Sensible Daten in der Cloud

Chancen und Herausforderungen in den Bereichen Datenschutz, Berufs- und Amtsgeheimnis

Dr. iur. Jürg Schneider, Rechtsanwalt, Partner

Vortrag Schaffhauser Juristenverein, 27. März 2018, Schaffhausen

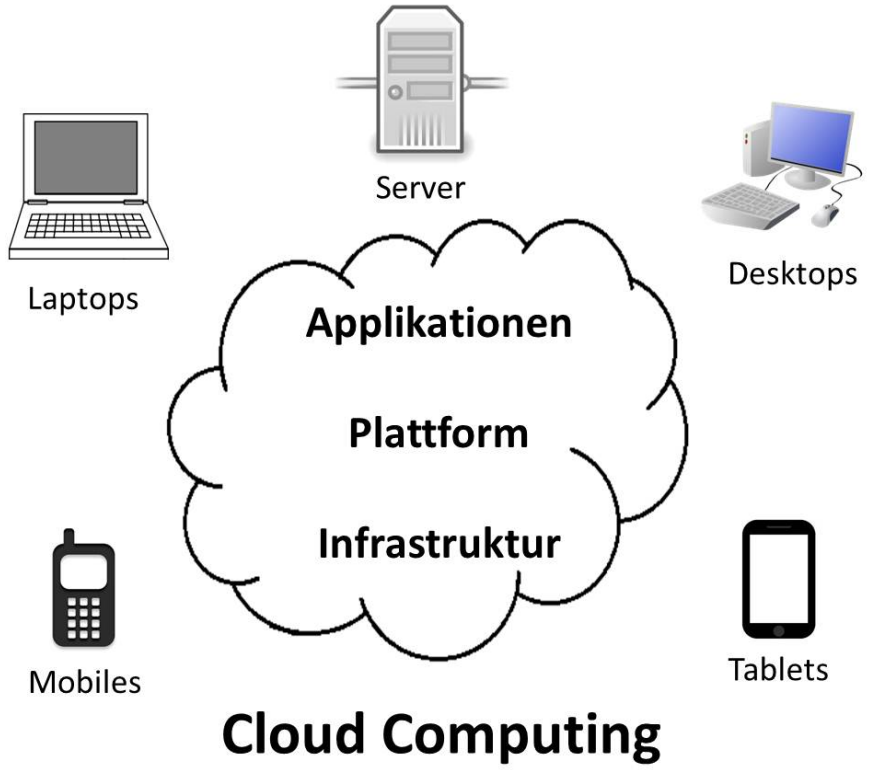
walderwyss rechtsanwälte

Übersicht

1. Cloud Computing
2. Datenschutz
3. Berufsgeheimnis
4. Amtsgeheimnis
5. Sicherheitsmassnahmen
6. Ausländische Cloud?
7. Take-aways

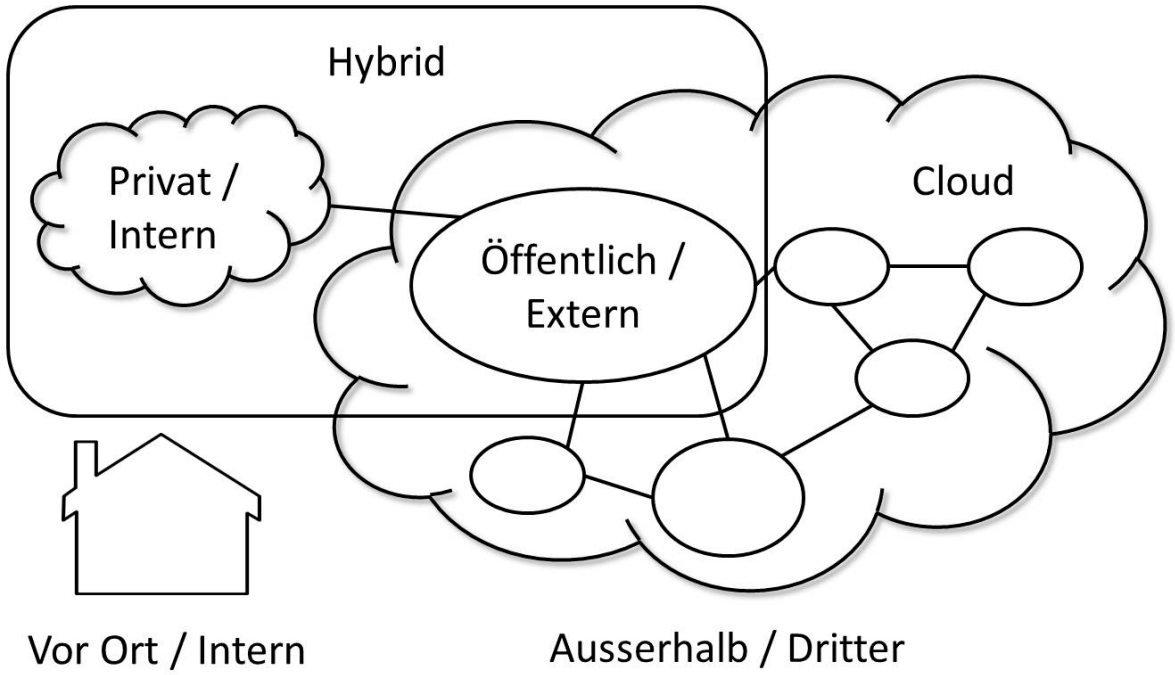
Cloud Computing (I)

