SKW
Schwarz
Rechtsanwälte

Rechtssicher in die Cloud

Aktuelle Lösungsansätze für rechtskonforme Cloud Services

RA Jan Schneider
Fachanwalt für Informationstechnologierecht

Cloud Conf 2011, München den 21. November 2011

„Ist Cloud Computing nicht …

… unsicher?“

… ein Kontrollverlust?“

…eine unerlaubte Datenübermittlung?“

… rechtlich problematisch?“

… datenschutzwidrig?“

Herausforderung:

Rechtskonforme Datenübermittlung

SKW
Schwarz
Rechtsanwälte

Bei der Nutzung von Cloud Services werden häufig

personenbezogene Daten übertragen.

SKW
Schwarz
Rechtsanwälte

Bei der Nutzung von Cloud Services werden häufig

personenbezogene Daten übertragen.

*„Angaben, anhand derer **natürliche Personen** bestimmbar sind“*

SKW
Schwarz
Rechtsanwälte

Bei der Nutzung von Cloud Services werden häufig

personenbezogene Daten übertragen.

*„Angaben, anhand derer **natürliche***
***Personen** bestimmbar sind“*

z. B. Name, Anschrift - auch E-Mail-Anschrift -, Alter,
Geschlecht, Beruf, Konfession, aber ggf. auch Fotos -

SKW
Schwarz
Rechtsanwälte

Herausforderung Datenübermittlung

- (auch) personenbezogene Daten sollen in die Cloud?

- Nein: → keine datenschutzrechtlichen Anforderungen! Z. B. bei
  - Anonymisierung der Daten
  - Verschlüsselung der Daten

SKW
Schwarz
Rechtsanwälte

Herausforderung Datenübermittlung

- (auch) personenbezogene Daten sollen in die Cloud?
- Ja:
  - → **Datenschutzgesetze** finden Anwendung (TMG, BDSG, LandesDSG)
  - → **Grundsatz:** Datenübermittlung ist nur dann zulässig, wenn hierzu ausdrückliche gesetzliche Ermächtigungsgrundlage auffindbar ist
  - → **zentrale Herausforderung:** Sicherstellung der datenschutzrechtlichen Zulässigkeit der Datenübermittlung

SKW
Schwarz
Rechtsanwälte

Lösungsansatz: Auftragsdatenverarbeitung („ADV“)

- ADV ist gesetzliches „Konstrukt“, beschrieben in § 11 BDSG
- **vertragliche Gestaltung** erforderlich – schriftlich und ausführlich!
- **Regelungskatalog** des § 11 BDSG!
- Einrichtung **technischer und organisatorischer Maßnahmen** durch den Cloud Service Provider („CSP“), § 9 BDSG
- **Prüfung** der Maßnahmen durch den Cloud Nutzer

Lösungsansatz: Auftragsdatenverarbeitung („ADV“)

- Konsequenz einer rechtmäßigen ADV:

Nutzer bleibt per Gesetz „**Herr seiner Daten**“

Ein „sicherer Hafen“?

Serverfarmen in Übersee

Ein sicherer Hafen? Serverfarmen in Übersee

Herausforderung:

Datenübermittlung an Server **außerhalb der EU** zulässig?

SKW
Schwarz
Rechtsanwälte

Ein sicherer Hafen? Serverfarmen in Übersee

<u>Diskussion der Datenschutzexperten:</u>

Kann eine Datenübermittlung nach „Übersee“
zulässige „Auftragsdatenverarbeitung“ (oder anderweit gesetzlich legitimiert) sein?

Ein sicherer Hafen? Serverfarmen in Übersee

Möglicher <u>Lösungsansatz</u> für die USA:

„Safe Harbor“ - Abkommen

SKW
Schwarz
Rechtsanwälte

Was ist „Safe Harbor“?

- Abkommen zwischen EU-Kommission und US-Regierung aus dem Jahre 2000
- Festlegung bestimmter datenschutzrechtlicher Maßnahmen
- Anerkennung der Maßnahmen durch die Unternehmen, die sich verbindlich zu den Grundsätzen des Safe Harbor bekennen („Selbstverpflichtung“)
- „Safe Harbor“ führt zu **angemessenem Datenschutzniveau**

the Directive if they include the Principles in written agreements with parties transferring data from the EU for the substantive privacy provisions, once the other provisions for such model contracts are authorized by the Commission and the Member States.

U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbor organizations, except where organizations have committed to cooperate with European Data Protection Authorities. Unless otherwise stated, all provisions of the Safe Harbor Principles and Frequently Asked Questions apply where they are relevant.

"Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form.

NOTICE: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

ONWARD TRANSFER: To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

SECURITY: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

„Safe Harbor“ noch zeitgemäß?

