CLOUD Rules & Regulations –

SFTI Position Paper (V1; Insurance Perspective)

Versionen

Version	Verfasser	Datum
0.1	Initialversion	
0.9	Version überarbeitet	03.10.2017
0.95	Input von Axa und Helvetia aufgenommen	11.11.2017
0.96	SFTI Sitzung vom 17.11.	17.11.2017
0.97	Nachbearbeitung, TM	18.12.2017
0.98	Anonymisierung, LH	08.05.2018
0.99	SFTI-Template, LH	08.07.2018
1	Finalization formatting, STE	09.07.2018

Inhaltsverzeichnis

1 Zweck des Dokuments

Dies Dokument hat das Ziel, die intern abgestimmte Position der Arbeitsgruppe Cloud, Versicherungen, festzulegen.

2 Auftrag an Arbeitsgruppe

Die Arbeitsgruppe hat festgelegt, dass sie ein Positionspapier erarbeiten möchte. Auf Basis dieses Papiers soll dann nachfolgend eine Abstimmung mit den Behörden (2) und ausgewählten Cloud Lieferanten (3) erfolgen.

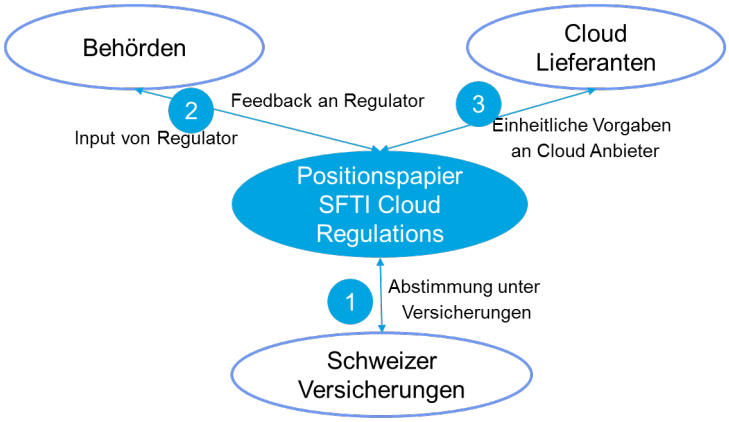

Abbildung 1: Kontextdiagramm der Arbeitsgruppe

3 Begriffe

3.1 Auslegung Cloud Computing

Cloud Computing ist ein viel benutzter Begriff. Idealerweise sichert Cloud Computing eine Transparenz für den Nutzer in drei Dimensionen (siehe **Fehler! Verweisquelle konnte nicht gefunden werden.**).

