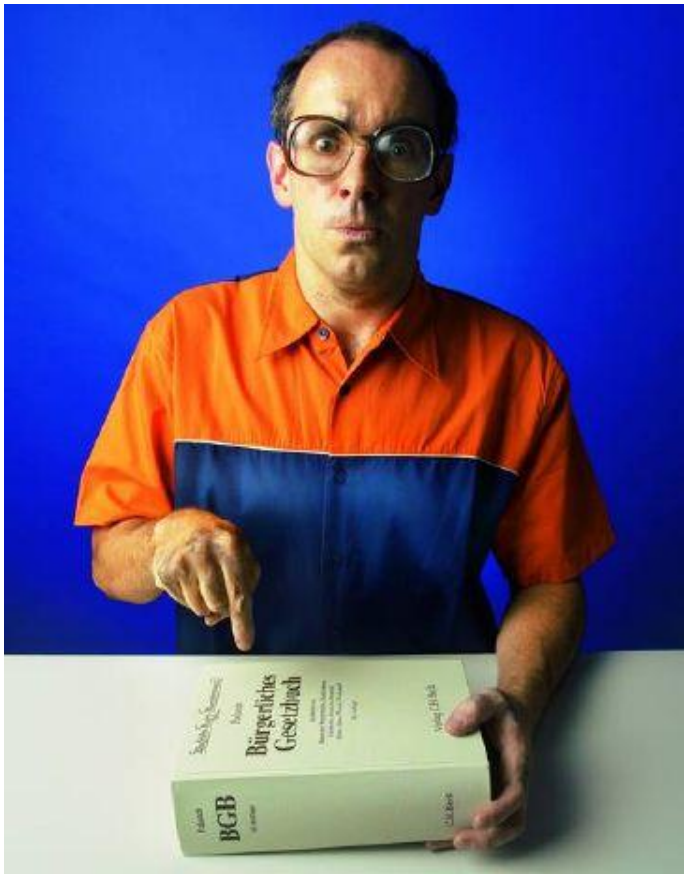
Cloud Computing: Neue Herausforderung für den Datenschutz

CeBIT Security Konferenz 2012
Hannover, 5. März 2012

RA Joerg Heidrich
Justiziar

Über den Referenten

- Studium der Rechtswissenschaften in Köln und Concord, NH, USA
- Justiziar des Heise Zeitschriften Verlags in Hannover (z.B. c‘t, iX, Technology Review, heise online)
- Daneben seit 2001 als Rechtsanwalt für Internet- und Medienrecht in Hannover tätig
- Fachanwalt für Informationstechnologierecht
- Mitherausgeber der Loseblattsammlung „Heise Online-Recht“
- Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD anerkannter Sachverständiger für IT-Produkte (rechtlich)



Themenübersicht

- Einführung
- Rechtliche Problematiken
- Vertragsrechtliche Probleme
- Internationale Verträge/Rechtswahl
- Einführung in den Datenschutz
- Datenschutz & Cloud Computing
- Weitergabe in Drittstaaten
- Fazit

Cloud Computing: Eine Einführung

RA Joerg Heidrich
Justiziar

Cloud Computing: Grundlagen

- Der Anwender bucht beim Cloud Service Provider (kurz: CSP), der die benötigte Hardware und Software betreibt und dem Anwender mit einer (genormten) Schnittstelle zur Verfügung stellt.
- **Flexibilität und Skalierbarkeit** von IT-Ressourcen
- Die „Wolke" ermöglicht, Ressourcen genau dann in der benötigten Menge zu erwerben, wenn diese wirklich benötigt werden.
- Die Abrechnung der Cloud-Dienste erfolgt **nutzungsabhängig** („On demand"- oder „As a Service"-Ansatz).
- Flexibilität und Skalierbarkeit von IT-Ressourcen ermöglicht **neue Geschäftsmodelle** – z.B.: Weihnachts-Shop - Vielzahl von Kaufabwicklungen innerhalb einer sehr kurzen Zeitspanne.

Argumente für Cloud Computing

- Unbegrenzte Skalierbarkeit: Anpassung der Leistungen an den jeweiligen Bedarf in Echtzeit
- Nahezu uneingeschränkte Verfügbarkeit
- Keine Personalkosten und -Risiken
- Kostentransparenz, Umwandlung von Fixkosten in variable Kosten je nach tatsächlich bestehenden Anforderungen
- Keine Kapitalbindung für Investitionen in Soft- und Hardware, Rechenzentrum, etc.
- Keine Kosten und Organisation für Updates oder defekte Hardware
- Einfache, uneingeschränkte Anbindung von Niederlassungen und Homeoffice

