Kinast & Partner

Rechtsanwälte
Externe Datenschutzbeauftragte

Datenschutz in der Cloud

Köln, den 23.09.2015

Übersicht

I. Einführung: Cloud Computing

II. Datenschutzrechtliche Probleme in der Cloud

Einführung: Cloud Computing

Definition von Cloud Computing

Bundesamt für Sicherheit in der Informationstechnik (BSI):

„CC bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz."

„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."

Cloud Computing

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)

Bedarfsgerechte Bereitstellung standardisierter Geschäftsanwendungen

IT-Ressourcen und Applikationen

Cloud Computing

Vorteile für Kunden

- Die Public Cloud ist ein Angebot eines frei zugänglichen Providers, der seine Dienste offen über das Internet für jedermann zugänglich macht. Webmailer-Dienste oder die bekannten Google-Docs sind ebenso Beispiele für Public Cloud Angebote wie die kostenpflichtigen Services eines Microsoft Office 365 oder eines SAP Business by Design.

- Dem gegenüber stehen Private Cloud Dienste. Der Kunde entscheidet z.B. über die Ausstattung, den Standort der Server und die Art sowie Anzahl der virtuellen Maschinen. Er teilt die Hardware mit keinem anderen und kann die Server in speziell gesicherten Datenzentren des Anbieters betreiben (lassen).

- Mit Hybrid Clouds werden Mischformen dieser beiden Ansätze bezeichnet. So laufen bestimmte Services bei öffentlichen Anbietern über das Internet, während datenschutzkritische Anwendungen und Daten durch das Unternehmen betrieben und verarbeitet werden.

Cloud Computing

Vorteile für Kunden

- 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“)

Cloud Computing

Public Cloud vs. Private Cloud

Public Cloud

- Anbieter stellt Kapazität & Software bereit
- Keine Anschaffungskosten
- Immer aktuellste Software
- Flexibilität in Service & Kapazität (lässt sich nach Bedarf aufstocken)
- Minimaler Managementaufwand
- Kostengünstig (wg. Standardisierung)

- Cloud offen für jeden
- Anbieter hostet Daten aller Kunden auf derselben Infrastruktur (standardisiert)
- Mehrere Kunden teilen sich die gleichen Ressourcen

Private Cloud

- Individualität
- Anbieter betreut z.B. Server des Kunden in hochsicheren Rechenzentren
- Hohe Sicherheit → Anbieter stellt Ressourcen über besonders sichere Leitungen zur Verfügung
- Möglichkeit zusätzliche Services mit dem Anbieter zu vereinbaren (z.B. mehr Service, höhere Verfügbarkeit, besserer Notfallplan)
- Kontrolle bleibt beim Kunden → Daten verlassen die unternehmensspezifische Cloud nicht

- Höhere Kosten
- Höhere Abhängigkeit von der Zuverlässigkeit des Anbieters, dessen Services, Technik und Verfügbarkeit

Cloud Computing

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** ...

- Kundensupport-Center (**Ticketsystem** mit zentralem Datenbestand) zur Anbindung von Niederlassungen im Ausland

Aber: Ausschöpfung der Vorteile häufig nur bei Public Clouds möglich

Datenschutzrechtliche Probleme der Cloud

Cloud Computing

Problem: Datenherrschaft

- **Physischer Standort** nicht bekannt (Widerspricht Auskunftsrecht gem. § 34 BDSG)

- Fehlende **Kontrollmöglichkeiten** im Sinne der Auftragsdatenverarbeitung (§ 11 II BDSG), insbesondere auch beim Subdienstleister

- Fehlende **Datentrennung**

- Fehlende **Datenminimierung** (Häufig diverse Kopien)

- **Verantwortlichkeit** für Daten liegt beim Auftraggeber (hier: Cloud-Kunden), wegen des Schutzinteresse des Betroffenen

Beispiel: AWS – Datenherrschaft des Auftraggebers gewährleistet?

