Cloud Computing und Datenschutz

Thilo Weichert

Bei der personenbezogenen Datenverarbeitung im Rahmen des Cloud Computing treten rechtliche und technische Fragestellungen auf, die bisher nur unzureichend aufgearbeitet sind. Da sich diese Form der Datenverarbeitung immer größerer Beliebtheit erfreut, ist es nötig, die Rahmenbedingungen des Datenschutzes abzuleiten und zu benennen. Im Folgenden erfolgt diese Aufarbeitung am Beispiel von Datenverarbeitungen durch nicht-öffentliche Stellen mit Sitz in Deutschland, für die das Bundesdatenschutzgesetz (BDSG) anwendbar ist. Für die Verarbeitung durch öffentliche Stellen des Bundes und der Länder gelten regelmäßig entsprechende Normen im BDSG bzw. in den Landesdatenschutzgesetzen (LDSG).

1. Zweck und Erscheinungsformen des Cloud Computing

„Cloud Computing“ steht für „Datenverarbeitung in der Wolke“. Die Wolke schwebt nicht am Himmel, sondern beschreibt eine zunächst noch nebulös bleibende, über Netze, v.a. über das Internet angeschlossene Rechnerlandschaft, in die die eigene Datenverarbeitung ausgelagert wird. Ziel ist es, informationstechnische (IT-) Dienstleistungen dynamisch und skalierbar nutzen zu können, d.h. externe Hard- und Software sowie Know-how im Interesse des *Einsparens von Ressourcen* zu nutzen. Im Idealfall soll es dem Nutzer egal sein können, ob gerade der eigene oder ein weit entfernter Computer eine Aufgabe löst. Teilweise werden ganze Verfahren in die Cloud verlagert; teilweise geht es auch nur darum, Bedarfsspitzen abzudecken, mit denen die eigene IT-Infrastruktur überfordert ist. Bezahlt wird regelmäßig neben einer Grundgebühr skaliert für die jeweilige Nutzung und Dienstleistung, zumeist nach Rechenleistung und Rechenzeit. Denkbar ist auch die Bezahlung pauschaler Flatrates.

Dieser Ansatz ist in der Informationstechnik (IT) nicht neu. Ihn gibt es unter dem Begriff „*Outsourcing*“, seit es Datenverarbeitung gibt. Datenschutzrechtlich diskutiert wurde und wird dieser Ansatz mit den Begriffen „Auftragsdatenverarbeitung“ und „Funktionsübertragung“ (s.u. 6.2). Ein aktueller Vorläufer des Cloud Computing ist das Grid Computing, das „Rechnen aus der Steckdose“. Das Grid Computing ist inspiriert von der Idee, Rechenleistung ähnliche der Versorgung mit Wasser oder Strom aus dem Netz zu beschaffen. Während aber beim Grid regelmäßig Rechner statisch gekoppelt sind, werden Cloud-Ressourcen zumeist flexibel bereit gestellt.

Beim Cloud Computing wird *unterschieden* zwischen Software-as-a-Service (SaaS), Storage-as-a-Service, Platform-as-a-Service (Paas), Infrastructure-as-a-Service (IaaS). Davon abgeleitet sind weitere Begriffe wie z.B. HPC-as-a-Service (HPC steht für High Performance Computing). Beim SaaS wird Software nicht auf dem eigenen Rechner installiert, sondern für den Bedarfsfall im Netz bereitgestellt. Storage-as-a-Service dient der Datensicherung und der Archivierung, entweder durch regelmäßige oder durch endgültige Speicherung von Datenbeständen. Eine Sonderform sind Replikationsdienste, also das Abspeichern von Daten im Netz, um hierauf im Bedarfsfall zugreifen zu können. PaaS stellt umfassende Anwendungen (Applikationen) fremden Nutzenden zur Verfügung, z.B. ein ganzes Customer Relation Management-(CRM-)System. Bei IaaS wird umfassende IT-Infrastruktur zur Verfügung gestellt.

Im Zusammenhang mit Cloud Computing fällt immer wieder der Begriff der „*Virtualisierung*“. Damit wird das Betreiben eines „virtuellen Computers“ auf einer (fremden) Hardware gemeint. Dabei erfolgt eine logische Trennung eines Programms vom Betriebssystem des genutzten

Rechners.

Ein weiterer im Kontext auftauchender Begriff ist *Service-orientierte Architektur* (SOA). Dabei geht es um die einheitliche Abbildung von Geschäftsprozessen auf einer heterogenen IT, mit der organisationsübergreifend Prozesse abgewickelt werden können. SOA steht zumeist im Kontext von Webservices, also mit der Sprache XML definierte Standards, mit denen Daten zwischen unabhängigen Organisationen ausgetauscht werden können.

Unterschieden werden kann zwischen Private- und Public-Clouds. *Private Clouds* sind vernetzte Rechner, die sämtliche unter der rechtlichen Verantwortung einer einzigen Daten verarbeitenden Stelle stehen. Eine besondere Form von In-House-Clouds sind virtualisierte Desktops mit einem Unternehmens-Betriebssystem, auf das Mitarbeiter über Thin Clients, mobile Laptops oder PCs zugreifen und hierüber Daten verarbeiten können. Als Private-Clouds werden auch Rechnernetze von rechtlich zueinander in einem engen Verhältnis stehenden Stellen bezeichnet, z.B. Stellen der öffentlichen Verwaltung oder eines Unternehmenskonzerns.

Bei *Public Clouds* wird die Rechenleistung von Dritten im Sinne des Datenschutzrechtes (§ 3 Abs. 8 S. 2 BDSG; s.u. 2.4) angeboten. Anbieter von Public Clouds sind die ganz großen globalen IT-Unternehmen, u.a. Amazon (EC2), Google, Microsoft, IBM oder Hewlett-Packard (zusammen mit Intel und Yahoo). Diese verarbeiten die Daten auf weltweit verteilten Servern bzw. Serverfarmen, die einem oder auch unterschiedlichen Anbietern gehören.

Neben kommerziellen Angeboten gibt es öffentliche, zumeist akademische Einrichtungen, die Cloud Computing zur Verfügung stellen. Hybride Clouds sind eine Mischung von Private- und Public-Clouds, also eine Nutzung sowohl von eigenen wie auch fremden Ressourcen. Unterschieden werden schließlich *Community-Clouds*, bei denen eine Cloud-Infrastruktur gemeinsam genutzt wird, wobei gemeinsame Anforderungen, z.B. zur Sicherheit, zum Datenschutz oder zu weiteren Compliance-Anforderungen kollektiv vereinbart und festgelegt werden..

Hinsichtlich der *agierenden Stellen* kann i.d.R. zwischen dem Cloud-Nutzer, dem Cloud-Anbieter und den Ressourcen-Anbietern unterschieden werden. Der Cloud-Nutzer ist die Stelle, die Rechenleistung von Cloud-Diensten in Anspruch nimmt. Der Cloud-Anbieter stellt diese Dienste dem Cloud-Nutzer bereit. Dieser kann sich von den Ressourcen-Anbietern unterscheiden, die i.d.R. dem Cloud-Anbieter für die Cloud-Datenverarbeitung ihre Hard- oder Software zur Verfügung stellen, damit diese zusammengefasst dem Nutzer angeboten werden können.

