Trust in IT

Gelöste und ungelöste Rechtsfragen im IT-Outsourcing und Cloud Computing

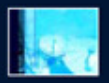
4. Februar 2010

Dr. Alexander Duisberg
Partner, Bird & Bird LLP

BIRD & BIRD

Übersicht

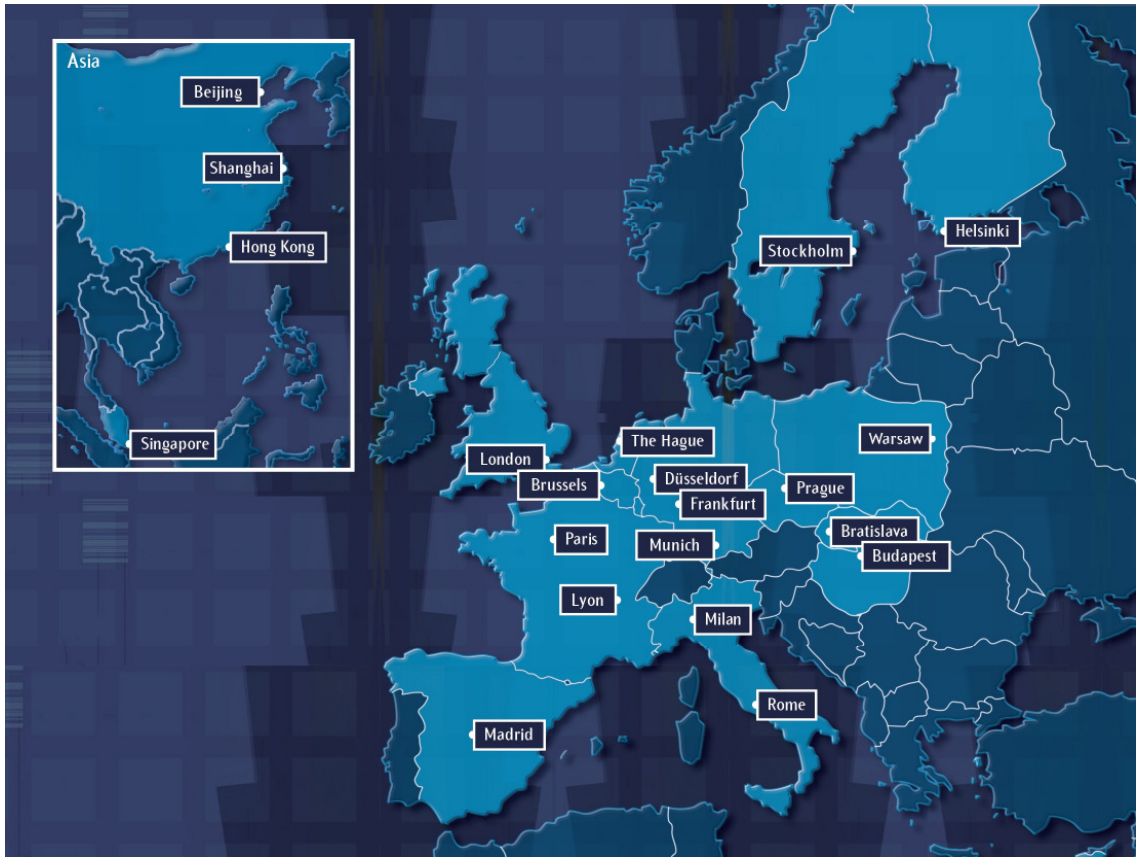
- Über Bird & Bird
- Definition / Merkmale des Cloud Computing
- Anwendbares Recht
  - Internationaler Kontext
  - Vertragstypologie
- Lizenzen / Urheberrecht
- Datenschutz und IT-Sicherheit
  - Personenbezogene Daten in der Cloud
  - Benachrichtigungspflichten bei Sicherheitspannen
- Fazit und Ausblick



Über Bird & Bird – Internationale Ausrichtung

- 21 Büros in Europa und Asien
- Mehr als 830 Anwälte
- Eine der wachstums-stärksten Kanzleien in Europa
- Zahlreiche Auszeich-nungen



