„NetApp Private Storage for Cloud“ – eine Stellungnahme unter Anlegung europäischer Datenschutzstandards

Von Rechtsanwalt und Fachanwalt für IT-Recht Dr. Jens Bücking*

Die „rechtssichere“ Verfügbarhaltung von unternehmenskritischer Information stellt eine zwingende Vorbedingung der „IT-Compliance“ – unabhängig von ihrer jeweiligen Rechtsgrundlage – dar, entsprechende Verfügbarkeitsgarantien, Backup- und Archivierungsprozesse sind zur Einhaltung der jeweils einschlägigen Compliance-Standards unabdingbar.

e|s|b Rechtsanwälte

Dresden Stuttgart Berlin Leipzig Prag

NetApp®

I. Executive Summary

Eine Übermittlung von Daten in die Cloud bedarf stets einer rechtlichen Legitimation. Gerade beim Problem der Übermittlung in unsichere „Drittstaaten“, wie die USA von Seiten der EU in datenschutzrechtlicher Hinsicht eingestuft wurde, hatten die meisten Anbieter bisher hauptsächlich auf die „Safe Harbor“-Selbst-Zertifizierung gesetzt. Nachdem nun der EuGH durch Urteil vom 06.10.2015 das Aus für „Safe Harbor“ verkündet hat, entfällt die prominenteste Lösung dieses datenschutzrechtlichen Problems. Auch die Nutzung der EU-Standardvertragsklauseln ist durch die Rechtsprechung des EuGH unsicher geworden. Diese beiden Prinzipien bildeten bisher jedoch stets die Grundlage für viele namhafte Cloud-Anbieter, um eine Datenübermittlung in die USA zu ermöglichen. Um dieser Rechtsunsicherheit zu entgehen und ein angemessenes Schutzniveau zu gewährleisten, welches einfach umzusetzen ist, bleibt derzeit nur der Weg zu einer hybriden Cloud Lösung, wie NetApp sie mit „NetApp Private Storage for Cloud“ anbietet. Diese Lösung weist den Unternehmen als „Herren ihrer Daten“ einen einfachen, rechtssicheren Weg, die Vorteile der Cloud weiterhin ohne Bedenken nutzen zu können. Dabei werden die Daten im jeweiligen Land nach den dort geltenden Anforderungen gespeichert und die Compute-Leistung kann aus der Public Cloud bezogen werden.

II. Bedrohungsszenarien

Die Themen Datensicherheit und Verfügbarkeit sind sonach aus der Unternehmenswirklichkeit nicht mehr wegzudenken. Während vormals der Schutz des geistigen Eigentums und die Innovationskraft die entscheidenden Faktoren für Marktverbleib und Markterfolg waren, kommt im Zeitalter der globalen Vernetzung von Daten und Systemen vor allem die jederzeitige Verfügbarkeit von Information (Daten) hinzu. Internationale Studien belegen etwa, dass 70% der Unternehmen, bei denen es zu katastrophalen Datenverlusten kam, innerhalb von 18 Monaten aufgeben mussten. Aus der Erkenntnis heraus, dass die Verfügbarkeit von Unternehmensdaten ein „do-or-die“-Kriterium darstellt, nehmen zahlreiche nationale und internationale (Spezial-) Gesetze und Regelwerke, z.B. auf einzelstaatlicher Ebene diverse nationale Datenschutzgesetze und Gesetze über das Recht der Handelsgesellschaften, in den USA der Sarbanes Oxley Act / SoA bzw. „SOX“, auf EU-Ebene die Abschlussprüferrichtlinie „Euro-Sox“, und international „Basel / Solvency II ff.“ etc., inzwischen Unternehmen und – nach vergleichbaren Regeln – die öffentliche Hand in die Pflicht zur Implementierung eines effektiven Risiko- und Informationsmanagements. Dessen Einhaltung ist „Chefsache“ und gehört als Teil der „Corporate Governance“ zu den unternehmerischen Lenkungsaufgaben. Dies wiederum impliziert Fragen der persönlichen Haftung des Managements, der Compliance- und Sicherheitsbeauftragten und weiterer Entscheider in Schlüsselpositionen. Im Falle erheblicher Pflichtenverstöße ist überdies der Versicherungsschutz des Unternehmens und der Mitglieder des Managements gefährdet.

