RA Arno Lohmanns
RA Sebastian Helmschrott, LL.M EuR

rbi Rechtsanwaltsgesellschaft

Cloud Computing

Chancen und Risiken
aus rechtlicher Sicht

Gliederung

- **Teil I: Begriffliche, technische und rechtliche Grundlagen**
- **Teil II: Chancen und Risiken des Cloud Computing**
- **Teil III: Möglichkeiten zur Reduzierung der Risiken**

Teil I: Begriffliche, technische und rechtliche Grundlagen

Gliederung:

- Definition Cloud Computing
- Gleichwertige Begriffe, vergleichbare Erscheinungsformen und historische Entwicklung
- Technische Grundlagen des Cloud Computing
- Service Ebenen des Cloud Computing
- Cloud Betriebsmodelle
- Sonstige Cloud Typen
- Abgrenzung von verwandten Erscheinungsformen
- Tatsächliche Verbreitung
- Vertragsrechtliche Einordnung (Grob- und Feinraster)
- Public Cloud in Deutschland und AGB-Recht

Definition Cloud Computing

(Def. des National Institute of Standards and Technology - NIST)

Cloud Computing ist eine Form der Bereitstellung von jederzeit nutzbaren und flexibel skalierbaren IT-Leistungen durch nicht fest zugeordnete IT-Ressourcen über Netze (Internet). Typische Merkmale sind die Bereitstellung in Echtzeit als Self Service auf Basis von Internettechnologien (insb. Virtualisierungstechnologie) und die Abrechnung nach Nutzung (pay per use).

Gleichwertige Begriffe und vergleichbare Erscheinungsformen

- Gleichwertige Begriffe: **Cloud Service**, **Cloud Dienste**
- Ähnliche Erscheinungsformen/Vorläufer in der historischen Vergangenheit:
  - **Stromlieferung/Telekommunikation** über öffentliche Netze (Beginn 20. Jh)
  - **Utility Computing** (1960 John McCarthy)
  - **Cluster- und Grid Computing** (ab 1970er)
  - **ASP** (wie Cloud, aber dedizierte Infrastruktur (Hard- und Software) pro Kunde, ab Ende 1990er)
- **Cloud Computing** ist ab 2005 das Ergebnis der technischen Evolution verschiedener HW- und SW-Technologien, selbst aber keine neue Technologie, sondern nur eine eigene Form der Bereitstellung von IT-Leistungen (eigenes Deployment Model)

  geprägt wurde der Begriff ab 2005 durch schnell wachsende Internetfirmen wie Amazon, Google und Yahoo

Technische Grundlagen des Cloud Computing

- ausreichende Leistungsfähigkeit der Netze, Hard- und Software, mobile Devices
- Zusammenfassung der Ressourcen (Virtualisierung der Hardware: physische Ressourcen werden durch eine Software (Hypervisor bzw. Virtual Machine Monitor) in einem virtuellen Pool zusammengefasst; Mandantenfähigkeit der Software: eine einzige Software wird einer Vielzahl von Kunden zur Verfügung gestellt, nur durch eine Programmlogik wird bei der Nutzung zwischen den Kunden separiert)
- Elastizität der Ressourcen (Automatisierte und sofortige Skalierbarkeit der Ressourcen)
- Leistungsbezug über ein Netzwerk (Endgerätunabhängig, insb. auch für mobile Anwendungen)
- Messungen des Ressourcenverbrauchs (z.B. Speicherplatz, CPU-Zyklen, Datenmenge)
- Selbstverwaltung der Ressourcen durch den Kunden

Service Ebenen des Cloud Computing

- Infrastructure as a Service (IaaS)

  Beispiele: Amazon Web Services (AWS); IBM Cloud Services; Fujitsu Cloud; Sealed Cloud der Fa. IDGard

- Platform as a Service (PaaS)

  Beispiele: Force.com; Google App Engine; MS Azure; Heroku;

- Software as a Service (SaaS)

  Beispiele: Mobile Apps; Gliffy; Google Doc; Google-G-Mail; MS Office365; Sales Force CRM; Zoho On-Demand Suite; SAP-Cloud Computing; Sage Online Services

- (X as a Service (XaaS))

  Beispiele:
  - Business Process as a Service (BPaaS),
  - Desktop as a Service (DaaS),
  - Security as a Service (SaaS),
  - Document Management as a Service (DMaaS)
  - Enterprise Content Management as a Servcie (ECMaaS).

Cloud - Betriebsmodelle

- Private Cloud: Cloud für die rein unternehmensinterne Nutzung
- Public Cloud: Cloudangebot an/für die Öffentlichkeit (B2B, B2C)
- Community Cloud: Cloud für bestimmte Gruppe von Nutzern (Konzerngesellschaften; Verbandsmitglieder; Kunden)
- Hybrid Cloud: Kombination der vorgenannten Clouds,

  z.B.

  - in einer Private Cloud eines Unternehmens wird Speicherplatz von einer Public Cloud (IaaS) bezogen;
  - Ein SaaS-Anbieter bezieht die Speicherkapazität aus eine Public Cloud (IaaS)

Sonstige Cloud-Typen

- Regionale Clouds: z.B. Deutsche und Europäische Clouds

  Infolge der Datenschutzdiskussionen der letzten Jahre bieten Cloud Service Provider (CSP) entweder nur noch regionale Clouds an (www.deutsche-wolke.de; www.e-mail-made-in-germany.de) oder bieten dem Kunden die Möglichkeit an, im Rahmen der Selbstverwaltung selbst festzulegen, in welchen Regionen/Ländern die Daten verarbeitet werden dürfen (z.B. bei Amazon Web Services).

- 1st and 2nd Generation Cloud:

  Im „Jahre 10“ des Clouds laufen die ersten Cloudmodelle aus und der Wechsel auf die 2. Generation/neuen Cloud Service Provider steht an.

