



Stellungnahme

des Deutschen Anwaltvereins durch
den Ausschuss Informationsrecht

zur Mitteilung der Europäischen Kommission
„Freisetzung des Cloud-Computing-Potenzials in
Europa“
COM(2012) 529 final

Stellungnahme Nr.: 2/2013

Berlin, im Januar 2013

Mitglieder des Ausschusses

- Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender und Berichterstatter)
- Rechtsanwältin Isabell Conrad, München (Berichterstatterin)
- Rechtsanwalt Prof. Niko Härting, Berlin
- Rechtsanwalt Peter Huppertz, LL.M., Düsseldorf
- Rechtsanwalt Prof. Dr. Jochen Schneider, München
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München (Berichterstatter)
- Rechtsanwalt und Notar Ulrich Volk, Wiesbaden
- Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Thomas Marx

Verteiler

Verteiler Europa

Europäische Kommission

- Generaldirektion Kommunikationsnetze, Inhalte und Technologien

Europäisches Parlament

- Ausschuss Industrie, Forschung, Energie
- Ausschuss Recht
- Ausschuss für Wirtschaft und Währung
- Ausschuss für bürgerliche Freiheiten, Justiz und Inneres
- Ausschuss Binnenmarkt und Verbraucherschutz

Rat der Europäischen Union

Europäischer Wirtschafts- und Sozialausschuss

Ausschuss der Regionen

Ständige Vertretung der Bundesrepublik Deutschland bei der EU

Justizreferenten der Landesvertretungen

Europäischer Datenschutzbeauftragte

Rat der Europäischen Anwaltschaften (CCBE)

Vertreter der Freien Berufe in Brüssel

Bundesverband der Deutschen Industrie (BDI) in Brüssel

Deutscher Industrie- und Handelskammertag (DIHK) in Brüssel

Verteiler Deutschland:

Bundesministerium des Innern

Bundesministerium der Justiz

Bundesministerium für Wirtschaft und Technologie

Deutscher Bundestag – Innenausschuss

Deutscher Bundestag – Rechtsausschuss

Deutscher Bundestag – Ausschuss für Wirtschaft und Technologie

Arbeitskreise Recht der Bundestagsfraktionen

Fraktionen der im Deutschen Bundestag vertretenen Parteien

Innenministerien und Senatsverwaltungen für Inneres der Länder

Justizminister und Justizsenatoren der Länder

Die Datenschutzbeauftragten des Bundes und der Länder

Bundesrechtsanwaltskammer

Bundesnotarkammer

Bundesverband der Freien Berufe

Deutscher Richterbund

Deutscher Notarverein

GRUR

BITKOM

DGRI

EDV-Gerichtstag

DAV-Vorstand und Geschäftsführung

Vorsitzende der DAV-Gesetzgebungsausschüsse

Vorsitzende des FORUMs Junge Anwaltschaft

Redaktion NJW

JUVE-Verlag

ver.di Bundesverwaltung, Fachbereich Bund und Länder, Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 67.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

A) Einleitung

Der DAV begrüßt die vorliegende Initiative der EU-Kommission. Denn die Initiative bietet Gelegenheit, sich den derzeit zahlreichen rechtlichen Fragestellungen, die mit dem Einsatz von Cloud Computing einhergehen, anzunehmen. Die von der Kommission in ihrer Mitteilung angesprochenen Themen sowie die herausgearbeiteten Schwerpunkte, wie beispielsweise die Fragmentierung des Binnenmarktes, die bestehenden vertraglichen Probleme und der vorliegende Normenschwungel, sind ebenfalls Themen, die der DAV als zu lösende Fragestellungen sieht.

Zum einen nimmt der DAV zu den drei von der Kommission vorgeschlagenen Schlüsselaktionen (unten B Ziffer I.) sowie zum anderen zur Frage des Verhältnisses der Mitteilung zum aktuellen Entwurf der EU-Datenschutzgrundverordnung (DS-GVO) und der Mitteilung insgesamt (unten B Ziffer II.) Stellung:

B) Zur Mitteilung

I. Zu den Schlüsselaktionen

1. Zu Schlüsselaktion 1: Lichten des Normenschwungels

- a) Ein Großteil der bei Cloud Computing zu klärenden Rechtsfragen betrifft Datenschutzthemen. Unabhängig von dem Kommissionsentwurf zu einer neuen Datenschutz-Grundverordnung (siehe dazu die Stellungnahme des DAV Nr. 47/2012 vom Mai 2012) wird für das Cloud Computing sehr zeitnah eine Lösung benötigt, also eine Lösung zunächst auf Basis schon bestehender Regelungen und Gesetze.

Erst mittelfristig sollte daher ein „Lichten des Normendschungels“ im Sinne von Verändern von bestehenden gesetzlichen Regelungen angegangen werden. Zeitlich deutlich schneller umsetzbar wären Schritte, die – unter Beibehaltung der derzeitigen nationalen Normen – in Richtung der Schaffung von Standardvertragsbedingungen gehen, wie von der Kommission hier vorgeschlagen.

Eine solche Lösung hätte den Vorteil, zeitnah umsetzbar zu sein, ohne das Gesetzgebungsverfahren durchlaufen zu müssen. Zudem würde man mit einer solchen Lösung direkt bei den Unternehmen ansetzen, die das größte Interesse an einer möglichst rechtssicheren Lösung haben.