Definition / Merkmale des Cloud Computing

- Keine eindeutige, allgemeingültige Definition
- Kennzeichnende Merkmale:
  - Pool aus verschiedenen IT-Leistungen
    - IT-Infrastruktur / Speicherkapazitäten / Datenbanken
    - "Software as a Service" (SaaA), "Platform as a Service" (PaaS) und "Infrastructure as a Service" (IaaS)
    - Anwendungen
  - On-Demand Leistung und i.d.R. auch Abrechnung
  - Netzwerk von Anbietern innerhalb der Cloud (Grid Computing)
- Public Cloud vs. Private Cloud

Anwendbares Recht – Internationaler Kontext (1)

- Ausgangspunkt: Kein globales (IT-) Recht

  ⇨ Nationales Recht ⇨ Deutsches IPR (EGBGB):

  - Grundsatz der freien Rechtswahl, Art. 27 Abs.1 S.1 EGBGB

    ABER: territoriale Anwendbarkeit des Datenschutzrechts und anderer regulatorischer Anforderungen (etwa TK-Recht)

  - Mangels Rechtswahl: Recht des Staates mit den engsten Verbindungen zum Vertrag, Art. 28 EGBGB



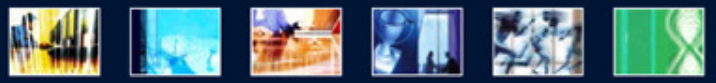



Anwendbares Recht – Internationaler Kontext (2)

- Recht des Staates, mit dem Vertrag (objektiv) die engsten Verbindungen aufweist, Art. 28 Abs.1 S.1 EGBGB
- Vermutung: Sitz des Leistungserbringers, Art. 28 Abs.2 S.1 EGBGB
  - "Cloud"
    - Nationale(r) Anbieter
    - Mehrere Anbieter verschiedener Nationen
- Widerlegung der Vermutung: nach Gesamtheit der Umstände engere Verbindung mit anderem Staat, Art. 28 Abs.5 EGBGB
- Ausnahme Verbraucherverträge: gewöhnlicher Aufenthalt des Verbrauchers, Art. 29 Abs.2 EGBGB

Anwendbares Recht – Vertragstypologie (1)

- Differenzierte Betrachtung der Leistungsbeziehungen
  - Kunde – Anbieter
    - Generalunternehmer (Single Point of Contact)
    - Multi-Vendor-Strategie
  - Anbieter – Anbieter (Verhältnisse innerhalb der Cloud)
- Je mehr / internationaler die Vertragsbeziehungen, desto höher die Komplexität der Verträge
  - Risiko mangelnder Kongruenz und Kompatibilität der vertraglichen Vereinbarungen, Systeme und / oder Services
  - Absicherung regulatorischer Vorgaben, Datensicherheit
  - Abwicklungsprobleme, z.B. Mängelgewährleistung



Anwendbares Recht – Vertragstypologie (2)

- Typenkombinationsvertrag
  - Aus mehreren Leistungsbestandteilen zusammengesetzter Vertrag
  - Mangels prägender Leistung: rechtliche Einordnung je Leistungsbestandteil
    - Für Software"überlassung": Mietrecht*
    - Regelmäßig auch dienstvertragliche und werkvertragliche Komponenten

* BGH-Urteil zu ASP-Vertrag: Zur-Verfügung-Stellen von (beim Anbieter verkörperter) Software zur Nutzung über Telekommunikation gegen Entgelt im Rahmen von ASP / SaaS = **Miete** (Urteil vom 15.11.2006 – XII ZR 120/04)

Lizenzen (1) – Urheberrechte in der Cloud

- Insb. bei Nutzung von Anwendungssoftware im Rahmen des Cloud Computing (→ Software as a Service)
- Insb. wenn Anbieter nicht zugleich Rechteinhaber / Hersteller der Software
- Differenzierung zwischen Kunde und Anbieter erforderlich






Lizenzen (2) – Urheberrecht bzgl. Anbieter

- Relevante Handlungen des Anbieters
  - **Vervielfältigung** (§ 69 c Nr. 1 UrhG)
    - Installation und Arbeitsspeicher hinsichtlich Anwendungssoftware
  - **Keine Vermietung** (§ 69 c Nr. 3 UrhG)
    - Körperliche Überlassung der Software erforderlich
    - Achtung: von reinem Zivilrecht abweichende Wertung
  - **Keine öffentliche Zugänglichmachung?** (§ 69 c Nr. 4 UrhG)
    - In der Regel nicht öffentlich wegen individueller vertraglicher Beziehung zwischen Anbieter und Kunde, § 15 UrhG