2. Praktische Probleme und rechtliche Fragestellungen

Bei der Realisierung des Cloud Computing gibt es eine Vielzahl von *technisch-praktischen Problemen*. So ist die Bandbreite der Netzverbindung von zentraler Bedeutung. Dauert das Rechnen im Netz zu lange, so gehen eingesparte Ressourcen an anderer Stelle wieder verloren.

Das zentrale Problem des Cloud Computing besteht darin, die *Integrität und Vertraulichkeit der Datenverarbeitung* des Cloud-Nutzers zu gewährleisten. Dies gilt nicht nur für die Verarbeitung personenbezogener, sondern sämtlicher Daten, bei denen es auf Vertraulichkeit und Integrität ankommt, z.B. für Betriebs- und Geschäftsgeheimnisse, für Forschungsdaten oder für anderweitig immateriell-rechtlich geschützte Daten. Es geht um das Unterbinden unberechtigter und schädigender Zugriffe Dritter.

Ein zentraler Aspekt jedes Cloud-Vertrages ist die Sicherheit der Datenverarbeitung. Hierzu

gehören Pflege- und Fehlerbeseitigungsmaßnahmen sowie Maßnahmen zur Abwehr von Angriffen und Störungen. Schon aus haftungsrechtlichen Gründen ist es von Bedeutung, dass die Verantwortlichkeit für spezifische Sicherheitsmaßnahmen eindeutig zugewiesen wird. Sicherheitszusagen können über *Security-Service-Level-Agreements* (SSLA) verabredet werden. Tatsächlich bleiben die Cloud-Anbieter bei ihren Garantien für Sicherheitsmaßnahmen „wolkig". SSLA haben regelmäßig den Charakter von allgemeinen Geschäftsbedingungen (AGB).

Rechtlich erfolgt die Bereitstellung und Nutzung von Clouds im Rahmen eines *Schuldvertrags*, bei dem sich eine Vielzahl von juristischen Fragestellungen ergeben können, die hier nicht näher behandelt werden können (z.B. Haftung, Gewährleistungsansprüche, Urheberrecht). Cloud-Verträge sind nicht eindeutig zuordenbar, sondern eine Typenmischung mit Anteilen eines Mietvertrags, einer Leihe und eines Dienst- und/oder eines Werkvertrages (Schulung, Pflege, Schnittstellenanpassung).

Die Archivierung von Daten in grenzüberschreitenden Clouds hat bzgl. steuerlich relevanten Aufzeichnungen Bedeutung, da diese nach § 146 Abs. 2 S. 1 AO grundsätzlich im Inland zu führen und aufzubewahren sind. Auf Antrag kann die zuständige Finanzbehörde nach dem zum 01.01.2009 eingefügten § 146 Abs. 2a AO bewilligen, dass die Dokumente in einem Mitgliedstaat der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums mit Amtshilfeübereinkommen (EWR, Island, Liechtenstein, Norwegen) archiviert werden. Die ausländische Finanzbehörde muss zustimmen und die deutsche Finanzbehörde muss auf die Dokumente zugreifen können. Nach § 148 AO dürfen *steuerrechtliche Unterlagen* außerhalb des EU/EWR-Raumes nach Bewilligung der Finanzbehörde nur aufbewahrt werden, wenn das Aufbewahren im Inland für den Steuerpflichtigen Härten mit sich brächte und die Besteuerung nicht beeinträchtigt wird.

Nach dem *Handelsrecht* müssen Buchungsbelege und Handelsbriefe im Inland aufbewahrt werden. Es besteht nach § 257 Abs. 4 HGB eine gesetzliche Aufbewahrungsfrist von 6 bzw. 10 Jahren. Ein explizites Verbot zur Nutzung eines Cloud Archiving besteht nicht.

Eine Cloud-Angebote richten sich direkt an die Verbraucherinnen und Verbraucher (z.B. Google Apps), so dass das nationale und das internationale *Verbraucherrecht* zu beachten ist.

Für die Ermittlung von *Straftaten und Ordnungswidrigkeiten* stellt die Speicherung von Daten in der Cloud dann ein Problem dar, wenn durch die Art und den Ort der Datenverarbeitung ein Zugriff für die Ermittlungs- und Sanktionsbehörden nicht möglich ist.

Wegen der Vielzahl der mit Cloud-Datenverarbeitungen verbundenen rechtlichen Fragen, die bisher keiner gesetzlichen Regelung zugeführt worden sind, kommt der Gestaltung dieser Beziehungen durch *IT-Vertrag* eine zentrale Bedeutung zu.

3. Anwendbarkeit des Datenschutzrechtes generell

Aus Datenschutzsicht relevant ist Cloud Computing nur, wenn personenbezogene Daten verarbeitet werden (§ 3 Abs. 1 BDSG), also wenn die verarbeiteten Einzelangaben einer bestimmten oder bestimmbaren natürlichen Person, also einem Menschen – dem Betroffenen – zugeordnet werden können. Betroffene können zum einen Mitarbeiter der verantwortlichen Stelle sein, die bei der Cloud-Nutzung beschäftigt werden und deren Daten in diesem Zusammenhang verarbeitet werden. In Hinblick auf die Nutzungsdaten ist das spezifische Arbeitnehmerdatenschutzrecht anwendbar. Regelmäßig verarbeitet werden zudem personenbezogene Daten als Gegenstand der Cloud-Anwendung, seien die Angaben zu Kundinnen und Kunden, zu Lieferanten und sonstigen

Geschäftspartnern oder von Personen, die mit dem Cloud-Nutzer in keinem spezifischen Verhältnis stehen.

Keine Anwendbarkeit des Datenschutzrechtes ist gegeben bei hinreichender Anonymisierung ehedem personenbezogener Daten. Als *anonymisiert angesehene Daten* (vgl. § 3 Abs. 6 BDSG) können durch ihre Verarbeitung in der Cloud reidentifizierbar werden, weil andere Cloud-Nutzer oder die Cloud- bzw- Ressourcen-Anbieter über Zusatzwissen verfügen, mit dem eine Reidentifizierung möglich ist.

Soweit kein objektiver, sondern ein relativer *Begriff der Personenbeziehbarkeit* vertreten wird, kann sich also die Qualität der Datenverarbeitung durch Cloud-Anwendungen ändern. Da es aber heute keines unverhältnismäßig großen Aufwandes an Zeit, Kosten und Arbeitskraft mehr bedarf, um durch komplexe Verknüpfungen in Netzen nicht eindeutig identifizierende Daten einer bestimmbaren Person zuzuordnen, ändert allein der Umstand einer Verarbeitung in einer Cloud an der Anwendbarkeit des Datenschutzrechtes nichts. Eine Personenbeziehbarkeit ist bei Einzeldatensätzen zu Personen regelmäßig anzunehmen. Gerade die elektronische Auswertbarkeit und die Integration in ein möglicherweise weltweites Netzwerk erhöht die Wahrscheinlichkeit des Vorliegens von Zusatzwissen, das eine Identifizierung der Betroffenen ermöglicht.