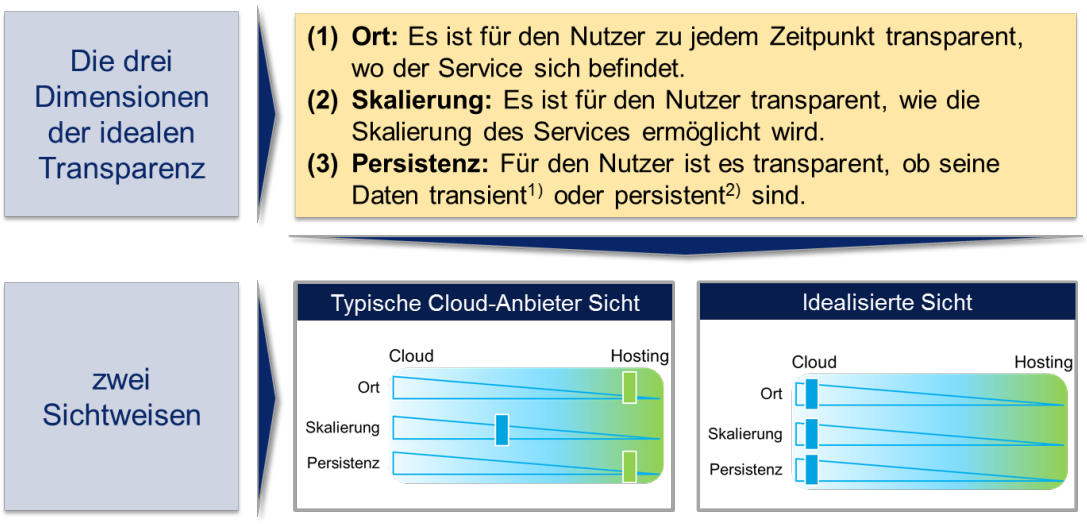

Abbildung 2: Dimensionen des Cloud-Computings

In der Praxis zeigt sich, dass bei jeder Dimension Einschränkungen möglich und auch erwünscht sind. Gleichwohl spricht man auch bei hohem Einschränkungsgrad von Cloud-Computing.

3.2 Service Modelle

In der Regel wird in folgende Servicemodelle unterschieden, wenn man Cloud Computing näher analysiert:

- Infrastruktur als ein Service (IaaS)
- Plattform als ein Service (PaaS)
- Software als ein Service (Saas)

In der **Fehler! Verweisquelle konnte nicht gefunden werden.** werden die verschiedenen Servicemodelle tabellarisch dargestellt und der On-Premise Variante gegenübergestellt. Die vertikale Achse beschreibt in Anlehnung an das ISO/OSI Modell die verschiedenen Schichten, beginnend mit der Schicht für Netzwerke und endend mit der Applikationsschicht.

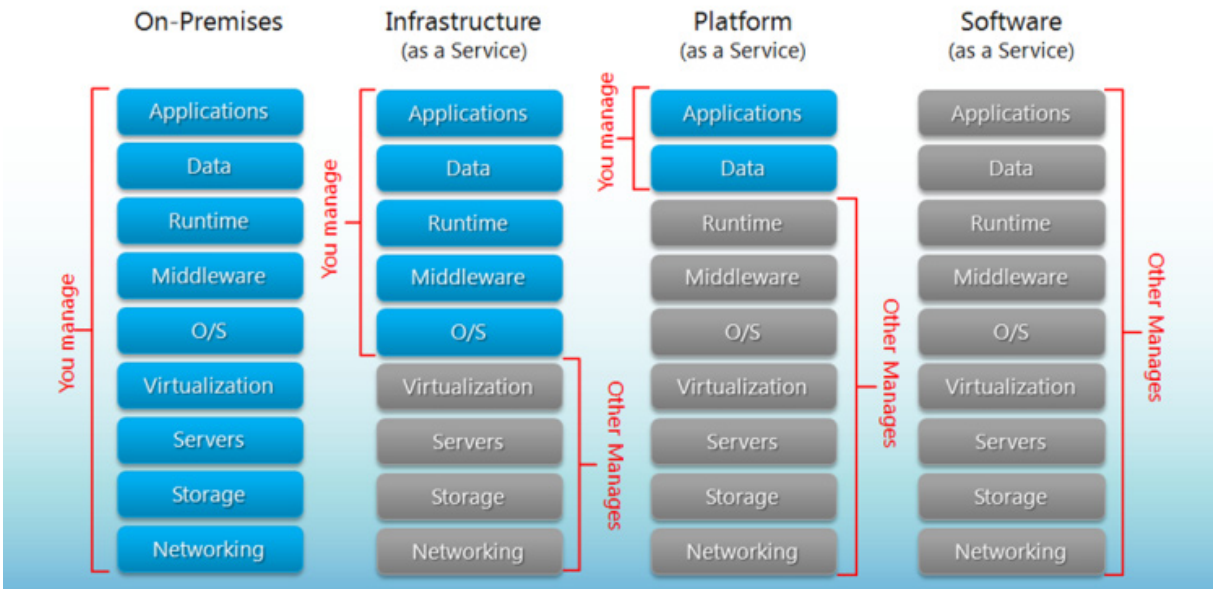

Abbildung 3: On-Premise und die verschiedenen Servicearten für Cloud Computing; Quelle http://www.hostingadvice.com/how-to/iaas-vs-paas-vs-saas/

Die Farben zeigen an, ob die Verwaltung der entsprechenden Schicht selbst oder durch Dritte erbracht wird. Es ist zu sehen, dass bei On-Premise alle Schichten noch selbst geleistet werden, während im Falle von SaaS alle Schichten vom Cloud-Dienstleister erbracht werden. Der Grad der Herausgabe von Services steigt als in der Abbildung von links nach rechts an.

