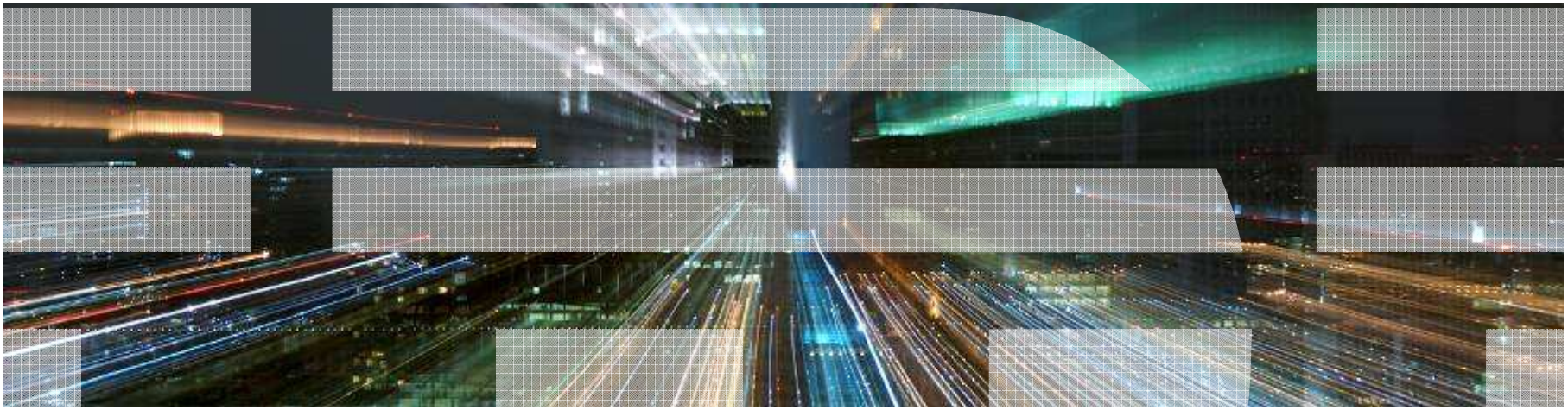
**Dr. Oliver Schaar, Rechtsanwalt**

# Rechtsfragen zu Cloud Computing

## Bird&Bird Law Camp 2011, Frankfurt, 02. April 2011



# Vorbemerkung

- **Cloud Computing ist kein Hype mehr, sondern “sichtbare Realität”**
- **Diskussion und Berichterstattung über Cloud Computing sind oftmals geprägt von einer gewissen Furcht, insbesondere wegen**
  - Datensicherheit
  - Datenverfügbarkeit
  - Rechtliche Zulässigkeit (zB. iH. auf Datenschutz)
- **Hilfe wird gefordert von**
  - Gesetzgeber (-> Datenschutzrecht, klare Gesetzeslage)
  - Juristen
  - aber selten: Techniker
- **Juristische Diskussion: tastend**
- **Nicht alle Rechtsfragen sind neu, einige aber neu zu diskutieren**

# Überblick

1. **Thesen**
2. **Definitionen, Modelle und Metriken**
3. **(Weitgehend) geklärte Rechtsfragen**
4. **Zu klärende Rechtsfragen**
5. **Zusammenfassung**

# 1. Thesen

1. Cloud Computing ist ein neues **Geschäftsmodell für SW Vertrieb** (insb. f. Abrechnung und Delivery)
2. Cloud Computing weist **technisch** viele Parallelen zu Outsouring auf (ist jedoch auch in dieser Beziehung kein “alter Wein in neuen Schläuchen” -> “Skalierbarkeit”, “Virtualisierung”)
3. Viele Rechtsfragen lassen sich anhand **existierender Geschäftsmodelle** beantworten
4. Einige Rechtsfragen sind **neu zu diskutieren**, dies insbesondere wegen “Wolkenaspekt” und “Angebot als Massengeschäft”
5. Einige Rechtsfragen erfordern eine tiefergehende Auseinandersetzung mit **technischen Aspekten**

- Themen, die **juristisch** diskutiert werden, sind vor allem

  - Vertragstypologie und Gestaltungsfragen
  - Urheberrecht
  - IT-Sicherheit (Compliance)
  - Schutz personenbezogener Daten
  - Vertraulichkeit, Spezialdatenschutz (§ 203 StGB)
  - § 613a BGB (“Betriebsübergang”)
  - Telekommunikationsrecht
  - Zurechnungs- und Beweislastfragen

