vogel & partner
rechtsanwälte

Cloud Computing und Compliance

Verträge, Urheberrecht, Datenschutz

Karlsruher Entwicklertag 2013
am 05.06.2013

Prof. Dr. Rupert Vogel
Tobias Haar, LL.M. (Rechtsinformatik)

Rechtsanwälte

Cloud Computing und Compliance

Agenda

- wirtschaftliche und technische Hintergründe, Arten von Clouds
- Vertragstypologie und -gestaltung
- Urheberrecht
- Datenschutz und Datensicherheit
- offene Fragen / Compliance
- Diskussion

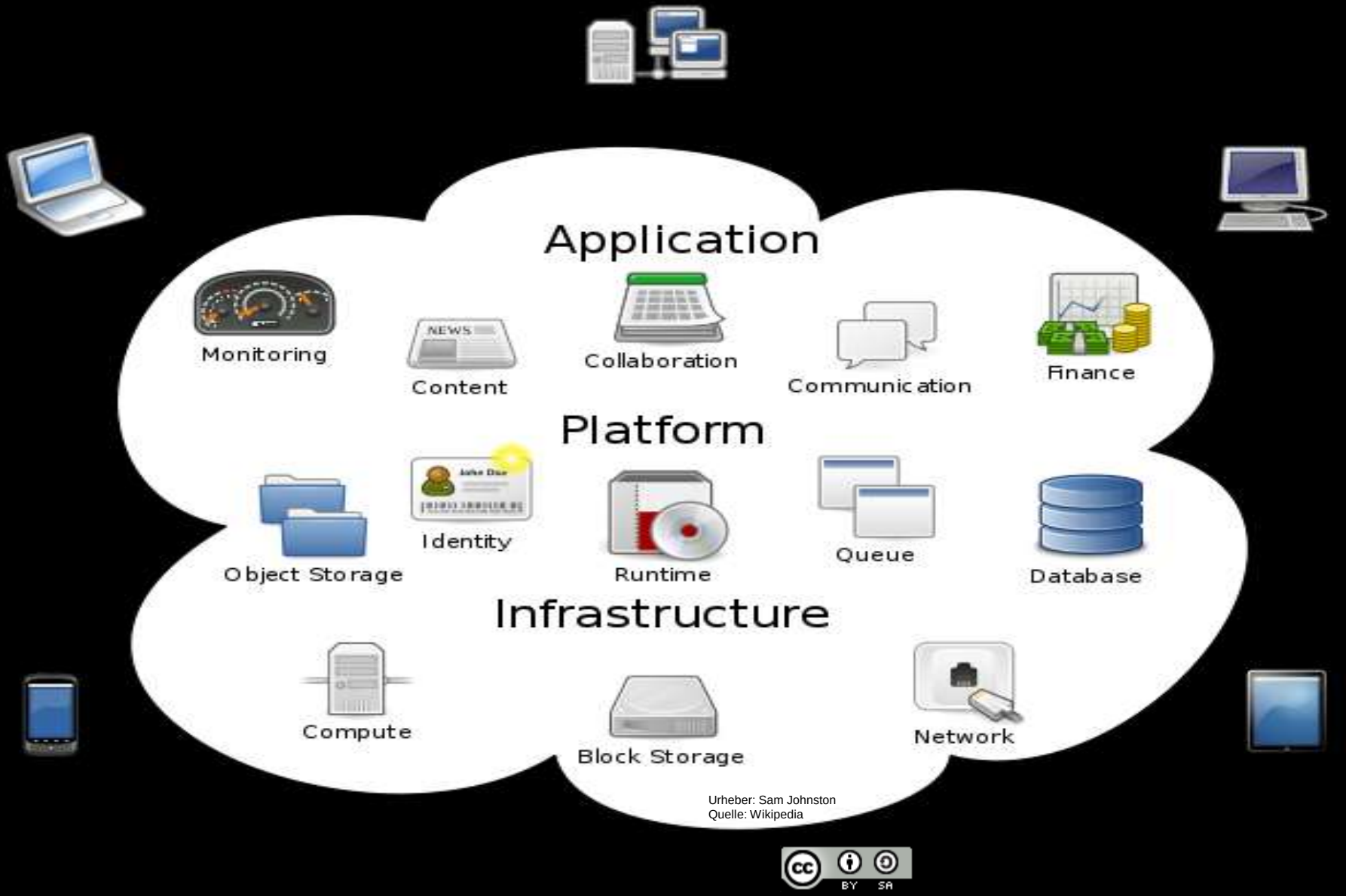
Wirtschaftliche und technische Hintergründe, Arten von Clouds

