zürcher anwaltsverband

Cloud Computing in der Anwaltskanzlei

Anwaltsforum vom 03.09.2015
erweiterte Fassung vom 05.09.2015

Lars Bauer
Wolfgang Straub

Übersicht

zürcher anwaltsverband

- Einführung: Merkmale und Besonderheiten von Cloud Services
- Datenschutz
- Anwaltsrecht
- Weitere rechtliche Vorgaben
- Vorgehensempfehlungen

Einführung

zürcher anwaltsverband

«Hidden Cloud»

- Die meisten Kanzleien dürften bereits in irgendeiner Form – oft unbewusst – Cloud-Dienste benutzen (z.B. E-Banking, Web-Konferenzen, juristische Informationsplattformen)
- Nur teilweise bekannte Nutzung von Cloud-Diensten durch Mitarbeiter
- Oft unbekannte Involvierung in Cloud-Dienste von Geschäftspartnern (z.B. Subakkordanten von Dienstleistern)

Pioniere mit bewusster Cloud-/Outsourcing-Strategie

- Punktuelle Nutzung von Cloud-Anwendungen in- und ausländischer Anbieter, z.T. auch mit Datenspeicherung im Ausland (z.B. File Sharing, Data Rooms, E-Discovery, CRM, Branchenanwendungen)
- Auslagerung der gesamten ICT auf Cloud-, Hybrid- oder lokale Infrastruktur eines Schweizer Anbieters

Einführung

zürcher anwaltsverband

Cloud Computing – Merkmale

Unscharfe Begrifflichkeiten; diverse Erscheinungsformen

Umschreibung: Ein Service-Modell, in dem ICT-Dienste (z.B. Anwendungen, Rechen- oder Speicherkapazität) aus einem Pool geteilter Ressourcen dynamisch an den Bedarf angepasst und über ein Netzwerk zur Verfügung gestellt werden.

Merkmale

- Pool geteilter Ressourcen: Hardware, Virtualisierungsumgebung, allenfalls virtuelle Server und Anwendungen (Multi-Tenancy)
- Dynamisch an den Bedarf angepasst:
  - Elastizität und Skalierbarkeit
  - Nutzungsabhängige Vergütung oder Mietmodell (z.B. monatliche Subskription)
- Zugang über ein Netzwerk (Internet, VPN): zeit-, orts- und geräteunabhängig

Einführung

zürcher anwaltsverband

Unterschiede zur herkömmlichen ICT (idealtypisch)

Cloud Computing	Herkömmliche ICT
Geteilte **Ressourcen**	Dedizierte Ressourcen (Hardware: Eigentum, Leasing oder Miete; eigene Softwarelizenzen)
Elastizität und **Skalierbarkeit**	Ressourcen auf Vorrat
Rasche **Verfügbarkeit**	Aufwendige Implementierung
Nutzungsabhängige **Vergütung** (OPEX)	Hohe Anfangsinvestition (CAPEX)
Zugang über Internet oder VPN; betriebs-systemunabhängige Web-Anwendungen	Oft nur lokaler Zugang und nicht webfähige, betriebssystemabhängige Anwendungen
Standardisierte **Verträge** und Leistungen	Individualisierte Verträge und Leistungen
Häufig intransparenter Beizug von **Subunternehmern**	Bessere vertragliche Einbindung von Subunternehmern
Beschränkte **Kontrolle** (→ Zertifizierungen)	Potentiell höhere Kontrollmöglichkeiten
Sichere und redundante Daten-speicherung (aber u.U. nicht lokalisierbar und/oder im Ausland)	Oft beschränkte Datensicherheit (aber Kontrolle über Ort der Datenbearbeitung)

Einführung

zürcher anwaltsverband

Service-Modelle – Technische und organisatorische Auslagerung

Software as a Service (SaaS) – «Ready to Use»
Bereitstellung von Anwendungen (z.B. Gmail, Dropbox, Office 365 online, WebEx, Clio, NetDocuments, Online-Banking)