- b) Soweit die Kommission in der Darstellung ihrer Schlüsselaktion 1 vor allem die technische und organisatorische Seite anspricht, begrüßt dies der DAV. Denn gerade aktuell wird deutlich, dass dem Prinzip „Datenschutz durch Daten-/IT-Sicherheit“ große Bedeutung zukommt. Die Frage des rechtlichen Dürfens kann nicht völlig losgelöst von dem betrachtet werden, was aufgrund technischer und organisatorischer Schutzmaßnahmen faktisch getan werden kann. Gerade angesichts Cloud Computing und Big Data ist eine der dringlichsten Aufgaben eines modernen Datenschutzrechts, international Anreize für die Entwicklung neuer datenschutzfreundlicher Techniken zu schaffen und nicht nur die Datenverarbeiter, sondern auch die IT-Hersteller in die Pflicht zu nehmen.

Standardisierte Vorgaben und (technische) Normen oder Empfehlungen zum Cloud Computing gehen insofern in die richtige Richtung.

Dies gilt umso mehr, als im Rahmen der in der Datenschutzrichtlinie 95/46/EG vorgesehenen Interessenabwägung (und den diesbezüglichen Regelungen dazu in den Mitgliedsländern) der technischen Absicherung der Verarbeitung von personenbezogenen Daten eine gewichtige Rolle zukommen und zu einer Bejahung überwiegender Unternehmensinteressen führen kann.

Wenn es insoweit standardisierte Vorgaben und Normen gibt, ebenso wie Zertifizierungsempfehlungen und/ oder –maßstäbe, tragen diese in erheblichem Umfang zur Rechtssicherheit bei.

- c) Die Kommission sollte dabei – gegebenenfalls in Verbindung mit dem ETSI – auch schon bestehende internationale Zertifizierungen beachten und in die Überlegungen einbeziehen, da diesbezüglich bereits viel Erfahrung bei den Unternehmen und in der Praxis vorliegt. Zu denken wäre etwa an die anerkannten Zertifizierungen wie ISO 27000 und 27001 oder SSAE16. Da bereits viele Unternehmen danach zertifiziert sind, wäre die Akzeptanz von neuen Standards und Normen umso höher, je mehr neue Zertifizierungen mit bekannten Ansätzen synchronisiert sind bzw. sich mit bekannten decken oder diese aufgreifen und zum Teil einer „EU-Cloud-Zertifizierung“ machen.
- d) Seit 1.9.2009 gilt in Deutschland eine Neufassung der Vorschrift zur Auftragsdatenverarbeitung (§ 11 Bundesdatenschutzgesetz (BDSG)). § 11 BDSG sieht u. a. die Pflicht vor, dass der Auftraggeber den Auftragnehmer vor Beauftragung anhand der Geeignetheit der technischen und organisatorischen Sicherheitsmaßnahmen sorgfältig auswählen muss. Um dies zu ermöglichen, müssen die Auftragnehmer die von ihnen getroffenen technischen und organisatorischen Maßnahmen auflisten, damit der Auftraggeber diese überprüfen kann. In der Praxis hat sich gezeigt, dass eine Vielzahl von Dienstleistern in hohem Maße überfordert waren und sind, nach den Vorgaben des deutschen Rechts (§ 9 BDSG und dessen Anlage) ihre eigenen Maßnahmen zu beschreiben. Obwohl die Neufassung des § 11 BDSG seit mehr als 3 Jahren in Kraft ist und nach herrschender Ansicht die Anforderungen an die Auswahl des Dienstleisters und an die konkrete und hinreichend detaillierte Festlegung der Sicherheitsmaßnahmen im Auftragsdatenverarbeitungsvertrag bereits davor galten, ist es heute noch an der Tagesordnung, als Auftraggeber von einem Dienstleister Unverständnis zu ernten oder Angaben zu erhalten, die an der Sache vorbei gehen. Vielen Dienstleistern fehlt nach wie vor ein (schriftliches) Sicherheitskonzept, das einer angemessenen Prüfung zugänglich wäre, und in vielen Auftragsdatenverarbeitungsverträgen fehlen ausreichende bzw. konkrete auftragsspezifische Festlegungen von Sicherheitsmaßnahmen, obwohl einige Datenschutzaufsichtsbehörden Musterauftragsdatenverarbeitungsverträge mit konkreten Beispielen (z. B. für Fernwartung oder Akten- und Datenträgervernichtung) veröffentlicht haben.

Es wird daher vom DAV für umso wichtiger erachtet, dass mit entsprechender Aufklärungsarbeit und Verbreitung von gut lesbaren, vom Dienstleister leicht ausfüllbaren und am besten an international schon etablierten (technischen) Normen ausgerichteten EU-Cloud-Empfehlungen oder Normen die Akzeptanz, aber auch das Verständnis für den technisch-organisatorischen Datenschutz erhöht wird.

- e) Um Wettbewerbsgleichheit zu erzielen und den Binnenmarktverkehr zu fördern, sind EU-weit geltende technische Empfehlungen und Vorgaben ein guter Weg, gegebenenfalls abgestuft nach Größe des Dienstleisters und Umfang der erbrachten Cloud-Leistungen. Das gilt zumindest für die Entwicklung von europäischen Cloud-Lösungen, weil dort die Durchsetzbarkeit und Kontrollierbarkeit von europäischen Normen und Standards am ehesten möglich ist.

