FORUM Wirtschaftsrecht - Band 19

Institut für Wirtschaftsrecht

Natalie Maier

Die Datenweitergabe im Rahmen des Cloud Computings unter besonderer Betrachtung von Unterauftragsverhältnissen

kassel university press

FORUM Wirtschaftsrecht

Band 19

Herausgegeben vom
Institut für Wirtschaftsrecht an der Universität Kassel

Die Datenweitergabe im Rahmen des Cloud Computings unter besonderer Betrachtung von Unterauftragsverhältnissen

Natalie Maier

kassel university press

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar

ISBN: 978-3-86219-834-4 (print)
ISBN: 978-3-86219-835-1 (e-book)
URN: http://nbn-resolving.de/urn:nbn:de:0002-38351

Printed in Germany

Vorwort der Herausgeber

Cloud Computing verspricht dem Nutzer größere Flexibilität, mehr Komfort und geringere Kosten und dem Anbieter große Gewinne. Soweit personenbezogene Daten in der Cloud verarbeitet werden, betrifft Cloud Computing aber noch eine dritte Rolle, nämlich die des Betroffenen. Dessen personenbezogene Daten werden von der verantwortlichen Stelle, dem Cloud-Nutzer, in die Cloud hochgeladen und dort eventuell auch verarbeitet. Ihm bringt Cloud Computing keine Vorteile, sondern setzt ihn zusätzlichen Datenschutzrisiken aus. Die Weitergabe personenbezogener Daten von der verantwortlichen Stelle an den Cloud-Anbieter ist daher an datenschutzrechtlichen Vorgaben zu messen und darf nur dann erfolgen, wenn sie diesen entspricht. Dies ist im Regelfall nur dann gegeben, wenn der Cloud-Anbieter die personenbezogenen Daten im Auftrag des Cloud-Nutzers, also der verantwortlichen Stelle, speichert oder verarbeitet. In diesem Fall wird der Cloud-Anbieter wie ein Rechenzentrum des Cloud-Nutzers angesehen. Die Weitergabe gilt nicht als Übertragung von Daten und bedarf keiner besonderen datenschutzrechtlichen Rechtfertigung.

Allerdings müssen die Voraussetzungen einer rechtmäßigen Auftragsdatenverarbeitung gegeben sein. Vor allem muss die verantwortliche Stelle die Verantwortung für die Datenverarbeitung beim Auftragnehmer behalten. Hierfür muss sie ihn gut auswählen, anweisen und kontrollieren. Dies ist allerdings besonders schwer bei einem echten Cloud Computing, das ja gerade dadurch so flexibel und kostengünstig sein kann, weil der Cloud-Anbieter viele – unter Umständen über die ganze Welt verteilte – Rechner nach Bedarf einsetzen und nach Belastung zwischen diesen flexibel wechseln kann. Gerade diese Unterauftragsverhältnisse erschweren es der verantwortlichen Stelle jedoch, die Verantwortung für die Datenverarbeitung zu behalten und wahrzunehmen.

Hier setzt die Untersuchung von Frau Maier an. Sie bietet eine eigenständige, systematische und sehr subtile Untersuchung der Zuläs-

sigkeit der Weitergabe von personenbezogenen Daten an Cloud-Anbieter und ihre Unterauftragnehmer innerhalb und außerhalb Europas. Für unterschiedliche Fallgestaltungen analysiert sie die Probleme, die bei der Weitergabe personenbezogener Daten an Cloud Computing-Unterauftragnehmer entstehen können, und entwickelt für sie konstruktiv datenschutzgerechte und praktikable Lösungen.

Die hier vorgelegte Masterarbeit der Universität Kassel im Studiengang Wirtschaftsrecht untersucht ein sehr aktuelles Problem der Datenschutzpraxis, nämlich die europäischen und internationalen Bezüge des Cloud Computing, und hat damit eine wesentliche Grundlage dafür gelegt, die Vertrauenswürdigkeit von Cloud Computing zu gewährleisten. Indem sie die unübersichtliche Konfliktlandschaft zutreffend „vermisst“ und überzeugende Positionen herausarbeitet, bietet sie eine differenzierte und belastbare rechtliche Bewertung der unterschiedlichen Konstellationen der Cloud Computing-Angebote und der Unterbeauftragung im inner- und außereuropäischen Ausland. Da Frau Maier das sehr anspruchsvolle und überdurchschnittlich schwierige Thema in hervorragender Weise bearbeitet hat, wurde ihre Untersuchung mit der Bestnote ausgezeichnet.

Für die Herausgeber

Prof. Dr. Alexander Roßnagel

Übersicht

Abkürzungsverzeichnis

Abs.	Absatz
BB	Betriebs-Berater
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drucks.	Bundestagsdrucksache
bzw.	beziehungsweise
CR	Computer und Recht
CRM	Customer Relationship Management
ders.	derselbe
DGRI	Deutsche Gesellschaft für Recht und Informatik e.V.
DSB	Datenschutz-Berater
DS-GVO	Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)
DuD	Datenschutz und Datensicherheit
e.V.	eingetragener Verein
et al.	et alii/ et aliae/ et alia
EU	Europäische Union

EU-DSRL	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie)
EWR	Europäischer Wirtschaftsraum
f., ff.	folgend (e)
FAQ	Frequently Asked Questions
GDD	Gesellschaft für Datenschutz und Datensicherheit e.V.
gem.	gemäß
Hrsg.	Herausgeber
HS	Halbsatz
i.S.d.	im Sinne des
i.V.m.	in Verbindung mit
IaaS	Infrastructure as a Service
IKT	Informations- und Kommunikationstechnik
IT	Informationstechnologie
ITRB	IT-Rechtsberater
iX	Magazin für professionelle Informationstechnik
K&R	Kommunikation und Recht
lit.	litera
MMR	Multimedia und Recht
NIST	National Institute of Standards and Technology
Nr.	Nummer
PaaS	Platform as a Service

PWC	Pricewaterhouse Coopers
RDV	Recht der Datenverarbeitung
Rn.	Randnummer
S.	Satz oder Seite
SaaS	Software as a Service
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
US	United States
USA	United States of America
USA Patriot Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
VBIBW	Verwaltungsblätter für Baden-Württemberg
VOICE	Verband der IT-Anwender e.V.
WP	Working Paper der Artikel-29-Datenschutzgruppe
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZEuS	Zeitschrift für europarechtliche Studien
ZUM	Zeitschrift für Urheber- und Medienrecht

Tabellenverzeichnis

1 Einleitung

Vereinfacht ausgedrückt, steht Cloud Computing für die Speicherung, Verarbeitung und Verwendung von Daten, die auf entfernten Servern lagern und auf die via Internet zugegriffen werden kann. Seine drei Formen Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS) und seine Erscheinungsarten Public, Private und Hybrid Cloud, die es im Laufe der Arbeit zu erläutern gilt, sind erst durch die Heranreifung neuer Technologien und den Ausbau breitbandiger Netze ermöglicht worden und versprechen viele Vorteile.[1]

Die Nutzung von online bereitgestellter Hard- und Software durch Cloud Computing ist eine Dienstleistung,[2] die viele Vorzüge gegenüber dem traditionellen Bezug von IT verspricht. Einer der wichtigsten Vorteile ist die flexible, skalierbare und kostengünstige Nutzung dieser Services.[3] Insbesondere Startupunternehmen werden durch die Nutzung von Cloudservices Investitionseinsparungen bei Hard- und Software versprochen. Zugleich sollen die Unternehmen solche Services nur in dem Umfang nutzen können, den sie auch tatsächlich benötigen.[4]

Etablierten Unternehmen bieten Cloudservices eine Möglichkeit zur Überbrückung von Lastspitzen, auf die Unternehmensserver häufig ausgelegt sind und die dafür verantwortlich sind, dass die IT-Kosten steigen, weil Ressourcen vorgehalten werden, die hohe Anschaffungs- und Betriebskosten verursachen, die jedoch die meiste Zeit nicht genutzt werden. Dies soll dank Cloud Computing der Vergangenheit angehören. Eine von der EU-Kommission in Auftrag gegebene Erhebung für das Jahr 2011 ergab, dass 81% der Unternehmen durch die Einführung des Cloud Computings 10-20% ihrer Kosten senken konn-

---

1 *Pauly*, in: Köhler-Schute (Hrsg.), Cloud Computing, S. 18 f.
2 *Spies*, MMR 2009, Heft 5, XI; *Pohle/ Ammann*, CR 2009, 273 (273).
3 *Kiehne*, in: Köhler-Schute (Hrsg.), Cloud Computing, S. 23.
4 *Bedner*, Cloud Computing, S. 69.

ten.[5] Zudem soll Cloud Computing die Flexibilität der Unternehmen steigern können, da ein zusätzlicher Bedarf an Rechenleistung oder Speicherkapazität nicht erst nach einer langwierigen Anschaffung der Hardware gedeckt werden kann, sondern sich in kurzer Zeit und mit geringem Managementaufwand durch die Nutzung von Cloudservices decken lässt.[6] Dabei wird das Investitionsrisiko sogar noch auf den Cloudanbieter verlagert.[7] Cloudservices können für Projekte genutzt werden, wobei auch die schrittweise Ersetzung der hauseigenen Rechenzentren und IKT-Abteilungen durch Cloudservices denkbar ist.[8]

Genauso wie man Speicherkapazitäten aus der „Cloud" beziehen kann, kann man im Rahmen von SaaS auch Software als Cloudservice beziehen. Die Vorteile bestehen darin, dass eine Überlizenzierung der im Unternehmen genutzten Software vermieden wird und sich der Cloudanbieter zudem darum kümmert, dass der Nutzer stets die aktuellste Softwareversion erhält. Dies führt auf Seiten des Cloudnutzers zu einem geringeren Wartungs- und Supportaufwand. Diese dargelegten Vorteile lassen sich bei der Nutzung von Public Clouds am ehesten erzielen,[9] weshalb im Laufe der folgenden Arbeit schwerpunktmäßig auf die Datenverarbeitung in Public Clouds eingegangen werden wird.

Wo viel Licht ist, ist auch viel Schatten. In diesem Sinne bietet das Cloud Computing nicht nur Vorteile, sondern weist auch einige Nachteile auf. Zum einen besteht die Gefahr unvorhersehbarer Fehler, da

---

5 *Bradshaw et al.,* Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take, S. 11, abrufbar unter: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf, Stand: 7.6.2014

6 *Kiehne,* in: Köhler/ Schute (Hrsg.), Cloud Computing, S. 25 f; *Bedner,* Cloud Computing, S. 48; *Kühling/ Biendl,* CR 2014, 150 (150).

7 *Arbitter et al.,* in: Köhler-Schute (Hrsg.), Cloud Computing, S. 35; *Nägele/ Jacobs,* ZUM 2010, 281 (282); *Karger/ Sarre,* in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 428.

8 *Europäische Kommission,* Freisetzung des Cloud-Computing-Potentials in Europa, S. 4; abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:-FIN:DE:PDF, Stand: 7.6.2014; *Bedner,* Cloud Computing, S. 2.

9 *Schultze-Melling,* ITRB 2011, 239 (239).

die beim Cloud Computing verwendeten Techniken komplex sind und der Nutzer auf funktionierende Infrastrukturen angewiesen ist.[10] Zum anderen besteht das Risiko von Lock-In-Effekten, was bedeutet, dass einmal in die Cloud eingebrachte Daten aus dieser nicht wieder problemlos herausgeladen werden können und der Wechsel von einem zu einem anderen Cloudanbieter erschwert wird.[11] Durch die gemeinsame Nutzung physischer Ressourcen in Public Clouds besteht weiterhin die Gefahr, dass Cloudnutzer auf die Daten anderer Nutzer zugreifen können.[12] Die größten Bedenken werden gegenüber Public Clouds geäußert, da sie zwar die größten Kosten- und Flexibilitätsvorteile bieten, diese jedoch darauf beruhen, dass diese Clouds aus vielen verteilten Servern und Rechenzentren bestehen, die zum Teil über Ländergrenzen hinweg verstreut sind und auch nicht immer nur einem Cloudanbieter als Betreiberunternehmen zugeordnet werden können.

1.1 Verteilte Ressourcen und Mitwirkung von Unterauftragnehmern

Durch die Nutzung verteilter Ressourcen lässt sich die Rechenleistung steigern und die Verfügbarkeit und Ausfallsicherheit erhöhen, weil die Wahrscheinlichkeit, dass alle verteilten Rechenzentren zur gleichen Zeit ausfallen, gering sein dürfte.[13] Zugleich ist eine solche Vorgehensweise kostengünstig, da bei der Nutzung verschiedener Server Restkapazitäten genutzt werden können und somit eine effiziente Ressourcenauslastung erreicht werden kann. Der Cloudnutzer wird jedoch regelmäßig nicht wissen, auf welche physischen Ressourcen er im Moment der Anwendung zugreift, weil dies von Zufälligkeiten wie unterschiedlichen Lastverteilungsalgorithmen, freien Kapazitäten und der Nachfrage abhängt und sich auch schnell wieder ändern kann.[14]

---

10 *Bedner,* Cloud Computing, S. 101.
11 *Schweda,* ZD-aktuell 2012, 30109.
12 *Paulus,* DuD 2011, 317 (319).
13 *Bedner,* Cloud Computing, S. 43.
14 *Roth,* in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 6 Rn. 196; *Bedner,* Cloud Computing, S. 154.

Für den Cloudnutzer hingegen erscheint die Cloud als ein einziges System.[15]

Verschärft wird diese Intransparenz dadurch, dass sich die Cloudanbieter zur Leistungserbringung gegenüber dem Kunden nicht nur ihrer eigenen verteilten Server und Rechenzentren bedienen, sondern hierfür auf Ressourcen von Subunternehmern als Unterauftragnehmer zurückgreifen.[16] Dass eine solche Unterbeauftragung häufig genutzt wird, um eine möglichst effiziente Kapazitätsverteilung zu erzielen und hierdurch ein kostengünstiges Angebot liefern zu können, zeigt eine Studie von Pricewaterhouse Coopers vom März 2013.[17] Hiernach nutzen rund 57% der befragten Cloudanbieter am deutschen Markt Unterauftragnehmer zur Leistungserbringung gegenüber dem Cloudnutzer. 7% der befragten Cloudanbieter gaben sogar an, über gar keine eigenen Rechenzentren zu verfügen und sich somit bei der Leistungserbringung komplett der Ressourcen von Unterauftragnehmern zu bedienen.[18] Häufig werden nicht nur einzelne, sondern gleich mehrere, unter Umständen wechselnde Unterauftragnehmer an der Leistungserbringung beteiligt, die ihrerseits wiederrum weitere Unterauftragnehmer beauftragen können.[19] Die Cloudanbieter schließen ihre Rechenzentren häufig mit denen ihrer Unterauftragnehmer zu einem Ressourcen-Pool zusammen. Erst durch diesen Zusammenschluss wird der Cloudanbieter oftmals in die Lage versetzt, seinen Cloudservice anbieten zu können. Auch Zusammenschlüsse von Rechenzentren aus unterschiedlichen Zeitzonen sind keine Seltenheit, weil der Cloudservice hierdurch nach dem „follow the sun"-Prinzip tageszeitabhän-

---

15 *Schulz*, MMR 2010, 75 (78).

16 *Bedner*, Cloud Computing, S. 37 f; *Schulz/ Rosenkranz*, ITRB 2009, 232 (233); *Niemann/ Hennrich*, CR 2010, 686 (691); *Schulz*, MMR 2010, 75 (78).