Es läge daher nicht nur unter betriebswirtschaftlichen Aspekten nahe, die Pflege von Daten und Systemen an zertifizierte Fachunternehmen zu vergeben bzw. bestimmte Verarbeitungsprozesse in global verfügbare Rechenzentren auszulagern. Dies erscheint indes angesichts immer neuer Horrorstatistiken über organisierte Betriebsspionage unter Risikogesichtspunkten nur noch unter engen Voraussetzungen - etwa bei zugesicherten EU/EWR-Lokationen nebst geeigneten Sicherheitszertifikaten, entsprechenden Weisungs- und Auditrechten gegenüber den Cloudanbietern etc. - vertretbar. Zuletzt nutzten zwar noch zahlreiche Unternehmen die Möglichkeit der „Safe Harbor“-Zertifizierung, um eine Datenübermittlung in die USA zu rechtfertigen. Denn die Weitergabe von Daten in die USA (als „unsicheres Drittland“ im datenschutzrechtlichen Sinne) war – abgesehen vom Erfordernis einer Rechtsgrundlage – nur zulässig, wenn bei der Empfängerstelle ein angemessenes Datenschutzniveau hergestellt wird und dies durch die entsprechende Zertifizierung bestätigt wird. Jedoch waren nach der (insoweit de facto maßgebenden) Stellungnahme der „Artikel-29-Datenschutzgruppe“ (als das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes) bereits massive Zweifel an der Effektivität von „Safe Harbor“ aufgekommen, da diese Zertifizierung in ihrer aktuellen Ausformung als per se nicht (mehr) geeignet angesehen wurde, ein angemessenes Datenschutzniveau zu gewährleisten – und daher „Safe Harbor“ auch haftungsrechtlich den „cloudsourcenden“ Unternehmen und ihren Entscheidern

keinen „Persilschein“ mehr auszustellen vermochte. Nachdem in Folge dessen auch auf der Ebene der verschiedenen nationalen Datenschutzbehörden (wie etwa in Deutschland dem „Düsseldorfer Kreis“ als führendes Gremium der Datenschutzbeauftragten des Bundes und der Länder) das „Safe Harbor“ - Prinzip als unzureichend kritisiert worden war, hat nun auch der Europäische Gerichtshof (EuGH) mit Urteil vom 06.10.2015 (C-362/14) diese Regelung zum Austausch von Daten zwischen den USA und der EU faktisch für ungültig erklärt. Die USA als „Drittland“ ohne ein dem EU-Level angemessenes Datenschutzniveau biete auch mit „Safe Harbor“ keinen ausreichenden Schutz für persönliche Daten. Derzeit sind 4410 US-Firmen nach „Safe Harbor“ zertifiziert, darunter auch die großen Cloud-Anbieter wie Microsoft, Apple, Adobe und Google.

Bei einer Datenübermittlung in die USA darf sich die für die Datenverarbeitung verantwortliche Stelle demnach ab sofort nicht mehr auf eine Selbstzertifizierung nach den „Safe Harbor“-Prinzipien verlassen sondern muss entweder die Einhaltung der Rechtmäßigkeitskriterien für jede Datenübermittlung im Einzelnen überprüfen, auf die EU-Standardvertragsklauseln zur Auftragsverarbeitung zurückgreifen oder sich gegebenenfalls konzernweit verbindliche Unternehmensdatenschutzregeln – sog. „binding corporate rules“ (BCR) – auferlegen und diese durch die zuständigen Datenschutzaufsichtsbehörden genehmigen lassen. Offen ist allerdings noch, ob die EU-Standartvertragsklauseln den strengen inhaltlichen Vorgaben, die der EuHG in seinem Urteil ebenfalls aufstellte, letztendlich standhalten werden, denn Aufsichtsbehörden können im Einzelfall Datentransfers auf dieser Grundlage untersagen, sofern die Rechte der Betroffenen nach Auffassung der Behörde nicht ausreichend gewahrt werden.

All dies scheint eine datenschutzkonforme Auslagerung von Datenverarbeitungen mit Personenbezug in die Clouds der Marktführer, die meist ausschließlich auf „Safe Harbor“ und auf die EU-Standardvertragsklauseln setzen, und bei denen es sich sämtlich um US-amerikanische Unternehmen handelt, auszuschließen. Jedoch zeigt sich der Markt der Datenmanagementlösungen innovativ. Im Fokus stehen hier namentlich Hybrid- und Multi-Cloud-Architekturen, die für sich in Anspruch nehmen, geeignete Antworten auf die aufgeworfenen Fragen zulässiger globaler Cloud-Nutzungen zu geben. Ob und unter welchen Voraussetzungen man diesem Anspruch gerecht werden kann, gilt es im Folgenden zu untersuchen:

III. Aktuelle Trends und Herausforderungen der IT

Die Auswertung von Daten zur Analyse und Implementierung in Geschäftsprozesse gehört aktuell zu den größten Herausforderungen im Bereich der IT. Klassische Enterprise-Prozesse lassen sich aufgrund immer größerer Datenmengen und Anforderungen an die Verarbeitungs- und Übertragungsgeschwindigkeit kaum mehr alleine „On Premise“ mit vertretbarem Aufwand an infrastrukturellen Ressourcen bewältigen. Die Unternehmensdaten müssen daher – unter jederzeitiger Kontrolle des insoweit verfügungsberechtigten und juristisch verantwortlichen Unternehmens als „Herr der Daten“ – in einem System gespeichert werden, das hohe Verfügbarkeit mit Ausfall- und Angriffssicherheit kombinieren kann. Für die Bereitstellung zeitgemäßer IT-Umgebungen ist der Einsatz von Cloud-Infrastrukturen daher letztlich unumgänglich.

