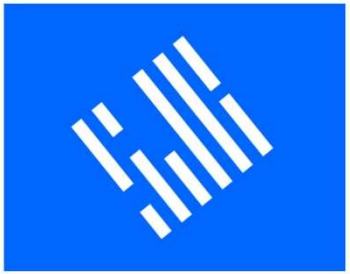
SJ Berwin LLP



Aktuelle Entwicklungen im Datenschutzrecht

eco Kompetenzgruppe e-commerce

Das Telemediengesetz und die Haftung von Plattformbetreibern

Frankfurt am Main, 13. März 2012

Manuela Finger, LL.M.
SJ Berwin LLP, Frankfurt am Main

Überblick

Aktuelle Entwicklungen im Datenschutzrecht

- TMG-Novelle
- EU-Datenschutzverordnung

Besondere Problembereiche

- Aktuelles zu Cookies
- Cloud Computing

TMG-Novelle

Entwurf zur Änderung des Telemediengesetzes

- Juni 2011: Gesetzentwurf des Bundesrats zur Änderung des TMG
- Probleme: mangelnde Transparenz, mangelnde Aufklärung, „Das Internet vergisst nichts“
- Ziele: Verbesserung des Datenschutzes im Internet, u.a. in sozialen Netzwerken
- Mittel: Verschärfung der Informationspflichten aller Dienstanbieter, besondere Pflichten für Anbieter von nutzergenerierten Inhalten, erleichterte Möglichkeit zur Datenlöschung durch Nutzer
- Stellungnahme der Bunderegierung vom 3. August 2011 weitaus zurückhaltender

Die wichtigsten Änderungen (1)

- Erweiterte allgemeine Informationspflichten, § 13 Abs. 1 S. 1 TMG-E

  → Datenschutzhinweise in allgemein verständlicher Form, leicht erkennbar, unmittelbar erreichbar

- Löschknopf und Löschroutine, § 13 Abs. 4 S. 1 Nr. 3 und 4 TMG-E

  → Löschknopf leicht erkennbar, unmittelbar erreichbar, ständig verfügbar

  → Löschroutine mit Ablauf des Jahres, das dem Jahr der letzten Nutzung folgt

Die wichtigsten Änderungen (2)

- Zusätzliche Pflichten der Anbieter von Telemediendiensten mit nutzergenerierten Inhalten, § 13a TMG-E

  → Sicherheitseinstellungen – Privacy by default (höchste Sicherheitsstufe nach Stand der Technik) und korrespondierende Unterrichtungspflicht

  → Auffindbarkeit/Auslesbarkeit durch Suchmaschinen

  → Aufklärungspflichten über Risiken, die mit der Preisgabe personenbezogener Daten verbunden sind

  →Löschung/Anonymisierung nutzergenerierter Inhalte

- Ordnungswidrigkeiten: Verstöße gegen die neuen Unterrichtungspflichten, Verpflichtung zum Bereithalten der Löschfunktion und Löschroutine sowie Verpflichtung in Bezug auf Sicherheitseinstellungen

TMG-Novelle

Nicht zu vergessen…

Die „Cookie-Regelung“ des § 13 Abs. 8 TMG-E

→ Erfasst jede Speicherung von Daten im Endgerät des Nutzers und jede Form von Endgeräten

→ Verstoß begründet keine Ordnungswidrigkeit

TMG-Novelle

Kritik

- Regelungen zur erhöhten Transparenz und Löschung von Nutzerkonten zwar begrüßenswert, aber…
- Keine klaren Handlungsanweisungen in Bezug auf Cookies
- Verbesserter Schutz in sozialen Netzwerken auf nationaler Ebene kaum erreichbar, Problem insbesondere bei Diensteanbietern in anderen Mitgliedstaaten oder im EU/EWG-Ausland
- Risiko der Benachteiligung inländischer Anbieter
- **Fazit:** Ein hinreichendes Schutzniveau könnte besser durch eine EU-weite Lösung hergestellt werden

