Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

MERKBLATT für die Informatiksupportgruppenleiter (ISL) in den Departementen 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]

Die Benutzerordnung für Telematikmittel der ETH Zürich (BOT) enthält keine Regelungen zu Cloud Computing. Die ETH Zürich verfügt derzeit (April 2012) auch über keine Cloud-Computing-Strategie.

Die Dienstleistung des Cloud-Computings betrifft einige Rechtsgebiete und bildet einen breiten Fragenkomplex. Die wesentlichen Punkte sollen nachstehend aufgeführt werden.

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*

[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).

2. Organisationsformen (Liefer-Modelle)[4]

a) Private Cloud
Der Begriff Private-Cloud wird ganz unterschiedlich gehandhabt. Private Clouds sind Organisationen (z.B. ETH Zürich), die durch ihre IT-Abteilung eigene Rechenzentren betreiben/eigene Server anmieten und ihre Dienste nur für ihre eigenen geschäftlichen Zwecke innerhalb ihrer eigenen privaten Netze verwenden und der Allgemeinheit nicht zur Verfügung stellen. Datensicherheit, 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) 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.

c) 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 entsprechender Tatsache 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.

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.

[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

- 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 Vertragsverlängerungen!**): 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.

2. Allgemeine datenschutzrechtliche Aspekte

a) Voraussetzungen bei der Datenbearbeitung durch Dritte

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, etwa durch Anonymisierung oder Verschlüsselung. Eine solche kann allenfalls bedeuten, dass die Daten durch den Anbieter nicht auftragsgemäss bearbeitet werden können und damit eine Auslagerung in eine Cloud sinnlos wird.[5]

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) 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.**[6] Der Cloud-Nutzer ist auch dafür verantwortlich, dass das Auskunftsrecht vom Cloud-Service-Anbieter jederzeit gewährleistet ist und die Daten jederzeit gelöscht werden können, wenn sie nicht mehr benötigt werden.

Daten von Mitarbeitenden der ETH Zürich dürfen an Dritte nur weitergegeben werden, wenn eine gesetzliche Grundlage dafür besteht oder die Person der Weitergabe zugestimmt hat (Art. 27 Abs. 3 Bundespersonalgesetz).

b) Voraussetzungen bei der Datenbekanntgabe ins Ausland

Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch eine Gesetzgebung fehlt, die einen **angemessenen Schutz** gewährleistet (Art. 6 Abs. 1, 2 DSG). Der

[5] Kurzgutachten Rechtsdienst ZHdK vom 8.2.2012 zur Nutzung von Cloud Computing
[6] EDOEB, *Erläuterungen zu Cloud Computing* vom Oktober 2011, S. 3

Eidgenössischedatenschutzbeauftragte (EDOEB) führt eine entsprechende Länderliste (www.edoeb.admin.ch).

3. **Regulatorische Anforderungen**

a) Geheimhaltungsvorschriften
- Geschäftsgeheimnisse (z.B. geplante und laufende Forschungsprojekte, laufende Patentverfahren, vertrauliche Lohndaten, Finanz und andere Geschäftsdaten der ETH Zürich)

(Die Mitarbeiter der ETH Zürich sind zur Verschwiegenheit über berufliche und geschäftliche Angelegenheiten verpflichtet; Art. 57 Personalverordnung ETH-Bereich)

b) Massnahmen
- Verpflichtung des Anbieters zur Geheimhaltung
- Verschlüsselung der Dateninhalte

4. ETH-interne Datenschutzbestimmungen

a) Daten (inkl. Lohndaten) von Angestellten und Professoren der ETH Zürich

Richtlinien über den Schutz und Umgang mit Personaldaten an der ETH Zürich (RSETHZ 612): Diese Richtlinien enthalten Regelungen über die Datenbeschaffung, die zuständigen Stellen für die Datenbearbeitung, die Zugriffsberechtigungen auf die Personalinformationssysteme (z.B. SAP-HR) sowie die Datenaufbewahrung.

b) 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). In Absprache mit ihm wird schriftlich festgehalten, welche Teilnehmer nach ihrem Ausscheiden aus dem Projektteam bzw. der ETH Zürich Zugang zu Daten und Materialien behalten sollen (Art. 12 Abs. 3).