- Als zu regelnde Risiken werden definiert: Beherrschbarkeit, Sicherheit, Zuverlässigkeit, Verantwortung (vgl. auch Diskussion vor rund 20 Jahren zum Thema “Outsourcing”)

# 2. Definitionen, Modelle und Metriken

# Was bedetet Cloud Computing?
## Mittlerweile besteht ein Grundverständnis über die Eigenschaften, die einer „*Cloud*“ zuzuordnen sind

Nutzungsabhängige (variable) Kosten / Capex vs. Opex /

In der Regel niedrigere Kosten

Kurzfristige, schnelle und flexible Bereitstellung

Unbeschränkter Zugriff via Internet-Technologie

Geschäftliche Aspekte

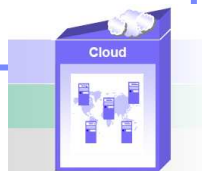
„Cloud Computing ist eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen.

Diese werden in Echtzeit als Service über das Internet bereitgestellt und nach Nutzung abgerechnet.

Damit ermöglicht Cloud Computing den Nutzern eine Umverteilung von Investitions- zu Betriebsaufwand.

Die IT-Leistungen können sich auf Anwendungen, Plattformen für Anwendungsentwicklungen und -betrieb und Basisinfrastruktur beziehen.“

*BITKOM: Cloud Computing - Evolution in der Technik, Revolution im Business; Berlin 2009*




