

Schweres Wetter:
Rechtliche Aspekte des Cloud Computing

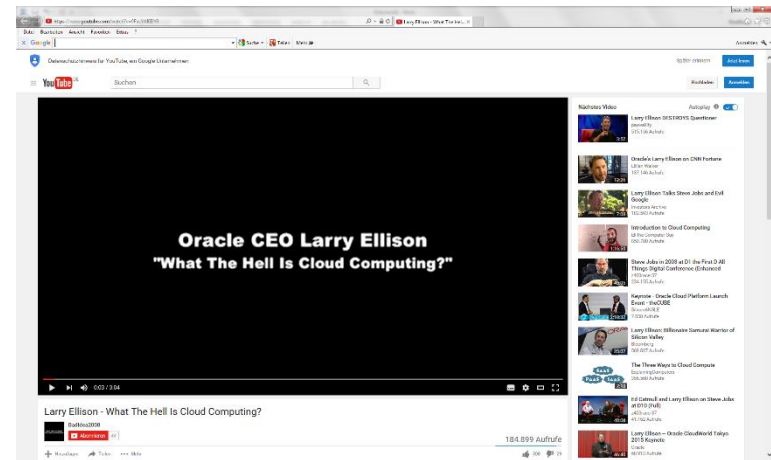
DNJV Frühjahrstagung
Rovaniemi, 21. Mai 2016

Übersicht:

Service aus dem Netz – so einfach wie Strom aus der Steckdose?

1. Was ist Cloud Computing?
2. Vertragsrecht und -praxis
3. Datenschutzrecht
4. Informationssicherheit, Compliance
5. Exkurs: Cloudnutzung in der anwaltlichen Praxis
6. Weitere Untiefen
7. Fazit und Ausblick

1. Was ist Cloud Computing?



<https://www.youtube.com/watch?v=0FacYAI6DY0>

“The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements. The computer industry is the only industry that is more fashion-driven than women's fashion.”

Larry Ellison (2008)

1. Was ist Cloud Computing?

→ grundlegende *technologische* Aspekte

- *Virtualisierung* von IT-Infrastrukturen einschl. HW, Netzwerke, Speicher- und Rechenkapazität, SW
- Unterschied zum *Application Service Providing*: bei ASP Koppelung an konkrete HW, meist Installation einer Zugriffs-SW erforderlich, Cloud ist mehrmandantenfähig („*one to many*“), weniger kundenindividuelle Anpassungen
- *Dynamisierung* durch Anpassung an Bedarf des Nutzers
- *Entlokalisierung* = von überall zugänglich
- *Streubesitz* an Daten durch Verteilung und Verarbeitung auf (verschiedenen) Servern, u.U. weltweit („*follow the sun*“)

1. Was ist Cloud Computing?

➔ grundlegende *technologische* Aspekte:
Unterscheidung nach Angebotsinhalt

- *SaaS*: Software as a Service = SW-Applikation
- *PaaS*: Plattform as a Service = Entwicklungsumgebung
- *IaaS*: Infrastructure as a Service = Prozessorleistung, Rechenkapazität, virtuelle HW-Ressourcen
- *SECaaS*: Security as a Service = IT-Sicherheitsmaßnahmen
- *BPaaS*: Business Process as a Service
- *XaaS* = Bündelung mehrerer Dienste

High Troposphere		Medium Troposphere		Low Troposphere		Towering vertical & Other-Accessories clouds			Surface based		
Ci spi	Cirrus spissatus	Ac flo	Alto cumulus floccus	Cu fra	Cumulus fractus	Cu con	Cumulus congestus	Vg	Vilga	Br	Brume
Ci fi	Cirrus fibratus	Ac cas	Alto cumulus castellatus	Cb cal	Cumulus humilis	Cu cir	Cumulonimbus calvus	Ro	Roll cloud	Fo	Fog
Ci unc	Cirrus uncinus	Ac lcs	Alto cumulus lenticularis	Cu med	Cumulus mediocris	Cb inc	Cumulonimbus incus	Ss	Shelf cloud		
Cc flo	Cirrocumulus floccus	As	Altostratus	Sc	Stratocumulus	Ae	Anvil	Wc	Wall cloud		
Cc fle	Cirrostratus fibratus			St	Stratus	Mn	Mammatus	Fc	Fusiel cloud		
Cc neb	Cirrostratus nebulosus			Ns	Nimbostratus	Pl	Pileus				