EU-Datenschutzverordnung

Geplante EU-Datenschutzverordnung

- **Januar 2012: Veröffentlichung des Vorschlags zur umfassenden Reform der von 1995 stammenden EU-Datenschutzregelungen**
- **<u>Ziel</u>: Modernisierung und Anpassung an die technologische Entwicklung und zunehmende Globalisierung**
- **<u>Insbesondere</u>: Stärkung der Persönlichkeitsrechte und des EU-Binnenmarkts**
- **Daneben Gewährleistung hohen Datenschutzniveaus durch polizeiliche und strafrechtliche Zusammenarbeit, ordnungsgemäße Durchsetzung der Vorschriften und globale Datenschutzstandards**
- **Verordnung statt Richtlinie → einheitlicher Rechtsrahmen in Europa**

EU-Datenschutzverordnung

Wichtige Änderungen (1)

- Deutlich erweiterter Anwendungsbereich auch auf Unternehmen außerhalb der EU, Art. 3 (2)
- Grundsätzlich ausdrückliche Einwilligung erforderlich, Art. 4 (8)
- Schutz von Minderjährigen unter 13 Jahren, Art. 8
- Stärkere Kontrollmöglichkeiten des Einzelnen
  - Right to be Forgotten, Löschpflichten, Art. 17
  - Privacy by design and by default, Art. 23
  - Recht auf Datenübertragbarkeit, Art. 18

EU-Datenschutzverordnung

Wichtige Änderungen (2)

- **Erweiterte Pflichten für Unternehmen**
  - **Transparenzpflichten, Art. 11**
  - **Informationspflichten, Art. 14**
  - **Unbeschränkte Auskunftsansprüche, Art. 15**
  - **Dokumentationspflichten, Art. 28**
  - **Informationspflicht bei Datenpannen gegenüber Aufsichtsbehörden und Betroffenen, Art. 31, 32**
- **Detaillierte Regelungen zu Datentransfer und Auftragsverarbeitung, Art. 40 ff.**

EU-Datenschutzverordnung

Wichtige Änderungen (3)

- **Verschärfte Sanktionen, bis zu 2% des weltweiten Jahresumsatzes**
- **One Stop Shop bei mehreren Niederlassungen in der EU, Art. 51**
- **Öffnungsklausel für Beschäftigtendatenschutz, Art. 82**

EU-Datenschutzverordnung

Ausblick

- **In Deutschland überwiegend positive Resonanz**
- **Insbesondere Sicherstellung eines angemessenen Datenschutzniveaus bei Social-Media Websites möglich**
- **Weitere Beratung durch Europaparlament und Rat der Europäischen Union**

Das „Cookie-Problem“

SJ Berwin LLP

Das „Cookie-Problem“

Ausgangslage

- Cookies = kurzer Eintrag in einer kleinen Datenbank oder Dateiverzeichnis, dient dem Austausch von Informationen oder der Archivierung von Informationen
- Gezielte Werbeansprache möglich (Online Behavioral Advertising)
- Art. 5 Nr. 3 E-Privacy-Richtlinie beschränkt Einsatz von Cookies
  - Gebrauch von Cookies von der vorherigen Einwilligung des Nutzers abhängig
  - Umsetzungsfrist E-Privacy-RL: 25. Mai 2011

Das „Cookie-Problem“

Lösung durch § 13 Abs. 8 TMG-E? NEIN!

- Wegen des Fristablaufs wurde lediglich die RL-Vorgabe beinahe wortlautgetreu abgeschrieben
- Offene Fragen:
  - Wann ist Einwilligung erforderlich?
  - Wie muss die Einwilligung eingeholt werden?
- Norm so nicht praxistauglich

Das „Cookie-Problem“

Praxishinweise Art. 29-Datenschutzgruppe (1)