Der Vorteil von europäischen Cloud-Lösungen wäre, dass sich die beteiligten Rechenzentren (Orte der Datenverarbeitung) und nach Möglichkeit auch die beteiligten Anbieter/Subunternehmer innerhalb der EU befinden. Allerdings sind gerade bei lokal begrenzten Cloud-Lösungen (Private Cloud, Euro Cloud) die Skaleneffekte und damit Preise für die Inanspruchnahme der Dienste eher hoch.

Hohe Skaleneffekte und damit die Möglichkeit, kostenlose Cloud-Dienste anzubieten (etwa Webmail-Dienste), ergeben sich dadurch, dass Rechenzentren möglichst in allen Zeitzonen („follow the sun“) am Cloud-Dienst beteiligt sind (so bei größeren Public Clouds). Nur sehr große internationale Cloud-Anbieter (etwa Amazon, Google, Microsoft, Apple, Salesforce) betreiben konzerneigene Rechenzentren rund um den Globus. Bei solchen Konzernen ist nicht ausgeschlossen, dass künftig in Europa entwickelte, international anerkannte Normen und Standards konzernweit beachtet werden. Allerdings ist die Förderung dieser sehr großen Anbieter unter wettbewerblichen Gesichtspunkten (Kartellrecht) nicht unproblematisch.

Will man dagegen den Wettbewerb beleben und kleine – auch europäische – Anbieter von Public Clouds fördern, sind naturgemäß an der Erbringung des Public Cloud-Dienstes viele außereuropäische Subunternehmer beteiligt und die Fluktuation unter den Subunternehmer ist regelmäßig groß. Dies erschwert die Durchsetzbarkeit und Kontrolle von Normen und Standards. Insoweit ist die Problematik mit dem

Datenexport in die USA und der Safe Harbour-Zertifizierung vergleichbar, bei der die europäischen Datenschutzaufsichtsbehörden nicht ausreichen lassen, dass das zertifizierte US-Unternehmen in der im Internet abrufbaren Safe Harbour-Liste eingetragen ist. Vielmehr soll der europäische Datenexporteur Garantien und Nachweise verlangen, dass die Safe Harbour-Prinzipien tatsächlich eingehalten werden. In Zusammenhang mit globalen Cloud-Lösungen müssten daher nicht nur Normen und Zertifizierungen entwickelt werden, sondern auch Verfahren, wie die Einhaltung der Zertifizierungskriterien überprüft und nachgewiesen werden kann. Einzelheiten zu Cloud-Anbietern/Subunternehmen in Drittstaaten außerhalb der EU siehe unten 2.b).

- f) Es ist nicht klar, ob die Kommission in ihrer Mitteilung COM(2012) 529 final eher Private Cloud / Euro Cloud oder Public Cloud-Lösungen anspricht. In der Einleitung zu dieser Mitteilung ist die Begriffsbestimmung von Cloud Computing zu ungenau. Da die Wirksamkeit und Effektivität der von der Kommission vorgeschlagenen Schlüsselaktionen von der Art des Cloud-Dienstes abhängt, empfiehlt sich eine genauere Differenzierung. Die Kommission erwähnt in ihrer Begriffsbestimmung zwar „entfernte Rechner“, meint aber eventuell „entfernte Rechenzentren“. Die Abgrenzung zwischen World Wide Web („überall und für jedermann Informationen zugänglich“) und Cloud Computing („überall und für jedermann Rechenleistung zur Verfügung“) ist zwar plakativ aber (gewollt) unscharf. Denn Cloud bietet nicht nur Rechenleistung, sondern auch Anwendungen/Applikationen und vor allem nahezu unbegrenzte Speicherkapazitäten und Datenverfügbarkeit von überall her (was die Kommission unter Ziffer 2 ihrer Mitteilung auch erwähnt). Insoweit ist Cloud mitverantwortlich für den Siegeszug der Smartphones und Tablets.
- g) Gleichzeitig kann – je nach Cloud-Dienst – eine enge Verbindung zwischen Cloud und den Phänomenen BYOD (Bring your own Device) und Big Data bestehen, die bei der Cloud-Strategie der Kommission berücksichtigt werden sollte. Eine undifferenzierte Förderung von Cloud kann praktisch bedeuten, dass herkömmliche Datenschutzprinzipien (z.B. Datenvermeidung und Datensparsamkeit, Löschung von Daten) zunehmend überholt sind und die Datennutzung vom ursprünglichen Zweck/Kontext der Datenerhebung und –verarbeitung gelöst wird. Ein weiterer Trend in Verbindung mit der Auslagerung von Daten in die Cloud (etwa im Zusammenhang

mit dem dienstlichen Einsatz von privaten Devices bei BYOD) ist, dass die Sicherheit von Daten zunehmend mit Mitteln sichergestellt wird, die eher nicht datenschutzfreundlich sind (z.B. umfassende Filtermaßnahmen mittels Data Loss Prevention-Systemen). Auslagerung in die Cloud kann zwar die von der Kommission angesprochene „massive Senkung der IT-Ausgaben bei den Nutzern“ bewirken. Gleichzeitig müssen jedoch gerade bei der Schlüsselaktion 1 der Kommission die internen Kosten für die Auslagerung von Daten – einschließlich Anpassung von individuellen Geschäftsprozessen des Auslagerers an Cloud-Standard(software)-Lösungen – und die Auslagerungsrisiken mitberücksichtigt werden. Die von der Kommission angesprochene Forderung einer Datenportabilität zugunsten des Auslagerers ist eine wichtige Maßnahme zur Förderung des Wettbewerbs. Gerade für den Schutz von personenbezogenen Daten und vertraulichen Unternehmensdaten (Geheimnisschutz) des Auslagerers wäre wichtig, dass u.a. Normen und Standards dafür entwickelt werden, dass Daten, die in die Cloud ausgelagert wurden, sicher (nachweisbar) gelöscht werden können. Die Kommission spricht in ihrer Mitteilung von „Datenumkehrbarkeit“, meint aber vermutlich Re-Transition – was in eine ähnlich Richtung geht wie Datenportabilität in Verbindung mit sicherer Löschung bei Cloud-Anbieter.