Moderne Strategien berücksichtigen hierbei den Einsatz von Multi-Cloud-Umgebungen – dies vor dem Hintergrund, dass sich die Cloud-Anbieter in Preis, Performance und Leistungsportfolio zum Teil erheblich unterscheiden. Digitale Geschäftsprozesse fordern heute maximale Flexibilität und Skalierbarkeit hinsichtlich der Storage-Kapazitäten und Verarbeitungsgeschwindigkeiten. Gleichzeitig muss das Gesamtsystem „gehärtet“ werden, da die Bedrohung durch Cyberangriffe exponentiell wächst. Dies führt sogleich zur nächsten Bedingung, die sich aus den rechtlichen Rahmenbedingungen ergibt. Die Verteilung von Aufgaben an mehrere Cloud-Anbieter darf nicht zu einem Absinken der Kontrollmöglichkeit auf die zu verarbeitenden Daten führen. Unternehmen müssen jederzeit sicherstellen können, dass ihnen der Anbieter und seine Sub-Servicedienstleister, die Orte und die Art und Weise der Datenverarbeitung nicht nur bekannt sind sondern unter ihrer vollständigen Kontrolle liegen. Dies gilt unter haftungsrechtlichen Aspekten einerseits für personenbezogene Daten, andererseits aber auch für sonstige geschäftskritische Informationen wie bspw. das geistige Eigentum, Forschungs-/ Entwicklungsdaten, beweiserhebliche Korrespondenz usw.

Diesen Herausforderungen kann mit dem klassischen Cloud-Computing und herkömmlichen IT-Architekturen nicht mehr in effektiver Weise begegnet werden. Neben den rechtlichen Rahmenbedingungen sind es die technisch-organisatorischen Schutzmaßnahmen und eine flexible, skalierbare und jederzeit verfügbare hoch performante Systemleistung, die das Management sicherstellen und unter fortwährender – und dokumentierter – Kontrolle halten muss. Problematisch ist hierbei, dass beim klassischen Outsourcing-Modell die Daten in der Cloud gespeichert und verarbeitet werden und nicht aus der Cloud – wohin der Weg jedoch, wie noch gezeigt wird, mit Blick auf das strenge rechtliche Rahmenwerk für die Übermittlung bestimmter Datenkategorien in Clouds außerhalb des EU/EWR-Raumes führen muss. Werden Daten allerdings in die Cloud verschoben, stehen Unternehmen oftmals vor dem Problem, dass ein späterer Restore nicht mehr gewährleistet ist. Gleiches gilt für die zwingend gebotene Löschbarkeit vormals in die Cloud ausgelagerter Daten, die – unbeschadet entsprechender Zusicherungen durch den Cloud-Anbieter – oftmals de facto nicht gegeben ist.

Dies weist fast zwangsläufig den Weg hin zu hybriden und Multi-Cloud-Architekturen, bei denen bestimmte Kategorien von Daten auf einem dedizierten eigenen Storage-System, das in Nähe eines Netzknotenpunktes bei einem Co-Locator aufgestellt wird und unter vollständiger Verfügungsgewalt des Unternehmens verbleibt, vorgehalten werden. Das Unternehmen bleibt hier Herr über seine Systeme und Daten, die es in jederzeitiger Alleinverfügbarkeit und unter ständiger Funktions- und Prozesskontrolle beim Co-Locator betreibt. Die Datenverarbeitungen selbst erfolgen sodann im eigentlichen Sinne nicht in der Cloud sondern aus der Cloud heraus, was in datenschutzrechtlicher Hinsicht Anlass zu einer Neubewertung gegenüber den klassischen Modellen der Datenübermittlung und Auftragsdatenverarbeitung gibt und – wie sogleich gezeigt wird – zur Eröffnung wesentlich weiterer Spielräume für die Nutzung von globalen Clouds führen kann.