Platform as a Service (PaaS) – «Ready to Build»
Bereitstellung von virtuellen Entwicklungs-, Integrations- und Betriebsumgebungen (z.B. Windows Azure, force.com, Mendix)

Infrastructure as a Service (IaaS) – «Ready to Rent»
Bereitstellung von virtuellen Infrastrukturdiensten (z.B. virtuelle Server, Rechenleistung, Speicherplatz)

… Desktop as a Service (DaaS), Network as a Service (NaaS), Identity as a Service (IDaaS) … Anything as a Service (XaaS)

Verantwortungsbereich des Anbieters

Einführung

zürcher anwaltsverband

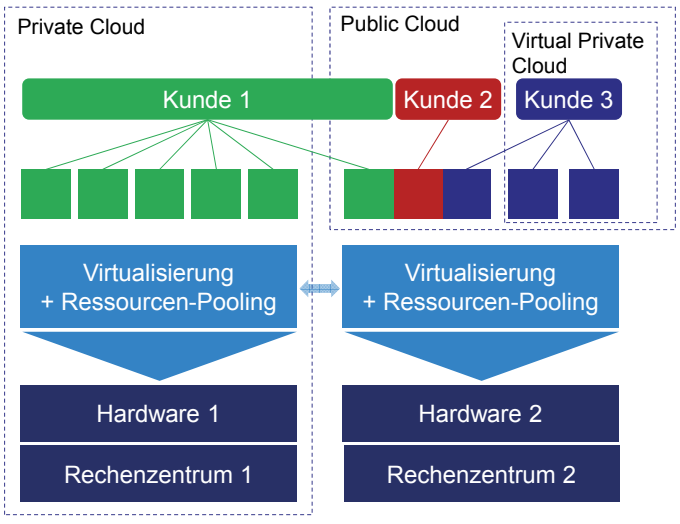
Organisationsformen – Grad der Exklusivität und Skalierbarkeit

- **Private Cloud:** Cloud-Infrastruktur wird exklusiv für eine Organisation betrieben (durch Organisation selbst oder Dritte). Exklusiver Zugriff für Angehörige der Organisation. Begrenzte Skalierbarkeit.
- **Community Cloud:** Cloud-Infrastruktur wird von mehreren Organisationen geteilt. Setzt gemeinsame Anliegen voraus. Erhöhte Skalierbarkeit.
- **Public Cloud:** Cloud-Dienste werden vom Anbieter auf einer von seinen Kunden gemeinsam genutzten Infrastruktur betrieben, die sich über mehrere Datencenter erstrecken kann. Kunden haben i.d.R. nur beschränkt Einfluss auf Ort der Datenbearbeitung. Optimale Skalierbarkeit.
- **Virtual Private Cloud:** Abgeschottete virtuelle Umgebung innerhalb einer Public Cloud, auf welche ausschliesslich ein bestimmter Kunde zugreifen kann. Wird von Anbietern häufig als Private Cloud bezeichnet.
- **Hybrid Cloud:** Kombination einer Private Cloud mit Diensten aus Public Clouds, Virtual Private Clouds, Community Clouds und/oder herkömmlichen IT-Umgebungen.

Einführung

zürcher anwaltsverband

Organisationsformen – Teilung von Ressourcen



Je nach Modell geteilte (multi-tenant) oder dedizierte virtualisierte Umgebung

i.d.R. keine Kontrolle über Virtualisierungsumgebung

i.d.R. keine Kontrolle über physische Infrastruktur

Einführung

zürcher anwaltsverband

Chancen für Anwaltskanzleien

- **Mobiles Arbeiten**: Orts-, zeit- und geräteunabhängiger Zugriff auf Anwendungen und Daten
- Einfache **Zusammenarbeit** im Team sowie mit Klienten und Dritten
- Erschwinglichkeit von **Anwendungen**, die sonst nur **Grosskanzleien** zur Verfügung haben (z.B. innovative ERP, CRM, DMS, E-Discovery-Systeme etc.)
- **Konsumententaugliche Entwicklungsumgebungen**, z.B. für Mobile Apps (Drag & Drop statt Programmieren); erlaubt stärkere Involvierung der Anwender in Entwicklung und Konfiguration von Anwendungen
- **Neue Geschäftsmodelle**, z.B. Online-Dienstleistungen, Anwaltsnetzwerke etc.
- **Konzentration aufs Kerngeschäft** und **Entlastung des IT-Personals von Routine-Aufgaben**

