Cloud Computing / SaaS: Verträge datenschutzkonform und rechtssicher gestalten

Rechtsanwalt Dr. Thomas Helbing

www.thomashelbing.com
helbing@thomashelbing.com
(0 89) 39 29 70 07

Inhalt

- Datenschutzrechtliche Grundlagen
- Fallstudie 1: EU-Clouds
- Fallstudie 2: Internationale-Clouds
- Fazit

Datenschutzrechtliche Grundlagen

Geltung des Datenschutzrechts

- Anwendungsbereich
  - Personenbezogene Daten
  - Erhebung, Verarbeitung und Nutzung
- Vorschriften
  - EU-Datenschutzrichtlinie 95/46/EU
  - Sitz der verantwortlichen Stelle
  - Bundesdatenschutzgesetz, Telemediengesetz, Telekommunikationsgesetz

Zwei-Stufen-Prüfung

- 1. Stufe: Erlaubnisnorm
  - Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur mit Einwilligung oder Erlaubnisnorm
  - Interessenabwägungsklausel
  - Sonderregelung bei Beschäftigtendaten
- 2. Stufe: Angemessenes Datenschutzniveau
  - Nur bei Übermittlung in „Drittland" relevant
  - EU-Standardvertragsklauseln
  - Safe Harbor (USA)
  - Binding Corporate Rules (Gruppenintern)

Schaubild Zwei-Stufen-Prüfung

Datenübermittler (EU)

Erste Stufe Datenübermittlung

Zweite Stufe Datenschutzniveau

Datenempfänger (Drittland)

Auftragsdatenverarbeitung

Auftragsdatenverarbeitung (controller-processor)

- Verarbeitung nach Weisungen und im Auftrag
- Keine „Übermittlung" innerhalb EU (Erste Stufe entfällt insoweit)
- Schriftlicher Vertrag nach § 11 BDSG erforderlich

Funktionsübertragung (controller-controller)

- Verarbeitung zu eigenen Zwecken / eigene Entscheidungsbefugnis
- „Übermittlung" bedarf einer Erlaubnisnorm

Fallstudie 1

EU-Clouds

Sachverhalt

- Der Mittelständler K will für verschiedene HR-Funktionen (Bewerbermanagement, Skill-Datenbank, Urlaubsplanung, Krankmeldungen, Reisemanagement, etc.) in Zukunft die Software des Anbieters A nutzen. A stellt die Software „as a Service“ zur Verfügung.
- A und K haben ihren Firmensitz in Deutschland.
- Kurz vor Vertragsschluss bittet K seinen betrieblich bestellten Datenschutzbeauftragten um „Prüfung“.

„Prüfung“

Auftragsdatenverarbeitungsvertrag

- Schriftlicher Vertrag (meist gesonderter Vertrag mit Verweis auf Service-Vertrag)
- Auftraggeber (Cloud-Nutzer) bleibt datenschutzrechtlich verantwortlich
- Auftraggeber muss Auftragnehmer (Cloud Anbieter) „sorgfältig auswählen"
- Vertrag muss inhaltlich 10-Punkte Katalog umsetzen
- Bei mangelhaften Verträgen: Bußgeld bis € 50.000,-
- Siehe auch (demnächst): „Leitfaden Cloud Computing & Datenschutz" des EuroCloud Deutschland_eco e.V.

Vertragliche Regelungen (1)