Angesichts des Personenbezugs vieler Datenkategorien hat sich der eigentliche Verarbeitungsprozess freilich auf „blinde", auf den temporären Massenspeicher der virtuellen Maschine des Cloud-Anbieters begrenzte Rechenoperationen zu beschränken. Durch die Flüchtigkeit des Speichers könnte dann gewährleistet werden, dass sämtliche Daten gelöscht werden, sobald die vom Unternehmen initiierte jeweilige Anwendung beendet ist, die virtuelle Maschine heruntergefahren wird oder technisch ausfällt. Benötigt wird daher eine Cloud-Struktur, die sich eignet für den Einsatz mit bestehenden Enterprise-Applikationen. Die Beweglichkeit der Daten, insbesondere ihre Restore-Fähigkeit – bei jederzeitiger Kontrollhoheit – muss über den gesamten Verarbeitungsprozess von der Wiege bis zum Grabe, also vom ersten „Computing-Job" aus der Cloud heraus bis zur Rückübertragung und „rückstandslosen" Löschung von den Systemen der Cloud-Anbieter sichergestellt sein und es müssen die dahingehenden Garantien der Anbieter vorliegen. Wenn diese Vorbedingungen gegeben und durch den Anbieter technisch-organisatorisch abgesichert (und im Idealfall auch versichert) werden können, stellen solche Cloud-Infrastrukturen eine sowohl unter kaufmännischen wie auch unter Performance-Kriterien echte Alternative zu On-Premise-Strukturen dar.

IV. NetApp Private Storage for Cloud

Hybride Cloud-Lösungen verbinden typischerweise eine private Cloud mit Public-Cloud-Umgebungen, wodurch die technischen Begrenzungen innerhalb der eigenen IT-Infrastruktur hinsichtlich Rechenleistung und Speicherplatz kurzfristig ausgeglichen oder ständig durch Inanspruchnahme externer Ressourcen und Services von unterschiedlichen Anbietern in einem Multi-Cloud-Modell in die Cloud hinein erweitert werden können.

Mit „NetApp Private Storage for Cloud" und der Entwicklung „Cloud ONTAP" beschreitet nun einer der führenden Anbieter von Datenmanagementlösungen den zuvor skizzierten Weg in eine hybride Multi-Cloud, aus der heraus Cloud-Ressourcen – unter gleichzeitiger Berücksichtigung der Beweglichkeit, Verfügbarkeit, Sicherheit, Vertraulichkeit und jederzeitiger Kontrollhoheit der applikationsrelevanten Daten – in Anspruch genommen werden können. Cloud ONTAP stellt ein Storage-Betriebssystem dar, das „per Mausklick" im Amazon Marketplace gebucht und als virtuelle

Appliance auf einer Amazon EC2-Instanz (virtuelle Maschine) installiert und bereitgestellt wird. Der Kunde erhält sodann einen Link auf die Konfigurationsoberfläche. Anschließend arbeitet Cloud ONTAP als Storage-Controller für das Datenmanagement innerhalb einer virtuellen Umgebung der Amazon-Cloud, die dort vom jeweiligen Unternehmen aufgebaut und betrieben wird. Die Abrechnung erfolgt minutengenau nach dem Consumption-Modell. Sämtliche Daten werden durch Cloud ONTAP verwaltet und verschlüsselt auf Amazon Elastic Blog Storage (EBS) Volumes gespeichert.

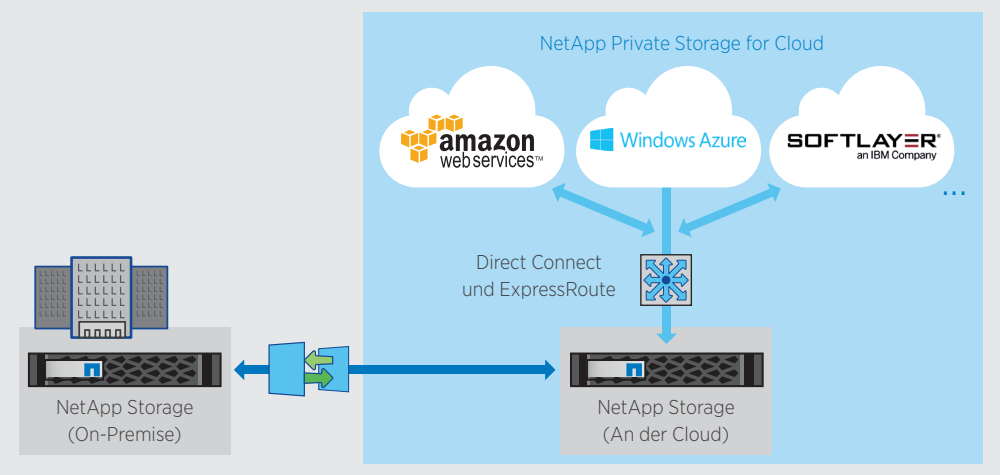

Abbildung 1: NetApp Private Storage for Cloud ermöglicht eine Hybrid-Cloud-Lösung, mit deren Hilfe Unternehmen ihre Daten nahe der Cloud vorhalten und Cloud-Ressourcen bei voller Kontrolle und Sicherheit optimal nutzen können.