3.3 Cloud-Strategie

3.3.1 Typische Gründe für Cloud-Lösungen

In der Regel wird zuerst aus **ökonomischer Sicht** für eine Cloud-Lösung plädiert. Dieses Argument verliert aber mit der Zeit an Gewicht. Dann stehen andere Argumente im Vordergrund.

Es ist auch zu festzustellen, dass vermehrt **neuartige und differenzierende Services** nur aus der Cloud angeboten werden. Eine Nutzung von solchen Services bedingt, dass das Unternehmen sich in die Lage versetzen muss, auch Cloud Services zu konsumieren. Hier sind als Beispiel Services zu nennen, die auf einer einzigartigen Rekombination von bestehende Services basieren oder etwa Algorithmen, die auf **Machine Learning** Mechanismen aufbauen.

Aus den Erfahrungsberichten kann man entnehmen, dass die **Innovationskraft** von Cloud-Anbietern zum Teil erheblich höher ist als dies von vielen Inhouse IT Abteilungen geleistet werden kann. Cloud Computing wird als Schlüssel gesehen, um die schnelle **digitale Transformation** innerhalb und ausserhalb von Unternehmen besser umzusetzen als das mit herkömmlichen Mitteln der Fall ist. Viele Unternehmen stellen ihr herkömmliches Entwicklungsverfahren um auf ein agiles Vorgehen. Sie versprechen sich davon, dass sie die sich schnell ändernenden und meist diffusen Anforderungen besser begegnen können.

Desweitern wird die **Skalierbarkeit** von Cloud-Anbietern ins Feld geführt. Intern ist der personelle und zeitliche Aufwand oft erheblich, um neuartige Lösungen auf die Beine zu stellen. Hier ist der professionelle Cloud-Anbietern meist überlegen. Schliesslich wird auch das **hohe Niveau der Security** von Cloud-Anbietern vorgebracht.

3.3.2 Multi-Cloud-Strategie

Viele grosse Software-Hersteller propagieren das Cloud-Computing. Aus Sicht des Cloud-Nutzers kann hier die Diskussion aufkommen, ob und wie mehrere Cloud-Lösungen miteinander kombiniert werden können.

Aus Sicht von bereits erfahrenen Unternehmen ist es eine grosse Herausforderung, eine Multi-Cloud-Strategie zu fahren. Als grösste Hindernisse für eine Multi-Cloud-Strategie für Pass und SaaS werden gesehen:

- Falls mehrere Cloud-Anbieter beteiligt wären, müsste die zeitlich miteinander abgestimmt sein. Dies ist völlig unmöglich.
- Der organisatorische Aufwand inklusive der rechtlichen Abklärungen ist hoch. Aus arbeitsöknonomischen Gründen wird der Cloud-Nutzer versuchen, hier die Anbieterzahl nicht gross werden zu lassen.

Es muss jedoch erwähnt werden, dass ein Unternehmen aus der Arbeitsgruppe schon auf dem Weg zu einer Multi-Cloud-Strategie ist. Es wurde eine OpenPaaS-Plattform entwickelt, über die langfristig die virtuellen Cluster transferiert werden können. Es soll jedoch nicht verschwiegen werden, dass bei der Automation zur Lastverteilung noch offene Punkte bestehen. Der Grund ist hier in den unterschiedlichen Technologiestapeln zu finden.