- B2B-Cloud (mit starker Tendenz zur Regionalisierung und Transparenz) oder B2C-Cloud (mit Tendenz zur Intransparenz)

Abgrenzung von verwandten Erscheinungsformen

- IT-Eigenbetrieb (On Premise IT): heute i.d.R. unter Einsatz einer privaten Cloud
- ASP: Service Provider bietet dem Kunden die Nutzung einer Applikation (Software) an, im Unterschied zum Cloud aber auf einer dedizierten Hard- und Software, die dem Kunden physisch zugeordnet ist.
- Outsourcing / Outtasking: beschreibt den Vorgang der Auslagerung von IT-Leistungen und Aufgaben an einen dritten Service Provider, im Unterschied zum Cloud kann dies auch kundenspezifische/nicht standardisierte Prozesse betreffen und teilt sich i.d.R. auf in einen Transition-Prozess (i.d.R. Werkvertrag) und einen Betriebsprozess (Dienst- oder Werkvertrag).
- Managed Services: Spielart des Outsourcing: ein Service Provider übernimmt und verwaltet definierte Dienstleistungen für seine Kunden (Begriff wird insbesondere verwendet für Hosting Services, VPN-Leistungen, VoIP-Leistungen, Leistungen im Zusammenhang mit Netzwerksicherheit, Kommunikationsdienste)

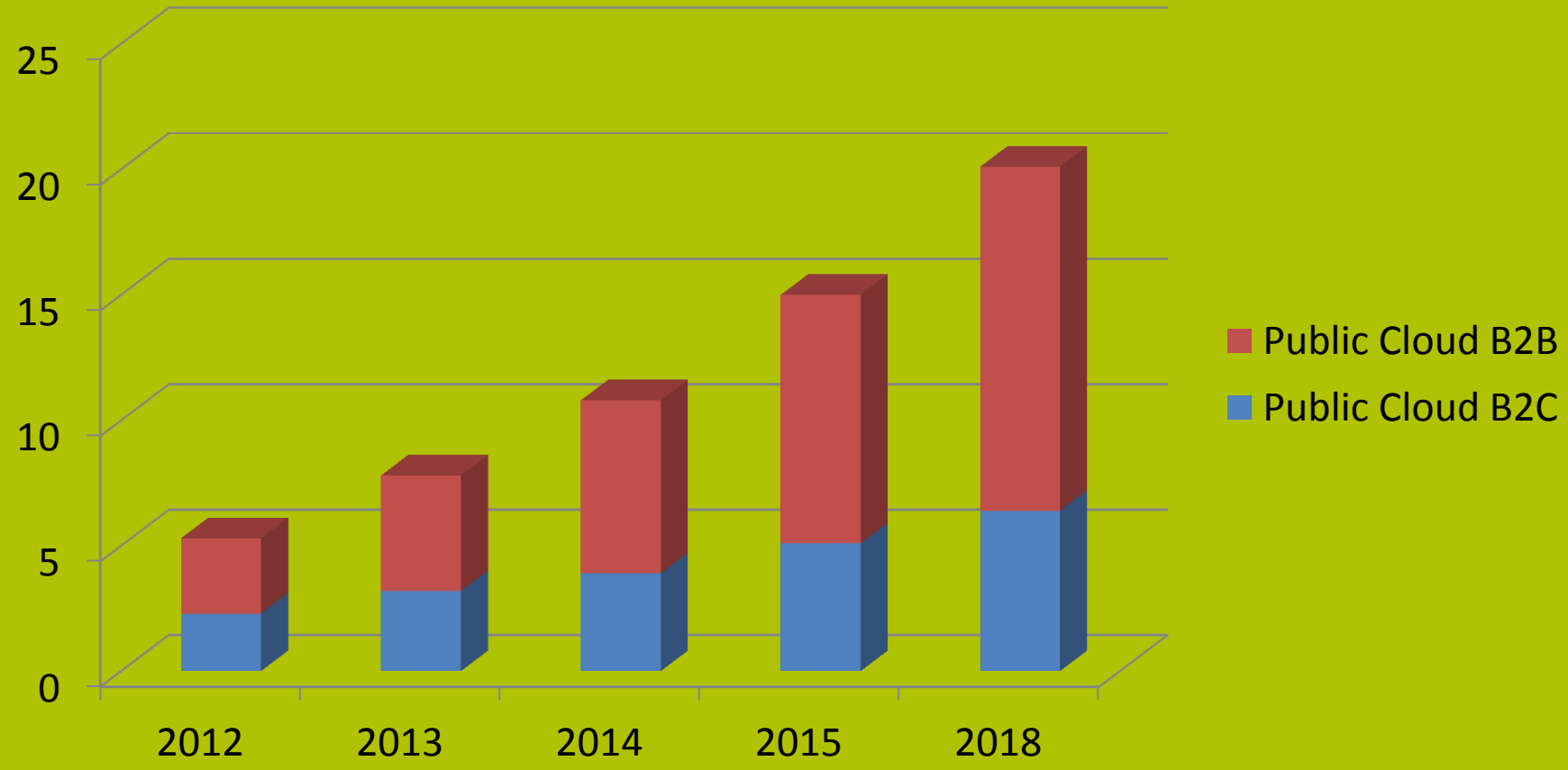
Verbreitung der Cloud

- bei Unternehmen ist **Private Cloud** seit Mitte der 1990er üblich (Intranet mit DMZ)
- **Public Cloud**:
  - ab 2000 Schwerpunkt **im B2C** (webbasierte E-Mail-Lösungen, Apps für mobile Endgeräte)
  - Ausgangspunkt der Public Cloud **im B2B** war u.a. Amazon ab 2005: Der Internet-Versandhändler „litt“ unter wechselnden Spitzenauslastungen seiner IT Systeme, z.B. im Weihnachtsgeschäft. Die Folge war eine Überdimensionierung während des restlichen Jahres. Aus der Not eine Tugend machend, war Amazon einer der ersten Anbieter von Rechenkapazitäten für Dritte.
  - erst seit ca. 2008 starkes Wachstum für Public / Hybrid Cloud-Modelle **im B2B** (Vorreiter Konzerne/KMUs hinken hinterher)