Zu den von NetApp angebotenen Lösungen gehört auch die (private) „Cloud an der Cloud". Kommt etwa innerhalb der eigenen On-Premise Enterprise-Infrastruktur ein „Clustered Data Ontap" zum Einsatz, lassen sich damit bestimmte Services in die Cloud hinein erweitern. Hierzu wird in einem Co-Location-Rechenzentrum ein unter ausschließlicher Verfügungsbefugnis des Kunden befindliches Storage-System aufgestellt, auf dem die Unternehmensdaten liegen. Das Rechenzentrum befindet sich in unmittelbarer geografischer Nähe zu den Anbietern, wodurch geringst mögliche Latenzzeiten und somit hohe Zugriffsraten auf Netzwerkebene möglich werden. Zwischen dem On-Premise NetApp-System und dem beim Co-Locator aufgestellten System wird eine Datenspiegelung eingerichtet, so dass die Daten zum Co-Location System repliziert werden und dort dann an der Cloud zur Verarbeitung zur Verfügung stehen – bei entsprechend kurzen Latenzzeiten. Zwischen dem NetApp Private Storage for Cloud und den einzelnen Public-Cloud-Anbietern werden direkte IP-Verbindungen hergestellt. Hierbei handelt es sich um exklusive Datenverbindungen, die nicht über das Internet geleitet werden. Die Services und Ressourcen der Public-Cloud-Anbieter greifen damit direkt auf die Daten des NetApp Private Storage des Kunden zu. Die Verarbeitung findet statt, ohne dass die Daten in die Public-Cloud des Anbieters verschoben werden.

Derlei innovative Lösungen machen es mithin entbehrlich, die Daten zu bewegen. Diese bleiben stattdessen in einem Storage-System gespeichert, das unter uneingeschränkter, dauerhafter Kontrollhoheit des Unternehmens verbleibt. Die gebuchten Public-Cloud-Services (Rechenleistung, Applikationen und weitere „as a"-Services) greifen dann zu bestimmten – vom anwendenden Unternehmen initiierten – Zeiten für die Vornahme bestimmter Verarbeitungen auf diese Daten zu. Mit Abschluss dieses Datenverarbeitungsvorganges melden sich die Services wieder ab oder – bildlich gesprochen – ziehen sich aus den Datenbeständen, die sie sich zur Abarbeitung in den Arbeitsspeicher gezogen hatten, wieder zurück. Während der Verarbeitung wurden zwar Änderungen an den Daten vorgenommen und auf deren Basis Ergebnisse erzeugt, Auswertungen erstellt etc. Jedoch kam es zu keinem Zeitpunkt zu einer „Abwanderung" – als „Datenübermittlung" im Rechtssinne – in die Cloud hinein, da der Speicherort der Daten eben gerade nicht in die Richtung der Public-Cloud zur dauerhaften Vorhaltung angelegt wurde, sondern – gleichsam diametral – das Unternehmen sich die Cloud-Services aus der Cloud heraus ins Haus holt. Dabei wird lediglich der Vorgang des „Computing" selbst, aber keine Speicherressourcen der Cloud an sich in Anspruch genommen. Es handelt sich letztlich um Rechenjobs, durch die bestimmte Prozesse ausgelagert werden können. Die Daten bleiben hierbei freilich stets auf dem im Eigentum oder (bei Eigenbesitz-Modellen wie z.B. Miete) jedenfalls unter eigentumsgleicher ausschließlicher Verfügungsbefugnis des Unternehmens stehenden Server.

V. Datenübermittlung / Auftragsdatenverarbeitung vs. Infrastrukturerweiterung

Dies vorausgeschickt, findet keine Datenübermittlung im Rechtssinne statt und es wäre – was der NetApp-Lösung gegenüber anderen internationalen Cloud-Modellen derzeit wohl zu einer Alleinstellung verhelfen dürfte – noch nicht einmal die Konstellation der Auftragsdatenverarbeitung (ADV) gegeben:

Denn letztlich handelt es sich gleichsam um den „verlängerten Arm" der On-Premise Enterprise-Prozesse: eine externe Applikation, die ausschließlich auf die Weisung des Eigentümers (bzw. ausschließlich Verfügungsberechtigten) und „Herren über seine Daten", also nach europarechtlicher Diktion des „für die Verarbeitung Verantwortlichen", „anspringt". Als solcher „verlängerter Arm" der eigenen IT-Infrastruktur-Ressourcen „an die Cloud heran", kommt es freilich nicht zu einer Übertragung von Daten in eine Drittverantwortung des Cloud-Anbieters. Hier ist zu trennen zwischen „Store" und „Compute": Beim Anbieter wird kein Speicher sondern nur Rechenleistung gemietet, seine Systeme nehmen mithin lediglich „blinde" Datenverarbeitungen vor. Die herkömmlich Cloud-typische (Rück-) Übertragung der zu verarbeitenden Daten in die vorgehaltenen Cloud-Strukturen findet nicht statt. Dann aber stellt sich dieser vom Unternehmen auf eigenen Systemen vollumfänglich durchkontrollierte Prozess der konkreten Datenverarbeitung als flüchtiger dar, da er allein im Arbeitsspeicher stattfindet. Die Rechenleistung wird ins Haus geholt, nicht etwa „cloudgesourct".

Dieser Unterschied ist entscheidend. Bei der ADV müssten – insoweit kaum praktikabel – aufwändige Vorprüfungen erfolgen und sodann umfangreiche Vertragswerke mit den verschiedenen Cloud-Anbietern im Einzelnen ausgehandelt werden. Diese Verpflichtung besteht sowohl nach der Europäischen Datenschutzrichtlinie (96/46/EG), die die datenschutzrechtlichen Mindeststandards beschreibt, die in den EU-Mitgliedstaaten durch nationale Gesetze sichergestellt werden müssen, als auch für deren avisierte Rechtsnachfolgerin, die EU-Datenschutz-Grundverordnung (DS-GVO). Eine ADV ist hiernach europarechtlich nur zulässig, wenn ein Gesetz dies gestattet oder ein schriftlicher Vertrag die ADV detailliert regelt.

Besteht letzteren Falls kein solcher Vertrag, stellt dies einen Verstoß gegen die Verpflichtung des Auftraggebers dar, die jeweiligen Verantwortlichkeiten in schriftlicher Form zu dokumentieren und kann Sanktionen nach sich ziehen. Der Auftragsverarbeiter ist vom „für die Verarbeitung Verantwortlichen" sorgfältig nach Kriterien wie Zuverlässigkeit, Leistungsfähigkeit, seinen dem Stand der Technik entsprechend zum Einsatz kommenden technisch-organisatorischen Sicherheitsmaßnahmen etc. auszuwählen. Die Auswahl beinhaltet insbesondere die Kontrolle der technisch-organisatorischen Maßnahmen vor Beginn der Datenverarbeitungen und sodann regelmäßig während der Laufzeit des ADV. Der entsprechende ADV-Vertrag muss bestimmte inhaltliche Mindestanforderungen erfüllen. Insbesondere muss geregelt sein, dass der Auftragsverarbeiter selbst sowie Personen, die ihm unterstellt sind und Zugang zu personenbezogenen Daten haben, diese Daten nur auf Weisung des „für die Verarbeitung Verantwortlichen" verarbeiten dürfen. Dessen ungeachtet muss der „für die Verarbeitung Verantwortliche" dennoch weiter rechtlich und tatsächlich in der Lage sein, in die Entscheidungen des Auftragsverarbeiters über die Mittel der Verarbeitung einzugreifen; die Gesamtverantwortung liegt nach wie vor bei ihm. Hieraus folgt, dass der „für die Verarbeitung Verantwortliche" alle eingesetzten Auftragsverarbeiter effektiv überwachen muss um zu gewährleisten, dass deren Entscheidungen im Einklang mit seinen Weisungen, dem ADV und dem Datenschutzrecht stehen. Sollte sich ein Auftragsverarbeiter nicht an die Beschränkungen der ihm vorgegebenen Verwendung der Daten halten, „mutiert" der Auftragsverarbeiter insoweit selbst zum – dann rechtswidrig agierenden – „für die Verarbeitung Verantwortlichen". Der ursprüngliche „für die Verarbeitung Verantwortliche" kommt seinerseits in Erklärungsnot, warum und wie der Auftragsverarbeiter gegen seinen Auftrag verstoßen konnte. Die Artikel 29-Datenschutzgruppe neigt dazu, in derartigen Fällen von einer gemeinsamen (auch haftungs-) rechtlichen Verantwortung auszugehen, da sich so der bestmögliche Schutz der Interessen der betroffenen Personen erreichen lässt. Eine wichtige Konsequenz der gemeinsamen Verantwortung liegt dann in der gesamtschuldnerischen Haftung für Schäden. Hinzu kommt, dass die EU-Datenschutzrichtlinie zwar im Grundsatz den „für die Verarbeitung Verantwortlichen" in der

Haftung sieht – abgesehen von den dargestellten Ausnahmen hindert dies aber die einzelstaatlichen Datenschutzgesetzgebungen nicht daran, in bestimmten Fällen auch den Auftragsverarbeiter haftbar zu machen.