Laut AWS (EU Datenschutz Whitepaper):

Kunden / Auftraggeber behalten die Kontrolle über ihre Inhalte und sind dafür verantwortlich und vollumfänglich befähigt, Sicherheitsanforderungen zum Schutz ihrer Inhalte zu regeln und zu kontrollieren, unter anderem:

- Bestimmung darüber, **wo ihre Daten und Inhalte abgelegt** werden, z.B. Art der Speicherumgebung und die geographische Lage des Speichers

- Bestimmung des **Formats des Inhalts**, z.B. nur Text, anonymisiert oder verschlüsselt durch die von AWS angebotene Verschlüsselung oder Verschlüsselung eines Drittanbieters

- Verwendung von **Zugriffskontrollen, Identitätsmanagement und Sicherheitsanmeldeinformationen**

- Nutzung von **SSL, Virtual Private Cloud, andere Netzwerksicherheitsmaßnahmen** zur Verhinderung unberechtigter Zugriffe

ABER: Kann dadurch die Datenherrschaft tatsächlich gewährleistet werden?

Cloud Computing

Problem: Drittländer

- Bei Datenverarbeitungen durch den Cloud-Anbieter außerhalb der EU/EWR: Geltung der besonderen Anforderungen der **§ § 4b, 4c BDSG** für den Drittstaatentransfer

- **Drittstaaten ohne angemessenes Datenschutzniveau**: Cloud-Anwender als verantwortliche Stelle muss **ausreichende Garantien** zum Schutz des Allgemeinen Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweisen, beispielsweise durch:
  - Standardvertragsklauseln
  - Binding Corporate Rules bzw. Processor Binding Corporate Rules
  - Safe Harbor Zertifizierung

- Bei Datenübermittlung an einen im Drittstaat ansässigen Unter-Anbieter bleibt **Verantwortlichkeit des Cloud-Anwenders: Ordnungsgemäße Auswahl verpflichtend**.
  - Prüfung der Datensicherheit genügt nicht.
  - Art. 29-Gruppe konkretisiert:
    - Verfügbarkeit
    - Vertraulichkeit
    - Integrität
    - Transparenz
    - Nicht-Verkettbarkeit
    - Intervenierbarkeit

Cloud Computing

Problem: Safe Harbor

Verarbeitung personenbezogener Daten durch den Cloud-Anbieter mit Sitz in den USA zulässig, wenn sich der Cloud-Anbieter zur Einhaltung der Safe-Harbor-Grundsätze verpflichtet hat?

- Keine flächendeckende Kontrolle dieser Selbstzertifizierung der Cloud-Anbieter durch die Kontrollbehörden in Europa und den USA **gewährleistet**

- **Daher:** Verpflichtung von deutschen Cloud-Anwendern, **Mindestkriterien** zu prüfen, bevor personenbezogene Daten an einen auf der Safe-Harbor-Liste geführten Cloud-Anwender übermittelt werden

- Es bestehen **folgende Prüfpflichten** für den Cloud-Anwender:
  - Überzeugung, ob das Zertifikat des Cloud-Anbieters noch gültig ist und sich auf die betreffenden Daten bezieht (z.B. Personaldaten)
  - Prüfung, ob der Cloud-Anbieter sich zur Zusammenarbeit mit den EU-Datenschutz-aufsichtsbehörden verpflichtet hat
  - Durchsetzung von Auskunftspflichten prüfen und vertraglich regeln

- **Dokumentationspflicht dieser Mindestprüfung** zum Nachweis bei der Aufsichtsbehörde

Cloud Computing

Problem: Datenzugriffe durch Dritte

- **Ausländische Ermittlungsbehörden** auf Grundlage unterschiedlicher Gesetze (z.B. Patriot Act, Foreign Intelligence Surveillance Act (FISA), Electronic Communications Privacy Act (ECPA), National Security Letters)
  - Verantwortlich bleibt der Auftraggeber und keine Berufung auf Art. 8 EMRK möglich

- Erforderlich: **Vertragliche Garantie** eines US-Anbieters, dass Daten den EWR **nicht** verlassen
  - Cloud-Anbieter muss sich dann vor den US-Gerichten **gegen den Zugriff durch Behörden** wehren, denn er würde mit einer Datenweitergabe aus einem EU-Rechenzentrum an US-Behörden das **EU-Recht (inkl. Vertragsrecht) verletzen**