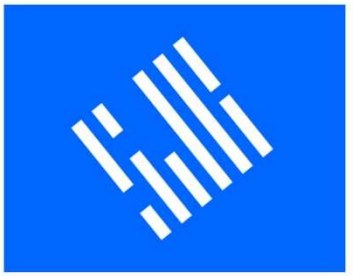
- Art. 29-Datenschutzgruppe = unabhängiges Beratungsgremium der EU-Kommission in Fragen des Datenschutzes
- Art. 5 E-Privacy-RL: erfasst Datenspeicherungen unabhängig von Personenbezug, regelmäßig wird aber eindeutige Kennung verarbeitet
- Ausnahmen vom Einwilligungserfordernis:
  - Sichere Session Cookies
  - Cookies zur Speicherung eines virtuellen Einkaufswagens
  - Security Cookies (z.B. Protokollierung fehlgeschlagener Logins)

Das „Cookie-Problem“

Praxishinweise Art. 29-Datenschutzgruppe (2)

- Einwilligung erfordert nicht zwingend ein Pop-Up-Fenster
  → nutzerfreundlichere Möglichkeiten:
  - Statische Informationsbanner an prominenter Stelle
  - Vorschalten eines Startbildschirms (Splash-Screen)
  - Standardvoreinstellung, die Datenübertragung erst nach Anklicken eines Einwilligungsbuttons erlaubt (Heise 2-Click für Facebook)
  - Standardvoreinstellung „Do not track“ im Browser
- Oftmals keine mehrfache Einwilligung erforderlich (z.B. wenn verschiedene Anbieter mit dem gleichen Werbenetzwerk zusammenarbeiten)

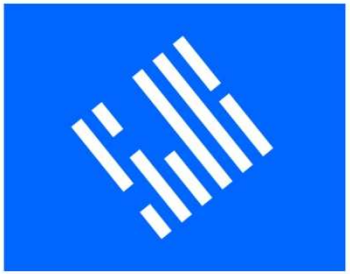
Cloud Computing



Wesen und Funktionsweise

- Cloud-Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netzwerk
- Begriffe: IaaS, PaaS, SaaS
- Public Cloud, Private Cloud, Community Cloud, Hybrid Cloud
- Server können einem bestimmten Anbieter gehören, aber auch unterschiedlichen Anbietern → Datenverarbeitung ggfls. über weltweit verteilte Server
- Benötigt ein Kunde Speicherplatz, können Server in Berlin, China und den U.S.A. gleichzeitig oder nacheinander Kapazitäten bieten