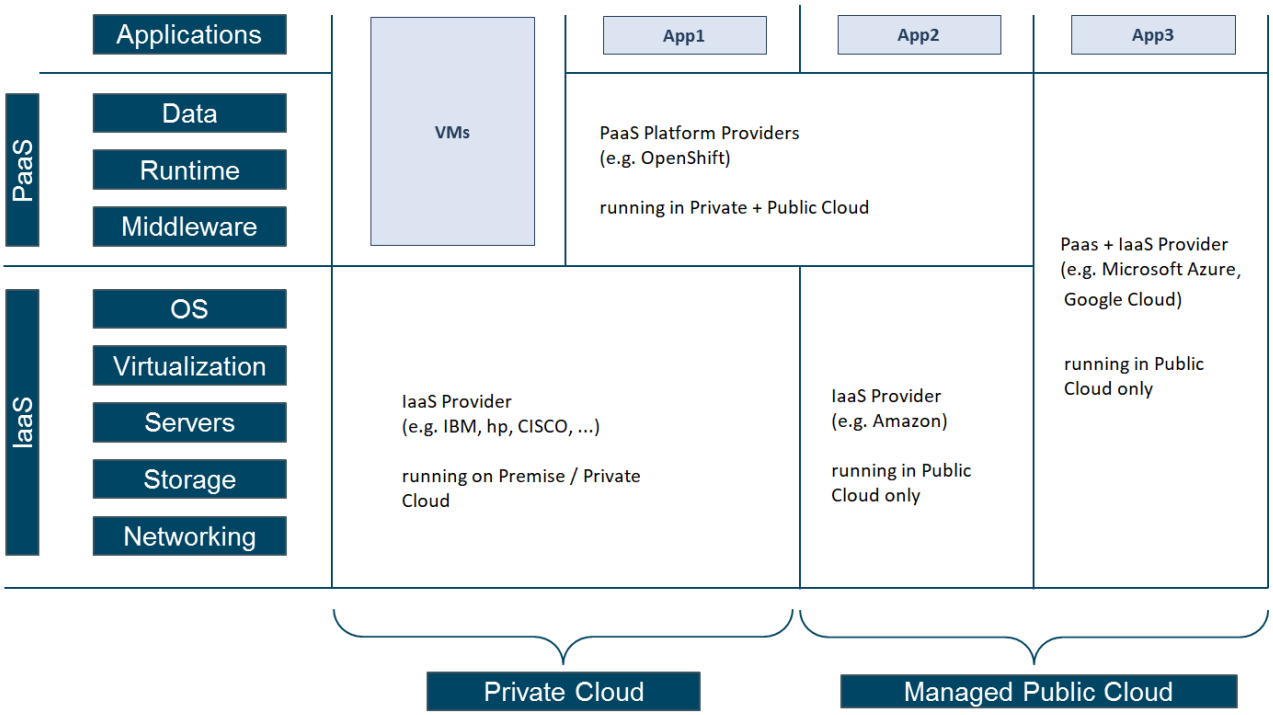

Abbildung 4: Beispiel für den Technologie Stack für eine Multi-Cloud-Strategie

3.3.3 Entscheidungsbaum für Cloud-Computing

Wie bereits oben ausgeführt gibt es unterschiedliche Servicemodelle für das Cloud Computing. Neben den erwähnten Servicemodellen kann noch unterschieden werden in: öffentlich und private Cloud-Modelle. Ein wichtiges Kriterium für den Entscheid privat oder öffentlich sind Sicherheitsaspekte. Bei sehr hohen Anforderungen wird aus heutiger Sicht die Tendenz eher zu einer private Cloud gehen. In der untenstehenden Abbildung ist ein Entscheidungsbaum aus der Praxis zu sehen.

