vogel & partner
rechtsanwälte

Cloud Computing und Compliance

Verträge, Urheberrecht, Datenschutz

9. Karlsruher IT-Tag
am 21.04.2012 in Karlsruhe

Prof. Dr. Rupert Vogel
Dr. Oliver Meyer-van Raay

Rechtsanwälte und
Fachanwälte für IT-Recht

RA Dr. Oliver Meyer-van Raay

Dr. Oliver Meyer-van Raay ist seit 2007 Rechtsanwalt und seit 2011 Partner der neu gegründeten, insbesondere auf das IT- Recht spezialisierten Kanzlei Vogel & Partner mit Sitz im Karlsruher Technologiepark. Er berät schwerpunktmäßig im Bereich des Urheber-, IT- und Datenschutzrechts.

Nach Studium und Referendariat in Münster (Westf.) war Herr Dr. Meyer-van Raay am KIT Karlsruhe als wissenschaftlicher Mitarbeiter am Institut für Informationsrecht tätig, wo er sich schwerpunktmäßig mit dem Urheber- und IT-Recht befasste und daneben eine Dissertation zum Softwarelizenzrecht verfasste.

Dr. Meyer-van Raay ist Lehrbeauftragter für EDV-Recht an der Dualen Hochschule Baden-Württemberg (Karlsruhe und Stuttgart) und Fachanwalt für IT-Recht.

RA Prof. Dr. Rupert Vogel

RA Prof. Dr. Rupert Vogel ist seit 1994 Rechtsanwalt und seit 2011 Partner der neu gegründeten, auf IT-Recht spezialisierten Kanzlei Vogel und Partner mit Sitz im Karlsruher Technologiepark. Er berät schwerpunktmäßig im Bereich des Urheber-, IT- und des deutsch-französischen Handelsrechts.

Nach Studium und Referendariat in Heidelberg und Dijon war er Assistent an der Universität Montpellier, wo er zu einem urheberrechtlichen Thema promovierte.

Er ist Fachanwalt für IT-Recht und Honorarprofessor an der Universität Mannheim (IT-Recht, Urheberrecht, Französisches Recht). Bei der Deutschen Gesellschaft für Recht und Informatik e. V. (DGRI) ist er Geschäftsführer und Co-Leiter des Fachausschusses Softwarerecht.

Agenda

- wirtschaftliche und technische Hintergründe, Arten von Clouds
- Abgrenzung zu ähnlichen Geschäftsmodellen und Praxisbeispiele
- anwendbares Recht und Rechtswahl
- Vertragstypologie und -gestaltung
- Urheberrecht
- Datenschutz und Datensicherheit
- offene Fragen / Compliance
- Diskussion

Cloud Computing und Compliance

"Das Bedürfnis nach Datensicherheit bringt Cloud Anbietern ein hübsches Verkaufsargument und Juristen lukrative Beratungsarbeit. Ob all der Schutz nötig ist, weiß keiner."

Zitiert nach ?

- ☑ BITKOM Leitfaden Cloud Computing
- ☑ Parteiprogramm 2011 der Piratenpartei
- ☑ FAZ vom 06.03.2012
- ☑ taz vom 16.03.2012