2. Zu Schlüsselaktion 2: Sichere und faire Vertragsbedingungen

a. Cloud sprengt herkömmliche Auftragsdatenverarbeitungskonzepte

Auch begrüßt der DAV die Vorschläge und das Vorgehen der Kommission. Die Möglichkeit (!), standardisierte Cloud Computing-Verträge nutzen zu können, kann sowohl helfen, Mitgliedsstaatenübergreifend für faire Bedingungen zu sorgen als auch ein forum shopping zu vermeiden.

Auf zivilrechtlicher Ebene wäre für den DAV ein Modell begrüßenswert, das am Modell der EU-Standardvertragsklauseln im Datenschutz ausgerichtet ist: Mehrere Varianten von vorgegebenen Standard-Verträgen, die verschiedene Cloud-Konstellationen betreffen und die die Parteien verwenden können, aber nicht müssen.

Dabei darf die datenschutzrechtliche Seite nicht vergessen werden:

Derzeit lässt sich die Beauftragung eines Cloud Providers innerhalb der EU über das Modell der Auftragsdatenverarbeitung abdecken und zwar mit dem Argument, dass bei Vorliegen einer Auftragsdatenverarbeitung der Dritte nicht mehr als Dritter anzusehen ist.

Im Übrigen fehlt diese Privilegierung in dem Kommissionsentwurf der neuen DS-GVO, siehe dazu die oben erwähnte Stellungnahme 47/2012 des DAV. Insofern regt der DAV nochmals dringend an, die Privilegierung für den Fall einer Auftragsdatenverarbeitung beizubehalten.

Das Modell der Auftragsdatenverarbeitung kommt aber selbst innerhalb der EU an seine Grenzen, wenn es um die typischen Fragen bei einer Cloud geht, etwa der Frage des Orts der Datenverarbeitung (kann sekundlich wechseln, wenn er überhaupt ermittelbar sein sollte) oder der Beherrschbarkeit der Cloud durch den Auftraggeber.

Das klassische Modell der Auftragsdatenverarbeitung wird bei Cloud regelmäßig verlassen. Bei den meisten Cloud-Diensten (v.a. bei Cloud-Storage und Software as a Service – SaaS) haben der Cloud Provider und evtl. auch seine Subunternehmer und ggf. andere Konzerngesellschaften des Providers bzw. der Subunternehmer zwar die Möglichkeit, auf die ausgelagerten Daten Zugriff zu nehmen. Der Cloud Provider speichert die Daten und hält sie zum Abruf über das Internet bereit. Bei Wartungstätigkeiten und Tests von IT-Systemen werden der Cloud Provider und/oder seine Subunternehmer die Daten – wenn überhaupt – nur beiläufig zur Kenntnis nehmen. Es muss nicht nur sichergestellt werden, dass ausgelagerte Daten nicht zu eigenen Geschäftszwecken des/der Cloud-Anbieter verarbeitet und genutzt werden. Wichtig wäre, dass der Auftraggeber insgesamt in die Lage versetzt wird, auch bei Auslagerung in die Cloud die Datenherrschaft zu behalten. Das ist derzeit v. a. bei Public Cloud-Lösungen nicht der Fall, u. a. weil Kontrollen und individuelle Weisungen des Auftraggebers kaum praktikabel sind. Die in § 9 BDSG und Anlage dazu vorgesehenen Kontrollgebote (im wesentlichen Zugangs-, Zutritts-, Zugriffs-, Auftrags-, Weitergabe-, Verfügbarkeits- und vor allem Trennungskontrolle) sind bei Public Cloud derzeit kaum umsetzbar.

Das deutsche Recht sieht für Wartung und Prüfung von IT-Systemen in § 11 Abs. 5 BDSG eine Regelung vor, die die Regelungen der Auftragsdatenverarbeitung als analog für anwendbar erklärt. Es stößt aber beim Cloud Computing ebenfalls an vorgenannte Grenzen: Der Ort der Datenverarbeitung wechselt stets und ist kaum bestimmbar, die Beherrschbarkeit der Daten (deswegen) nur in Ausnahmefällen gegeben.

Im Übrigen sieht § 11 BDSG die Verpflichtung vor, den Auftragsdatenverarbeitungsvertrag schriftlich abzuschließen (also in Papierform mit Unterschrift). Dies ist v. a. bei Public Cloud-Lösungen eher unpraktikabel, weil die Beauftragung, Änderung und Beendigung der Dienste üblicherweise rein elektronisch (im Portal) erfolgt.

Diesbezüglich ist nach Ansicht des DAV gesetzgeberische Aktivität auf EU-Ebene gefordert.