Zentralisierung / Virtualisierung

Vollständige, lastabhängige Skalierbarkeit

Automatisierung / Standardisierung

Multi-Mandantenfähigkeit

Technische Aspekte

# Cloud-Angebote gliedern sich in 3 Produktarten

## Cloud Project Based Services

Cloud Enablement – Beratung und Implementierung

Service Product Portfolio - **Privat**

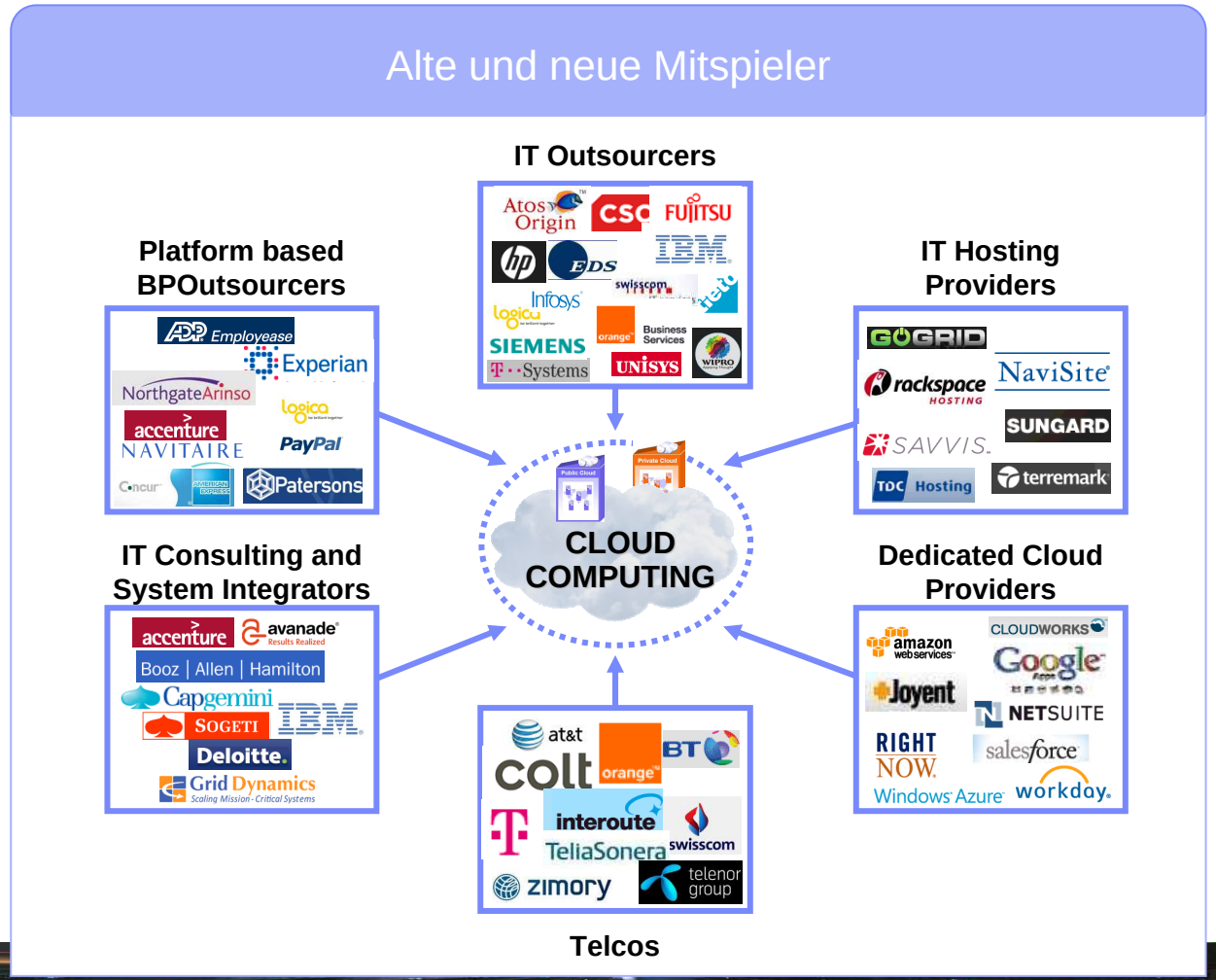
## Cloud Delivered Services

Cloud Consumption – Die IBM Cloud - Elastische, virtualisierte, im Preis flexible, zentral-gehostete Anwendungen & Infrastruktur - **Public**

## Cloud Platform Products

Cloud **Enablement** - Infrastruktur SW und HW zur Entwicklung von Public, Private und Hybrid Clouds

# Die Anbieterlandschaft ist überaus heterogen. Neue Mitspieler treffen auf etablierte, Internet-Firmen auf traditionelle Service-Provider.



# 3. (Weitgehend) geklärte Rechtsfragen

# Vertragstypologie

1. **Typologisch**: Elemente aus Miet- und Dienstvertrag, ausnahmsweise auch Werkvertrag
   - Miete: Zur-Verfügungstellen von Software und Speicherkapazitäten (Besitzverschaffung nicht erforderlich)
   - Dienstleistung: Pflege von Software, Nutzungsunterstützung
   - Werkleistung: Installations- und Anpassungsleistungen (sofern ausnahmsweise geschuldet)
2. Rückgriff auf Rspr. und Literatur zu **ASP- und Outsourcingtypologien** (BGH Entscheidung vom 15. November 2006 zum ASP)
3. Bereitstellung und Verfügbarkeit wird per Leistungsbeschreibung und SLA beschrieben
4. Breite Varianz der im Markt anzutreffenden SLA Zusagen