17 *PWC*, Cloud Computing – Navigation in der Wolke, abrufbar unter: http://www.pwc.de/de_DE/de/prozessoptimierung/assets/evolution-in-der-wolke-reifegrad-der-cloud-services-steigt2.pdf, Stand: 7.6.2014

18 *PWC*, Cloud Computing – Navigation in der Wolke, S. 40.

19 *Arbitter et al.*, in: Köhler-Schute (Hrsg.), Cloud Computing, S. 48.

gig aus dem Rechenzentrum erbracht werden kann, in dem die Auslastung am geringsten ist.[20]

Diese kurze Darstellung lässt erahnen, wie komplex und intransparent die Strukturen im Rahmen des Cloud Computings werden können, wenn in der Welt verstreute Ressourcen unterschiedlicher Unterauftragnehmer zur Leistungserbringung genutzt werden, sodass es nicht verwundert, wenn die Unternehmen Vorbehalte äußern, sobald es um die Auslagerung personenbezogener oder für das Unternehmen wichtiger Daten wie Unternehmensgeheimnisse in eine Public Cloud geht. Diese Befürchtungen werden umso nachvollziehbarer, wenn man bedenkt, dass es aus technischer Sicht keinen großen Unterschied macht, ob auf die Ressourcen europäischer Unterauftragnehmer oder auf diejenigen außerhalb von EU-oder EWR Staaten (sog. Drittstaaten) ansässiger zurückgegriffen wird, dies jedoch datenschutzrechtlich einen großen Unterschied macht, da aus europäischer Sicht außerhalb von EU-Staaten[21] kein angemessenes Datenschutzniveau vorherrscht und somit nicht von einem adäquaten Schutz dorthin ausgelagerter Daten ausgegangen werden kann. Ein angemessenes Datenschutzniveau ist grundsätzlich jedoch für die Zulässigkeit der Datenweitergabe an einen Cloudanbieter oder Unterauftragnehmer unerlässlich. Aufgrund der Mehrzahl der Beteiligten auf der Seite des Cloudanbieters muss zunächst festgestellt werden, wo der Cloudanbieter und dessen Unterauftragnehmer ansässig sind und an welcher „Stelle" es an einem angemessenen Datenschutzniveau mangelt. Aus der Sicht eines deutschen Unternehmens als Cloudnutzer ergeben sich somit vier Fälle, die Tabelle 1 entnommen werden können und auf die im Laufe der Arbeit ausführlich eingegangen werden wird.

---

[20] *Conrad/ Hausen,* in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 2 Rn. 306; *Opfermann,* ZEuS 2012, 121 (126); *Conrad/ Hausen,* in: Büchner/ Briner (Hrsg.), DGRI Jahrbuch 2009, S. 37.

[21] Der Begriff „EU" wird im Folgenden aus Gründen der Vereinfachung auch für die Mitgliedsstaaten des gleichgestellten EWR verwendet werden.

	Cloudnutzer	Cloudanbieter	Unterauftragnehmer
Fall A	Deutschland	EU	EU
Fall B	Deutschland	Drittstaat	Drittstaat
Fall C	Deutschland	EU	Drittstaat
Fall D	Deutschland	Drittstaat	EU

Tabelle 1: Ansässigkeit der am Cloud Computing Beteiligten

Nach dieser Schilderung überrascht es nicht, dass die Erfüllung datenschutzrechtlicher Vorgaben als eine der derzeit größten Herausforderungen beim Cloud Computing gesehen wird,[22] die sich umso schwieriger gestaltet, je heterogener und verstreuter die in die Cloud eingebundenen Ressourcen und deren jeweilige Betreiberunternehmen sind.[23]

Auf dem Markt gibt es mehrere Vertragsmodelle, aus denen der Cloudnutzer wählen kann. Beim sogenannten Single Point of Contract werden alle vertraglich zugesicherten Leistungen durch einen Cloudanbieter erbracht. Solche Verträge werden nur größere Cloudanbietern bieten können, da nur sie über genügend eigene Ressourcen verfügen werden, um ihre unterschiedlichen Cloudservices auch ohne Zuhilfenahme fremder Ressourcen erbringen zu können.[24] Eine weitere Mög-

---

22 *Splittgerber/ Rockstroh,* BB 2011, 2179 (2180); *Schuster/ Reichl,* CR 2010, 38 (41); *Stögmüller,* in: Leupold/ Glossner (Hrsg.), Teil 5 Rn. 345; *Gaul/ Koehler,* BB 2012, 2229 (2229); *Europäische Kommission,* Freisetzung des Cloud-Computing-Potentials in Europa, S. 10; *PWC,* Cloud Computing – Navigation in der Wolke, S. 28, abrufbar unter: http://www.pwc.de/de_DE/de/prozessoptimierung/assets/evolution-in-der-wolke-reifegrad-der-cloud-services-steigt2.pdf, Stand: 7.6.2014

23 *Karger/ Sarre,* in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 435.

24 *Niemann/ Hennrich,* CR 2010, 686 (691); *Bedner,* Cloud Computing, S. 37.

lichkeit besteht in der Beauftragung eines Generalanbieters, der zur Leistungserbringung mit oder ohne Zustimmung des Cloudnutzers weitere Unterauftragnehmer einsetzt.[25] In der Praxis benötigen vor allem kleinere Cloudanbieter die Ressourcen der Unterauftragnehmer, um die Vollauslastung der eigenen Infrastrukturen zu verhindern.[26] Im Rahmen des Cloud Computings gibt es auch ein Multi Vendor Modell, bei dem die in der Cloud zur Verfügung gestellten Cloudservices durch verschiedene Anbieter erbracht werden und der Cloudnutzer je nach Bedarf auf einen der Cloudanbieter zurückgreifen kann, der seinerseits wiederum Unterauftragnehmer beauftragt, um eine bestmögliche Kapazitätsauslastung und Ressourcenverwendung zu erzielen.[27] Das Multi Vendor Modell soll jedoch im Rahmen der vorliegenden Arbeit nicht näher betrachtet werden, da der Bezug von Cloudservices von einem Generalunternehmer genügend Flexibilität und Raum für wirtschaftliche Vorteile bietet und zusätzlich den Vorteil aufweist, dass es nur einen Vertragspartner gibt, der die gesamte Leistungserbringung koordiniert und der Cloudnutzer daher kaum Knowhow benötig, um die Cloudservices nutzen zu können.[28]

1.2 Gang der Arbeit

Nachdem im ersten Kapitel eine Einleitung in das Thema der Arbeit gegeben worden und auf das Problem der verteilten Ressourcen und der Vielzahl der an der Erbringung der Cloudservices beteiligten Akteure auf der Seite des Cloudanbieters eingegangen worden ist, beleuchtet das zweite Kapitel den Begriff des Cloud Computings und die diesem zugrunde liegende Technik. Weiterhin findet dort die Erläute-

---

25 *Söbbing,* MMR 2008, Heft 5, XII (XIII); *Niemann/ Paul,* K&R 2009, 444 (446); *Söbbing,* in: Leible/ Sosnitza (Hrsg.), Onlinerecht 2.0, S. 44.

26 *Niemann/ Hennrich,* CR 2010, 686 (691); *Bedner,* Cloud Computing, S. 37.

27 *Söbbing,* MMR 2008, Heft 5, XII (XIII); *Niemann/ Paul,* K&R 2009, 444 (446); *Söbbing,* in: Leible/ Sosnitza (Hrsg.), Onlinerecht 2.0, S. 44; *Bierekoven,* in: Bartsch/ Briner (Hrsg.), DGRI Jahrbuch 2010, S. 100.

28 *BITKOM,* Leitfaden Cloud Computing, S. 35; *Bierekoven,* in: Bartsch/ Briner (Hrsg.), DGRI Jahrbuch 2010, S. 99; *Niemann/ Paul,* K&R 2009, 444 (446).

rung der bereits erwähnten Formen und Erscheinungsarten des Cloud Computings statt.

Das dritte Kapitel stellt den Anwendungsbereich des Bundesdatenschutzgesetzes dar. Dort wird im Besonderen auf personenbezogene Daten, sowie den sachlichen und räumlichen Anwendungsbereich des Bundesdatenschutzgesetzes eingegangen.

Kapitel vier behandelt die Zulässigkeit der innereuropäischen Datenverarbeitung. In diesem Kapitel werden die Einwilligung des Betroffenen und die Auftragsdatenverarbeitung als Legitimationsgrundlagen der Datenverarbeitung in der „Wolke" betrachtet. Dafür wird zunächst der Begriff der Auftragsdatenverarbeitung erläutert und anschließend geklärt, ob die Formen des Cloud Computings als Auftragsdatenverarbeitung angesehen werden können. Nach der Darstellung der gesetzlichen Anforderungen an die Auftrags- und Unterauftragsvergabe und den teilweise auftretenden Problemen ihrer Erfüllung beim Cloud Computing, wird zum Ende des Kapitels ein Zwischenfazit gezogen.

Kapitel fünf behandelt die Zulässigkeit der Datenübermittlung ins außereuropäische Ausland. Zunächst wird geprüft, ob die Erlaubnisnormen des § 28 Abs. 1 S. 1 BDSG die Datenübermittlung in die Cloud legitimieren können. Da für die Zulässigkeit einer Datenübermittlung ins außereuropäische Ausland das Datenschutzniveau beim Datenempfänger maßgeblich ist, werden die zur Verfügung stehenden Möglichkeiten zu dessen Herstellung, wie beispielsweise die Safe Harbor Zertifizierung, behandelt. Einen großen Teil dieses Kapitels nimmt die Frage ein, welche Möglichkeiten zur Herstellung eines angemessenen Datenschutzniveaus bei der Unterauftragsvergabe bestehen. Dabei ist danach zu unterscheidet, wo Cloudanbieter und Unteraufragnehmer ansässig sind. Den Abschluss des Kapitels bildet ein Zwischenfazit.

Kapitel 6 setzt sich mit der geplanten Datenschutz-Grundverordnung vom Januar 2012 auseinander. In diesem Kapitel werden nur diejenigen Themengebiete aufgegriffen, die auch im Rahmen der Arbeit nach

der geltenden Rechtslage dargestellt worden sind. Dies betrifft die Datenverarbeitung in Drittstaaten und die Auftragsdatenverarbeitung. Kapitel 7 bildet das Fazit und somit das Ende der Arbeit.

2 Einführung in Begriff und Technik des Cloud Computings

Cloud Computing wird oftmals als die „Datenverarbeitung in der Wolke“ bezeichnet.[29] Diese Art der Datenverarbeitung stellt nach der überwiegenden Literaturmeinung keine neue Technologie dar, sondern ist vielmehr eine Kombination von vorhandenen Technologien, Outsourcing-Konzepten und Geschäfts- und Abrechnungsmodellen.[30]

Der Definition des National Institute of Standards and Technology (NIST) nach, ist Cloud Computing „ein Modell zur Ermöglichung eines ubiquitären, komfortablen, auf Abruf verfügbaren Netzzugriffs auf einen gemeinsamen Pool aus konfigurierbaren Rechenressourcen (z.B. Netze, Server, Speicher, Anwendungen und Dienste), der schnell und mit geringfügigem Verwaltungsaufwand bzw. minimaler Interaktion mit dem Cloudanbieter bereitgestellt und öffentlich verfügbar gemacht werden kann.“[31] Cloud Computing zeichnet sich weiterhin durch eine hohe Dynamik aus. Dies betrifft auch den Ort der Datenverarbeitung, der sich schnell ändern kann und von verschiedenen Faktoren abhängt. Die Ressourcenpools aus eigenen und angemieteten Ressourcen des Cloudanbieters sind häufig aufgrund ihrer Belegenheit in unterschiedlichen Zeitzonen, einer günstigen Stromversorgung oder eines kühlen Klimas in verschiedenen Ländern und Kontinenten verteilt.[32] Unvorhersehbare Umstände wie die Überlastung oder der Ausfall eines Rechenzentrums können ebenso einen Einfluss auf den Standort der Daten haben wie die Übertragung von Kopien an andere

---

29 *Weichert*, DuD 2010, 679 (679); *Grünwald/ Döpkens*, MMR 2011, 287 (287).

30 *Maisch/ Seidl*, VBIB 2012, 7 (7); *Schuster/ Reichl*, CR 2010, 38 (38); *Conrad/ Hausen*, in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 2 Rn. 305.

31 *National Institute of Standards and Technology (NIST)*, The NIST Definition of Cloud Computing, S. 3, abrufbar unter: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, Stand: 7.6.2014

32 *Söbbing*, in: Leible/ Sosnitza (Hrsg.), Onlinerecht 2.0, S. 40.

Rechenzentren, um im Störungsfall die Online-Verfügbarkeit des Cloudservices garantieren zu können.[33]

Da es unterschiedliche Ansätze bei der Programmierung einer Cloud Computing Architektur und eine Vielzahl unterschiedlicher Services gibt, hat sich eine Definition der vom Cloud Computing erfassten Services bisher nicht herausgebildet, wobei es jedoch einige technische Bestandteile gibt, die als für das Cloud Computing typisch angesehen werden.[34] Den technischen Grundstein des Cloud Computings bildet die Virtualisierungstechnik, die es erlaubt, Hard- und Software voneinander zu trennen und auf einer physisch vorhandenen Hardwarelandschaft, mehrere virtuelle Softwarestrukturen zu betreiben. Diese virtuellen Softwarestrukturen können sowohl voneinander abgeschirmt als auch miteinander verbunden werden. Durch die Virtualisierungstechnik entstehen virtuelle Systemlandschaften, denen Steuerungsprogramme je nach Zeitpunkt, Verteilungsalgorithmus und Auslastung physische Hardwareressourcen zuweisen.[35] Den Kern der Virtualisierungstechnik bildet die Virtualisierungsebene, auch Hypervisor, genannt. Darunter werden Softwarekomponenten verstanden, die den gleichzeitigen Betrieb von Systemen mehrerer Cloudnutzer auf einer physischen Plattform derart umsetzen, dass sich die Systeme der einzelnen Cloudnutzer in logisch getrennten Bereichen befinden, sich die Cloudnutzer jedoch die zur Verfügung stehenden Ressourcen teilen und hierdurch eine maximale Auslastung der Ressourcen stattfinden kann.[36] Der Hypervisor ist somit eine relevante Sicherheitskomponente in virtuellen Systemen, weil ein Zugriff auf die Daten aller

---

33 *International Working Group on Data Protection in Telecommunications,* WP on Cloud Computing – Privacy and data protection issues, S. 7, abrufbar unter: http://www.datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf., Stand: 7.6.2014

34 *Nägele/ Jacobs,* ZUM 2010, 281 (281); *Niemann/ Paul,* K&R 2009, 444 (445); *Opfermann,* ZEuS 2012, 121 (124), *Janisch,* Cloud Computing und Datenschutz, S. 1; *Wagner/ Blaufuß,* BB 2012, 1751 (1751).

35 *Nägele/ Jacobs,* ZUM 2010, 281 (281).