Durch *Pseudonymisierung*, also das Ersetzen der Identifikationsmerkmale einer natürlichen Person durch ein anderes Merkmal (§ 3 Abs. 6a BDSG), wird die Anwendbarkeit des Datenschutzrechtes nicht ausgeschlossen. Durch diese Methode kann eine Identifizierung der Betroffenen derart erschwert werden, dass ein Schutzniveau erreicht wird, das eine Datenverarbeitung zulässig macht.

4. Anwendbarkeit des nationalen Datenschutzrechts

Clouds sind tendenziell grenzüberschreitend: Es gibt keine technischen Gründe zur Berücksichtigung territorialer Grenzen. Anderes gilt für das Datenschutzrecht. Dieses knüpft an den Ort einer Datenverarbeitung an. Nach der Europäischen Datenschutzrichtlinie (EU-DSRL) soll aber innerhalb des europäischen Binnenmarktes der Umstand einer grenzüberschreitenden Datenverarbeitung kein rechtliches Hindernis mehr darstellen (Art. 1 Abs. 2 EU-DSRL). Voraussetzung dafür ist aber die Gewährleistung eines hinreichenden Datenschutzes. Durch die Überschreitung der nationalen Grenzen soll es nicht zu einer Rechtebeschneidung für die Betroffenen kommen und schon gar nicht zu einem „Race to the bottom“ bei den Schutzstandards. Gemäß Art. 4 Abs. 1 a), b) EU-DSRL kommt es für die Anwendbarkeit einzelstaatlichen Rechts darauf an, in welchem Mitgliedstaat die Daten verarbeitende Niederlassung ihren Sitz hat.

Beim grenzüberschreitenden Cloud-Computing ist nicht gewährleistet, dass in den von der konkreten Anwendung tangierten Staaten überhaupt Regelungen zum Datenschutz und zum Datenschutz bestehen. Befinden sich die genutzten Rechner eventuell gar außerhalb jeglichen nationalen Territoriums, also auf hoher See, so ist das Fehlen von rechtlichem Persönlichkeitsschutz gewiss (sog. Offshoring).

Hat die Daten verarbeitende Stelle keine Niederlassung im EU/EWR-Raum, so kann nach § 1 Abs. 5 S. 3 BDSG ein *im Inland ansässiger Vertreter* benannt werden, dem gegenüber das anwendbare nationale Datenschutzrecht geltend gemacht werden kann.

5. Verantwortlichkeit

In einer Cloud droht die Verantwortung für die konkrete Verarbeitung und für eventuelle

Persönlichkeitsverletzungen hinter den grenzüberschreitenden Wolken zu verschwinden. Für die datenschutzrechtliche Bewertung von Cloud-Anwendungen ist daher eine präzise Klärung der Verantwortlichkeiten vor zentraler Bedeutung. Anknüpfungspunkt ist der Begriff der „*verantwortlichen Stelle*“ nach § 3 Abs. 7 bzw. Art. 2 c) EU-DSRL. Dabei handelt es sich um jede Person oder Stelle, „die personenbezogene Daten für sich selbst … verarbeitet … oder dies durch andere im Auftrag vornehmen lässt“. Nach Art. 2 c) S. 1 EU-DSRL ist verantwortlich, wer „über die Zwecke und Mittel der Verarbeitung entscheidet“. Dies ist beim Cloud Computing zunächst der Cloud-Nutzer, der sich zur Nutzung entschließt und die Daten in die Cloud eingibt. Nach § 3 Abs. 7 BDSG wird die Verantwortung nicht auf den eigenen tatsächlichen Machtbereich beschränkt, sondern auch auf die Auftragsdatenverarbeitung erstreckt. In § 11 Abs. 1 S. 1 BDSG wird bekräftigt, dass bei der Auftragsdatenverarbeitung der Auftraggeber für die Einhaltung der Vorschriften über den Datenschutz verantwortlich ist. Dies bedeutet: Durch die Beauftragung und Einschaltung Dritter kann sich eine Stelle ihrer Verantwortung nicht entziehen. Wohl aber ist es möglich, dass hierdurch zusätzliche Verantwortlichkeiten bei der dritten Stelle entstehen.

Gegenstand der Verantwortlichkeit ist zunächst die materiell-rechtliche Zulässigkeit der Verarbeitung. Diese kann verwaltungs-, zivil- und strafrechtliche Implikationen haben. Die verantwortliche Stelle ist Adressat von Verfügungen der Aufsichtsbehörde nach § 38 BDSG, von privatrechtlichen Betroffenenansprüchen, z.B. auf Auskunft, Löschung, Berichtigung oder Schadenersatz, sowie von strafrechtlichen oder Bußgeld-Sanktionen (z.B. nach den §§ 43, 44 BDSG).

6. Abgrenzung Funktionsübertragung – Auftragsdatenverarbeitung

Nach Art. 17 Abs. 2 EU-DSRL regeln die Mitgliedstaaten, „dass der für die Verarbeitung Verantwortliche im Fall einer *Verarbeitung in seinem Auftrag* einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen.“ Die Auftragsdatenverarbeitung ist national in § 11 BDSG normiert.

Keine Auftragsdatenverarbeitung ist gegeben, wenn ein Empfänger ein Dritter ist. Dies ist nach § 3 Abs. 8 S. 2 BDSG jede Stelle außerhalb des Inlands bzw. *außerhalb eines Mitgliedstaates der Europäischen Union* (EU) oder des Europäischen Wirtschaftsraumes (EWR). In diesem Fall kann die Privilegierung der Datenverarbeitung nach § 11 BDSG nicht in Anspruch genommen werden. Vielmehr müssen die rechtlichen Voraussetzungen für eine Datenübermittlung (§ 3 Abs. 4 Nr. 4 BDSG) gegeben sein. Der Gesetzgeber unterstellt, dass bei derartigen Übermittlungs-Konstellationen, wie sie beim Cloud Computing üblich sind, besondere persönlichkeitsrechtliche Risiken entstehen, weil von der verantwortlichen Stelle, vom Betroffenen oder von den staatlichen Aufsichtsbehörden keine hinreichende Kontrolle der Datenverarbeitung möglich ist.

6.1 Auftragsdatenverarbeitung

Cloud Computing ist aus technischer Sicht *klassische Auftragsdatenverarbeitung*, wie sie in § 11 BDSG geregelt ist. Der Auftraggeber, d.h. der Cloud-Nutzer, soll vollständig über die Art und Weise der Datenverarbeitung bestimmen. Cloud- und Ressourcen-Anbieter erfüllen reine Hilfs- und Unterstützungsfunktionen und sind – idealtypisch – völlig von den Vorgaben der verantwortlichen Stelle abhängig. Der Auftraggeber bleibt für die Sicherstellung der Vertraulichkeit und Integrität der Daten verantwortlich. Dieser Verantwortung kann er auf der Basis der etablierten

Cloud-Strukturen im Allgemeinen nicht gerecht werden, bei denen Dienste angeboten werden, zu denen die Dienstleister gegenüber dem Cloud-Nutzer keine Auskunft geben zur Art und zum Ort der Verarbeitung und zu den Sicherungsmaßnahmen. Dem gegenüber ist an eine datenschutzgerechte Datenverarbeitung in der Cloud vorstellbar, wenn dem Cloud-Nutzer als verantwortliche Stelle umfassende Transparenz über diese Rahmenbedingungen und Wahlmöglichkeiten gewährt werden.

