CLOUDwerker

Rechtliche Fragen im Umgang mit Cloud Technologien

17.11.2014 – Stuttgart –

Der Referent: RA Dr. Carsten Ulbricht

- IT-Recht / Gewerblicher Rechtsschutz und Datenschutz
- Spezialisierung auf Internet und Social Media
- Blog „Web 2.0, Social Media & Recht“

www.rechtzweinull.de

www.twitter.com/intertainment

Bartsch Rechtsanwälte

Bartsch
Rechtsanwälte

Ihre Partner für Unternehmensrecht

Wirtschaftsrecht / IT-Recht / Bau-und Immobilienrecht
Arbeitsrecht / Handels- und Gesellschaftsrecht / Erbrecht

Prof. Dr. Michael Bartsch
Ina Bender
Thorsten Culmsee
Joachim Dorschel
Dr. Stephanie Funk
Ulrich. A. Götz
Dr. Alexander Hoff
Jenny Hubertus
Anne Menzerath
Dr. Reinhard Möller
Sabine Przerwok
Dr. Carsten Ulbricht M.C.L.
Thorsten Walter

STANDORT STUTTGART:
Stafflenbergstrasse 24
70172 Stuttgart
Telefon: +49 (0)721 504472-0
Telefax: +49 (0)721 504472-01
E-Mail: cu@bartsch-rechtsanwaelte.de

STANDORT KARLSRUHE
Bahnhofstraße 10
76137 Karlsruhe
E-Mail: mail@bartsch-rechtsanwaelte.de

Überblick

A. Einführung

B. Anwendbares Recht

C. Vertragsgestaltung

D. Urheberrecht

E. Datenschutz und –sicherheit

F. Zusmmenfassung und Resümee

A. Einführung

Dienstleistungsmodelle

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)

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

B. Anwendbares Recht

Internationales Vertragsrecht

Rechtswahl

- B2B: zulässig
- B2B: gegenüber Verbrauchern gilt gewähltes Recht, jedoch Günstigkeitsvergleich zugunsten Verbraucher

keine Rechtswahl

- objektive Anknüpfung an vertragscharakteristische Leistung: Recht des Anbieters
- B2C: Recht am gewöhnlichen Aufenthalt des Verbrauchers

➔ Tipp: Kunde sollte auf Rechtswahl drängen

C. Vertragsgestaltung

Vertragstypologie

Bestimmung des **Leitbilds** der Klauselkontrolle nach § 307 Abs. 2 BGB bei standardisierten Verträgen

Unterschiedliche Leistungen / unterschiedliche Schwerpunkte

- ➔ **typengemischte** Verträge ...
- ➔ ... mit im Wesentlichen **mietvertraglichem** Charakter;
  - nach BGH Application Service Providing = Mietvertrag
  - 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

- ➔ grundsätzlich 100% Verfügbarkeit geschuldet

Im Wesentlichen **dienst- und werkvertragsrechtlich** zu qualifizierende Zusatzleistungen, z.B. Support, Updates, Back-ups

Vertragsgestaltung

Empfehlung

- Gestaltung eines einheitliches Leistungsstörungsrecht und Kodifizierung von Verfügbarkeitsquoten mittels **Service Level Agreements**
- Leistungsgegenstand, Verfügbarkeit, Performance (insb. Antwortzeit), Übergabepunkte, Reaktions- und Beseitigungszeiten etc.
- Beauftragung von **Subunternehmern**, z.B. Amazon Web Services

  ➔ Cloud-Anbieter häufig als Generalunternehmer
- Regelungen zum **Notfall-Management**
- Regelung zum **Vertragsende**, insbesondere zur **Datenherausgabe** (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 (99,x %)

- wichtig: Bezugszeitraum
- Messung, Berichtswesen, Sanktionen
- z.T. Lastobergrenzen
- aus Kundensicht möglichst unmittelbare Auswirkungen auf Vergütung
- optional: maximale Ausfallzeiten pro Ausfall

Verfügbarkeitsklauseln

- »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.“

Verfügbarkeitsklauseln

- **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. (...)

Auszug aus Amazon Web Services Customer Agreement

D. Urheberrecht

Urheberrecht

Merke:

Anbieter braucht Zustimmung/Lizenz für Cloud Computing

Betroffene Verwertungsrechte:

- Vervielfältigung (§ 69c Nr. 1 UrhG)
- Öffentliche Zugänglichmachung per Internet (§ 69c Nr. 4 UrhG)(str.)
- Cloud Computing als eigenständige Nutzungsart (§ 31 UrhG) (str.)