36 *Birk/ Wegener,* DuD 2010, 641 (642); *Bierekoven,* ITRB 2010, 42 (42); *Beckereit,* in: Köhler-Schute (Hrsg.), Cloud Computing, S. 70.

virtuellen Maschinen, die er verwaltet, erfolgen kann, wenn er übernommen oder überwunden werden kann.[37]

2.1 Formen des Cloud Computings

Hinsichtlich der technischen Ausgestaltung lassen sich anhand des sogenannten delivery models mindestens drei Formen des Cloud Computings unterscheiden.[38] Man unterscheidet zwischen Infrastructure as a Service (Iaas), Platform as a Service (PaaS) und Software as a Service (SaaS). Die oberste Schicht ist die Anwendungsschicht, darunter liegt die Plattformschicht, gefolgt von der Infrastrukturschicht als der untersten Ebene. Die wohl am meisten verbreitete Form des Cloud Computings ist SaaS.[39] Diese Form ermöglicht dem Cloudnutzer Software zu nutzen, die sich auf der Infrastruktur des Cloudanbieters befindet, ohne dass diese auf dem eigenen Rechner installiert werden braucht.[40] Der Cloudnutzer hat in diesen Fällen keinen Einfluss auf die Virtualisierungsebene oder das Betriebssystem.[41] Das Angebot von SaaS auf dem Markt ist bereits breit gefächert und es werden zahlreiche Services angeboten. So funktionieren Free-Mail-Dienste und soziale Netzwerke SaaS-basiert. Die Cloudnutzer können die Softwarefunktionen über das Anklicken von Buttons im Browserfenster bedienen. Gleiches gilt für Online-Shops und virtuelle Marktplätze, bei denen Softwareapplikationen wie Warenkorb, Such- oder Preisvergleichsfunktionen als integrierte Webseitenbedienung zur Verfügung gestellt werden.[42] Der Cloudnutzer nutzt dabei meist den Webbrowser zum Zugang.[43] Für Unternehmen bietet sich SaaS für Mailservices oder als Office- und Textverarbeitungssoftware an. Im Unternehmensumfeld

---

37 *Heidrich/ Wegener,* MMR 2010, 803 (803); *Birk/ Wegener,* DuD 2010, 641 (642).

38 *Opfermann,* ZEuS 2012, 121 (124); *Niemann/ Paul,* K&R 2009, 444 (445).

39 *Opfermann,* ZEuS 2012, 121 (124); *Schmidt-Bens,* Cloud Computing S. 16; *PWC,* Cloud Computing – Navigation in der Wolke, S. 22.

40 *Nägele/ Jacobs,* ZUM 2010, 281 (281).

41 *Heidrich/ Wegener,* MMR 2010, 803 (804); *Brömmer/ Tresp,* in: Köhler-Schute (Hrsg.), Cloud Computing, S. 52.

42 *Pohle/ Ammann,* K&R 2009, 625 (630).

43 *Opfermann,* ZEuS 2012, 121 (124); *Roth,* in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 6 Rn. 50.

relevant sind auch das Customer Relationship Management (CRM), die Planung von Unternehmensressourcen via Enterprise Resource Planning (ERP) oder das Lieferkettenmanagement „Supply Chain Management", die auch als SaaS am Markt angeboten werden.[44]

Platform as a Service (PaaS) beinhaltet neben der Zurverfügungstellung der Hardware und der Virtualisierungsebene, die Zurverfügungstellung einer Entwicklungsumgebung.[45] PaaS richtet sich primär an Softwareentwickler, die ihre Anwendungen in einer vorinstallierten Entwicklungsumgebung programmieren können.[46] Das Angebot im Rahmen von PaaS kann sowohl Anwendungsinfrastruktur wie Datenbanken und Middleware, als auch Anwendungssoftware umfassen.[47] PaaS ist die am zweithäufigsten genutzte Form des Cloud Computings.[48]

Bei Infrastructure as a Service (IaaS) stellt der Cloudanbieter seinen Nutzern einen Teil seiner Infrastruktur zur Verfügung. Dabei kann es sich um Ressourcen zum Betrieb eines virtuellen Systems handeln, um Speicherplatz, um Netzwerkbandbreite oder auch um eine Mischung davon. Der Cloudanbieter bleibt in der Verantwortung für den Betrieb der Hardware und des Hypervisors, während der Nutzer sich um die Installation und den Betrieb des Betriebssystems und um die Anwendungskomponenten kümmert.[49] Die Infrastruktur wird über eine Benutzerschnittstelle verwaltet und die Abrechnung erfolgt nutzungsbasiert. Für den Cloudnutzer ist die flexible und skalierbare Verfügbarkeit der Ressourcen vorteilhaft, da er auf diese in Zeiten hoher Auslas-

---

44 *Schmidt-Bens*, Cloud Computing, S. 16; *Bedner*, Cloud Computing, S. 70.

45 *Nägele/ Jacobs*, ZUM 2010, 281 (282).

46 *Heidrich/ Wegener*, MMR 2010, 803 (804); *Roth*, in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 6 Rn. 51.

47 *Hennrich*, CR 2011, 546 (547); *Bierekoven*, ITRB 2010, 42 (43).

48 *Beckereit*, in: Köhler-Schute (Hrsg.), Cloud Computing, S. 87; *Redeker*, IT-Recht, Rn. 1127.

49 *Heidrich/ Wegener*, MMR 2010, 803 (803); *Birk/ Wegener*, DuD 2010, 641 (642); *Roth*, in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 6 Rn. 52.

tung zurückgreifen kann, ohne eine eigene kosten- und wartungsintensive Hardware vorhalten zu müssen.[50]

2.2 Erscheinungsarten des Cloud Computings

Beim Cloud Computing wird zudem zwischen verschiedenen Erscheinungsarten unterschieden, je nachdem wer die Cloudumgebung oder die bereitgestellten Ressourcen nutzen kann. Public Clouds zeichnen sich dadurch aus, dass ihr Angebot der Allgemeinheit zur Verfügung steht. Sie scheinen aktuell die Erscheinungsart zu sein, die sich in der Breite durchgesetzt hat.[51] Bei Public Clouds haben die Nutzer in der Regel keine Möglichkeit mitzuentscheiden, mit welchen anderen Nutzern sie sich die Hardware teilen.[52] Dies hat seinen Grund in der hohen Standardisierung der technischen und rechtlichen Gesichtspunkte, die erst eine hohe Flexibilität und Skalierbarkeit ermöglichen.[53]

Private Clouds sind in sich geschlossene Umgebungen, die nur einem bestimmten Nutzerkreis wie beispielsweise einem Unternehmen zur Verfügung stehen. Den Betrieb der virtualisierten IT-Infrastruktur übernimmt dabei das Unternehmen selbst oder auch ein externer Cloudanbieter.[54] Da dem Nutzer exklusiv Ressourcen zur Verfügung gestellt werden, können maßgeschneiderte Lösungen wie eine individuelle Konfiguration oder die Festlegung von Leistungsparametern durchgesetzt werden. Denkbar sind jedoch auch standardisierte und vorkonfigurierte „in a box"-Lösungen.[55] Durch die geschlossene Umgebung können keine anderen Cloudnutzer auf die eigenen Daten zugreifen, was sich als Vorteil darstellt. Nachteilig wirkt sich jedoch aus, dass Private Clouds aufwendiger zu realisieren sind und ihre Nutzung

---

50 *Hennrich,* CR 2011, 546 (547).
51 *Birk/ Wegener,* DuD 2010, 641 (642); *Heidrich/ Wegener,* MMR 2010, 803 (803).
52 *Heidrich/ Wegener,* MMR 2010, 803 (803); *Birk/ Wegener,* DuD 2010, 641 (642).
53 *Hennrich,* CR 2011, 546 (547).
54 *Heidrich/ Paul,* K&R 2009, 444 (445); *Hennrich,* CR 2011, 546 (547); *Brömmer/ Tresp,* in: Köhler-Schute (Hrsg.), Cloud Computing, S. 52; *Giebichenstein,* BB 2011, 2218 (2218); *Schmidt-Bens,* Cloud Computing, S. 19.
55 *Hennrich,* CR 2011, 546 (547).

daher teurer ausfällt. Der Cloudanbieter verliert einen Teil seiner Flexibilität, weil er individualisierte Lösungen zuschneiden und zugleich für jeden Cloudnutzer die Hochverfügbarkeit der entsprechenden Ressourcen gewährleisten muss, da er diese nicht zwischen mehreren Nutzern aufteilen kann.[56] Zudem existieren Mischformen dieser beiden Erscheinungsarten. Die Community Cloud dient der gemeinsamen Nutzung von Anwendern aus einem Anwendungsbereich. Sie hat den Vorteil, dass die Anwender aufgrund ihrer Zugehörigkeit zu einem Anwendungsbereich in etwa die gleichen Anforderungen an die Sicherheit stellen und dass durch die gemeinsame Nutzung Vorteile in den Bereichen der Skalierbarkeit und der Betriebskosten genutzt werden können.[57]

Eine Hybrid Cloud setzt sich aus mehreren Public und Private Clouds zusammen, die miteinander vernetzt werden können.[58] Auf diese Weise können unkritische Daten in einer Public Cloud verarbeitet, während personenbezogene Daten und Betriebsgeheimnisse nur Private Clouds anvertraut werden.[59] Einigen Einschätzungen zufolge wird die Nutzung dieser Erscheinungsart in der Zukunft zunehmen.[60]

---

56 *Heidrich/ Wegener,* MMR 2010, 803 (804); *Birk/ Wegener,* DuD 2010, 641 (642); *Opfermann,* ZEuS 2012, 121 (125); *Hennrich,* CR 2011, 546 (547); *Schmidt-Bens,* Cloud Computing, S. 19.

57 *Birk/ Wegener,* DuD 2010, 641 (642).

58 *Heidrich/ Wegener,* MMR 2010, 803 (804).

59 *Maisch/ Seidl,* VBIBW 2012, 7 (8).

60 *Pohle/ Ammann,* CR 2010, 273 (274), *Janisch*, Cloud Computing und Datenschutz, S. 4.

3 Anwendungs- und Geltungsbereich des Bundesdatenschutzgesetzes

Der Anwendungsbereich des Bundesdatenschutzgesetzes ist eröffnet, wenn personenbezogene Daten i.S.d. § 3 Abs. 1 BDSG erhoben, verarbeitet oder genutzt werden. Aus datenschutzrechtlicher Sicht ist Cloud Computing daher nur relevant, wenn personenbezogene Daten verarbeitet werden. Der Vollständigkeit halber sei angemerkt, dass das Bundesdatenschutzgesetz gem. § 1 Abs. 3 S. 1 BDSG nur subsidiär zur Anwendung kommt, soweit bereichsspezifisches Datenschutzrecht nicht einschlägig ist. Da es sich jedoch bei Cloudservices nach herrschender Meinung nicht um Telekommunikations-Dienste im Sinne des Telekommunikationsgesetzes handelt[61] und in diesem Zusammenhang auch die Anwendung des Telemediengesetzes für Inhaltsdaten, die in die Cloud gegeben werden, abgelehnt wird,[62] wird auf die Darstellung dieser speziellen Regelungen verzichtet werden und statt dessen auf die Vorgaben des deutschen Datenschutzrechts im Bundesdatenschutzgesetz eingegangen, da die Nutzung von Cloudservices durch in Deutschland ansässige Unternehmen im Mittelpunkt der vorliegenden Arbeit stehen soll. Wann das Bundesdatenschutzgesetz zur Anwendung kommt, wird im Folgenden dargestellt werden.

3.1 Normadressaten und personenbezogene Daten

Das Bundesdatenschutzgesetz gilt gem. § 1 Abs. 2 Nr. 1 und 3 BDSG für nicht-öffentliche Stellen und öffentliche Stellen des Bundes. Im Folgenden werden jedoch nur nicht-öffentliche Stellen im Sinne privatwirtschaftlicher Unternehmen behandelt.

Gem. § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Ebenso wird in Abs. 1 die Bezugs-

---

61 *Schuster/ Reichl*, CR 2010, 38 (43); *Heidrich/ Wegener*, MMR 2010, 803 (805); *Schmidt-Bens*, Cloud Computing, S. 24; *Boos/ Kroschwald/ Wicker*, ZD 2013, 205 (206).

62 *Heidrich/ Wegener*, MMR 2010, 803 (805); *Bedner*, Cloud Computing, S. 117.

person der personenbezogenen Daten als „Betroffener“ definiert. Der Betroffene ist derjenige, dessen Persönlichkeitsrecht das Gesetz gem. § 1 Abs. 1 BDSG zu schützen bezweckt.[63] Eine Person ist bestimmt, wenn festgestellt werden kann, dass sich die Angaben auf sie und auf keine andere Person beziehen. In erster Linie geschieht dies anhand des Namens.[64] Die Bestimmbarkeit einer Person setzt die Möglichkeit ihrer Identitätsbestimmung voraus, wobei eine Vielzahl unterschiedlicher Identifizierungsmerkmale bestehen kann. Welche Information eine Person bestimmbar machen, kann nicht abstrakt generell beurteilt werden, vielmehr ist auf die konkreten Umstände des Einzelfalls abzustellen. Die Bestimmbarkeit hängt auch davon ab, welcher Aufwand betrieben werden muss, um die Informationen, die für die Identifizierung notwendig sind, zu erlangen.[65] Gemäß Erwägungsgrund 26 der EU-Datenschutz-Richtlinie (EU-DSRL)[66] sollen bei der Entscheidung über die Bestimmbarkeit einer Person alle Mittel berücksichtigt werden, die vernünftigerweise von einem verantwortlichen Datenverarbeiter oder einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen. Im Rahmen des Cloud Computings können personenbezogene Daten zum einen bei der Nutzung des Cloudservices beispielsweise als Zugangsdaten natürlicher Personen wie der Mitarbeiter des cloudnutzenden Unternehmens oder in Form von IP-Adressen vorliegen. Zum anderen können es Inhaltsdaten sein, die in der Cloud verarbeitet werden. Dies betrifft vor allem personenbezogene Daten über Kunden, Lieferanten oder sonstige Geschäftspartner. Zu denken ist an schützenswerte Angaben aus der Gehaltsabrechnung, der Zeiterfassung oder der E-Mail-Archivierung.[67]

---

63 *Dammann,* in: Simitis (Hrsg.), BDSG 2011, § 3 Rn. 40; *Buchner,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 3 Rn. 11.

64 *Dammann,* in: Simitis (Hrsg.), BDSG 2011, § 3 Rn. 40.

65 *Buchner,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 3 Rn. 11.

66 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:DE:PDF, Stand: 7.6.2014

67 *Weichert,* DuD 2010, 679 (681); *Heidrich/ Wegener,* MMR 2010, 803 (805); *Splittgerber/ Rockstroh,* BB 2011, 2179 (2180).

In § 3 Abs. 9 BDSG werden zudem einige Kategorien personenbezogener Daten aufgezählt, die als sensitive Daten bezeichnet werden.[68] Auch Unternehmen können beispielsweise im Besitz von Gesundheitsdaten oder von Informationen über die Gewerkschaftszugehörigkeit ihrer Mitarbeiter sein und auf die Idee kommen, diese in die Cloud auszulagern, sodass auch sensitive Daten im Rahmen des Cloud Computings Bedeutung erlangen können. Das Bundesdatenschutzgesetz sieht in § 28 Abs. 6 -9 und § 29 Abs. 5 BDSG Sonderregelungen für den Umgang mit sensitiven Daten vor,[69] die sich von denen für personenbezogene Daten unterscheiden und strengere Anforderungen an die Erhebung, Verarbeitung und Nutzung dieser Daten stellen. Im Laufe dieser Arbeit wird aus Platzgründen nicht auf den besonderen Umgang mit sensitiven Daten weiter eingegangen werden können, sodass es beim Betrachtungsgegenstand der personenbezogenen Daten bleiben wird.

