IHDE & PARTNER
RECHTSANWÄLTE

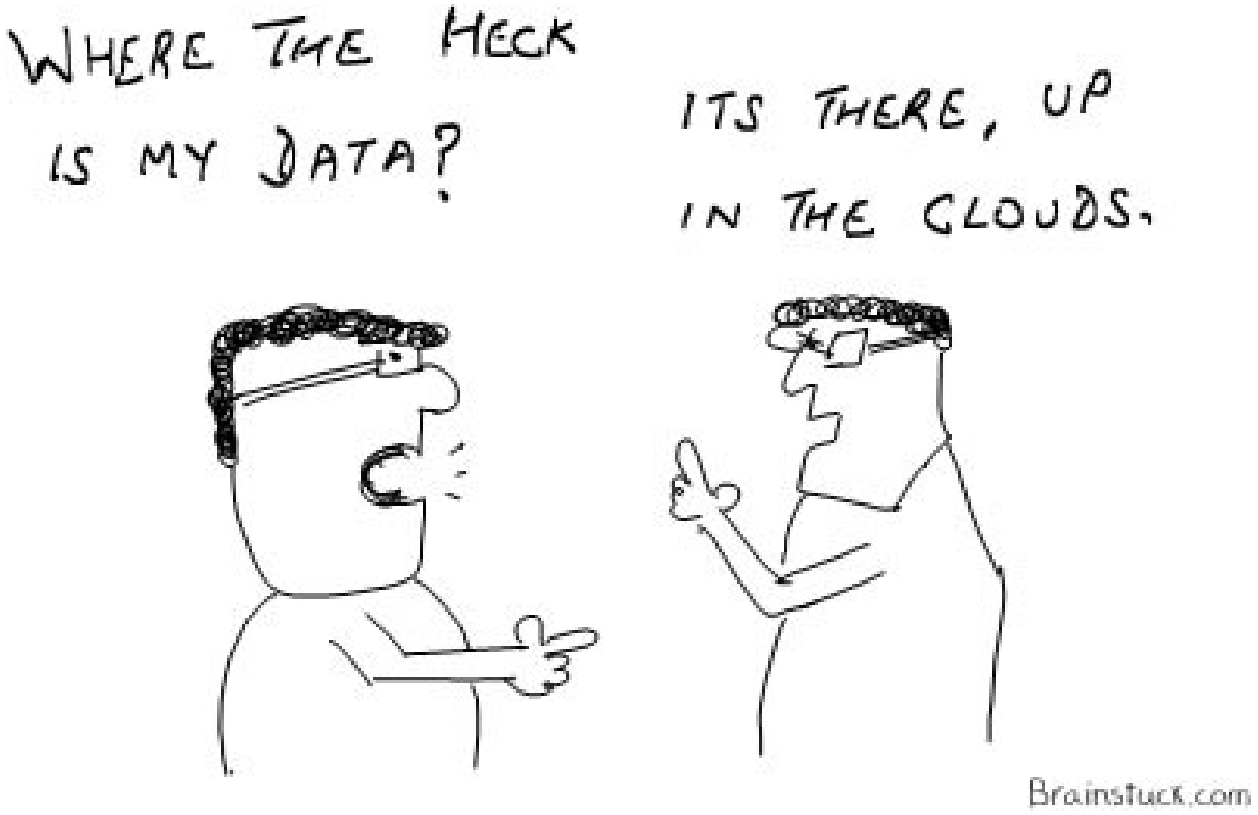
Cloud Computing & Datenschutz

Fabian Laucken

Fachanwalt für Informationstechnologierecht und
Fachanwalt für Gewerblichen Rechtsschutz

www.ihde.de

Handlungsfeldkonferenz „Internet der Dienste“



Mit freundlicher Genehmigung von Brainstuck.com - Anshul Maheshwari

Pressespiegel:

Computer

„Datenkraken“-Preise für die Cloud und Innenminister

Wegen eklatanter Mängel beim Datenschutz hat der Verein Foebud seine diesjährigen Negativpreise verliehen, die „BigBrotherAwards“. Unter den sieben „Preisträgern“ sind diesmal zwei Innenminister, zwei Softwarefirmen und das sogenannte Cloud Computing.

werde damit eklatant verletzt, hieß es in der Begründung. „Wer Adressbücher und Fotos oder Archive, Vertriebsinfos und Firmeninterna unverschlüsselt in den undurchsichtigen Nebel der Cloud verlagert, handelt mindestens fahrlässig“, meinte die Jury.