- **Aber aktuell:** Auch europäische Tochtergesellschaften von US-Anbietern unterliegen dem Patriot Act
  - Rechtsgrundlage **Stored Communications Act (18 U.S.C. § § 2701-2712),**
  - des **US District Court Southern District of New York, 25.4.14:** Aufbau, Historie des Gesetzes und praktische Erwägungen lassen auch **extraterritoriale Anordnungen** zu

- **Nationale Ermittlungs-/Strafverfolgungsbehörden (z.B. BND, BfV)** sind u.U. (unabhängig von einer Cloud Lösung) legitimiert gem. StPO, BNDG, G10-Gesetz auf Daten zuzugreifen bzw. diese heraus zu verlangen

Beispiel: AWS – Zugriffsrechte von Regierungen?

Laut AWS (EU Datenschutz Whitepaper):

„Die meisten Länder haben Gesetze zum Zugriff auf Daten, die auch über die Landesgrenzen hinaus anwendbar sein sollen."

Beispiel: US Patriot Act

„Der Patriot Act unterscheidet sich nicht von den Gesetzen vieler anderer Industriestaaten, welche die Regierungen ermächtigen, Informationen im Zusammenhang mit den Ermittlungen zu internationalem Terrorismus und anderen Angelegenheiten des Auslandsgeheimdienstes zu erhalten. Jedes Verlangen auf Herausgabe von Dokumenten unter dem Patriot Act erfordert einen Gerichtsbeschluss, der darlegt, dass das Verlangen im Einklang mit den Gesetzen steht, z.B. dass das Verlangen mit rechtmäßigen Ermittlungen zusammenhängt."

AWS-Policy:

- Keine Offenlegung von Kundeninhalten, *außer dies ist erforderlich,* ***um rechtlich gültigen und bindenden Anordnungen wie einer richterlichen AO nachzukommen***
- Prüfung jedes Ersuchens, um Richtigkeit und Übereistimmung mit geltendem Recht zu verifizieren
- ***Benachrichtigung*** des Kunden vor der Herausgabe

Problem: Subdienstleister

- Oft „**Kettenverarbeitung**“ durch Einsatz von Sub-Dienstleister(n)
  → Dadurch fehlende Transparenz und Datenherrschaft (s.o.)
- Werden Sub-DL ausgetauscht, erfährt der Kunde dies nicht
- Es droht Einhaltung lediglich der lokalen Gesetze der Länder der Firmensitze der jeweiligen Subdienstleister, obwohl im Interesse des Cloud-Kunden die für ihn bzw. für diene Kunden geltenden Gesetze zur Anwendung kommen müssten (Haftung!)
- Wenn der Cloud-Kunde **selbst DL** ist:
  → zwangsläufige juristische Mängel, wenn Datensicherheit auch beim Sub-DL vertragsgemäße Aufgabe des Cloud-Anwenders gegenüber dem Kunden ist

Beispiel: AWS – Zugriffsmöglichkeiten von Subdienstleistern?

Laut AWS (EU Datenschutz Whitepaper):

- Einsatz von „verschiedenen externen Subunternehmern, die AWS bei der Erbringung der Services unterstützen“
- Subdienstleister „haben keinen Zugriff auf Kundeninhalte“
    - Aber sie dürften dennoch sehr nahe an den Daten sein und damit greift lediglich ein Minus an Datensicherheit gegenüber den Subunternehmern
- Einsatz von „vertraglichen Schutzmaßnahmen“, die AWS überwacht, um zu gewährleisten, dass die „geforderten Standards aufrecht erhalten werden“
    - Begriff „vertraglichen Schutzmaßnahmen“ wird nicht näher definiert!
    - Ebenso wenig ist fraglich, was „geforderte Standards“ sind

Problem: AGB /Vertragsgestaltung

AGB

- Analyse der AGBs in Praxis zeigt: Formulierungen sehr anbieterfreundlich zum Nachteil des Kunden

- Oft keine Beachtung/Anwendung der Regelungen zur ADV (§ 11 BDSG)

- Verwendung und Auslegung von AGBs gem. dem Recht des Sitzlandes des Cloudanbieters

➢ Folge: Verstöße des Anbieters fallen auf Kunden zurück, d.h. hohes Haftungsrisiko des Unternehmens

Vertragsgestaltung

- einheitliches **Leistungsstörungsrecht /Kodifizierung von Verfügbarkeitsquoten** mittels Service Level Agreements

- **Leistungsgegenstand, Verfügbarkeit, Performance (insb. Antwortzeit), Übergabepunkte, Bezugsgrößen, Messpunkte, Reaktions- und Beseitigungszeiten** etc.