Fraglich ist, wie mit personenbezogenen Daten umzugehen ist, wenn sie durch ein Verschlüsselungsverfahren mithilfe eines Kennzeichens und eines Schlüssels hinreichend anonymisiert werden. § 3 Abs. 6 BDSG behandelt die Veränderung personenbezogener Daten, die dazu führt, dass Einzelabgaben über persönliche oder sachliche Verhältnisse nicht oder nur noch mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Für alle Personen oder Stellen, die verschlüsselten Daten berechtigt oder unberechtigt wieder entschlüsseln können, sind diese Daten personenbezogene Daten, für alle anderen nicht.[70]

Kann sichergestellt werden, dass personenbezogene Daten bereits vor dem Transfer in die Cloud mit einem Schlüssel, der dem Stand von Wissenschaft und Technik entspricht, verschlüsselt werden und dieser Schlüssel dem Cloudanbieter nicht bekannt ist, so bestehen beim

---

68 *Simitis,* in: ders. (Hrsg.), BDSG 2011, § 3 Rn. 250.
69 *Simitis,* in: ders. (Hrsg.), BDSG 2011, § 3 Rn. 250.
70 *Roßnagel/ Scholz,* MMR 2000, 721 (725).

Transfer und der weiteren verschlüsselten Speicherung dieser ehemals personenbezogenen Daten keine datenschutzrechtlichen Probleme, da sie keinen Schutzgegenstand des Datenschutzrechts mehr darstellen.[71] Zudem würden diese verschlüsselten Daten für einen unberechtigten Angreifer keinen Wert besitzen.[72] Es bleibt dennoch zu beachten, dass auch die Verschlüsselung von Daten keinen 100%igen Schutz davor bietet, dass Dritte wie z.B. der Cloudanbieter den Personenbezug wiederherstellen können. Dieses Risiko ist jedoch bei Verfahren, die dem Stand der Technik entsprechen, nur mit einem erheblichen Aufwand zu realisieren, weshalb von einem hinreichenden Schutz der ehemals personenbezogenen Daten ausgegangen werden kann.[73]

Die Verschlüsselung ist derzeit vor allem für die Absicherung des Übertragungsweges und für die Speicherung von Daten relevant. Sollen personenbezogene Daten in der Cloud nicht nur gespeichert, sondern auch verarbeitet werden können, bieten Verschlüsselungsverfahren derzeit keine Lösung, weil die Daten für eine Verarbeitung in unverschlüsselter Form vorliegen müssen und sie daher entweder unverschlüsselt in die Cloud eingebracht werden müssen oder der Cloudanbieter und seine Unterauftragnehmer den Schlüssel kennen müssen, um die Daten entschlüsseln zu können.[74] Abhilfe sollen sogenannte voll homomorphen Verschlüsselungen schaffen, mit denen Daten cloudbasiert auf Servern ausgelagert und verarbeitet werden können, ohne dass sie vorher entschlüsselt werden müssen. Wird bei dieser Verschlüsselung das Ergebnis der Verarbeitung entschlüsselt, zeigt sich das gleiche Ergebnis als wenn von Beginn an mit entschlüsselten

---

71 *Köhler/ Arndt/ Fetzer,* Recht des Internet, Rn. 974; *Roth,* in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 6 Rn. 197; *Weichert,* DuD 2010, 679 (681); *Kroschwald,* ZD 2014, 75 (79).

72 *Schmidt-Bens,* Cloud Computing, S. 74.

73 *Köhler/ Arndt/ Fetzer,* Recht des Internet, Rn. 974.

74 *Wagner/ Blaufuß,* BB 2012, 1751 (1751); *Heidrich/ Wegener,* MMR 2010, 803 (804); *Bedner,* Cloud Computing, S. 215; *Kroschwald,* in: Taeger (Hrsg.), Law as a Service (LaaS), S. 300.

Daten gearbeitet worden wäre.[75] Bis heute befindet sich kein solches effizientes Verschlüsselungsverfahren am Markt, jedoch arbeiten eine Reihe von Forschungsprojekten an derartigen Verfahren,[76] sodass es wohl nur eine Frage der Zeit sein dürfte, bis solche Verfahren die Marktreife erreichen.

3.2 Sachlicher Anwendungsbereich

Im sachlichen Anwendungsbereich erstreckt es sich das Bundesdatenschutzgesetz gem. § 1 Abs. 2 Nr. 1 bis 3 BDSG auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die zuvor genannten Stellen. Das Erheben von Daten ist in § 3 Abs. 3 BDSG definiert und meint die Beschaffung von Daten über den Betroffenen; der Gesetzgeber geht dabei von einer zielgerichteten Beschaffung der Daten aus.[77] In der Überzahl der vorgestellten Cloudservices stellt der Cloudanbieter jedoch, je nach Angebot nur die Infrastruktur oder die Software zur Verfügung und verhält sich hinsichtlich der Beschaffung der personenbezogenen Daten passiv. Er ist vielmehr darauf angewiesen, die Daten vom Cloudnutzer zu erhalten, weshalb er selbst regelmäßig keine Daten erheben wird.[78] Die Verarbeitung stellt gem. § 3 Abs. 4 S. 1 BDSG den Sammelbegriff für das Speichern, Verändern, Übermitteln, Löschen und Sperren personenbezogener Daten dar. Der Begriff des Speicherns wird in § 3 Abs. 4 S. 2 Nr. 1 BDSG definiert und bezeichnet das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf Datenträgern zum Zwecke der weiteren Verarbeitung oder Nutzung. Der Begriff des Speicherns hat eine hohe Bedeutung für das Cloud Computing, weil die in die Cloud ausgelagerten Daten in dieser gespeichert werden.[79]

---

75 *Simonite,* Sicheres Computing für die Cloud, abrufbar unter: http://www.heise.de/tr/artikel/Sicheres-Computing-fuer-die-Cloud-1021071.html, Stand: 7.6.2014; *Lapp,* in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 26 Rn. 77.

76 Einen Überblick gibt: *Brenner,* iX 2012, 120 (121 ff.)

77 *Gola/ Schomerus (Hrsg.),* BDSG, § 3 Rn. 24; *Jotzko,* MMR 2009, 232 (235).

78 *Engels,* K&R 2011, 548 (548 f.).

79 *Bedner,* Cloud Computing, S. 118.

Verändern ist gem. § 3 Abs. 4 S. 2 Nr. 2 BDSG das inhaltliche Umgestalten von gespeicherten personenbezogenen Daten. Es ist im Rahmen des Cloud Computings für alle Dienste relevant, die über die bloße Speicherung von Daten hinausgehen.[80]

Der Begriff der Übermittlung ist für das Cloud Computing ebenso von großer Bedeutung.[81] Übermitteln ist gem. § 3 Abs. 4 S. 2 Nr. 3 BDSG die Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten, indem die Daten entweder an diesen weitergegeben werden oder diesem zur Einsicht oder zum Abruf bereitgehalten werden, wobei Dritter gem. § 3 Abs. 8 S. 2 BDSG jede Person oder Stelle sein kann, die nicht der verantwortlichen Stelle zugerechnet wird. Als verantwortliche Stelle wird wiederrum gem. § 3 Abs. 7 BDSG jede Person oder Stelle angesehen, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Aus der Definition der Dritten sind zudem gem. § 3 Abs. 8 S. 3 BDSG Betroffene, sowie Personen und Stellen ausgenommen, die im Inland oder in der EU personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

Löschen ist gem. § 3 Abs. 4 S. 2 Nr. 5 BDSG die Unkenntlichmachung gespeicherter personenbezogener Daten. Das Löschen ist für alle Cloudservices relevant, denn spätestens nach der Beendigung des Vertragsverhältnisses zwischen dem Cloudnutzer und dem Cloudanbieter, sind alle personenbezogenen Daten auf den Servern des Cloudanbieters und seiner Unterauftragnehmer zu löschen. Das Sperren ist in § 3 Abs. 4 S. 2 Nr. 4 BDSG legaldefiniert und bezeichnet das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken. Diese Form der Verarbeitung hat im Rahmen des Cloud Computings nur eine untergeordnete Bedeutung.[82] Nutzen ist gem. § 3 Abs. 5 BDSG jede Verwendung per-

80 *Bedner,* Cloud Computing, S. 119.
81 *Bedner,* Cloud Computing, S. 118.
82 *Bedner,* Cloud Computing, S. 119.

sonenbezogener Daten, bei der es sich nicht um eine Verarbeitung handelt.

Bei nicht-öffentlichen Stellen muss die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten gem. § 1 Abs. 2 Nr. 3 BDSG zudem mithilfe von Datenverarbeitungsanlagen erfolgen. Im Rahmen des Cloud Computings werden die Daten vor und nach dem Transfer an den Cloudanbieter über technische Anlagen wie Server verarbeitet, sodass immer eine automatisierte Datenverarbeitung i.S.d. Bundesdatenschutzgesetzes vorliegen wird.[83]

3.3 Räumlicher Anwendungsbereich

Aus technischer Sicht ist es für das Cloud Computing irrelevant, ob die durch den Cloudnutzer ausgelagerten Daten auf den Servern des Cloudanbieters oder seiner Unterauftragnehmer verarbeitet werden und wo diese Server in der Welt gelegen sind. Aus datenschutzrechtlicher Sicht ist dies jedoch bedeutsam, weil das Bundesdatenschutzgesetz nach dem Ort der Datenverarbeitung differenziert und hierfür unterschiedliche Regelungen bereithält, weshalb es gilt den räumlichen Anwendungsbereich näher zu beleuchten.[84]

Das Bundesdatenschutzgesetz gilt grundsätzlich für jede Verwendung personenbezogener Daten innerhalb Deutschlands, soweit nicht bereichsspezifische oder landesgesetzliche Vorschriften Vorrang genießen.[85] Es beruht auf der EU-Datenschutz-Richtlinie, in der das sogenannte Territorialprinzip aus Art. 4 EU-DSRL verankert ist. Dieses Prinzip wird im deutschen Recht in § 1 Abs. 5 S. 2 BDSG aufgegriffen und bedeutet, dass das Recht des Staates Anwendung findet, in dem die Datenverarbeitung stattfindet.[86] Der Gesetzgeber beurteilt nur danach, ob personenbezogene Daten in seinem Kompetenzbereich erho-

---

83 *Opfermann,* ZEuS 2012, 121 (132).

84 *Weichert,* DuD 2010, 679 (682); *Niemann/ Paul,* K&R 2009, 444 (448 f.).

85 *Simitis,* in: ders. (Hrsg.), BDSG 2011, § 1 Rn. 158; *Gola/ Schomerus* (Hrsg.), BDSG, § 1 Rn. 23.

86 *Opfermann,* ZEuS 2012, 121 (128).

ben, verarbeitet oder genutzt werden sollen; auf die Nationalität oder den Sitz der verantwortlichen Stelle kommt es nicht an, sodass auch ausländische Stellen, die in Deutschland personenbezogene Daten verarbeiten, ebenso wie inländische Stellen deutschem Datenschutzrecht unterliegen.[87] Hierbei ist es auch nicht von Bedeutung, ob personenbezogene Daten von In- oder Ausländern verwendet werden, da das BDSG nicht nach der Nationalität der Betroffenen unterscheidet.[88]

Das Territorialprinzip wird in § 1 Abs. 5 S. 1 HS 1 BDSG zugunsten des sogenannten Sitzlandprinzips verlassen, soweit es um den Datenverkehr zwischen EU-Staaten geht. Das Sitzlandprinzip besagt für den Fall, dass Daten auf deutschem Gebiet erhoben werden, die dafür verantwortliche Stelle jedoch ihren Sitz in einem EU-Staat hat, nicht das deutsche Recht Anwendung findet, sondern das des Sitzstaates.[89] Das Sitzlandprinzip hat seinen Grund in der Vereinheitlichung der Datenschutzniveaus in den EU-Staaten in Zuge der EU-Datenschutz-Richtlinie. Nach dem Willen des Gesetzgebers soll es einen Kompromiss darstellen zwischen den Belangen der Wirtschaft auf der einen Seite, indem diese gem. § 1 Abs. 5 S.1 HS 1 BDSG ihr gewohntes nationales Datenschutzrecht exportieren kann und nicht durch ihr unbekanntes Recht in ihrer unternehmerischen Tätigkeit gehemmt wird und der Rechtssicherheit, insbesondere im Zusammenhang mit den Schutzrechten der Betroffenen auf der anderen Seite, die sich hinter der Ausnahmeregelung des § 1 Abs. 5 S.1 2. HS BDSG für Niederlassungen verbirgt.[90]

Diese Ausnahmeregelung aus § 1 Abs. 5 S.1 HS 2 BDSG, auch modifiziertes Sitzlandprinzip genannt, gilt für die Fälle, in denen eine verantwortliche Stelle aus einem EU-Staat eine Niederlassung im Inland unterhält und von dieser Niederlassung aus vorgeht, sodass dann für

---

87 *Simitis*, in: ders. (Hrsg.), BDSG 2011, § 4b Rn. 8.

88 *Simitis*, in: ders. (Hrsg.), BDSG 2011, § 4b Rn. 9.

89 *Opfermann*, ZEuS 2012, 121 (128); *Gabel*, in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 1 Rn. 54; *Gola/ Schomerus* (Hrsg.), BDSG, § 1 Rn. 27.

90 BT-Drucks. 14/4329, S. 31, abrufbar unter: http://dip21.bundestag.de/dip21/btd/14/043/1404329.pdf, Stand: 7.6.2014

die Tätigkeit der betreffenden Niederlassung uneingeschränkt das Bundesdatenschutzgesetz gilt.[91] Im Zusammenhang mit Cloud Computing sollte nicht unerwähnt bleiben, dass bloße Serverstandorte mangels effektiver Tätigkeitsausübung nicht vom Begriff der Niederlassung erfasst sind.[92] Nach § 1 Abs. 5 S. 4 BDSG findet das Sitzlandprinzip wiederrum in den Fällen Anwendung, in denen nur ein Datentransfer bereits erhobener und gespeicherter Daten über deutsches Territorium erfolgt, ohne dass die Daten in Deutschland zur Kenntnis genommen werden.[93]

Zusammenfassend wird man im Anwendungsfall des Cloud Computings meist davon ausgehen können, dass die Daten bereits im Inland durch die cloudnutzenden Unternehmen erhoben worden sind und somit unter den Anwendungsbereich des Bundesdatenschutzgesetzes fallen,[94] sodass für das internationale Cloud Computing nur die Frage der Zulässigkeit der Übermittlung ins außereuropäische Ausland zu klären gilt. Die Rechtfertigung dieser Übermittlung bestimmt sich nach dem Datenschutzrecht des Staates, in dem der Übermittelnde sitzt, sodass für Datenübermittlungen aus Deutschland deutsches Datenschutzrecht Anwendung findet[95] und im Folgenden daher darauf Bezug genommen wird.

---

91 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 1 Rn. 54; *Gola/ Schomerus* (Hrsg.), BDSG, § 1 Rn. 28; *Dammann,* in: Simitis (Hrsg.), BDSG 2011, § 1 Rn. 199.

92 *Artikel-29-Datenschutzgruppe*, WP 56, S. 9, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_de.pdf, Stand: 7.6.2014; *Dammann,* in: Simitis (Hrsg.), BDSG 2011, § 1 Rn. 203.

93 *Gola/ Schomerus* (Hrsg.), BDSG, § 1 Rn. 30; *Jotzko,* MMR 2009, 232 (235).

94 *Bedner,* Cloud Computing, S. 122; *Eckhardt,* Information Management und Consulting, 4/2010, 55 (58).

95 *Opfermann*, ZEuS 2012, 121 (129).