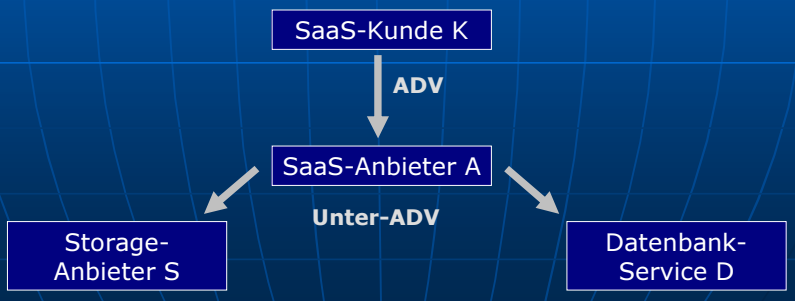
- Kontrollrechte
  - Auftraggeber muss Recht haben, selbst oder durch Dritte Datenverarbeitung zu kontrollieren, ggf. vor Ort
  - Regelung: Formale Anforderungen (Ankündigung, keine Störung des Geschäftsbetriebs), Kostentragung, Mitwirkungspflicht
- Technische und organisatorische Schutzmaßnahmen
  - Auftraggeber hat sich hiervon vor Vertragsschluss und danach regelmäßig zu überzeugen.
  - Ergebnisse sind zu dokumentieren.
  - Praktische Umsetzung: Auftragnehmer legt Sicherheitskonzept vor, Festlegung von Zertifizierungen, Testaten oder Erklärungen des Auftraggebers.
  - „BSI Mindestanforderungen an Cloud-Computing"
  - ULD:
    - Ort der Datenverarbeitung und beteiligte Unternehmen offen legen
    - Vertragliche Audits durch unabhängige Dritte vereinbaren
    - Verschiedene Modelle in Bezug auf Security Levels und Locations anbieten

Vertragliche Regelungen (2)

- Rückgabe von Daten
  - Regeln, wie Rückgabe am Ende der Vertraglaufszeit erfolgt
  - Regelungspunkte: Rückgabe und Löschung plus Bestätigung durch Auftraggeber, eigenständiger Export durch Auftragnehmer, Unterstützung bei Migration, Fristen, Format, Vergütung, Datenträger/-transfer
- Subunternehmer
  - Etwaige Berechtigung des Auftragnehmers, Subunternehmer einzuschalten ist vertraglich zu regeln
  - Regelungsmöglichkeiten: Zustimmungserfordernis, Mitteilungspflicht, Weitergabe Vertragsbedingungen, gleiches Sicherheitsniveau, unmittelbare Kontrollrechte, ggf. Differenzierung nach Lokation/Gruppenzugehörigkeit

Sachverhalt Ergänzung

- Der Anbieter A greift für den Betrieb seines „Software as a Service"-Angebots auf Cloud-Storage Dienste des Anbieters S zurück. Daneben nutzt A die Firma D zur Wartung seiner Datenbank-Server.
- S hat seinen Sitz in Irland, D sitzt in Österreich.



Auswirkungen Ergänzung

- Verhältnis A-S und A-D
  - Verträge zur Auftragsdatenverarbeitung nötig
  - Wenn D im Rahmen von Wartungsarbeiten lediglich Zugriff auf Daten hat, genügt ggf. vereinfachter ADV (§ 11 (5) BDSG)
- Verhältnis A-K
  - Einschaltung von S und B muss nach der Subunternehmer Regelung zulässig sein

Fallstudie 2

Internationale Clouds

Sachverhalt

- Der Fahrzeughersteller K möchte ein Online-basiertes System zur Verwaltung seiner Kundenbeziehungen (CRM) verwenden, das von A zur Verfügung gestellt werden soll.
- K sitzt in Deutschland, Anbieter A in den USA

Anforderungen bei Drittländern

- Erste Stufe: Erlaubnisnorm
  - Privileg des § 11 BDSG greift nicht mehr: Es liegt eine „Übermittlung" vor
  - Rechtsgrundlage: Interessenabwägung
  - ULD (unklar):
    - Kein Interesse des Cloud Nutzers?
    - Dafür: § 11 BDSG analog? „Sicherheitshalber" Anforderungen des § 11 BDSG umsetzen?
- Zweite Stufe: angemessenes Datenschutzniveau
  - Anbieter A nimmt am Safe Harbor Programm teil, oder
  - A und K schließen einen Vertrag mit den EU Standardvertragsklauseln

Safe Harbor

- Nur verfügbar für US-Gesellschaften, die der Aufsicht der FTC unterliegen
- Beachtung bestimmter allgemeiner „Safe Harbor Principles"
- Verfahren:
  - Selbstzertifizierung durch US-Gesellschaft
  - Erklärung gegenüber FTC (jährlich)
  - Öffentlichmachung
- Bedenken Deutscher Aufsichtsbehörden:
  - Beschluss des "Düsseldorfer Kreises" vom 29. April 2010
  - Auftraggeber muss sich Zertifizierung und Beachtung der Safe Harbor Principles nachweisen lassen, darf sich nicht auf Behauptung des Anbieters verlassen.
  - Mindestprüfung: Aktuelle Zertifizierung, Umsetzung des „Notice" Principles (sofern anwendbar)