# Vertragsgestaltung

Grundsätzlich analog klassisches Outsourcing

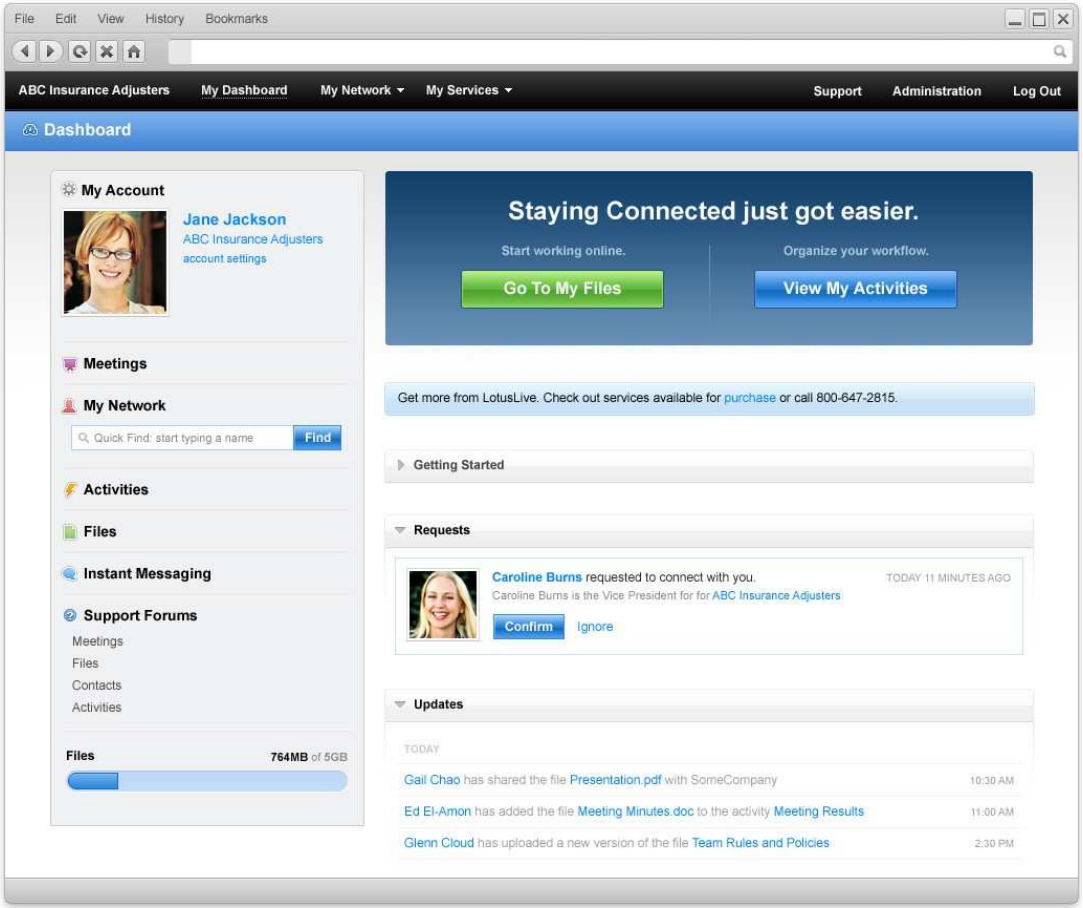
1. Keine grundlegenden Andersartigkeiten
2. Von zentraler Relevanz: **Detaillierte Leistungsbeschreibung** - welche Leistungen werden wie erbracht – in der Praxis oftmals problematisch wegen
   - Kundenwunsch nach kurzen Verträgen im Massengeschäft
   - Änderung der Leistungserbringung während Vertragsdurchführung
3. Im Unternehmensbereich werden oftmals auch Lösungen zu den Themen „Eskalation“ oder „Notfall- und Exitmanagement“ vereinbart
4. **Unterschiede zur Outsourcing-Vertragsgestaltung** ergeben sich vor allem aus zwei Aspekten:
   - „Cloud Computing“ ist oftmals Massengeschäft, bei dem die Verhandlung und Individualisierung von Verträgen nicht erwünscht ist -> „one size fits all“
   - Bei Cloud Computing sind die Daten typischerweise nicht einer dedizierten Hardwareeinheit zugeordnet, sondern werden oftmals global verschoben und ggf. auf andere Anbieter verlagert -> es bedarf daher typischerweise einer vertraglichen Abdeckung der Themen „Datensicherheit“ und „Datenschutz“

# Urheberrecht

1. **Urheberrechtliche Nutzung durch den Cloud Kunden (herrschende Meinung)**
   - Anwender nimmt bei Zugriff über Browser **keine urheberechtlich relevante Handlung** insbesondere keine Vervielfältigung auf seinem PC vor (vergleichbar mit Terminalbetrieb)
   - **Keine Vervielfältigung** (§ 69c Nr. 1 UrhG) durch den Kunden, die er technisch auch nicht bewerkstelligen kann
   - So nachzulesen bei Schuster/Reichl, CR 2008, 38 (40 f.), Nägele/Jacobs, CR 2010, 281 (288)
   - hM. **nicht ganz unproblematisch**, da nach meiner Ansicht der dem jeweiligen Cloud-Angebot zugrundeliegende Programmcode zumindest zum Teil und vorübergehend in den Arbeitsspeicher des jeweiligen „Client Rechners“ oder aber des „Cloud Servers“ geladen werden muss.
   - Die **vorübergehende Speicherung im Arbeitsspeicher** stellt nach heute ganz h.M. eine Vervielfältigung dar (OLG Celle, CR 1995, 14; Dreier/Schulze/Dreier § 69c, Rn. 8; Marly Softwareüberlassungsverträge Rn. 159ff. – jüngst: BGH Beschluss vom 03. Februar 2011 – Fragen an Europ. GH zur Vorabentscheidung über „Gebrauchtsoftware“, insb. Rn. 13)
   - Auch § 44a UrhG („Vorübergehende Vervielfältigungshandlungen“) greift m.E. nicht
   - hM geht mglw. irrig davon aus, dass die Funktion des „Client Rechners“ sich auf die reine Darstellung beschränkt („Fenster“)
   - Mglw. ist das Thema unter Hinzuziehung von technischem Sachverstand zukünftig **differenzierter zu betrachten** (insb iH auf verschiedene technische Lösungsansätze); dies auch mit Blick auf Ergebnis der hM
   - Gegeben ist wohl auch öffentliche Zugänglichmachung, § 69c Nr. 4 UrhG