Verbreitung der Public Cloud

Umsatz mit Public Cloud Leistungen in Mrd. Euro in Deutschland

(Quelle: Experton Group/Bitkom e.V., 2013)



Rechtsanwaltsgesellschaft

Weniger geeignete Anwendungsbereiche

(in aufsteigender Reihenfolge)

- personenbezogene Daten sind betroffen
- sensible Betriebsgeheimnisse sind betroffen
- für bestimmte Berufsgruppen aufgrund zusätzlicher gesetzlicher Anforderungen
  (Gesundheitswesen, Verschwiegenheitsträger)
- wegen immer noch zu hohen Geschwindig-keitseinbußen / Verfügbarkeitsproblemen;

  Bsp: Teile einer Produktionssteuerung eines Unternehmens können nicht in die Cloud ausgelagert werden, da dies bei dieser Anwendung noch immer zu nicht akzeptablen Geschwindigkeitsverlusten/Verfügbarkeitsproblemen führt

Vertragsrechtliche Einordnung I

Grobes Raster

- **Mietvertrag**:

SaaS, PaaS, IaaS, ASP

Grund: Überlassung von Ressourcen/Software zur Nutzung durch den Kunden

- **Dienst- oder Werkvertrag**:

XaaS, Managed Services, Outsourcing

Grund: Service Provider nutzt selbst Ressourcen, Technologien (inkl. Software), um einer Dienst- oder Werkleistung (Business Process, Managed Services) gegenüber dem Kunden zu erbringen.

Vertragsrechtliche Einordnung II

Feines Raster für SaaS

- **Miete**:
  - Bereitstellung und Nutzung der Software
  - Speicherkapazität
- Dienst:
  - Unterstützungsleistungen
- Werk:
  - Anpassungsleistungen
  - Datensicherung
  - Datenmigration

Vertragsrechtliche Einordnung II

Feines Raster für IaaS

- **Miete**:
  - Speicherkapazität
  - Server
  - Hardwarekomponenten
- Dienst:
  - Bereitstellung einer Bandbreite
  - Unterstützungsleistungen
- Werk:
  - Datensicherung
  - Installation
  - Datenmigration

Vertragsrechtliche Einordnung II

Feines Raster für PaaS

- **Miete**:
  - Speicherkapazität
  - Bereitstellung und Nutzung von Entwicklungssoftware
  - Bereitstellung und Nutzung von Programmiersprachen
- Dienst:
  - Unterstützungsleistungen
  - Pflege der vom Kunden auf der Plattform eingestellten Software
- Werk:
  - Datensicherung
  - Installation

Public Cloud in Deutschland und AGB-Recht

- Public Cloud Angebote betreffen wegen der gewünschten Skaleneffekte i.d.R. weitgehende **standardisierte Leistungen** auf Basis **standardisierter Prozesse**

  Standardisierungsgrad: IaaS (sehr hoch); PaaS (hoch); SaaS (mittel)
- Die Anbieter sind wegen der immensen Investitionskosten eher **große regionale oder globale Player**, insbesondere bei IaaS oder PaaS
- Cloud bewirkt daher eine „**Industrialisierung der IT**“
- Aus dem vorgenannten Grund wird der Kunde mit **standardisierten Musterverträgen** konfrontiert (wie bei Strom- oder Telekommunikationsanbietern)
- Es besteht daher kaum Raum für individuelle Vertragsgestaltung und führt **bei Verträgen nach deutschem Recht zur Anwendung des AGB-Rechts** mit weitgehenden Konsequenzen für die Anbieter und Kunden.

Public Cloud und AGB-Recht

- Konsequenzen des AGB Rechts für Cloud Service Providers (CSP):
  - Musterverträge unterliegen einer gerichtlichen Inhaltskontrolle sowohl im B2C als auch im B2B;
  - Klauseln, die zu weitgehend vom gesetzlichen Mietrecht zum Nachteil des Kunden abweichen, sind unwirksam, es sei denn, diese wurden „individuell verhandelt“;
  - Es ist für die CSP(s) nahezu unmöglich, Musterverträge zu entwerfen, die diesen Anforderungen standhalten bzw. mit jedem Kunden individuell zu verhandeln;
  - große Rechtsunsicherheit und Risiken für CSP(s).
- Konsequenzen des AGB Rechts für Kunden:
  - Kunden (Unternehmen wie Verbraucher) genießen in Deutschland aufgrund des AGB-Rechts weitgehend Schutz;
  - Wenn Sie nicht verhandeln konnten, gilt weitgehend deutsches Mietrecht, wenn Sie verhandeln konnten, gelten die verhandelten Klauseln, sofern der CSP diese wirklich inhaltlich zur Disposition gestellt hat.
  - Achtung bei Flucht eines CSPs ins ausländische Recht!

Teil II: Chancen und Risiken des Cloud Computing (aus Sicht des Kunden)

Gliederung:

1. **Chancen des Cloud Computing**
   - Wirtschaftliche Vorteile
   - Technische Vorteile
   - Rechtliche Vorteile
   - Ökologische Vorteile
2. **Risiken des Cloud Computing**
   - Organisatorische Risiken
   - Technische Risiken
   - Rechtliche Risiken

Chancen des Cloud Computing

Wirtschaftliche Vorteile:

- Skaleneffekt: Investitionskosten werden auf eine Vielzahl von Kunden umgelegt;
- Ressourcenauslastung wird verbessert: Ein Inhouse Data Center weist ein durchschnittliche Auslastung von 15-20% aus, ein Cloud Data Center eine durchschnittliche Auslastung von 70%);
- Beim Kunden verwandeln sich Kapitalkosten zu Operativen Kosten (von CapEx zu OpEx);
- Kunde erzielt zusätzliche Einsparungen bei Personal- und Energiekosten;
- Kunde kann sich auf das Kerngeschäft konzentrieren.