Argumente gegen Cloud Computing

- Fehlende Transparenz
- Möglichkeit des Zugriffs lokaler Behörden
- Vermengung von Kunden, Daten und Diensten
- Verlust der Kontrolle über Daten und Prozesse
- Abhängigkeit vom Anbieter/Schwierigkeiten bei Migration
- Einbußen beim Know-how
- Zentraler Angriffspunkt
- Fehlende Nachhaltigkeit: Erheblicher Energieverbrauch
- Erhebliche juristische Probleme

Überwachung in der Cloud I

- Kommentar von Microsoft zu der Löschung:

  *„Im Hinblick auf eine sichere und erfreuliche Erfahrung für alle Windows Live Benutzer, werden Bilder, die **vollständige oder teilweise Nacktheit zeigen**, nicht zugelassen.*

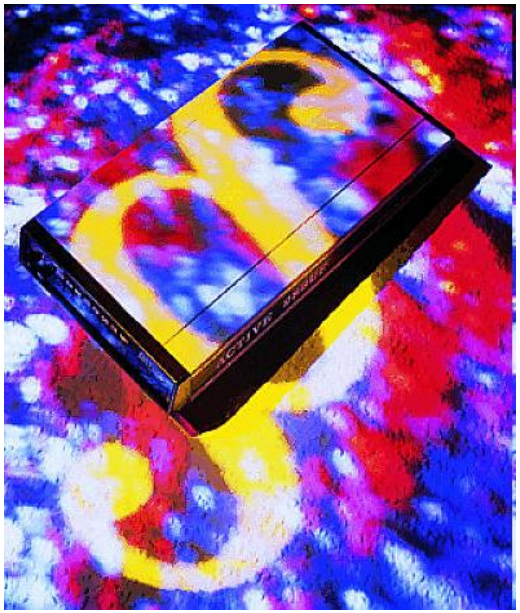
  Unser Sicherheits-Software hat einige von Ihnen gespeicherte Bilder als solche identifiziert, die diesen Verhaltenkodex verletzen.“