Bei einer klassischen Auftragsdatenverarbeitung muss sich der Auftraggeber umfassend darüber vergewissern, dass die technisch-organisatorischen Maßnahmen wie die materiellen Vorgaben des Auftragnehmers beachtet werden. Der damit verbundene Aufwand ist aber genau das, wovon sich die verantwortlichen Stellen durch die Nutzung der Cloud entledigen wollen. Diese *Entledigung von Kontrollen und Weisungen* können nur durch zwei Vorgehensweisen akzeptiert werden: 1. die verbindliche Zusage des Auftragnehmers in Form einer umfassenden Selbstbindung und 2. die Übertragung der Kontrolle, ob diese Pflichten beachtet werden, an eine unabhängige und kompetente Stelle. Dies kann in der Form erfolgen, dass sich sämtliche Anbieter bestimmten externen Audits oder Zertifizierungen unterwerfen.

6.2 Funktionsübertragung

Die Anforderungen an eine Funktionsübertragung sind weitergehend. Die Datenschutzgesetze gehen davon aus, dass der Übermittlungsempfänger von Daten selbst für die weitere Verarbeitung verantwortlich ist. Dies können aber beim Cloud Computing die Cloud- und Ressourcen-Anbieter nicht gewährleisten, da diese von der konkreten Datenverarbeitung im Idealfall nichts bewusst mitbekommen und mitbekommen sollen. Andererseits sind die Cloud-Nutzer verpflichtet, die Übermittlungsanforderungen jedes einzelnen Datums zu sichern.

Hierzu gehört zunächst, dass an der Übermittlung in die Cloud ein vertragliches oder sonstiges berechtigtes Interesse besteht und diese Übermittlung erforderlich ist (§ 28 Abs. 1 S. 1 Nr. 1, 2 BDSG). Besteht zwischen dem Cloud-Nutzer und dem Betroffenen eine vertragliche Beziehung, so kann diese sich auch auf die Cloud-Verarbeitung erstrecken. Ist dies nicht ausdrücklich geregelt, so muss die Cloudnutzung „erforderlich“ sein. Spätestens am Erforderlichkeitskriterium, das die „Dienlichkeit“ seit dem 01.09.2009 ablöste, scheitert jede Cloud-Übermittlung: Es ist wohl nicht begründbar, dass die Nutzung einer Cloud mit Verarbeitern außerhalb des EU/EWR-Raumes zwingend ist. Es ist kaum zu widerlegen, dass es auch adäquate Cloud-Angebote innerhalb Europas gibt. Allein der Umstand, dass Cloud-Angebote mit Einbindung von Anbietern außerhalb des EU/EWR-Raumes möglicherweise etwas kostengünstiger sind, genügt für die Erforderlichkeit i.S.d. § 28 BDSG nicht.

Besteht zwischen Cloud-Nutzer und Betroffenen keine Vertragsbeziehung, so muss der Cloud-Nutzer zur Legitimation einer Funktionsübertragung ein berechtigtes Interesse geltend machen können. Wieder ist fraglich, ob allein das Kostensparinteresse des Cloud-Nutzers ein berechtigtes Interesse begründet. Dies mag allenfalls dann der Fall sein, wenn diese Ersparnis erheblich ist.

Darüber hinausgehend müssten die schutzwürdigen Interessen der Betroffenen adäquat gesichert werden (§ 28 Abs. 1 S. 1 Nr. 2 BDSG). Die schutzwürdigen Interessen können durch Maßnahmen gewährleistet werden, die in § 11 BDSG vorgesehen sind. Diese Anforderungen sind lediglich die Grundlage zur Wahrung der Betroffeneninteressen. Sie genügen aber nicht zur Kompensation der Aufgabe der rechtlichen Verantwortlichkeit durch den Cloud-Nutzer im Fall einer Funktionsübertragung. Hierfür ist eine weitergehende Bindung der Übermittlungsempfänger nötig,

die einen Ausgleich für den Umstand schafft, dass die datenschutzrechtliche Verantwortung vom Cloud-Nutzer auf den Cloud- und Ressourcen-Anbieter übergeht. Diese Kompensation kann in der Verabredung empfindlicher Vertragsstrafen für eine nicht weisungsgemäße, insbesondere in Form einer zweckwidrigen Datenverarbeitung, gesehen werden und in der Einräumung von Weisungs-, Kontroll- und Betroffenenrechten, die über die einer einfachen Auftragsdatenverarbeitung hinausgehen.

Zusätzlich zu diesen generell für Datenübermittlungen geltenden Anforderungen müssen bei Cloud-*Übermittlungen ins Drittausland*, also außerhalb des EU/EWR-Raumes die Voraussetzungen der §§ b, 4c BDSG gegeben sein.

7. Problem: Drittzugriff

7.1 Legale Zugriffsmöglichkeiten Dritter

Durch die Verlagerung des Ortes der Datenverarbeitung in einen anderen Staat ergibt sich, dass Dritte, die keine Cloud- oder Ressourcen-Anbieter sind, in diesem Staat möglicherweise tatsächlich und evtl. auch auf rechtlicher Grundlage Zugriff auf diese Daten nehmen (dürfen). Dies gilt vorrangig für die *Behörden der „inneren Sicherheit"*, also Polizei, sonstige Strafverfolgungsbehörden, nationale Geheimdienste, oder Finanzbehörden. Es ist nicht auszuschließen, dass das nationale Recht, etwa wegen eines völligen Fehlens von Datenschutzrestriktionen, sogar den Zugriff durch private Dritte erlaubt. Je niedriger das Datenschutzniveau in dem Staat ist, in dem die Datenverarbeitung tatsächlich stattfindet, desto größer ist die Gefährdung der Betroffeneninteressen durch die Cloud-Datenverarbeitung. Die Motivation für derartige legale Zugriffe muss nicht in der Gefahrenabwehr oder der Ermittlung von kriminellen Handlungen liegen. So gehört es zu den rechtlichen Aufgaben und Befugnissen vieler nationaler Geheimdienste, für die heimischen Interessen Wirtschaftsspionage zu betreiben. Dies kann in keinem Fall im Interesse des Cloud-Nutzers und sollte auch nicht in dem der Cloud- und Ressourcen-Anbieter liegen, lässt sich aber rechtlich nicht und faktisch nur schwer verhindern.

Denkbare Bedarfsträger an Cloud-Daten im öffentlichen Bereich sind neben den klassischen Sicherheitsbehörden *Finanzbehörden*, die z.B. über den Zugriff auf Bankdaten Erkenntnisse zur Steuerhinterziehung und zum Steuerbetrug zu erlangen versuchen. Eine andere Bedarfslage kann sich für Aufenthalts-, Asyl- und Einwanderungsbehörden ergeben, bei denen Erkenntnisse aus dem Heimatstaat von hoher Relevanz sind, wofür Clouds eine Quelle sein können.