Aber auch schon jetzt könnten Standard-Vertragsbedingungen der Kommission eine Hilfe bei der Interessenabwägung sein.

b. Berücksichtigung von Nicht-EU-Lösungen/ Sub-Unternehmern

Bislang unberücksichtigt ist in der Mitteilung, dass die meisten Cloud Angebote von Anbietern außerhalb der EU stammen (siehe auch oben 1. e-g). Auch wenn es nicht das Ziel der Mitteilung und der Kommission ist, außereuropäischen Wettbewerb zu fördern, ist es für die europäischen Unternehmen oft ein Fakt, dass die bislang führenden Cloud Anbieter zu Konzernen in den USA und speziell bei Fujitsu in Japan gehören. Selbst kleine europäische SaaS-Anbieter arbeiten regelmäßig mit außereuropäischen Rechenzentrums-Infrastructure as a Service (IaaS)-Anbietern zusammen. Es ist also – zumindest mittelfristig – nicht änderbar, dass europäische Cloud-Kunden mit Cloud-Anbietern außerhalb der EU arbeiten.

Datenschutzrechtlich kann dies bei Anbietern mit Sitz in nicht sicheren Drittstaaten auf massive Probleme stoßen, ist jedenfalls mit hohem Aufwand verbunden.

Dies gilt umso mehr, wenn – wie häufig – Subunternehmer eingesetzt werden, die (ebenfalls) außerhalb der EU ihren Sitz haben.

Dies kann auch der Fall sein, wenn der eigentliche Cloud-Anbieter in der EU seinen Sitz hat, sich aber beispielsweise eines Subunternehmers in Indien bedient und sei es nur zu Wartungs- oder Entwicklungszwecken, aber mit etwaiger Zugriffsmöglichkeiten auf die Daten, die wiederum meist personenbezogen sind oder sein können.

Gemäß dem bisherigen Modell der Datenschutzrichtlinie 95/46/EG gibt es ein zwei-stufiges Modell: Auf der ersten Stufe ist zu fragen, ob ein Unternehmen personenbezogene Daten generell übermitteln darf, in einer etwaigen zweiten Stufe, ob die Daten – wenn eine Übermittlung grundsätzlich zulässig ist – an eine Empfänger gehen dürfen, der seinen Sitz außerhalb der EU hat.

Es sollte seitens der Kommission beachtet werden, dass zunächst vor allem auf der ersten Stufe klare Regelungen benötigt werden, die für das Übermitteln von Daten in eine Cloud greifen und schon diese Übermittlung für sich genommen legitimieren. Da in dem derzeitigen Entwurf der DS-GVO (noch) eine Privilegierung für die Auftragsdatenverarbeitung fehlt, entstünden auf der ersten Stufe deutliche Probleme.

Betreffend der zweiten Stufe könnte eine Lösung, die kurzfristig umsetzbar wäre, die Schaffung einer zusätzlichen Fassung von EU-Standardvertragsbedingungen speziell für Cloud sein. Diese neue Fassung sollte sich nach Ansicht des DAV an den controller-to-processor-Klauseln aus 2010 orientieren, aber vor allem den Umstand berücksichtigen, dass – eventuell fluktuierende – Subunternehmer in Nicht-EU-Ländern eingeschaltet werden oder werden können.

Insofern wäre auch eine Klärung wichtig, ob beim Einsatz von Subunternehmern in Nicht-EU-Staaten

- der Datenexporteur mit seinem direkten Vertragspartner, also dem Cloud Provider, einen EU-Standardvertrag, oder
- aber der Datenexporteur direkt mit dem Subunternehmer den EU-Standardvertrag abzuschließen hat und der eigentliche Vertragspartner diesem beitrifft – so seit Jahren in Deutschland, aber auch Österreich von den Datenschutzbehörden empfohlen.

Gerade beim Cloud Computing stößt diese Empfehlung an ihre Grenzen, da weder der Auftraggeber noch die Subunternehmer Interesse haben, möglicherweise Dutzende von EU-Standardverträgen abschließen und auf jede Änderung bei den Subunternehmen (und seien es nur Umfirmierungen) reagieren zu müssen. Vielmehr will der Auftraggeber in aller Regel nur einen, am liebsten sogar in der EU tätigen Cloud Provider als Ansprechpartner und (Datenschutz-)Vertragspartner haben.

Als Alternative für eine mittelfristige Lösung wäre denkbar, das Instrument der Binding Corporate Rules (BCR), das bislang nur konzernintern anwendbar ist, auf die Datenübermittlung in die Cloud (unter Beteiligung von außereuropäischen Anbietern/Subunternehmern) zu übertragen. Voraussetzung ist, dass die Verbindlichkeit der BCR bei dem/den beteiligten Cloud-Anbietern sichergestellt und sicherzustellen ist. Daran fehlt es momentan noch. Allerdings können globale/internationale Zertifizierungen hier künftig Vorteile bringen.

Aus Sicht des DAV kommt also der Frage und Diskussion des Einsatzes von Subunternehmern eine wichtige Rolle zu, die die Kommission berücksichtigen sollte, gerade bei der Diskussion und Entwicklung von Standardvertragsbedingungen, seien es zivilrechtliche oder (neue) datenschutzrechtliche Bedingungen.

