h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

DIPLOMARBEIT

THOMAS LIEBLANG

DIE RECHTLICHE PROBLEMATIK DES CLOUD COMPUTING – EIN VERGLEICH DES DEUTSCHEN UND AMERIKANISCHEN RECHTS

Referent: Prof. Dr. Diana D. Chiampi Ohly, LL.M. (Duke), Attorney-at-Law (New York)
Koreferent: Prof. Dr. Thomas Wilmer

Vergabedatum: 01. März 2010
Abgabedatum: 31. Mai 2010

Gliederung des Vortrags

- Definition Cloud Computing
- Das Geschäftsmodell
- Problemstellung
- rechtliche Grundlage Datentransfer
- Datenschutzrechtliche Aspekte des Cloud Computing im deutsch-amerikanischen Rechtsvergleich
- Fazit

Definition

- neues Modell des Rechenzentrums- und IT-Infrastruktur-Outsourcings
- Daten und Anwendungen werden ausgelagert und dezentral gespeichert
- ASP + Speicher und Datenbanken
- weltweite Serverfarmen / Netzwerke die Daten miteinander austauschen

Definition

"It is a style of computing where massively scalable IT-related capabilities are provided - as a service - using Internet technologies to multiple external customers."

Die Arten der Clouds

Private Cloud

- Unternehmensintern
- Zugang über Intranet
- auf ausgewählte Nutzer beschränkt
- Individualisierung und Anpassung an unternehmensspezifische Anforderungen
- Interne Datenspeicher

Public Cloud

- von IT-Dienstleister betrieben
- Zugriff über das Internet
- virtualisierte IT-Umgebung wird i. d. R. von mehreren Kunden gleichzeitig genutzt
- Standardisierte Leistungen
- Variable Kosten
- Einfluss auf die IT-Sicherheit und den Ort der Datenspeicherung ?

Vorteile

- Abrechnung überwiegend nach tatsächlich genutzten Kapazitäten (Pay as you grow)
- Geringere Fixkosten:

  ->Speicher-/ Rechnerkapazitäten (-)

  ->ungenutzten Lizenzkosten (-)
- zeit- und ortsunabhängig
- unbegrenzte Ressourcen
- Mobil und Flexibel

Vorteile

- Pflege und Instandhaltung der Anwendungen
  -> jederzeit aktuellste Version
  -> kein Risiko, Betriebsabläufe unterbrechen zu müssen
- IT-Personalkosten sinken

„Die Vorteile von Cloud Computing liegen auf der Hand: Unternehmen müssen nur noch genau die IT-Leistung bezahlen, die sie auch nutzen, da alle Services bedarfsgerecht skaliert und aus Fixkosten variable Kosten werden"

Problemstellung

- Virtualisierung von Systemen, Daten und Anwendungen
- Standort der Ressourcen ist wirtschaftlich nicht mehr von Bedeutung, hat aber **rechtliche Relevanz**

-> Ein Nutzer weiß im Zweifel nicht mehr, wo sich seine Daten zu einem bestimmten Zeitpunkt gerade befinden !

-> eine Cloud kann global aufgestellt sein und Serverressourcen in vielen Ländern nutzen