EU Standardvertragsklauseln

- Von der EU Kommission festgelegter Standardvertrag für den Umgang mit personenbezogenen Daten
  - Im Anhang sind Angaben zu Daten, Verarbeitungszwecken und Datensicherheit zu ergänzen
  - Ansonsten keine inhaltliche Änderung zulässig
  - Ggf. um Anforderungen nach § 11 BDSG zu ergänzen
- Neue Fassung vom 15. Mai 2010 für „controller processor" Transfers
- Schwierigkeiten: Ausländisches Unternehmen unterwirft sich EU-Recht und -Aufsicht

1. Ergänzung Sachverhalt

- Einzelne Ergänzungsmodule (Newsletterversand) des von K genutzten CRM werden nicht von A selbst betrieben, sondern von dem US Software-Unternehmen E.

Subunternehmer bei Drittländern

- Bei EU Standardvertrag (Clause 11)
  - Voraussetzungen:
    - Einwilligung K (Generaleinwilligung mgl.), und
    - Weitergabe Vertragsbedingungen (Mitunterzeichnen möglich, aber bedenklich)
  - Folgen:
    - A muss Liste aller Subunternehmer führen
    - A muss K Verträge mit Subunternehmern zur Verfügung stellen
    - A steht für die Datenverarbeitung durch E gegenüber K ein
- Bei Safe Harbor: Onward-Transfer Principle
  - Voraussetzungen bei Unterauftragsdatenverarbeitern:
    - E befindet sich in einem Land mit „angemessenem Datenschutzniveau" (z.B. EU) , oder
    - E ist selbst Safe Harbor zertifiziert, oder
    - E verpflichtet sich gegenüber A schriftlich zur Beachtung der Safe Harbor Principles

2. Ergänzung Sachverhalt

- Der Betrieb des Online-CRM erfolgt durch verschiedene Rechenzentren weltweit, die von lokalen Tochtergesellschaften von A betrieben werden.

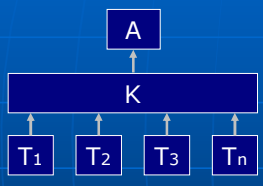
Binding Corporate Rules

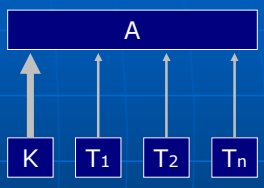
- A legt sich und Tochterunternehmen rechtsverbindliche Regelungen für den Umgang mit personenbezogenen Daten auf
- Innerhalb der Unternehmensgruppe herrscht dann ein angemessenes „Datenschutzniveau" (Safe Haven)
- Anforderungen
  - Inhaltliche Umsetzung der Vorgaben der EU Kommission
  - Rechtsverbindlich nach innen und außen
  - Zustimmung der EU Datenschutzbehörden (teilweise „mutual recognition")

3. Ergänzung Sachverhalt

- Der Fahrzeughersteller K ist ein internationaler Konzern. Die Konzernmutter sitzt in Hamburg. Der Verkauf der Fahrzeuge erfolgt durch die lokalen Tochtergesellschaften T in und außerhalb der EU.
- Einzelne Regionen werden zentral durch eine Tochtergesellschaft bedient (z.B. Osteuropa durch die Österreichische Tochter).
- Alle Töchter sollen das CRM von A nutzen

Vertragspartner Konzern





Ein Vertrag A-K
Konzerninterne Verträge K-T

Rahmenvertrag A-K
Individualverträge A-T

Fazit

Fazit

- Datenschutz ernst nehmen!
- EU-Clouds: § 11 BDSG umsetzen
- Internationale-Clouds: Zusätzlich EU Standardvertragsklauseln
- Subunternehmer nicht vergessen (auch im Konzern)