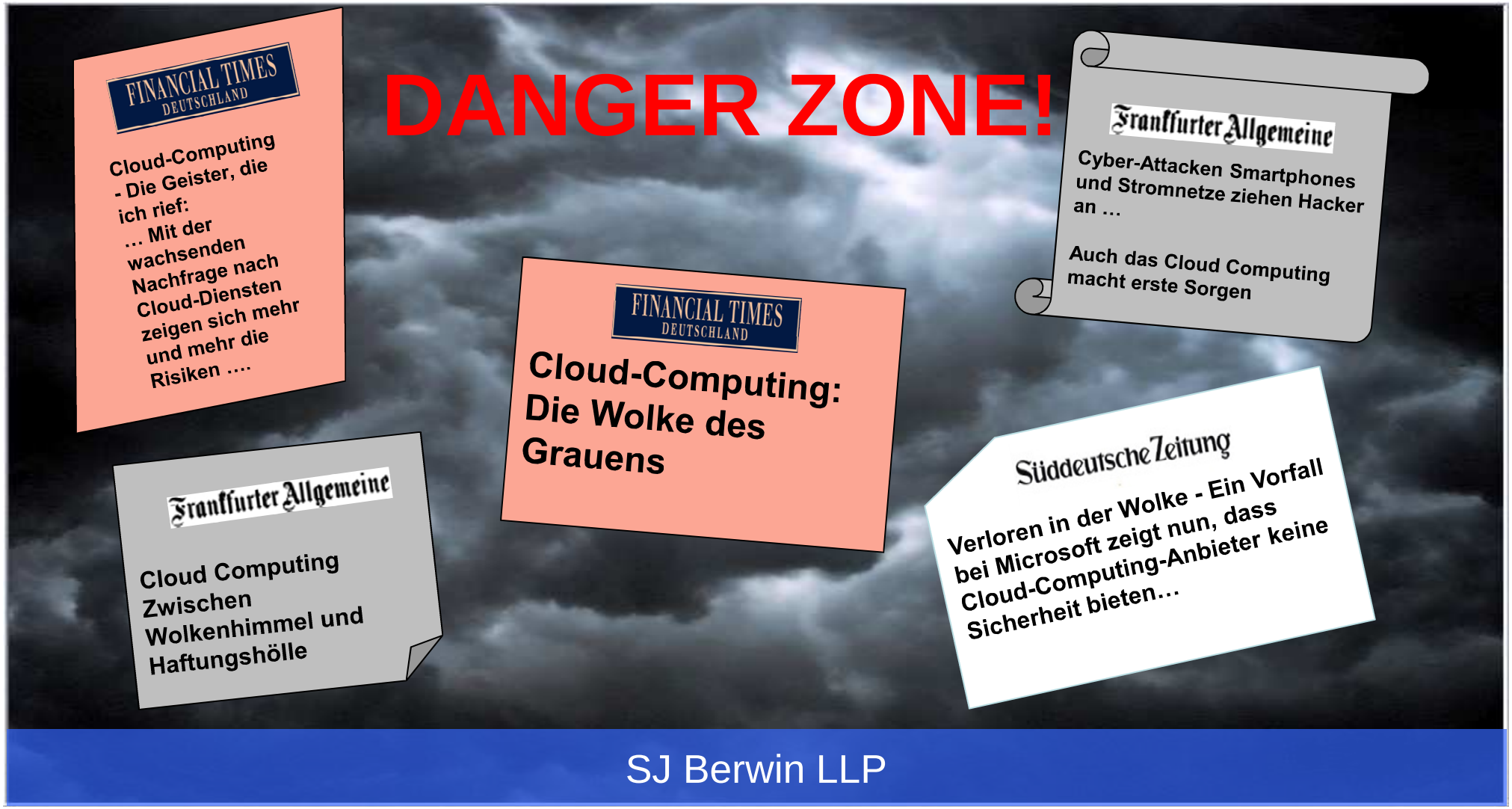
Cloud Computing



Vorteile des Cloud-Computing

- Flexibilität bei Buchung, Nutzung und Stilllegung von Rechenkapazitäten nach Bedarf (Skalierbarkeit)
- Einfacher Erwerb, verbrauchsabhängige Bezahlung
- Betriebsrisiko für Software und Anwendungen auf Dritte ausgelagert, Einsparpotential bei Anschaffung, Betrieb und Wartung von IT-Systemen
- Ubiquitäre Verfügbarkeit

Cloud-Computing



SJ Berwin LLP

Cloud-Computing

Gefahren und Risiken

- Cloud-Anwender bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich, **§ 11 Abs. 1 BDSG**
- Kein direkter Zugriff auf Infrastruktur → Datenschutzrechtliche Pflichten nur schwer zu erfüllen
- Problem insbesondere bei Auslagerung auf Server außerhalb der EU/EWR

Cloud-Computing

Sicheres Cloud-Computing

- **Sorgfältige Auswahl und Kontrolle des Anbieters**

  →Transparente Information des Anbieters, ggf. Zertifizierung oder Gütesiegel

- **Schriftlicher Vertrag über Auftragsdatenverarbeitung, insbesondere**
  - **Umfang, Art, Zweck, Ort der vorgesehenen Datenverarbeitung, Art der Daten und Kreis der Betroffenen**
  - **Technisch-organisatorische Maßnahmen**
  - **Kontrollrechte des Nutzers**
  - **Rückgabe von Daten**
  - **Einschaltung von Subunternehmern**