Realized by Antonio Ciccolella
on/2018

1. Was ist Cloud Computing?

➔ grundlegende *technologische* Aspekte:
Unterscheidung nach Benutzerkreis

- *Private Cloud*: unternehmensinternes (standortübergreifendes) Netzwerk
- *Public Cloud*: unbestimmte Zahl an Anwendern
- *Community Cloud*: geschlossener Benutzerkreis aus mehreren Private Clouds
- *Hybrid Cloud*: Kombination von Private und/oder Public und/oder Community Clouds

1. Was ist Cloud Computing?

→ grundlegende *technologische* Aspekte:
Lokalisation

- Deutsche Cloud
- EU-Cloud (einschl. EWR)
- Weltweite Cloud

1. Was ist Cloud Computing?

→ grundlegende *wirtschaftliche* Aspekte

Vorteile:

- ➔ Skalierbarkeit
- ➔ wenig Investitions-, Betriebs-, Wartungsaufwand
- ➔ nutzungsabhängige Vergütung
- ➔ immer Stand der Technik
- ➔ überall Zugriff
- ➔ *SW wird zum Bedarfsgegenstand*

Nachteile:

- ➔ Intransparenz der Prozesse und u.U. der Kosten
- ➔ Risiko mangelnde Daten- und IT-Sicherheit
- ➔ Interoperabilität, Integration von Applikationen
- ➔ *Abhängigkeit*
- ➔ *Verlust der Kontrolle auf Daten und Prozesse*
- ➔ *Kritikalität der SW in Bezug auf Sicherheit und Verfügbarkeit*



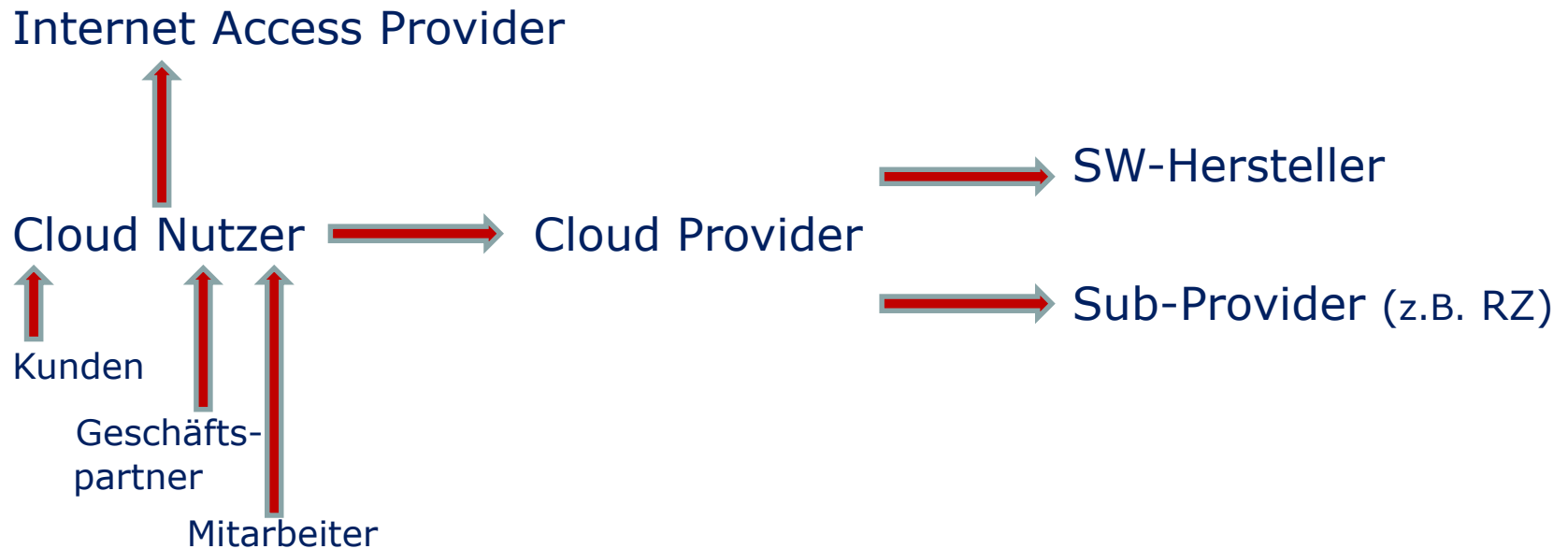
1. Was ist Cloud Computing?