4 Zulässigkeit der innereuropäischen Datenverarbeitung

Im Bundesdatenschutzgesetz gilt der Grundsatz, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten eines Erlaubnistatbestandes bedarf, um rechtmäßig zu sein. Die Bekanntgabe personenbezogener Daten an Dritte stellt eine Verarbeitung gem. § 3 Abs. 4 S. 2 Nr. 3a BDSG dar. Eine Verarbeitung personenbezogener Daten ist jedoch gem. § 4 Abs. 1 BDSG nur zulässig, wenn der Betroffene eingewilligt hat oder eine gesetzliche Erlaubnisnorm vorliegt.

4.1 Einwilligung als Legitimation

Die Einwilligung stellt gem. § 4a BDSG eine Möglichkeit dar, datenschutzrechtliche Einschränkungen aufzuheben, wenn ansonsten keine Rechtsnorm vorliegt, die die Verarbeitung personenbezogener Daten gestattet. Fraglich ist, ob die Einwilligung im Rahmen des Cloud Computings ein praktikabler Weg ist, um die Verarbeitung personenbezogener Daten zu legitimieren.

Die informierte Einwilligung des Betroffenen trägt dessen Recht auf informationelle Selbstbestimmung Rechnung. Der Betroffene ist gem. § 4a Abs. 1 S. 2 BDSG auf den Zweck der Verarbeitung hinzuweisen, denn er kann nur frei über die Einwilligung entscheiden, wenn er die vorgesehene Verarbeitung kennt und weiß, worin er einwilligt. Dieses Erfordernis setzt die Einsichtsfähigkeit des Betroffenen in die Tragfähigkeit seiner Entscheidung voraus.[96]

Die Abgabe der Einwilligung hat zudem freiwillig zu erfolgen. Dies ist nicht der Fall, wenn die Einwilligung unter Ausnutzung einer wirtschaftlichen Machtposition erzwungen wird.[97] Erzwungene oder nicht hinreichend erläuterte Einwilligungen geben nicht den wahren Willen

---

[96] *Gola/ Schomerus (Hrsg.),* BDSG, § 4a Rn. 25; *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 4a Rn. 31.

[97] *Gola/ Schomerus (Hrsg.),* BDSG, § 4a Rn. 19; *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 4a Rn. 24

des Betroffenen wider und sind daher nichtig.[98] Gem. § 4a Abs. 1 S. 3 BDSG ist die Einwilligung vom Betroffenen grundsätzlich in Schriftform für die Zukunft abzugeben. Der Betroffene kann eine einmal erteilte Einwilligung regelmäßig auch wieder zurücknehmen. Mit dem Widerruf wird der Verarbeitung ex nunc die erforderliche Rechtsgrundlage entzogen.[99]

Damit der Betroffene in die Datenverarbeitung einwilligen kann, sind ihm diesbezüglich detaillierte Informationen wie beispielsweise der Zweck der Erhebung, Verarbeitung oder Nutzung, der Umfang der erhobenen Daten und die weiteren Verarbeitungsschritte explizit mitzuteilen. Während bei der Private Cloud der Umfang der Datenverarbeitung begrenzbar und der Ort der Datenverarbeitung bestimmbar ist, sind genaue vorherige Informationen bezüglich des Ortes und des Zeitpunktes der Datenverarbeitung, sowie der etwaigen Beteiligung von Unterauftragnehmern bei der Private Cloud nicht einfach zu erteilen,[100] sodass sich immer die Frage stellt, ob der Betroffene hinreichend informiert worden ist. Aus diesem Grund und aufgrund der Möglichkeit des jederzeitigen Widerrufs sollte die Einwilligung im Rahmen des Cloud Computings mit Vorsicht gehandhabt werden. Weiterhin berührt eine Datenverarbeitung in der Cloud in der Regel eine Vielzahl von Betroffenen, die alle in die Datenverarbeitung einwilligen müssen, weshalb die Einwilligung nicht als praktikable Legitimation einer Datenverarbeitung im Rahmen des Cloud Computings angesehen werden kann.

4.2 Auftragsdatenverarbeitung gem. § 11 BDSG

Die cloudbasierte Datenverarbeitung kann datenschutzrechtlich jedoch auch legitimiert werden, wenn die Voraussetzungen einer Auftragsdatenverarbeitung gem. § 11 BDSG vorliegen, weshalb zunächst dargestellt werden soll, wodurch sich die Auftragsdatenverarbeitung

98 *Gola/ Schomerus (Hrsg.),* BDSG, § 4a Rn. 22.

99 *Gola/ Schomerus (Hrsg.),* BDSG, § 4a Rn. 38; *Simitis,* in: ders, (Hrsg.), BDSG 2011, § 4a Rn. 102.

100 *BITKOM,* Leitfaden Cloud Computing, S. 62.

auszeichnet und welche Anforderungen der Gesetzgeber an einen Auftragsdatenverarbeitungsvertrag stellt.

Die Auftragsdatenverarbeitung bezeichnet die Auslagerung der Datenverarbeitung von einer verantwortlichen Stelle auf ein in ihrem Auftrag stehendes Hilfsorgan.[101] Der Auftraggeber als verantwortliche Stelle betraut demnach den Auftragnehmer mit der Durchführung der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, wobei es auch ausreichend sein soll, wenn der Auftragnehmer nur Teile dieser Tätigkeiten übernimmt oder diese nur in einem geringen Umfang oder zeitlich begrenzt betreibt.[102]

Die Regelung der Auftragsdatenverarbeitung in § 11 BDSG soll sicherstellen, dass für die Datenverarbeitung außerhalb der verantwortlichen Stelle die gleichen Datenschutz- und Datensicherungsstandards gelten wie für eine Datenverarbeitung durch die verantwortliche Stelle selbst.[103] Dogmatisch handelt es sich bei der Auftragsdatenverarbeitung nicht um einen Erlaubnistatbestand i.S.d. § 4 I BDSG; vielmehr beruht das Rechtsinstitut der Auftragsdatenverarbeitung auf einer gesetzlichen Fiktion.[104]

Das Konstrukt der Auftragsdatenverarbeitung basiert auf der Norm des § 3 Abs. 8 S. 3 BDSG. Danach wird derjenige, der im räumlichen Anwendungsbereich der Norm die Funktion des Auftragsdatenverarbeiters übernimmt, nicht als „Dritter“ i.S.d. Bundesdatenschutzgesetzes angesehen. Dies hat zur Folge, dass die Übertragung personenbezogener Daten keine Übermittlung i.S.d. § 3 Abs. 4 S. 1 Nr. 3 BDSG darstellt und somit keines gesetzlichen Erlaubnistatbestandes oder einer Einwilligung des Betroffenen bedarf.[105] Der Gesetzgeber sieht den

---

101 *Wächter*, CR 1991, 333 (333).

102 *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 22 f.; *Petri,* in: Simitis (Hrsg.), BDSG 2011, § 11 Rn. 12; *Müthlein,* RDV 1992, 63 (64).

103 *Petri,* in: Simitis (Hrsg.), BDSG 2011, § 11 Rn. 1; *Gabel,* in: Taeger/ Gabel, Kommentar zum BDSG, § 11 Rn. 1.

104 *Dammann,* in: Simitis (Hrsg.) BDSG 2011, § 3 Rn. 244.

105 *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 1; *Engels,* K&R 2011, 548 (548); *Müthlein,* RDV 1992, 63 (64).

Auftragnehmer vielmehr als „verlängerten Arm“ des Auftragsgebers und wertet beide Parteien als eine Einheit.[106] Im Umkehrschluss geht aus § 3 Abs. 8 S. 3 BDSG hervor, dass für Stellen außerhalb des Geltungsbereichs der EU-Datenschutz-Richtlinie, denen die Verarbeitung personenbezogener Daten übertragen wird, die Privilegierung des § 11 BDSG nicht gilt.[107] Folglich werden nur Auftragnehmer aus der EU dem deutschen Auftragnehmer gleichgestellt.[108] Soll die Privilegierung des § 11 BDSG greifen, sind somit nur in der EU gelegene Server und Rechenzentren zu nutzen, wenn es um die Verarbeitung personenbezogener Daten geht. Maßgeblich ist immer der Ort der Datenverarbeitung und nicht der Sitz oder die Nationalität des datenverarbeitenden Unternehmens.[109]

Die Auftragsdatenverarbeitung privilegiert den soeben spezifizierten Auftragnehmer, da der Auftraggeber als verantwortliche Stelle gem. § 11 Abs. 1 S. 1 BDSG auch nach der Beauftragung, die Verantwortung für die Einhaltung aller datenschutzrechtlichen Bestimmungen beibehält und sich aus dieser auch nicht lösen kann.[110] Damit die Privilegierung des § 11 BDSG greifen kann, ist von den beteiligten Parteien eine Reihe von Mindestanforderungen einzuhalten, die die inhaltliche Ausgestaltung des Auftragsdatenverarbeitungsvertrags zum Gegenstand haben.[111] Nach der Konzeption des § 11 BDSG liegt eine Auftragsdatenverarbeitung nur in den Fällen vor, in denen der Auftragnehmer ohne einen Wertungs- oder Entscheidungsspielraum auf Wei-

---

106 *Wronka*, RDV 2003, 132 (132); *Gola/ Schomerus (Hrsg.)*, BDSG, § 11 Rn. 3; *Müthlein*, RDV 1993, 165 (166).

107 *Niemann/ Hennrich*, CR 2010, 686 (688); *Schulz*, in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 413; *Dammann*, in: Simitis (Hrsg.), BDSG 2011, § 3 Rn. 246; *Gola/ Schomerus (Hrsg.)*, BDSG, § 11 Rn. 16; *Petri*, in: Simitis (Hrsg.), BDSG 2011, § 11 Rn. 8; *Büllesbach*, Transnationalität und Datenschutz, S. 69.

108 *Nielen/ Thum*, K&R 2007, 171 (171); *Gola/ Schomerus* (Hrsg.), BDSG, § 3 Rn. 55; *Rittweger/ Schmidl*, DuD 2004, 617 (617).

109 *Dammann*, in: Simitis (Hrsg.) BDSG 2011, § 3 Rn. 246; *Gabel*, in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 25; *Plath*, in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 52.

110 *Gabel*, in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 3; *Wächter*, CR 1991, 333 (334).

111 *Gabel*, in: Taeger/ Gabel, Kommentar zum BDSG, § 11 Rn. 1.

sung des Auftraggebers hin agiert. Soll der Auftraggeber beispielsweise den Auftrag in eigener Verantwortung wahrnehmen oder werden ihm die Daten für eigene Geschäftszwecke überlassen, so ist der Auftragnehmer als Dritter i.S.d. § 3 Abs. 8 S. 2 BDSG zu qualifizieren, sodass die Weitergabe der Daten als Übermittlung zu werten ist, die gem. § 4 Abs. 1 BDSG wiederrum einer datenschutzrechtlichen Rechtfertigung bedarf.[112]

4.2.1 Abgrenzung zwischen Auftragsdatenverarbeitung und Funktionsübertragung

In der Literatur wird die Auftragsdatenverarbeitung von der Funktionsübertragung abgegrenzt,[113] weshalb nun geschaut werden soll, anhand welcher Kriterien dies geschieht. Es sei vorab erwähnt, dass die Abgrenzung nicht einfach zu bewerkstelligen ist, weil der Übergang in der Literatur zum Teil als fließend bewertet wird.[114] Ob eine Auftragsdatenverarbeitung oder eine Funktionsübertragung vorliegt, ist in jedem Fall anhand einer Einzelfallbetrachtung zu beurteilen.[115]

Keine Auftragsdatenverarbeitung, sondern eine Funktionsübertragung soll vorliegen, wenn nicht nur die Verarbeitung der Daten, sondern auch die ihr zugrundeliegende Aufgabe, zu deren Erfüllung die Datenverarbeitung notwendig ist, übertragen wird.[116] Dies hat zur Folge, dass die Stelle, der die Funktion übertragen wird, selbst zur verantwortlichen Stelle wird und als Dritter im Sinne des Bundesdatenschutzgesetzes angesehen wird, sodass die Datenweitergabe eine Übermittlung im Sinne des § 3 Abs. 4 S. 2 Nr. 3 BDSG darstellt.[117]

---

112 *Gabel,* in: Taeger/ Gabel, Kommentar zum BDSG, § 11 Rn. 12.

113 *Petri,* in: Simitis (Hrsg.), BDSG 2011, § 11 Rn. 22; *Gola/ Schomerus* (Hrsg.), BDSG, § 11 Rn. 9.

114 *Nielen/ Thum,* K&R 2006, 171 (175); *Büllesbach,* Transnationalität und Datenschutz, S. 69.

115 *Gola/ Schomerus* (Hrsg.), BDSG, § 11 Rn. 9.

116 *Gola/ Schomerus* (Hrsg.), BDSG, § 11 Rn. 9; *Wächter*, CR 1991, 333 (333); *Wronka,* RDV 2003, 132 (133); *Müthlein,* RDV 1993, 165 (166).

117 *Wächter*, CR 1991, 333 (333); *Petri,* in: Simitis (Hrsg.), BDSG 2011, § 11 Rn. 22; *Müthlein,* RDV 1993, 165 (167).

Im Laufe der Zeit sind in der Literatur viele Versuche unternommen worden, Abgrenzungskriterien zur besseren Unterscheidbarkeit beider Rechtsfiguren zu bilden, wobei sich die meisten jedoch als nicht praktikabel erwiesen haben.[118] Auf einige in der Literatur vertretene Abgrenzungskriterien soll nun eingegangen werden. Teilweise wird in der Literatur die Meinung vertreten, dass eine Auftragsdatenverarbeitung ausscheidet, wenn die Stelle, die die Daten erhält, eine eigenverantwortliche Tätigkeit übernimmt. Als Abgrenzungskriterium soll der Spielraum dienen, der der datenempfangenden Stelle, neben den Weisungen der datenübermittelnden Stelle, zur freien Gestaltung bleibt. So soll eine Funktionsübertragung vorliegen, wenn nicht die Datenverarbeitung oder Datennutzung als solche Vertragsgegenstand ist, sondern eine konkrete Aufgabe, zu deren Erfüllung die überlassenen Daten hilfsweise benötigt werden.[119] Aus dieser Ansicht geht hervor, dass derjenige die datenschutzrechtliche Verantwortung tragen soll, der auch die Entscheidungen trifft.[120] Diese Ansicht wird jedoch kritisch hinterfragt. Es wird zu bedenken gegeben, dass die Eigenverantwortung bei der Durchführung der Tätigkeit im Verhältnis Auftraggeber zu Auftragnehmer nicht zwingend mit der datenschutzrechtlichen Verantwortlichkeit einhergeht. So wird als Beispiel angeführt, dass ein Datenvernichter, der eigenverantwortlich über die Art und Weise der Löschung entscheidet und gegenüber dem Auftraggeber für den Erfolg seiner Tätigkeit verantwortlich ist, trotz dieser Eigenverantwortung nach allgemeiner Auffassung als Auftragsdatenverarbeiter angesehen wird, weshalb das Kriterium der eigenverantwortlichen Tätigkeit kein geeignetes Kriterium der Abgrenzung sei.[121]

Nach einer anderen Meinung sollen die Gefahrerhöhung für den Betroffenen und die Überwachbarkeit durch den Auftraggeber geeignete Kriterien sein, um eine Abgrenzung vorzunehmen.[122] Demnach soll

---

118 *Petri,* in: Simitis (Hrsg.), BDSG 2011, § 11 Rn. 24; *Grützmacher*, ITRB 2007, 183 (185).
119 *Müthlein,* RDV 1993, 165 (166 f.).
120 *Sutschet,* RDV 2004, 98 (99).
121 *Sutschet,* RDV 2004, 98 (99).
122 *Kramer/ Hermann,* CR 2003, 938 (939).

eine Auftragsdatenverarbeitung stets dann vorliegen, wenn sich der Auftragnehmer an die Vorgaben des Auftragsdatenverarbeitungsvertrags hält und die Daten nur mechanisch erhoben oder verarbeitet werden, weil dadurch kein zusätzliches Gefahrenpotential für den Betroffenen geschaffen werde und der Auftragnehmer bei seiner Tätigkeit der Aufsicht und den Weisungen des Auftragsgebers unterliegt.[123] Da der mechanische Umgang mit den Daten von den Anhängern dieser Ansicht nicht näher erläutert wird, kann darin kein geeignetes Kriterium zur Abgrenzung gesehen werden.[124]

Ein weiteres Unterscheidungskriterium wird in der Übertragung einer Funktion gesehen. Jedoch wird auch dieses Abgrenzungskriterium als zum Teil untauglich erachtet, da der Begriff der Funktion als unklar angesehen wird.[125] So wird kritisiert, dass im Falle der Übermittlung von Arbeitnehmerdaten an einen Steuerberater zum Zwecke der Gehaltsabrechnung von einer Auftragsdatenverarbeitung ausgegangen wird, während die selbe Übermittlung zum Zweck der steuerlichen Beratung als Funktionsübertragung gewertet wird, obwohl die Gefährdungslage für den Betroffenen in beiden Fällen gleich sei und sich eine derartige Differenzierung nicht aus dem Begriff der Funktion ableiten lasse.[126] Auch wenn diese Kritik sicherlich ihre Berechtigung hat und sich die Grenzziehung zwischen einer Auftragsdatenverarbeitung und einer Funktionsübertragung sehr schwierig gestalten kann, ist das namensgebende Kriterium der Übertragung einer Funktion von den hier vorgestellten Kriterien immer noch das am meisten geeignete, um eine Grenzziehung vorzunehmen.[127]

Auch im Rahmen des Cloud Computings ist eine Grenzziehung mitunter nicht einfach, da als Cloudservices auch ganze Geschäftsprozesse wie CRM oder ERP angeboten werden und die ursprünglichen

---

123 *Kramer/ Hermann,* CR 2003, 938 (939 f.).