Chancen des Cloud Computing

Wirtschaftliche Vorteile am Beispiel für Windows Exchange Platinum Server 2013 (25GB)
(Quelle: IT Business im Mittelstand 10/2014 – Was kostet die Cloud, S. 31)

Kostenart	Eigenbetrieb	Cloud Lösung
Lizenzen		
Windows Server 2012 R2 Lizenz (Open)	880,31 Euro	0,00 Euro
Windows Server 2012 R2 User-Lizenz (Open)	335,30 Euro	0,00 Euro
Windows Server 2013 Standardlizenz (Open)	705,95 Euro	0,00 Euro
Windows Server 2013 Benutzerlizenz (Open)	774,70 Euro	0,00 Euro
Hardware		
Durchschnittliches Serversystem, nicht redundant	2.500,00 Euro	0,00 Euro
Externes Backup-Laufwerk inkl. Medien	400,00 Euro	0,00 Euro
Einrichtung		
Einrichtung Exchange-System (ca. 2 PT)	1.800,00 Euro	0,00 Euro
Einrichtung Hardware und Netzwerk (ca. 1 PT)	900,00 Euro	0,00 Euro
Übergabe, Dokumentation, Tests (ca. 0,5 PT)	450,00 Euro	0,00 Euro
Laufende Gebühren		
Raummiete (ca. 3 m²)	360,00 Euro	0,00 Euro
Klimatisierungskosten (ca.)	130,87 Euro	0,00 Euro
Stromkosten (200W/h für Server)	436,25 Euro	0,00 Euro
Wartungsvertrag Exchange 2013 (ca.)	1.200,00 Euro	0,00 Euro
Antispam- und Antivirus-Server	475,20 Euro	0,00 Euro
Cloud-Kosten		
Hosted Exchange	0,00 Euro	838,80 Euro

Chancen des Cloud Computing

Wirtschaftliche Vorteile am Beispiel für Windows Exchange Platinum Server 2013 (25GB)

(Quelle: IT Business im Mittelstand 10/2014 – Was kostet die Cloud, S. 31)

Kostenübersicht (einmalig und jährlich)	Eigenbetrieb	Cloud-Lösung
Einmalige Kosten	8.296,26 Euro	0,00 Euro
Jährliche Kosten	2.111,45 Euro	838,80 Euro
Kostenübersicht (Gesamtkosten)		
1. Jahr	11.348,58 Euro	838,80 Euro
2. Jahr	2.111,45 Euro	838,80 Euro
3. Jahr	2.111,45 Euro	838,80 Euro
4. Jahr	2.111,45 Euro	838,80 Euro
5. Jahr	2.111,45 Euro	838,80 Euro
Gesamtkosten in 5 Jahren	19.794,37 Euro	4.194,00 Euro

Chancen des Cloud Computing

Technische Vorteile:

- Größere Flexibilität und Skalierbarkeit

  Bsp:

  - Unternehmen kann neue Geschäftsprozesse oder Businessmodelle schneller implementieren;
  - Reorganisationen im Unternehmen, M&A Prozesse werden erleichtert;
  - Start-Ups können mit wenig Kapital Business Modelle testen;
  - Zu viel gemietete Ressourcen können untervermietet werden (Kunde wird zum Reseller; es entstehen komplexe Wertschöpfungsnetze).

- Schnelle Realisierbarkeit

  Bsp.: Cloud-Lösungen lassen sich kurzfristig realisieren zum Abfedern von Spitzenlasten oder als Teil der Desaster Recovery Strategie.

- Umsetzbarkeit auch bei geringem Know-How

Chancen des Cloud Computing

Technische Vorteile:

- **Höhere IT-Sicherheit**: CSP erreicht i.d.R. ein Sicherheitsniveau, an welches Unternehmen, insb. KMU(s) nicht heranreichen.
  Bsp. „Sealed Cloud“ der Fa. IDGARD in München
- **Professionalisierung der IT**: CSP erreicht auch in Hinblick auf Qualität/Verfügbarkeit/Performanz des Service also auch in Hinblick auf Professionalität der Mitarbeiter ein höheres Niveau als es bei In-House-Lösungen erreichbar wäre.

Chancen des Cloud Computing

Wirtschaftliche und technische Vorteile

Aus den wirtschaftlichen und technischen Vorteilen wird gefolgert:

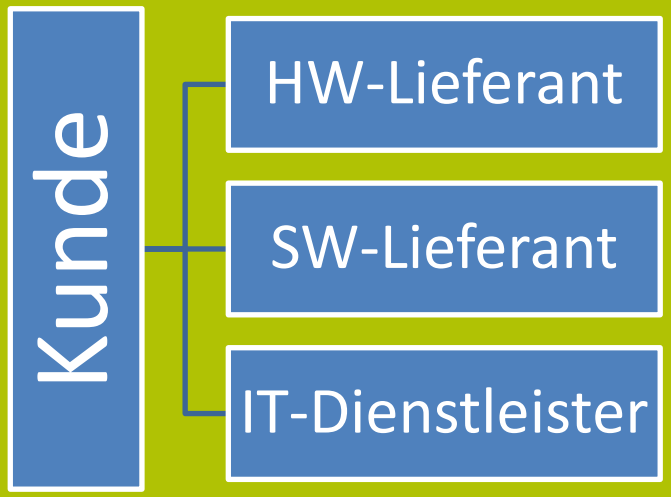
Cloud ist Evolution in der Technik,

Revolution für das Business

Chancen des Cloud Computing

Rechtliche Vorteile

Eigenbetrieb



Situation Cloud

Rechtsanwaltsgesellschaft

Chancen des Cloud Computing

Rechtliche Vorteile

Eigenbetrieb:

