Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

MERKBLATT für die Angehörigen der Departemente zu rechtlichen Aspekten des Cloud Computings

A. Allgemeine Bemerkungen

Von Cloud-Computing kann gesprochen werden, wenn die Punkte, *zeitnahe, automatisierte Beschaffung*, *Zugang über Internet*, *Ressourcen Pooling, Schnelle Elastizität* und *Messbarer Leistungsbezug* erfüllt sind gesprochen werden. [1] Die *Virtualisierung* alleine macht noch kein Cloud-Computing aus.[2]

B. Dienste und Organisationsformen im Cloud-Computing

1. IT-Leistungen die als Dienste bereitgestellt werden[3]

IaaS-Dienste (Infrastructure as a Service): bieten lediglich virtualisierte Hardware-Ressourcen zur Nutzung. Der Nutzer (ETH Zürich) ist selbst dafür verantwortlich, die gewünschte Software auf dem „nackten Rechner zu installieren und zu unterhalten. Das Leistungsangebot ist bei den heutigen IaaS-Anbietern zunehmend standardisiert. Beispiele: *Amazone EC2, CloudSigma*

PaaS-Dienste (Platform as a Service): Cloud-Anbieter entwickelt eine Anwendung und stellt diese den Nutzern in der Cloud zur Verfügung. Die Bewirtschaftung der Daten mittels dieser Anwendung erfolgt jedoch durch den Nutzer selber. Beispiele: *Google App Machine, Microsoft Azure*

SaaS –Dienste (Software as a Service)**:** Diese Dienste bieten fertige Anwendungen, welche über Webbrowser genutzt werden. Der Cloud-Nutzer ist nur Konsument. Er bewirtschaftet weder die Anwendungen noch die Daten mehr. Ihm wird einzig in der Cloud eine Funktionalität zur Verfügung gestellt, um dort Daten bearbeiten zu können. Beispiele: *Google Mail, Maps, Calender*

2. Organisationsformen (Liefer-Modelle)[4]

a) Private Cloud
Private Clouds werden exklusiv für eine Organisation betrieben. Diese kann umfassend Einfluss nehmen und damit auch die Erfüllung von spezifischen Sicherheitsstandards sicherstellen. Datensicherheit,

[1] Definition gemäss NIST: „Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned an d released with minimal management effort or service provider interaction".
[2] Kommentar zur Cloud-Computing Strategie der Schweizer Behörden vom 14.11.2011 (ISB), S. 13 siehe http://www.isb.admin.ch/themen/architektur/00183/01368/01372/index.html?lang=de
[3] U. Heck, Vorstudie zu Cloud Computing in Schweizer Behörden vom 21.10.2010, S. 9 (http://www.isb.admin.ch/themen/architektur/00183/01368/01372/index.html?lang=de).
[4] Heck, Vorstudie zu Cloud Computing in Schweizer Behörden vom 21.10.2010, S. 11, Kommentar zur Cloud-computing Strategie der Schweizer Behörden vom 14.11.2011 (ISB), S. 11 f., S. 14

Corporate Governance und Zuverlässigkeit liegen damit in ihrem eigenen Einflussbereich. Im Bereich Legal Compliance bietet die Private-Cloud ebenfalls eine bessere Kontrolle und Flexibilität auf spezifische Anforderungen.

b) Community Cloud
Community Clouds sind Verbände von Private-Clouds mehrerer Organganisationen mit gemeinsamen Anforderungen und/oder Interessen. (z.B. die ETH-Bereichsinstitutionen))

c) Public Cloud
Dienste werden gegen Bezahlung oder kostenlos der Allgemeinheit zur Verfügung gestellt. Die oben genannten Aufgaben, die ein Unternehmen in der Private Cloud vornimmt, werden in der Public Cloud von einem Drittanbieter übernommen. Aufgaben und Services von unterschiedlichen Kunden werden dabei auf derselben Infrastruktur gemeinsam gehostet und verarbeitet. Ein einzelner Kunde hat keine Kenntnis darüber, wessen Dienste ebenfalls auf derselben Infrastruktur gespeichert und verarbeitet werden. Die Sicherstellung von Datenhoheit und Informationssicherheit werden teilweise oder vollständig an Dritte abgegeben, was den Kontrollaufwand für den Leistungsbezüger erhöht. Verschlüsselungstechnologien können Lösungen bieten.

d) Hybrid Cloud
Mischung aus der Private und der Public Cloud. Dabei verfügen Unternehmen zwar über ihre eigene Private Cloud, verwenden aber zusätzlich Dienste aus der Public Cloud von externen Anbietern.

C. Rechtliche Aspekte

Bei der Nutzung von Cloud Computing werden Verträge zwischen der ETH Zürich als „Cloud-Nutzerin“ und dem „Cloud Anbieter“ geschlossen. Bei der heute bereits mancherorts bestehenden Nutzung von SaaS-Diensten durch ETH-Mitarbeitende sind sich diese entsprechenden Tatsachen wohl kaum bewusst. **Es ist aber festzuhalten, dass die Nutzung von virtualisierter IT-Infrastruktur im Cloud-Computing durch die ETH Zürich nichts anderes als die Beschaffung einer IT-Dienstleistung ist, die grundsätzlich den ETH-internen Regeln betreffend Einkauf von Dienstleistungen gemäss Art. 86 f. Finanzreglement ETH Zürich bzw. Art. 69 f. (Zeichnungsberechtigung/Ausgabekompetenz) unterliegt.** Es gelten damit dieselben Regelungen wie bei der Beschaffung von physischen Dienstleistungen oder Hardware, d.h. die Verträge müssen im Regelfall durch den Einkauf der Informatikdienste und allenfalls durch den Rechtsdienst geprüft werden. Solche Beschaffungen unterliegen im Übrigen auch dem Vergaberecht. Auch bei der Inanspruchnahme von kostenlosen Diensten sind die „Cloud-Nutzer“ aufgefordert, die betreffenden AGB’s zu prüfen, eine Risikoabschätzung vorzunehmen und im Zweifelsfall die Mitarbeiter der Informatik-Support-Gruppe des Departements zu kontaktieren.