124 So auch: *Grützmacher*, ITRB 2007, 183 (185); *Petri,* in: Simitis (Hrsg.), BDSG 2011, § 11 Rn. 24; *Bedner,* Cloud Computing, S. 135; *Sutschet,* RDV 2004, 98 (99).

125 *Sutschet,* RDV 2004, 98 (99).

126 *Sutschet*, RDV 2004, 98 (99).

127 *Bedner,* Cloud Computing, S. 136.

Aufgaben des Auftraggebers vom Auftragnehmer mitausgeführt werden, sodass sich zwangsläufig die Frage aufdrängt, ob in diesen Fällen wirklich von einer Auftragsdatenverarbeitung ausgegangen werden kann.[128] Für den überwiegenden Teil der Cloudservices wird eine Funktionsübertragung jedoch ausscheiden, sodass im Folgenden geschaut werden soll, ob Cloud Computing Auftragsdatenverarbeitung darstellt.

4.2.2 Cloud Computing als Auftragsdatenverarbeitung

Ob Cloud Computing und die unter diesem Begriff angebotenen Cloudservices als Auftragsdatenverarbeitung angesehen werden können, hängt vom genauen Schutzumfang des § 11 BDSG ab. Zum Schutzzweck und -umfang des § 11 BDSG im Zusammenhang mit Rechenzentren und Rechenkapazität werden in der Literatur zwei Auffassungen vertreten.[129]

Nach einer Ansicht umfasst der Schutzzweck des § 11 BDSG diejenigen Fälle, in denen externe Stellen personenbezogene Daten des Auftraggebers zur Kenntnis nehmen oder auf diese einwirken.[130] Demzufolge soll keine Auftragsdatenverarbeitung vorliegen, wenn der Auftragnehmer keine Eingriffsmöglichkeiten in die eigentliche Datenverarbeitung hat. Damit eine Auftragsdatenverarbeitung angenommen werden kann, muss die beauftragte Person unterstützend tätig sein. Eine unterstützende Tätigkeit wird angenommen, wenn der Rechenzentrumsbetreiber Sicherungskopien anfertigt und deren Aufbewahrung übernimmt.[131] Werden Rechenzentren jedoch online oder ausschließlich durch den Auftraggeber gesteuert, soll kein Fall von Auf-

---

128 *Bedner,* Cloud Computing, S. 136.

129 *Müthlein,* RDV 1993, 165 (167); *von Sponeck,* CR 1992, 594 (595); *Walz,* in: Simitis (Hrsg.), BDSG 2006, § 11 Rn. 14; *Eckhardt,* in: Köhler/ Schute (Hrsg.), Cloud Computing, S. 185; *Schuster/ Reichl,* CR 2010, 38 (42); *Müglich,* CR 2009, 479 (482); *Bedner,* Cloud Computing, S. 136;

130 *Müthlein,* RDV 1993, 165 (167); *von Sponeck,* CR 1992, 594 (595).

131 *Gola/ Schomerus (Hrsg.), BDSG,* § 11 Rn. 8; *Müthlein,* RDV 1993, 165 (168); *Engels,* K&R 2011, 548 (549).

tragsdatenverarbeitung vorliegen,[132] weil eine bloße Sachherrschaft über die Rechenanlage und das Ausführen von Hilfsdiensten, um den Betrieb der Anlage zu gewährleisten, für die Annahme einer Auftragsdatenverarbeitung nicht ausreichen soll.[133] So soll das bloße Anmieten von Rechenzentren und Rechenkapazität von einem Dritten keine Auftragsdatenverarbeitung darstellen, wenn sich die Tätigkeit des Dritten im reinen Maschinenbetrieb erschöpft.[134] Somit soll nach der ersten Auffassung immer dann keine Auftragsdatenverarbeitung vorliegen, wenn der Kunde reine Rechenleistung erhält und die Verarbeitung der Daten ausschließlich selbst ohne die Unterstützung des externen Rechenzentrumsbetreibers durchführt, sodass in diesem Fall die gesamte Verantwortung beim Kunden verbleibt und nicht übertragen wird.[135]

Die zweite Literaturmeinung vertritt die Ansicht, dass der Schutzzweck des § 11 BDSG alle Konstellationen erfasst, in denen externe Stellen die Daten des Auftraggebers zur Kenntnis nehmen oder auf ihren Inhalt einwirken können. Daher soll auch die reine Zurverfügungstellung von Rechnerkapazität durch einen Dritten ein Fall der Auftragsdatenverarbeitung sein, wenn die technische Möglichkeit des Datenzugriffs gegeben ist oder zumindest nicht ausgeschlossen werden kann.[136]

Schließt man sich der ersten Literaturmeinung an, so wird der Cloudservice IaaS regelmäßig nicht als Auftragsdatenverarbeitung angesehen werden können, da der Cloudnutzer hierbei die Kontrolle über die Datenverarbeitung behält und der Cloudanbieter nur die Rechenleistung oder den Speicherplatz zur Verfügung stellt, ohne bei der Da-

---

132 *Müthlein*, RDV 1993, 165 (167).

133 *von Sponeck*, CR 1992, 594 (595).

134 *Müthlein*, RDV 1993, 165 (168); *von Sponeck*, CR 1992, 594 (594 f.); *Gola/ Schomerus (Hrsg.)*, BDSG, § 11 Rn. 8; *Spindler/ Schuster (Hrsg.)*, Recht der elektronischen Medien, § 11 Rn. 7.

135 *Müthlein*, RDV 1993, 165 (168).

136 *Walz*, in: Simitis (Hrsg.), BDSG 2006, § 11 Rn. 14; *Eckhardt*, in: Köhler/ Schute (Hrsg.), Cloud Computing, S. 185; *Schuster/ Reichl*, CR 2010, 38 (42); *Müglich*, CR 2009, 479 (482).

tenverarbeitung unterstützend tätig zu werden, auf diese einzuwirken oder die Daten zur Kenntnis zu nehmen.[137] Dieser Auffassung wird jedoch entgegen gehalten, dass bereits in der Bereitstellung der Infrastruktur eine Unterstützungshandlung gesehen werden könne und außerdem durch die physische und lokale Verarbeitung der Daten in den Servern des Anbieters auf die Daten eingewirkt werde. Als Beispiel für eine Einwirkung wird ein Stromausfall im Rechenzentrum angeführt, der zu einem Datenverlust führen könne.[138] Die Frage, welcher Literaturmeinung man folgt, ist jedoch bei der Beurteilung von IaaS nebensächlich, da es bei diesen Services regelmäßig zum angebotenen Leistungsspektrum gehören wird, dass der Cloudanbieter neben der Sorge um die Einsatzbereitschaft des Systems, auch das Anfertigen von Sicherungskopien und Backups der Daten übernimmt, sodass man auch nach der ersten Literaturmeinung zu dem Ergebnis kommen wird, dass bei IaaS eine Auftragsverarbeitung im Sinne des § 11 BDSG vorliegt.[139]

Auch bei den Cloudservices PaaS und SaaS wird man nach beiden Literaturmeinungen zu dem Ergebnis kommen, dass eine Auftragsdatenverarbeitung gem. § 11 BDSG vorliegt. Schließlich werden bei diesen Cloudservices die Daten sowohl beim Cloudanbieter als auch beim Nutzer verarbeitet, wobei der Cloudanbieter häufig auch noch unterstützend tätig wird, sodass auch nach der ersten Literaturmeinung von einer Auftragsdatenverarbeitung ausgegangen werden kann.[140] Bei SaaS wird die Unterstützung durch die komplette anbieterseitige Bereitstellung der Software zur Grundlage des Geschäftsmodells. Da die zweite Literaturmeinung schon die bloße Möglichkeit des Datenzugriffs genügen lässt, um eine Auftragsdatenverarbeitung zu beja-

137 *Engels,* K&R 2011, 548 (549).
138 *Bedner,* Cloud Computing, S. 138.
139 *Bedner,* Cloud Computing, S. 138; *Janisch*, Cloud Computing und Datenschutz, S. 9; *Schuster/ Reichl*, CR 2010, 38 (49).
140 *Bedner,* Cloud Computing, S. 138.

hen, kann die Nutzung von PaaS und SaaS in jedem Fall als Auftragsdatenverarbeitung angesehen werden. [141]

Es sei erwähnt, dass im überwiegenden Teil der Literatur die Frage, ob einzelne Cloudservices als Auftragsdatenverarbeitung zu qualifizieren seien oder nicht, gar nicht gestellt wird, sondern davon ausgegangen wird, dass die Vorschriften der Auftragsdatenverarbeitung für das Cloud Computing einschlägig seien, soweit die Verarbeitung in der EU stattfinde.[142] Aus diesem Grund wird bei der innereuropäischen cloudbasierten Datenverarbeitung nur auf den Fall eingegangen, in dem der Cloudanbieter als Auftragsdatenverarbeiter fungiert und nicht selbst zur verantwortlichen Stelle wird.

4.2.3 Anforderungen an das Auftragsdatenverarbeitungsverhältnis

Der Auftraggeber bleibt im Rahmen einer Auftragsdatenverarbeitung gem. § 11 Abs. 1 S. 1 BDSG als Herr über die Daten datenschutzrechtlich verantwortlich. Der Mindestinhalt eines Auftragsdatenverarbeitungsvertrags wird in § 11 Abs. 2 S. 2 BDSG durch das Gesetz im Rahmen des sogenannten „10-Punkte-Katalogs“ gesetzlich vorgegeben,[143] der im Folgenden näher betrachtet wird.

4.2.3.1 Pflichten des Auftraggebers

§ 11 Abs. 2 S. 1 BDSG verpflichtet den Auftraggeber, den Auftragnehmer sorgfältig auszuwählen. Die Auswahl des Auftragnehmers ist eng geknüpft an die technischen und organisatorischen Maßnahmen, die von diesem angeboten werden, weshalb die Datensicherungsmaßnahmen des Auftragnehmers mit der Schutzbedürftigkeit der betref-

---

141 *Bedner,* Cloud Computing, S. 138; *Bergt,* DuD 2013, 796 (796).

142 *Niemann/ Paul,* K&R 2009, 444 (449); *Schuster/ Reichl,* CR 2010, 38 (38); *Schulz,* in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 411; *Karger/ Sarre,* in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 434; *Heidrich/ Wegener,* MMR 2010, 803 (805 f.); *Niemann/ Hennrich,* CR 2010, 686 (687); *Schulz/ Rosenkranz,* ITRB 2009, 232 (235); *Conrad,* in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 25 Rn. 348; *Borges,* DuD 2014, 165 (165).

143 *Vander,* K&R 2010, 292 (294); *Söbbing,* in: Leible/ Sosnitza (Hrsg.), Onlinerecht 2.0, S. 69; *Bierekoven,* in: Bartsch/ Briner (Hrsg.), DGRI Jahrbuch 2010, S. 110.

fenden Daten zu korrespondieren haben.[144] Im Rahmen einer sorgfältigen Auswahl muss sich der Auftraggeber ein möglichst umfassendes Bild von seinem Auftragnehmer verschaffen. Die nötigen Informationen kann er sich beispielsweise durch die Einholung von Auskünften, die Vorlage von Prüfberichten und Zertifizierungen oder die Besichtigung des Rechenzentrums verschaffen.[145]

Eine weitere Pflicht besteht in der schriftlichen Auftragserteilung gem. § 11 Abs. 2 S. 2 BDSG, wobei es auf die Rechtsnatur des Vertrages nicht ankommen soll.[146] Das Schriftformerfordernis gilt ausschließlich für den Abschluss des Vertrags, nicht hingegen für die Weisungen, die im Rahmen des Vertragsverhältnisses erteilt werden.[147] In diesem Zusammenhang sieht § 11 Abs. 2 S. 2 Nr. 1 BDSG vor, dass Gegenstand und Dauer des Auftrags festzulegen sind. Diese werden sich jedoch regelmäßig aus dem zugrundeliegenden Dienstleistungsvertrag ergeben, weshalb es genügen soll, auf die dortigen Festlegungen zu verweisen.[148]

Weiterhin sind gem. § 11 Abs. 2 S. 2 Nr. 2 BDSG Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und Nutzung, die Art der Daten und der Kreis der Betroffenen festzulegen. Dies erfordert eine genaue Beschreibung der Leistungen im Vertrag, die vom Auftragnehmer zu erbringen sind.[149] Da nur allgemeine Angaben zu der Art der Daten und zum Kreis der Betroffenen gefordert werden, ist eine präzise Beschreibung nicht erforderlich, sodass Kategorisierungen und Abstrahierungen als ausreichend angesehen werden.[150] So soll es zur Beschreibung der Art der Daten genügen, sie als Mitarbei-

---

144 *Petri,* in: Simitis (Hrsg.), BDSG 2011, § 11 Rn. 56; *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 32.

145 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 33.

146 *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 95.

147 *Maisch/ Seidl,* VBIBW 2012, 7 (11).

148 *Gola/ Schomerus (Hrsg.),* BDSG, § 11 Rn. 18; *Maisch/ Seidl,* VBIBW 2012, 7 (11).

149 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 43.