Die Vollharmonisierung des Datenschutzrechts innerhalb Europas – was eines der Ziele der DS-GVO ist – ist zwar grundsätzlich geeignet, Auftragsdatenverarbeitungsstrukturen und Auslagerung von Daten innerhalb der EU zu erleichtern. Denn nach derzeit geltendem Recht machen die unterschiedlichen nationalen Vorgaben an die Auftragsdatenverarbeitung selbst innereuropäische Lösungen unter Beteiligung mehrerer Unternehmen nur schwer handhabbar. Doch die von der Kommission angesprochene „Fragmentierung des digitalen Binnenmarktes innerhalb der EU“ ist gerade bei Cloud ein eher kleiner Aspekt. Wesentlich wichtiger wären globale Lösungen – v. a. einheitliche Datenschutz- und Vertragsrahmen für die Beauftragung von Cloud-Anbietern in den USA, in Japan und Indien. Dieses Ziel wird durch den Entwurf der DS-GVO eher behindert als gefördert. Denn die Diskrepanz zwischen dem europäischen Recht (v. a. wegen des Verbotsprinzips) und dem Datenschutzrecht in „unsicheren Drittstaaten“ wird zunehmen.

3. Zu Schlüsselaktion 3: Förderung einer gemeinsamen Führungsrolle des öffentlichen Sektors durch eine europäische Cloud-Partnerschaft

Auch hier begrüßt der DAV die Pläne der Kommission der Schaffung einer europäischen Cloud-Partnerschaft als Dachorganisation, um zunächst Bedarf und Wünsche zu ermitteln.

Ähnlich wie in der Privatwirtschaft könnten auch hier feste Vergabebedingungen angedacht und EU-weit eingeführt werden, ebenso wie Standardvertragsklauseln, siehe dazu oben und als Beispiel in Deutschland die verschiedenen EVB-IT (Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen).

III. Weitere Anmerkungen

1. Kein Ausschluss an der Cloud-Teilnahme für Berufsgeheimnisträger

Berufsgeheimnisträger (Anwälte, Ärzte etc.) sollten von der Nutzung von Cloud Services nicht per se ausgeschlossen sein. Aufgrund zum Teil sehr strenger nationaler Gesetzgebung kann es derzeit aber rechtlich schwierig sein, als Berufsgeheimnisträger rechtmäßig Cloud Services zu nutzen. Tatsächlich aber nutzen bereits viele Anwälte und Ärzte Cloud-Dienste, etwa im Zusammenhang mit einer Smartphone-Nutzung.

Dies betrifft nicht nur die Anwaltschaft oder Ärzte, sondern viele andere Bereiche bis zu Großkonzernen wie die Versicherungs- oder Gesundheitswirtschaft.

Eine ähnliche Situation ergibt sich, wenn es um besondere Arten von personenbezogenen Daten geht, für deren Verarbeitung – also auch Speicherung – meist eine Einwilligung der Betroffenen nötig ist, die im Cloud-Geschäft kaum praktikabel einholbar sein dürfte.

Wenn die technische und organisatorische Absicherung der dem Cloud-Anbieter anvertrauten Daten ausreichend hoch sowie auch auf rechtlicher Seite – etwa mit Sanktionen oder bestimmten Service Level Agreements (SLAs) – gesorgt ist, ist nicht einzusehen, warum ein Verbot der Auslagerung von besonders sensiblen Daten in die

Cloud aufrecht erhalten werden soll, dass durch die Praxis ohnehin längst überholt ist, weil bereits jetzt schon gerade die kleinen Arztpraxen und Anwaltskanzleien Cloud-Dienste (etwa Webmail-Dienste) nutzen.

Der Weg, in die Cloud nur verschlüsselte Daten zu übertragen, sollte – zumindest nach derzeitigem Stand der Technik – nicht überbewertet werden, denn oft reicht die Performance dafür nicht aus. Zum anderen darf technisch nicht übersehen werden, dass bei einer Verschlüsselungslösung nicht nur die Daten auf den Speichermedien, sondern auch im Arbeitsspeicher der Server des Cloud Computing Providers verschlüsselt ist, was technisch nicht trivial umzusetzen ist. Gleichwohl sollten Entwicklungen im Bereich der homomorphen Verschlüsselung und sonstige Verschlüsselungslösungen gefördert werden, so dass diese Lösungen in Zukunft praktikabel und kostengünstig einsetzbar sind.

Nach Ansicht des DAV sollte die Kommission die Thematik der Berufsgeheimnisse bei ihren Schlüsselaktionen und vor allem im Sinne einer rechtlichen Lösung umfänglich mitbedenken. Anderenfalls besteht die Gefahr, ganze Branchen vom Cloud Computing auszuschliessen.

2. Betriebs- und Geschäftsgeheimnisse

In Hinblick auf die Vorgaben aus dem Compliance-Bereich greift die Mitteilung der Kommission nach Auffassung des DAV das Problem der Kontrolle der tatsächlichen Datenhaltung noch nicht präzise genug auf, ebenso wie die Thematik von etwaigen Betriebs- und Geschäftsgeheimnissen noch nicht ausreichend beachtet wird.

Das Thema hat zwei Aspekte:

Zum einen geht es darum, dass auf die Daten in der Cloud niemand Zugriff erhält, über den der Auftraggeber nicht Bescheid weiß und jeder Berechtigte auch nur den Zugriff erhält, der ihm eingeräumt ist. Neben entsprechenden vertraglichen Vereinbarungen und Verpflichtungen sind dafür auch Kontrollen erforderlich, die der Auftraggeber und/oder ein vertrauenswürdiger Dritter durchführen müssen.