Besonders problematisch wird der tatsächliche und der rechtlich erlaubte Zugriff, wenn eine Datenverarbeitung in einem Staat erfolgt, die nicht nur keinen hinreichenden Datenschutz gewährleisten kann, sondern darüber hinausgehend bewusst und gezielt Menschenrechte ignoriert und Rechtsschutz verweigert, der Menschen politisch, ethnisch, religiös, wirtschaftlich oder aus anderen Gründen verfolgt. So können staatliche Zugriffe auf Cloud-Rechner durch staatliche oder halbstaatliche Einrichtungen in *Diktaturen* wie z.B. dem Iran oder China Informationen offenbaren, die zur Grundlage von weiterer Überwachung, Verfolgung, Verhaftung, bis hin zur Tötung genommen werden.

Der legale Zugriff auf Cloud-Daten kann u.U. durch *technische Vorkehrungen* verhindert werden. Eine Pseudonymisierung kann eine Auswertung verhindern, wenn die Daten erlangenden Bedarfsträger keinen Zugang zu den Zuordnungsmerkmalen haben. Entsprechendes gilt für die Verschlüsselung von Daten, wenn keine Entschlüsselungsmöglichkeiten bestehen, oder für die Verarbeitung in virtuellen Räumen, zu denen die Bedarfsträger faktisch keinen lesenden Zugriff

nehmen können.

Berücksichtigt werden muss, dass es in vielen Staaten rechtliche Regelungen gibt, mit denen die Datenverarbeiter, also hier die Cloud- und Ressourcenanbieter unter Androhung staatlicher Sanktionen verpflichtet werden können, Schutzvorkehrungen gegen unberechtigten Zugriff entweder völlig zu unterlassen oder auf behördliche Aufforderung aufzuheben. So gibt es selbst in westlichen demokratischen Staaten gesetzliche Regelungen zur *Herausgabepflicht von Schlüsseln* zur Entschlüsselung behördlicher geforderter Daten. Berücksichtigt werden muss weiterhin, dass es insbesondere im Sicherheitsbereich in fast allen Staaten behördliche Befugnisse gibt, technische Sicherungsvorkehrungen zu überwinden.

7.2 Illegale Zugriffsmöglichkeiten in der Cloud

Je nach den vorgesehenen und umgesetzten Sicherheitsvorkehrungen besteht zudem ein Angriffsrisiko durch *unberechtigte Dritte* auf die von Cloud-Nutzern verarbeiteten Daten. Ist die verantwortliche Stelle bei eigener Verarbeitung bzgl. der IT-Sicherheit des eigenen Glückes Schmidt, so verliert sie beim Cloud Computing regelmäßig völlig die Herrschaft über die Sicherheitsmaßnahmen. Datensicherheit ist regelmäßig ein Bestandteil des Serviceangebots.

Denkbar sind *Beeinträchtigungen sämtlicher Schutzziele* technisch-organisatorischer Datensicherheitsmaßnahmen, also der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Transparenz für die Berechtigten, der Revisionssicherheit oder der Unverknüpfbarkeit der verarbeiteten Daten.

Ein besonderes Risiko besteht darin, dass über die Cloud völlig neue *Angriffsmöglichkeiten von Cyberkriminellen* eröffnet werden. Diese können die schwächste Sicherheitsstelle der Cloud nutzen, um in diese einzudringen. Da die Cloud- und Ressourcenanbieter kein eigenes Interesse an der Datenverarbeitung, sondern nur an deren Vergütung haben, ist es Kriminellen u.U. leicht möglich, unerkannt in die Rolle des Nutzenden zu schlüpfen, um die Datenverarbeitung auszuspionieren und/oder zu sabotieren.

Unberechtigte Zugriffe können durch *technisch-organisatorische Maßnahmen*, wie sie in § 9 BDSG und Art. 17 Abs. 1 EU-DSRL obligatorisch vorgesehen sind, eingeschränkt oder gar vermieden werden. Zu beachten ist aber, dass die gesetzliche Verpflichtung zu derartigen Vorkehrungen nur bei Cloud- und Ressourcenanbietern im EU/EWR-Raum besteht. Dessen ungeachtet bestehen auch hier oft große Umsetzungsdefizite. Während jedoch gegen legale Zugriffsrechte auf Cloud-Daten keine vertraglichen Absprachen zwischen Nutzer und Cloud-Anbieter helfen, können gegen ungesetzliche Zugriffe vertraglich umfassende und wirksame Sicherungsmaßnahmen verabredet werden.

8. Beschränkte Datenschutzkontrolle

Bei einer Tatbegehung von Datenschutzverstößen in der Cloud außerhalb des deutschen Territoriums werden die gesetzlichen und faktischen Ermittlungsmöglichkeiten nach deutschem Recht regelmäßig fehlen. Rechtlich ist die Datenschutzkontrolle der Aufsichtsbehörden in den Bundesländern auf das jeweilige Landesterritorium beschränkt. Innerhalb der EU bzw. dem EWR kann eine gegenseitige Amtshilfe der Aufsichtsbehörden erfolgen, die bisher jedoch wegen des damit verbundenen Aufwandes nur im Einzelfall praktisch durchgeführt wird. Anlasslose Kontrollen, wie sie in § 38 Abs. 1 S. 1 BDSG und Art. 28 Abs. 3 EU-DSRL vorgesehen sind, sind als koordinierte oder gemeinsame Kontrollen in Clouds mit Drittauslandsbezug praktisch nicht

möglich. Aber selbst innerhalb der EU und des EWR gibt es für solche grds. mögliche Kontrollen keine Beispiele. Dies führt dazu, dass verantwortliche Stellen, die sich *Datenschutzkontrollen entziehen* wollen, gezielt Clouds nutzen können. Dies gilt insbesondere für Verarbeitungen im Drittausland, also außerhalb des EU/EWR-Raumes, da hier jede Kontrolle von der vertraglichen Einräumung von Kontrollrechten durch die Cloud- und Ressourcenanbieter abhängt, die vom Cloud-Nutzer durchgesetzt werden müsste, der i.d.R. selbst kein Interesse an der Datenschutzkontrolle hat.

Datenschutzverstöße können zugleich auch *Straftatbestände* erfüllen, so dass strafrechtliche Ermittlungen nach der StPO möglich sind. Dem Problem der Ermittlungserschwernis durch externe Datenverarbeitung wurde strafprozessual mit der Einfügung eines neuen § 110 Abs. 3 StPO in einem gewissen Maße Rechnung getragen, der den Zugriff auf externe Speichermedien eröffnet.

9. Mindestanforderung Auftragsdatenverarbeitung

Die rechtlichen Mindestanforderungen für jede Cloud-Anwendung ist die Beachtung der Regelungen zur Auftragsdatenverarbeitung. Dies gilt selbst im Fall einer Funktionsübertragung, da durch den Umstand, dass eine Verarbeitung im Drittausland erfolgt, keine Absenkung des Datenschutzniveaus für die Betroffenen erfolgen darf.