- Cloud Computing: Servicemodelle
  - IaaS
  - PaaS
  - SaaS
  - XaaS



Cloud Computing (II)

- Cloud Computing: Liefermodelle
  - Public Cloud
  - Private Cloud
  - Hybrid Cloud
  - Community Cloud



Cloud Computing (III)

- Vorteile
  - Kostenreduktion
    - Nutzungsabhängige Gebühr, variable Kosten, Economies of Scale
  - Effizienzsteigerung
    - Skalierbarkeit, Ortsunabhängigkeit, Erschwinglichkeit
  - Fokussierung auf Kerngeschäft
  - Datensicherheit
    - Professionalität, Knowhow, Backup

Cloud Computing (IV)

- Risiken
  - Kontrollverlust über die Daten
    - Verfügbarkeit, Lock-in Effekt, Insolvenz
  - Compliance
    - Besondere Geheimhaltungspflichten, Zugriff ausländischer Behörden auf Daten
  - Vertragsgestaltung
    - Präzise Servicebeschreibung, Allokation Verantwortlichkeiten, Haftung

Cloud Computing (V)

– Vermehrt Public Clouds:

– Vermehrt SaaS:

Datenschutz (I)

- Sachdaten vs. Personendaten
- Anonymisierung, Pseudonomisierung und Verschlüsselung
- «normale» Personendaten» vs. besonders schützenswerte Personendaten und Persönlichkeitsprofile
- Cloud-Anbieter ist Auftragsdatenbearbeiter (Art. 10*a* DSG)
- Datenherrschaft bleibt beim Auftraggeber (keine «echte» Weitergabe an Dritte)
- Einwilligung der betroffenen Personen ist nicht notwendig!

Datenschutz (II)

- Anforderungen (Art. 4 ff. und Art. 10*a* DSG):
  - Einhaltung datenschutzrechtlicher Grundsätze (insb. Art. 4 und 5 DSG)
  - Übertragung entweder gestützt auf Vereinbarung oder auf Gesetz
  - Bearbeitung nur für Zwecke des Auftraggebers (nur soweit es der Auftraggeber selbst tun dürfte und nur soweit der Auftraggeber den Cloud-Anbieter ermächtigt)
  - Keine vertragliche oder gesetzliche Geheimhaltungspflicht
  - Gewährleistung Datensicherheit und deren Überwachung
  - Zusätzliche Garantien bei Bekanntgabe in Länder ohne angemessenen Datenschutz (Art. 6 Abs. 2 lit. a DSG)
- Anforderungen kant. Datenschutzgesetze: ähnlich (für den Beizug von Cloud-Anbietern braucht es keine ausdrückliche gesetzliche Grundlage, da keine «echte» Weitergabe an Dritte stattfindet)
- Beizug eines Cloud-Anbieters ist grundsätzlich zulässig

Berufsgeheimnis (I)

- Art. 321 Abs. 1 StGB

  «….Rechtsanwälte, …., Ärzte, … sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, werden, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.»