- Kunde trägt Schnittstellenrisiken
- Kunde trägt i.d.R. Risiken für verursachte Schäden selbst (es sei denn, er kauft ausnahmsweise beim SW- oder HW-Hersteller)
- Kunde kann allenfalls Nacherfüllung verlangen oder Kaufpreis mindern

Cloud Service:

- Kunde hat oft **kein Schnittstellenrisiko** (Service aus einer Hand)
- Kunde kann CSP **für verursachte Schäden mietrechtlich in Anspruch nehmen**
- Kunde kann zusätzlich **Vergütung mindern** und **Fehlerbeseitigung** verlangen

Chancen des Cloud Computing

Rechtliche Vorteile

Exkurs zur Gewährleistung und Haftung beim Mietrecht:

- **§ 536 a BGB**: CSP haftet für **anfängliche Mängel** verschuldensunabhängig, für **Mängel, die erstmalig während der Laufzeit auftreten**, verschuldensabhängig; bei SW gibt es nur anfängliche Mängel, bei HW auch solche während der Laufzeit (Verschleiß).
- CSP trägt daher – anders als bei Kaufrecht – **Haftungsrisiko für Drittkomponenten**. Dieses Risiko kann der CSP AGB-rechtlich kaum ausschließen;

  Anm: In vergleichbaren Branchen hat der Gesetzgeber reagiert: Gesetzliche Haftungsbegrenzung für TK-Anbieter (§ 44a TKG) und Stromanbieter (§ 18 NAV)
- **§ 536 BGB**: CSP hat daneben – als Teil der Miete - Fehler fortlaufend zu beseitigen und die Cloud zu aktualisieren, so dass sie für den „vertragsgemäßen Gebrauch tauglich bleibt“.
- **Achtung:** „Flucht“ des CSP ins ausländische Recht oder in **§ 536b BGB**: Hinweis auf Mängel bei Vertragsschluss (z.B. SLA)

Chancen des Cloud Computing

Ökologische Vorteile:

- heute verschlingt das Internet (insb. Rechenzentren) bereits erheblichen Anteil des weltweiten Energiebedarfs und trägt entsprechend zum CO2-Ausstoss bei;
- das Web soll um 2030 so viel Strom verbrauchen, wie heute die gesamte Weltbevölkerung (vgl. Die Welt vom 25.11.2011);
- optimierte Ressourcen-Verteilung durch Cloud Services anstelle singulärer Rechenzentren für jedes Unternehmen ist auch ökologisch sinnvoll.

Risiken des Cloud Computing

Organisatorische Risiken:

- **Kontrollverlust (Loss of Governance)**

- **Abhängigkeit vom CSP (Lock-In-Effect)**

Risiken des Cloud Computing

Kontrollverlust (Loss of Governance):

- „Cloud“ impliziert fehlende Transparenz (wo stehen die Rechenzentren? Wo sind die Daten?)
- fehlender Einfluss auf Release-/Produktplanung des CSP
- fehlender Einfluss auf Risk Manangement des CSP(defect oder disaster recovery Planung) des CSP
- fehlender Einfluss auf Personalmanagement des CSP
- fehlender Einfluss auf mögliche Beeinträchtigungen durch Drittnutzer (co-tenant activities) oder durch die Lieferkette des CSP (supply-chain);
- fehlender Einfluss auf das unternehmerische Schicksal des CSP (Insolvenz; Übernahme durch Dritten)

Risiken des Cloud Computing

Abhängigkeit vom CSP (Lock-In-Effect) :

- **fehlende Daten-Standards und anbieterspezifische Schnittstellen** führen zu erheblichen Aufwand bei einem Wechsel des CSP oder im Falle einer Rückführung des Service (insbesondere bei Insellösungen), sog. ungenügende Portabilität

  Seit 2009 gibt es internationale Standardisierungsinitiativen für Interoperabilität und Datenübertragung: Global Inter-Cloud Technology Forum (CMWG); Cloud Auditing Data Federation Work Group (CADF), Cloud Computing Interoperability Forum (CCIF)

- **fehlende Transparenz bei der Abrechnung**: die fehlende Nachprüfbarkeit der Abrechnung (Pay per Use) ist in der Praxis häufig ein Problem (Messtools befinden sich in der Kontrolle des CSP)

Risiken des Cloud Computing

Technische Risiken:

- **Allgemeine IT-Risiken:**

Menschliches Versagen (Passwortverluste), Technisches Versagen, Interne und Externe Angriffe,

- **Cloud spezifische Risiken:**

- Unüberprüfbare Datenhaltung
- Mangelhafte Kontrollmöglichkeiten über CSP
- Vervielfältigung und Verteilung der Daten
- Gesteigerte Komplexität der IT mit Risiken für die Interoperabilität

Risiken des Cloud Computing

Rechtliche Risiken:

- Unüberschaubare Risiken aus fremden Rechtsordnungen
- Konflikt mit Datenschutzrecht
- Konflikt mit Exportkontrollrecht
- Konflikt mit Arbeitsrecht
- Konflikt mit berufs- oder branchenspezifischen Anforderungen

Risiken des Cloud Computing

Risiken aus fremden Rechtsordnungen:

- Gesetzliche oder ungesetzliche Zugriffsmöglichkeiten im Ausland (z.B. subpoena und e-discovery in USA, US Patriot Act)

- Bietet der CSP das Cloud Computing nach ausländischem Recht an, kann das massive Auswirkung auf das Geschäftsmodell und vertragliche Risikoverteilung haben:
  - Angloamerikanische Rechtsordnung: Cloud-Vertrag ist kein Mietvertrag, sondern ähnelt Lizenz- oder Servicevertrag, Maintenance wird separat fakturiert, SLA(s) reduzieren Verfügbarkeiten
  - Deutschland: Teile des Maintenance sind im Mietmodell inkludiert, nur Upgrades werden separat fakturiert, Gesetz geht von 100% Verfügbarkeit aus.