Die Anforderungen an eine Auftragsdatenverarbeitung wurden mit Wirkung vom 01.01.2009 in § 11 Abs. 2 BDSG konkretisiert. In einem schriftlichen Auftrag, also einem zivilrechtlichen Vertrag, sind präzise festzulegen: 1. Gegenstand und Dauer des Auftrags, 2. Umfang, Art und Zweck der Verarbeitung, Art der Daten und Kreis der Betroffenen, 3. die Datensicherungsmaßnahmen nach § 9 BDSG, 4. Berichtigung, Löschung und Sperrung der Daten, 5. die (Kontroll-)Pflichten der Auftragnehmer (AN), 6. Unterauftragsverhältnisse, 7. Kontrollrechte der Auftraggeber (AG), 8. Mitteilungspflichten der AN bei Verstößen, 9. Weisungsbefugnisse und 10. Datenlöschung beim AN. Nach § 11 Abs. 2 S. 4, 5 BDSG muss sich der AG regelmäßig über die Beachtung der Datensicherungsmaßnahmen überzeugen, was zu dokumentieren ist.

Gemäß § 11 Abs. 2 S. 1 ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen *sorgfältig auszuwählen*. Dies gilt nicht nur für den Cloud-Anbieter als erster Auftragnehmer, sondern auch für die Ressourcenanbieter als Unterauftragnehmer i.S.v. § 11 Abs. 2 Nr. 6 BDSG. Der Auftraggeber hat sich nach § 11 Abs. 2 S. 4 BDSG vor dem Beginn der Verarbeitung insofern zu vergewissern. Dies ist dem Cloud-Nutzer nur möglich, wenn er sämtliche an der Verarbeitung beteiligten Stellen kennt. Da es ihm faktisch nicht selbst möglich ist, die Zuverlässigkeit sämtlicher Cloud-Teilnehmer und die dortige Datensicherheit zu überprüfen, muss er sich auf externe Prüfungen verlassen (können). In einer Selbstzertifizierung kann keine zuverlässige Prüfung gesehen werden. Mindestvoraussetzungen sind, dass eine externe Überprüfung durch eine unabhängige Stelle erfolgt, die einen Prüfbericht vorlegt, der vom Cloud-Nutzer kontrolliert werden kann. Wegen der Vielzahl der möglicherweise vorhandenen Cloud-Beteiligten muss der Nutzer angezeigt bekommen, bei welchen Anbietern derzeit eine Verarbeitung konkret erfolgt. Anderenfalls kann der Nutzer seinen Aufgaben als verantwortliche Stelle nicht nachkommen.

Es sollte sich von selbst verstehen, dass bei der Benennung der technisch-organisatorischen Maßnahmen nicht nur die abstrakte Methode oder das Schutzziel benannt werden müssen, sondern das *konkret genutzte Sicherungsmittel* (Abs. 2 S. 2 Nr. 3). Dies gilt auch für die Kontrollmaßnahmen nach Abs. 2 Nr. 5, die vom Cloud-Anbieter gegenüber den Ressourcenanbietern durchgeführt werden müssen. Dazu gehört, dass die Anbieter vertraglich

verpflichtet werden müssen, spezielle Überprüfungen auf ungewöhnliche oder unzulässige Aktivitäten hin zuzulassen und tatsächlich durchzuführen. Auf Initiative des Nutzers muss die eine konkrete Verarbeitungskontrolle möglich sein, also ein Zugriff auf die jeweiligen Protokolldaten.

Im Auftrag müssen die Voraussetzungen und Verfahren bei *unerwarteten bzw. unzulässigen Verarbeitungen* festgelegt werden: Bei welchen Vorfällen muss eine Information des Nutzers unaufgefordert stattfinden? Hierbei ist die Regelung des § 42a BDSG zu berücksichtigen, die den Nutzer als verantwortliche Stelle verpflichtet; diese Verpflichtung ist an den Auftragnehmer weiterzugeben.

Wegen des standardisierten Vorgehens ist bei Cloud-Anwendungen i.d.R. de facto das Erteilung von Weisungen des Nutzers nicht umsetzbar. Dies muss kompensiert werden durch O*ptionsangebote*, die dem Nutzer die Auswahl bestimmter Ressourcen, Orte (Länder), Sicherheitsniveaus sowie sonstiger Anbieter- und Nutzungsmerkmale eröffnet. Dies ist in jedem Fall nötig, wenn an die konkrete Verarbeitung zusätzliche rechtliche Anforderungen gestellt werden, so wie dies z.B. bei besonderen Datenkategorien nach § 3 Abs. 9 BDSG, bei Daten von Finanzdienstleistern (§ 25a KWG), bei Sozialgeheimnissen (§ 80 SGB X) oder bei besonderen Berufs- und Dienstgeheimnissen der Fall ist.Bei der Verarbeitung von sensitiven Daten können diesen Kennungen beigefügt werden, die das Verarbeitungsregime in der Cloud bestimmen. Dies muss in den vertraglich zugesicherten Sicherheitspolicies aufgenommen werden.

Regelungsbedürftig ist die *Haftung* der Cloud- und Ressourcen-Anbieter gegenüber den Nutzern. Durch die Verarbeitung in der Cloud können sowohl direkt Schäden für den Nutzer entstehen wie auch persönlichkeitsrechtliche Schäden der von der Datenverarbeitung Betroffenen, die diese nach § 7 BDSG oder nach den §§ 823, 847 BGB gegenüber dem Nutzer geltend machen können. Die Haftungsregelung des Cloud-Vertrages sollte sicherstellen, dass alle vom Nutzer nicht zu vertretende Schäden vom Cloud-Anbieter übernommen werden. Wegen der Ubiquität des möglichen Schadenseintrittsortes und der Ressourcen-Anbieter ist dringend zu empfehlen, zwischen Anbieter und Nutzer im Vertrag eine Festlegung des anwendbaren Rechtes und des Gerichtsortes vorzunehmen.

Bei längerfristigen Cloud-Verarbeitung muss geklärt werden, was mit den gespeicherten Daten passiert, wenn ein *Cloud- oder Ressourcenanbieter insolvent* wird oder von einem anderen Unternehmen übernommen wird. Nach Abschluss der Verarbeitung müssen die verarbeiteten Daten gelöscht werden. Es bedarf noch einer vertieften Untersuchung, welche Protokolldaten für welche Zeit aufbewahrt werden müssen und dürfen. Auch dies ist im Auftrag festzulegen.

Nicht zuletzt muss im Vertrag gewährleistet werden, dass im Fall einer *Datenschutzkontrolle* nach § 38 BDSG diese ungehindert durchgeführt werden kann und im Fall der Wahrnehmung von Betroffenenrechten (§§ 33 ff. BDSG) diese uneingeschränkt in Anspruch genommen bzw. umgesetzt werden können.