Quelle: www.focus.de 14.04.2012

DEUTSCHE VERUNSICHERT

Wie sicher sind meine Daten in der „Cloud“?

Eine Studie enthüllt: Fast 80 Prozent der Deutschen machen sich Sorgen um ihre Online-Daten. BILD.de zeigt, wie sicher Daten in der

Quelle: www.bild.de 37.07.2012

CLOUD-SPEICHERDIENSTE

Sicherheitsprobleme bei Dropbox und Konkurrenten

Fraunhofer-Forscher haben Speicherdienste wie Dropbox und Cloudme getestet. Fazit: Keiner ist wirklich sicher, teils können Kundendaten mit Suchmaschinen gefunden werden.

Quelle: www.zeit.de 15.05.2012

Auffassung der Aufsichtsbehörden

- Cloud Computing ist (generell) datenschutzrechtlich unzulässig
- 26.9.2011: Orientierungshilfe Cloud Computing (Arbeitskreis Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder)
- 28./29.9.2011: Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Datenschutzkonforme Gestaltung und Nutzung von Cloud Computing
- 1.7.2012: Stellungnahme der Artikel 29 Gruppe zum Cloud Computing
- 13.7.2012: Pressemitteilung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein: „ULD: Datenschutzkonformes Cloud Computing ist möglich“

Volkszählungsurteil des BVerfG von 1983

- Aus der Menschenwürde und dem Recht auf freie Entfaltung der Persönlichkeit folgt das „*Recht auf informationelle Selbstbestimmung*“
- *„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. (…) Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. (…) Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein “belangloses” Datum mehr.*“

Bundesdatenschutzgesetz

- Schutzgegenstand sind personenbezogene Daten
- Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. (§ 3 Abs. 1 BDSG), z.B. Kundendaten, Daten von Mitarbeitern etc.
- Verbot mit Erlaubnisvorbehalt: Die Erhebung und Verwendung personenbezogener Daten ist grundsätzlich verboten, soweit kein Erlaubnistatbestand greift
- Datensicherung (Schutz vor Verlust, Sabotage, unbefugtem Zugriff)
- Grundsatz der Datensparsamkeit, Zweckbindung, Erforderlichkeit

Dürfen personenbezogene Daten beim Cloud Computing-Anbieter gespeichert und dort verarbeitet werden?

- Ausgangspunkt: Es handelt sich zunächst um eine Übermittlung von Daten, da Daten an einen *Dritten* weitergegeben werden.
- Übermittlung ist nur zulässig mit (1.) Einwilligung des Betroffenen (§ 4a BDSG) oder wenn (2.) die Übermittlung „zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme, dass schutzwürdiges Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt“ (§ 28 Abs. 1 Nr. 2 BDSG).
- Reine Kostenersparnis beim Cloud-Computing-Kunden reicht in der Regel nicht aus.

„Ausweg“ - Auftragsdatenverarbeitung

- Stellen, die personenbezogene Daten „im Auftrag“ erheben, verarbeiten oder nutzen, gelten nicht als „Dritte“ (§ 3 Abs. 8 S. 2 BDSG)
- Also dann: keine „Übermittlung“ personenbezogener Daten „an Dritte“ im Sinne des Datenschutzrechts
- Der Auftraggeber wird weiter als verantwortlicher „Herr der Daten“ angesehen. Er ist und bleibt verantwortlich (§ 11 Abs. 1 BDSG).

Voraussetzungen für eine rechtmäßige Auftragsdatenverarbeitung:

Eine Vereinbarung zur Auftragsdatenverarbeitung (ADVV), die

- schriftlich abgeschlossen werden muss und
- den in § 11 Abs. 2 BDSG vorgeschriebenen Mindestinhalt (hierzu sogleich) aufweist.
- Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren. Standards und Zertifizierung?