Definition von Cloud Computing

- BSI: *„CC bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von CC angebotenen Dienstleistungen umfasst das komplette Spektrum der IT und beinhaltet u.a. Infrastruktur (z.B. Rechenleistung, Speicherplatz), Plattformen und Software“.*

Dienstleistungsmodelle/ Drei-Ebenen-Modell

- Infrastructure-as-a-Service (IaaS)
  Desktop Cloud: Rechenleistung u. Speicherplatz, Netzwerk-Infrastruktur-Funktionalitäten
- Platform-as-a-Service (PaaS)
  Developer Cloud/ Entwickler-Plattform
  Entwicklung und Integration von Anwendungskomponenten
- Software-as-a-Service (SaaS)
  Bündelung und bedarfsgerechte Bereitstellung standardisierter Geschäftsanwendungen (IT-Ressourcen und Applikationen)



Urheber: Sam Johnston
Quelle: Wikipedia

Verwendungsmodelle (Cloud Deployment Models)

- Private Cloud
  unternehmens-, körperschaftsinterne Infrastruktur
- Public Cloud
  Vielzahl von Kunden (auch konzernintern)
- Hybrid Cloud
  Kombination von Private und Public Clouds

Vorteile für Kunden

Bereitstellung von überwiegend standardisierten IT-Leistungen über das Internet

- weltweiter Zugriff auf Daten
- Skalierbarkeit von Diensten
- geringere Kosten bei Hardware, lokaler Infrastruktur
- Nutzung professioneller Infrastruktur ohne eigenen Know-how-Aufbau
- Einsparung bei Betriebsorganisation
- Ersparnis von großen Investitionen, Abrechnung nach tatsächlichem Verbrauch („*pay as you go*“)

Risiken

- Risiken
  - Datenschutz (personenbezogene Daten)
  - Datensicherheit
  - Vertraulichkeit
  - Verfügbarkeit
  - Internationales Recht
  - regulatorische Vorgaben
- Aktuelle Diskussion in Branche über Rechtslage
- Lösung: Risikomanagement und Vertragsgestaltung

Vertragstypologie und Vertragsgestaltung

Vertragstypologie

- Warum überhaupt wichtig? Bestimmung des **Leitbilds** der Klauselkontrolle nach § 307 Abs. 2 BGB bei standardisierten Verträgen
- Unterschiedliche Leistungen / unterschiedliche Schwerpunkte → **typengemischte** Verträge …
- … mit im Wesentlichen **mietvertraglichem** Charakter; nach BGH ASP = Mietvertrag (Software müsse immer irgendwo verkörpert sein, um überhaupt nutzbar zu sein)
- Auch der Einsatz von Virtualisierungstechniken (im Unterscheid zum ASP) ändert an dieser Einordnung im Ergebnis nichts
- Problem: Garantieverpflichtung des § 535 Abs. 1 S. 2 BGB → grds. 100% Verfügbarkeit geschuldet
- Im Wesentlichen **dienst- und werkvertragsrechtlich** zu qualifizierende Zusatzleistungen, z.B. Support, Updates, Back-ups

Vertragsgestaltung

- einheitliches Leistungsstörungsrecht und Kodifizierung von Verfügbarkeitsquoten mittels **Service Level Agreements**
- Leistungsgegenstand, Verfügbarkeit, Performance (insb. Antwortzeit), Übergabepunkte, Bezugsgrößen, Messpunkte, Reaktions- und Beseitigungszeiten etc.
- Beauftragung von **Subunternehmern**, z.B. Amazon Web Services; Cloud-Anbieter häufig als Generalunternehmer (z.B. auch TK-Anbindung)
- Regelungen zum Notfall-Management, zur **Vertragsabwicklung** / zum Exit Management und zur Datenherausgabe am Vertragsende (z.B. Datenformate)
  - Problematisch: Zurückbehaltungsrecht an Daten
  - Problematisch: Leistungsverweigerungsrecht bei Zahlungsverzug