1. Vertragsrechtliche Aspekte

Bei der Nutzung von Cloud Computing sind die Verträge (Service Level Agreements) der Anbieter und ggf. die Allgemeinen Geschäftsbedingungen auf folgende Kriterien, die Risiken für die ETH Zürich beinhalten können, zu prüfen und ggf. zu verhandeln, anzupassen oder neu zu definieren. Vertragsbedingungen, die nachteilig für die ETH Zürich sind, sind zu vermeiden.

- Qualität der Leistungen des Anbieters (Performance, Verfügbarkeit, Verantwortungsbereiche des Kunden, Vertraulichkeit, Integrität) zu prüfen. **Service Descriptions sind dabei auch bei Standard Services relevant!**
- Sicherheit (Zugriffsmethoden/-rechte, Schutz der Infrastruktur, Applikationen gegen externe Angriffe, Datensicherung, Zertifizierung z.B. ISO 27001)
- Vertragsbeendigung (**Wichtig: Die ETH Zürich akzeptiert keine automatische Vertrags-verlängerungen!**): Fixe, minimale Vertragsdauer verlangen!
- Haftung: Haftungsausschlüsse zugunsten des Anbieters, welche die Risiken auf die ETH Zürich abwälzen, sind zu vermeiden.
- Gerichtsstand/Rechtsdurchsetzung: Ganz heikel, denn bei grossen Anbietern kann sich die ETH Zürich kaum durchsetzen mit CH-Recht oder Gerichtsstand Zürich. Der Gerichtsstand sollte wenn immer möglich in der Schweiz sein und der Vertrag sollte CH-Recht unterliegen.
- Urheberrechte: : Dem Cloud Provider dürfen nicht automatisch die inhaltlichen Nutzungsrechte zustehen (z.B. Google bei gewissen Angeboten).

Die vertragsrechtlichen Aspekte sind vielfältig und es ist vor Abschluss eines Vertrags die ISG, die Beschaffungsstelle der Informatikdienste und/oder der Rechtsdienst beizuziehen. .

2. Datenschutzrechtliche Aspekte

Werden bei der Nutzung von Cloud Computing personenbezogene Daten bearbeitet, so liegt aus datenschutzrechtlicher Sicht üblicherweise eine Datenbearbeitung durch Dritte im Sinne von Art. 10a Datenschutzgesetz (DSG) vor. Die Datenschutzbestimmungen gelten solange, als hinter den Daten identifizierbare Personen erkannt werden können. Wird die Erkennbarkeit verunmöglicht, liegt keine datenschutzrechtliche relevante Handlung vor.

Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz an einen Cloud-Service Anbieter übertragen werden, wenn die Daten durch den Service-Anbieter nur so bearbeitet werden, wie der Auftraggeber (Cloud-Nutzer d.h. ETH Zürich) es selbst tun dürfte, und wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. **Der Cloud-Service-Anbieter muss also verpflichtet werden, sich vollumfänglich an die in der Schweiz geltenden Datenschutzbestimmungen zu halten. Dies gilt in gleichem Masse für allfällige Subunternehmer.** Zudem müssen die Personendaten durch angemessene **technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.**[5] Personendaten dürfen zudem nicht ins Ausland bekannt gegeben werden, wenn dadurch eine Gesetzgebung fehlt, die einen **angemessenen Schutz** gewährleistet (Art. 6 Abs. 1, 2 DSG).

Personaldaten: Bei der Bearbeitung von Daten (inkl. Lohndaten) von Angestellten und Professoren der ETH Zürich sind primär die ***Richtlinien über den Schutz und Umgang mit Personaldaten an der ETH Zürich*** (RSETHZ 612; www.rechtssammlung.ethz.ch) zu beachten und einzuhalten.

[5] EDOEB, *Erläuterungen zu Cloud Computing* vom Oktober 2011, S. 3, http://www.edoeb.admin.ch/themen/00794/01124/01768/index.html

Forschungsdaten: Die Aufbewahrung von und Rechte an Primärdaten und Materialien, die Veröffentlichung von Forschungsergebnissen während laufendem Patentverfahren, etc. , sind in den ***Richtlinien für Integrität in der Forschung und gute wissenschaftliche Praxis an der ETH Zürich (RSETHZ 414)*** verbindlich geregelt. Die **Projektleitung (in der Regel also der zuständige Professor) ist für das Management der Daten (Aufbewahrung, Datenzugang, Einhaltung des Datenschutzes, Geheimhaltung, etc.) verantwortlich (Art. 11 Abs. 4 der Richtlinien) und sie hat deshalb zu entscheiden**, unter Vornahme einer umfassenden Risikoeinschätzung, ob Forschungsdaten der Gruppe in eine Cloud ausgelagert werden sollen.