Dazu muss aber eine entsprechende (rechtliche) Infrastruktur hergestellt werden, die bzw. deren Aufbau die EU fördern kann, etwa durch entsprechende Regelungen in Standardverträgen.

Dieses Thema betrifft neben Datenschutzaspekten zum anderen aber auch (und in vielen Fällen vor allem) Aspekte des Betriebsgeheimnisschutzes. Bisher hat sich die Kommission damit nur am Rande beschäftigt, sollte aber auch diese Aspekte bei der weiteren Diskussion beachten.

Ferner geht es um den Schutz der Daten gegen Veränderung und Löschung, beabsichtigt oder versehentlich. Auch dazu muss es Sicherheitsvorkehrungen geben, die wiederum vom Auftraggeber kontrolliert werden müssen, also eine entsprechende Infrastruktur, aber auch begleitende rechtliche Regelungen benötigen.

Vorgenannte Punkte verlangen, dass die beteiligten Datenverarbeiter vor der ersten Verarbeitung (nicht notwendig vor Vertragsschluss) dem Kunden bekannt sind. Zumindest beim Einsatz von Subunternehmern kann dies problematisch werden. Befinden sich diese außerhalb der EU, kommen zusätzliche rechtliche Schwierigkeiten hinzu, die zumindest teilweise im Rahmen von Muster- oder Standardvertragsklauseln aufgefangen werden können.

Gerade insofern können solche eine Rolle spielen, um außereuropäischen Anbietern mit solchen Standardklauseln genügend Verhandlungsgewicht entgegenstellen zu können.

Der Aspekt der Kontrolle wird von der Kommission unter dem Stichpunkt „Vertrauen“ zwar schon angesprochen – aber nach Ansicht des DAV nur unpräzise.

Denkbar ist es insofern, die den Auftraggeber treffenden Kontrollpflichten und –rechte vertraglich und in Form von (technischen und organisatorischen) Normen aufzufangen, was bei den beiden diesbezüglichen Schlüsselmaßnahmen 1 und 2 zu berücksichtigen ist.

Der Schutz von Betriebsgeheimnissen, der gewahrt bleiben muss, wird dagegen bislang noch deutlich zu wenig aufgegriffen. Gerade zu diesem Punkt regt der DAV an, das

weitere Vorgehen, insbesondere in Hinblick auf zu schaffende Standardregelungen, und dazu zu treffende Maßnahmen noch genauer zu beachten.

3. Staatlicher Zugriff auf Cloud-Daten in Drittstaaten

Ein weiteres Problem – nicht nur bei Cloud-Diensten für den öffentlichen Bereich, sondern auch für Cloud-Dienste in der Privatwirtschaft – ist die Gefahr staatlicher Eingriffe in Drittstaaten in die in der Cloud gespeicherten Daten. Das spielt auch dann eine Rolle, wenn ein EU-Unternehmen einen EU-Cloud Provider beauftragt, sich dieser aber eines Nicht-EU-Subunternehmers bedient.

Insofern hilft wahrscheinlich nur eine Harmonisierung (auch über den Datenschutz hinaus). Außerhalb der EU ist das Problem rechtlich kaum lösbar, aber dennoch zu diskutieren.

Eine Lösung könnte in dem Einsatz von Verschlüsselungstechniken liegen, die aber ebenfalls staatlichen Zugriffen entzogen sein müssen. Entsprechende Empfehlungen zum Einsatz solcher Techniken in geplanten Standard- und Musternormen sowie -verträgen, die die Kommission schaffen will, können hilfreich sein.

4. Cloud-Dienste für die öffentliche Verwaltung

Kritisch ist, dass die Cloud-Strategie der Kommission für den nicht-öffentlichen und für den öffentlichen Bereich im Wesentlichen gleich ist und im öffentlichen Bereich private Clouds eher die Ausnahme sein sollen.

Für eine Cloud, die von der öffentlichen Verwaltung genutzt wird, gibt es zusätzliche Voraussetzungen:

Es geht dabei um Hilfsdienste für die staatliche Verwaltung. Die dort verwendeten und ggf. in der Cloud gespeicherten Daten sind Daten des Staates, möglicherweise auch sensible personenbezogene Daten. Dies bedingt, dass hohe Investitionen in die Sicherheit der Cloud-Dienste getätigt werden müssen und ein hohes Vertrauen in die Dienstleister

herrschen muss, bevor eine solche Aufgabe einem Cloud-Dienstleister als externen Dienstleister übertragen werden kann.

Es erscheint zweifelhaft, ob diese Voraussetzungen in jedem Fall durch private Dienstleister erfüllt werden können.

Auch interne Clouds der öffentlichen Verwaltung (etwa durch dafür zuständige Behörden oder von einzelnen öffentlichen Körperschaften getragene gemeinsame Unternehmen) sind denkbar und in vielen Fällen sicher notwendig.

In allen Fällen muss sichergestellt werden, dass bei Cloud-Dienstleistern, die in einem EU-Mitgliedsstaat für Verwaltungen eines anderen Staates oder von Teilkörperschaften eines anderen Staates Dienstleistungen erbringen, ein Zugriff staatlicher Stellen des Sitzstaates des Dienstleisters auf dort gespeicherte Daten nur dann erfolgt, wenn dies aufgrund einer gesetzlichen Regelung zur Datenübermittlung zwischen Mitgliedern der EU mit Zustimmung des Staates geschieht, um dessen Daten es geht. Eine Förderung EU-weiter von der öffentlichen Verwaltung genutzter Clouds setzt Normen des EU-Rechts voraus, die die Einhaltung dieser Anforderung sicherstellen.