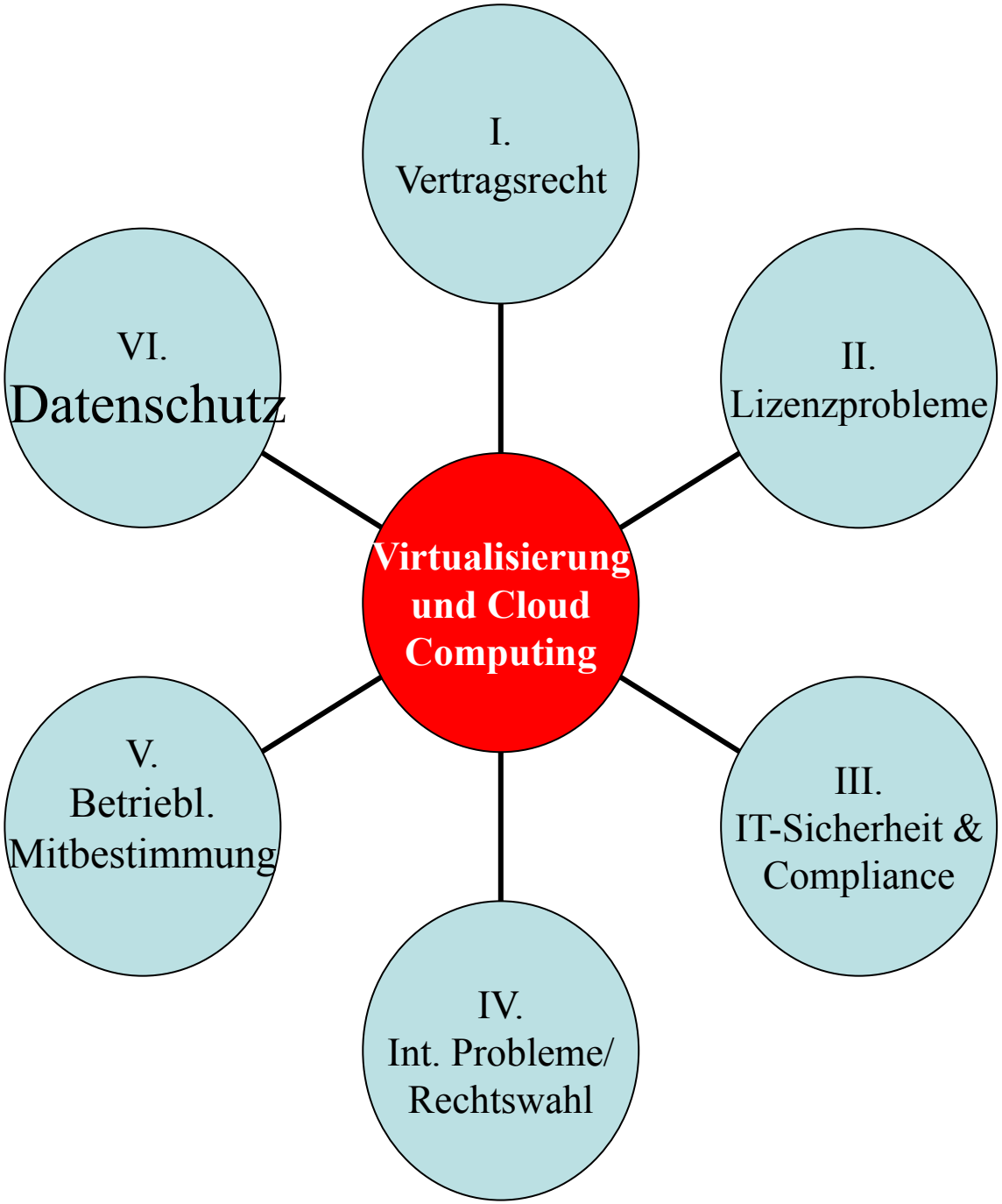
Überwachung in der Cloud II

- Apple MobileMe Servicebedingungen

  „*Apple behält sich jedoch das Recht vor, jederzeit **zu prüfen, ob Inhalte angemessen sind und mit diesen Servicebedingungen übereinstimmen**, und Apple ist berechtigt, Inhalte jederzeit ohne vorherige Ankündigung nach **eigenem Ermessen** herauszufiltern, zu verschieben, abzulehnen, zu modifizieren und/oder zu entfernen, wenn diese Inhalte gegen diese Servicebedingungen verstoßen oder auf andere Weise zu beanstanden sind.“*

Rechtliche Grundproblematik




I.
Vertragsrecht
II.
Lizenzprobleme
III.
IT-Sicherheit &
Compliance
IV.
Int. Probleme/
Rechtswahl
V.
Betriebl.
Mitbestimmung
VI.
Datenschutz
Virtualisierung
und Cloud
Computing

Rechtliche Fragestellungen

Eigene Daten werden in die Obhut von Dritten gegeben

- Wo befinden sich die Daten geografisch?
- Wie sind die Daten gesichert?
- Wer hat wie Zugriff auf die Daten?

Verhältnis zum Anbieter

- Kontrollmöglichkeiten und Überwachung
- Werden (offene) Standards verwendet?
- Wird der Anbieter auch auf lange Sicht zur Verfügung stehen?
- Was passiert bei Insolvenz oder Ausfall?
- Zugriffsmöglichkeiten z.B. für Steuerprüfung
- Rechtsdurchsetzung

Intern oder Extern?

- Besondere rechtliche Probleme ergeben sich lediglich dann, wenn Daten „nach Außen“, also **an Dritte weitergegeben werden.**
- Ansonsten sind meist nur die allgemeinen Anforderungen an Datenschutz, Lizenzrecht und IT-Sicherheit zu beachten
- Bei Weitergabe von personenbezogenen Daten an Dritte entstehen vor allem Probleme im Bereich des Datenschutzes
- Besondere Probleme bei Weitergabe von Daten ins Ausland, insbesondere außerhalb der EU
- Möglichst genaue Lösung der zu erwartenden Probleme im Bereich der vertraglichen Vereinbarungen notwendig

I. Vertragsgestaltung

- Aufgrund der erheblichen technischen und rechtlichen Risiken müssen im Rahmen der Vertragsgestaltung mit dem Anbieter die relevanten Rechte und Pflichten möglichst **detailliert und exakt dargestellt** werden.
- Bereits der Vertragstyp ist juristisch umstritten. Vermutlich handelt es sich um einen Mischvertrag, z.T. wird auch ein Mietverhältnis angenommen

  Die Vertragsform ist für die Haftung des Anbieters erheblich!

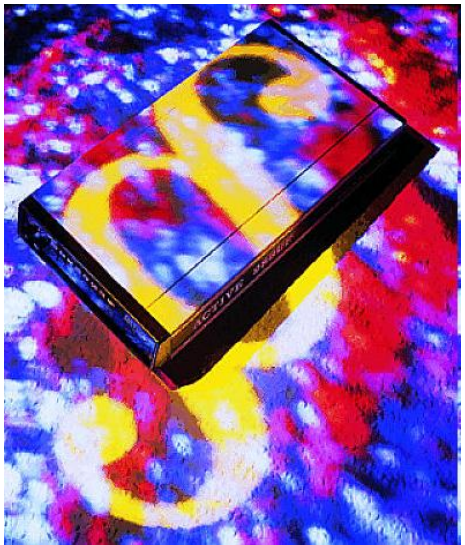
  Rechtsprechung zu diesem Problemkreis existiert bislang nicht.
- **Service Level Agreement** (SLA) muss vereinbart werden, insbesondere auch hinsichtlich Reaktionszeiten.
- Festlegung des **anzuwendenden Rechts**
- Sehr komplizierte Materie: Frühzeitige Hinzuziehung eines **spezialisierten Anwalts** unbedingt notwendig!