→ grundlegende **rechtliche** Aspekte:
Herausforderungen bei der Vertragsgestaltung

- Internationalität
- Mehrzahl von Prozessbeteiligten
- Standardisierung der Vertragsbedingungen
- Parteien meist nicht auf Augenhöhe
- Kritikalität der Leistung für den Anwender
- u.U. Online-Vertragsschluss
- Datenschutz, Informationssicherheit

1. Was ist Cloud Computing?

→ grundlegende **rechtliche** Aspekte:
die Prozess- und Vertragskette



1. Was ist Cloud Computing?

→ grundlegende *rechtliche* Aspekte:
betroffene Daten

- Personenbezogene Daten (§3 Abs. 1 BDSG)
- Geschäftsgeheimnisse, insbes. Know-how, IP
- sonstige unternehmensrelevante Informationen
- Big Data
- ...und zwar jeweils eigene und/oder solche, die von Dritten stammen

2. Vertragsrecht und -praxis

→ *Rechtswahl*

- wenn keine ausdrückliche Rechtswahl: i.d.R. Recht am Sitzort der Partei, die die vertragscharakteristische Leistung erbringt
- *Rechtswahl unbedingt vertraglich regeln*
- ggf. trotz Rechtswahl zwingend anwendbare Normen (bspw. Verbraucherschutz, Datenschutz)
- trotz Rechtswahl/Gerichtsstand Problem der Durchsetzbarkeit von Ansprüchen, Vollstreckbarkeit
- Sonderaspekt: Deliktsrecht (Bsp. Datenverlust oder -beschädigung), Stichwort Streuschaden – wohl Koppelung an Vertragsstatut

2. Vertragsrecht und -praxis

→ (deutsche) Vertragstypologie



2. Vertragsrecht und -praxis

→ *(deutsche) Vertragstypologie*

- BGH 2006: ASP = überwiegend mietrechtlicher Charakter
- zu Cloud: Schrifttum uneinheitlich
- Tendenz: jedenfalls SaaS ebenfalls überwiegend mietrechtlich
- bei IaaS/PaaS möglich: überwiegend dienstvertraglicher Charakter

Einordnung wichtig wegen:

- Ausfüllung evtl. vertraglicher Regelungslücken
- Rechtsfolgen, z.B. Mängelansprüche
- und:



2. Vertragsrecht und -praxis

→ *(deutsche) Vertragstypologie*



AGB sind wegen unangemessener Benachteiligung unwirksam, wenn die Klausel mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht vereinbar ist (§307 BGB)

2. Vertragsrecht und -praxis

→ *Leistungsbeschreibung*

- Je kritischer die Prozesse, desto detaillierter die Leistungsbeschreibung
- Kontrolle (bewahren), bspw. Ort der Datenverarbeitung
- Abhängigkeiten (vermeiden), bspw. proprietäre Datenformate
- Keine AGB-Kontrolle für reine Leistungsbeschreibungen
- Abgrenzung zu verkappten Haftungsbeschränkungen
- Beistellungen, Mitwirkungspflichten (💣 Bsp. Datensicherung)
- Leistungsverweigerungsrechte, Sperrung