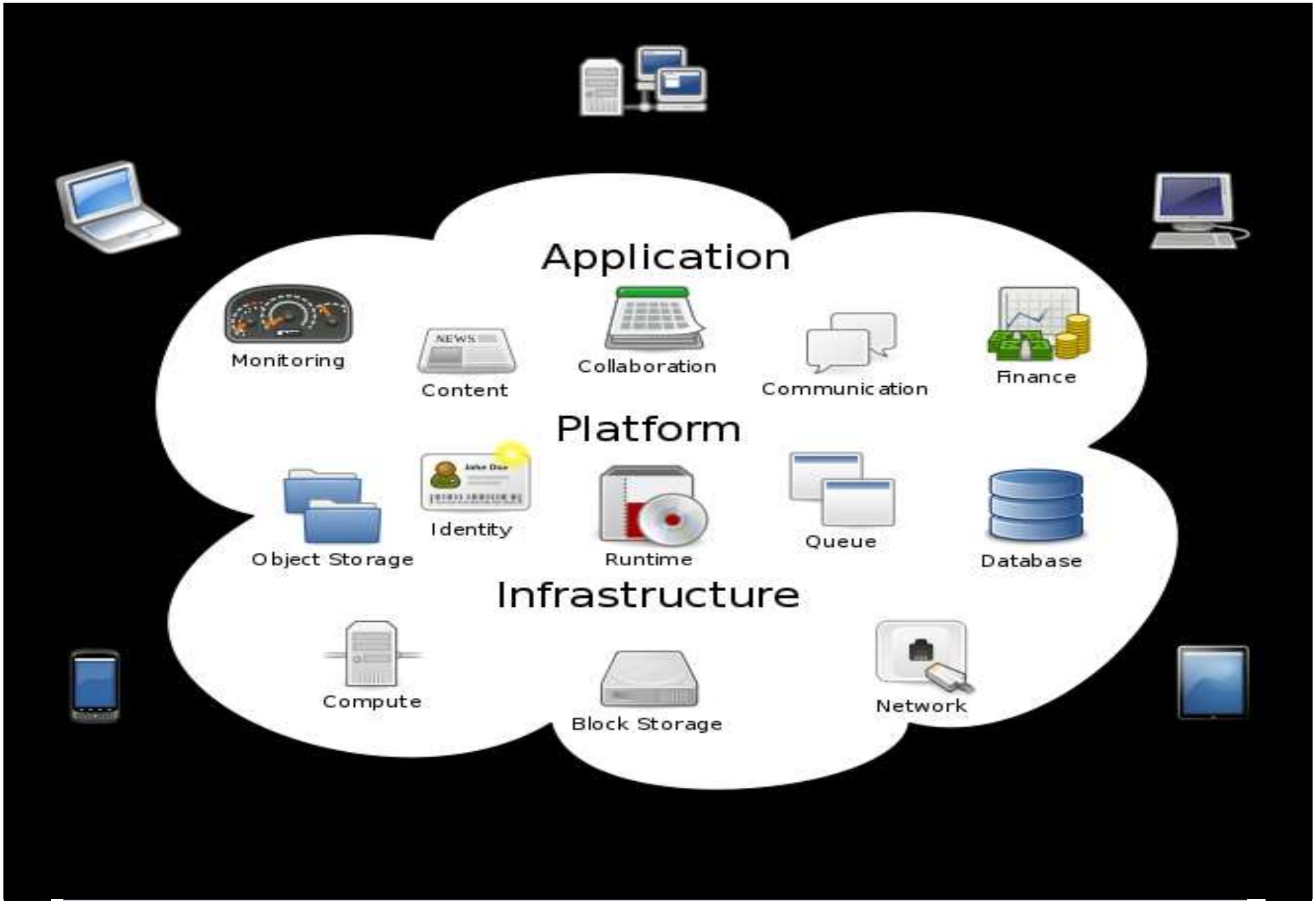
Wirtschaftliche und technische Hintergründe, Arten von Clouds, Antworten des Rechts (Compliance)

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*“)

Rechtsdiskussion

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

Abgrenzung zu ähnlichen Geschäftsmodellen und Praxisbeispiele

Abgrenzung zu ASP und Outsourcing

- ASP: Keine Auslagerung interner IT-Funktionen, sondern Einkauf neuer IT-Services von außen
- Unterscheide zum ASP vor allem in der **Serverarchitektur**
  - ASP: Single Tenancy (Software wird über Netzwerk einem Client zur Verfügung gestellt)
  - Cloud: Multi Tenancy (von mehreren Nutzern / Clients gleichzeitig und unabhängig voneinander nutzbar - mehrmandantenfähig)
- Unterschied IaaS zum klassischen Outsourcing: fehlende feste Zuordnung von physikalischen Ressourcen

  → **Virtualisierung** der Ressourcen als Kernmerkmal

  → **Perspektivwechsel** vom Rechenzentrum zur Leistung
- Application Management: Entwicklung und Betreuung von Applikationen und Anwendern

Einige Anwendungsfälle aus der Praxis

- CRM-Software, z.B. von Salesforce, für Vertriebsmitarbeiter eines Energieversorgers in Ergänzung der hauseigenen CRM-Lösung
- Fernnutzung einer Anwendungssoftware zur Absatzplanung (auch über mobile Endgeräte) als SaaS-Lösung
- E-Mail-Archivierung in der Cloud (Zugriff auch über iPhone-Client)
- Daneben z.B. ERP, HR, Collaboration, Energiemanagement, Transportroutenplaner …
- z.B. SaaS in Kombination mit einem cloudbasierten Kundensupport-Center (Ticketsystem mit zentralem Datenbestand) zur Anbindung von Niederlassungen im Ausland
- häufig Generalunternehmermodell (statt Multi-Vendor-Strategie)
- Ausschöpfung der Vorteile häufig nur bei Public Clouds möglich