II. Lizenzrechtliche Probleme

- Durch das leichte Einrichten und Ändern von virtuellen Maschinen ist das Thema Lizenzierung der benötigten Software besonders zu beachten.
- Möglichst **flexibles Lizenzmanagement** gefordert.
- Verschiedene Lizenzmodelle möglich, z.T. werden auch schon entsprechende Lizenzen angeboten.
- Erhebliche Vereinfachung durch Nutzung von freien Virtualisierungslösungen, die oft unter der GNU General Public License (GPL) angeboten werden.
- (Eigentlich kein juristisches Problem)

III. IT-Sicherheit & Compliance

- Bei der Verlagerung von IT-Prozessen aus dem unmittelbar eigenen Verantwortungsbereich sind vor allem die Anforderungen an **IT-Sicherheit und Compliance** zu beachten!
- Die Verantwortlichen haben für die Einhaltung der Vorgaben persönlich zu sorgen, ggf. **Delegieren** auf die entsprechenden Fachkräfte im Unternehmen.
- Anderenfalls droht eine **persönliche zivil- und sogar strafrechtliche Haftung der jeweiligen Geschäftsführung**.



III. IT-Sicherheit & Compliance: Haftung

Amazon Web Services™ Customer Agreement

7.2. Security

We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. (...)

***We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications*.**

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

30.06.2011 13:05

US-Behörden dürfen auf europäische Cloud-Daten zugreifen

Cloud-Anbieter wie Microsoft müssen US-Strafverfolgungsbehörden Zugriff auf von Kunden gespeicherte Daten gewähren, **berichtet[1]** der US-Branchendienst *ZDNet*. Das betrifft auch in der EU ansässige Firmen und in europäischen Rechenzentren liegende Daten, wie Microsofts britischer Direktor Gordon Frazer anlässlich der Markteinführung von Microsofts Office 365 in London erklärte. Er antwortete damit auf die Frage, ob Microsoft zusichern könne, dass in seinen EU-Rechenzentren gespeicherte Daten Europa niemals verlassen könnten.

Da das Unternehmen seinen Firmensitz in den USA habe, müsse es die dortigen Gesetze befolgen, sagte Frazer. Das gilt insbesondere für den **Patriot Act[2]**, der US-Strafverfolgern weitreichende Zugriffsrechte auf Daten gibt. Frazer zufolge würden Kunden über die Herausgabe von Daten "informiert, wann immer das möglich ist". Eine Garantie dafür könne er jedoch nicht geben. Denn in den USA kann das FBI mit einem **National Security Letter[3]** (NSL) ein Redeverbot (**Gag order[4]**) für den Betreffenden aussprechen. In diesem Fall darf er nicht einmal sagen, dass er einen NSL erhalten hat.

Ein **Online-Dokument[5]** in Microsofts **"Trust Center"[6]** bestätigt Frazers Aussagen und stellt klar, dass es keineswegs nur um Verfahren im Zusammenhang mit dem Patriot Act geht. Dort heißt es: "Unter bestimmten Umständen kann Microsoft Daten ohne Ihre vorherige Zustimmung weitergeben. Dazu gehört die Befolgung rechtlicher Anforderungen." Fordere eine Regierungsstelle Daten eines Kunden an, werde man sie zunächst an diesen verweisen. Sei das Unternehmen **gezwungen[7]**, selbst zu antworten, werde es nur das zwingend Erforderliche herausgeben. Es wolle zudem alles "geschäftlich Vernünftige" unternehmen, um seine Kunden von dem Vorgang zu unterrichten – es sei denn, das ist rechtlich nicht möglich.

Nach Einschätzung von Thilo Weichert, Chef des **Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein[8]** (ULD), steht eine solche Datenweitergabe aus dem EU-Gebiet heraus im Widerspruch zu europäischem Datenschutzrecht. Das Risiko einer Datenweitergabe stelle die Vertraulichkeit der auf Microsoft-Rechenzentren gehosteten Daten und Anwendungen infrage und entziehe bestehenden Verträgen zur Datenverarbeitungsdienstleistung die Grundlage. Nach Auffassung Weicherts lasse sich daraus einerseits ein Sonderkündigungsrecht ableiten, und andererseits schließe es Service-Provider wie den Office-365- und Windows-Azure-Anbieter Microsoft als Kandidaten für personenbezogene IT-Dienstleistungen aus. Unternehmen sollten sich daher bei der Nutzung von Cloud-Diensten für personenbezogene Daten ausschließlich auf rein europäische Service-Provider beschränken.