- 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

Cloud Computing

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 …")

Beispiel: AWS 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. (...)

Technisch-organisatorische Maßnahmen

▪ Technische Sicherheit ist zumindest bei großen Cloud-Anbietern durchaus (durch Zertifizierungen nach ISO 27001, SOC oder PCI DSS) gegeben, aber…

- **Fehlende Transparenz** der technischen Sicherheit wg. unzureichender Informationen vom Anbieter über die Verarbeitungsprozesse (vgl. §§ 9, 11 BDSG)

▪ **Kontrollpflicht**: Auftraggeber sollte sich vor Beginn der Datenverarbeitung und dann regelmäßig von der Einhaltung der Maßnahmen des Anbieters zu überzeugen

- **Problem**: Kontrollpflicht kann kaum umgesetzt werden, da vertraglich zumeist nicht vorgesehen bzw. auf Prüfung der Aktenlage beschränkt.

Beispiel: AWS – Technische Datensicherheit gewährleistet?

Laut AWS (EU Datenschutz Whitepaper):

- Differenzierung zwischen **Verantwortlichkeit des Kunden** (Technische Datensicherheit in der Cloud) und **Verantwortlichkeit von AWS** (Technische Datensicherheit der Cloud-Umgebung)

- **Überprüfung der Wirksamkeit** der technischen Sicherheit, einschließlich der Sicherheit der physischen Rechenzentren **durch externe Auditoren**

- Auf schriftliche Anfrage des Kunden und nach Unterzeichnung einer Vertraulichkeitsvereinbarung „kann" AWS eine **Zusammenfassung des Prüfberichts** übersenden
    - Nachhaken?
    - Mängelbehebung?
    - Massstab der Prüfung?

Cloud Computing

Beispiel: AWS – Wie steht es um den Datenschutz tatsächlich?

- April 2015: Bekanntgabe von AWS, dass die luxemburgische CNPD die Datenverarbeitungsvereinbarung geprüft habe und AWS damit die EU-Datenschutzgesetze erfülle

- Tatsächlich schränkt die luxemburgische Behörde die Aussagen erheblich ein:
  - Sehr begrenzte Untersuchung, dasBeschränkung auf die Datenverarbeitungsvereinbarung und den Annex 2 der Standardvertragsklauseln von Amazon
  - Keine Bestätigung dafür, dass AWS in der Praxis generell den EU-Datenschutzbestimmungen entspräche

- Kritik aus der Wirtschaft:
  - Es kann tatsächlich nicht festgestellt werden, ob das von AWS vorgegebene Daten-schutzniveau dem in Deutschland geforderten entspricht, weil sich die Ausführungen ausschließlich auf EU-Recht beziehen
  - Zertifizierungen erfolgen nach einer Analyse, die der zu zertifizierende Dienst selbst vornimmt

Kinast & Partner
Rechtsanwälte
Externe Datenschutzbeauftragte

Ihr Ansprechpartner

Kinast & Partner Rechtsanwälte
RA Dr. Karsten Kinast, LL.M.
kinast@kinast-partner.de
Mobil: +49 (0)1520 – 905 32 14

Standort Köln:
Venloer Straße 24 · 50672 Köln
Telefon: +49 (0)221 - 222 183-0
Telefax: +49 (0)221 - 222 183-10

Standort Frankfurt am Main:
Schneckenhofstr. 27 · 60596 Frankfurt a.M.
Telefon: +49 (0)69 - 247 47 11–0
Telefax: +49 (0)69 - 247 47 11–10

Standort München:
Fürstenstraße 5 · 80333 München
Telefon: +49 (0)89 - 244 14 25-0
Telefax: +49 (0)89 - 244 14 25-10

Standort Nürnberg:
Schmausenbuckstr. 90 · 90480 Nürnberg
Telefon: +49 (0)911 - 477 103-0
Telefax: +49 (0)911 - 477 103-10