150 *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 101; *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 43.

terdaten oder Kundendaten anzugeben.[151] Teilweise wird im Zusammenhang mit § 11 Abs. 2 S. 2 Nr. 2 BDSG gefordert, dass der Auftraggeber Art und Umfang der Datenverarbeitung, sowie Ort und Zeit vollständig zu kennen oder zu beherrschen hat, wobei zugleich angemerkt wird, dass dies nach derzeitigem Stand der Technik beim Cloud Computing nicht möglich sei.[152]

Der Blick ins Gesetz zeigt, dass eine solche Anforderung gesetzlich nicht verankert ist und sich allenfalls aus der Stellung des Auftragsdatenverarbeiters als Herr der Auftragsdatenverarbeitung herleiten ließe.[153] Daher wird zum Teil die Meinung vertreten, dass es im Rahmen des Cloud Computings ausreichend sein soll, wenn der Cloudnutzer die örtlichen und zeitlichen Umstände der Datenverarbeitung nachträglich mittels Monitoringmaßnahmen wie beispielsweise automatisierten Protokollierungen nachvollziehen kann, die ihm ermöglichen zu sehen, an welchen physischen Standorten welche personenbezogene Daten zu welchen Zeitpunkten gespeichert und verarbeitet worden sind.[154]

Dieser Vorschlag ist zu begrüßen, wobei es selbstverständlich nicht sein darf, dass der Cloudanbieter die Daten an beliebige Rechenzentren auf der ganzen Welt weiterleitet und der Nutzer davon erst im Nachhinein erfährt. Vielmehr muss eine gewisse Eingrenzung der möglichen Standorte schon im Voraus erfolgen. Eine mögliche Eingrenzung kann darin liegen, dass nur Rechenzentren in der EU genutzt werden. Solche Möglichkeiten bestehen in der Tat auch in der Praxis. Beispielsweise sichert Fujitsu seinen Cloudnutzern auf Wunsch zu, dass ihre Daten nicht ins Ausland verlagert werden.[155] Im Hinblick

---

151 *Gola/ Schomerus (Hrsg.),* BDSG, § 11 Rn. 18a; *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 101.

152 *Schuster/ Reichl,* CR 2010, 38 (41); *Heidrich/ Wegener,* MMR 2010, 803 (806).

153 *Bedner,* Cloud Computing, S. 143.

154 *International Working Group on Data Protection in Telecommunications,* WP on Cloud Computing – Privacy and data protection issues, S. 3; *Schröder/ Haag,* ZD 2012, 362 (364).

155 *Kiehne,* in: Köhler-Schute (Hrsg.), Cloud Computing, S. 29.

auf die automatisierte Protokollierung ist zudem wichtig, dass aus den Protokolldateien hervorgeht, in welcher Weise die Daten vom Cloudanbieter oder Unterauftragnehmer genutzt worden sind und dass diese Dateien nicht kompromittierbar sind, da der Cloudnutzer nur dann nachvollziehen kann, ob die vertraglich zugesicherten Bestimmungen auf Anbieterseite auch eingehalten worden sind.[156]

Nach § 11 Abs. 2 S. 2 Nr. 4 BDSG ist die Berichtigung, Löschung und Sperrung von Daten ebenfalls zu regeln. Der Adressat der Regelung ist gem. § 11 Abs. 1 S. 2 BDSG der Auftraggeber. Dieser muss sicherstellen können, dass er in der Lage ist, die entsprechenden Rechte gegenüber seinem Auftragnehmer durchzusetzen.[157] Der Auftragnehmer ist auf die Umsetzung der Weisungen des Auftraggebers beschränkt und von sich selbst aus nicht zur Berichtigung, Löschung und Sperrung der Daten berechtigt.[158] Im Rahmen des Cloud Computings kann die Berichtigung, Löschung oder Sperrung auch per Webinterface oder sonstiger Software vom Cloudnutzer angewiesen werden; der Anweisung hat der Cloudanbieter zu entsprechen.[159] Gem. § 11 Abs. 2 S. 2 Nr. 10 BDSG ist zudem die Rückgabe überlassener Datenträger und die Löschung der beim Auftragnehmer gespeicherten Daten bei Beendigung des Auftrags zu regeln. Im Interesse des Auftraggebers sollte der Umfang der Datenherausgabe weit gefasst werden, da der Auftraggeber in der Regel nicht nur ein Interesse an den Daten hat, die er dem Auftragnehmer ursprünglich überlassen hat, sondern auch an den Daten interessiert ist, die der Auftragnehmer im Rahmen der Auftragserfüllung geschaffen hat.[160] Aufgrund der Vielzahl der am Cloud Computing beteiligten Rechenzentren ist besonders darauf zu achten, dass die Daten überall zu löschen sind. Dies sollte sich jedoch im Vertrag zwischen Cloudnutzer und Cloudanbieter ver-

156 *Schröder/Haag,* ZD 2012, 362 (364).

157 *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 103; *Gola/ Schomerus (Hrsg.),* BDSG, § 11 Rn. 18c.

158 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 45; *Wächter,* CR 1991, 333 (335).

159 *Bedner,* Cloud Computing, S. 141 f.

160 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 51.

einbaren lassen. Der Cloudanbieter muss diese Verpflichtung wiederrum in seine Verträge mit den Unterauftragnehmern aufnehmen.

Weiterhin legt das Bundesdatenschutzgesetz dem Auftraggeber Kontrollpflichten auf. So ist es gem. § 11 Abs. 2 S. 4 BDSG die Pflicht des Auftraggebers, sich von den getroffenen technischen und organisatorischen Maßnahmen des Auftragnehmers zu überzeugen. Die erste Prüfung hat vor Beginn der Datenverarbeitung zu erfolgen. Während der Vertragslaufzeit sind weitere Kontrollen durchzuführen.[161] Das Unterlassen der Kontrolle vor Beginn der Datenverarbeitung ist gem. § 43 Abs. 1 Nr. 2b BDSG sanktionsbewährt. Bei der Überwachung des Auftragnehmers geht es in erster Linie darum sicherzustellen, dass die verabredeten technischen und organisatorischen Maßnahmen zur Erledigung des Auftrags ordnungsgemäß implementiert sind. Eine nähere Prüfung der Maßnahmen ist erforderlich, um Unzulänglichkeiten identifizieren zu können, bevor es zu der eigentlichen Datenverarbeitung kommt.[162] Für die weiteren Kontrollen sind gesetzlich keine festen Prüfintervalle vorgegeben. Diese sollen sich vielmehr aus den Umständen des Einzelfalls und insbesondere aus der Art, der Schutzbedürftigkeit und dem Umfang der verarbeiteten Daten ergeben.[163] An die Kontrollintensität der Folgekontrollen stellt der Gesetzgeber geringere Anforderungen als an die Kontrollen vor Beginn der Datenverarbeitung, weil der Auftraggeber auf bestehendem Wissen aufsetzen soll.[164] Das Ergebnis der Kontrollen ist gem. § 11 Abs. 2 S. 5 BDSG zu dokumentieren, wobei keine besonderen Anforderungen an Art und Umfang der Dokumentation gestellt werden.

Auch für den Cloudanbieter gilt es, geeignete Maßnahmen zur Datensicherheit zu treffen, um den Schutz der ihm anvertrauten Daten zu

---

161 *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 113; *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 35.

162 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 36.

163 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 37; *Vander,* K&R 2010, 292 (295).

164 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 37; *Hallermann,* RDV 2012, 226 (228).

gewährleisten. Der Cloudnutzer hat zu prüfen, ob die Maßnahmen, die sich aus § 9 BDSG und dessen Anlage ergeben, geeignet sind, um den Schutz der Daten zu gewährleisten und ob die Maßnahmen letztendlich vom Cloudanbieter auch umgesetzt werden.[165] Dies gestaltet sich jedoch bei Public Clouds als schwierig, da der genaue Ort der Daten vorab meist nicht bekannt ist. Da der Ort der Datenverarbeitung vorher nicht festgestellt werden kann, kann der Cloudnutzer seinen Kontrollpflichten nur nachkommen, wenn er alle Rechenzentrumsstandorte aufsucht. Mag dies bei Cloudanbietern, die wenige Rechenzentren in einer begrenzten örtlichen Umgebung betreiben noch mit vertretbarem Aufwand und vertretbaren Mitteln geschehen, stößt diese Kontrollmöglichkeit allein schon bei zusammengeschalteten Rechenzentren in der EU an die Grenze des Machbaren, zumal im Vorhinein nicht bekannt ist, ob ein bestimmtes Rechenzentrum im Laufe der Vertragsbeziehung überhaupt genutzt wird.[166] Sind Unterauftragnehmer im Spiel, scheitert die Vor-Ort-Kontrolle aus Gründen der Praktikabilität. Weiterhin ist zu bedenken, dass Cloudanbieter meist nicht bereit sein werden, ihre Rechenzentren von Kunden vor Ort besichtigen zu lassen, da Vor-Ort-Kontrollen physische Angriffe auf die Hardware und Infrastruktur ermöglichen und auch Lücken im Sicherheitskonzept vor Ort schneller aufgespürt werden können.[167]

Der Gesetzgeber schreibt jedoch auch keine Begehung vor Ort vor, sodass der Auftraggeber beim Auftragnehmer vor Ort auch nicht vor-

---

165 *Eckhardt*, in: Köhler/ Schute (Hrsg.), Cloud Computing, S. 187.

166 *Niemann/ Hennrich*, CR 2010, 686 (691); *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Orientierungshilfe – Cloud Computing, S. 9; *Trusted Cloud*, Datenschutzrechtliche Lösungen für Cloud Computing, S. 6 f., abrufbar unter: http://www.trusted-cloud.de/documents/Datenschutzrechtliche-Loesungen-fuer-Cloud-Computing.pdf, Stand: 7.6.2014; *Bierekoven*, in: Bartsch/ Briner (Hrsg.), DGRI Jahrbuch 2010, S. 108; *Kühling/ Biendl*, CR 2014, 150 (152).

167 *Bedner*, Cloud Computing, S. 145 f; *Weiss*, DuD 2014, 170 (170 f.); *Kühling/ Biendl*, CR 2014, 150 (152).

stellig werden muss.[168] Vielmehr soll die Kontrolle durch Datenschutz-Audits, Zertifizierungen oder Testate ersetzt werden können.[169] Die Kontrollpflicht soll daher als erfüllt angesehen werden, wenn der Cloudanbieter und seine Unterauftragnehmer Prüfberichte, Zertifikate oder Testate vorlegen können, die sich am Maßstab des § 9 BDSG orientieren und der Gefährdungslage der Datenverteilung in der Wolke gerecht werden.[170] Die ausgelagerte Kontrolle durch Sachverständige im Rahmen von Zertifizierungen und Audits hat zudem den Vorteil, dass sie in den meisten Fällen effektiver sein dürfte, da in der Praxis wohl nicht jeder Cloudnutzer die Kenntnisse haben wird, um Mängel aufspüren zu können.

4.2.3.2 Pflichten des Auftragnehmers

Da § 11 Abs. 2 S. 4 BDSG zwar vorsieht, dass sich der Auftraggeber von den technischen und organisatorischen Maßnahmen des Auftragnehmers zu überzeugen hat, jedoch nichts zu Art und Umfang der zu diesem Zweck durchzuführenden Kontrollen und den damit einhergehenden Duldungs- und Mitwirkungspflichten des Auftragnehmers aussagt, bedarf es nach § 11 Abs. 2 S. 2 Nr. 7 BDSG entsprechender vertraglicher Regelungen, die sich an § 11 Abs. 2 S. 4 BDSG zu orientieren haben. Die Duldungs- und Mitwirkungspflichten des Auftragnehmers gestalten sich spiegelbildlich zu den Kontrollrechten des Auftraggebers, sodass es die Pflicht des Auftragnehmers darstellt, diese zu dulden und daran mitzuwirken.[171] Dies gilt auch im Rahmen des Cloud Computings.

---

168 BT-Drucks. 16/13657, S. 18, abrufbar unter: http://dip21.bundestag.de/dip21/btd/16/136/1613657.pdf, Stand: 19.6.201; *Eckhardt,* DuD 2009, 587 (589); *Weichert,* DuD 2010, 679 (682); *Vander,* K&R 2010, 292 (295); *Hallermann,* RDV 2012, 226 (226); *Borges,* DuD 2014, 165 (168).

169 BT-Drucks. 16/13657, S. 18; *Petri,* in: Simitis (Hrsg.), BDSG 2011, § 11 Rn. 59.

170 *Eckhardt,* in: Köhler/ Schute (Hrsg.), Cloud Computing, S. 187; *Niemann/ Hennrich,* CR 2010, 686 (691); *Schweda,* ZD-aktuell 2012, 30109.

171 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 48; *Hoeren,* DuD, 2010, 688 (690).

Problematisch ist, dass das Kontrollrecht gem. § 11 Abs. 2 S. 2 Nr. 7 BDSG und die entsprechenden Duldungs- und Mitwirkungspflichten derart verstanden werden, dass sich der Cloudnutzer ein Recht zur Kontrolle vor Ort in den Rechenzentren vorbehalten muss.[172] Dies ist allerdings wie bereits geschildert nur schwer zu realisieren, da häufig nicht klar ist, wo genau sich die Daten in der Wolke befinden und welches Rechenzentrum zu einem bestimmten Zeitpunkt genutzt wird. Erschwerend kommt hinzu, dass Cloudanbieter häufig die Standorte ihrer Rechenzentren verheimlichen.[173] Als Konsequenz der problematischen Durchsetzung der Kontrollrechte wird gefordert, dass in solchen Fällen Cloudservices nicht zur Verarbeitung personenbezogener Daten genutzt werden dürften.[174] Andere Meinungen sehen die Umsetzung der Vorgabe über die Kontrolle vor Ort nicht per se als unmöglich an, sondern fordern auf diesem Wege Präzisierungen vom Cloudanbieter, um die Vorgabe erfüllen zu können.[175] Wie diese Präzisierungen aussehen sollen, wird jedoch nicht ausgeführt.

Eine weitere Pflicht ergibt sich aus § 11 Abs. 4 i.V.m. § 9 BDSG und verpflichtet den Auftragnehmer zur eigenverantwortlichen Festlegung und Durchführung von Maßnahmen zur Datensicherheit, um den vom Bundesdatenschutzgesetz geforderten Schutz personenbezogener Daten sicherzustellen.[176] Neben den Duldungs- und Mitwirkungspflichten und der Pflicht zur Datensicherung besteht auch die Pflicht zur Wahrung des Datengeheimnisses gem. § 11 Abs. 4 i.V.m. § 5 BDSG. Weiterhin hat der Auftragnehmer einen betrieblichen Datenschutzbeauftragten zu benennen, der als Ansprechpartner bei der Auftragsdurchführung dient.[177]

---

172 *Eckhardt,* in: Köhler/ Schute (Hrsg.), Cloud Computing, S. 187; *Borges,* DuD 2014, 165 (165).

173 *Bedner,* Cloud Computing, S. 148.

174 *Engels,* K&R 2011, 548 (550).

175 *Eckhardt,* in: Köhler/ Schute (Hrsg.), Cloud Computing, S. 187.

176 *Wächter,* CR 1991, 333 (335).

177 *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 104; *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 46.

Ebenso ist gem. § 11 Abs. 2 S. 2 Nr. 8 BDSG festzulegen, dass der Auftragnehmer dem Auftraggeber Verstöße gegen das Bundesdatenschutzgesetz oder den Auftragsdatenverarbeitungsvertrag mitteilen muss. Der Wortlaut der Norm lässt die Interpretation zu, dass nicht jede Unregelmäßigkeit bei der Datenverarbeitung vom Auftragnehmer an den Auftraggeber zu melden ist, auch wenn dies im Sinne des Auftraggebers als einzigem für die Einhaltung des Datenschutzes Verantwortlichen sein dürfte.[178] Grundsätzlich ist es auch beim Cloud Computing vertraglich darstellbar, dass Cloudanbieter und Unterauftragnehmer zur Mitteilung ihrer Verstöße verpflichtet sind.