Manches kann auch ohne Cloud erreicht werden, i.d.R. aber mit grösserem Aufwand und höheren Kosten

Einführung

zürcher anwaltsverband

Technische Herausforderungen und Probleme

- Abhängigkeit von **performanten Netzwerken**
- **Kontrollverlust**, v.a. in Multi-Tenant-Umgebungen
  - Fremde Hardware
  - Beschränkte oder gar fehlende Lokalisierbarkeit der Daten
  - Häufig mehrere Hilfspersonen des Providers
  - Eingeschränkte Kontrollmöglichkeiten für einzelne Kunden → Delegierung von Audits an unabhängige Zertifizierungsstellen und andere Dritte
- **Integration** mit anderen Systemen und Anwendungen
- Allenfalls beschränkte **Portabilität der Daten**

Einführung

zürcher anwaltsverband

Was ist gefährdet?

Klienteninteressen

- Daten (Verfügbarkeit, Vertraulichkeit, Integrität)

Anwaltsinteressen

- Eigene Handlungsfähigkeit (Lock-in-Effekte)
- Reputation

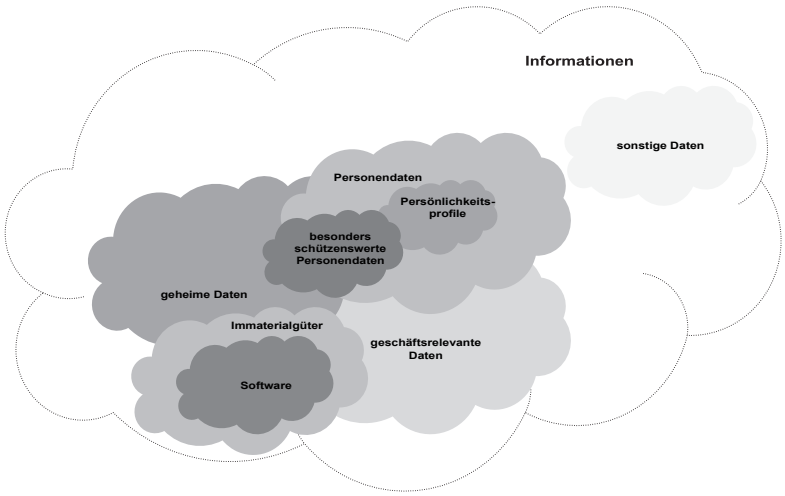
Compliance mit Vorschriften

- Anwaltsrecht
- Datenschutzrecht
- Buchführungs- und Archivierungsvorschriften
- Steuerrecht

Einführung

zürcher anwaltsverband

Potenziell betroffene Informationen



→ je nach Art der Information gelten unterschiedliche rechtliche Anforderungen

Datenschutz

zürcher anwaltsverband

Generelle Anforderungen an Datensicherheit

Personendaten müssen durch **angemessene technische und organisatorische Massnahmen** gegen unbefugtes Bearbeiten geschützt werden (Art. 7 DSG)

- Zweck der Datenbearbeitung
- Art der betroffenen Daten
- Art und Umfang der Datenbearbeitung
- Einschätzung der möglichen Risiken für die betroffenen Personen
- gegenwärtiger Stand der Technik

→ Beurteilung im Einzelfall (Interessenabwägung)

Datenschutz

zürcher anwaltsverband

Auslagerung der Datenverarbeitung

Voraussetzungen gemäss Art. 10a DSG

- Kein **gesetzliches/vertragliches Verbot**
- Daten dürfen von Provider nur so bearbeitet werden, wie Auftraggeber dies selbst tun dürfte.
- Angemessene **technische und organisatorische Sicherung**