- Hilfspersonen sind ans Berufsgeheimnis gebunden
- Beizug Dritter muss nicht notwendig sein (es reicht, wenn es der Übung entspricht) (BGE 121 IV 45)
- Einwilligung des Geheimnisherrn ist gemäss wohl herrschender Lehre nicht erforderlich (contra: Wolfgang Wohlers, Gutachten im Auftrag des Datenschutzbeauftragten des Kantons Zürich, 2016)

Berufsgeheimnis (II)

- Bundesamt für Justiz (21. Juni 1999): Outsourcing der Rechnungsstellung und der IT-Leistungen durch Ärzte ist auch ohne Einwilligung der Patienten zulässig
- Bezirksgericht Zürich: Beizug eines «Schreibbüros» durch einen Arzt ist zulässig (Urteil GG150233-L, 18. November 2015)
- Beizug ist grundsätzlich zulässig, wenn die rechtlich geschützten Interessen des Geheimnisherrn dadurch nicht gefährdet werden! D.h. mindestens gleiches Schutzniveau
- Bedingung: Risikomanagement und State of the Art Sicherheitsmassnahmen

Amtsgeheimnis (I)

- Art. 320 Abs. 1 StGB

  «Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft»
- Hilfspersonen werden nicht explizit erwähnt
- Auffassung Bundesrat (Revision Bundesgesetz über die Informationssicherheit, BBL 2017, 3077 f.)
  - Weitergabe an IT-Dienstleister verletzt Amtsgeheimnis, es sei denn, eine Einwilligung der vorgesetzten Behörde liegt vor
  - Art. 320 StGB sei ausdrücklich auf Hilfspersonen auszuweiten, damit IT-Dienstleister ebenfalls dem Amtsgeheimnis unterstellt sind

Amtsgeheimnis (II)

- Aber
  - mehrere kantonale Aufsichtsbehörden haben die Auslagerung durch Gemeinwesen wiederholt als im Grundsatz zulässig angesehen (z.B. Ziff. 4.2 Leitfaden «Bearbeiten im Auftrag» der Datenschutzbeauftragten Kanton Zürich, Februar 2018);
  - privatim anerkennt, dass im Einzelfall auch bei einem Zugriff auf Patientendaten «vertraglich abgesicherte Lösungen» möglich sind (Medienmitteilung, 17. Mai 2017, (http://www.privatim.ch/wp-content/uploads/2017/05/MM_privatim_170517.pdf);
  - Bundesamt für Gesundheit: Auslagerung durch Krankenversicherer ist zulässig, sofern der Dienstleister funktionell in die Schweigepflicht und in das bereichsspezifische Datenschutzrecht eingebunden ist (inkl. Auslagerung ins Ausland, wenn Art. 6 DSG eingehalten wird) (Kreisschreiben Nr. 7.1 «Datenschutzkonforme Organisation und Prozesse der Krankenversicherer» vom 1. November 2014, Ziffer 5);
  - Veronika Blattmann: Auftragsverhältnis genügt, um den Auftragnehmer als die eine öffentliche Funktion ausübende Person zu qualifizieren (sog. funktionale Beamtenstellung) (in: Baeriswyl/Rudin, Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), Zürich 2012, 6 N9);
  - etc.

Amtsgeheimnis (III)

- Korrekte Fragestellung:

  «Ist die Auslagerung mit dem Geheimhaltungsinteresse und dem Geheimhaltungswillen des Geheimnisherrn zu vereinbaren?»

- Es ist nicht entscheidend, ob die Hilfsperson einer gesetzlichen Strafandrohung untersteht (andere wirksame Massnahmen können dies ersetzen)
- Beizug ist grundsätzlich zulässig, wenn die rechtlich geschützten Interessen des Geheimnisherrn dadurch nicht gefährdet werden! D.h. mindestens gleiches Schutzniveau
- Bedingung: Risikomanagement und State of the Art Sicherheitsmassnahmen
- Achtung: Es wird z.T. explizit verlangt, dass die Mitarbeiter direkt in das Kontroll- und Weisungsrecht des öffentlichen Organs eingebunden werden (Stichwort: Datenschutzrevers)
- Aber: einschlägige Rechtsprechung fehlt, Auffassung Bundesrat