Sonderproblem: Nutzung von Drittsoftware / Open Source Software (OSS)

E. Datenschutz & Datensicherheit

Einführung

- Int. anwendbares Recht: **Territorialitätsprinzip**
- **Personenbezogene Daten** sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)

➔ Personenbezogene Daten sind häufig Gegenstand der Datenverarbeitung

➔ Datenschutzrecht daher für die Verarbeitung in der Cloud in aller Regel zu beachten

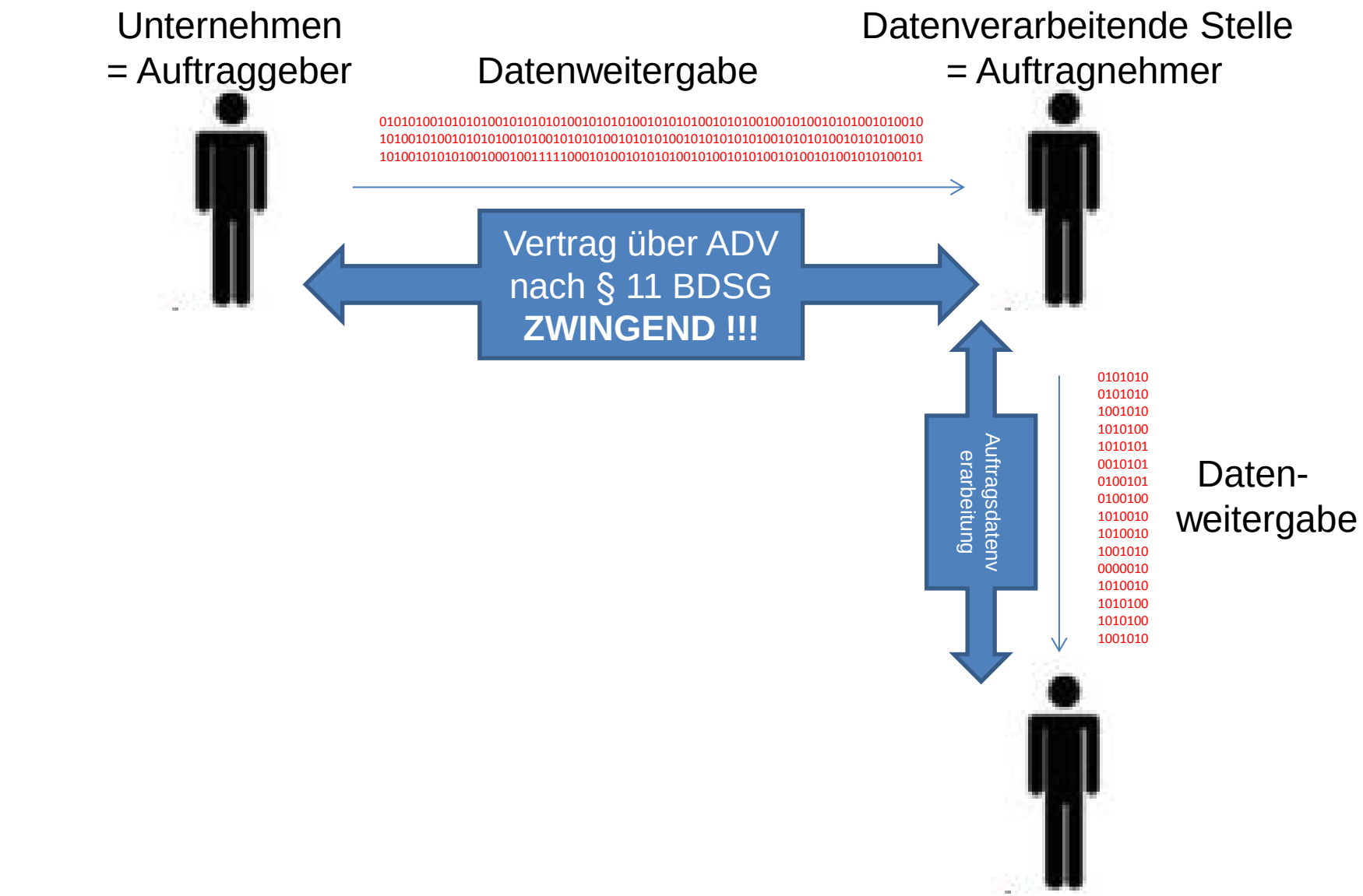
➔ Lösung der datenschutzrechtlichen Probleme teilweise über **Anonymisierung** personenbezogener Daten im Wege der Verschlüsselung

Datenschutz

Verbot mit Erlaubnisvorbehalt

- Die Übermittlung an und die Verarbeitung durch den Cloud-Anbieter bedarf einer **Rechtfertigung**
- Wichtigste **gesetzliche Erlaubnistatbestände** für die Verarbeitung durch den Cloud-Anbieter
  - ➔ Wahrung berechtigter Interessen, Interessenabwägung
  - ➔ häufig nicht einschlägig
- Einwilligung der Betroffenen: in der Regel unpraktikabel
  - ➔ bei Vielzahl von Betroffenen
  - ➔ ausreichende Information bei Datenverarbeitung schwierig
- Entbehrlich bei Auftragsdatenverarbeitung …

