Gerrit Hornung/Stephan Sädtler

Europas Wolken

Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing

Reformvorschlag prallt auf technische Innovation: So könnte man die Situation zwischen dem Entwurf der EU-Kommission vom 25.1.2012 und den von großen Hoffnungen begleiteten Anwendungen des Cloud Computings beschreiben. Datenschutzrechtliche Unsicherheiten sind eines der größten Umsetzungshindernisse dieser Technologie – werden diese durch den Reformvorschlag beseitigt? Die Analyse zeigt, dass dies nur unzureichend der Fall ist.

I. Einleitung

Die *EU-Kommission* hat Anfang des Jahres einen viel diskutieren Reformvorschlag für die Fortentwicklung des europäischen Datenschutzrechts vorgelegt. Er besteht aus einer Gesamtstrategie[1] und Vorschlägen für eine Datenschutz-Grundverordnung (DS-GVO-E)[2] als Ersatz der Datenschutzrichtlinie 95/46/EG (DSRL)[3] sowie für eine Richtlinie im Bereich des Sicherheitsrechts.[4] Ein explizites Ziel ist die Anpassung an die Herausforderungen, die die technischen Innovationen hervorrufen, die seit Verabschiedung der DSRL im Jahre 1995 eingetreten sind.[5] Das betrifft insbesondere das Internet und den einhergehenden Anstieg des internationalen elektronischen Datenverkehrs.

Eine der derzeit am stärksten diskutierten Innovationen ist das Cloud Computing, dem bis 2025 allein in Deutschland ein Marktvolumen von 30 Mrd. Euro vorausgesagt wird.[6] Die hier schon existierenden und in der Entwicklung befindlichen Technologien, Anwendungen und Geschäftsmodelle werden datenschutzrechtlich nach dem Ergebnis der europäischen Reform beurteilt werden. Es ist deshalb aus zwei Gründen wichtig, die Auswirkungen des Reformvorschlags auf das Cloud Computing zu untersuchen: Zum einen müssen Entwickler und Anwender frühzeitig wissen, welche datenschutzrechtlichen Regeln sie künftig einzuhalten haben. Zum anderen muss sich aus der Regulierungsperspektive der Entwurf auch und gerade am Beispiel technischer Innovationen wie dem Cloud Computing bewähren.

II. Cloud Computing und der Datenschutz

Der Begriff „Cloud Computing" wird nicht immer einheitlich verwendet und fasst häufig unterschiedliche Anwendung zusammen,[7] so dass es kaum möglich ist, eine rechtliche Bewertung „des" Cloud Computings vorzunehmen. Allgemeinen kann man dieses verstehen als „ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."[8]

Die Implementierung von Cloud Anwendungen bringt eine Reihe technischer Schwierigkeiten mit sich, auch wenn viele der derzeit als „Cloud" bezeichneten Systeme und Verfahren schon zuvor im Einsatz waren. Verfolgt man die aktuellen Debatten, so kann man allerdings den Eindruck gewinnen, dass die technischen Herausforderungen deutlich leichter zu bewältigen sind als die rechtlichen: Gerade datenschutz- und datensicherheitsrechtliche Fragen werden immer wieder als wesentlicher Unsicherheitsfaktor für Anbieter und Kunden genannt.[9]

Um eine optimale Auslastung von Speicher- und Rechen-Ressourcen zu erreichen, können sich komplexe Cloud-Systeme über weltweit verteilte Cluster erstrecken.[10] Viele der Infrastrukturen haben ihren Ursprung in den USA;[11] der Markt wird von dort ansässigen Unternehmen wie z.B. *Microsoft, Amazon, Oracle, Salesforce, Google, Apple* und *Facebook* dominiert.[12] Technisch ist der damit verbundene weltweite Datentransfer in großen Mengen längst kein Problem mehr: Die Datenströme stoppen nicht an den Ländergrenzen von EU und EWR,[13] wohl aber die Durchsetzbarkeit des europäischen Rechts. Die daraus folgende Notwendigkeit einheitlicher datenschutzrechtlicher Mindeststandards ist überdeutlich, international aber kaum umzusetzen.

Einige technische Besonderheiten treten erschwerend hinzu. Eine genaue Lokalisierung der Daten zu jedem

▷ Prof. Dr. Gerrit Hornung, LL.M., ist Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau und Direktor am dortigen Institute of IT-Security and Security Law (ISL). Stephan Sädtler ist Wissenschaftlicher Mitarbeiter am genannten Lehrstuhl und Fachanwalt für IT-Recht. Der Text ist im Zusammenhang mit dem BMWi-geförderten Projekt „SkIDentity – Vertrauenswürdige Identitäten für die Cloud", FKZ 01MD11031, entstanden.

1 Der Schutz der Privatsphäre in einer vernetzten Welt, KOM(2012) 9 endg.

2 VO zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endg.; s. z.B. *Hornung*, ZD 2012, 99; *Härting*, BB 2012, 459; *Lang*, K&R 2012, 145; *Schneider/Härting*, ZD 2012, 199; *Reding*, ZD 2012, 195; *De Hert/Papakonstantinou*, CLSR 28 (2012), 130.

3 RL 95/46/EG, ABl. EG Nr. L 281 v. 23.11.1995, 31.

4 KOM(2012) 10 endg.; s. *Bäcker/Hornung*, ZD 2012, 147; die RL soll den Rahmenbeschluss 2008/977/JI (ABl. EU Nr. L 350 v. 30.12.2008, 60) ersetzen.

5 S. die Begründung der DS-GVO-E, KOM(2012) 11 endg., 4.

6 S. *Berlecon IDD*, Das wirtschaftliche Potential des Internet der Dienste, 2010, S. 5.

7 Unterschieden wird zum einen zwischen *Infrastructure as a Service (SaaS)*, *Platform as a Service (PaaS)* und *Software as a Service (SaaS)* und zum anderen zwischen privaten, öffentlichen und hybriden Clouds. Auf die Unterschiede wird eingegangen, soweit sie relevant sind.

8 Definition der US-Standardisierungsstelle NIST, s. *https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html*.

9 S. *BITKOM*, Cloud Computing – Evolution in der Technik, Revolution im Business, 2009, S. 38; *Splittgerber/Rockstroh*, BB 2011, 2179 (2180), m.w.N.; zum Ganzen: *Metzger/Reizt/Villar*, Cloud Computing. Chancen und Risiken aus technischer und unternehmerischer Sicht, 2011, S. 47 ff., 141 ff.

10 S. *Metzger/Reizt/Villar*, Cloud Computing. Chancen und Risiken aus technischer und unternehmerischer Sicht, 2011, S. 50; s.a. *Söbbing* in Leible/Sosnitza, Online-Recht 2.0, 2011, S. 35, 40; *BSI*, Sicherheitsempfehlungen für Cloud Computing Anbieter, 2011, S. 19; *Weichert*, DuD 2010, 679 (682).

11 S. *Schmidt-Bens*, Cloud Computing Technologien und Datenschutz, 2012, S. 53.

12 Eine Übersicht über gängige Anbieter und Anwendungen in *Metzger/Reizt/Villar*, Cloud Computing. Chancen und Risiken aus technischer und unternehmerischer Sicht, 2011, S. 90 ff.

13 S. *Reding*, ZD 2012, 195 (196).

Zeitpunkt und die Kontrolle komplexer Cloud-Infrastrukturen sind – jedenfalls aus Nutzersicht – nur bedingt möglich.[14] Verschärft wird die datenschutzrechtliche Problematik zusätzlich durch die Multi-Mandantenfähigkeit der Systeme, bei der einzelne Instanzen (Hardware bzw. Software) in einer gemeinsam genutzten Umgebung vielen Nutzern zur Verfügung stehen.[15] Da in vielen Cloud-Anwendungen aufgrund von Virtualisierung keine physikalische Trennung der Daten stattfindet, besteht ein erhöhtes Risiko eines unautorisierten Datenzugriffs durch Dritte, wenn keine ausreichenden Vorkehrungen zur abgesicherten Mandantentrennung getroffen werden.[16]

Überdies sind gängige Verschlüsselungstechniken nur eingeschränkt nutzbar, die ansonsten viele datenschutzrechtliche Probleme lösen können.[17] Zwar wird es häufig möglich sein, die Daten auf dem Transportweg und auf den Servern des Providers zu verschlüsseln. Wenn dieser jedoch eine Entschlüsselungsmöglichkeit hat, bleiben wichtige Datenschutzfragen (insbesondere die Datenübermittlung in Drittstaaten) bestehen. Die vorzugswürdige Verschlüsselung auf dem System des Nutzers[18] ist für aktuelle Cloud-Anwendungen nur sehr beschränkt nutzbar, da die Verarbeitung verschlüsselter Daten zwar erforscht wird, derzeit aber noch nicht praxistauglich ist.[19] Eine Ende-zu-Ende Verschlüsselung ist deshalb nur beim reinen Daten-Storage möglich.

