung des Anbieters gegen den Datenschutz verstossen?
- ☐ Sind Sachverhalte definiert, die als mitzuteilende Verstösse des Anbieters oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen dem Nutzer angezeigt werden müssen?

### 5.4.5 Dokumentation

- ☐ Existiert eine Dokumentation/ein Konzept, welche technischen und organisatorischen Massnahmen der Anbieter umzusetzen hat?
- ☐ Hat der Nutzer ein Vetorecht, wenn der Anbieter dieses Konzept (und Änderungen daran) umsetzen will?

### 5.4.6 Kontrollmöglichkeiten des Nutzers

- ☐ Existieren Regelungen zu Kontrollrechten des Nutzers und zu den entsprechenden Duldungs- und Mitwirkungspflichten des Anbieters?
- ☐ Ist ein Kontrollrecht des Nutzers und/oder eines vom Anbieter beauftragten Dritten vor Ort beim Anbieter oder seinen Subauftragnehmern ausdrücklich vereinbart?
- ☐ Existieren (kumulativ oder alternativ zu den Kontrollen durch den Nutzer) regelmässige Kontrollen/Audits und Zertifizierungen, die den Datenschutz beim Anbieter und die Verpflichtungen gegenüber dem Anbieter kontrollieren und zertifizieren?
- ☐ Ist eine Regelung zur Mitwirkung des Anbieters und den entstehenden Kosten getroffen?

### 5.4.7 Überbindung auf Subunternehmer

- ☐ Hat der Anbieter seine Subunternehmer an dieselben Verpflichtungen gebunden, die er gegenüber dem Nutzer eingeht?
- ☐ Bedarf der Einsatz/Wechsel von Subunternehmern der Zustimmung vom Nutzer?

### 5.4.8 Abbildung der Security Massnahmen

Verträge über Cloud Services sollten in einem Abschnitt, oft in einem Anhang, die sicherheitsrelevanten Vorgaben an den Dienstleister nennen.

Die Ausführungen in Ziffer 6 beschreiben die massgeblichen Anforderungen.

# 6 Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit)

## 6.1 Grundlagen

Für ein zuverlässiges und sicheres Cloud Computing ist als Grundlage ein effizientes Management der Informationssicherheit (Information Security Management System, ISMS) auf Seiten des CSP unerlässlich. Es empfiehlt sich, sich für Aufbau und Betrieb eines ISMS an ISO 27001/2 oder am BSI-Standard 100-2 zur IT-Grundschutz-Vorgehensweise (der ISO 27001/2 abdeckt) zu orientieren.

Wesentliche Bestandteile eines ISMS sind eine funktionierende Sicherheitsorganisation und ein Informationssicherheitskonzept als Werkzeuge des Managements zur Umsetzung der Sicherheitsstrategie.

Ein CSP sollte die Sicherheitsorganisation nutzen, um hierüber geeignete Ansprechpartner für seine Kunden zu benennen, die Sicherheitsfragen der Nutzer beantworten können. Informationssicherheit ist ein Prozess und sollte daher im Sinne eines PDCA Zyklus (Plan-Do-Check-Act) fortlaufend weiterentwickelt werden.

Damit CSPs nachweisen können, dass sie auch bei hohem Schutzbedarf bezüglich Vertraulichkeit und Verfügbarkeit ausreichend Sicherheit gewährleisten, ist eine Zertifizierung des Informationssicherheitsmanagements sinnvoll. Vorzugsweise sollten CSPs nach ISO 27001 auf Basis von IT-Grundschutz, ISO 27001 oder einem anderen etablierten Standard zertifiziert sein.

Für die Security Anforderungen wird, basierend auf der Graphik in Ziffer 3, S. 13, nach IaaS, PaaS und SaaS unterschieden.