2. Vertragsrecht und -praxis

➔ *Service Levels*

- Verfügbarkeit
 - ➔ % pro Zeitraum, max. Ausfallzeit am Stück
 - ➔ Berechnung und Ausnahmen (bspw. Wartung)
 - ➔ Übergabe-/Messpunkte und Monitoring
- Reaktions- und Lösungszeiten bei Störungen
 - ➔ für verschiedene Fehlerklassen
- Sanktionierung bei Nichterreichung
 - ➔ Service Credits
 - ➔ Minderung vs. pauschalierter Schadensersatz vs. Vertragsstrafe
 - ➔ Verhältnis zu sonstigen Rechtsbehelfen

2. Vertragsrecht und -praxis

→ *Urheberrechtliche Aspekte*

- Ebene SW-Hersteller – Cloud Provider
 - ➔ CP braucht Berechtigung zur Vervielfältigung und öffentlichen Zugänglichmachung, ggf. auch Bearbeitungsrechte
 - ➔ Berechtigung zur Einschaltung von Sub-Providern, bspw. RZ
- Ebene Cloud Provider – Cloud Nutzer
 - ➔ i.d.R. einfache, zeitlich beschränkte, nicht übertragbare und nicht unterlizenzierbare Nutzungsrechte
- Nachgeschaltete User („Sekundärnutzungsberechtigte“)
 - ➔ Konzernlizenzen
 - ➔ Direktzugriff für Kunden, Geschäftspartner des Cloud Nutzers
- Auffangklausel §31 Abs. 5 UrhG Zweckübertragungslehre

2. Vertragsrecht und -praxis

→ Gewährleistung, Haftung

- Mietrechtliche Gewährleistung = ständige Aufrechterhaltung der vertragsgemäßen Nutzungsmöglichkeit
- §536a BGB verschuldensunabhängige Schadensersatzhaftung für anfängliche Mängel
- Typische Haftungsbeschränkungen: 
 - ➡ Kardinalpflichtverletzung
 - ➡ Summenmäßige Beschränkung
 - ➡ Ausschluss mittelbarer und Folgeschäden
 - ➡ Daten- und Programmverlust
 - ➡ §44a TKG
-  Nach deutschem Recht sind Haftungsbeschränkungen in AGB quasi unmöglich.

2. Vertragsrecht und -praxis

➔ *EXIT-Klauseln*



- Ordentliche Kündigungsfristen ggf. unterschiedlich für Cloud Provider und Cloud Nutzer
- Fristlose Kündigungsgründe definieren
- *Abwicklung bei Vertragsende:*
 - ➔ Datenrückgabe, -löschung
 - ➔ Migrationsunterstützung auf neuen Dienstleister
- *Absicherung der Nutzung bei Wegfall des Providers:*
 - ➔ Escrow (?) bei Cloud eher ungewöhnlich, praktischer Nutzen fraglich

3. Datenschutzrecht

- Datenschutzrecht = öffentliches Recht ➡ keine Rechtswahl
- Problem: Daten/~verarbeitung EU-/weltweit verstreut
- §1 Abs. 5 BDSG: grds. Territorialitätsprinzip
- Ausnahme: Sitzlandprinzip für Cloud Provider in EU/EWR
- Rückausnahme: wenn Cloud Provider Niederlassung in DE
- ab Mai 2018: Art. 3 EU-DS-GVO Markortprinzip
- wenn Cloud Provider außerhalb EU/EWR: BDSG, wenn Datenverarbeitung in DE startet
- Problem: angemessenes Schutzniveau
- ➡ Umgehung BDSG nahezu unmöglich
- Folgeproblem: Durchsetzbarkeit Einhaltung BDSG beim Cloud Provider

3. Datenschutzrecht

→ Grundsätze

- Erheben, Verarbeiten, Nutzen personenbezogener Daten
- ...durch Cloud Nutzer und Cloud Provider bzw. über die von ihm bereitgestellte IT-Architektur
- jeder Datenrelevante Vorgang muss auf seine Zulässigkeit hin untersucht werden, bspw.
 - Erheben beim Cloud Nutzer
 - Hochladen in die Cloud
 - dort Speicherung und Verarbeitung, bspw. Zusammenführen mit anderen Daten
 - Weitergeben innerhalb der Cloud oder in andere Cloud
 - Bereithalten zum Abruf durch Dritte