Mindestinhalt einer ADVV:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Anlage zu § 9 Abs. 1 BDSG:

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1.Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2.zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3.zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4.zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

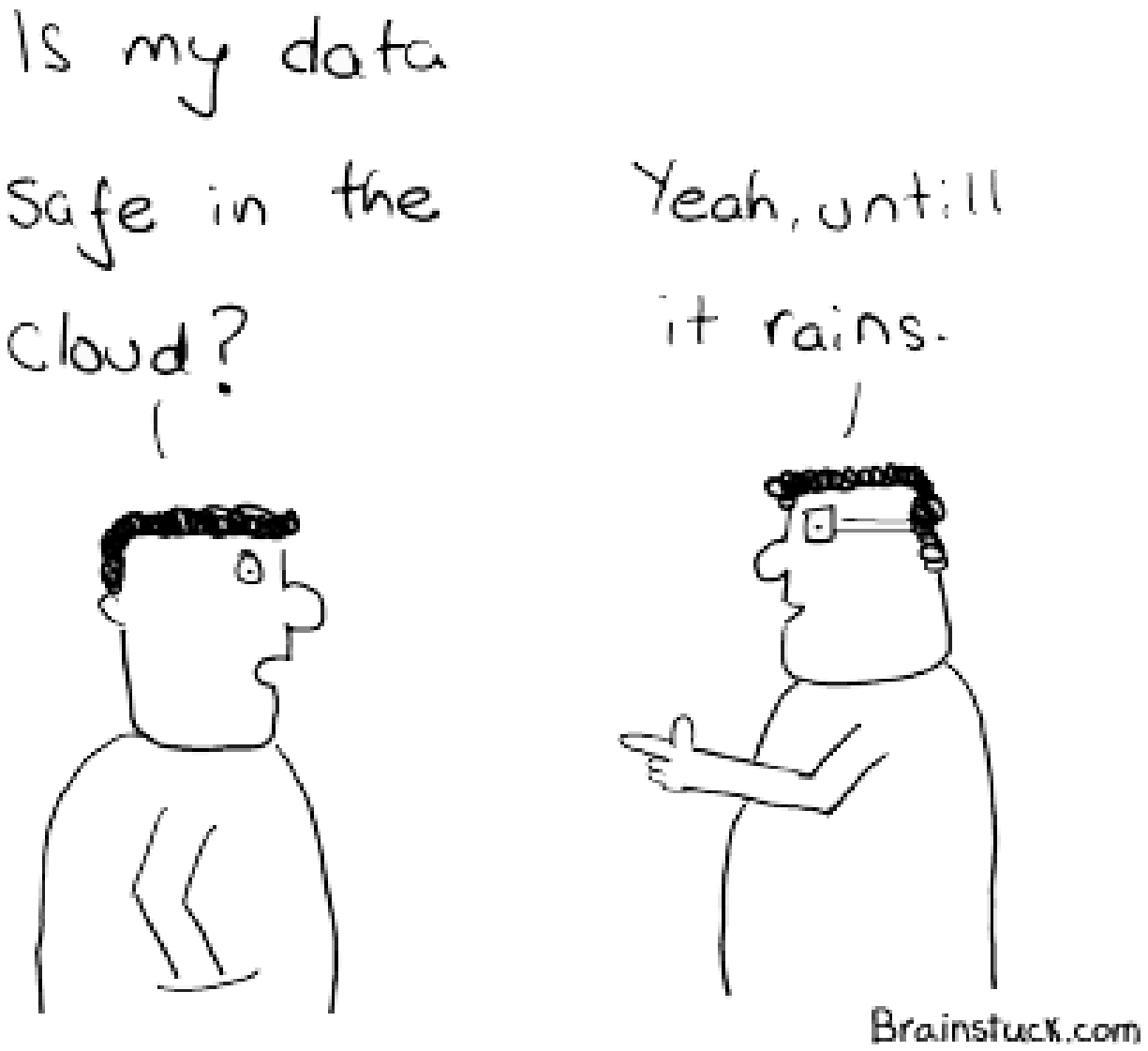
Anlage zu § 9 Abs. 1 BDSG (Fortsetzung):

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Cloud Computing und Datenschutz können kompatibel sein

Zu verlangen sind aber nach Ansicht der Aufsichtsbehörden (Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 29./29.9.2011) mindestens:

•offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,
•transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,
•die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und
•aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.



Mit freundlicher Genehmigung von Brainstuck.com - Anshul Maheshwari

Internationales Cloud Computing I

•Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten „im Auftrag“ erheben, verarbeiten oder nutzen, gelten nicht als „Dritte“ (§ 3 Abs. 8 S. 2 BDSG)

•Diese Einschränkung stellt eine Abweichung von der EU-Datenschutzrichtlinie dar.