- Gefährdung unternehmenskritischer Informationen

Akzeptanz

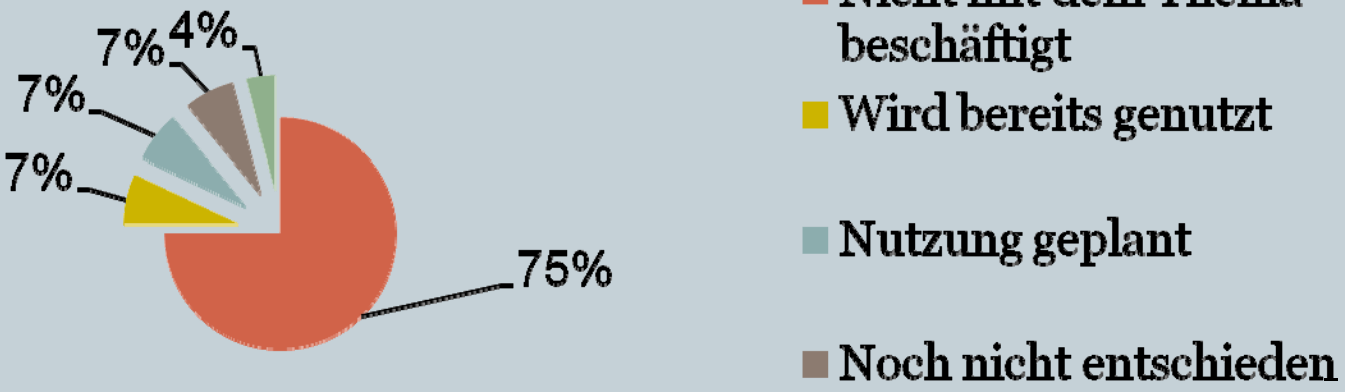
- virtuelle Nutzung von CC-Angeboten wird stark zunehmen
- bisher zögern viele Unternehmen: Sicherheitsbedenken
- Befragte IT-Manager: die Hauptgründe gegen dauerhaften Einsatz von CC sind

-> fehlendes Vertrauen in die Daten-Sicherheit

-> die Unvereinbarkeit mit unternehmensinternen IT-Vorschriften

-> sowie die Befürchtung, bei der umfassenden Nutzung externer Dienstleister die Kontrolle über den IT-Prozess zu verlieren

Akzeptanz



- nach einer Prüfung gegen die Nutzung von Cloud Computing entschieden
- vorrangig Sicherheitsbedenken und die Verletzung gesetzlicher Regelungen
- 50 % der befragten Großunternehmen (> 5000 MA) nutzen bereits CC
- viele mittelständische Betriebe lehnen das Cloud Computing ab

Datenschutzrechtliche Aspekte

- Problem: Daten in der Cloud
- liegen nicht zentral an einem Speicherort, sondern i. d. R. auf mehrere Standorte verteilt
- können jederzeit den Standort wechseln
- I. d. R. weiß der Nutzer nicht, wo seine Daten gerade gespeichert werden
- Häufig personenbezogene Daten von Arbeitnehmern oder Kunden, die vertrauliche oder sicherheitskritische Informationen beinhalten können
- Diese sensiblen Daten unterliegen wegen der globalisierten und unternehmensübergreifenden Serververknüpfungen und Datenspeicherungen einem erhöhten Risiko, zumal, wenn es sich um eine Public Cloud handelt

Datenschutz in der BRD

- Entgegen dem Wortsinn des Begriffs Datenschutz sollen nicht die Daten als solche geschützt werden, sondern das **Persönlichkeitsrecht** der Personen, deren Daten verarbeitet werden
- **informationelle Selbstbestimmung**: Jeder Träger von Grundrechten hat das Recht selbst zu entscheiden, wer zu welchem Zweck welche Daten über diese Person verarbeitet oder nutzt

„Grundrecht auf Datenschutz“

- BDSG richtet sich grundsätzlich an die verantwortlichen Stellen einer Datenverarbeitung

  -> Verfügungsmacht über die Daten

Datenschutz in der BRD

… der Datenschutz hat also zur Aufgabe, das Persönlichkeitsrecht in der Informationsgesellschaft durch die Einräumung von Partizipations-, Abwehr- und Kommunikationsrechten der Individuen an den sie betreffenden Informations- und Kommunikationsvorgängen zu sichern

Übertragung der Daten in einer Cloud

- Die Verarbeitung gem. § 32 BDSG sieht eine einwilligungsfreie Verarbeitung, Erhebung und Nutzung von **Arbeitnehmerdaten** vor
- Eine obligatorische Einwilligung in die Datenverarbeitung, wie sie standardisiert in einem Arbeitsvertrag auftauchen kann, ist legal
- Somit ist eine entsprechende Verarbeitung von personenbezogenen Daten aufgrund der arbeitsvertraglichen Einwilligung durch den Arbeitnehmer wesentlich erleichtert worden
- Z.B. Personalabrechnungssoftware

§ 11 Auftragsdatenverarbeitung

- **Befugnisnorm**
- Verpflichtung AG, den AN hinsichtlich Datenschutzniveau sorgfältig auszuwählen
- Umfang, Art und Zweck der Datenverarbeitung und die endgültige Löschung der Daten bei Auftragsende
- Endgültige Löschung aller Daten bei AN und Erfüllungsgehilfen möglich ? Digitale Spuren
- Transfer nur in Staat der EU oder EWR
- Der AG als **Herr der Daten**

-> AG muss sich regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen !

- Konflikt: Daten auf globaler Ebene ständig in Bewegung ! An welchem Ort befinden sich bestimmte Teile der Datenpakete unter welchen Sicherheitsbedingungen gerade ?

Anlage zu § 9 S. 1 BDSG

- technische und organisatorische Maßnahmen:
- Unbefugte dürfen

  -keinen Zugang/Zugriff auf die Daten haben

  - personenbezogene Daten dürfen bei der Verarbeitung, Nutzung und nach der Speicherung nicht gelesen, kopiert, verändert oder entfernt werden

-> Aber: Vielzahl von in die Wertschöpfungskette des Cloud Compting involvierte Unternehmen und Serverfarmen

-> weltweite Vernetzung der Datenstränge. Kontrolle wer berechtigterweise Zutritt, Zugriff und Zugang zu den Daten hat ? Tatsächliches Vorgehen notwendig ! Herr der Daten ?

-> Widerspruch zwischen der Geschäftsidee des Cloud Computing und dem Umstand, dass der AG jederzeit Art und Umfang der Datenverarbeitung sowie Zeit und Ort vollständig kennen und beherrschen muss

Datenübermittlung gem. § 28 BDSG

- Interessenabwägung der überwiegend wirtschaftlichen (Kostenersparnis) und organisatorischen (Zeitersparnis) Interessen des Kunden und dem Schutz der Daten
- Herrschende Meinung: Vorrang des Schutzbedürfnisses (restriktive Auslegung)
- BGH: ausgewogene Mittel-Zweck-Relation / Einzelfallbetrachtung: Übermaßverbot / Grundsatz der Datensparsamkeit: nur so viele personenbezogene Daten, wie zur Zweckerreichung zwingend notwendig, übermitteln … ! …
- Um erfolgreich wirtschaften zu können und hierfür das Konzept des Cloud Computing optimal ausnutzen zu können, müsste das Schutzinteresse des Betroffenen hinter dem wirtschaftlichen Interesses des Unternehmers zurücktreten -> Realistisch ?

Datenschutz innerhalb der EU

- Die EG-Datenschutz-Richtlinie hat die **Harmonisierung der Rechtsvorschriften** der Mitgliedstaaten über die Verarbeitung personenbezogener Daten zum Ziel

- Die Grundsätze der EG-Datenschutzrichtlinie sind Datenqualität und –verhältnismäßigkeit, Transparenz, Sicherheit, Rechte der Betroffenen, Beschränkung der Übermittlung in Drittländer und **besonderer Schutz für sensible Daten.**

Datentransfer außerhalb des EWR

- Niederlassung des AN außerhalb des EWR: gem. § 1 Abs. 5 S. 2 BDSG gilt deutsches Recht (Territorialprinzip)
- Gemäß §§ 3 und 4 b BDSG ist die Übermittlung von Daten aus Deutschland heraus generell nur unter **strengen Voraussetzungen** möglich
- Sollte ein Drittland kein angemessenes, also dem europäischen Datenschutzrecht gleichwertiges Datenschutzniveau bieten können, so Treffen die Mitgliedstaaten die **erforderlichen Maßnahmen**, um Datenübermittlungen in dieses Land zu **verhindern**.
- Schweiz, Kanada, Argentinien, Guernsey, Insel Man und Jersey (+), **USA (-)**
- Um in einem Drittland ein vergleichbares Datenschutzniveau gewährleisten zu können, stehen den Parteien eines Cloud Computing Geschäftsprozesses mehrere Möglichkeiten offen um einen Datentransfer zu legitimieren

Binding Corporate Rules

- verbindlichen Unternehmensregeln
- Instrument zur internationalen Transaktion von Daten eines **Unternehmensverbundes**
- **„Codes of Conduct“** für den internationalen Verkehr von Daten
- Regelung für den weltweiten Datenverkehr in einer organisatorischen Einheit
- rechtlich bindend
- unerheblich in welchem Land sich die Unternehmensleitung befindet oder in welchem Land sich der Besitzer der Daten befindet
- Genehmigungsverfahren ist sehr zeitaufwendig, übermäßige bürokratischen Ausgestaltung
- Ein Cloud-Anbieter, der über ein Netzwerk weltweit verteilter Unternehmensbeteiligungen Daten verarbeitet, haftet demnach für die Fehler, die in einem Drittland geschehen.