Datenschutz

zürcher anwaltsverband

Auslagerung der Datenverarbeitung ins Ausland

Voraussetzungen gemäss Art. 6 DSG (zusätzlich zu Art. 10a DSG):

- ‚**Gleichwertige Datenschutzgesetzgebung**' (auch Daten von juristischen Pers.) **oder**
  - Einwilligung der Betroffenen (→ eventuell auch Mitarbeitende, Vertragspartner des Klienten!), oder
  - 'hinreichende Garantien' (z.B. EDÖB Mustervertrag) und Information des EDÖB

→ Siehe auch *Erläuterungen EDÖB zu Cloud Computing*

Anwaltsrecht

zürcher anwaltsverband

BGFA

- **Generalklausel**: Sorgfältige und gewissenhafte Berufsausübung (Art. 12 lit. a BGFA)
- Wahrung des **Berufsgeheimnisses**, auch durch Hilfspersonen (Art. 13 Abs. 2 BGFA, Art. 321 StGB)
  → Provider muss vertraglich als Hilfsperson eingebunden werden!
- Vermeidung von **Interessenkonflikten** zwischen Provider und Klienten (Art. 12 lit. c BGFA)
- Verletzungen von BGFA-Pflichten sind **Offizialdelikte**

→ Siehe auch *CCBE Guidelines on the use of cloud computing services by lawyers*

Zugriffsmöglichkeiten durch ausländische Behörden

Mögliche **Anknüpfungen** (z.B. US Patriot Act, Foreign Intelligence Surveillance Act, US Code 1881a):

- Standort des Rechenzentrums
- Sitz oder Kotierung des Unternehmens oder des Konzerns
- dauerhafte Geschäftstätigkeit

Bearbeitung von Klientendaten im Ausland

Zulässigkeit der Auslagerung von Klientendaten ohne Zustimmung der Klienten **kontrovers**

- Provider im Ausland sind bei Geheimnisverletzung **nicht als Hilfspersonen gemäss Art. 321 StGB strafbar** und müssen Klientendaten eventuell gestützt auf ausländisches Recht an Behörden herausgeben.
- Kann dieses Problem technisch gelöst werden (z.B. durch Verschlüsselung, verteilte Datenspeicherung, Anonymisierung der Daten)?

Bearbeitung von Klientendaten im Ausland

Verschlüsselung (I)

- Derzeit nur möglich bei **statischer Datenspeicherung** (Datenbearbeitung erfordert in der Regel vorgängige Entschlüsselung).
- Qualität der Verschlüsselung ist abhängig von **Verschlüsselungsalgorithmus, Schlüssellänge und Passwortqualität**
- Liegt **Schlüssel nur bei der Kanzlei oder beim Provider**?
- Mögliche **Schwachstellen**:
  - Ausländische Behörde hat 'zweiten Schlüssel'
  - Behörde zwingt Provider zur Herausgabe des Schlüssels
  - Verschlüsselung wird mit entsprechender Rechenleistung gebrochen
  - Sicherheitslücken im Verschlüsselungsalgorithmus werden ausgenützt

Anwaltsrecht

zürcher anwaltsverband

Bearbeitung von Klientendaten im Ausland

Verschlüsselung (II)

- Sichere Verschlüsselungsalgorithmen verlieren durch die Zunahme der Rechenleistung im Lauf der Zeit ihre **Wirksamkeit**.
- Für den Fall, dass Sicherheitslücken bekannt werden, ist entscheidend, ob die Daten **sofort gelöscht** werden können oder ob sie z.B. noch lange Zeit auf Backupsystemen des Providers gespeichert werden.
- **Anforderungen** an die Verschlüsselung sind abhängig von der **Art der Klientendaten** (wenn fremde Staaten sich für diese interessieren könnten, sind die Anforderungen besonders hoch).
- Auch aus **anonymisierten Daten** kann oft auf Personen zurückgeschlossen werden. Durch die Zunahme verfügbarer Informationen im Internet und Big Data Analytics können heute anonyme Daten in Zukunft repersonalisiert werden.