•Folge: Privilegierung der Auftragsdatenverarbeitung greift nicht, wenn die Erhebung und Verarbeitung oder Nutzung außerhalb der EU/EWR stattfindet und dies vertraglich sichergestellt ist, z.B. durch entsprechende Garantien. Der Sitz des Auftragnehmers ist unerheblich.

Internationales Cloud Computing II

•Es gilt: Übermittlung ist nur zulässig mit (1.) Einwilligung des Betroffenen (§ 4a BDSG) oder wenn (2.) die Übermittlung „zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme, dass schutzwürdiges Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt“ (§ 28 Abs. 1 Nr. 2 BDSG).

•DAV, Stellungnahme aus 08/2011: *„In der Bundesrepublik Deutschland ist eine privilegierte Auftragsdatenverarbeitung nach den Regelungen des Bundesdatenschutzgesetzes sogar in sicheren Drittländern nicht möglich. Dies führt dazu, dass Cloud Computing in der Regel selbst dann unzulässig ist, wenn die Datenverarbeitung in solchen Ländern stattfindet, die nach der Ansicht der EU ein geeignetes Datenschutzniveau aufweisen.“*

•Wertungen aus § 11 BDSG können mE im Rahmen der Interessenabwägung nach § 28 BDSG berücksichtigt werden.

Internationales Cloud Computing III

•Erforderlich ist in jedem Fall ein angemessenes Datenschutzniveau in dem betreffenden Drittland

- Anerkanntes sicheres Drittland (Schweiz, Kanada (nur teilweise), Argentinien, Vogtei Guernsey und die Insel Man)
- Standardvertragsklauseln (EU Standard Clauses)
- Binding Corporate Rules im Konzern
- Safe-Habour (USA), soweit sich das betr. Unternehmen den Safe-Harbour-Prinzipien unterworfen hat: Liste des US-Handelsministeriums, u. a. Microsoft, Google, Facebook (!)

•Vorsicht ist geboten bei Werbeaussagen:

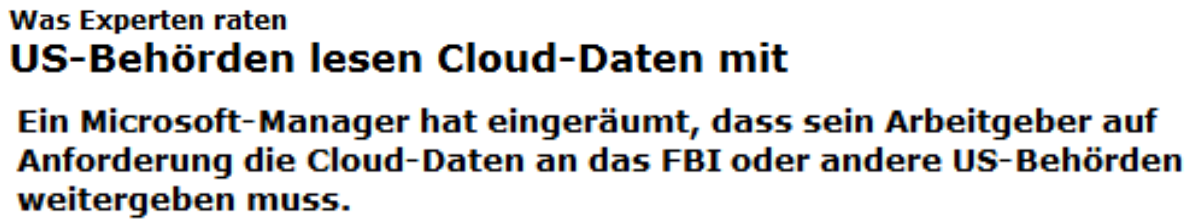
Kontroverse um Datenschutz in der Cloud

Salesforce und Hamburger CRM-Anbieter Wice streiten vor Gericht

it-business.de vom 4.1.2012

Internationales Cloud Computing IV

- Exkurs: US Patriot Act



Was Experten raten

US-Behörden lesen Cloud-Daten mit

Ein Microsoft-Manager hat eingeräumt, dass sein Arbeitgeber auf Anforderung die Cloud-Daten an das FBI oder andere US-Behörden weitergeben muss.

www.cio.de 26.7.2011

- ULD vom 15.11.2011: „Aus Sicht einer Datenschutz-aufsichtsbehörde kann auf die derzeitige Rechtslage in der Form reagiert werden, dass in Verträgen zur Auftragsdatenverarbeitung (z. B. beim Cloud Computing) ein explizites Verbot der Herausgabe von Daten an US-Behörden ausgesprochen wird, verbunden mit einer Vertragsstrafe, für den Fall, dass doch Daten absprachewidrig an die USA weitergegeben werden.“

Fazit

Anmerkungen oder Fragen?

Fabian Laucken
Fachanwalt für Informationstechnologierecht und
Fachanwalt für gewerblichen Rechtsschutz

Ihde & Partner Rechtsanwälte
Adresse: Schönhauser Allee 10-11, 10119 Berlin
E-Mail: fabian.laucken@ihde.de
Tel: (+49) (0)30 - 44318660, Fax:(+49) (0)30 - 44318679