10. Technisch-organisatorische Lösungen

Die technischen und organisatorischen Maßnahmen der Datensicherung nach § 9 BDSG bzw. Art. 17 Abs. 1 EU-DSRL müssen dem Nutzer offengelegt werden und sind gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG ausdrücklich im Vertrag zu benennen. Es kann also nicht das Prinzip „*security by obscurity*“ - Sicherheit durch Geheimhaltung - gelten, so wie dies heute weitgehend praktiziert wird. Symptomatisch hierfür ist die Darstellung des Google-Managers Kai Gutzeit – Chef für Clouddienste in Mittel- und Nordeuropa – zur von seinem Unternehmen erbrachten

Datensicherheit. Diese sei zunächst eine Frage des Vertrauens, das heutzutage ja auch der Kreditkarte und den Banken entgegengebracht würde. Sollte aber jemand tatsächlich in die streng geheimen Google-Rechenzentren eindringen, so fände der Einbrecher „gar nichts“ Verwertbares, nämlich nur „bedeutungslose Bits und Bytes“, da Google eigene Dateisysteme verwende.

Gefordert ist vielmehr „*security by transparency*“. Die Maßnahmen müssen dem Stand der Technik entsprechen. Im Rahmen der vorliegenden rechtlichen Darstellung können die nötigen technisch-organisatorischen Vorkehrungen nicht erschöpfend dargestellt werden. Zwingend ist, dass die Zugriffsmöglichkeiten auf die verarbeiteten Daten, evtl. abgesehen von administrativen Rechten, technisch beschränkt werden auf die vom Nutzer genannten Berechtigten. Hierzu sind ein differenziertes Zugriffsregime, Verschlüsselungsmöglichkeiten und evtl. Pseudonymisierungswerkzeuge geeignet.

Cloud Computing bedeutet, dass mehrere Nutzende auf den gleichen Rechnern und Plattformen arbeiten. Dadurch entstehen Risiken, sie sich aus einer nicht hinreichenden Trennung der gespeicherten Daten ergeben. Der Cloud-Auftrag muss zur Absicherung der *Abschottung der einzelnen Auftragsverhältnisse* voneinander die Methoden zur Trennung der Daten unterschiedlicher Auftraggeber präzise benennen. Erfolgt dies durch Verschlüsselung, so muss geprüft werden, ob die genutzten Systeme eine hinreichende Sicherheit bieten und nicht durch andere Nutzende oder durch die Anbieter selbst einfach kompromittert werden können.

Dem Nutzer sind mit einer praktikablen Nutzeroberfläche die schon genannten Optionsmöglichkeiten zu eröffnen und die nötigen Hilfen zur Umsetzung der *nutzerseitigen Anwendungssicherheit*.

Es bedarf beim Cloud-Anbieter und im Cloud-Verbund eines *dokumentierten Datenschutzmanagements*, zu dem ein IT-Sicherheitsmanagement und ein Vorfallmanagement gehört.Auf die Notwendigkeit einer transparenten Auditierung durch eine unabhängige Stelle wurde schon hingewiesen. Eine solche Auditierung ist leider bisher nur in engen Grenzen gesetzlich geregelt (z.B.§§ 4 Abs. 2, 43 Abs. 2 LDSG SH). Die Umsetzung des § 9a BDSG lässt weiter auf sich warten.

11. Außereuropäische Clouds

Werden Stellen außerhalb der Europäischen Union mit einbezogen, so sind Clouds wegen der damit zwangsläufig erfolgenden Datenübermittlung, für die es *keine datenschutzgesetzliche Legitimation* gibt, grundsätzlich unzulässig.

Ein weitgehend freier Datenfluss in Staaten außerhalb des EU/EWR-Raumes ist aber evtl. möglich, wenn in den Drittstaaten ein *angemessenes Datenschutzniveau* besteht (§ 4b Abs. 2, 3 BDSG). Dies wurde für bestimmte Staaten durch die EU-Kommission festgestellt, z.B. für die Schweiz, Kanada oder Argentinien. Die Feststellung der Angemessenheit des Datenschutzniveaus in einem außereuropäischen Staat hat jedoch nicht zur Folge, dass Stellen dort rechtlich als Auftragnehmer gemäß § 11 BDSG behandelt werden können. Sie bleiben Dritte mit der Folge, dass eine Datenweitergabe als Übermittlung zu kennzeichnen ist.

Da die Datenverarbeitungen im Rahmen einer Cloud nicht dem Übermittlungserfordernis der Erforderlichkeit nach § 28 BDSG genügen können und in jedem Fall als Auftragsdatenverarbeitung durchgeführt werden müssen, bleiben Clouds mit außereuropäischen Anbietern datenschutzrechtlich unzulässig. Dies hat dazu geführt, dass einzelne Cloud-Anbieter den Nutzern

die Möglichkeit einräumen, eine Datenverarbeitung *ausschließlich innerhalb des EU/EWR-Raumes* durchführen zu lassen.

Dieses Ergebnis lässt sich nur dadurch vermeiden, dass man eine ungewollte Regelungslücke annimmt und die Regelungen der Auftragsdatenverarbeitung analog anwendet. Die EU-Kommission hat mit Entscheidung vom 27.12.2001 spezielle Standardvertragsklauseln für die Auftragsvergabe in Drittstaaten festgelegt, die die Einhaltung ausreichender Garantien beim Auftragnehmer gemäß Art. 26 Abs. 2 EU-DSRL sicherstellen sollen. Dies bedeutet, dass neben dem Abschluss eines *EU-Standardvertrages* den verbindlichen Vorgaben des § 11 BDSG vollständig genügt werden muss.

Allein die Selbstzertifizierung von US-Unternehmen zu *Safe Harbor* genügt in keinem Fall, um ein den EU-Standards entsprechendes Datenschutzniveau zu erreichen. Auch Cloud-Verträge, die sich an „Safe-Harbor"-Maßstäben orientieren, sind unzureichend. Diese Maßstäbe dienten der Schaffung einer tragfähigen Brücke zwischen den strengen europäischen Datenschutzregeln und dem in vieler Hinsicht nicht existierenden Datenschutzniveau in den USA. Zielsetzung des Safe Harbors war es, eine praktikable Lösung für die zwangsläufig zwischen den USA und Europa notwendigen Datenübermittlungen zu schaffen. Keinesfalls kann aber Safe Harbor dazu dienen, die strengeren Datenschutzvorschriften in Europa zu umgehen, so wie dies beim Cloud Computing der Fall wäre.

Cloud-Anbieter wie Google oder Salesforce mit Sitz in den USA weisen sich zwecks Nachweis ihrer Vertrauenswürdigkeit mit einem *SAS-70-Typ-II Zertifikat* aus. Dies bedeutet, dass die Datenzentren durch unabhängige Dritte kontrolliert werden sollen. Diese Maßnahme genügt nur teilweise den Anforderungen der Auftragsdatenverarbeitung. Sie berücksichtigt z.B. nicht die materiellen und prozeduralen Betroffeneninteressen bei Übermittlungen.

Möglich ist auch, dass sich die an einer Cloud beteiligten Unternehmen verbindlichen Unternehmensregeln (sog. *Binding Corporate Rules* – BCRs) geben und unterwerfen, wodurch ein angemessenes Schutzniveau nach Art. 26 Abs. 2 EU-DSRL bzw. § 4c Abs. 2 BDSG per Vertrag hergestellt werden soll. Dieses zunächst für internationale Konzerndatenverarbeitung entwickelte rechtliche Instrumentarium lässt sich auf die Cloud- und Ressourcenanbieter übertragen. Nach den Empfehlungen der Art.-29-Datenschutzgruppe in der EU muss im Rahmen von BCR die Hauptniederlassung oder ein von der Unternehmensgruppe benanntes Gruppenmitglied für die Verstöße aller verbundenen Unternehmen außerhalb der EU einstehen. Diese BCRs bedürfen der Genehmigung durch die zuständigen Datenschutzaufsichtsbehörden.