Neue Geschäftsmodellansätze mit Cloud Computing

- **App-orientierte Geschäftsmodellansätze** auf der Basis von Cloud Computing (Siemens White Paper 2011)
  - Apps als „Micro-SaaS“ Lösung – Funktionen der Apps werden aus der Cloud bezogen; Vision: Internet-basierte App-Plattformen auf der Basis von Cloud Computing, z.B. für folgende Anwendungen:
  - Smart Traffic zur Verkehrssteuerung und Stauvermeidung
  - eCar Mobility: Telematic Services für professionelles Flottenmanagement, Lademanagement
  - Gesundheitsplattformen: Verwaltung (und Austausch?) von Gesundheits- und Fitnessdaten unter Beteiligung von Krankenkassen, Arbeitgebern, Krankenhäusern, Ärzten, Apotheken, Geräteherstellern etc. → Unterstützung der privaten Gesundheitsvorsorge

Anwendbares Recht und Rechtswahl

Internationales Vertragsrecht

Rechtswahl

- B2B: nach Art. 3 I Rom I zulässig
  - B2C: Art. 6 Rom I ist sachlich anwendbar

    (℗ auch nicht körperliches Online-Produkt +)

    ⇨ Günstigkeitsvergleich zugunsten Verbraucher

keine Rechtswahl

- objektive Anknüpfung an vertragscharakteristische Leistung – Art. 4 II Rom I (bei Dienstvertrag Art. 4 Abs. 1b Rom I): Recht des Anbieters
  - B2C: Recht am gewöhnl. Aufenthalt des Verbrauchers

Internationales Deliktsrecht

- Grundsatz: Recht des Schadenseintrittsorts – Art. 4 I Rom II

  (Ausnahme: gemeinsamer gewöhnlicher Aufenthalt – Art. 4 II Rom II)
- Ⓟ: Wo ist „Schadeneintrittsort“?
  - Zielrechner/ Hauptrechner?
  - Speicherort der geschädigten Daten?
  - Mosaikbetrachtung?
  - „gewöhnlicher Abrufort“
  - bei enger Verbindung Anknüpfung an Vertragsstatut – Art. 4 III S. 1 Rom II
- Subunternehmer?
- vorherige Rechtswahl mögl. (Art. 14 I b Rom II; Ausnahme IP-Rechte – Art. 8 II)

Internationales Urheberrecht

- Territorialitätsprinzip/ Schutzlandprinzip (Anknüpfung)
- Mosaikbetrachtung (Rspr.?)
- Wie bei Senderecht: Anknüpfung an Herkunftsland des Anbieters o. Serverstandort?
- Bogsch-Theorie: zusätzlich zum Recht des Sendelandes auch Recht des Empfangslandes?
- Einschränkung des Schutzlandprinzips: hinreichender Inlandsbezug notwendig?
- Einheitstheorie ./. Spaltungstheorie
  - h.M.: Einheitstheorie
    - Verpflichtungs- und Verfügungsgeschäft unterstehen Vertragsstatut
  - Spaltungstheorie: nur f. Verpflichtung Vertragsstatut, Verfügung nach Recht des Schutzlandes

Vertragstypologie und Vertragsgestaltung

Vertragstypologie

- Warum überhaupt wichtig? Bestimmung des **Leitbilds** der Klausel-kontrolle 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)

- Unterschiede bei Service-Arten (IaaS, PaaS, **SaaS**)
- Vervielfältigung (§ 69c Nr. 1 UrhG) +
- Vermietung (§ 69c Nr. 3 UrhG)?

  Def.: zeitlich begrenzte Gebrauchsüberlassung für unmittelbare

  o. mittelbare Erwerbszwecke

  Ⓟ: Überlassung eines Vervielfältigungsstückes?

  - analoge Anwendung wie bei unkörperlicher Verbreitung – § 69c Nr. 3 S. 2 UrhG?
  - wie ASP-Rechtsprechung?

Verhältnis Softwarehersteller – Anbieter (2)

- Öffentliche Zugänglichmachung (§ 69c Nr. 4 UrhG)?
  - Vorfrage: Schutzumfang § 69c UrhG (Computerprogramm)
    - Benutzeroberfläche als Werk?
    - Benutzeroberfläche als Teil des Computerprogramms?
    - OLG München (GRUR-RR 2009, 91 – ASP): Zugänglichmachung per ASP auf Computerprogramm reicht für § 69c Nr. 4 UrhG?
- Ⓟ: Öffentlichkeit?
- 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

- (e. M.) reiner Programmlauf urheberrechtlich nicht relevant
- (e. M.) Vervielfältigungshandlungen im Browser-Cache u. Arbeitsspeicher → Vervielfältigung (aber § 44 a UrhG)
- (e. M.) bestimmungsgemäße Benutzung durch Berechtigten (§ 69 d Abs.1 UrhG)
- (e.M.) § 69 d Abs. 1 UrhG für Handlungen auf Server des Anbieters?