Wie schwierig die Rechtslage zu beurteilen ist, erfuhren wir per Nachfrage bei Microsoft Deutschland: Dort war ad hoc nur die Antwort zu erhalten, man befolge selbstverständlich alle geltenden Gesetze. Was dies allerdings bedeutet, wenn US-amerikanische und europäische Gesetze zu widersprüchlichen Anforderungen führen, konnte man bei Microsoft so schnell nicht kommentieren. Besser könnten Großunternehmen fahren, die zum Beispiel Microsoft Office 365 als Angebot des deutschen Providers T-Systems nutzen und sich dann darauf verlassen können, dass ihre Daten ausschließlich auf Servern unter Kontrolle dieses Providers gespeichert werden. (**ck[9]**)

IV. Internationale Probleme/Rechtswahl

- **Problem der Rechtswahl**

  Wahl des Rechts eines Landes, nachdem der geschlossene Vertrag zu behandeln ist

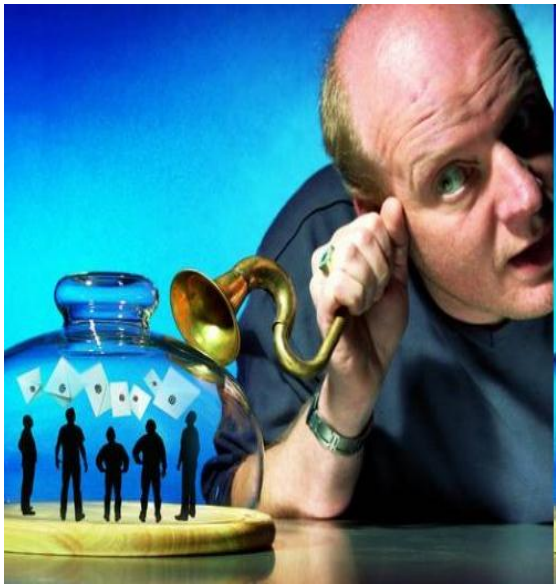
- **Problem der Rechtsdurchsetzung**

  Bereits in Deutschland kann eine Rechtsdurchsetzung auch aufgrund des hohen technischen Tiefgangs des Sachverhalts enorm erschwert werden.

  Schwierige Rechtsdurchsetzung in allen Ländern außerhalb der EU, insbesondere in Asien

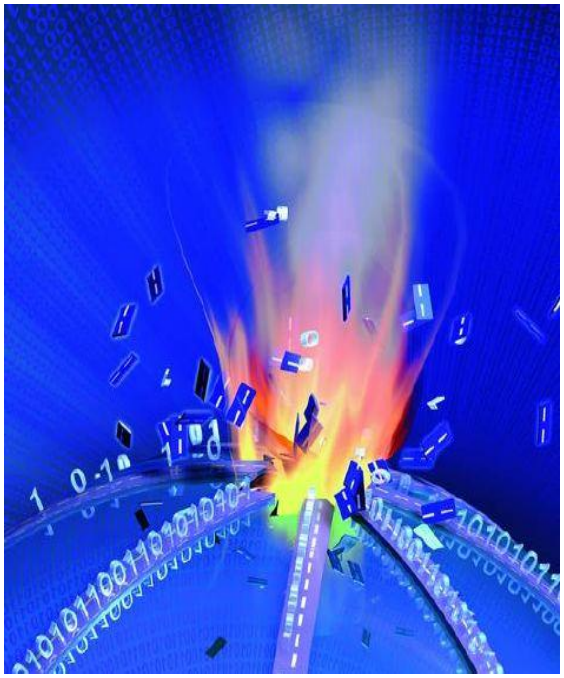
  In einigen Fällen dürfte nicht einmal klar sein, in welchen Ländern die Daten überhaupt physisch gespeichert werden.

V. Betriebliche Mitbestimmung/Betriebsrat



- Das Betriebsverfassungsgesetz räumt dem Betriebsrat in § 87 Abs. 1 Nr. 6 BetrVG sehr weitgehende **Mitbestimmungsmöglichkeiten** im Hinblick auf technische Einrichtungen ein, die der Überwachung des Verhaltens oder der Leistung der Arbeitnehmer dienen können.
- Um eine solche Einrichtung kann es sich bei dem Einsatz von Virtualisierung oder Cloud Computing handelt, soweit diese die Arbeitnehmer tangiert (z.B. Festhalten des Ein- und Ausloggens).
- Bei der Einführung solcher Techniken sollte daher stets auch die **betriebliche Mitbestimmung** berücksichtigt werden (sofern ein Betriebsrat vorhanden ist)!