2. **Urheberrechtliche Nutzung durch den Cloud Provider**
   - Cloud Provider muss sich die Rechte zur Nutzung der urheberrechtlich relevanten Inhalte des Kunden einräumen lassen

# Beispiel für Rechteeinräumung an Cloud Provider unter IBM LotusLive




**LotusLive t's and c's**

"11. Ownership of Content

[...] You confirm that you have ***all necessary authorities*** to allow IBM to host, cache, record, copy, and display Content solely for the purpose of providing the Service to you. [...] If you choose to transmit your Content to a third party site which may be linked to or accessible by the Service, you are providing IBM with the consent to enable such transmission of Content, and you remain liable for such transmission.

12. Representations and Warranties About Content

You represent and warrant that you: (i) are the ***owner or authorized licensee*** of any and all Content; and [...] (iii) that you have ***all required permissions and consents from any third party*** whose personal information you may have posted or uploaded to the Service."

## IT-Sicherheit

1. Verantwortlichkeit für IT Sicherheit liegt beim Unternehmen, das einen bestimmten Dienst nutzt.
2. Anbieter differenzieren sich über Preis und Lösungsangebot, inkl. Sicherheit
3. Als Minimal-Anforderungen werden genannt: Aussagen zu physischer Sicherheit, Perimeter-Firewalls, Load Balancing und möglicherweise Intrusion Detection und -Prevention. Preisabhängig.
4. Analog der bisherigen Problemfelder und Vertragsbausteine beim Outsourcing. Spezifikum wenn IT Infrastruktur vorwiegend im Ausland zu finden ist: Prüf- und Aufsichtspflichten erhöht?
5. Wenn Verschlüsselungstechnologien eingesetzt werden, sind EG Dual-use VO und US Export Kontrollgesetze zu beachten

## Compliance

1. SOX Section 404 (analoger Prüfungsstandard in Deutschland PS 951): SAS 70 Report ist als Nachweis, dass ausgelagerte Geschäftsprozesse ordnungsgemäß kontrolliert werden, anerkannt.
2. SAS70 Prüfungen gemäß Typ I (Prüfung des Kontroll-Designs) und Typ II (Prüfung der Kontrolleffektivität)

# 4. Zu klärende Rechtsfragen

- ## Schlechtleistung
  1. SLA/SLC Konzept -> gut für Anbieter, da §§ 307 ff BGB nicht anwendbar („Leistungsbeschreibung“)
  2. Übergänge zu „Geschäftsbedingungen“ sind in diesem Bereich fließend (zB Definierung der Konsequenzen von Schlechtleistung)
  3. Haftung für Pflichtverletzung, §§ 280, 281 ff. BGB
  4. Zurechnung von Handlungen der Erfüllungsgehilfen nach § 278 BGB
- ## Anwendbarkeit von TMG und TKG
  1. Nach wohl hM. sind beide Gesetze nicht anwendbar
  2. Begründung jedoch oftmals weniger dogmatisch als vielmehr ergebnisorientiert
  3. Zweifel verbleiben vor allem bei der Frage, ob Cloud-Kommunikationsdienste (zB. Cloud-basierte Messaging- oder VoIP-Lösungen) nicht als Telekommunikationsdienst anzusehen sind (vgl. § 3 Nr. 24 TKG)

# Auftragsdatenverarbeitung nach § 11 BDSG

1. Datenverarbeitung in der Cloud stellt sich in der Regel als Auftragsdatenverarbeitung nach § 11 BDSG dar
2. **Innerhalb der Grenzen der EU rechtlich** im Grundsatz **unproblematisch**, da die Überlassung personenbezogener Daten im Rahmen der Auftragsdatenverarbeitung praktisch als „rechtliches Nullum“ betrachtet wird. Aber Achtung: Privilegierung der Auftagsdatenverarbeitung in Europa entfällt, wenn Zugriff aus Drittstaaten (zB. zu Wartungszwecken) vorliegt.