Da wie gesehen „Safe Harbor“ nicht mehr als Legitimation in Anspruch genommen werden kann sondern es sich bei der Nutzung von US-Clouds grundsätzlich um eine Datenübermittlung in einen unsicheren Drittstaat handelt, wäre nach Maßgabe der Artikel 29-Gruppe zusätzlich eine Vereinbarung über die ADV mit den soeben dargestellten Inhalten zur Erfüllung der streng abzuwägenden Erforderlich- und Verhältnismäßigkeitsanforderungen, die an eine solche Datenübermittlung gestellt werden, nötig. Damit aber wären an eine zulässige Datenverarbeitung in der US-Cloud kaum überwindbare Hürden geknüpft.

Jedoch spricht vieles dafür, dass die hier zu bewertende Konstellation der hybriden Cloud-Lösung, wie „NetApp Privat Storage for Cloud“ sie ermöglicht, weder als Datenübermittlung noch als ADV sondern als Erweiterung der IT-Ressourcen des Unternehmens (und mithin als verlängerter Arm der eigenen Infrastruktur und Datenverarbeitungsprozesse) angesehen werden kann:

Zwar stünde der Umstand, dass sich Cloud-Services oder in die Cloud ausgelagerte Applikationen die zu verarbeitenden Daten von der beim Co-Locator aufgestellten Kundenmaschine „abholen“, einer Datenübermittlung im Rechtssinne nach Lesart der Gerichte und Datenschutzbehörden noch nicht entgegen. Denn das Merkmal der „Übermittlung“ ist nicht gleichzusetzen mit einem „Transport“ zu einem Dritten, also einem Export der Daten. Vielmehr ist die Übermittlung umfassend durch ein „Bekanntgeben“ zu definieren. Ausschlaggebend ist die Verbreitung der in den Daten enthaltenen Informationen. Auf die Art und Weise der Darstellung der Daten oder des Zugangs zu ihnen und auf die Einzelheiten des Vorgangs der Informationsvermittlung kommt es hiernach nicht an, weil jede Vergrößerung des Personenkreises, dem die Information zugänglich ist, die Belange der Betroffenen berührt. Hierfür genügt jede Handlung, durch die die Daten in den Bereich des Adressaten gelangen, gleichgültig wie dies im Einzelnen geschieht, also etwa auch durch ein Abrufverfahren. Datenübermittlung läge demnach auch vor, wenn der Zugang zu den Daten übermittelt wird und die Daten somit für den Empfänger nutzbar sind. Hier muss die übermittelnde Stelle zwar die Daten zunächst zu diesem Zweck bereithalten, also eine entsprechende technische und organisatorische Konstellation geschaffen haben, doch geht die entscheidende Aktivität vom Empfänger aus. In diesem Fall ist erst die Einsicht bzw. der Abruf, also die konkrete Inbesitznahme der Daten durch die Empfängeraktivität der Übermittlungsvorgang.

An einem Einsehen oder Abrufen im Rechtssinne fehlt es freilich, wenn das Bekanntgabe-Moment an den Dritten entfällt, weil sich die Datenverarbeitungsvorgänge wie in einer flüchtigen „Black Box“ ohne Zugriffs- und Nutzungsrechte des Dritten – als die beschriebene Verlängerung der IT-Ressourcen des Unternehmens – darstellen. Diese reine Infrastrukturnutzung ist sonach nicht als Datenübermittlung zu qualifizieren. Sie stellt freilich noch nicht einmal eine ADV dar, wenn die im Rechtssinne verantwortliche Stelle – d.h. das Unternehmen, das sich die jederzeitige Herrschaft über seine Daten sichern muss, da es über die Zwecke und Mittel der Verarbeitung entscheidet – diese Verantwortung weder überträgt noch durch Einbindung eines ein- und anzuweisenden Auftragsdatenverarbeiters erweitert sondern sich lediglich fremder Infrastruktur bedient. Dies ist der Fall, wenn lediglich Datenverarbeitungsanlagen gemietet oder sonst genutzt werden und diese von der verantwortlichen Stelle betrieben werden und der „Vermieter“ – im Untersuchungsbeispiel etwa Amazon – somit nur durch Eigentums- oder Besitzverletzungen Zugriff auf die Daten erlangen könnte. Maßgebend ist hier die Funktionsherrschaft über den Datenverarbeitungsvorgang als entscheidendes Kriterium für die Kontrolle über technische Systeme.