→ Klientendaten bzw. Personendaten werden durch Verschlüsselung oder Anonymisierung nicht einfach rechtlich irrelevant.

Müssen Klienten über Auslagerung informiert werden?

CCBE Guidelines:
"*A lawyer might consider informing his future clients that the law firm uses cloud computing services. The insertion of information into the general conditions of a legal-service agreement would be particularly advisable in cases when a law firm uses services of a cloud provider with servers located in a different jurisdiction. In such a case, a lawyer might need to obtain informed consent from his client to store confidential data on such servers*."

http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/07092012_EN_CCBE_gui1_1347539443.pdf

Anwaltsrecht

zürcher anwaltsverband

Müssen Klienten über Auslagerung informiert werden?

Es sind verschiedene Ebenen zu unterscheiden:

- **Datenschutzrechtlich**: Information ist sinnvoll, aber nicht zwingend, wenn die Anforderungen des DSG eingehalten werden.
- **Standesrechtlich**: Da kontrovers ist, ob eine Auslagerung ins Ausland überhaupt zulässig ist, sollten Klienten mindestens analog zum Rundschreiben 2008/7 der Finma informiert werden.
- **Vertragsrechtlich**: →Auslegung des Mandatsvertrages – auch anhand der datenschutzrechtlichen und der standesrechtlichen Vorgaben. In die Auslegung könnten zur Konkretisierung des Sorgfaltsmassstabes auch die CCBE Guidelines und das Finma Rundschreiben 2008/7 einfliessen.
- Eventuell weitere Ebenen, falls Anwaltskanzlei ausserhalb der klassischen Anwaltstätigkeit zusätzlichen Regularien untersteht.

Weitere rechtliche Vorgaben

zürcher anwaltsverband

Buchführungs- und Aufbewahrungspflichten

GebüV, Anwaltsrecht, Steuerrecht, Sozialversicherungsrecht

- **Geschäftsrelevante Daten** und Dokumente müssen insbesondere so aufbewahrt werden, dass sich feststellen lässt, ob sie nachträglich verändert wurden.
- **Archivierung** grundsätzlich auch in Cloud möglich, erfordert aber spezielle Massnahmen (z.B. Zeitstempel, Signaturen).
- **Zugriff von der Schweiz aus** muss jederzeit möglich sein.
- **Abläufe und Verfahren** müssen schriftlich festgelegt und **dokumentiert** werden. Zudem sind die entsprechenden Hilfsinformationen aufzubewahren (z.B. Protokolle und Logfiles).

Vorgehensempfehlungen

zürcher anwaltsverband

- Analyse der **Interessenlage**
- Bestimmung des **auszulagernden Bereiches**
- Analyse der **rechtlichen Anforderungen** und der notwendigen Ressourcen
- Analyse der wirtschaftlichen, technischen und rechtlichen **Chancen und Risiken**
- Festlegung einer **Strategie**
- Festlegung der **Kriterien für die Auswahl** und die Zusammenarbeit mit dem Provider
- Regelung der Zuständigkeiten und **Verantwortlichkeiten** zwischen den Parteien → Siehe auch *Checkliste Cloud Verträge in der Anwaltskanzlei* und *CCBE Guidelines*
- **Instruktion und Überwachung** des Providers
- Eventuell **Information/Zustimmung der Klienten** einholen

Fragen, Anregungen, Kritik?

zürcher anwaltsverband

Lars Bauer
Schellenberg Wittmer AG
Löwenstrasse 19 / Postfach 1876
8021 Zürich

lars.bauer@swlegal.ch
www.swlegal.ch

Wolfgang Straub
Augsburger Deutsch & Partner
Effingerstrasse 17 / Postfach 5860
3001 Bern

wolfgang.straub@ad-p.ch
www.it-recht.ch