Schließlich liegt sog. Business-Clouds (etwa bei der Dokumentation und Verwaltung von Kundendaten in Customer-Relationship-Management-Systemen)[20] regelmäßig ein Mehrpersonenverhältnis zugrunde. Das führt zu komplizierten vertragsrechtlichen Konstellationen, v.a., wenn Cloud Provider sich weltweiter Subunternehmer bedienen. Daraus resultieren insbesondere Probleme im Bereich der Auftragsdatenverarbeitung.[21] Insgesamt kann festgehalten werden, dass die datenschutzrechtliche Zulässigkeit des Cloud Computings weithin ungeklärt ist und bisher in der Diskussion mehr Fragen aufgeworfen als Antworten gegeben werden.

III. Folgen des Reformvorschlags

Gemäß Art. 2 DS-GVO-E werden vorbehaltlich vorrangiger Regelungen des Datenschutzes in der elektronischen Kommunikation[22] alle Anwendungen des Cloud Computings erfasst, in denen personenbezogene Daten verarbeitet werden. Wie bisher in Deutschland bleiben unternehmensbezogene Daten außen vor.[23] Entsprechend dem allgemeinen Regelungsziel der Technikneutralität enthält der Entwurf keine cloud-spezifischen Regelungen. Viele der vorgeschlagenen Bestimmungen sind allerdings für das Cloud Computing als Querschnittsmaterie von weitreichender Bedeutung und führen hier zu besonderen Problemen.

1. Ziele und Wechsel zur Verordnung

Die Ziele des Verordnungsentwurfs der *EU-Kommission* entsprechen denen der DSRL, nämlich Harmonisierung und freier Datenverkehr einerseits, hohes Datenschutzniveau andererseits.[24] Diese Ziele können in Konflikt geraten, ihr Spannungsverhältnis kann aber auch durch ein einheitliches und unmittelbar bindendes Regelungsgefüge aufgelöst werden. Hierzu schlägt die Kommission den Wechsel zum Instrument der Verordnung vor, deren unmittelbare Anwendbarkeit (Art. 288 Abs. 2 AEUV) erhebliche Folgen für Cloud Provider, ihre Kunden, betroffene Dritte, Aufsichtsbehörden und Gerichte mit sich bringen würde.[25] Anzuwenden wäre nicht mehr deutsches Datenschutzrecht, sondern direkt die DS-GVO-E, für deren Auslegung der EuGH im Vorabentscheidungsverfahren (Art. 267 Abs. 1 lit. b AEUV) zuständig wäre. Weite Teile der deutschen bereichsspezifischen Regelungen würden obsolet.[26] Dieser Effekt ginge weit über die Harmonisierungswirkung der DSRL hinaus, die nach Ansicht des EuGH zwar zu einer „grundsätzlich umfassenden Harmonisierung“[27] führt, aber den Mitgliedstaaten dennoch einen weiten Handlungsspielraum einräumt und sie ermächtigt, für bestimmte Fälle besondere Regelungen beizubehalten oder einzuführen, solange dies im Einklang mit dem Ziel der Richtlinie geschieht, ein Gleichgewicht zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre zu wahren.[28]

Es lässt sich zwar beobachten, dass sich der Entwurf teilweise an die deutschen Vorschriften anlehnt.[29] Er enthält aber auch Abweichung zu Lasten der Betroffenen, wie z.B. den Verzicht auf die Schriftform der Einwilligung (Art. 7 DS-GVO-E) und die Bestellpflicht eines betrieblichen Datenschutzbeauftragten erst ab 250 Mitarbeitern (Art. 35 Abs. 1 lit. b DS-GVO-E). Aus der europäischen Gesamtsicht besteht demgegenüber eine wesentliche Verbesserung darin, dass das Datenschutzniveau in einigen anderen Mitgliedstaaten angehoben wird. Die durch den Wechsel zur Verordnung angestrebte Harmo-

14 S. *Söbbing* in Leible/Sosnitza, Online-Recht 2.0, 2011, S. 61, der die Lokalisierungsmöglichkeiten auch für den Cloud Provider in Frage stellt; *Velev/Zlateva* in Camenisch/Kisimov/Dubovitskaya, Open Research Problems in Network Security, LNCS 6555/2011, S. 140, 143; *Art. 29 Datenschutzgruppe*, Opinion 05/2012 on Cloud Computing, 2012, S. 17.

15 S. *BITKOM*, Cloud Computing – Evolution in der Technik, Revolution im Business, 2009, S. 24.

16 S. *http://www.computerwoche.de/management/cloud-computing/2363872/index2.html.*

17 Hierzu *Heidrich/Wegener*, MMR 2010, 803 (804 f.); *Schmidt-Bens*, Cloud Computing Technologien und Datenschutz, 2012, S. 73 f.

18 S. *BSI*, Sicherheitsempfehlungen für Cloud Computing Anbieter, 2011, S. 36.

19 S. *http://www.heise.de/-1021361.html; Schmidt-Bens*, Cloud Computing Technologien und Datenschutz, 2012, S. 74.

20 Ähnlich die Konstellation, die der Bewertung der *Art. 29 Datenschutzgruppe*, Opinion 05/2012 on Cloud Computing, 2012, S. 4) zugrunde liegt.

21 S. z.B. *Metzger/Reizt/Villar*, Cloud Computing. Chancen und Risiken aus technischer und unternehmerischer Sicht, 2011, S. 55; s.a. unten III.4.

22 Die RL 2002/58/EG (ABl. EG 2002 Nr. L 201, 37) in der zuletzt durch Art. 2 der Richtlinie 2009/136/EG (ABl. EG 2009 Nr. L 337, 11) geänderten Form wird durch den Reformvorschlag nicht berührt.

23 Derartige Cloud-Anwendungen erzeugen allerdings zumeist immer noch personenbezogene Bestands- und Nutzungsdaten. Die Auswirkungen des Entwurfs auf Länder wie Österreich, in denen das Datenschutzrecht auch Daten juristischer Personen erfasst (s. *Knyrim*, Datenschutzrecht, 2. Aufl. 2012, S. 11 f.), sind bislang unklar.

24 S. die Begründung der DS-GVO-E, KOM (2012) 11 endg., 1; zur DSRL *Ehmann/Helfrich*, EG-DSRL, 1999, Einl. Rz. 4.

25 S. *Hornung*, ZD 2012, 99 (100).

26 Kritisch hierzu z.B. der Bundesrat, BR-Drucks. 52/12 (B), 2.

27 EuGH, Urt. v. 6.11.2003 – Rs. C-101/01, CR 2004, 286 = Slg. 2003, I-12971 – Lindqvist – Rz. 96; bekräftig in EuGH, Urt. v. 16.12.2008 – Rs. C-524/06, CR 2009, 581 = EuZW 2009, 183 – Huber Rz. 51.

28 EuGH, Urt. v. 6.11.2003 – Rs. C-101/01, CR 2004, 286 = Slg. 2003, I-12971 – Lindqvist Rz. 97; s. insoweit einerseits eher die Spielräume betonend: *Jacob*, RDV 1993, 11; *Simitis*, NJW 1998, 2473 (2476); *Simitis*, DuD 2000, 714; *Simitis*, NJW 1997, 281 (282); *Dammann/Simitis*, EG-DSRL, 1997, Einl. Rz. 10; *Roßnagel/Pfitzmann/Garstka* Modernisierung des Datenschutzrechts, 2001, S. 55 ff.; andererseits eher für nur geringe Regelungsmöglichkeiten der Mitgliedstaaten *Brühann*, EuZW 2009, 639 ff.; *Hoeren*, RDV 2009, 89 ff.; differenzierend *Lütkemeier*, DuD 1995, 597 (598).