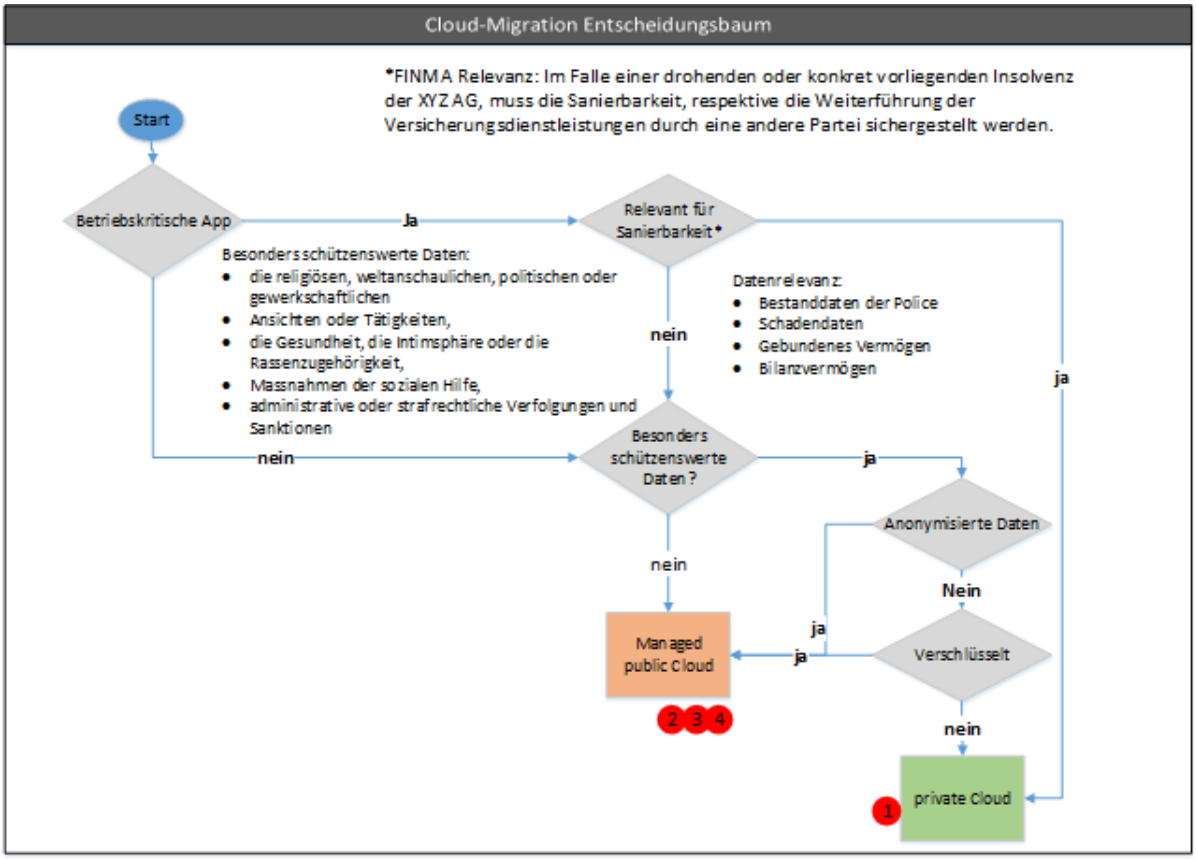

Abbildung 5: Entscheidungsbaum für Cloud-Computing

3.4 Anpassung des Geschäftsplans

Die Einführung von Cloud-Computing für Kernprozesse wird in der Regel zu einer **Geschäftsplanänderung** führen, wenn es die Kernprozesse betrifft. Grundlage ist das VAG. Eine Kontaktaufnahme zur Klärung der Sachlage mit der Finma hat sich nach bisherigen Erfahrung immer als sinnvoll herausgestellt. Insofern ist hier den Anliegen der Aufsichtsbehörden besonders Rechnung zu tragen.

4 Überblick zu den verschiedenen Aspekten im Cloud-Computing

Sinnvollerweise definiert der Auftraggeber zum vornherein, für welche Arten von Daten und betroffene Geschäftsprozesse überhaupt Cloud Computing in Frage kommen kann. Sollen auch besonders schützenswerte Personendaten oder Teile von Prozessen in die Cloud ausgelagert werden, muss man sich den Risiken einer Auslagerung solcher Daten umso mehr bewusst sein, da insbesondere auch das Reputationsrisiko bedeutend höher ist.