EU Standard Vertragsklauseln

- Die Standardvertragsklauseln beziehen sich nur auf den Datenschutz
- Mitgliedstaaten müssen die Vertragsklauseln anerkennen
- **angemessene Garantien** hinsichtlich des Datenschutzes
- anwendbares Recht ausschließlich das Recht des Heimatlandes des AG
- Individualabreden, die auf die spezifischen Bedürfnisse der Vertragspartner abzielen, nur schwer möglich

  -> Zeit- und Geldintensiv

Die Safe-Harbour-Richtlinie

- ausreichendes Schutzniveau , wenn die datentransferierenden Unternehmen dem vom US-Handelsministerium entwickelten Safe-Harbour-Abkommen beitreten
- mehr als 1.000 Unternehmen beigetreten, darunter internationale Konzerne wie Microsoft, General Motors und Amazon

FAQ als Richtlinie:

- Zweck der Datenerhebung und –verwendung
- Schutz vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung
- Dateninhabern muss der Zugang, sowie Korrektur- und Löschungsmöglichkeiten gewährleistet und eine Wahlmöglichkeit eingeräumt werden, ob die Daten überhaupt transferiert werden dürfen

Safe Harbour

- Unternehmen können sich entsprechend der Safe-Harbour-Prinzipien einmal jährlich selbst oder durch ein externes Unternehmen zertifizieren
- Die Unternehmen müssen sich zwar verpflichten sich an die Grundsätze des Safe Harbor Abkommens zu halten, sind aber selbst dafür verantwortlich, dass ihre Angaben der Wahrheit entsprechen. Kontrolliert wird die Einhaltung dieser Bestimmungen wiederum von den Unternehmen selbst
- Selbstregulierend soll der in FAQ 6 genannte Umstand wirken, dass ein Verstoß gegen die Anwendung der Grundsätze einen Straftatbestand darstellt
- Aufsichtsbehörde ist die Federal Trade Commission

Unterschiedliche Rechtsphilosophie

- In Europa umfassend geltende Gesetze
- das amerikanische Rechtsdenken baut fast ausschließlich auf sektoriell geltende gesetzliche Regelungen baut
- Staatliche Regulation wird vermieden, wenn **Selbstregulierungsmaßnahmen der Wirtschaft**, wie im Falle der Selbstzertifizierung bei Safe-Harbour, ausreichend erscheinen. Dagegen sind in Europa behördliche Kontrollen unabdingbar

„Es ist unser gemeinsames Ziel, die in immer größerem Umfang zwischen Europa und den USA ausgetauschten personenbezogenen Daten effektiv zu schützen und damit die demokratische Gestaltung der globalen Informationsgesellschaft sicherzustellen“

*Peter Schaar, Bundesbeauftragter für den Datenschutz

Datenschutz in den USA

- Die USA gelten aus Sicht der EU als Land mit **inadäquatem Datenschutz**
- Die US-Regierung forciert aktiv die Mechanismen der Selbstregulierung beim Datenschutz
- Kein vergleichbares Datenschutzgesetz
- **Sektorielle Bestimmungen**, die eine Verarbeitung personenbezogener Daten branchenspezifisch regeln
- **Einzelregelungen in Bundesstaaten** mit unterschiedlichem Datenschutzniveau
- Ein übergeordnetes Datenschutzrecht, welches personenbezogene Daten schützt, die über eine Cloud in die USA transferiert wurden, gibt es nicht !