## 6.2 Für Infrastructure as a Service (IaaS)

### 6.2.1 Massnahmen im Rechenzentrum

Rechenzentren sind die technische Basis von Cloud Computing. Insofern ist es wichtig, dass jeder Cloud Services Provider (CSP) die Sicherheit seiner Anlagen nach dem aktuellen Stand der Technik gewährleistet. Folgende Aspekte müssen dabei berücksichtigt werden:

- ☐ Redundante Auslegung aller wichtigen Versorgungskomponenten (Strom, Klimatisierung der Rechenzentren, Internetanbindung, Verkabelung, etc.)
- ☐ Überwachung des Zutritts: Zutrittskontrollsystem, Videoüberwachungssysteme, Bewegungssensoren, Sicherheitspersonal, Alarmsysteme, etc.
- ☐ Zwei-Faktor-Authentisierung für den Zutritt ins Rechenzentrum
- ☐ Brandschutz: Brandmeldeanlage, Brandfrüherkennung, geeignete Löschtechnik, regelmässige Brandschutzübungen
- ☐ Infrastruktur, die ausreichenden Widerstand gegen Elementarschäden und unbefugtes Eindringen bietet, namentlich:

  Redundante Rechenzentren, die mindestens so weit voneinander entfernt sind, dass ein Schadensereignis nicht gleichzeitig das ursprünglich genutzte Rechenzentrum und das, in dem die Ausweichkapazitäten genutzt werden, beeinträchtigt

### 6.2.2 Massnahmen betreffend Serversicherheit

Serversicherheit bildet die Basis für jeglichen Betrieb von Betriebs-, Managementsystemen sowie Middleware- und Softwareprodukten.

Darauf bezogene Massnahmen sind namentlich:

- ☐ Technische Massnahmen zum Schutz der Server (Host Firewalls, regelmässige Integritätsüberprüfungen, Server-based Intrusion Detection Systems)
- ☐ Sichere Grund-Konfiguration der Server (z. B. Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste, etc.)
- ☐ Möglichkeit, für Kunden eigene Images für virtuelle Maschinen einzusetzen oder qualitätsgesicherte Images des Providers zu nutzen (nur bei IaaS, bei PaaS/SaaS: Sichere Default-Konfiguration des Gastbetriebssystems durch den Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste, etc.)

### 6.2.3 Massnahmen betreffend Netzsicherheit

Netzsicherheit ist kein klar definierter Begriff, sondern umfasst sämtliche Massnahmen zur Planung, Ausführung und Überwachung der Sicherheit in Netzwerken. Diese Massnahmen sind keinesfalls nur technischer Natur, sondern beziehen sich auch auf die Organisation, den Betrieb und schlussendlich auch auf die rechtlichen Anforderungen.

- ☐ Sicherheitsmassnahmen gegen Malware (Virenschutz, Trojaner-Detektion, Spam-Schutz, etc.)
- ☐ Sicherheitsmassnahmen gegen netzbasierte Angriffe (IPS/IDS-Systeme, Firewall, Application Layer Gateway,etc.)
- ☐ DDoS-Mitigation (Abwehr von DDoS-Angriffen)
- ☐ Geeignete Netzsegmentierung (Isolierung des Management-Netzs vom Datennetz)
- ☐ Sichere Konfiguration aller Komponenten der Cloud-Architektur
- ☐ Fernadministration durch einen sicheren Kommunikationskanal (z. B. SSH, IPSec, TLS/SSL, VPN) Verschlüsselte Kommunikation zwischen Cloud Computing Anbieter und Cloud Computing Nutzer (z. B. TLS/SSL)
- ☐ Verschlüsselte Kommunikation zwischen Cloud Computing Standorten
- ☐ Verschlüsselte Kommunikation mit Drittdienstleistern, falls diese für das eigene Angebot notwendig sind
- ☐ Redundante Vernetzung der Cloud-Rechenzentren

### 6.2.4 Massnahmen betreffend Datensicherheit

Beim Begriff Datensicherheit handelt es sich um eine Definition, welche im Rahmen der DIN 44300 festgelegt ist, und Daten in der EDV zum einen vor Datenverlust, zum anderen aber auch vor unberechtigtem Zugriff oder unrechtmässiger Veränderung durch Dritte bewahren soll.