Lizenzen (3) – Urheberrecht bzgl. Kunden

- Relevante Handlungen des Kunden
  - Oftmals keine urheberrechtlich relevante Handlung hinsichtlich Anwendungssoftware
    - Keine eigene Vervielfältigung, § 69 c Nr.1 UrhG (Einzelfallbetrachtung anhand technischer Details)
    - Keine Verantwortlichkeit wegen Auslösens einer Vervielfältigung, §§ 97, 69 c Nr.1 UrhG
  - Vervielfältigung der Client- oder Browser-Software
    - Nutzungsrecht erforderlich, sofern nicht bereits vorhanden, § 69 c Nr.1 UrhG

Datenschutz & IT Sicherheit (1)

- Datenschutz
  - § 11 BDSG (Auftragsdatenverarbeitung)
  - §§ 28 ff BDSG (Rechtsgrundlagen für Weitergabe)
  - § 9 BDSG (technische und organisatorische Maßnahmen)
  - §§ 33 ff. BDSG (Rechte der Betroffenen)
- IT Sicherheit
  - z.B. §§ 91 Abs.2, 93 AktG
  - Verfügbarkeit (Erreichbarkeit, Datensicherung, Wiederherstellung)
  - Zugangskontrolle (Authentizität, Integrität, Vertraulichkeit)
- Benachrichtigungspflichten bei Sicherheitspannen

Datenschutz & IT Sicherheit (2)

- Auftragsdatenverarbeitung, § 11 BDSG
  - Auftragsdatenverarbeiter ist kein "Dritter" iSd BDSG
  - Nur in EWR (sonst gelten weitere Voraussetzungen!)
  - Weisungsbefugnis
  - Kontrolle (?)
  - Technische und organisatorische Maßnahmen (§ 9 BDSG) ⇨ welche nationale Rechtsordnung gilt?

⇨ bei Public Cloud kaum denkbar

⇨ bei (reiner) Private Cloud möglich






Datenschutz & IT Sicherheit (3)

Datentransfers außerhalb EWR (Grid, Spiegelung…)

- Einwilligung oder gesetzliche Ermächtigung
  - §§ 28 ff. BDSG
    - Vertragszweck (-)
    - Interessenabwägung
- "Sicheres Drittland"? Safe Harbour? Sonst:
  - Model Clauses
  - Bei konzerninterner Private Cloud ggf. Binding Corporate Rules

Datenschutz & IT Sicherheit (4)

Branchenspezifische Besonderheiten

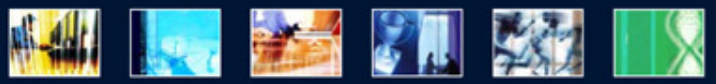
- Geheimnisträger, § 203 StGB
  - U.a.: Ärzte; Anwälte und Steuerberater; Kranken-, Unfall- und Lebensversicherungen
  - "Gehilfe" (str.) ⇨ Maßstab des § 11 BDSG?
    - Public Cloud (-)
    - Private Cloud?
- Finanzdienstleistungen, § 25 a KWG
- Sozialdaten, §§ 67 ff. SGB X

Datenschutz & IT Sicherheit (5)

§ 9 BDSG (techn. und org. Maßnahmen), z.B.

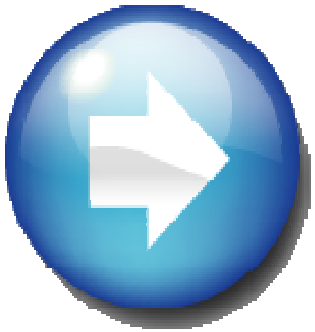
...

3. *zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems **Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen** können, und dass **personenbezogene Daten** bei der Verarbeitung, Nutzung und nach der Speicherung **nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können** (Zugriffskontrolle), …*
5. *zu gewährleisten, dass **nachträglich überprüft und festgestellt werden kann**, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle), …*
8. *zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*



Datenschutz & IT Sicherheit (6)

- Rechte der Betroffenen
  - § 33 BDSG (Benachrichtigung) über:
    - Identität der verantwortlichen Stelle
    - **Ort der Datenverarbeitung**
  - § 35 BDSG (Berichtigung, Löschung und Sperrung)
- Praktische Durchführbarkeit in der Public / Private Cloud?