Verfügbarkeitsklauseln

- **Gegenstand** und Inhalt der Verfügbarkeit
  - Spezifizierung: Software-Module, Funktionen, Prozesse etc.
  - Festlegung bestimmter Betriebszeiten; Wartungsfenster
  - geplante / ungeplante, angekündigte / nicht angekündigte, verschuldete / unverschuldete Wartungsmaßnahmen
- **Verfügbarkeitsquoten** („*ninety-nine-point-something*“)
  - wichtig: Bezugszeitraum
  - Messung, Berichtswesen, Sanktionen, Bonus-Malus-Regelung etc. (z.T. Lastobergrenzen in AGB der Anbieter)
  - aus Kundensicht möglichst unmittelbare Auswirkungen auf Vergütung
  - optional: maximale Ausfallzeiten pro Ausfall
- Regelung – soweit möglich – als Bestandteil der **Leistungsbeschreibung** (nicht: „*Wir übernehmen keine Haftung, soweit …*“)

Verfügbarkeitsklauseln – 2 Beispiele

- »Aus technischen und betrieblichen Gründen sind zeitweilige Beschränkungen und Unterbrechungen des Zugangs zum ... Online-Service möglich. Zeitweilige Beschränkungen und Unterbrechungen können beruhen auf höherer Gewalt, Änderungen und Verbesserungen an den technischen Anlagen oder auf sonstigen Maßnahmen, z.B. Wartungs- oder Instandsetzungsarbeiten, die für einen einwandfreien oder optimierten ... Online-Service notwendig sind, oder auf sonstigen Vorkommnissen, z.B. Überlastung der Telekommunikationsnetze.«
- „Der Dienst ist zu 98 % im Kalendermonatsmittel verfügbar. Nichtverfügbarkeit ist anzunehmen, wenn der Dienst aufgrund von Umständen, die im Verantwortungsbereich des Anbieters liegen, vollständig nicht zur Verfügung steht. Nichtverfügbarkeit ist nicht anzunehmen, wenn der Dienst aufgrund von [höhere Gewalt, Fehlbedienung, geplante Wartungszeiten] nicht erreichbar ist. Der Anbieter darf den Dienst zum Zwecke der Wartung vorübergehend abschalten (geplante Wartungszeiten). Der Anbieter wird dem Nutzer geplante Wartungszeiten mindestens 2 Tage im Voraus über die Internetseite … ankündigen. Insgesamt darf die Dauer geplanter Wartungszeiten 12 Stunden im Monat nicht überschreiten.“
- vgl. z.B. auch Beispielsvertrag des BITKOM zum ASP und *Roth-Neuschild*, ITRB 2012, 67 ff.

Beispiel: Amazon Web Services Customer Agreement

- **2.1 To the Service Offerings.** We may change, discontinue, or deprecate any of the Service Offerings (including the Service Offerings as a whole) or change or remove features or functionality of the Service Offerings from time to time. We will notify you of any material change to or discontinuation of the Service Offerings.
- **3.1 AWS Security.** Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.
- **3.2 Data Privacy.** We participate in the safe harbor programs described in the Privacy Policy. You may specify the AWS regions in which Your Content will be stored and accessible by End Users. We will not move Your Content from your selected AWS regions without notifying you, unless required to comply with the law or requests of governmental entities. (...)

Urheberrecht

Verhältnis Softwarehersteller – Anbieter (1)

- Merke: Anbieter braucht Zustimmung/Lizenz für Cloud Computing
- Betroffene Verwertungsrechte
  - Vervielfältigung (§ 69c Nr. 1 UrhG) +
  - Vermietung (§ 69c Nr. 3 UrhG)?

  Def.: zeitlich begrenzte Gebrauchsüberlassung für unmittelbare o. mittelbare Erwerbszwecke
- Öffentliche Zugänglichmachung per Internet (§ 69c Nr. 4 UrhG)?
- Cloud Computing als eigenständige Nutzungsart (§ 31 UrhG)?

  (nach der Verkehrsauffassung als solche hinreichend bestimmt u. klar abgrenzbar, wirtschaftl.-techn. als einheitlich u. selbstständig sich abzeichnende konkrete Art u. Weise der Nutzung)

Verhältnis Anbieter - Kunde

- Sonderproblem: Darf durch Mitarbeiter/Freelancer erstellte SW für Cloud Computing genutzt werden?
- Mitarbeiter: Arbeitgeber hat im Zweifel wirtschaftliche Verwertungsrechte (§ 69 b Abs. 2 UrhG)
- Freelancer
  - geplantes Cloud Computing muss i. Zw. in Nutzungsrechtseinräumung vereinbart sein (höchstens stillschweigende Vereinbarung)
  - Zweckübertragungsgrundsatz (§ 31 Abs. 5 UrhG): Die Nutzungsrechte bleiben im Zweifel beim Urheber/Freelancer. Auftraggeber bekommt nur das, was ausdrücklich vereinbart ist!