- ☐ Datensicherheit im Lebenszyklus der Kundendaten definieren und umsetzen
- ☐ Sichere Isolierung der Kundendaten (z. B. virtuelle Speicherbereiche, Tagging, etc.)
- ☐ Regelmässige Datensicherungen, deren Rahmenbedingungen (Umfang, Speicherintervalle, Speicherzeitpunkte und Speicherdauer) für die Kunden nachvollziehbar sind.
- ☐ Daten müssen auf Wunsch des Kunden vollständig und zuverlässig gelöscht werden
- ☐ Starke Authentisierung (Zwei-Faktor-Authentisierung) für Administratoren des CSP
- ☐ Rollenbasierte Zugriffskontrolle und regelmässige Überprüfung der Rollen und Rechte
- ☐ Least Privilege Model (Nutzer bzw. CSP-Administratoren sollen nur die Rechte besitzen, die sie zur Erfüllung ihrer Aufgabe benötigen
- ☐ Vier-Augen-Prinzip für kritische Administrationstätigkeiten
- ☐ Starke Authentisierung (z. B. Zwei-Faktor-Authentisierung) für Cloud-Kunden

### 6.2.5 Massnahmen betreffend Notfallmanagenemt

Notfallmanagement: Das Notfallmanagement umfasst alle Massnahmen, die es braucht, einen Desaster-Fall, wie z.B den Ausfall eines Rechenzentrums, abzudecken.

- ☐ Der Cloud-Anbieter muss ein Notfallmanagement aufsetzen und betreiben
- ☐ Der CSP muss seinen Kunden die Priorisierung des Wiederanlaufs für die angebotenen Cloud-Dienste transparent machen
- ☐ Regelmässige Notfall-Übungen (z. B. zu Ausfall eines Cloud Computing Standorts)
- ☐ Der CSP sollte nachweisen, dass sein Notfallmanagement auf einem international anerkannten Standard wie z. B. ISO 25999 oder BSI-Standard 100-4 basiert (z. B. anhand Notfallvorsorgekonzept und Notfallhandbuch)

## 6.3 Für Platform as a Service (PaaS)

Die vorstehend für IaaS angebrachten Empfehlungen kommen auch für PaaS zum Tragen. Zusätzlich ist für PaaS Folgendes anzumerken:

- ☐ Sicherheit muss Bestandteil des Software Development Life Cycle-Prozesses sein (Reviews, Automatisierte Tests, Vulnerability Tests, etc.)
- ☐ Sichere Isolierung der Anwendungen (PaaS)
- ☐ Einhaltung von Sicherheits-Mindeststandards der zur Verfügung gestellten Webanwendungen (z. B. Prinzipien zur sicheren Software-Entwicklung nach OWASP)
- ☐ Richtlinien für Kunden zur Erstellung von sicheren Anwendungen (PaaS)
- ☐ Automatische Überprüfung von Kunden-Anwendungen auf Anwendungs-Schwachstellen, insbesondere vor Inbetriebnahme (PaaS)
- ☐ Patch- und Änderungsmanagement (zügiges Einspielen von Patches, Updates, Service Packs) sowie Release Management
- ☐ Sicherstellung der Patchverträglichkeit auf Testsystemen vor Einspielen in Wirkbetrieb

## 6.4 Für Software as a Service (SaaS)

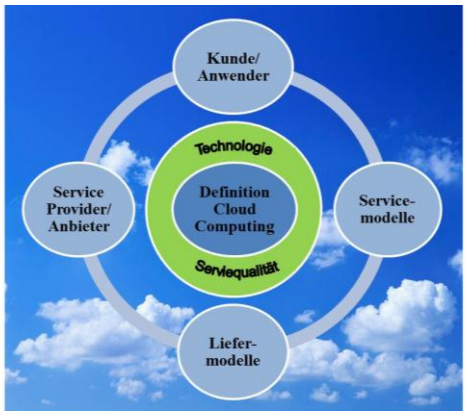
Die vorstehend für IaaS und PaaS angebrachten Empfehlungen kommen auch für SaaS zum Tragen. Zusätzlich ist für SaaS Folgendes anzumerken:

- ☐ Mandantenfähigkeit prüfen
- ☐ Berechtigungskonzept und Zugriffsmanagement prüfen
- ☐ Releasemanagement und Maintenance sicherstellen
- ☐ Offenheit und Schnittstellen prüfen
- ☐ Skalierbarkeit, Preis- und Verrechnungsmodell klären
- ☐ Browserfähigkeit resp. Portabilität sicherstellen
- ☐ Anpassbarkeit und Supportoptionen klären

# 7 Glossar Cloud Computing

Ein Paradigmawechsel führt meistens dazu, dass zu Beginn Begriffe von Seiten Anbietern und Beratern unklar definiert sind, unterschiedlich interpretiert und ausgelegt werden. Mit der Zeit konsolidieren sich dann meistens die Begriffe zu Themenbereichen und führen zu einer gemeinsamen Sprache. Zusätzlich zu den Begriffen kommt die Sicht des Betrachters und Nutzers, denn dieser sollte auch das gleiche verstehen und daraus seinen Nutzen erkennen und ableiten können.