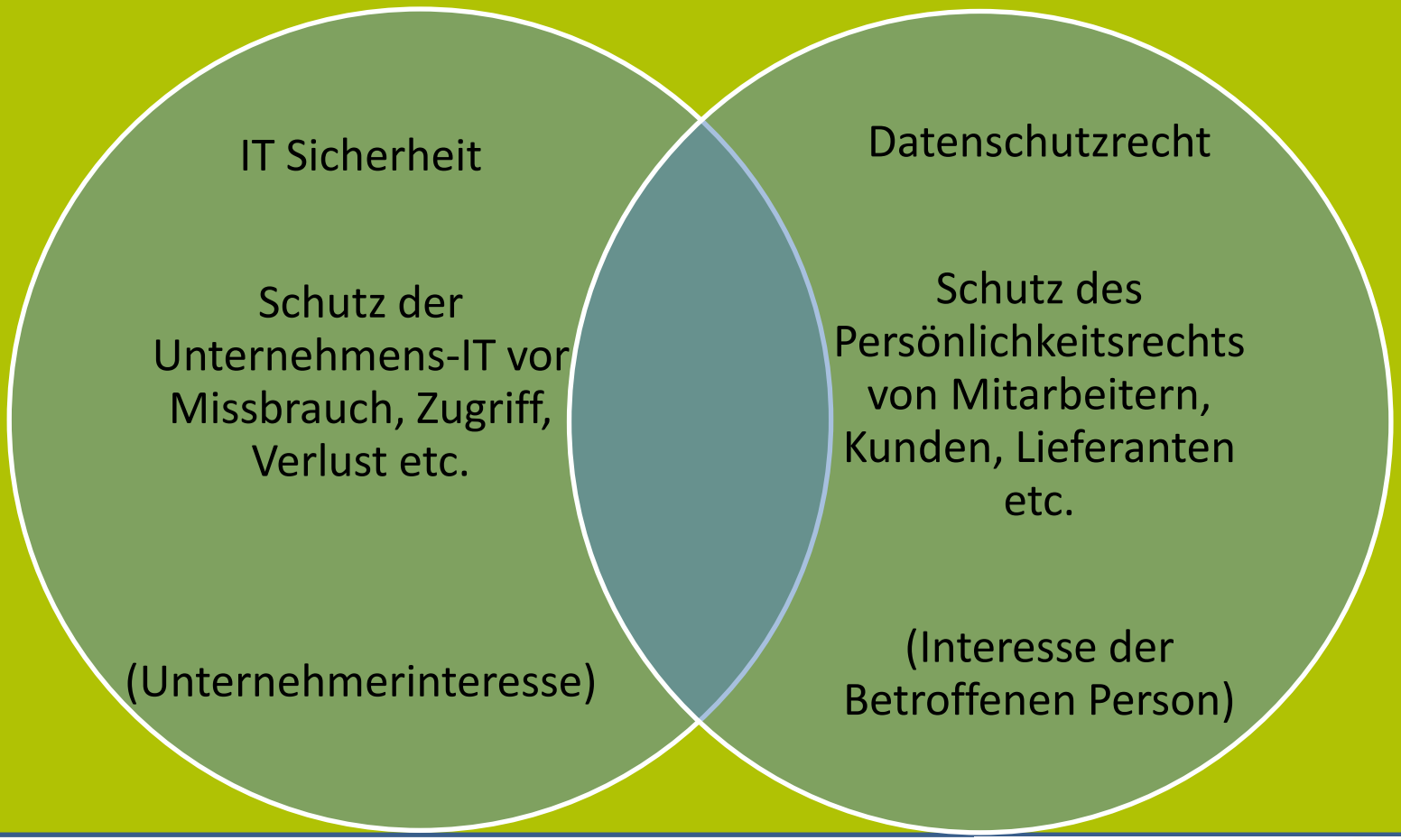
- Urheberrechtliche Probleme

Risiken des Cloud Computing

Konflikt mit Datenschutzrecht:

- Datenschutzrechtlich Anforderungen erfordern spezielle Vertragsgestaltung
- In der Regel besteht Verantwortlichkeit des Auftraggebers (Kunde) für datenschutzrechtlich Compliance des Auftragnehmers (CSP)

Grundzüge Datenschutzrecht I



rbi Rechtsanwaltsgesellschaft

Grundsätze Datenschutzrecht II

- Grundsätzliches Verbot mit Erlaubnisvorbehalt!

- D.h. jegliche Nutzung personenbezogener Daten ist verboten außer die Nutzung ist ausdrücklich gesetzlich erlaubt.

Grundsätze Datenschutzrecht III

- Was bedarf Erlaubnis beim Cloud Computing?
  - § 3 BDSG: Erhebung und Verarbeiten von personenbezogenen Daten bedarf Erlaubnis.
  - Verarbeiten ist das Speichern, Verändern, **Übermitteln**, Sperren und Löschen personenbezogener Daten.
  - **„Übermittlung“ = Senden der Daten in die „Cloud“** (sogar Zugriffsverschaffung auf eigene Server).
  - **Str**: liegt noch Übermittlung personenbezogener Daten vor, wenn diese verschlüsselt sind und Cloud Anbieter Personenbezug nicht herstellen kann?
- Woher kommt gesetzliche Erlaubnis?
  - **Einwilligung** des Betroffenen nicht praktikabel (schriftlich/informiert/jederzeit widerruflich)
  - Gesetzliche Rechtfertigung: v.a. § 28 ff BDSG, wenn zur Wahrung eigener Geschäftsinteressen erforderlich und Abwägung der Interessen im Einzelfall
  - Interesse des Unternehmers an „Outsourcing“ nicht ausreichend für RF nach § 28 BDSG!

