Cloud-Computing - rechtliche Aspekte

Forum **7-it**

RA Rainer Friedl

München, 16. November 2015

Verpflichtung zur IT-Compliance: Haftung des Vorstands/Geschäftsführer für IT-Risiken

- Vorstandspflicht bei AGs (§ 93, Abs.1 AktG)
  - „… Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden …“
  - Pflicht zum Risikomanagement § 91, Abs. 2. AktG

    „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“

- **Ausstrahlungswirkung auf Geschäftsführer anderer Gesellschaftsformen:** je nach Größe, Komplexität und Struktur eines Unternehmens sind die Geschäftsführer durch analoge Anwendung ebenso verpflichtet/betroffen (vgl. § 43 GmbHG).

Vertragliche Rahmenbedingungen

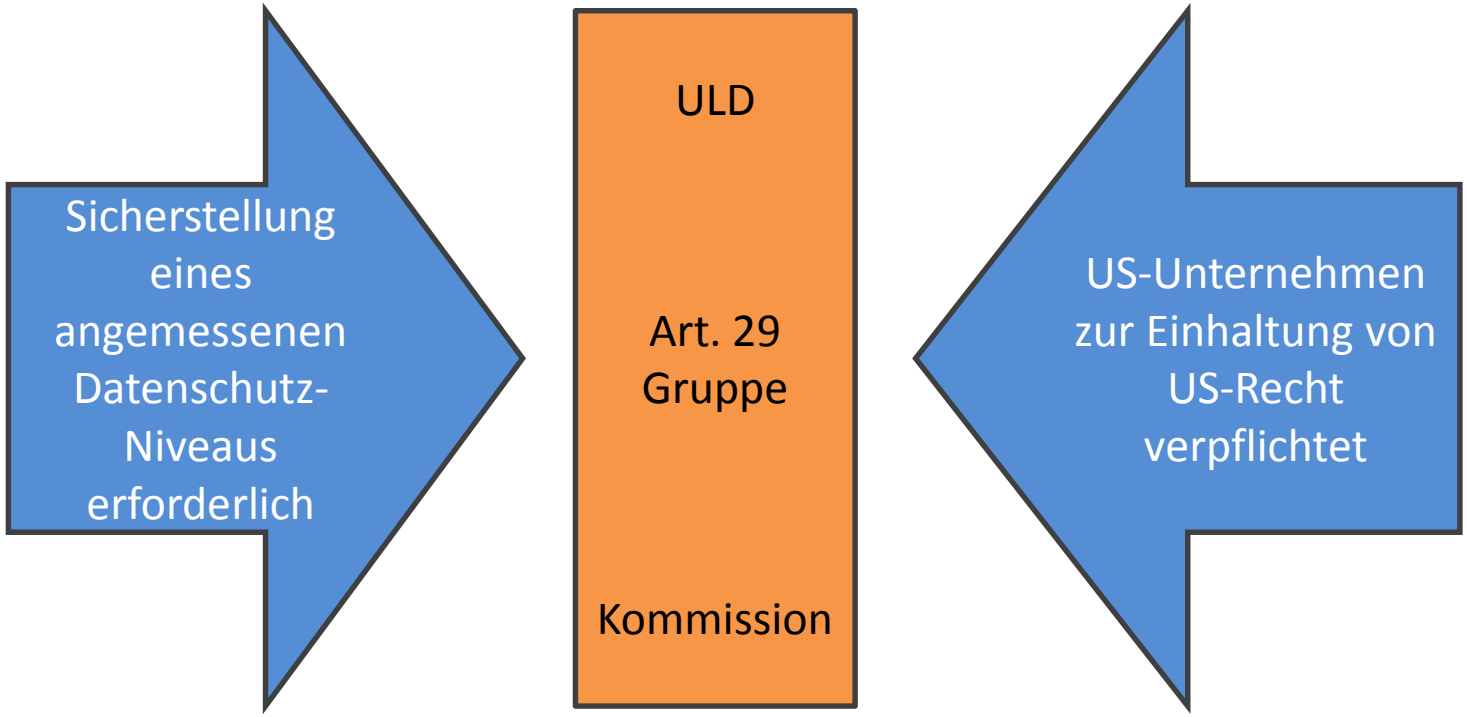
- Cloud-Anwendungen müssen mit dem Anbieter immer vertraglich fixiert werden.
- AGBs von Anbietern müssen überprüft und ggf. angepasst und ergänzt werden.
- Auftragsdatenverarbeitung i.d.R. erforderlich (TOM!).
- Anbieter im EWR-Ausland oder mit Auslandsbezug erfordern zusätzliche Prüfungen.