Mit Cloud Computing haben sich folgende Themenbereiche, Begriffe und Sichten entwickelt:




**Definition Cloud Computing**

„Cloud Computing ist ein Modell, das es erlaubt, bei Bedarf, jederzeit und überall bequem über ein Netz auf einen gemeinsam genutzten 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. (NIST, National Institute of Standards and Technology)

**Technologie**

Jeder Cloud Service beinhaltet, abhängig vom Angebot einen in sich abgestimmten Technologiepool der von mehreren Kunden unabhängig über das Internet genutzt wird. Das heisst, dass Operating System, Server- und Storage-Infrastruktur mit der Middleware und Anwendung abgestimmt werden müssen. Die im Pool eingesetzten Technologien sind abhängig von den Kombinationsmöglichkeiten der gewählten Technologie Anbietern.

**Servicemodelle**

Cloud Services sind On-Demand-Software- (Anwendungen, Betriebssysteme, Middleware, Management- und Entwicklungs-Tools) sowie On-Demand-Infrastruktur-Services (Hardware, Speicher, Netze), die webbasiert und mandantenfähig sind und jeweils dynamisch an die Erfordernisse der Geschäftsprozesse angepasst werden können. Bei den Servicemodellen unterscheidet man folgende drei Ebenen:

**Infrastructure as a Service (IaaS)**

Der Cloud Service beinhaltet über das Internet, auf Subskriptionsbasis (On Demand) genutzte IT-Infrastruktur wie Platz, Klima, Netzwerk, Server, Speicher bis zum Betriebssystem und dem zugehörigen Betriebs-Monitoring. Auf diesem Service können von Nutzern jeweils individuelle Middleware- und/oder Anwendungsumgebungen frei implementiert und genutzt werden.

**Platform as a Service (PaaS)**

PaaS baut auf IaaS auf. Diese Dienstleistung ermöglicht es dem Nutzer, seine benötigte Middleware (Tools, Datenbanken etc.) On Demand zusammenzustellen. Die Anbieter können auf der Plattform für Ihre Nutzer oder ihre eigene Anwendungssoftware entwickeln, betreiben und über das Internet nutzen.

**Software as a Service (SaaS)**

SaaS baut auf PaaS und IaaS auf und ist die angebotene Dienstleistung, die dem Nutzer den grössten Nutzen bringt. Die Anwendungssoftware ist über den Browser On Demand, mobil und kann von vielen Standorten von mehreren Usern gleichzeitig genutzt werden.

**Public Cloud**

Die Public Cloud kann von beliebigen Anwendern (Privatpersonen oder Unternehmen) genutzt werden. Sie steht öffentlich zur Verfügung und die Nutzer sind nicht mehr abhängig von interne IT Ressourcen und eigenen Investitionen.

**Hybrid Cloud**

Hybrid Cloud ist eine Kombination zwischen Public Cloud Services, Private Cloud Services und oder in Verbindung mit dedizierten, Firmen spezifischen IT Lösungen. Das Modell kann einerseits somit individuell auf die konkreten Anforderungen des jeweiligen Nutzers ausgerichtet werden, andererseits kommen solche Ansätze immer auch in Umstellungs- phasen von In-House zu Cloud Computing vor.

**Service Provider**

Service Provider sind Anbieter von Cloud Services (IaaS, PaaS oder SaaS). Sie sind die verantwortlichen Ansprechpartner für die Anwender und haben mit ihnen einen Dienstleistungsvertrag für die Nutzung der angebotenen Cloud Services.

**Kunde/Anwender/Nutzer**

Kunden/Anwender/Nutzer können abhängig von den Cloud Services Privatpersonen oder Unternehmen sein. Anwender sind verantwortlich, dass Ihre Anforderungen bezüglich Datenhaltung, Sicherheit und Risiken über den Vertrag mit dem Service Provider abgedeckt sind.

**Liefermodelle**

Werden die Cloud Services nach dem Anwendungszweck unterschieden, so gibt es zur Zeit folgende vier Liefermodelle: Public Cloud – Private Cloud – Community Cloud – Hybrid Cloud (siehe nachfolgende Darstellung im Einzelnen).