„invasion of privacy“

- baut auf die Eigenverantwortlichkeit der verarbeitenden Unternehmen
- „codes of conduct“ der Industrie / sich **selbst-regulierenden** Handelsvereinigungen
- Marktanteile und Wettbewerbsvorteile, aktives **Marketinginstrument**
- **Vertrauen** gegenüber den Verbrauchern aufbauen
- Verbraucherschutzvorschriften: in den USA ist es ausreichend, wenn sich ein Unternehmen oder ein Unternehmensverband dazu verpflichtet, **eigenverantwortlich Regeln** für den Umgang mit personenbezogenen Daten aufzustellen
- Zertifizierung von externem Unternehmen, ob die vorgegebenen Richtlinien eingehalten werden: Verleihung von **Zertifikat / „Privacy Statement“**
- **->** Federal Trade Commission kann Unternehmen auf SchE verklagen

Vorteile der Selbstregulierung

- Bürokratieabbau
- Unternehmen und Verbände bringen ihre Erfahrungen aus der Praxis im Umgang mit der Verarbeitung personenbezogener Daten ein
- branchenspezifische Eigenheiten können berücksichtigt und individuell auch auf die Organisationsformen angepasst werden
- Schneller und flexibler als dies eine Regierung mit Änderungsgesetzen verabschieden kann
- Unternehmen und Verbände können dezentral auf sich veränderte Marktgegebenheiten oder technologische Neuerungen reagieren

Vorbild USA

- Meldepflicht für Unternehmen bei Sicherheitsverletzungen personenbezogener Daten geplant (§ 44 a BDSG).
- Meldepflicht auf Grundlage der „Security Breach Notification Management Policy“
- jedes Unternehmen, das personenbezogene Daten verarbeitet muss einen "breach of security" an alle Betroffenen melden
- organisatorische Implementierung des Meldesystems in einem Unternehmen
- interne Verfahren zur Aufdeckung und Meldung von Sicherheitsverstößen im Umgang mit personenbezogenen Daten
- Unternehmen müsste dann die zuständige Aufsichtsbehörde informieren

Datenschutz in den USA

- USA: zahlreiche Diebstähle personenbezogener Daten und Finanzdaten
- Einer Studie der Firma AOL nach ist Daten- oder auch Identitätsdiebstahl im Internet das Hauptsicherheitsbedenken in der amerikanischen Öffentlichkeit geworden
- Datendiebstahl das führende Verbrechen in den USA mit über 10 Millionen Opfern alleine im Jahr 2003
- In Europa gibt es kein Vergleichbar hohes Aufkommen an Datendiebstählen wie in den USA.

Datenschutz in den USA

- Beispiele:

  „Security Breach Notification Management Policy“
- Februar 2005: Bank of America. Im Februar 2005 verkündete die Bank den Verlust von Sicherungskopien von Kundendaten : 1,2 Millionen Karteninformationen.
- Juni 2005: Citigroup, Verlust von über 3,9 Millionen unverschlüsselter Datensätze von Bankkunden verloren
- 2007 zufolge sind in den USA über 163 Millionen Datensätze mit personenbezogenen Daten an unbefugte Dritte gelangt

Privacy Rights Clearinghouse

- kritisiert das Datenschutzniveau in den USA als nicht ausreichend
- dokumentiert in einer Liste alle Datenverluste und Diebstähle seit Januar 2005..
- Die gegenwärtige Zahl: **511,928,363** Datenmissbräuche
- Umfrage der Washington Post 2005:
- 84 % aller befragten US-Bürger sind der Meinung, dass datenverarbeitende Unternehmen nicht genug in die Sicherung personenbezogener Daten investierten
- 72 % aller befragten Bürger fürchten direkt die Risiken des Online-Datendiebstahls
- Im Internet: http://www.privacyrights.org/data-breach

Fazit

- Strenge Regularien der Europäischen Datenschutzrichtlinie / BDSG vs. wirtschaftlich effizientes Cloud Computing
- Risiko gegen geltendes Recht zu verstoßen
- Herr der Daten unterliegt der Verantwortung, jederzeit in der Verfügungsgewalt der Daten zu sein und deren Sicherheit zu gewährleisten.
- Kein adäquates Datenschutzniveau in den USA
- Kann Safe Harbour ein adäquates europ. Datenschutzniveau gewährleisten ?
- klare vertragliche Regelungen schaffen, um Ihre Ansprüche vertraglich durchsetzen zu können
- Vertragsmuster der EU als Garantie der europäischen Standard -> Vertragliche Absicherung

Vielen Dank für Ihre Aufmerksamkeit