29 So auch die zuständige Kommissarin, s. *Reding*, ZD 2012, 195 (197).

nisierung ist auch aus Anbietersicht erforderlich,[30] weil diese sonst ihre Geschäftsmodelle nach einer Vielzahl unterschiedlicher Rechtsordnungen ausrichten müssten. Zwar wird mit der DS-GVO-E im weltweiten Cloud Markt nur eine Teilharmonisierung erzielt. Immerhin werden aber europäische Angebote ermöglicht – und vielleicht sogar Anreize für weltweite Standards gesetzt.

Auch innerhalb Europas bleiben allerdings noch Unsicherheiten: Die DS-GVO-E ist trotz des Anwachsens des Regelungsumfangs immer noch sehr generisch formuliert, so dass sich die konkreten Pflichten der Anbieter weithin erst aus den Ausführungsbestimmungen der *EU-Kommission* ergeben werden. Außerdem werden die harmonisierten Regeln immer noch durch nationale Behörden angewendet, die sie unterschiedlich auslegen können. Dies zu vermeiden ist Sinn und Zweck des komplizierten Kohärenzverfahrens nach Art. 57 ff. DS-GVO-E.[31]

2. Räumlicher Anwendungsbereich

Eine wichtige Neuerung mit Auswirkungen insbesondere auf das Cloud Computing enthalten die Vorschriften über den räumlichen Anwendungsbereich in Art. 3 DS-GVO-E. Während ähnlich wie bisher Tätigkeiten einer Niederlassung eines Verantwortlichen oder (nunmehr ausdrücklich) eines Auftragsverarbeiters in der EU erfasst sind (Art. 3 Abs. 1 DS-GVO-E), ergeben sich Änderungen für Verantwortliche außerhalb der EU und des EWR.[32] Diese sind bisher nach Art. 4 Abs. 1 lit. c DSRL erfasst, wenn sie zur Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreifen, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass die Mittel nur zur Durchfuhr verwendet werden. In Deutschland wird dies durch die abweichende Formulierung in § 1 Abs. 5 Satz 2 BDSG umgesetzt, wonach entscheidend ist, ob „im Inland" personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Diese Abweichung ist einer der Gründe für die umstrittene Frage, wann eine Erhebung über das Internet stattfindet, sofern sich Server eines Unternehmens außerhalb der EU oder des EWR befinden.[33]

Nunmehr schlägt die *EU-Kommission* gem. Art. 3 Nr. 2 DS-GVO-E vor, Verantwortliche außerhalb der EU zu erfassen, deren Datenverarbeitung entweder dazu dient, in der EU ansässigen Personen „in der Union Waren oder Dienstleistungen anzubieten" (lit. a) oder der Beobachtung ihres Verhaltens dient (lit. b). Insoweit würde die Verordnung Klarheit schaffen, allerdings das neue Problem aufwerfen, wann eine Cloud-Dienstleistung i.S.v. Art. 3 Nr. 2 lit. a DS-GVO-E den Betroffenen „in der Union" angeboten wird. Da dies nur im Zweipersonenverhältnis mit dem Cloud Provider erfolgen kann, werden Cloud Provider außerdem nicht erfasst, wenn ein in der EU ansässiges Unternehmen seine Kundendaten in die Cloud transferiert: Dieses (unternehmensbezogene) Angebot wird regelmäßig nicht dazu dienen, den betroffenen Kunden Waren oder Dienstleistungen anzubieten. Das EU-Unternehmen und seine Datenübermittlung unterfallen dann zwar der DS-GVO-E, der außereuropäische Cloud Provider jedoch anders als im Zweipersonenverhältnis nicht.

Im Zweipersonenverhältnis wird es oftmals zur Anwendbarkeit der DS-GVO-E kommen, wenn Anbieter Dienstleistungen direkt für den europäischen Markt anbieten. Dies kann zu weitreichenden Pflichten für Cloud Provider führen, die z.B. bei der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten nach Art. 35 DS-GVO-E auch ihre interne Organisation betreffen. Völlig unklar – und in Art. 51 DS-GVO-E ungeregelt – ist, welche Aufsichtsbehörde zuständig sein soll.[34] Eine Aufsicht europäischer Behörden ist schon aus völkerrechtlichen Gründen nicht möglich, im Ausland gibt es jedoch nicht immer vergleichbare Stellen. Eine Reihe von Pflichten, die nach dem Vorstehenden auch außereuropäische Cloud Provider treffen, sind aber ohne eine Aufsichtsbehörde nicht oder nicht vollständig erfüllbar (z.B. Art. 28 Abs. 3, Art. 29, Art. 31, Art. 32, Art. 34 und Art. 37 DS-GVO-E).

Ein ungelöstes Problem ist daneben, dass die daraus folgende Anwendbarkeit europäischen Datenschutzrechts mit Normen des Sitzlands in Konflikt kommen kann. Dies stellt z.B. US-Anbieter vor Probleme, die weitreichenden Eingriffsbefugnisse der US-Behörden (u.a. eDiscovery-Regelungen, Patriot Act und Foreign Intelligence Surveillance Act)[35] unterliegen. Diese und andere Gesetze verpflichten US-Unternehmen – und Tochterunternehmen mit Sitz in EU oder EWR – auf Verlangen zur Herausgabe von Daten an Gerichte und Behörden und werden in Bezug auf Kriterien und Verfahren als nicht konform mit europäischen Datenschutzstandards erachtet.[36] Der durch US-amerikanische Unternehmen beherrschte Markt könnte hierdurch entscheidend verändert werden, da nunmehr nicht mehr nur der Datenexporteur, sondern auch der Datenempfänger, z.B. der Cloud Provider oder Subunternehmer sich in einem derzeit scheinbar unauflösbaren Dilemma befänden.

3. Verarbeitungsgrundlage, Betroffenenrechte und Pflichten der Verantwortlichen

a) Rechtsgrundlage

Art. 6 DS-GVO-E hält – trotz teilweiser Kritik[37] – am allgemeinen Verbotsprinzip fest. Aus dem Katalog der Erlaubnistatbestände werden für Cloud Provider vor allem die Erfüllung eines Vertrages (lit. b) und die Einwilligung (lit. a) in Betracht kommen.

Bei direkter Rechtsbeziehung zwischen Anbieter und Betroffenem (Zweipersonenverhältnis) bildet regelmäßig der Vertrag die Rechtsgrundlage. Fehlt dieser, bleibt die Rolle der Einwilligung zu klären (Art. 7 i.V.m. Art. 6 Abs. 1 lit. a DS-GVO-E), die bisher als für das Cloud Computing wenig praktikabel gilt.[38] In Mehrpersonen-

30 S. *BITKOM/VOICE*, Empfehlungen für den Cloud Computing-Standort Deutschland, 2012, S. 9.

31 Dieses wirft eigene kompetentielle Probleme auf (*Hornung*, ZD 2012, 99 [105]), die allerdings für die Cloud Provider weniger relevant sind.

32 S. *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 1 Rz. 28; *Hornung*, ZD 2012, 99 (102).

33 Dazu *Dammann* in Simitis, BDSG, 7. Aufl. 2011, § 1 Rz. 217 ff., 223 f.; *Jotzo*, MMR 2009, 232 (235 ff.); in diesem Zusammenhang auch *Art. 29 Datenschutzgruppe*, Opinion 08/2010 on Applicable Law, 2010, S. 30 f.

34 S. BR-Drucks. 52/12 (B) (2), 20.

35 S. *Hansen*, DuD 2012, 407 (410); *Nägele/Jacobs*, ZUM 2010, 281 (290); *Spies*, ZD-Aktuell 2012, 03062; zur Gefahr des Zugriffs durch Drittstaaten *Art. 29 Datenschutzgruppe*, Opinion 05/2012 on Cloud Computing, 2012, S. 5.

36 S. *ULD, https://www.datenschutzzentrum.de/internationales/20111115-patriot-act.html*; s.a. *http://business.chip.de/news/Exklusiv-EU-Datenschutz-geht-ueber-US-Patriot-Act_50158975.html*.