Übersicht: Auftragsdatenverarbeitung



Auftragsdatenverarbeitung

- Sorgfältige **Auswahl und Überwachung** des Cloud-Anbieters hinsichtlich der von ihm getroffenen techn. und organisatorischen Maßnahmen
  - ➔ Kunde muss „Herr der Daten“ bleiben
  - ➔ Prüfung der gesamten Cloud-Lieferkette erforderlich

  Problem: Große Anbieter gestatten aber häufig keinen Einblick

- **Schriftliche Erteilung** des Auftrags

- **10-Punkte-Katalog** mit erforderlichen Mindestregelungen

Auftragsdatenverarbeitung

Mindestinhalte gemäß § 11 Abs.2 BDSG

- 1. der Gegenstand und die Dauer des Auftrags,
- 2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- 3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
- 4. die Berichtigung, Löschung und Sperrung von Daten,
- 5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- 6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,

Auftragsdatenverarbeitung

Mindestinhalte gemäß § 11 Abs.2 BDSG

- 7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- 8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
- 9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- 10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Auftragsdatenverarbeitung

Einhaltung der Anforderungen an die AuftragsDV-Vereinbarung

- Standardverträge der Anbieter oftmals unzureichend
- in der Regel nicht verhandelbar, da Leistungen standardisiert
- unzureichende Auftragserteilung bußgeldbewehrt

<u>Lösungsmöglichkeiten</u>

- Auswahl eines **geeigneten Anbieters** (z.B. Microsoft und Salesforce ADV auf Nachfrage)
- **Private Cloud:** Bei konzernbetriebener Private Cloud Ausgestaltung als Auftragsdatenverarbeitung; bei Eigenbetrieb nicht erforderlich

Auftragsdatenverarbeitung (außerhalb EWR)

Nach h.M. keine Auftragsdatenverarbeitung in Drittstaaten

- ➔ Cloud-Anbieter ist **Dritter**
- ➔ **Einwilligung in Übermittlung** oder
- ➔ **Gesetzlicher Erlaubnistatbestand erforderlich**

Voraussetzung für die Zulässigkeit einer Datenverarbeitung in Drittstaaten ist außerdem die Sicherstellung eines **angemessenen Datenschutzniveaus**

- Unterwerfung des Anbieters unter Safe Harbor (umstritten)
- EU-Standardvertragsklauseln
- Binding Corporate Rules

Dazu auch noch **entsprechende** Anwendung der Regeln zur Auftragsdatenvereinbarung (tvA)

Datensicherheit

Warum IT-Sicherheit?

Grundwerte:

- **Vertraulichkeit** (Schutz vertraulicher Informationen vor unbefugter Preisgabe geschützt werden)
- **Verfügbarkeit** (Benutzer stehen Dienst-leistungen oder auch Informationen zum geforderten Zeitpunkt zur Verfügung)
- **Integrität** (Daten sind vollständig und unverändert)

Datensicherheit

- 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, Bestätigungsvermerke unabhängiger Auditoren u.ä.

Datensicherheit

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

F. Zusammenfassung und Resümee

Bartsch
Rechtsanwälte

Zusammenfassung

Für Cloud Anbieter:

- Angemessenes Datenschutzniveau (Server in Europa)
- Transparente und ausgewogene Vertragsgestaltung,
- Definition der Leistungsgüte und Verfügbarkeit (SLA)
- Einräumung von Nutzungsrechten an Fremdsoftware
- Gewährleistung von Datenschutz und –sicherheit
- Auftragsdatenverarbeitungsvertrag anbieten

Zusammenfassung

Für (Unternehmens-)kunden:

- Anbieterauswahl (Europa)
- Absicherung über Vertragsgestaltung (SLA) vor allem im Hinblick auf Datenschutz und –sicherheit, Verfügbarkeit und Ausstiegsszenarien
- Auftragsdatenverarbeitungsvertrag

Bartsch Rechtsanwälte

Weiterführende Links

- Übersicht “Social Media & Recht„
  (www.kurzlink.de/socialweb)
- Social Media Marketing & Recht – Dos and Donts beim Werben im Social Web
  (www.kurzlink.de/some)
- Social Media Guidelines & Recht – Warum Unternehmen und Mitarbeiter klare Richtlinien brauchen
  (www.kurzlink.de/guidelines)
- Social Media Richtlinien – (Rechtliche) Leitplanken schaffen Medienkompetenz
  (www.kurzlink.de/medienkompetenz)
- Enterprise 2.0 & Recht – Blogs, Wikis und Social Networks im Intranet
  (http://kurzlink.de/enterprise20)

Bartsch Rechtsanwälte

Literatur

www.kurzlink.de/smbuch

www.rechtzweinull.de

XING

twitter

Bartsch Rechtsanw
Dr. Carsten Ulbricht M.
Rechtsanwalt

Stafflenbergstraße 24
70184 Stuttgart
Telefon: +49 (0)711 23 84 953
Fax: +49 (0) 711 23 84 9531
E-Mail: cu@bartsch-rechtsanwaelte.de
Blog: www.rechtzweinull.de

36

Bartsch Rechtsanwälte