- neu: Client Access License: schuldrechtliche Gestattung, nicht dinglich?

Datenschutz und Datensicherheit

Bestimmung des relevanten Datenschutzregimes

- **Territorialitätsprinzip**: Ort der Erhebung oder Verarbeitung der Daten → insb. Ort der Speicherung
- Innerhalb EU/EWR („EU-Clouds"): **Sitzlandprinzip**, d.h. Recht des Staates, in dem der Anbieter seinen Sitz hat, es sei denn Niederlassung im Inland(§ 1 Abs. 5 BDSG)
- Außerhalb EU/EWR anwendbares Recht nicht immer zweifelsfrei feststellbar aufgrund Dezentralität, Flexibilität und Mobilität
- Einheitliches europäisches Datenschutzrecht durch geplante **EU-Verordnung** (Vollharmonisierung) – nur wann?
- Cloud-Computing als ein Grund für die Notwendigkeit einer Datenschutzreform von EU-Kommission genannt
- Vereinfachung internationaler Datentransfers insbesondere durch klare Vorgaben für Binding Corporate Rules

Anwendung des Datenschutzrechts

- Anwendbarkeit setzt Vorliegen personenbezogener Daten voraus:
- **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 gem. § 28 BDSG:
  - erforderlich aufgrund Schuldverhältnisses mit Betroffenem
  - 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)

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

- Einhaltung der Anforderungen an die AuftragsDV-Vereinb.
  - Standardverträge 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
  - **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
  - ausreichende Information bei ausländischer Cloud schwierig
  - 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
- **entsprechende** Anwendung von § 11 Abs. 2 BDSG

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

Zusammenfassung Datenschutz & Datensicherheit

- Datenschutz muss kein „*Dealbreaker*“ sein
- Auswahl eines Anbieters, der Abschluss einer Auftragsdatenverarbeitungsvereinbarung anbietet
- Problem der Kontrolle der Datensicherheitsmaßnahmen des Anbieters → Zertifizierung als mögliche Lösung
- Angemessenes Datenschutzniveau bei außereuropäischen Clouds zu beachten
- Private Clouds als mögliche Lösung: Dritte nicht involviert oder als Auftragsdatenverarbeitung gestaltbar
- Einbeziehung in das Risikomanagement von Unternehmen
- Haftungsrisiko für Unternehmensleitung

Offene Fragen

Offene Fragen / Compliance

- **Schutzziele**
  - Verfügbarkeit
  - Vertraulichkeit
  - Integrität
  - Authentizität
  - Zurechenbarkeit
- **Rechtsgrundlagen**
  - Gewährleistung der Vertraulichkeit u. Integrität informationstechnischer Systeme (aPR bei Grundrechtsbindung)
  - § 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)
    - 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)

Zugriff auf Cloud-Services über Apps / Smartphones

- **Datenschutzrechtliche und Sicherheitsaspekte**
  - Möglichkeit des Zugriffs von App-Entwicklern auf Adressbücher
  - Nutzerprofile mittels Gerätekennung (UDID) – personenbezogen?
- **Bring Your Own Device**
  - Keine klare Trennung zwischen privater und dienstlicher Nutzung → Nutzung von privaten Geräten zu betrieblichen Zwecken
  - In der Praxis im Regelfall keine entsprechenden Vereinbarungen / Regelungen zwischen AG und AN
  - Lizenz- und arbeitsrechtliche Probleme (z.B. fehlende Netzwerklizenzen; betriebliche Übung?)
  - IT-Compliance: Verwaltung unterschiedlichster Mobilgeräte, revisionssichere Archivierung etc.
  - Auftragsdatenverarbeitungsvereinbarung mit dem Mitarbeiter?

Einzelfragen zu Compliance

- Haftung des Anbieters (TMG ?)
  - h.M.: nicht anwendbar
- Fernmeldegeheimnis TK-Dienstleistung (TKG)?
  - h.M.: nicht anwendbar
  - + bei TK-basierten Diensten
  - § § 92, 109, 44a TKG
- Geheimnisschutz/ Berufsgeheimnisträger
  - Ⓟ straflose Weitergabe an „Gehilfen“ / Anbieter als Gehilfe?
- Insolvenz des Anbieters
- Betriebsübergang (§ 613a BGB)
  - „Cloudsourcing“ ?
- Handels- und Steuerrecht, z.B. § 146 AO, GDPdU
- Kartellrecht

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 & Dr. Oliver Meyer-van Raay
Rechtsanwälte und Fachanwälte für IT-Recht

rv@vogel-partner.eu om@vogel-partner.eu

www.vogel-partner.eu