37 S. z.B. *Schneider*, AnwBl. 2011, 233 ff.; *Härting*, BB 2102, 459 (460); a.A. *Hornung*, ZD 2012, 99 (101).

38 S. *BITKOM*, Cloud Computing – Evolution in der Technik, Revolution im Business, 2009, S. 52; für Altverträge ebenso *Schmidt-Bens*, Cloud Computing Technologien und Datenschutz, 2012, S. 29.

verhältnissen verschärft sich das Problem: Wenn Unternehmen ihre Kundendaten in Cloud Anwendungen verarbeiten wollen, wird dies häufig nicht für den Vertragszweck erforderlich sein, so dass hier ausschließlich die Einwilligung weiter hilft. Hier enthält der Entwurf Änderungen gegenüber dem deutschen Recht: Erstens besteht – wie in Art. 7 lit. a DSRL, aber anders als in § 4a Abs. 1 Satz 3 BDSG – kein grundsätzliches Schriftformerfordernis, auch wenn wegen der Beweislast des Verantwortlichen (Art. 7 Abs. 1 DS-GVO-E) zu einer sicheren Dokumentation geraten werden muss.[39] Zweitens setzt Art. 7 i.V.m. Art. 4 Nr. 8 DS-GVO-E die „Kenntnis der Sachlage" voraus. Dies entspricht Art. 2 lit. h DSRL,[40] ist aber eine Abschwächung zu den Informationspflichten aus § 4a Abs. 1 Satz 2 BDSG. Drittens schließt Art. 7 Abs. 4 DS-GVO-E eine Einwilligung explizit für den Fall eines „erheblichen Ungleichgewichts" aus. Dies könnte Cloud-Anwendungen im Arbeitsverhältnis betreffen.[41] Jenseits derartiger Fälle ist aber unklar, wann im Cloud Bereich ein so starkes Ungleichgewicht vorliegt, dass es auch unter Berücksichtigung des Grundsatzes der Selbstbestimmtheit die Einschränkung rechtfertigt.[42] Hierfür werden wirtschaftliche Abhängigkeiten, die individuelle Situation des Betroffenen und die Verfügbarkeit zumutbarer Alternativen zu berücksichtigen sein.

b) Vergessenwerden und Datenübertragbarkeit

Der Entwurf enthält neben den bekannten Betroffenenrechten auch zwei neue, nämlich die Rechte auf Vergessenwerden (Art. 17 Abs. 2 DS-GVO-E) und Datenübertragbarkeit (Art. 18 DS-GVO-E). Ersteres wird von der *EU-Kommission* besonders hervorgehoben, ist der Sache nach allerdings lediglich eine Informationspflicht im Fall der Veröffentlichung von Daten, wenn die veröffentlichende Stelle die Daten im Anschluss selbst löschen muss. Da Cloud Computing nicht auf die Veröffentlichung von Daten zielt, ergeben sich keine spezifischen Probleme.

Demgegenüber müssen sich Cloud Provider, die im Endkundenbereich tätig sind, auf das neue Recht auf Datenübertragbarkeit einstellen. Es soll den Betroffen vor Lock-In-Effekten schützen, indem es einen problemlosen Anbieterwechsel ermöglicht.[43] Soweit also personenbezogene Daten „elektronisch in einem strukturierten gängigen elektronischen Format verarbeitet" werden (dies dürfte mit zunehmender Standardisierung häufig der Fall sein), darf der Betroffene eine Kopie verlangen und die Daten zu einem anderen Anbieter überführen, ohne dabei vom ersten Anbieter behindert zu werden. Es bleibt abzuwarten, welche Auswirkungen dies auf die Geschäftsmodelle der Cloud Provider haben wird.[44] So dürfte die Umsetzung bei reinen Storage-Angeboten eher unproblematisch sein. Jedenfalls wird das Recht auf Datenübertragbarkeit aber im Mehrpersonenverhältnis zu Problemen führen, da es dem Betroffenen zusteht, der hier jedoch nicht mit dem Vertragspartner des Cloud Providers identisch ist. In diesen Fällen vermag der normierte Anspruch des Betroffenen aus Art. 18 Abs. 2 DS-GVO-E sog. vertragliche „Exit-Klauseln" zugunsten des Cloud-Anwenders nicht zu ersetzen.

c) Transparenzpflichten

Bei den Vorgaben fallen Neuerungen der Transparenzpflichten auf, die in Art. 11 ff. DS-GVO-E und an mehreren anderen Stellen erheblich detaillierter ausfallen. So statuiert Art. 5 lit. a DS-GVO-E die Verarbeitung in einer „für die betroffene Person nachvollziehbaren Weise", Art. 11 DS-GVO-E fordert darüber hinaus eine „nachvollziehbare und für jedermann leicht zugängliche Strategie" für die Verarbeitung. Entgegen der Kritik der Werbewirtschaft[45] handelt es sich hierbei gerade wegen der vielfach unübersichtlichen Struktur der Verarbeitungsprozesse um sinnvolle Vorschläge. Die Aufgabe – der sich insbesondere die *EU-Kommission* im Rahmen der Verabschiedung von Ausführungsbestimmungen stellen muss – liegt darin, insbesondere kleine und mittlere Unternehmen nicht zu überfordern. Große, professionell arbeitende Anbieter im Bereich des Cloud Computings werden dagegen regelmäßig über entsprechende interne Vorgaben und Dokumentationen verfügen. Hier bestehen zwei Herausforderungen: Zum einen ist eine sinnvolle Abgrenzung der Pflichten im Mehrpersonenverhältnis vorzunehmen, um die Cloud Nutzer, die die Daten ihrer Kunden in der Cloud verarbeiten wollen, nicht zu überfordern. Zum anderen dürfen bei aller Transparenz die legitimen Interessen der Anbieter nicht übergangen werden, keine schützenswerten Unternehmensinformationen zu offenbaren. Das gilt umso mehr, als im Cloud-Bereich die technische Organisation der Datenhaltung wesentlicher Bestandteil des Betriebsmodells ist und deshalb entsprechend gehütet wird.[46] Eine Lösung könnten unabhängige Prüfungen im Bereich von Zertifizierungen, Datenschutzsiegeln und -zeichen bilden.[47]

d) Melde- und Benachrichtigungspflichten

Der Stärkung der Transparenz dienen auch die in Art. 31 und 32 DS-GVO-E enthaltenen Melde- und Benachrichtigungspflichten („data breach notification"). Dieses sinnvolle Instrument ist auf der Basis US-amerikanischer Vorbilder seit 2009 bereits in Art. 4 Abs. 3 und 4 der Datenschutzrichtlinie für die elektronische Kommunikation (2002/58/EG)[48] enthalten und in Deutschland neben der Umsetzung in § 93 Abs. 3 i.V.m. § 109a TKG auch in § 42a BDSG, § 83a SGB X und § 15a TMG eingeführt worden.[49] Für deutsche Anbieter würden sich hier vor allem zwei Punkte ändern. Zum einen greifen die Art. 31 und 32 DS-GVO-E bei jeder „Verletzung des Schutzes personenbezogener Daten" (Art. 4 Abs. 9 DS-GVO-E). Dies gilt auch für § 109a TKG, nicht jedoch für § 42a BDSG, § 83a SGB X und § 15a TMG, die das Drohen einer „schwerwiegenden Beeinträchtigung" verlangen. Zum anderen enthält der Vorschlag eine Frist

39 S. *Hornung*, ZD 2012, 99, 102 f.

40 So auch *Breilinger/Scheuing*, RDV 2012, 64 (70).

41 S. Vorbemerkung (34) der DS-GVO-E, KOM(2012) 11 endg., 25.

42 Grundsätzlich kritisch *Schneider/Härting*, ZD 2012, 199 (201 f.); *Härting*, BB 2102, 459 (463).

43 S. *Hornung*, ZD 2012, 99 (103); *Art. 29 Datenschutzgruppe*, Opinion 05/2012 on Cloud Computing, 2012, S. 5.

44 So kritisiert z.B. *Microsoft* wegen des schnellen technischen Wandels und der Systemvielfalt die Möglichkeit der Kommission, gem. Art. 18 Abs. 3 DS-GVO-E technische Standards vorzuschreiben, s. *http://www.microsoft.eu/Portals/0/Document/Technology%20Policy/Microsoft%20position%20on%20EU%20Privacy%20Regulation%20-%20February%202012.pdf*, S. 5.

45 S. *http://www.heise.de/-1586145.html:* Die Kommission solle „keinen Kampf gegen die Wirtschaft führen".

46 *Metzger/Reizt/Villar*, Cloud Computing. Chancen und Risiken aus technischer und unternehmerischer Sicht, 2011, S. 51.

47 S. dazu noch unten III. 6.

48 I.d. Fassung der RL 2009/136/EG v. 25.11.2009 zur Änderung der RL 2002/22/EG, der RL 2002/58/EG und der Verordnung (EG) Nr. 2006/2004, ABl. EU 2009 Nr. L 337, 11.