3. **Rechtliche Hürde 1 – Anforderungen des BDSG an Auftragsdatenverarbeitung**
   - Anforderungen von § 11 Abs. 2 BDSG und der Anlage zu § 9 BDSG müssen erfüllt sein
   - Kontrollen: AG muß Art und Umfang der DV vollständig kennen z.B. Zutritt, Zugang und Zugriffskontrollen in allen beteiligten RZ (Nr. 1-3 Anlage zu § 9 BDSG)
   - Detaillierte Festlegung der Unterauftragsverhältnisse
   - § 11 Abs. 2 S.4: AG hat sich regelmässig von der Einhaltung der Maßnahmen zu überzeugen (Reicht es aus, Prüfberichte zur Verfügung zu stellen? s.a. BITKOM Leitfaden)

4. **<u>Rechtliche Hürde 2 – Verlagerung der Daten ausserhalb der EU</u>**
   - Keine grundsätzliche Privilegierung
   - Nur dann **zulässig**, wenn

     a) **ausdrückliche Zustimmung** des Datenrechtssubjekts zu eben dieser Verlagerung vorliegt (Problem „informierte Einwilligung“ vs. „Wolkenflexibilität), oder

     b) **angemessenes Datenschutzniveau** im Drittstaat sicherggestellt ist (zB. Schweiz, Kanada, Argentinien). Verlagerung in die USA nur, wenn die jur. Person ein entsprechendes Safe Harbour Zertifikat besitzt oder Model Clauses etabliert sind (auch hier Problem der „Wolkenflexibilität“).
   - **Neue EU Model Clauses**: Neufassung vom 05. Februar 2010 für controller-processor Konstellationen. Neufassung tritt ab dem 15. Mai 2010 in Kraft (Erleichterung der Einschaltung von Subunternehmern durch Anbieter)

5. Viele Anrufe an **nationalen und europäischen Gesetzgeber**, einen transparenten Rechtsrahmen zu schaffen, der Cloud Computing unter klar definierten Voraussetzungen ermöglicht

6. Datenschutzrechtliche Schwierigkeiten ließen sich **technisch** lösen durch
   (a) lokale Serverlösungen,
   (b) Verschlüsselung („Verschlüsselung ‚in der Cloud/vor der Cloud“ / „homomorphe Verschlüsselung“ -> Zukunft)

- ## Spezialdatenschutz § 203 StGB (Verletzung von Privatgeheimnissen)
  1. Vorsatztat des Geheimnisträgers, ggf. **Beihilfe des Providers**, Gehilfenvorsatz muß sich auf die Haupttat beziehen.
  2. **Strafbarkeit str.** („straflose notwendige Beihilfe“?)
  3. Empfehlung, dass sich von § 203 StGB geschützte Daten zunächst **nicht für eine Public Cloud** eignen
  4. **Problembereiche**: Gesundheitskarte mit Cloudapplikationen, private Krankenversicherung „on demand“, „Rechtsberatung aus der Cloud“
  5. **Verschlüsselung** als mögliche Lösung -> s.o., Datenschutz
  6. **Achtung**: § 203 StGB ist nicht mit § 11 BDSG „synchronisiert“ -> dh. erlaubte Auftragsdatenverarbeitung kann ohne weiteres eine strafbare Verletzung von Privatgeheimnissen darstellen

- ## Weitere diskutierte Felder
  1. Internationales Privatrecht (vgl. Nordmeier, MMR, 2010, 151 ff.)
  2. Zugriffsrechte der Strafverfolgungsbehörden auf Daten in der Cloud (Obenhaus, NJW 2010, 651 ff.)

# 5. Zusammenfassung

- **Weitgehend geklärt**

1. Vertragstypologie und Gestaltungsfragen
2. Urheberrecht
3. IT-Sicherheit (Compliance)

- **Weiter zu klären**

1. Anwendbarkeit von Telekommunikationsrecht und Telemedienrecht
2. Schutz personenbezogener Daten
3. Vertraulichkeit, Spezialdatenschutz (§ 203 StGB)

# Fragen