3. Datenschutzrecht

→ *Auftragsdatenverarbeitung §11 BDSG*

- Vorteil: Transfer zum Cloud Provider muss nicht als eigenständiger Übermittlungsvorgang gerechtfertigt werden
- kommt nur für DE- und EU/EWR-Cloud in Betracht §3 Abs. 8 BDSG
- Abzugrenzen von *Funktionsübertragung*
- Voraussetzungen:
 - Cloud Nutzer = ADV-AG „Herr der Daten“
 - schriftlicher Vertrag
 - Cloud Provider = ADV-AN unterliegt Weisungen
 - technische/organisatorische Schutzmaßnahmen §9 BDSG
 - Problem: **Kontrolle** §11 Abs. 2 Satz 4 BDSG
- wenn (-) dann ggf. Rechtfertigung der Datenübermittlung gem. §28 Abs. 1 Nr. 2 BDSG (*Interessenabwägung*)

3. Datenschutzrecht

→ *Cloud Provider in sog. Drittländern*

- bei Cloud Provider außerhalb EU/EWR wg. §3 Abs. 8 BDSG keine Auftragsdatenverarbeitung
- ↗ Transfer zum Cloud Provider muss als Übermittlungsvorgang gerechtfertigt werden
- bei Übermittlung in Drittländer Problem: **angemessenes Schutzniveau**, herzustellen bspw. über:
 - Binding Corporate Rules (Großkonzerne)
 - EU-Standardvertragsklauseln
 - Angemessenheitsbeschluss EU-Kommission, bspw. CH, CA
 - USA: 2000 bis 2015 Abkommen EU-Kommission mit FTC



3. Datenschutzrecht

→ *Cloud Provider in den USA – das Ende von Safe Harbor*

- 6.10.2015 EuGH: Kommissionsentscheidung bzgl. Safe Harbor ist ungültig
- Reaktionen: Umstellung auf EU-Standardvertragsklauseln
💣 laut einigen Datenschutzbehörden ebenfalls problematisch
- Bußgeldverfahren gegen Unternehmen, die noch nicht umgestellt haben → Hamburg: HmbBfDI hat 40 Unternehmen angeschrieben, 7 Bußgeldverfahren eingeleitet (Info Stand 19.4.2016)
- derzeit Diskussion über neues Abkommen *EU-US Privacy Shield*
- Verhaltensempfehlung:



KEEP
CALM
AND
LOOK
BUSY

3. Datenschutzrecht

→ *EU-Datenschutz-Grundverordnung*

- 4.5.2016 Veröffentlichung im Amtsblatt der EU
- Geltung ab **25.5.2018**
- keine ausdrückliche Regelung zum Cloud Computing
- **Art. 3: Markortprinzip** = DS-GVO gilt auch für außereuropäische Unternehmen, die als „Verantwortliche“ oder „Auftragsverarbeiter“ auf dem europäischen Markt tätig sind (selbst wenn die eigentliche DV nicht in der Union stattfindet)
- **Art. 28:** Auftragsverarbeiter (systematisch orientiert an §11 BDSG)
- **Art. 44 ff.:** Datenübermittlung in Drittländer (ähnlich bisherigen Grundsätzen, *angemessenes Datenschutzniveau* etc.)
- **Art. 83:** Bußgelder bis 4% des weltweiten Jahresumsatzes bzw. € 20 Mio. (der höhere Betrag zählt, Datenschutzrecht als „neues Kartellrecht“)

3. Datenschutzrecht

➔ Herausforderung Data Economy

- Cloud Provider kann „im Vorbeigehen“ massenweise Daten sammeln, auswerten, *kommerzialisieren*
- eigene Wertschöpfung aus den vom Cloud Nutzer eingestellten Daten und nebenbei anfallenden Metadaten
- §87a UrhG Recht des Datenbankherstellers
- ➔ künftig *Datenverwertungsklausel* in Verträge