12. Diskussionsstand

Clouds werden auf dem globalen Markt angeboten und werden auch von deutschen Unternehmen sowie auch von Privatnutzenden bei der Verarbeitung personenbezogener Daten genutzt. Diese Form der Datenverarbeitung erfolgt weitestgehend im Verborgenen für die Betroffenen, die Aufsichtsbehörden und die Öffentlichkeit. Dass über konkrete Anwendungen - außer Werbeveröffentlichungen und informationstechnische Darstellungen - nichts bekannt wird, ist kein Hinweis darauf, dass keine Datenschutzverstöße und Persönlichkeitsverletzungen stattfänden. Keiner der direkt Beteiligten – Nutzende, Cloud-Anbieter sowie Ressourcenanbieter – hat ein zunächst ein Interesse daran, dass Verstöße bekannt werden. Angesichts der öffentlich zugänglichen Informationen und der Rechtslage muss davon ausgegangen werden, dass heute bei sehr vielen Cloud-Anwendungen strukturell Datenschutzrechtsverstöße angelegt sind und auch massenhaft erfolgen.

Soweit ersichtlich, werden Cloud-Anwendungen – noch – nicht von *öffentlichen Stellen* in Deutschland genutzt. Wohl aber ist bekannt, dass auch öffentliche Stellen angesichts des Zwangs zur Kosteneinsparung diese Möglichkeiten erwägen und prüfen. Bei Großunternehmen ist sowohl wegen der eigenen vorhandenen Ressourcen wie auch aus Gründen des Schutzes des eigenen Daten die Nutzung offensichtlich noch begrenzt auf private oder zumindest akribisch ausgewählte Clouds. Das Hauptanwendungsfeld des kommerziellen Cloud Computing dürfte derzeit bei mittleren und kleinen Unternehmen mit begrenzten Rechenkapazitäten und begrenztem rechtlichen und technischen Know-how liegen.

Zwar ist den Anbietern die Notwendigkeit von Vertraulichkeit und Integrität bewusst, aber nur aus Gründen der *Marktpositionierung*, nicht aus Gründen des Grundrechtsschutzes oder wegen der Notwendigkeit der Beachtung des Datenschutzrechtes. Cloud Computing ist ein weiteres Beispiel dafür, dass im Markt zunächst das praktisch gemacht wird, was technisch und ökonomisch möglich ist und sinnvoll erscheint. Erst durch öffentliche Skandalisierung und durch staatliche Kontrollen ist eine zunehmende Orientierung an den rechtlichen Vorgaben zu erwarten. Hierfür sind auch bisherige juristische Publikationen ein Indiz, deren Ausgangspunkt die Macht des Faktischen ist und eine Anpassung des Rechtes hieran fordern oder behaupten. Dabei werden die persönlichkeitsrechtlichen Konsequenzen entweder überhaupt nicht angesprochen oder verharmlost.

13. Handlungsbedarf

Auf internationaler Ebene hat sich die US-dominierte Cloud Security Alliance (CSA) gebildet, deren Ziel es ist, Richtlinien für ein sicheres Cloud Computing zu erarbeiten. **Mit EuroCloud Deutschland_eco** gibt es seit Kurzem einen *Verband der deutschen Cloud Computing-Industrie*, der in das europäischen EuroCloud-Netzwerk eingebunden ist. EuroCloud Deutschland_eco hat sich zur Aufgabe gemacht, mehr Transparenz für die Anwendenden zu schaffen, ein Gütesiegel einzuführen, Rechtsfragen zu klären, den Dialog zwischen Anbietern und Nutzern zu fördern und Cloud Computing-Kompetenz zu vermitteln.

Versteht man Datenschutz als digitalen Grundrechts- und Menschenrechtsschutz, so ist dieser keine länderspezifische Diskriminierung von Cloud-Anbieter, kein Marktverzerrer und kein Technikhindernis, sondern vielmehr „*Cloud-Enabler*“. Ohne die Gewährleistung des nötigen Schutzniveaus ist ein professioneller Einsatz dieser Systeme nicht verantwortbar.

Durch *internationale Regelungen* wäre es zweifellos möglich, für das Cloud-Computing die Ortsabhängigkeit von Datenverarbeitung bei dieser Art der Verarbeitung aufzuheben und ausschließlich das Regime des Cloud-Nutzers oder des direkten Vertragspartners des Nutzers als Cloud-Anbieter für anwendbar zu erklären. In diese Richtung sind aber Bestrebungen bisher nicht ersichtlich. Angesichts der uneinheitlichen und teilweise fehlenden und unzureichenden nationalen Rechtsregeln für Datenverarbeitung allgemein und für den Datenschutz speziell sind internationale Normen derzeit noch nicht realistisch. Daher gibt es keine Alternative zur Durchsetzung eines klaren rechtlichen Schutzregimes, das bei der verantwortlichen Stelle, also dem Cloud-Nutzer, ansetzt.

Dafür ist zunächst nötig, eine *objektive Bestandsaufnahme* vorzunehmen. Markttransparenz und Transparenz der auf dem Markt befindlichen Cloud-Datenverarbeitungsprozesse kann schon selbst zu einer gewissen Marktbereinigung führen und ist unabdingbare Voraussetzung für eine öffentliche Diskussion aller Betroffenen. Hierzu gehören nicht nur Nutzer und Anbieter, sondern auch die Aufsichtsbehörden, die Informationstechnik, v.a. die Forschung zur Sicherheitstechnik, der Verbraucherschutz und schließlich natürlich auch die Öffentlichkeit und die Politik.

Forschung, Wirtschaft und Aufsichtsbehörden sind aufgefordert, mit den zuständigen Organisationen *Schutzstandards*, sog. Protection Profiles für Clouds zu erarbeiten sowie Auditierungsverfahren zu entwickeln und zu etablieren. Als Vorstufe für eine internationale Regulierung können noch zu erarbeitende spezifische Standardvertragsklauseln bzw. verbindliche Unternehmensregeln (BCR, s.o. 11) dienen.

Das derzeit noch bestehende Grundprinzip der „freien Cloud“ genügt nicht den Anforderungen eines modernen Datenschutzes und kann nur als Spiel- oder Versuchsapplikation verstanden werden, aus der sich „*trusted and trustworthy Clouds*“ entwickeln, bei denen Datenschutz- und Datensicherheitsgarantien integriert sind. Diese vertrauenswürdigen Clouds müssen im Markt verfügbar gemacht werden - oder der Grundsatz des Cloud Computing kann keinen Bestand haben.

Dr. Thilo Weichert ist Landesbeauftragter für Datenschutz Schleswig-Holstein und damit Leiter des Unabhängigen Landeszentrums für Datenschutz, Kiel