Rechtliche Aspekte	Vollumfängliches Auditier-Recht zum ausgelagerten Geschäftsbereich	Grenzüberschreitende Datenbekanntgabe
	Schweigepflicht und Überbindung an alle Involvierten	Sicherstellung der Auskunfts-, Berichtigungs-und Löschrechte
	Exit Szenario im Insolvenz Fall des Cloud Anbieters. Repatriierung – Szenarien für einen möglichen Rückführungsfall erarbeiten (Highlevel)	Exit Szenario im Insolvenz Fall Versicherung
	Beizug von Dritten	
	Politische Einflussfaktoren in das Risk Management miteinbeziehen	
Interne Informationssicherheitsaspekte	Sichere und verschlüsselte Datenablage	Sicherer und stark verschlüsselter Datenverkehr
	Interne Risikobeurteilung mit allen wichtigen Stakeholdern	Relevante, neue IT-Governance Kontrollpunkte und deren Prüfung
	Autorisierung und sichere Authentisierung der Benutzer	
	Feste Kriterien und Generischer Prozess erarbeiten zur Klassifizierung der unterschiedlichen Cloudlösungen	
Lieferantenspezifische Aspekte	Analyse des Cloud-Vertrags / AGB zur Identifikation notwendiger Erweiterungen	ISO Zertifizierungen und Audit Reports zum Cloud Dienst & Lokation

Tabelle 1: Überblick zu den verschiedenen Aspekten

5 Rechtliche Aspekte

5.1 Einleitung

Bei der Ausarbeitung der vertraglichen Grundlagen sollte eine ausführliche Risikoanalyse durchgeführt werden. Diese sollte insbesondere die technischen, finanziellen, **operationellen und politischen Risiken** abdecken sowie jene, welche sich aus dem operativen Geschäftsbetrieb des Anbieters ergeben, umfassen. Eine Bonitätsprüfung des Anbieters sollte dies ergänzen. Es ist zu beachten, dass diese Prüfung auch nach Vertragsabschluss regelmässig, das heisst mindestens alle Jahre durchgeführt wird. Sinnvollerweise wird dazu eine standardisierte Checkliste, welche spezifisch an die Bedürfnisse des Auftraggebers angepasst wurde, verwendet. Aufgrund einer möglichen Konkursabwicklung eines Providers im Ausland können die Länder aufgrund politischer Unruhen verhindern, dass die Daten in die Schweiz rückgeführt werden können (Repatriierung).

Es ist schwierig die rechtlichen Grundlagen aus heutiger Sicht zu beurteilen, da sowohl das DSG wie auch das Rundschreiben noch in der Entwurfsphase sind.

5.2 Auditierungsrecht

Dem Auftraggeber und möglichen Aufsichtsbehörden ist ein Einsichtsrecht auszubedingen.

Der Auftraggeber ist vertraglich zu verpflichten, der FINMA sämtliche Auskünfte und Unterlagen bezogen auf den ausgelagerten Geschäftsbereich zur Verfügung zu stellen, die sie für die Aufsichtstätigkeit benötigt. Falls Prüftätigkeiten an die Revisionsstelle des Cloud Anbieters delegiert werden, ist ihr Bericht der FINMA, der internen Revisionsstelle und der Prüfgesellschaft des auslagernden Auftraggebers auf Anfrage zur Verfügung zu stellen.

Auch bei einer Auslagerung ins Ausland ist sicherzustellen, dass der Auftraggeber und eine allfällige Aufsichtsbehörde ihr Prüfrecht wahrnehmen können.

Der Anbieter von Cloud-Services muss in der Schweiz aufgrund von gesetzlichen Vorgaben das Recht auf Auditierung zulassen. Grundlage hierfür sind das Rundschreiben von der Finma sowie für die Krankenversicherung die Vorgaben durch das BAG.