49 Näher z.B. *Gabel*, BB 2009, 2045; *Eckhardt/Schmitz*, DuD 2010, 390; *Ernst*, DuD 2010, 472; *Hanloser*, MMR 2010, 300; *Hornung*, NJW 2010, 1841.

von lediglich 24 Stunden für die Meldung. Dies könnte in der Praxis vor allem bei komplexen Strukturen wie im Cloud Computing zu Problemen führen. Allerdings sieht Art. 31 Abs. 1 Satz 2 DS-GVO-E auch die Möglichkeit einer späteren Meldung vor, sofern dieser eine entsprechende Begründung beigefügt wird. Als Begründung sollte insbesondere der interne Ermittlungsaufwand in komplizierten Fällen akzeptiert werden. Denkbar ist auch eine zweistufige Meldung zunächst über die Tatsache, dann über Einzelheiten des Vorfalls. Wenn diese Optionen praxisgerecht umgesetzt werden, dürfte sich die Kritik an der Frist als unberechtigt herausstellen.

e) Betriebliche Datenschutzbeauftragte

Während in Deutschland schon lange verbindliche Vorgaben für die Einrichtung betrieblicher Datenschutzbeauftragter bestehen, führt der Entwurf diese erstmals auch auf EU-Ebene ein. Nicht-hoheitliche[50] Cloud Provider müssten einen Datenschutzbeauftragen bestellen, wenn sie entweder 250 oder mehr Mitarbeiter beschäftigen (Art. 35 Abs. 1 lit. b DS-GVO-E) oder ihre Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung erforderlich machen (lit. c).[51] Dies gilt gem. Art. 3 Abs. 2 lit. a DS-GVO-E auch für die Unternehmen, die Cloud-Angebote an Personen in der EU richten. Die Mitarbeiterzahl in Art. 35 Abs. 1 lit. b DS-GVO-E ist zu hoch gewählt und in ihrer Absolutheit als Kriterium ungeeignet.[52] Dem kommt aber im Rahmen des Cloud Computings weniger Relevanz zu, da in aller Regel lit. c greifen wird.

f) Sanktionsmöglichkeiten

Letztendlich steht und fällt die Wirksamkeit der Rechte und Pflichten mit den Sanktionsmöglichkeiten, die öffentlich-rechtlich (Bußgelder) oder zivilrechtlich (Schadensersatz) sein können. Die *EU-Kommission* hat hier erhebliche Erweiterungen und Präzisierungen vorgenommen. Besonders hart könnten weltweit operierende Cloud Provider getroffen werden, weil sich die Geldbußen nach dem weltweiten Jahresumsatz berechnen und bis zu 2 % von diesem erreichen können (Art. 79 Abs. 6 DS-GVO-E). Daneben gewährt Art. 77 DS-GVO-E einen Schadensersatzanspruch. Dieser basiert auf Art. 23 DSRL und ist um einen direkten Anspruch gegen den Auftragsverarbeiter erweitert. Ungelöst bleibt dabei aber weiterhin die Bemessung des Schadens; insbesondere fehlt eine Regelung zu immateriellen Schäden.[53]

Weitere Sanktionen regeln die Mitgliedstaaten (Art. 78 Abs. 1 DS-GVO-E); diese müssen wirksam, verhältnismäßig und abschreckend sein (Art. 78 Abs. 1 Satz 3 DS-GVO-E). Zu denken ist in Bezug auf den Abschreckungseffekt an die Einführung verhältnismäßig hoher Streitwerte, wie man sie aus dem deutschen Urheber- oder Wettbewerbsrecht kennt. Gerade im Bereich des Cloud Computings könnte dies aber auch den Missbrauch fördern.

4. Auftragsdatenverarbeitung

Ein Cloud Provider wird im Mehrpersonenverhältnis regelmäßig als Auftragsverarbeiter (Art. 4 Abs. 6 DS-GVO-E) des Cloud Nutzers fungieren, der wiederum Verantwortlicher gegenüber dem Betroffenen bleibt.[54] Der Anbieter wird sich wiederum regelmäßig weiterer Subunternehmer in Drittstaaten zur Erfüllung seiner Vertragspflichten bedienen, so z.B. bei der Anmietung von Speicherplatz.[55] Wie in Art. 17 Abs. 2, Abs. 3 DSRL und (viel detaillierter) § 11 Abs. 2 BDSG muss die Grundlage einer wirksamen Auftragsdatenverarbeitung ein Vertrag mit weithin vorgegebenem Inhalt sein (Art. 26 Abs. 2 DS-GVO-E). Anders als bisher wird aber explizit die Rechtsfolge eines Verstoßes gegen diesen Vertrag klargestellt: Der Auftragsverarbeiter gilt gem. Art. 26 Abs. 4 DS-GVO-E selbst als Verantwortlicher.[56]

Auch im Übrigen entspricht Art. 26 in weiten Teilen § 11 BDSG[57] und regelt die Auftragsdatenverarbeitung damit erheblich detaillierter als die DSRL. Das gilt insbesondere für den sehr feingranular vorgegebenen Inhalt der einzelnen Teile des Auftragsverhältnisses in Art. 26 Abs. 2 DS-GVO-E. Allerdings wird im Rahmen des Anforderungskataloges zu Recht das Fehlen von Angaben zu Gegenstand und Dauer des Auftrags, Umfang, Art und Zweck der Verarbeitung, der Datenart und dem Kreis der Betroffenen bemängelt.[58]

Schon die Überschrift zu Kapitel IV schließt Auftragsverarbeiter ein und bringt so zum Ausdruck, dass ihre Pflichten detaillierter werden. Sie sind ebenso wie die Verantwortlichen zur Dokumentation verpflichtet (Art. 28 DS-GVO-E), müssen mit der Aufsichtsbehörde zusammenarbeiten (Art. 29 DS-GVO-E), technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung treffen (Art. 30 DS-GVO-E), Auftraggeber über „Datenpannen" informieren (Art. 31 Abs. 2 DS-GVO-E), unter bestimmten Voraussetzungen eine Datenschutz-Folgenabschätzung durchführen (Art. 33 Abs. 1 DS-GVO-E) oder eine Vorabgenehmigung einholen (Art. 34 Abs. 1 DS-GVO-E), einen (eigenen)[59] Datenschutzbeauftragten benennen (Art. 35 Abs. 1 DS-GVO-E) sowie die Regeln zur Übermittlung in Drittländer einhalten (Art. 40 ff. DS-GVO-E). Die Befugnisse der Aufsichtsbehörden nach Art. 53 DS-GVO-E können sich nunmehr ausdrücklich auch an Auftragsverarbeiter richten. Im Ergebnis werden Cloud Provider in Auftragsverhältnissen weithin den Verantwortlichen gleichgestellt.

50 Für die ebenfalls diskutierten „privaten öffentlichen", also verwaltungseigenen Clouds ist nach Art. 35 Abs. 1 lit. a DS-GVO-E in jedem Fall ein Datenschutzbeauftragter zu bestellen.

51 Die Formulierung „von betroffenen Personen" im Entwurfstext (anders EG 75) ist nach Auskunft aus der Kommission ein Redaktionsfehler.

52 S. *Hornung*, ZD 2012, 104; *Gola*, EuZW 2012, 332 (333); s.a. die Stellungnahmen der *GDD*, *https://www.gdd.de/nachrichten/arbeitshilfen/Stellungnahme%20DS-GVO-E%20endgx.pdf*, S. 3 f. und des *BVD*, *https://www.bvdnet.de/fileadmin/BvD_eV/pdf_und_bilder/bvd-allgemein/Stellungnahme_BvD_Entwurf_EU_Datenschutzverordnung_1203 2012.pdf*, S. 4.

53 S. *Schneider/Härting*, ZD 2012, 199 (202).

54 Zu dieser Einordnung nach § 11 BDSG *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 11 Rz. 8; *Petri* in Simitis, BDSG, 7. Aufl. 2011, § 11 Rz. 30; *Weichert*, DuD 2010, 679 (682); *Schulz*, MMR 2010, 75 (78); *AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Orientierungshilfe Cloud Computing, 2011, S. 8 ff.

55 S. *BITKOM*, Cloud Computing – Was Entscheider wissen müssen, 2010, S. 66; *AK Technik und Medien*, Orientierungshilfe Cloud Computing, 2011, S. 8; *Art. 29 Datenschutzgruppe*, Opinion 05/2012 on Cloud Computing, 2012, S. 6, 9.