Cloud Computing & Datenschutz



RA Joerg Heidrich
Justiziar

Grundlagen des Datenschutzes

RA Joerg Heidrich
Justiziar

§ 1 Bundesdatenschutzgesetz (BDSG)

„Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird”

Grundrecht auf Datenschutz

- Datenschutz gewährleistet das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen
- **Recht auf „informationelle Selbstbestimmung“** ist ein Grundrecht
- Der „**gläserne Bürger**“ bzw. „gläserne Verbraucher“ sollen vermieden werden (Volkszählungsurteil)
- Der Bürger hat das Recht, über die Verbreitung seiner Daten selbst zu entscheiden sowie Kontrollmöglichkeiten

Welche Daten sind geschützt?

Personenbezogene Daten

Definition in § 3 BDSG

„Einzelangaben über persönliche oder sachliche Verhältnisse einer **bestimmten** oder **bestimmbaren natürlichen Person“**

Personenbezogene Daten

- Daten sind personenbezogen, wenn sie eindeutig einer **bestimmten natürlichen Person zugeordnet sind** oder diese Zuordnung zumindest mittelbar erfolgen kann (personenbeziehbaren Daten).
- Beispiele für personenbezogene Daten:

  - Name, Alter, Familienstand, Geburtsdatum
  - Anschrift, Telefonnummer, E-Mail Adresse
  - genetische Daten und Krankendaten
  - Werturteile, zum Beispiel Zeugnisse
- Auch Daten, über die sich **mittelbar ein Personenbezug** herstellen lässt, sind als personenbeziehbare Daten anzusehen

  Beispiel: Kfz-Kennzeichen, Kontonummer, Matrikelnummer

  Entscheidend ist allein, dass es gelingen kann, die Daten mit vertretbarem Aufwand einer bestimmten Person zuzuordnen.

Besondere Arten von personenbez. Daten

Besondere Arten personenbezogener Daten sind sensible Angaben über eine Person wie:

- Rassische und ethnische Herkunft
- politische Meinungen
- Religiöse Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit
- Sexualleben
- strafrechtliche Verurteilungen usw.

Für diese personbezogenen Daten gilt ein besonderer Schutz!

Datenschutzrechtlich nicht relevante Daten

- Sämtliche Daten, die **nicht personenbezogen** oder beziehbar sind, fallen nicht unter den Datenschutz.

  Hierzu gehören z.B.

  - Anonyme Statistiken
  - Lagerbestände
  - Verkaufsdaten
  - Produktionsdaten
- Nicht unter den Datenschutz fallen zudem Daten über juristische Personen wie z.B. Kapitalgesellschaften oder Vereine.

Rechte des Betroffenen

- Informations- und Auskunftsrecht gegenüber privaten und staatlichen Stellen
- Auch im Klageweg im Rahmen der Auskunftsklage
- Recht auf Anrufung der Datenschutzbehörden
- u.U. Schadensersatzanspruch

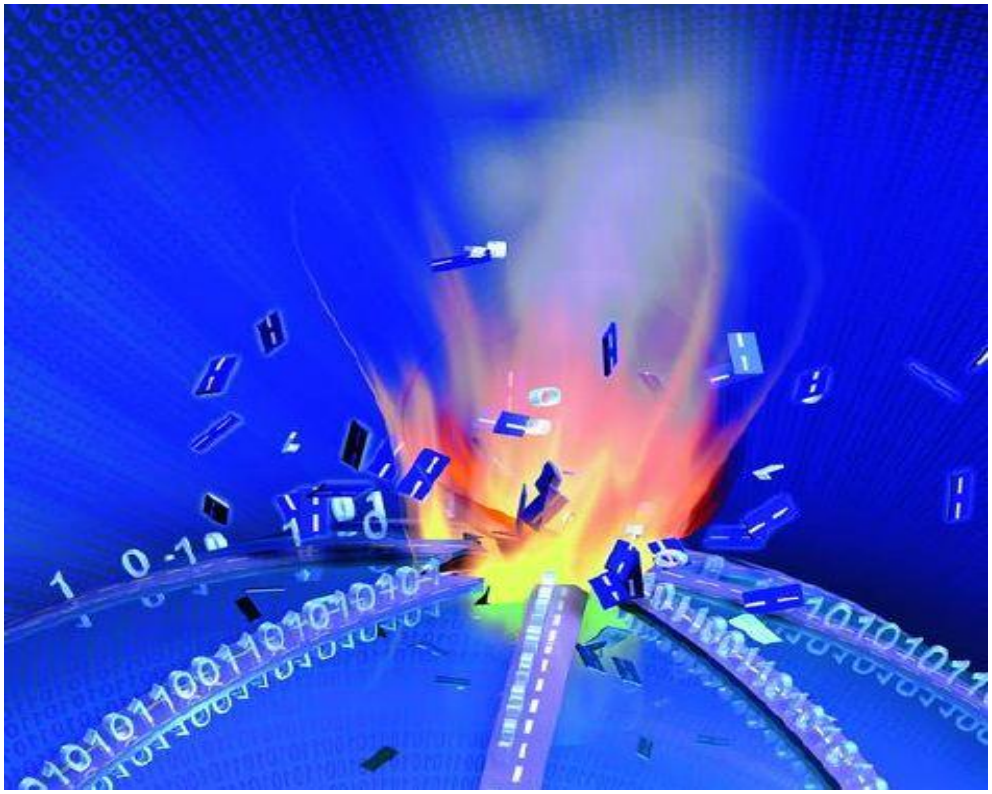
Rechte des Betroffenen: T5F

„Thoms Fassung von Framstags freundlichem Folterfragebogen“ (T5F)