- World Wide Computing  Datenschutz 3.0 ?

Benachrichtigungspflichten bei Sicherheitspannen – Seit 1. September 2009: § 42 a BDSG

- Seit 1. September 2009 Benachrichtigungspflicht, wenn:
  - bestimmte Arten von personenbezogenen Daten
  - unrechtmäßig übermittelt wurden oder auf sonstige Weise unrechtmäßig Dritten zur Kenntnis gelangt sind, und
  - schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

- Relevante Arten personenbezogener Daten:
  - Daten zu Bank- oder Kreditkartenkonten
  - "besondere Arten personenbezogener Daten" (§ 3 Abs. 9 BDSG), d.h. Angaben über rassische/ethnische Herkunft, politische, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben
  - Daten, die einem Berufsgeheimnis unterliegen (betrifft etwa Versicherungen, Wirtschaftsprüfungs- oder Steuerberatungsgesellschaften)
  - Daten, die sich auf (Verdacht auf) strafbare Handlungen oder Ordnungswidrigkeiten beziehen

Benachrichtigungspflichten bei Sicherheitspannen – Durchführung (1)

- Wer muss benachrichtigt werden?
  - Zuständige Aufsichtsbehörde und
  - Betroffene (alle Personen, deren Daten von der Sicherheitspanne betroffen sind)

- Wann muss benachrichtigt werden?
  - Aufsichtsbehörde: "unverzüglich" nach Kenntnis
  - Betroffene: "Responsible Disclosure":

    unverzüglich, nachdem
    - "angemessene Maßnahmen zur Sicherung der Daten" ergriffen worden sind (bzw. hätten ergriffen werden können)
    - Strafverfolgung der etwaigen Täter durch Mitteilung an die Betroffenen nicht mehr gefährdet wird






Benachrichtigungspflichten bei Sicherheitspannen – Durchführung (2)

Wie muss die Benachrichtigung aussehen?

- Gegenüber Betroffenen
  - verständliche Darstellung der Art der Sicherheitspanne
  - empfohlene Maßnahmen zur Minderung nachteiliger Folgen

  - Kollektivbenachrichtigung möglich, falls individuelle Benachrichtigung unverhältnismäßig aufwändig wäre:
    - durch Anzeigen von mindestens einer halben Seite in mindestens zwei bundesweit erscheinenden Tageszeitungen (vom Bundesrat als unverhältnismäßig kritisiert), oder
    - durch eine andere, gleich effektive Maßnahme

Benachrichtigungspflichten bei Sicherheitspannen – Durchführung (3)

Wie muss die Benachrichtigung aussehen?

- Gegenüber Aufsichtsbehörde darzustellen:
  - Art der Sicherheitspanne
  - Mögliche nachteilige Folgen der unrechtmäßigen Kenntniserlangung
  - Die zur Abwendung nachteiliger Folgen ergriffenen Maßnahmen
- Verstoß und Geldbußen:
  - Erforderliche Benachrichtigung erfolgt *nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig* (§ 43 Abs. 2 Nr. 7, Abs. 3 BDSG)
  - Geldbußen von bis zu EUR 300.000
  - Sogar höher, wenn das Unternehmen aus Nichterfüllung der Benachrichtigungspflicht höheren wirtschaftlichen Vorteil gezogen hat (§ 43 Abs. 3 Satz 3 BDSG)

Fazit und Ausblick

- Vielfalt der Clouds ⇨ vielschichtige Vertragsgestaltungen
- Internationalität der Cloud ⇔ nationale regulatorische Beschränkungen
- Regulatorische Kundenanforderungen ⇨ (eher) Private Cloud

- Welche Grenzen setzen Datenschutz und Datensicherheit?

ODER

- Wird die universelle Durchsetzung von nationalem Datenschutz in der Cloud scheitern?

Ihre Fragen…

Vielen Dank.

Alexander Duisberg
Partner
Bird & Bird LLP

Pacellistraße 14
80333 München
T: +49-89-3581 6239
F: +49-89-3581 6011
E-mail: alexander.duisberg@twobirds.com

JUVE 2008 AWARDS
Kanzlei des Jahres für IT