Grundzüge Datenschutzrecht IV – Datenschutzrechtliche Erlaubnis b. Cloud

- Woher also Erlaubnis für Übermittlung an Cloud Anbieter?
- Lösung § 3 Nr. 8 BDSG: Ein Dritter, der im Auftrag eines anderen Daten innerhalb der EU verarbeitet, ist kein „Dritter“ im Sinne des BDSG (sog. Auftragsdatenverarbeitung - ADV).
- Damit liegt keine Übermittlung an Dritten vor und es bedarf keiner Erlaubnis.
- Cloud Anbieter wird datenschutzrechtlich als Organisationseinheit des Auftraggebers gesehen; d.h. Auftraggeber ist rechtlich für die Compliance des Cloud Anbieters verantwortlich.
- **Diese Rechtsfolge greift nur, wenn schriftliche ADV im Sinne des § 11 BDSG geschlossen wird.**

Problem der Entgrenzung der Cloud

- Sonderproblem bei Cloud: Entgrenzung, d.h. Anbieter sitzt nicht in EU oder Daten werden auch außerhalb der EU gespeichert („Export“)
- Fiktion des § 3 Nr. 8 BDSG greift im Nicht-EU Bereich nicht mehr, d.h. es liegt eine nach BDSG zu rechtfertigende Übermittlung von Daten vor.
- Lösung:
  - Vereinbarung der sog. EU Standard Terms, wenn kein ausreichendes Schutzniveau im Zielland oder Safe Harbour (Anwendung ohnehin strittig)
  - Dokumentation des Abwägungsvorgang nach § 28 BDSG, idR auch Abschluss einer ADV

Datenschutzrecht und Cloud – Die ADV

- Erforderlicher Vertragsinhalt der ADV in § 11 BDSG geregelt.
- Kern: Da Auftraggeber für Einhaltung des Datenschutzrechts verantwortlich ist stellt ADV sicher, dass er dies gegenüber dem Cloud Anbieter sicherstellen kann. Grundproblem des AG in Cloud ist fehlende Transparenz (Speicherorte, Wer hat Zugriff, etc.). Deshalb v.a. zu regeln:
  - Umfang und Inhalt von Weisungsrechten
  - Speicherorte
  - Zugangsrechte, z.B. Recht zur Untervergabe
  - Kontrollrechte
- Zusätzlich werden technisch-organisatorische Maßnahmen („TOMs“) des Cloud Anbieters vertraglich festgelegt (Verschlüsselung, Zugangskontrollen etc.).
- Achtung: Fehlen schriftlicher ADV kann für beide Seiten OWI-Tatbestand darstellen

Fazit Datenschutzrecht und Cloud

- Cloud Computing und Datenschutzrecht kein Widerspruch an sich.
- Aus Datenschutzrecht aber rechtliche und organisatorische Anforderungen sowohl an Auftragnehmer als auch an Auftraggeber.
- In der Praxis erleichtern Dienstleister oft durch Standardverträge (ADV) und Prozesse (Vorlage TOMs, Zertifikate, Testate etc.).
- EU-basierte Clouds haben geringere Anforderungen und größere Professionalität der Anbieter in DS-rechtlichen Belangen (ADV, Zertifizierungen, etc.).

Risiken des Cloud Computing

Konflikt mit Exportkontrollrecht:

Die Ausfuhr von **sensiblen elektronischen Daten** (Software, Informationen über die Herstellung sensibler Güter) kann eine Exportgenehmigung erfordern;

- EU-Exportkontrolle: Bereits der Upload von genehmigungspflichtigen Daten in die Cloud ist genehmigungspflichtig nach Artt. 1 u. 3 EG-Dual-Use-VO;
- US-Exportkontrolle: Werden Daten in die Cloud gestellt, die das Produkt von US Gütern/Software ist, kann auch US-Exportkontrollrecht gelten.

Risiken des Cloud Computing

Konflikt mit Steuerrecht:

Will der Kunde steuerrechtlich relevante Daten (Fibu) in die Cloud stellen, gilt Folgendes:

- Verarbeitung in Deutschland: kein Problem
- Verarbeitung in der EU: **Bewilligung** durch Finanzamt auf Antrag erforderlich (§ 146 Abs. 2a AO);
- Verarbeitung außerhalb der EU: **Bewilligung** erfolgt nur, falls **nachgewiesen** wird, dass die Besteuerung nicht beeinträchtigt wird (§ 146 Abs. 2a S.5 AO)

Risiken des Cloud Computing

Konflikt mit Arbeitsrecht:

Digitales Zugangssystem für die Cloud kann ein Mitbestimmungsrecht des Betriebsrates bei der Einführung von Cloud-Services gemäß § 87 Abs. 1 Nr. 6 BetrVG auslösen, da eine Überwachung des Arbeitsverhaltens und der Arbeitsleistung der zugangsberechtigten Mitarbeiter durch den Arbeitgeber möglich ist.

Risiken des Cloud Computing

Konflikt mit spezifischen berufs- oder branchen-spezifischen Anforderungen:

- **Banken/Versicherungen:** Besondere Vorgaben (KWG i.V.m. MaRisk; VAG) an Banken/ Versicherungsunternehmen bei der Auslagerung von Versicherungs- und Bankdaten;
- **Gesundheitswesen:** An die Verarbeitung personenbezogener Gesundheitsdaten in der Cloud werden durch das BDSG besondere Anforderungen gestellt;
- **Verschwiegenheitsverpflichtete Berufsträger**: Berufsträger, die gesetzlichen Verschwiegenheitspflichten unterliegen (§ 203 StGB) wie z.B. Anwälte, Ärzte, können Dienste, die vertrauliche Daten verarbeiten, nur mit Risiken in die Cloud auslagern.