Hiermit fordere ich Sie im Rahmen des §34 BDSG auf

1. mir unentgeltlich Auskunft zu erteilen, welche Daten über mich bei Ihnen gespeichert sind und zu welchem Zweck (§ 34 I-III BDSG i.V.m. §6 II, § 28 Abs. 4),
2. mir mitzuteilen, aus welcher Quelle Sie diese Daten erhalten haben (§ 34 I Nr.1 BDSG),
3. sofern eine Weitergabe stattfand, mir alle weiteren Empfänger meiner Daten zu nennen (§ 34 I Nr.2 BDSG),
4. sofort sämtliche über mich bei Ihnen gespeicherte Daten aus Ihren Beständen zu löschen (§ 35 II BDSG).
5. Mir eines Kopie Ihres öffentlichen Verfahrensverzeichnisses nach § 4e BDSG zu übersenden.

Cloud Computing: Datenschutzprobleme

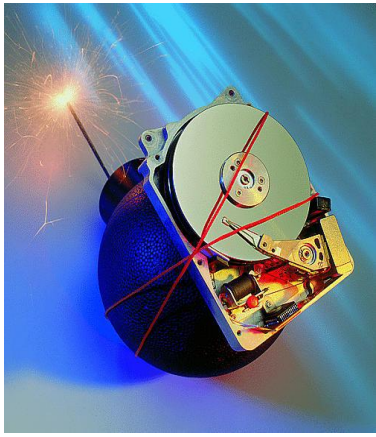


RA Joerg Heidrich
Justiziar

Grundsätze I

- Datenschutz ist nur dann relevant, wenn **personenbezogenen Daten in die Cloud** ausgelagert werden.
- Regelmäßig relevant: Daten von Kunden, Lieferanten oder Mitarbeitern.
- Besonders zu schützen sind „besondere Arten personenbezogener Daten“ wie Rasse, Religion, sexuelle Vorlieben, Krankheitsdaten.
- Handelt es sich dagegen um nicht personenbezogene Daten (z.B. technische Zeichnungen, Lagerbestandslisten, anonyme Statistiken), so greift der Datenschutz nicht.
- Aber: Besonders unternehmensrelevante Daten können trotzdem unter **Compliance-Aspekten** besonders schutzwürdig sein (Konteninformationen, Berufsgeheimnisse, u.a.).

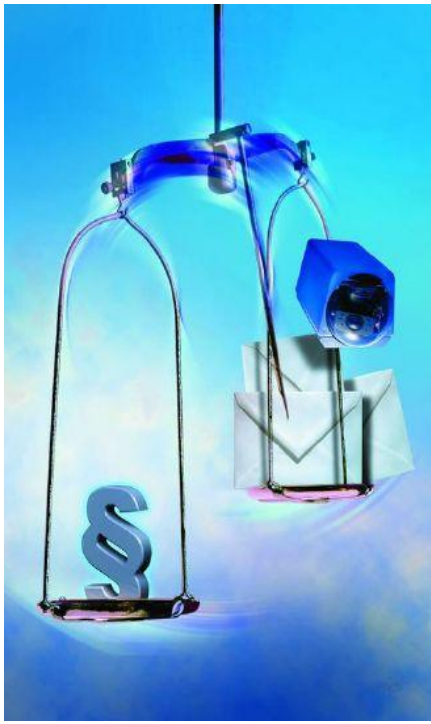
Grundsätze II



- Cloud Computing stellt sich rechtlich als **Auftragsdatenverarbeitung** dar.
- Rechtliche Fiktion: Es findet keine Weitergabe an Dritte statt, der Empfänger der Daten verarbeitet diese nur „im Auftrag“.
- **Vorteil:** Einfacherer Transfer, insbesondere muss nicht die Erlaubnis der Betroffenen eingeholt werden.
- **Nachteil:** Der Auftraggeber bleibt datenschutzrechtlich verantwortlich und „Herr des Verfahrens“

  Insbesondere trägt der Provider keine eigene Verantwortung für die Verarbeitung der Daten.
- Aufgrund von zahlreichen Missbrauchsfällen 2009 neue und **strenge Anforderungen** an die Auftragsdatenverarbeitung nach BDSG-Reform.