Das Geschäftsmodell der Anbieter von Cloud-Services basiert auf der Vereinheitlichung ihres Angebots möglichst auf der gesamten Welt. Lokale Abweichungen sind hier nicht willkommen, jedoch ist in letzter Zeit zu beobachten, dass hier manche Anbieter differenziert zu betrachten sind.

➢ *Praxis*

Die Bereitschaft der Anbieter zum Einräumen des Auditierrechts variiert. Manche sind Kooperation und manche sehen es in den Geschäftsmodellen nicht vor.

5.3 Grenzüberschreitende Datenbekanntgabe

Wie in **Fehler! Verweisquelle konnte nicht gefunden werden.** kann die Bestimmtheit des Orts variieren. So kann das Backup einer produktiven Instanz an einem anderen Ort stattfinden.

Die Sanierbarkeit bzw. Abwickelbarkeit des Unternehmens in der Schweiz muss gewährleistet sein. Der Zugriff auf die **sanierungsrelevanten Daten** muss jederzeit in der Schweiz möglich sein. Dies bedeutet, dass das Format für den Export der Daten festgelegt und der Import beim Nutzer in zielführender Zeit möglich sein muss. Der Cloud-Dienstleister muss entsprechende organisatorische und finanzielle Vorsorge treffen, um im Falle der Sanierung mitwirken zu können.

Als ein gangbarer Weg hat sich gezeigt, dass entweder

- die Datenhaltung in der Schweiz erfolgt oder
- Eine aktuelle Kopie der Daten in die Schweiz existiert

Offen ist der Punkt, ob sanierungsrelevante Daten in der Schweiz verarbeitet werden müssen oder lediglich ausgelesen werden können.

➢ *Praxis*

Es sind genau den Ort festzulegen, wo die Daten abgelegt werden dürfen. Das beginnt bei den Nutzdaten und geht bis hin zu den Log Daten und Backupdaten.

Der Dataowner muss sich festlegen, welche Datenkategorien für ein Outsourcing infrage kommen und welche nicht. Er sollte für sich weiter definieren, in welche Länder Daten outsourct werden dürfen und in welche eine Übermittlung ausgeschlossen ist. Grundlage dazu ist eine Kriterienkatalog oder Entscheidungsbaum.

Soll eine Übermittlung ins Ausland vorgenommen werden, so ist darauf zu achten, dass auch von diesem Land ein ausreichender Datenschutz gewährleistet werden kann. Entweder findet sich das Land auf der Liste des eidgenössischen Datenschutzbeauftragten, welches einen ausreichenden Datenschutz gewährleistet oder es sind ergänzende datenschutzrechtliche Bestimmungen zu formulieren.

5.4 Schweigepflicht

Die Schweigepflicht betrifft nicht nur den direkten Vertragspartner, sondern sollte sich auf Dritte erstrecken, welche für die Vertragserfüllung notwendig sind. Konkret bedeutet dies, dass auch Sublieferanten und externe Mitarbeiter unter die Schweigepflicht fallen sollten.

➢ *Praxis*

- Er wurde das Beispiel genannt, dass der Cloud-Lieferant eine Informationspflicht hat, welche Mitarbeiter zur Vertragserfüllung hinzugezogen werden. Änderungen sind ebenfalls mitzuteilen.
- Die Transitivität der Schweigepflicht erstreckt sich über die gesamte Kette. Diese Kette und ihre Dokumentation werden im Vertrag als Pflicht festgehalten.

5.5 Beizug von Dritten

Der Beizug von Dritten (Hilfspersonen) ist von einer vorgängigen Genehmigung oder mindestens Informationspflicht abhängig zu machen. Es ist darauf zu achten, dass diese bezüglich Datenschutz und Informationssicherheit denselben Pflichten unterworfen werden.

5.6 Form

Ein Vertrag muss in schriftlicher Form abgefasst sein.