Teil III - Möglichkeiten zur Reduzierung der Risiken

- **Einführung Cloud-spezifischer Unternehmensprozesse**
  - Strategie
  - Beschaffung
  - Management und Überwachung
- **Reduktion vertraglicher Risiken**

Einführung Cloud-spezifischer Unternehmensprozesse

Klassischer Beschaffungsprozess beim IT- Eigenbetrieb

IT Fachabteilung
- Bedarfsanalyse
- Budgetfreigabe

Einkauf
- Lieferantenauswahl
- Verhandlung

Legal Department
- Finale Verhandlung und Freigabe des Einkaufvertrages
- Abschluss Beschaffung

Involvierte Stakeholder

rbi Rechtsanwaltsgesellschaft

Einführung Cloud-spezifischer Unternehmensprozesse

Notwendiger Prozess für Cloud-Einführung

Involvierte Stakeholder

Cloud Strategie	•Erstellung einer Cloud Strategie ist ein eigenes unternehmensinternes Projekt •Beteiligung aller wesentlichen Stakeholder	GF, CIO, LD, HR, Export, Datenschutzb.
Vorbereitung und Planung	•Auf Basis der Strategie werden auszulagernde Funktionen/Applikationen/ Ressourcen identifiziert •Vorbereitung der Integration in bestehende Unternehmensprozesse	IT, Einkauf, Fachabt.
Auswahl eines CSP	•Kriterienkatalog für Anbieterauswahl •Benchmarking der Anbieter	IT, Einkauf, LD
Vertrag und Detail-planung	•Verhandlung mit einem oder mehreren Anbietern (Shortlist) •Detailplanung bzgl Integration der Cloud-Services in bestehende Unternehmensprozesse	LD, HR, Export, Datenschutzb.
Migration und Betrieb	•Migration / Customizing zum Zwecke der Inbetriebnahme der Cloud-Services •Betrieb: fortlaufende Aktualisierung der Sicherheit, Benchmarking-Prozess, Auditierungs-Prozess, SLA-Überprüfung	IT , Contract Management

Einführung Cloud-spezifischer Unternehmensprozesse

- Der Schritt in die Cloud ist mit einem komplexen Entscheidungsprozess verbunden, der die Einbindung einer Vielzahl von Entscheidungsträgern (Stakeholder) erfordert

  Abwägung zwischen wirtschaftlichen/technischen und rechtlichen Vorteilen (siehe oben Punkt 2.) gegenüber organisatorischen, technischen, rechtlichen Risiken (siehe oben Punkt 3.), jeweils mit unterschiedlichen Eintrittswahrscheinlichkeiten

- Der klassische IT Beschaffungsprozess eignet sich nicht für Cloud Computing (Haftungsrisiko für CIO/Geschäftsführung wegen Organisationsverschulden)

Reduktion vertraglicher Risiken

Reduktion vertraglicher Risiken muss in zwei Phasen erfolgen:

- **Bei der Auswahl des CSP (Benchmark der T&C(s))**
- **Bei der Verhandlung mit dem CSP**

Reduktion vertraglicher Risiken

Auf folgende Regelungsmöglichkeiten sollten Kunden in den beiden Phasen (Benchmark/ Verhandlung) achten:

1. **Klauseln zum Schutz vor Loss of Governance**
2. **Klauseln zum Schutz vor Lock-In Effekten**
3. **Klauseln zum Schutz vor technischen Risiken**
4. **Klauseln zum Schutz vor rechtlichen Risiken insb. vor Datenschutzrisiken**

Klauseln zum Schutz vor Loss of Governance

- Zustimmungsvorbehalt für Sublieferanten
- Festlegung der Datenverarbeitungsorte
- Zustimmungsvorbehalt für Verlagerung der Datenverarbeitung
- Zustimmungsvorbehalt für Austausch von Schlüsselpersonal, ggf. zusätzlich ein Austauschrecht
- Mindestvorgaben an die Leistung (SLA, Performance, Redundanz)
- Mindestvorgaben an die Qualität des Personals
- Auditierungsklauseln (zwingend für BDSG)
- Regelung zu den technischen und organisatorischen Maßnahmen zum Datenschutz (zwingend für das BDSG)
- Regelungen zur Prüfbarkeit der Leistungsmessung und Abrechnung
- Regelungen zur künftigen Release-Entwicklung oder zum Schutz vor einseitigen Leistungsänderungen durch CSP (Einstellung von Funktionen)
- Regelungen für Eskalationsprozessen

Klauseln zum Schutz vor Lock-In Effekten

- Einseitige Verlängerungsoptionsrechte des Kunden;
- Angemessene Auslauffristen im Falle der Kündigung;
- Klauseln zu Termination Support durch CSP, zum Exit Management (Datenmigration zum Zwecke der Rückführung bzw. Überleitung auf neuen CSP);
- Escrow-Vereinbarungen; Vertragsübernahme durch anderes Glied in der Lieferantenkette;
- Klauseln zur Absicherung der Business-Continuity/ zur Disaster Recovery

Klauseln zum Schutz vor technischen Risiken

- SLA´s (Verfügbarkeiten, Reaktions- und Instandsetzungs-zeiten)
- Regelungen zu den technischen und organisatorischen Maßnahmen zum Datenschutz/Sicherheit (im Bereich Datenschutz ist dies Teil der ADV)
- Regelungen zur Datenintegrität, zur Portierbarkeit (Datenformate)
- Regelungen zur Rechteverwaltung (Zugangsrechte, Passwörter)
- Regelungen zur Verschlüsselung
- Regelungen zur Umfang der Redundanz
- Regelungen zum Back-Up

Klauseln zum Schutz vor rechtlichen Risiken insb. Datenschutzrisiken

- Spezielle am Telekommunikationsgeheimnis ausgerichtete Geheimhaltungsklauseln
- Compliance-Klauseln
- Exportkontrollklauseln
- ADV-Vereinbarungen u. ggfs. EU Standard Terms
- Freistellungsklauseln für Schutzrechtsprobleme
- Meldepflichten des CSP für Risikolagen (co tenant-activities; interne oder externe Angriffe)