Auftragsdatenverarbeitung, § 11 BDSG



- **Was ist das?**

  Erhebung, Nutzung oder Verarbeitung personenbezogener Daten durch einen Dritten im Auftrag und im Rahmen der Weisungen des Auftraggebers

  Es reicht, wenn die Möglichkeit besteht, Einsicht in derartige Daten zu erhalten!
- **Beispiele**

  Callcenter, Direktmarketing, Lohnbuchhaltung, Wartung des Systems durch Dritte, Aktenvernichtung
- In der Vergangenheit gab es gerade in diesem Bereich massiven Missbrauch
- Daher wesentliche Verschärfung der Voraussetzungen!

Zu beachtende Punkte nach § 11 BDSG

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.

Weitere Voraussetzungen

- Vereinbarung in Standard-AGB reichten nicht, es muss mit jedem Dienstleister eine **gesonderter Vertrag** geschlosse werden.
- **Kontrollpflichten!**

  *„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.“*
- Pflicht zu **persönlichen Kontrollen** zumindest bei wichtigen Aufträgen!
- Alternativ: Kontrollen durch einen Sachverständigen oder Vorlage eines Datenschutzgutachtens.
- Erhebliche Bußgeldgefahr bei Nichteinhaltung.

Datenweitergabe ins Ausland

- Datenübermittlungen **innerhalb des europäischen Binnenmarktes** sind unter denselben Voraussetzungen zulässig wie Übermittlungen im Inland.
- Für die Frage, ob eine Datenübermittlung in ein Drittland zulässig ist, kommt es entscheidend darauf an, ob bei der empfangenden Stelle im Drittland ein **angemessenes Datenschutzniveau** gewährleistet ist.

  Bisher hat die Europäische Kommission lediglich für einige wenige Länder wie Kanada, die Schweiz oder Argentinien entsprechende Feststellungen getroffen.
- Keine „sicheren“ Drittstaaten sind insbesondere die USA, China, Indien!
- Vor Ort legale Zugriffsmöglichkeiten der Behörden beachten.

Datenweitergabe ins Ausland

- Die **USA** (auch Indien, China, Japan!) zählt datenschutzrechtlich zu den so genannten „**unsicheren Drittstaaten**“.
- Bisher grundsätzlich Möglichkeit für US-Unternehmen, Safe Harbor beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die **Safe Harbor Principles** zu beachten.
- Aber: Der Düsseldorfer Kreis hat im April 2010 erklärt, dass sich Datenexporteure in Deutschland nicht auf die Behauptung einer Safe-Harbor-Zertifizierung von US-amerikanischen Unternehmen verlassen dürfen.
- Wohl h.M.: **Kein Datenexport in die USA in Rahmen von Cloud Computing zulässig!**
- Alternative: Individuelle Zustimmung der einzelnen Betroffenen oder Abschluss eines besonderen Vertrags nach EU-Vorlage.

Fazit: Bedenkenlose Nutzung

- Nutzung einer **private Cloud**
- Speicherung von **verschlüsselten Daten** in der Cloud
- Speicherung von nicht personenbezogenen und nicht unternehmensrelevanten Daten in der Cloud
- (Informierte!) Einwilligung der Betroffenen Dateninhaber in diese Art der Speicherung

Fazit: Vorsicht bei der Nutzung

- Speicherung von **nicht personenbezogenen aber unternehmensrelevanten** Daten in der Cloud
- Speicherung von **unverschlüsselten personenbezogenen Daten**

Fazit: Rechtlich verbotene Nutzung

- Nutzung einer Cloud mit Rechnern **außerhalb der EU** (hM)
- Speicherung von **besonders geschützten personenbezogenen Daten** in der Cloud, z.B. mit religiösem Bezug!
- Fehlende oder nur oberflächliche vertragliche Regelungen inkl. Regelung der Auftragsdatenverarbeitung

Gesamtfazit

- Bei der Nutzung von Virtualisierung und Cloud Computing besteht generell ein **gesteigertes technisches und rechtliches Risiko**. Damit erhöhen sich auch die Anforderungen zur Einhaltung gesetzlicher und unternehmensinterner Compliance-Vorgaben.
- Aus Datenschutzsicht empfiehlt es sich dringend, einen Provider zu wählen, der garantiert, dass seine Daten auf Servern **in Deutschland oder innerhalb der EU** bleiben.
- Hohe Anforderungen an die Vertragsgestaltung, möglichst genaue Regelung von „worst case“ Fällen und SLA.
- Lizenzrechte beachten!
- Betriebliche Mitbestimmung berücksichtigen.

Heise Zeitschriften Verlag

RA Joerg Heidrich
Fachanwalt für IT-Recht
Heise Zeitschriften Verlag
Helstorfer Straße 7
30625 Hannover

Telefon: 05 11 - 53 52 293
www.heise.de
joerg.heidrich@heise.de

Twitter: @dasgesetzbinich