56 Bisher kann diesem Problem vorrangig nur mit der Aufnahme eine Vertragsstrafenregelung angemessen beigekommen werden, vgl. dazu *AK Technik und Medien*, Orientierungshilfe Cloud Computing, 2011, S. 8.

57 S. auch *Lang*, K&R 2012, 145 (149).

58 So der Bundesrat, BR-Drucks. 52/12 (B) (2), 16; *GDD*, *https://www.gdd.de/nachrichten/arbeitshilfen/Stellungnahme%20DS-GVO-E%20endgx.pdf*, S. 12.

59 Bislang ist zumindest in Deutschland der Datenschutzbeauftragte des Auftraggebers auch für die Datenverarbeitung beim Auftragnehmer zuständig, s. *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 11 Rz. 21a.

Schließlich haften Cloud Provider als Auftragsverarbeiter selbst (Art. 75 und Art. 77 DS-GVO-E) statt wie bisher grundsätzlich nur vertraglich gegenüber dem Anwender. Der Betroffene hat derzeit Ansprüche gegen den Verantwortlichen (Art. 23 DSRL, § 11 Abs. 1 Satz 2 i.V.m. § § 7, 8 BDSG) und erhielte durch Art. 77 DS-GVO-E in dem Auftragsverarbeiter einen anderen Schuldner (Abs. 1, wenn nur der Auftragsverarbeiter verantwortlich ist); im Fall gemeinschaftlicher Verantwortlichkeit besteht Gesamtschuldnerschaft (Abs. 2).

a) Subunternehmer

Während die – weitgehend übliche – Einschaltung von Subunternehmern durch den Cloud Provider als Auftragsverarbeiter bisher meist Verhandlungssache der Parteien ist, bedarf der Provider gem. Art. 26 Abs. 2 lit. d DS-GVO-E der vorherigen Zustimmung des Cloud Anwenders als Auftraggeber. Diese Vorschrift dürfte erhebliche Auswirkungen auf die Flexibilität[60] von Cloud-Anwendungen haben, da die Fluktuation der Subunternehmer typisch und zu Beginn des Vertragsverhältnisses oft noch nicht bekannt ist, wo und durch wen die Daten z.B. bei einem nur kurzzeitig gestiegenen Bedarf an Rechenleistung verarbeitet werden.[61] Als Folge ist die Einbeziehung von Unteranbietern bislang häufig für den Kunden intransparent.[62] Dies wäre in Zukunft mit Art. 26 Abs. 2 lit. d DS-GVO-E nicht vereinbar. Eine Lösung könnte darin liegen, den Auftragsverarbeiter relativ allgemein zur Einbeziehung von Unterauftragnehmern zu ermächtigen, ohne diese und die konkreten Verarbeitungsvorgänge (ganz) exakt zu benennen. Mit Blick auf den Schutzzweck der Regelung werden einer solchen Vertragsgestaltung allerdings Grenzen gesetzt sein. So wird man zumindest die Benennung des Unterauftragnehmers verlangen müssen, da ansonsten der von Art. 26 Abs. 1 DS-GVO-E vorgegebene Sorgfaltsmaßstab bei der Auswahl von Auftragsverarbeitern ausgehebelt würde. Demgegenüber könnte man bei der konkreten Inanspruchnahme eines Subunternehmers mehr Flexibilität zulassen. In jedem Fall muss aber gewährleistet sein, dass dem Subunternehmer dieselben Pflichten auferlegt werden, wie dem Auftragsverarbeiter.[63]

b) Compliance Kontrolle

Wie bisher stehen dem Cloud Nutzer als Auftraggeber weitgehende Weisungsbefugnisse zu (Art. 26 Abs. 2 lit. a DS-GVO-E), und er muss sich von der Einhaltung der Pflichten überzeugen (lit. h). Zur umstrittenen Frage der Pflicht des Auftraggebers zur Prüfung vor Ort[64] enthält die DS-GVO-O keine Regelung.[65] Schon bisher werden die Vorgaben in der Praxis kaum im Sinne einer individuellen Kontrolle durch die Auftraggeber umgesetzt. Hintergrund ist, dass Auftragnehmer zwar rechtlich untergeordnet sein sollen, tatsächlich aber professionelle Anbieter von Rechenzentren und anderen Infrastrukturen sind. Sie geben faktisch die Art und Weise der Datenverarbeitung vor, sind nur eingeschränkt bereit, diese anzupassen und stehen aufgrund ihrer Betriebs- und Geschäftsgeheimnisse detaillierten Kontrollen durch ihre Kunden skeptisch gegenüber. Diese Probleme sind im Bereich des Cloud Computings noch größer als bei anderen Auftragsverhältnissen. Gerade gegenüber weltweit operierenden (US-)Konzernen ist die Durchsetzung effektiver Kontrollen jedes einzelnen Cloud Kunden unrealistisch. Eine Lösung kann hier nur im Bereich zertifizierter Kontrollmechanismen liegen, auf die die Kunden der Cloud Provider vertrauen dürfen. Derartige Mechanismen sind in der DS-GVO-E allerdings im Rahmen der Auftragsverarbeitung nicht vorgesehen.

5. Grenzüberschreitender Datenverkehr

Aufgrund der im Rahmen des Cloud Computings häufigen Datenübermittlung in Staaten außerhalb der EU und des EWR und der Speicherung auf Servern in diesen Staaten ist Kapitel V DS-GVO-E von besonderer Bedeutung.[66] Art. 40 DS-GVO-E verbietet grundsätzlich die Übermittlung in Drittstaaten, sofern die Voraussetzungen des Kapitels nicht erfüllt sind und adressiert hierbei nunmehr auch direkt den Auftragsverarbeiter. Die Regelungen basieren zunächst auf Art. 25 und Art. 26 DSRL, gehen aber in Anlehnung an § § 4b, 4c BDSG (z.B. bei den Binding Corporate Rules) über diese hinaus. Wie bisher ist die Übermittlung bei Vorliegen eines Angemessenheitsbeschlusses (Art. 41 DS-GVO-E) zulässig, allerdings ist kaum anzunehmen, dass dieses Instrument künftig mehr Bedeutung erlangen wird als bisher.

Im Übrigen kann die Übermittlung aufgrund von Ausnahmen (Art. 44 DS-GVO-E) zulässig sein.[67] Wegen ihres Einzelfallcharakters werden diese für Standardverfahren im Cloud Computing kaum relevant werden. Allein die Vorteile des Cloud Computings machen eine Übermittlung in Drittstaaten noch nicht i.S.v. Art. 44 Abs. 1 lit. b DS-GVO-E „für die Erfüllung eines Vertrags" erforderlich.[68] Art. 44 Abs. 1 lit. h DS-GVO-E, der aufgrund der allgemeinen Formulierung in vielen Fällen droht, die Reglungen des Art. 40–43 DS-GVO-E auszuhebeln, setzt eine „nicht als häufig oder massiv" zu bezeichnende Übermittlung voraus, die im standardisierten Cloud Computing aber regelmäßig vorliegen wird.[69]

Für das internationale Cloud Computing werden dagegen die „geeigneten Garantien" nach Art. 42 DS-GVO-E wichtig sein, soweit diese eine allgemeine, nicht nur einzelfallbezogene Datenübermittlung zulassen. Das betrifft verbindliche unternehmensinterne Vorschriften (Binding Corporate Rules, ausdrücklich in Art. 43 DS-GVO-E),[70] von *EU-Kommission* oder Aufsichtsbehörden angenommene Standardschutzklauseln und Vertragsklauseln. Unternehmensinterne Vorschriften könnten z.B. für „private" Clouds der Unternehmen Anwendung finden, wenn diese grenzüberschreitend operieren. Gemäß Art. 43 Abs. 1 DS-GVO-E werden diese Vor-

60 S. *Lang*, K&R 2012, 145 (149 f.); s.a. *Art. 29 Datenschutzgruppe*, Opinion 05/2012 on Cloud Computing, 2012, S. 5 f., 9 f.

61 S. *Splittgerber/Rockstroh*, BB 2011, 2179 (2181).

62 S. *AK Technik und Medien*, Orientierungshilfe Cloud Computing, 2011, S. 8.

63 S. *Art. 29 Datenschutzgruppe*, Opinion 05/2012 on Cloud Computing, 2012, S. 19.

64 Für eine regelmäßige, aber nicht zwingende Kontrolle vor Ort z.B. *Petri* in Simitis, BDSG, 7. Aufl. 2011, § 11 Rz. 59, ähnlich: *AK Technik und Medien*, Orientierungshilfe Cloud Computing, 2011, S. 9; *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 11 Rz. 21.