- Beschluss des „**Düsseldorfer Kreises**“ vom 28.04.2010; Festlegungen für Cloud Computing:
  - **Inhalt:**
    - **Prüfung des Nachweises** über Beitritt zu „Safe Harbor“
    - **Nachweis über die Einhaltung** der Informationspflichten nach Safe Harbor durch den Cloud Service Provider
  - Festlegungen entfalten keine unmittelbare Rechtswirkung, gleichwohl beachtlich
  - Festlegungen sind in der Diskussion

Checkliste

- Ist der CSP beim Safe Harbor-Programm des US-Handelsministeriums **registriert**?
- **Gewährleistet** der CSP ausdrücklich die Einhaltung der Safe Harbor-Prinzipien?
- Erfolgt ein **Nachweis** über die Einhaltung von „Safe Harbor“, z. B. durch Zertifikate (ggf. SSAE 16, ISAE 3402 u. SAS 70 Type II)?

Ausblick

- „Safe Harbor“ hat nach Potential
- Alternative zu EU-Standardvertragsklauseln (+ ergänzende Regelungen)

Projekt

Datensicherheit!

SKW
Schwarz
Rechtsanwälte

Projekt Datensicherheit!

- **<u>Herausforderungen</u>**:
  - Etablierung der **technischen und organisatorischen Maßnahmen** zum Datenschutz (§ 9 BDSG)
  - optimale **IT-Sicherheit** herstellen

Projekt Datensicherheit!

- **<u>Lösung</u>:**
  - moderne Rechenzentren der großen CSP‘s
  - Dokumentation der Maßnahmen in **“Datensicherheitskonzepten“**

    → Notwendiger Bestandteil der vertraglichen Vereinbarungen!

Projekt Datensicherheit!

- „**Checkliste**“:
  - Modernes Hochsicherheits-Rechenzentrum?
  - Standort des Rechenzentrums?
  - Ausführliche, verbindliche und belastbare **Beschreibung** der vom CSP getroffenen technischen und organisatorischen Maßnahmen?

Showstopper

Patriot Act?

SKW Schwarz Rechtsanwälte

Showstopper Patriot-Act?

USA PATRIOT Act

*„**U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism **Act**“*

US-amerikanisches **Bundesgesetz**,
verabschiedet am 25. Oktober 2001

SKW
Schwarz
Rechtsanwälte

Showstopper Patriot-Act?

- Patriot Act erlaubt den US-Behörden unter bestimmten Voraussetzungen einen Zugriff auf Unternehmensdaten
- Alle US-Unternehmen unterliegen dem Patriot Act
- (Cloud-) Kunden werden über die Datenherausgabe ggf. nicht informiert.

Überlegungen zum Patriot Act

- Regierungen verfügen in aller Regel über „Möglichkeiten“, Zugriff auf Daten und Informationen zu erlangen
- Anwendungsbereich des PA ist **eng** → Bekämpfung des Terrorismus
- Anwendung des PA dürfte eher **selten** bleiben

SKW
Schwarz
Rechtsanwälte

Überlegungen zum Patriot Act

- Maßnahmen d. PA seit Mai 2011 **gerichtlich überprüfbar** → vertragliche Handlungspflicht aufnehmen?
- „Gegenmittel“ ggf.: **Verschlüsselung** der Daten?
- „Gegenmittel“ ggf.: Vertragsschluss mit EU-Tochter?
- „Sicherheit“ durch **vertragliches Herausgabeverbot**?

Odyssee in die Cloud?

Prüfung der Maßnahmen zum Datenschutz

Eine Odyssee in die Cloud? - Prüfung der Maßnahmen

<u>Herausforderung</u>:

Prüfung der Einhaltung der **technischen und organisatorischen Maßnahmen** durch den Cloud Nutzer (§ 11 BDSG)

Eine Odyssee in die Cloud?

Schwierigkeit:

Prüfung vor Ort beim CSP durch den Cloud Nutzer häufig **nicht praktikabel**

Eine Odyssee in die Cloud?

- **<u>Lösungsansatz</u>**:

§ 11 BDSG schreibt **keine Prüfung vor Ort** durch den Nutzer vor.

SKW
Schwarz
Rechtsanwälte

Checkliste

- **Testate** bzw. **Auditierung** durch unabhängige Stellen - z. B. Wirtschaftsprüfer?

- **Zertifizierung** des CSP? Z. B. nach **ISO 27001**, SSAE 16, ISAE 3402 u. SAS 70 Type II,

- Sonstige **Nachweise**?

Fazit und Ausblick

- Cloud Computing hat **Potential**!

- Die rechtlichen Herausforderungen sind **lösbar** – mit einem konstruktiven und praxisnahen Ansatz.

- Datenschutzrechtler und -behörden, anwaltliche Berater, Rechtsprechung und Gesetzgeber sind gemeinsam aufgerufen, **praxisnahe Lösungen** zu erarbeiten

SKW
Schwarz
Rechtsanwälte

Bei Fragen oder Anmerkungen:

Jan Schneider
Rechtsanwalt
Fachanwalt für IT-Recht
SKW Schwarz Rechtsanwälte
40212 Düsseldorf
Steinstraße 1 / KÖ
T +49 (0)211 82 89 59 – 0
j.schneider@skwschwarz.de
www.skwschwarz.de

Herzlichen Dank für Ihre Aufmerksamkeit!