Datenschutz und Datensicherheit

Anwendung (deutschen) Datenschutzrechts

- Int. anwendbares Recht: **Territorialitätsprinzip**
- **Personenbezogene Daten** sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener):
  - Mitarbeiterdaten
  - Kunden-/Lieferantendaten

  ⇨ Personenbezogene Daten sind häufig Gegenstand der Datenverarbeitung, Datenschutzrecht daher für die Verarbeitung in der Cloud in aller Regel zu beachten
- Lösung der datenschutzrechtlichen Probleme durch **Anonymisierung** personenbezogener Daten im Wege der Verschlüsselung ? → geeignet u.U. für Archivierungssysteme bei „starker“ Verschlüsselung; im Übrigen problematisch

Übermittlung der Daten an den Cloud-Anbieter

- **Verbot mit Erlaubnisvorbehalt**
  - Die Übermittlung an und die Verarbeitung durch den Cloud-Anbieter bedarf einer Rechtfertigung
  - insb. bei Funktionsübertragung, z.B. auf Accounting-Provider
- Wichtigste **gesetzliche Erlaubnistatbestände** für die Verarbeitung durch den Cloud-Anbieter
  - Wahrung berechtigter Interessen, Interessenabwägung

    ⇨ häufig nicht einschlägig
- **Einwilligung** der Betroffenen: in der Regel unpraktikabel bei Vielzahl von Betroffenen, ausreichende Information bei DV in Cloud schwierig (hohe Anforderungen der Rspr. an Bestimmtheit der Einwilligung auch im B2B-Bereich)
- entbehrlich, wenn sog. **Auftragsdatenverarbeitung** …

Auftragsdatenverarbeitung (innerhalb EU/EWR)

- Sorgfältige **Auswahl und Überwachung** des Cloud-Anbieters hinsichtlich der von ihm getroffenen techn. und organisatorischen Maßnahmen
  - Kunde muss „Herr der Daten“ bleiben → muss sich in tatsächlichen und rechtlichen Gegebenheiten widerspiegeln
  - Prüfung der gesamten Cloud-Lieferkette erforderlich (Wo sind die Daten? Wer hat Zugriff?)
  - Große Anbieter gestatten aber häufig keinen Einblick
- **Schriftliche Erteilung** des Auftrags
- **10-Punkte-Katalog** mit erforderlichen Mindestregelungen, u.a.
  - Ort der Datenverarbeitung
  - Kontrollrechte und Weisungsbefugnisse des Kunden
  - Festlegung von Unterauftragsverhältnissen

Auftragsdatenverarbeitung (innerhalb EU/EWR)

- Einhaltung der Anforderungen an die AuftragsDV-Vereinb.
  - Standardverträge der Anbieter oftmals **unzureichend**
  - in der Regel **nicht verhandelbar**, da Leistungen standardisiert
  - unzureichende Auftragserteilung für Auftraggeber / Kunden (!) **bußgeldbewehrt**
- Lösungsmöglichkeiten
  - Auswahl eines **geeigneten Anbieters**, z.B. bieten Microsoft und Salesforce Abschluss einer AuftragsDV-Vereinbarung an (zumindest auf Nachfrage); innereurop. Subunternehmer

    oder
  - **Private Cloud:** Bei konzernbetriebener Private Cloud Ausgestaltung als Auftragsdatenverarbeitung; bei Eigenbetrieb nicht erforderlich

Rechenzentren außerhalb des EWR

- Nach h.M. keine Auftragsdatenverarbeitung in Drittstaaten
  → Cloud-Anbieter ist Dritter, **Einwilligung in Übermittlung** erforderlich
  - Gesetzlicher Erlaubnistatbestand: Interessenabwägung
- Voraussetzung für die Zulässigkeit einer Datenverarbeitung in Drittstaaten ist außerdem die Sicherstellung eines **angemessenen Datenschutzniveaus** („Datentransfervehikel“)
  - Unterwerfung des Anbieters unter Safe Harbor (von Aufsichtsbehörden zunehmend kritisch gesehen)
  - EU-Standardvertragsklauseln (*EU model clauses*)
  - Binding Corporate Rules → Problem: Genehmigungsverfahren
- Dazu auch noch **entsprechende** Anwendung der Regeln zur Auftragsdatenvereinbarung (so jedenfalls einige dt. Aufsichtsbeh.)?