65 Für eine entsprechende Regelung der Bundesrat, s. BR-Drucks. 52/12 (B) (2), 16.

66 Der *DAV* erachtete es im Vorfeld des DS-GVO-E als unmöglich, Cloud Computing mit Drittstaaten zu erleichtern und dabei das Datenschutzniveau zu bewahren, s. *http://anwaltverein.de/downloads/Stellungnahmen-11/43-2011-SN-Cloud-Computing.pdf*, S. 3. Zu Anforderungen außerhalb des Datenschutzes s. *Wagner/Blaufuß*, BB 2012, 1751.

67 Außer den Bsp. im Text Einwilligung, wichtige Gründe des öffentlichen Interesses, Erforderlichkeit im Umfeld von Rechtsansprüchen, Schutz lebenswichtiger Interessen und bestimmte Registerübermittlungen.

68 Entsprechend des Meinungsstandes zu § 28 Abs. 1 BDSG: *Schmidt-Bens*, Cloud Computing Technologien und Datenschutz, 2012, S. 70 ff.

69 S. im Kontext des Art. 26 DSRL *Art. 29 Datenschutzgruppe*, Opinion 05/2012 on Cloud Computing, 2012, S. 18.

70 Bisher schon § 4c Abs. 2 2. HS Alt. 2 BDSG geregelt.

schriften der Genehmigung einer Aufsichtsbehörde bedürfen und müssen nach Art. 43 Abs. 2 DS-GVO-E bestimmte Mindestanforderungen erfüllen. Die Wirkung der Binding Coporate Rules ist wiederum auf die Übermittlung innerhalb einer Unternehmensgruppe, bzw. innerhalb eines Konzerns begrenzt. Vor allem in Bezug auf sog. Public Clouds kann so die Problematik des Drittstaatentransfers nicht umfänglich gelöst werden.

Die *EU-Kommission* kann nach Art. 43 Abs. 3 DS-GVO-E Kriterien und Anforderungen für verbindliche unternehmensinterne Vorschriften erlassen. Über den Anforderungskatalog aus Art. 43 Abs. 2 DS-GVO-E hinaus hat hier die *Art.-29-Datenschutzgruppe* sinnvolle Vorschläge vorgelegt,[71] die u.a. klare Regelungen zur Verantwortlichkeit und Haftung, die effektive Zusammenarbeit mit den Aufsichtsbehörden, effektive Kontroll- und Auditierungsprozesse, eine fortlaufenden Anpassung der Regelungen und deren Transparenz beinhalten.

Standard-Datenschutzklauseln können nunmehr neben der *EU-Kommission* auch von einer Aufsichtsbehörde im Rahmen des Kohärenzverfahrens (Art. 57 ff. DS-GVO-E) festgelegt und von der *EU-Kommission* für allgemein gültig erklärt werden. Diese Klauseln müssten künftig alle Auftrags- und Unterauftragsverhältnisse des Cloud Computings umfassen und sich nicht wie bisher auf das Verhältnis zwischen außereuropäischen Auftrags- und Unterauftragsverarbeitern beschränken.[72] Der Meinungsstreit zur deutschen Rechtslage, ob hier zusätzlich zu den EU-Standardvertragsklauseln die Voraussetzungen des § 11 BDSG vorliegen müssen,[73] würde sich bei Geltung der DS-GVO erledigen, da in jedem Fall sowohl Art. 26 als auch Art. 40 ff. DS-GVO-E zu berücksichtigen wären.

Ein wesentliches Element sämtlicher Instrumente zur Wahrung eines angemessen Datenschutzniveaus muss die Gewährleistung individueller Rechte des Betroffenen sein. Dies ist bislang unzureichend umgesetzt, da es zwar für verbindlichen Unternehmensregelungen (Art. 43 Abs. 1 lit. b DS-GVO-E), nicht aber für Standardvertragsklauseln obligatorisch ist.[74]

Inwieweit die Instrumente zur Gewährleitung eines angemessenen Datenschutzniveaus Akzeptanz finden, bleibt abzuwarten. Zwar hat z.B. *Microsoft* für seinen Cloud-Dienst „CRM-Online" gerade EU-Mustervertragsklauseln angekündigt,[75] was hinsichtlich einheitlicher Standards hoffen lässt. Allerdings bleibt offen, wie *Microsoft* das Problem der Herausgabepflicht gegenüber US-Behörden lösen will. Zudem müssten die Klauseln stets den Veränderungen der Verarbeitung angepasst werden.

6. Neue Datenschutzinstrumente

Eines der Hauptprobleme des Cloud Computings besteht in der faktischen Umsetzung und Überprüfung der datenschutzrechtlichen Verpflichtungen. Vor allem aufgrund der für den Betroffenen teilweise intransparenten weltweiten Datenverarbeitung gewinnt der Datenschutz durch Technik besondere Bedeutung.[76] Es ist deshalb sehr zu begrüßen, dass die *EU-Kommission* in Art. 23 Abs. 1 DS-GVO-E eine entsprechende Regelung vorschlägt, die gerade für das Cloud Computing von erheblicher Relevanz sein wird.

In der Sache bleiben die vorgeschlagenen Regelungen allerdings weit hinter den Erwartungen, und vor allem hinter dem Notwendigen zurück: So sind die Anforderungen an die Gestaltung datenschutzfreundlicher Techniken nur sehr vage formuliert. Die Konkretisierung der Vorschriften wird in die Hände der *EU-Kommission* gelegt (Art. 23 Abs. 3 und 4 DS-GVO-E). Dabei ist sie sogar in ihrer Entscheidung über das „Ob" derartiger Konkretisierungen frei, was eine große Lücke im Regelungssystem hinterlässt. Demgegenüber würden differenzierte Zugriffsregime, Verschlüsselungstechnologien und Pseudonymisierungswerkzeuge effektiven Datenschutz in der Cloud ermöglichen.[77] Leider schweigt der Entwurf hierzu ebenso wie zur Umsetzung von Konzepten der Anonymisierung.[78] Es ist auch noch nicht erkennbar, ob die *EU-Kommission* im Rahmen der delegierten Rechtsakte Datensicherheitsmaßnahmen vorgeben wird, die dem Niveau von § 9 BDSG nebst der zugehörigen Anlage entsprechen.[79] Eine Absenkung würde im Rahmen des Cloud Computings zu erheblichen Nachteilen führen.

Der europäische Gesetzgeber ist hier gefordert, ein entsprechendes Anreizsystem zu entwerfen.[80] Ob Anforderungen an technische und organisatorische Schutzmechanismen eingehalten werden, kann gerade im Bereich des Cloud Computings sinnvollerweise durch Zertifizierungen, Datenschutzsiegel und -zeichen kontrolliert werden. Auch hierzu hat die *EU-Kommission* einen Vorschlag gemacht, der allerdings noch vager ist: *EU-Kommission* und Mitgliedstaaten werden in Art. 39 DS-GVO-E lediglich zur Förderung von Zertifizierungsverfahren verpflichtet. Hier sind deutlich mutigere und verbindlichere Schritte erforderlich.[81] Besonders im Bereich des Cloud Computings, in dem komplexe und häufig intransparente Systeme eingesetzt werden, sind automatische Verfahren, die auf Standards basieren und entsprechend zertifiziert sind, unabdingbar.[82] Dabei sollte eine Unterscheidung nach Cloud-Typen berücksichtigen, dass dem Cloud Nutzer z.B. im Rahmen einer IaaS-Anwendung weit mehr Selbstverantwortung zukommt, als bei einer SaaS-Anwendung.[83] Standardisierte Datenschutztechnik ist eine sinnvolle Alternative zu unpraktI-

71 S. *Art. 29 Datenschutzgruppe*, Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate rules.

72 S. Beschluss der Kommission vom 5.2.2010 über Standardvertragsklauseln, ABl. EU Nr. L 39 v. 12.2.2010, EG 23; dazu auch *BITKOM/VOICE*, Empfehlungen für den Cloud Computing-Standort Deutschland, 2012, S. 10 f.