Das gilt insbesondere für das Trennungsgebot. Es muss nicht nur, aber gerade auch bei Cloud-Lösungen im öffentlichen Bereich sichergestellt sein, dass Daten verschiedener Behörden sowie Daten, die für verschiedene Zwecke erhoben, verarbeitet und genutzt werden, hinreichend sicher getrennt sind und dass nicht etwa die Trennung durch einen Administrationsfehler aufgehoben werden kann.

5. Ergänzende Aspekte zum Verhältnis der Cloud-Strategie der Kommission zur EU-DS-GVO

Die Kommission geht davon aus, dass die DS-GVO ein wichtiger Baustein ihrer Cloud-Strategie ist und europäische Cloud-Potenziale fördert. Das Gegenteil ist jedoch der Fall. Viele Cloud-Lösungen sind mit den gängigen europäischen Prinzipien des Datenschutzrechts – die in der DS-GVO im Wesentlichen unverändert bleiben – nicht vereinbar:

- a) Cloud fördert, wie erwähnt, das Big Data-Phänomen, weil die IT-Infrastruktur (Rechenleistung, Speicherkapazität) des Cloud-Kunden – anders als beim Inhouse-Betrieb – kaum begrenzt ist. Mehr Daten liefern bessere Ergebnisse als die Anwendung intelligenterer Algorithmen auf bestehenden Daten. Insoweit besteht ein grundsätzlicher Zielkonflikt mit dem Verbotsprinzip, der Zweckbindung von Daten und dem Gebot der Datenvermeidung und Datensparsamkeit.
- b) Bereits die Auslagerung von Daten an den Cloud-Anbieter ist nach dem geltenden Datenschutzrecht und nach dem Entwurf der DS-GVO verboten, jedenfalls soweit die Grenzen der Auftragsdatenverarbeitung gesprengt werden (siehe oben 1. und 2.).
- c) Fraglich ist, inwieweit bei Cloud-Diensten die Anonymisierung und Pseudonymisierung von Daten umsetzbar sind. Durch eine Zunahme von Datenquellen, Datenmengen und Verknüpfungsmöglichkeiten werden die Anforderungen an Pseudonymisierungs- und Anonymisierungstechniken weiter steigen.
- d) Gleichzeitig steigen – gerade bei Auslagerung in außereuropäische Cloud-Lösungen – die Anforderungen an die Revisionssicherheit und an die Gewährleistung der Nachvollziehbarkeit von Datenverarbeitungen. Protokollierung von Datenverarbeitungen stößt an Grenzen. Soweit etwa die europäische Finanzverwaltung eine Auslagerung von steuer- und buchhaltungsrelevanten Informationen ins EU-Ausland grundsätzlich untersagt – es sei denn, der Steuerpflichtige hält gespiegelte Datensätze im Inland bzw. in der EU vor – sind den Cloud-Potenzialen Grenzen gesetzt.
- e) Wer soll bei Cloud-Lösungen Betroffenenrechte sicherstellen? Wer ist im Hinblick auf die Data Breach Notification, die in der DS-GVO mit einem Meldezeitfenster von 24 Stunden erheblich verschärft wird, zur Meldung verpflichtet (der Cloud Provider oder der Kunde) und ist das kurze Zeitfenster einzuhalten? Es ist durchaus sachgerecht, dass im Entwurf der DS-GVO der Auftragnehmer stärker in die Pflicht genommen wird. Im Übrigen jedoch sieht die DS-GVO keine neuen modernen Instrumente vor, die Cloud-Lösungen fördern könnten.

f) Was jetzt schon im E-Commerce/Performance-Marketing u. ä. gilt, wird zunehmend für alle Bereiche der Datenverarbeitung in der Cloud (Screening etc.) gelten:

Wirksame Einwilligungen werden zunehmend schwerer gestaltbar, da

- Datenkategorien,
- Nutzungszwecke,
- Datenempfänger

kaum noch transparent im Vorhinein festlegbar sind. Insoweit ist es konsequent, wenn der Entwurf der DS-GVO in Art. 7 Abs. 4 das Instrument der Einwilligung als datenschutzrechtliche Erlaubnis weiter entwertet. In Zusammenschau mit dem Verbotsprinzip und dem geltenden Auftragsdatenverarbeitungs- und BCR-Konzept ist jedoch festzustellen, dass sehr viele Cloud-Lösungen nach geltendem Datenschutzrecht unzulässig sind und dass die DS-GVO, wenn sie wie geplant in Kraft treten sollte, daran nichts ändern wird. Genau das Gegenteil wird jedoch mit der Cloud-Strategie der Kommission bezweckt.

Der DAV regt an, dass sich die für die Cloud-Strategie zuständige Generaldirektion der Kommission für neue, zeitgemäße, Cloud-kompatible Datenschutzprinzipien und deren Integration in den Entwurf der DS-GVO einsetzt, so dass möglichst ein einheitlicher globaler oder zumindest international kompatibler Rechtsrahmen entsteht. Der DAV hat insoweit bereits gesondert Stellung genommen. Nur so ist die Nutzung von europäischen Cloud-Potentialen möglich.