Nach diesem funktionellen Ansatz, den im Grundsatz auch die Artikel 29-Datenschutzgruppe vertritt, sind auch die Fälle zu lösen, in denen Rechenkapazität auf externen Servern angemietet wird und die verantwortliche Stelle dort selbstständig personenbezogene Daten verarbeitet. Stellt ein Rechenzentrum einem Kunden seine Systeme oder Dienste ganz oder teilweise hinsichtlich einzelner Datenverarbeitungen zur Verfügung und nutzt dieser sie online im Wege einer gegen Kenntnisnahme Dritter abgeschotteten Datenverarbeitung, liegt keine ADV vor sondern eine selbstständige Datenverarbeitung durch den Kunden. Dies ist jedenfalls dann anzunehmen, wenn wie im Untersuchungsbeispiel NetApp Private Storage for Cloud der Kunde allein und ausschließlich darüber entscheidet, welche

Daten wann und in welcher Weise verarbeitet werden und er auch selbst über die dafür notwendigen Programme und Algorithmen bestimmt. Das Cloud-Rechenzentrum beschränkt sich darauf, für die Einsatzbereitschaft zu sorgen und über die Dauer der Nutzung Buch zu führen. In diesen Fällen bedarf es keines Rückgriffs auf das Regime der Auftragsdatenverarbeitung. Die Verantwortung für den Datenschutz verbleibt beim Unternehmen.

Nach Ansicht einiger europäischer Datenschutzexperten soll eine ADV zwar auch in den Fällen vorliegen, in denen der Auftragnehmer lediglich die IT-Ressourcen wie etwa Speicher oder Server zur Verfügung stellt, die der Auftraggeber über das Internet nutzen kann, da auch in diesen Fällen im Regelfall die Auftragnehmer die technischen Einwirkungs- und Zugriffsmöglichkeiten auf die vorhandenen personenbezogenen Daten hätten. Die Artikel-29-Datenschzugruppe der EU-Kommission hat sich hierzu bislang nicht geäußert. Folgte man diesem Ansatz, änderte sich an dem Befund, dass es sich in der dargestellten Konstellation nicht um ADV handelt, gleichwohl nichts. Denn abweichend von dem beschriebenen Regelfall bestehen solche Einwirkungs- und Zugriffsmöglichkeiten wie zuvor dargestellt im Untersuchungsbeispiel nicht. Wenn und soweit der Dienstleister keinen Zugriff auf die Daten erhält, die auf einem bestimmten Speichermedium verarbeitet werden (ähnlich einem Server-Housing), dürfte auch nach Maßgabe dieser Ansicht lediglich eine Verlängerung der Verantwortlichkeiten des Unternehmens (als „für die Verarbeitung Verantwortlicher“) durch Erweiterung ihrer Infrastruktur-Ressourcen vorliegen und nicht auf die Grundsätze der ADV zurückgegriffen werden müssen.

VI. Fazit

Lösungen wie NetApp Private Storage for Cloud, die in Kooperation mit Amazon, Microsoft, IBM und diversen Kollokationsanbietern entwickelt wurden, stellen eine Hybrid Cloud-Storage-Infrastruktur zur Verfügung, bei der das Kontroll-Element auf demselben Level wie bei On-Premise-Architekturen gehalten werden kann, dies bei gleichzeitiger Nutzung sämtlicher Vorzüge von Public-Cloud-Services. Die Verarbeitung findet statt, ohne dass die Daten in die Public-Cloud des Anbieters verschoben werden. Damit ist sowohl eine Datenmigration zwischen verschiedenen Anbietern als auch eine Datensynchronisation nicht mehr erforderlich. Da die Daten auf dem eigenen Storage-System des Unternehmens gespeichert bleiben, ist die vollständige Kontrollhoheit gewährleistet. Diese Konstellation unterfällt als technische Verlängerung der unter ausschließlicher Eigenkontrolle stehenden IT-Ressourcen des Unternehmens nicht den strengen Voraussetzungen an zulässige Datenübermittlungen in Drittstaaten und stellt sich auch nicht als – umfänglich vertraglich und kontrolltechnisch abzusichernde – Auftragsdatenverarbeitung dar.

* Der Autor ist Rechtsanwalt und Fachanwalt für IT-Recht. Er ist darüber hinaus Gründungspartner der Rechtsanwaltskanzlei esb Rechtsanwälte (http://www.kanzlei.de) sowie zugleich Fachbuchautor im IT-Recht und Lehrbeauftragter an der Hochschule für Technik in Stuttgart und als associate Professor an der E.N.U. in Kerkrade, Niederlande tätig.