73 S. *Schmidt-Bens*, Cloud Computing Technologien und Datenschutz, 2012, S. 62 ff.; bejahend *Weichert*, DuD 2010, 679 (686); Hintergrund ist § 3 Abs. 8 Satz 3 BDSG, wonach außereuropäische Auftragsdatenverarbeiter stets „Dritte" und der Datentransfer folglich eine Übermittlung ist, s. *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 4b Rz. 5, *Petri* in Simitis, BDSG, 7. Aufl. 2011, § 11 Rz. 30; s.a. *BITKOM/VOICE*, Empfehlungen für den Cloud Computing-Standort Deutschland, 2012, S. 11; *DAV, http://anwaltverein.de/downloads/Stellungnahmen-11/43-2011-SN-Cloud-Computing.pdf*, S. 4.

74 S. BR-Drucks. 52/12 (B) (2), 19.

75 S. *http://www.heise.de/-1585115.html.*

76 Z.B. *Hansen* in Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 3.3; in Bezug auf die Reform *Hornung*, ZD 2011, 51 ff.; in Bezug auf das Cloud Computing *AK Technik und Medien*, Orientierungshilfe Cloud Computing, 2011, S. 13 ff.

77 S. *Weichert*, DuD 2010, 679 (686); *BITKOM*, Cloud Computing – Was Entscheider wissen müssen, 2010, S. 69 f.

78 S. *Hornung*, ZD 2012, 99 (103).

79 S. BR-Drucks. 52/12 (B) (2), 15.

80 S. *BITKOM/VOICE*, Empfehlungen für den Cloud Computing-Standort Deutschland, 2012, S. 12; *DAV, http://anwaltverein.de/downloads/Stellungnahmen-11/43-2011-SN-Cloud-Computing.pdf*, S. 4.

81 S. *Hornung*, ZD 2012, 99 (103).

82 S. *BITKOM/VOICE*, Empfehlungen für den Cloud Computing-Standort Deutschland, 2012, S. 13.

83 S. *Velev/Zlateva* in Camenisch/Kisimov/Dubovitskaya, Open Research Problems in Network Security, LNCS 6555/2011, S. 145.

kablen Pflichten, die von den Anbietern nicht eingehalten werden können. Sie dienen sowohl den Anbietern, da sie sich an einheitlichen Maßstäben orientieren können, als auch den Betroffenen, die auf die Zertifizierungen vertrauen können.

IV. Fazit

Die Analyse der Auswirkungen des Entwurfs auf das Cloud Computing ergibt ein ambivalentes Bild. Angesichts des praktisch durchgängig transnationalen Charakters des Cloud Computings ist das Ziel einer verstärkten Harmonisierung zu begrüßen, das mit dem Wechsel zur europaweit unmittelbar geltenden Verortung und der Erweiterung des räumlichen Anwendungsbereiches erreicht werden soll. Allerdings bleibt abzuwarten, inwieweit die Instrumente zur Gewährleistung eines angemessen Schutzniveaus in Drittstaaten Akzeptanz finden werden.

In materiell-rechtlicher Hinsicht enthält der Entwurf keine cloud-spezifischen Regelungen, wohl aber eine Reihe von Neuerungen, die – wie z.B. die Änderungen zur Einwilligung, die Regelungen zu betrieblichen Datenschutzbeauftragten, die Benachrichtigungspflichten bei „Datenpannen" und die Höhe der Bußgelder – erhebliche Auswirkungen auf Cloud Provider und ihre Kunden haben werden. Insgesamt zeigt sich allerdings, dass die konkreten Auswirkungen auf beide Gruppen und die datenschutzrechtlich Betroffenen weithin davon abhängen würden, in welcher Form die *EU-Kommission* von den Befugnissen zur delegierten Rechtssetzung Gebrauch machen würde. Da der Text vielfach (sehr) unbestimmte Generalklauseln enthält, ist völlig unklar, ob Cloud Provider weniger oder mehr Probleme haben würden, die entsprechenden Anforderungen zu erfüllen. Die *EU-Kommission* könnte z.B. in ihren Rechtsakten gleichfalls mit Generalklauseln arbeiten (und die Konkretisierung den nationalen Aufsichtsbehörden überlassen), oder selbst detailliert und technikspezifisch Vorgaben machen. Hier wären auch spezifische Anforderungen an das Cloud Computing oder einzelne Verfahren und Anwendungen möglich. In dieser Unsicherheit zeigt sich besonders plastisch, dass der Entwurf hinsichtlich der Kompetenzen der *EU-Kommission* nicht nur mit Blick auf Art. 290 Abs. 1 AEUV primärrechtlich bedenklich,[84] sondern auch sachlich unangemessen weit ist.

Sowohl im Gesetzgebungsverfahren (in dem dies noch verändert werden könnte) als auch im Rahmen der delegierten Rechtssetzung wird es darauf ankommen, zwischen dem klassischen Zweipersonenverhältnis und den Mehrpersonenverhältnissen der sog. „Business-Clouds" zu unterscheiden. Während die meisten Regelungen des Entwurfs für erstere umsetzbar erscheinen, ist dies bei letzteren nicht immer der Fall. Gerade hier wären effektive Vorgaben für einen Datenschutz durch Technik und entsprechende Auditierungs- und Gütesiegelverfahren erforderlich, die die besonderen Rechtsbeziehungen der Beteiligten berücksichtigen. Nur so können in dem schnell wachsenden Weltmarkt des Cloud Computings datenschutzfreundliche Technologien[85] implementieren werden.

84 S. *Hornung*, ZD 2012, 99 (105); ebenso der Bundesrat, BR-Drucks. 52/12 (B) (2), 27.

85 Z.B. die automatisierte Erkennung, Auswertung und Steuerung der Ortsbezogenheit der Daten, s. *Hansen*, DuD 2012, 407 (410); *International Working Group on Data Protection in Telecommunications*, „Sopot Memorandum", 2012, S. 4.

Rechtsprechung zum Computerrecht

BGH: Kein Anspruch auf Unterlassung vermeintlicher Verstöße in künftigen Vergabeverfahren

BGB §§ 241 Abs. 2, 280 Abs. 1, 311 Abs. 2

Leitsatz

Einem (potentiellen) Bieter steht gegen den öffentlichen Auftraggeber kein aus bürgerlich-rechtlichen Vorschriften herzuleitender Anspruch darauf zu, die Verwendung bestimmter als vergaberechtswidrig erachteter Vergabebedingungen in etwaigen zukünftigen Vergabeverfahren zu unterlassen (Fortführung von BGH, Urt. v. 11.9.2008 – I ZR 74/06, BGHZ 178, 63 = CR 2009, 175 m. Anm. Bandehzadeh/Plog = MDR 2009, 456 – bundesligakarten.de).

BGH, Urt. v. 5.6.2012 – X ZR 161/11 (OLG München v. 11.11.2010 – U (K) 2872/10; LG München I v. 31.3.2010 – 37 O 17734/09)

Aus dem Tatbestand:

[1] Die Klägerin verlangt Schadensersatz und Unterlassung im Zusammenhang mit der Nichtberücksichtigung ihres Angebots in einer Jahresausschreibung der Beklagten zur Lieferung von StVO-Hinweisschildern und Zubehörteilen sowie Demontage, Montage und Änderung von Transparenten, Großschildern und Aufstellvorrichtungen zur Unterhaltung und Erneuerung auf den Betriebsstrecken einer Dienststelle der Autobahndirektion Südbayern. Zu den Vergabeunterlagen gehörte die Klausel 32 „Fachpersonal", die, soweit hier von Interesse, lautet: (...)

[2] Das Angebot der Klägerin war zwar das wirtschaftlich günstigste, wurde von der Beklagten aber von der Wertung ausgeschlossen, weil die Klägerin die Fachpersonalklausel nicht erfüllt. (...)

Aus den Entscheidungsgründen:

(...)

[7] II. Die gegen diese Beurteilung gerichteten Angriffe der Revision haben Erfolg. Die vom Berufungsgericht gegebene Begründung trägt die ausgesprochene Abweisung der Klage nicht.

[8] Die Verneinung eines durch einen Vergaberechtsverstoß der Beklagten ausgelösten Schadensersatzanspruchs der Klägerin wegen fehlenden Vertrauens in die Rechtmäßigkeit des Vergabeverfahrens ist mit der neueren, allerdings erst nach Verkündung des Berufungsurteils ergangenen Rechtsprechung des BGH nicht vereinbar. Danach ist der auf Verstöße des öffentlichen Auftraggebers gegen Vergabevorschriften gestützte Schadensersatzanspruch des Bieters nicht daran geknüpft, dass der klagende Bieter auf die Einhaltung dieser Regelungen durch den Auftraggeber vertraut hat. Maßgeb-