Sicherheitsmassnahmen

- **Risikobasierter Ansatz**: durch Risikomanagement und State of the Art Sicherheitsmassnahmen Interessenausgleich schaffen
- Technische, organisatorische und vertragliche Massnahmen, z.B.:
  - Sorgfältige Auswahl, Instruktion und Kontrolle des Cloud-Anbieters
  - Unterauftragnehmer nur mit vorgängiger Einwilligung (so neu Art. 8 Abs. 3 E-DSG)
  - Einbindung in Risikomanagement und IKS, angemessene Organisation des Cloud-Anbieters
  - Business Continuity, Vermeidung eines «Vendor Lock-in», Datenportabilität
  - Geschützte Datencenter
  - Anonymisierung/Pseudonomisierung/Verschlüsselung und Schlüsselmanagment
  - Datentrennung (physisch oder logisch)
  - Technische und vertragliche Zugangs- und Nutzungsbeschränkungen, Protokollierung von Zugriffen
  - Zertifizierungen, Audits, Penetration Tests
  - Spezifische Vertraulichkeitsvereinbarungen/Datenschutzrevers

Ausländische Cloud?

- Ausser in Ausnahmefällen nicht explizit verboten und somit nicht strafbar (Art. 1 StGB, Legalitätsprinzip)
- Im Ausland sind Geheimnisverletzungen häufig auch strafbar (z.B. § 203 StGB-D)
- Vertragliche Regelung (z.B. Konventionalstrafen)
- Ausländische Cloud erhöht das Risiko nicht notwendigerweise (allenfalls sogar Risikoverminderung)
- Gesetzgebung im Ausland bietet allenfalls besseren Schutz (z.B. EU-DSGVO bietet für Personendaten von natürlichen Personen einen erhöhten Schutz; hohe Sanktionen)
- Zugriffsmöglichkeiten ausländischer Behörden auf Personendaten werden im Rahmen von Art. 6 DSG toleriert
- Zugriffsmöglichkeiten ausländischer Behörden unterliegen allenfalls restriktiveren Anforderungen
- Internationale Abkommen bzw. Amts- und Rechtshilfe sehen Datenlieferung ins Ausland vor
- Ausländische Cloud ist nicht *per se* rechtswidrig!
- Bedingung: mit adäquaten Sicherheitsmassnahmen (sowie Risikomanagement) sind allfällige Standortrisiken zu begrenzen (z.B. Verschlüsselung und Key Management beim Auftraggeber)

Take-aways

- Effizienz, Kostenreduktion aber auch Sicherheitsaspekte sprechen vermehrt für Cloud-Lösungen und stellen eine Chance dar
- Die Auslagerung von Datenbearbeitungen in die Cloud ist mangels ausdrücklichem gesetzlichem Verbot erlaubt, sofern durch Risikomanagement und Sicherheitsmassnahmen ein Interessenausgleich geschaffen wird und die anwendbaren gesetzlichen Anforderungen beachtet werden
- Dies gilt häufig auch dann, wenn Berufsgeheimnisse und/oder Amtsgeheimnisse betroffen sind und/oder wenn es sich um «ausländische Clouds» handelt
- Bei sensiblen Daten (besonders schützenswerte Personendaten und Persönlichkeitsprofile, Berufsgeheimnisse und/oder Amtsgeheimnisse) und/oder «ausländischen Clouds» sind die Anforderungen an Risikomanagement und Sicherheitsmassnahmen höher
- Achtung: in vielen Bereichen (noch) keine gefestigte Rechtsprechung und keine einstimmige Lehre!
- **Rechtmässigkeit muss im Einzelfall überprüft werden**
- Restrisiko allenfalls durch Einwilligungen (betroffene Personen, vorgesetzte Behörde) ausschliessen

Danke für Ihre Aufmerksamkeit

Kontaktdetails

Walder Wyss AG
Dr. iur. Jürg Schneider
Seefeldstrasse 123
Postfach 1236
8034 Zürich
Tel. +41 44 498 95 71
Fax +41 44 498 98 99
juerg.schneider@walderwyss.com
www.walderwyss.com