RIP, Safe Harbor: Was nun? Theoretische Alternativen:

- Einwilligung
- Erforderlich zur Erfüllung einer vertraglichen Verpflichtung
- EU-Standardvertragsklauseln (Office 365 „Zusatzoption“)
- Vertragliche Datenschutz-Regelung
- Binding Corporate Rules (BCR)

Übertragung/Verarbeitung in USA erlaubt?

Massenhafte, anlasslose Überwachungspraxis in den USA



Microsofts aktueller Vorstoß in Deutschland: If you make it there, you make it everywhere

Aussagen Microsoft (http://www.microsoft.com/de-de/cloud/deutsche-datentreuhand.aspx):

- "Sämtliche Kundendaten und erforderlichen Systeme befinden sich in deutschen Rechenzentren."
  => Erfreulich

- "Ein eigenständiges deutsches, vom öffentlichen Internet getrenntes Datennetzwerk wird genutzt.„
  => öffentliches Internet? Was genau nutzt das?

- "Ein deutscher Datentreuhänder kontrolliert physischen und technischen Zugriff auf Kundendaten."
  => Was ist ein Datenschutz-Treuhänder?
  => Kontrolle der Zugriffe?

- Bekenntnis, anwendbaren Compliance-Anforderungen und Zertifizierungen zu entsprechen.
  => Bekenntnis ist genau was?

Vorbereitung einer Cloud-Nutzung: Technische Machbarkeitsstudie - Proof of Concept

- Technische Rahmenbedingungen (Internetbandbreite, Verfügbarkeit von abhängigen Diensten insbes. bei Hybrid-Lösungen)
- Service-Definitionen und Service-Abhängigkeiten prüfen
- Welche Prozess-Anpassungen sind notwendig

Vorbereitung einer Cloud-Nutzung: Rechtliche Machbarkeitsstudie

Rechtliche Rahmenbedingungen müssen geplant und geprüft werden, insbesondere:

- Allgemeine Gesetze und VOen:
  StGB, Arbeitsrecht, TKG, TMG, AO mit GoBS und GDPdU, …
- Datenschutz und (besondere) personenbezogene Daten
- Standes-/berufsrechtliche Vorgaben (Ärzte, Steuerberater, Rechtsanwälte, Gesundheitswesen, Banken, etc.)
- IPs und vertragliche Vereinbarungen mit Dritten
- Lizensierungen (schon wegen Einsparungspotenzial)
- Behörden: VO für die Vergabe öffentlicher Aufträge
- Auswahl des Anbieters (Begründung)
- Kontrollrechte

Vorbereitung einer Cloud-Nutzung: Risikoanalyse und -bewertung

Zusätzliche Risiken müssen identifiziert und unter Beachtung von IS-Prinzipien bewertet werden (Verfügbarkeit, Vertraulichkeit, Integrität):

Wichtige Cloud-Zusatzrisiken:

- Zugriff auf die Daten durch den Cloud-Anbieter
- Zugriffsmöglichkeiten durch staatliche Behörden aufgrund der (ggf. ausländischen) Jurisdiktion, die für den Cloud-Anbieter zutrifft
- Nicht-Verfügbarkeit der Daten und Dienste
- Kompromittierung der Authentisierung
- Datenverlust
- Datenmanipulation

Wichtige Aspekte der Informationssicherheit

- Überarbeitung des Sicherheitskonzeptes unter Cloud-Aspekten.
- Informations-“Assets“: Analyse, Qualifizierung, Handhabung.
- Ergebnisse von Risikobetrachtungen nicht ignorieren und in Prozesse und Richtlinien integrieren.
- Prüfung technischer Möglichkeiten zur Umsetzung/Einhaltung von Richtlinien.
- Schulung der Mitarbeiter.

Vielen Dank …

… für Ihre Aufmerksamkeit!

Noch Fragen?