Cloud Computing

Grenzüberschreitender Datenverkehr

- grenzüberschreitender Datenverkehr liegt auch vor, wenn ausländische Ressourcen oder ausländische Subunternehmer eingesetzt werden
- innerhalb der EU/des EWR unproblematisch aufgrund weitgehend harmonisierten Datenschutzniveaus
  - ➔ Verpflichtung, dass nur technische Infrastrukturen verwendet werden, die sich physikalisch auf dem Gebiet des EWR befinden
- Problem: Cloud mit Bezug außerhalb der EU/des EWR
- Drittstaatentransfer erfordert nach § § 4b, 4c BDSG Garantien zur Einhaltung eines angemessenen Datenschutzniveaus und Zulässigkeit der Übermittlung

Cloud Computing

Grenzüberschreitender Datenverkehr

1. Drittstaat mit angemessenem Datenschutzniveau: Schweiz, Kanada (teilweise), Argentinien, Guernsey, Isle of Man
2. EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern
   - **Klauseln müssen unverändert übernommen werden!**
   - Nach Auffassung deutscher Datenschutzbehörden Ergänzung um Vorgaben des § 11 Abs. 2 BDSG erforderlich
3. USA: Safe Harbor (Selbstzertifizierung), zusätzlich Auftragsverarbeitungsvertrag erforderlich
4. Verbindliche Unternehmensregelungen (Binding Corporate Rules)

Cloud Computing

Grenzüberschreitender Datenverkehr außerhalb EU/EWR

Insbesondere: USA

USA Patriot Act erlaubt amerikanischen Behörden unter bestimmten Voraussetzungen Einsicht in Daten, die in der Cloud gespeichert sind

Cloud Computing

Datenschutzkonforme Lösungen

- Vollständige Verschlüsselung von Daten, so dass nur Cloud-Nutzer Daten entschlüsseln kann?
  - ➔ Anonymisierung
  - aber: nicht für jede Art von Geschäftsprozess geeignet
- Private Cloud?
  - ➔ Anwender kann Rahmenbedingungen genau festlegen und Anforderungen nach § 11 BDSG erfüllen
  - aber: Kostenvorteile schwinden wegen Mehraufwand
- EU/EWR-Cloud?

Manuela Finger
Senior Associate
IP/IT, Frankfurt

Manuela Finger ist Anwältin im Frankfurter Büro von SJ Berwin und Mitglied der Praxisgruppe IP/IT/Commercial.

Frau Finger berät deutsche und internationale Mandanten auf allen Gebieten des gewerblichen Rechtsschutzes und der Informationstechnologie, unter anderem im Marken-, Geschmacksmuster-, Urheber- und Wettbewerbsrecht. Sie berät zudem im Lizenzvertragsrecht und Vertriebsrecht. Ein Schwerpunkt ihrer Tätigkeit liegt im Bereich der neuen Medien, einschließlich der Beratung zu allen Aspekten des E-Commerce, der interaktiven Unterhaltung, Onlinemedien, Broadcasting, Jugendschutz und Datenschutzrecht. Ihre Tätigkeit umfasst sowohl die Beratung als auch die Prozessführung.

Frau Finger studierte Rechtswissenschaften an der Universität Konstanz. Nach ihrem zweiten Staatsexamen im Jahr 2000 in Stuttgart war sie als wissenschaftliche Mitarbeiterin am Lehrstuhl von Prof. Dr. Karl-Heinz Fezer insbesondere im gewerblichen Rechtsschutz tätig. 2005 absolvierte sie den Studiengang „Master of Laws in European Intellectual Property Law“ (LL.M.) an der Universität Stockholm. Vor ihrem Beitritt zu SJ Berwin im Jahr 2007 arbeitete Frau Finger im Frankfurter Büro von Freshfields Bruckhaus Deringer.

Manuela Finger ist Mitglied in der deutschen Vereinigung für gewerblichen Rechtsschutz und Urheberrecht e.V. Sie publiziert regelmäßig zu Themen im Bereich des geistigen Eigentums und der neuen Medien.

Vielen Dank

für Ihre Aufmerksamkeit!

Manuela Finger
Senior Associate
IP/IT
Frankfurt
Tel.: + 49 (0)69 50 50 32 113
manuela.finger@sjberwin.com