**Private Cloud**

Hier werden die Cloud Services in einem geschlossenen Netzwerk, wie z.B. innerhalb eines Firmen-Intranets bereit gestellt. Das Rechenzentrum und die IT Ressourcen werden vom Unternehmen selbst betrieben und verwaltet.

**Community Cloud**

Bei diesem Modell handelt es sich fast ausschliesslich um Services, die von einigen oder mehreren Unternehmen mit gleichen oder ähnlichen Anforderungen oder aus der gleichen Branche gemeinsam genutzt werden. In der Regel besteht das Liefermodell auf dem Konzept eines Public Clouds, wird aber nur von einem bestimmten Kundenkreis genutzt

**Servicequalität**

Die Anforderungen an die Servicequalität ist einerseits pro Anwender oder Anwendergruppe individuell. Andererseits für die Service Provider ein entscheidender Faktor für Ihren Erfolg. Sie müssen ihre Servicequalität auf ihre Kundenbedürfnisse ausrichten.

# 8 Quellennachweise

BSI: Sicherheitsempfehlungen für Cloud Computing Anbieter

PAC Outsourcing Research Programm von Karsten Leclerque / September 2010 “Cloud vs. Out-Sourcing: Cloutsourcing 2020”

IDC Whitepaper von Holger Eriksdotter / 6.5.2011 “Gründe für Cloud Computing ändern sich”

Kommentar zur Cloud-Computing-Strategie der Schweizer Behörden, Bern, 14.11.2011.

„Cloud Computing in Deutschland“ Umfrage von Deloitte und BITKOM, Februar 2011

„Cloud Computing in Switzerland“ Umfrage von Cambridge Technology Partners, September 2011

„Pan European Study“ Umfrage von Easynet, Mai 2011

# 9 Abkürzungen

| | | | |
|---|---|---|---|
| **AGB** | Allgemeine Vetragsbestimmungen | **IPS / IDS** | Intrusion prevention System / Intrusion detection System |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik | **ISDS** | Informationssicherheit- und Datenschutzkonzepte |
| **Capex** | Capital expenditure | **ISMS** | Information Security Management System |
| **CRM** | Customer Relationship Management | **ISO** | International Organization for Standardization |
| **CSP** | Cloud Service Provider | **IT** | Informations Technologie |
| **DDoS** | Distributed Denial of Service | **Opex** | Operational expenditure |
| **DIN** | Deutsche Industrie Norm | **OWASP** | Open Web Application Security Project |
| **DLP** | Data Loss Prevention | **PET** | Privacy Enhancing Technology |
| **DSP** | Datenschutz | **PaaS** | Platform as a Servive |
| **EDÖB** | Eidgenössicher Datenschutz- und Öffentlichkeitsbeautragte | **PDCA** | Plan-Do-Check-Act |
| **EDV** | Elektronische Daten verarbeitung | **SaaS** | Software as a Service |
| **IaaS** | Infrastructure as a Service | **SSH** | Secure Shell |
| **ICT** | Information and Communication Technology | **SSL** | Secure Socket Layer |
| **IP** | Internet Protocoll | **TCO** | Total Cost of Ownership |
| **TLS** | Transport Layer Securi- | **VPN** | Virtual private Network |
| **VIS** | Verordnung über die Informatiksicherheit | | |

## 10 Autoren

Heinz Dill, Geschäftsführer CBusiness Services GmbH / EuroCloud Swiss

Yvonne Thoma, Business Manager Utility & Cloud Services Hewlett-Packard (Schweiz) GmbH / EuroCloud Swiss

Prof. Dr. Stella Gatziu Grivas, Dozentin Fachhochschule Nordwestschweiz, Leiterin Kompetenzschwerpunkt Cloud Computing

Alain Beuchat, Partner IT Advisory, KPMG AG, Zürich

Dr. Christian Laux, Rechtsanwalt, LAUX LAWYERS, Zürich

Marco Marchesi, President & Chairman, ISPIN AG, Zürich

Ueli Brügger, Managing Security Consultant, Information Security Society Switzerland (ISSS)

**EuroCloud Swiss**
Verein zur Förderung von Cloud Computing
8000 Zürich

E-Mail: info@eurocloudswiss.ch
Web: www.eurocloudswiss.ch