c) Finanzdaten

Das Finanzreglement der ETH Zürich (RSETHZ 245) enthält in Art. 49 eine grundsätzliche Bestimmung zur Bearbeitung und dem Zugriff von Finanzdaten. Gestützt auf diese Bestimmung hat der Vizepräsident für Finanzen und Controlling Ausführungsbestimmungen zu erlassen (bisher nicht erfolgt).

d) Studierendendaten

Art. 36b neu ETH-Gesetz bildet voraussichtlich ab dem 1.1.2013 (Inkrafttreten des revidierten Bundespersonalgesetzes) die gesetzliche Grundlage für die Bearbeitung von Studierendendaten in elektronischen Systemen. Dabei ist die Bekanntgabe besonders schützenswerter Daten und Persönlichkeitsprofilen durch ein Abrufverfahren nur innerhalb der ETH Zürich gestattet. Das Rektorat wird entsprechende Ausführungsbestimmungen erlassen. Die Arbeiten dazu werden in den kommenden Monaten aufgenommen. Bereits heute bestehen diverse Weisungen der Rektorin zur Bearbeitung von Studierendendaten (vgl. www.weisungen.rektorat.ethz.ch).

5. Fazit

Die **ETH Zürich ist verantwortlich für die Einhaltung von datenschutzrechtlichen Vorschriften und haftet bei allfälligen Verletzungen von Datenschutzbestimmungen** gegenüber von betroffenen Personen. Sie sollte sich deshalb gut überlegen, welche Anwendungen und Daten sie am eigenen Standort behalten will und welche in die Cloud wandern sollen. Zu diesem Zweck muss sie im Vorfeld eine sorgfältige Prüfung des Cloud-Service-Anbieters und eine **umfassende Risikoeinschätzung** in organisatorischer (inkl. Kosten/Nutzen), rechtlicher und technischer Hinsicht vornehmen.

Über ihre Geschäftsdaten (Personaldaten, Forschungsrohdaten, Finanzdaten u.a.) sollte die ETH Zürich zudem aus Gründen der Corporate Governance und Legal Compliance die Datenhoheit und Informationssicherheit beibehalten und deshalb nicht an einen Drittanbieter abgeben.

Weiterführende Links

- Bundesgesetz über den Datenschutz (DSG): http://www.admin.ch/ch/d/sr/2/235.1.de.pdf
- Verordnung zum Bundesgesetz über den Datenschutz (VDSG): http://www.admin.ch/ch/d/sr/2/235.11.de.pdf
- Bundespersonalgesetz (BPG): http://www.admin.ch/ch/d/sr/172_220_1/a27.html
- ETH Open Access Policy: http://www.open-access.ethz.ch/oazurich/policy
- Erläuterung zu Cloud Computing: http://www.edoeb.admin.ch/themen/00794/01124/01768/index.html
- Richtlinien über den Schutz und den Umgang mit Personaldaten an der ETH Zürich: http://www.rechtssammlung.ethz.ch/pdf/612_richtlinien_personaldaten.pdf
- ETH Richtlinien für Integrität in der Forschung und gute wissenschaftliche Praxis: http://www.rechtssammlung.ethz.ch/pdf/414_Integrität_Forschung.pdf

Für die Bearbeitung von Personendaten bei der Nutzung elektronischer Infrastruktur des Bundes gilt zudem Art. 57i f. Regierungs- und Verwaltungsorganisationsgesetz (RVOG) sowie die Bestimmungen der entsprechenden Verordnung , die seit 1.4.2012 in Kraft ist:

http://www.admin.ch/ch/d/sr/c172_010.html und http://www.admin.ch/ch/d/sr/1/172.072.de.pdf

Für allgemeine datenschutzrechtliche Fragen stehen Ihnen alle Mitarbeitenden des Rechtsdienstes der ETH Zürich, für datenschutzrechtliche oder vertragsrechtliche Fragen mit Bezug auf Cloud-Computing steht Ihnen RA lic.iur. Brigitte Schiesser, zur Verfügung.