5.7 Interne Informationsicherheitsaspekte

5.7.1 Verschlüsselung der Datenablage (Data at Rest)

Die Datenablage sollte wenn möglich verschlüsselt abgelegt werden. Jedoch ist zu bemerken, dass eine Verschlüsselung auch gewichtige Nachteile mit sich bringt, die technisch bedingt sind. Verschlüsselte Daten lassen sich nicht indexieren, die Abfragen sind also entsprechend langsamer als mit einer Indizierung.

➢ *Praxis*

In der Praxis hat es sich bewährt, die nicht öffentlichen Daten zu verschlüsseln und dass der Schlüssel in der Hand des Versicherers ist.

Mögliche Varianten sind: Bring your own key vs Hold your own key Stark verschlüsselter Datenverkehr (Data in Transit)

Es ist Standard, Daten verschlüsselt zu übertragen. Jedoch ist zu bemerken, dass im Kontext Krankenversicherung ggfs. auf stark verschlüsselte Verfahren abgestellt werden muss, wenn es sich um besonders schützenswerte Daten handelt. Eine Einschränkung kann sich aus technische Restriktionen beim Mobile Computing ergeben.

5.7.2 Interne Risikobeurteilung

Die standardisierte interne Risikobeurteilung (siehe Template-Liste)muss jedes Unternehmen entlang seiner strategischen und sonstigen Vorgaben ausführen. In diesem Dokument wird nicht weiter dazu Stellung bezogen.

5.7.3 IT-Governance

Die IT-Governance ist im Kontext Cloud Computing von erheblicher Relevanz. Es ist zu beobachten, dass es zu einer signifikanten Ressourcenverschiebung kommt. Die operativen Tätigkeiten sind eher beim Cloud-Lieferanten zu finden, die Instanzen für Kontrolle und Governance beim Nutzer von Cloud-Services werden stark aufgebaut.

Es ist im Vertrag festzulegen, welche Berichtspflichten der Cloud-Lieferanten haben müssen.

➢ *Praxis*

Es ist festzulegen, wie der Umgang mit Logfiles ist. Der Zugriff auf die Logfiles muss ggfs. sichergestellt sein.

Cloud-Lieferanten werden in der Regel ihre Tools einsetzen. Der Wunsch ggfs. die Tools vom Cloud-Nutzer einzusetzen wird oft abschlägig beschieden. Eine Integration mit dem Systems Management beim Cloud-Nutzer ist oft nicht möglich.

5.7.4 Autorisierung/Authentisierung

Hier muss aus Sicht vom Cloud-Nutzer eine Güterabwägung zwischen Sicherheitsanliegen und Benutzerfreundlichkeit stattfinden.

5.8 Lieferantenspezifische Aspekte

5.8.1 Analyse Cloud-Verträge/branchenspezifische Erweiterungen

Für Banken gibt es bei den grossen Cloud-Lieferanten branchenspezifische Erweiterungen. Für die Versicherungen ist ebenfalls eine solche Erweiterung anzustreben.

5.8.2 Einholung der nachträglichen Kundenzustimmung

Betrachtung der aktuellen Vertraglichen Regelungen, die einer Cloud Nutzung im Wege stehen. AVB oder Nutzungsbedingungen.

➢ *Praxis*

Muss geprüft werden und wenn notwendig, muss das Opt-in eingeholt werden.

5.8.3 ISO Zertifizierungen

Zertifizierungen (z.B. ISO27001) und Attestierungen (siehe ISAE SOC 2 Typ II) sind zwar hilfreich, jedoch wird nach Erfahrungen mehr Wert auf die Attestierungen gelegt.

Der Umfang der General Controls im Kontext eines IKS (Internen Kontrollsystem) ist entsprechend anzupassen und zu erweitern.

Nicht nur das Design von Kontrollsystemen ist wichtig und wird überprüft, sondern vor allem muss das System dem Realitätscheck standhalten.

- *Praxis*

Microsoft ist in diesem Thema ein Experte und kann hier auf viel Erfahrung bauen. Für den Cloud-Nutzer ist dies von Vorteil.

***