4. Informationssicherheit, Compliance

➔ *Schwachstellen und Risiken des Cloud Computing*

- Daten weltweit gestreut ➔ Risiko Kontrollverlust
- Sabotage / Spionage (insb. Hacking), Datenlecks ➔ Risiko Datenverlust, -beschädigung, -manipulation, -zerstörung, Verlust unternehmenskritischer Informationen
- insgesamt: hohe Risiken für **Verfügbarkeit, Unversehrtheit, Vertraulichkeit und Authentizität** von Daten und Prozessen
- plötzliche Insolvenz des Cloud Providers 💣 Escrow bei SaaS nicht üblich und praktischer Nutzen sowieso fraglich
- Stress bei Vertragsbeendigung und -abwicklung (Bsp. Datenherausgabe)

4. Informationssicherheit, Compliance

➔ *Prozessgestaltung beim Cloud Nutzer*

- 1. Stufe: In-house Datenschutz und IT-Sicherheit
- 2. Stufe: sorgfältige Auswahl des richtigen Cloud Providers
 - ➔ Orientierung an **Zertifizierungen** (bspw. **ISO 27018**)
 - ➔ je nach Daten-Kritikalität und Sensibilität ggf. nur EU-Cloud
 - ➔ besonders sensible Daten ggf. nicht auslagern
- 3. Stufe: Absicherung gegenüber Cloud Provider
 - ➔ Verpflichtungen nach **§11 BDSG (Art. 28 EU-DS-GVO)**
 - ➔ IT-Security Rules
 - ➔ IT-spezifische Versicherung verlangen
 - ➔ laufend kontrollieren, bspw. WP-Prüfberichte verlangen

Arbeitshilfen: z.B. www.trusted-cloud.de



5. Exkurs: Cloudnutzung in der anwaltlichen Praxis



- Strafrechtlich sanktionierte Pflicht zur Geheimniswahrung §203 StGB
- ein dem Anwalt *anvertrautes Geheimnis* (i.d.R. gesamte Mandantenakte) darf nicht unbefugt *offenbart* werden
- *Offenbarung durch Cloudnutzung?*
 - für Offenbarung ausreichend wenn Zugriffsmöglichkeit auf Daten
 - Offenbarung (-) wenn *nur Speicherung* in der Cloud und Einsatz von Standard-Technik Verschlüsselung
 - Offenbarung (+) wenn *auch Verarbeitung* in der Cloud (SaaS), denn DV in verschlüsseltem Zustand nach SdT wohl nicht möglich
- kein Ausweg, den Cloud Provider als *berufsmäßig tätigen Gehilfen* i.S.v. §203 StGB zu betrachten
- Ausweg über *Einwilligung* denkbar, aber praktisch praktische Herausforderung, alle denkbaren DV-Prozesse im Voraus zu erfassen

6. Weitere Untiefen

- Arbeitsrecht, insbes. Mitbestimmung Betriebsrat
- Steuerrecht, wg. AO elektron. Bücher nur in EU-Cloud
- GoB, GoBS
- Straf- und Strafprozessrecht, z.B. Ermittlungsbefugnisse
- Cloudnutzung durch Behörden, Vergaberecht
- Kartellrecht, marktbeherrschende Stellung großer Cloud Provider
- Sozialgeheimnis
- Bankgeheimnis, §25 KWG, MaRisk
- Fernmeldegeheimnis §88 TKG

7. Fazit und Ausblick

- Cloud Computing ist doch nicht nur neuer Wein in alten Schläuchen
- hohe Skalierbarkeit vs. höhere Risiken für Daten und Prozesse, deren Verlust oder Beschädigung den Fortbestand des Unternehmens gefährden kann
- durch das Ende von Safe Harbor im Focus der Datenschutzbehörden
- wachsende Herausforderungen im Zuge der Data Economy



Vielen Dank für Ihre Aufmerksamkeit !

SCHULZ NOACK BÄRWINKEL
RAin Corinna Rindfleisch
Baumwall 7
20459 Hamburg
www.snb-law.de
Tel. 040/36 97 96 0
Fax 040/36 20 88
c.rindfleisch@snb-law.de