Datensicherheit – Kontrollerfordernis in der Cloud

- Die Auftragsdatenverarbeitungsvereinbarung hat die vom Cloud-Anbieter zu treffenden **technischen und organisatorischen Maßnahmen** im Einzelnen festzulegen
- Die technischen und organisatorischen Maßnahmen sind als „technischer Datenschutz“ in § 9 BDSG i.V.m. der Anlage zu § 9 geregelt: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, getrennte Verarbeitungsmöglichkeit
- Vertragsverhandlung bei großen Cloud-Anbietern unmöglich
- Lösung: Wahl des **geeigneten Anbieters** oder **Private Cloud**
- Orientierung, z.B. an BSI-Mindestsicherheitsanforderungen, ISO-Zertifizierungen, SAS-70-Bestätigungsvermerke unabhängiger Auditoren …

Datensicherheit – Kontrollerfordernis in der Cloud

- **Kontrollpflicht**: Auftraggeber hat sich vor Beginn der Datenverarbeitung und dann regelmäßig von der Einhaltung der Maßnahmen des Anbieters zu überzeugen
  - Bei länderübergreifenden Clouds Vor-Ort-Prüfung praktisch kaum durchführbar, aber eigene Recherchen erforderlich …
  - **Zertifizierung** der Cloud-Anbieter durch unabhängige Stelle als mögliche Lösung,

    ABER: „entbindet nicht von Kontrollpflichten“ (Arbeitskreis der Datenschutzbeauftragten)
  - Standards zu hinterfragen und auf den jeweiligen **Einzelfall** anzupassen
  - Kontrolle **vor Beginn** für Kunden bußgeldbewehrt mit bis zu 50.000 EUR

Offene Fragen

Offene Fragen / Compliance

- **Schutzziele von Compliance („Rechtsbefolgung“)**
  - Verfügbarkeit
  - Vertraulichkeit
  - Integrität
  - Authentizität
  - Zurechenbarkeit
- **Rechtsgrundlagen**
  - Gewährleistung der Vertraulichkeit u. Integrität informationstechnischer Systeme (so Bundesverfassungsgericht)
  - § 13 IV TMG, § 109 TKG, § 91 II AktG, § § 202a ff., 303a StGB, § 33 WpHG u. § 25a KWG; Konkretisierung über Anlage zu § 9 S. 1 BDSG
  - allg. Compliance (§ 93 Abs. 1 AktG, § 43 GmbHG): Geschäftsführer/Vorstand muss Risikomanagement-System einrichten
    - Mindestsicherheitsanforderungen
    - ISO 27001 etc.
    - Best Practices von Behörden u. Industrieverbänden

Lösungen

- Verpflichtung zum Risikomanagement im Allgemeinen
- technische Lösungen (Verschlüsselung)
- vertrauensbildende Maßnahmen
  - transparente Verträge und Leistungsdefinitionen
  - Zertifizierung und Audit-Rechte
  - IT-Sicherheitsmanagement
  - „Cloud-Beauftragter“ (entsprechend DSB)

Literatur und Links

- BITKOM-Leitfaden: http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf
- EuroCloud Leitfaden: http://www.eurocloud.de/2010/12/02/eurocloud-leitfaden-recht-datenschutz-compliance/
- Orientierungshilfe – Cloud Computing vom 26.09.2011 (Konferenz der DSB):

  http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf
- BSI Eckpunktepapier Cloud Computing: https://www.bsi.bund.de/
- Stellungnahme ULD / Weichert:

  https://www.datenschutzzentrum.de/cloud-computing/

Vielen Dank für Ihre Aufmerksamkeit!

Prof. Dr. Rupert Vogel
Rechtsanwalt & Fachanwalt für IT-Recht
rv@vogel-partner.eu

Tobias Haar, LL.M. (Rechtsinformatik)
Rechtsanwalt
th@vogel-partner.eu

www.vogel-partner.eu