Schließlich wird der Auftragnehmer gem. § 11 Abs. 3 S. 1 BDSG dazu verpflichtet, die Daten nur im Rahmen der Weisungen des Auftraggebers zu verarbeiten oder zu nutzen. Dies korrespondiert mit der Pflicht des Auftraggebers zur Weisungserteilung. § 11 Abs. 2 S. 2 Nr. 9 BDSG greift die Weisungserteilung zusätzlich auf und verlangt, dass der Umfang der Weisungsrechte festzulegen ist. In diesem Zusammenhang werden die im Auftrag enthaltenen Festlegungen der zu erbringenden Leistungen des Auftragnehmers sowie die technischen und organisatorischen Schutzmaßnahmen als Weisungen angesehen.[179]

Die Vorschriften des Bundesdatenschutzgesetzes sind insoweit eindeutig, jedoch wirft die Praxis des Cloud Computings die Frage auf, wie die Erteilung von Weisungen durch den Cloudnutzer funktionieren soll, wenn die Angebote größtenteils auf standardisierten Verfahrensabläufen beruhen und die Durchsetzung individueller Wünsche tatsächlich kaum oder nur in Form allgemeiner Anforderungen wie beispielsweise technischer Sicherheitsstandards realisiert werden kann. Vor diesem Hintergrund werden dem Cloudanbieter Optionsangebote abverlangt, bei denen Nutzer zwischen Ressourcen, Ländern, Sicherheitsniveaus und anderen Nutzungsmerkmalen wählen

178 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 49.
179 *Schweda,* ZD-aktuell 2012, 30109.

können sollen.[180] Dieser Vorschlag wird als praxistaugliche Lösung erachtet, jedoch wird zu bedenken gegeben, dass Cloudanbieter häufig gar keine Optionsangebote anbieten könnten, da sie entweder nur standardisierte Hilfsfunktionen anbieten könnten oder Optionsangebote ihrem Geschäftsmodell zuwiderliefen.[181] Konkrete Einzelabreden und individuelle Weisungsmöglichkeiten werden daher wohl nur bei Community Clouds umgesetzt werden können.[182]

4.2.3.3 Pflichten bezüglich technischer und organisatorischer Maßnahmen

Gem. § 11 Abs. 2 S. 2 Nr. 3 BDSG sind weiterhin die vom Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit und zum Schutz personenbezogener Daten festzulegen. Gemeint sind damit die Vorgaben aus § 9 BDSG und der Anlage zu § 9 S. 1 BDSG, die in allen Rechenzentren des Cloudanbieters und seiner Unterauftragnehmer zu treffen sind.[183] § 9 S. 1 BDSG verpflichtet Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, diejenigen technischen und organisatorischen Maßnahmen zu treffen, die für die Gewährleistung eines hohen Maßes an Datensicherheit erforderlich sind. Gem. § 9 S. 2 BDSG ist eine Maßnahme nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Die Anlage, auf die in § 9 S. 1 BDSG verwiesen ist, konkretisiert diese Maßnahmen. Sie sind im Auftrag konkret zu benennen.[184]

In der Literatur wird zum Teil gefordert, dass nicht nur die abstrakte Methode oder das Schutzziel vom Cloudanbieter zu benennen ist, sondern auch das konkret genutzte Sicherungsmittel.[185] Dieser Forde-

---

180 *Weichert,* DuD 2010, 679 (685).

181 *Niemann/ Hennrich,* CR 2010, 686 (692); *Maisch/ Seidl,* VBIBW 2012, 7 (12).

182 *Bedner,* Cloud Computing, S. 151.

183 *EuroCloud Deutschland_eco e.V.,* Leitfaden Cloud Computing, S. 16; *Bedner,* Cloud Computing, S. 162.

184 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 44; *Gola/ Schomerus (Hrsg.),* BDSG, § 9 Rn. 2; *Bergt,* DuD 2013, 796 (797),

185 *Weichert,* DuD 2010, 679 (685); *Müglich,* CR 2009, 479 (483 f.).

rung, die dem Ziel der Transparenzerhöhung dient, wird entgegengehalten, dass Cloudstrukturen komplex seien und Cloudanbieter zudem ein Interesse daran hätten, ihr Geschäftsmodell nicht komplett offenzulegen.[186]

Ob alle 8 Punkte der Anlage 1 zu § 9 Abs. 1 BDSG beim Cloud Computing erfüllt werden können, ist fraglich, da die Vorgaben aus § 11 Abs. 2 S. 2 Nr. 3 und die des Anhangs zu § 9 BDSG aus einer Zeit stammen, in der klassische Auftragsverhältnisse in 1:1-Verhältnissen die Regel waren und die Vorgaben nicht darauf zugeschnitten sind, dass Leistungen durch mehrere Beteiligte von verteilten Rechenzentren aus erbracht werden, wie es beim Cloud Computing üblich ist. Daher stellt sich die Frage, ob die Maßnahmen für alle an der Erbringung des Cloudservices beteiligten Rechenzentren, auch die etwaiger Unterauftragnehmer, in derart konkreter Weise festgelegt werden können wie es das Bundesdatenschutzgesetz fordert.[187] Im Folgenden soll insbesondere auf die Vorgaben eingegangen werden, die im Rahmen des Cloud Computings problematisch sind.

Nr. 1 der Anlage betrifft die Zutrittskontrolle und verlangt, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren ist, damit diese von vorneherein keine Möglichkeit zur unbefugten Kenntnis- und Einflussnahme erhalten.[188] Die Zutrittskontrolle erfordert neben typischen baulichen Gebäude- und Raumsicherungsmaßnahmen unter Umständen auch die optische Abschirmung der Anlage.[189] Weiterhin muss neben der physischen Absicherung sichergestellt sein, dass nur derjenige Zutritt erhält, der hierzu auch berechtigt ist. Dies kann beispielsweise durch Berechtigungsausweise, Pförtner oder

---

186 *Niemann/ Hennrich,* CR 2010, 686 (690); *Vander,* K&R 2010, 292 (294).

187 *Conrad/ Hausen,* in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 2 Rn. 308; *Söbbing,* in: Leible/ Sosnitza (Hrsg.), Onlinerecht 2.0, S. 73.

188 *Gola/ Schomerus* (Hrsg.), BDSG, § 9 Rn. 22; *Heibey,* in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Kap. 4.5 Rn. 39.

189 *Ernestus,* in: Simitis (Hrsg.), BDSG 2006, § 9 Rn. 72; *Roth,* ITRB 2010, 60 (60).

ausweisbasierte Schranken erreicht werden.[190] In Bezug auf Cloudrechenzentren ergeben sich keine Besonderheiten, da wie bereits festgestellt, im Rahmen der Auftragsdatenverarbeitung keine Vor-Ort-Begehung vorgeschrieben ist und es auch nicht dem Vorgehen der Cloudanbieter und dessen Unterauftragnehmern entspricht, ihren Kunden physischen Zutritt zu ihren Rechenzentren zu gewähren.

Die Zugangskontrolle nach Nr. 2 der Anlage soll verhindern, dass Unbefugte die Datenverarbeitungssysteme nutzen können. Im Gegensatz zur Zutrittskontrolle ist damit das Eindringen in das EDV-System selbst gemeint.[191] Die Zugangskontrolle betrifft auch den Zugang über Netzwerke wie beispielsweise über das Internet, was insbesondere für das Cloud Computing bedeutsam ist.[192] Als konkrete Maßnahmen für das Cloud Computing kommen die Absicherung mittels Firewalls, der Schutz mittels Passwörtern und die Protokollierung der Passwortnutzung zur nachträglichen Nachvollziehung von Zugriffen in Betracht.[193]

Die Zugriffskontrolle nach Nr. 3 der Anlage soll als Ergänzung zur Zugangskontrolle sicherstellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich nur auf die Daten zugreifen können, die von ihrer Zugriffsberechtigung erfasst sind und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Im Rahmen einer datenschutzgerechten Organisation ist sicherzustellen, dass der Zugriff nur auf solche Daten erfolgt, die der Mitarbeiter zur Erledigung der ihm übertragenen Aufgaben benötigt.[194] Im Rahmen des Cloud Computings muss sichergestellt sein, dass die einzelnen virtuellen Maschinen voneinander abgetrennt sind und dass nur auf die Daten derjenigen virtuellen Maschinen zugegriffen werden kann, die von der Zugriffsberechtigung gedeckt

---

190 *Gola/ Schomerus* (Hrsg.), BDSG, § 9 Rn. 22; *Roth,* ITRB 2010, 60 (61).

191 *Gola/ Schomerus* (Hrsg.), BDSG, § 9 Rn. 23; *Laue/ Stiemerling,* DuD 2010, 692 (695).

192 *Ernestus,* in: Simitis (Hrsg.), BDSG 2011, § 9 Rn. 89; *Heibey,* in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Kap. 4.5 Rn. 43.

193 *Bedner,* Cloud Computing, S. 165.

194 *Gola/ Schomerus* (Hrsg.), BDSG, § 9 Rn. 24.

sind.[195] Alleinige Vollzugriffe der Administratoren auf Daten sollten vermieden werden.[196] Hier wird ebenso eine Protokollierung erfolgter Zugriffe vorgeschlagen.[197]

Nr. 4 der Anlage behandelt die Weitergabekontrolle. Demnach muss gewährleistet sein, dass personenbezogene Daten bei der elektronischen Übertragung, während des Transports oder während ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist. Davon erstfasst ist sowohl die elektronische Übermittlung via Telekommunikation als auch der herkömmliche Transport von Datenträgern. Der herkömmliche Transport von Datenträgern kann auch beim Cloud Computing Bedeutung erlangen, weil beispielsweise das erstmalige Einbringen der Daten in die Cloud durch das Zusenden von Datenträgern schneller und günstiger erfolgen kann als auf elektronischem Wege. Beide Möglichkeiten der Übermittlung haben verschlüsselt zu erfolgen.[198] Sind die Daten im Rechenzentrum angelangt, müssen die Datenträger vor Diebstahl und sonstiger unbefugter Kenntnisnahme geschützt werden. Ebenso sind die leitungsgebundenen Übertragungswege beispielsweise mittels Firewalls zu schützen. Im Rahmen der zur Weitergabekontrolle gehörenden Übermittlungskontrolle wird auch die Angabe der konkreten Person, die die Daten erhalten soll, gefordert.[199] Dies ist beim Cloud Computing, das durch weltweit verteilte Server und der Beteiligung von Unterauftragnehmern gekennzeichnet ist, nicht ohne weiteres möglich, da ab einer bestimmten Anzahl von Unterauftragnehmern vor dem konkreten Datenverarbeitungsvorgang nicht festgestellt wer-

---

195 *Pohle/ Ammann,* K&R 2009, 625 (640); *Bedner,* Cloud Computing, S. 167.

196 *Artikel-29-Datenschutzgruppe,* Stellungnahme 05/2010 zum Cloud Computing, S. 19, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf, Stand: 7.6.2014

197 *Laue/ Stiemerling,* DuD 2010, 692 (695); *Schröder/ Haag,* ZD 2012, 362 (364).

198 *Bedner,* Cloud Computing, S. 167.

199 *Ernestus,* in: Simitis (Hrsg.), BDSG 2011, § 9 Rn. 119; *Reindl,* in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 450.

den kann, wann und wohin Daten übermittelt werden.[200] Um die Übermittlungen zu beherrschen, wird in Bezug auf Cloud Computing die Protokollierung vorgeschlagen. Um aussagekräftig zu sein, muss diese auch die Unterauftragnehmer erfassen.[201]

Die Eingabekontrolle nach Nr. 5 der Anlage soll sicherstellen, dass im Nachhinein überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht worden sind. Dies soll die Nachprüfbarkeit eines Verarbeitungsvorgangs sicherstellen und durch Protokollierungen erreicht werden können.[202] Für das Cloud Computing ergeben sich aus dieser Kontrollanforderung keine Besonderheiten.

Die Auftragskontrolle nach Nr. 6 der Anlage betrifft den Bereich der Auftragsdatenverarbeitung und ergänzt die Regelungen in § 11 BDSG.[203] Danach hat der Aufragnehmer zu gewährleisten, dass die im Auftrag zu verarbeitenden Daten nur nach den Weisungen des Auftragsgebers verarbeitet werden. Die Auftragskontrolle verpflichtet zunächst den Auftragnehmer, jedoch mittelbar auch den Auftraggeber, der klare und widerspruchsfreie Weisungen zu erteilen hat, damit der Auftragnehmer seiner Verpflichtung nachkommen kann und für die Befolgung der Weisungen Maßnahmen treffen kann.[204] Wie bereits erläutert, sind die meisten derzeit am Markt befindlichen Cloudservices standardisiert und bieten den Cloudnutzern wenig bis gar keinen Spielraum, um eigene Weisungsbefugnisse durchsetzen zu können, sodass die Auftragskontrolle nur eingeschränkt stattfinden kann.

Die Verfügbarkeitskontrolle nach Nr.7 der Anlage hat den Schutz vor zufälliger Zerstörung und Verlust, beispielsweise in Folge von Brän-

---

200 *Conrad/ Hausen,* in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 2 Rn. 310.

201 *Bedner,* Cloud Computing, S. 169.

202 *Gola/ Schomerus, (Hrsg.),* BDSG, § 9 Rn. 26; *Laue/ Stiemerling,* DuD 2010, 692 (695).

203 *Roth,* ITRB 2010, 60 (62).

204 *Gola/ Schomerus, (Hrsg.),* BDSG, § 9 Rn. 27; *Ernestus,* in: Simitis (Hrsg.), BDSG 2011, § 9 Rn. 147; *Roth,* ITRB 2010, 60 (62).

den, Wasserschäden oder Stromausfällen, zum Ziel. Beispiele für Sicherungsmaßnahmen sind die Auslagerung von Sicherungskopien, die Bereitstellung von Notstromaggregaten und einer unterbrechungsfreien Stromversorgung.[205] Diese Maßnahmen gelten für das Cloud Computing ebenso, wobei aufgrund der Daten und ihrer Bedeutung für die unterschiedlichen Kunden höhere Anforderungen an die Sicherungsmaßnahmen verlangt werden wie beispielsweise das Vorhalten von Daten an einem zweiten gespiegelten Rechenzentrum an einem anderen Ort.[206]

Das Trennungsgebot aus Nr. 8 der Anlage soll sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten auch getrennt voneinander verarbeitet werden können. Es verlangt keine räumliche Trennung in der Art, dass Daten in gesonderten Systemen oder Datenträgern gespeichert werden müssen,[207] vielmehr kann die Trennung auch logisch erfolgen.[208] Beim Cloud Computing findet die Trennung aufgrund der Mehrmandantenfähigkeit sowohl physisch als auch virtuell statt, indem Hypervisoren unterschiedliche virtuelle Maschinen bereitstellen und voneinander abschotten. Die Virtualisierungstechnik gilt als derart ausgereift, dass das Trennungsgebot im Regelfall als erfüllt angesehen werden kann.[209]

4.2.4 Anforderungen an die Unterauftragsverarbeitung in Fall A

§ 11 Abs. 2 S. 2 Nr. 6 BDSG behandelt im Rahmen der Auftragsdatenverarbeitung die Berechtigung zur Begründung von Unterauftragsverhältnissen auf Seiten des Auftragnehmers. Diese Rechtsnorm besagt, dass die Einschaltung von Unterauftragnehmern der Zustimmung des Auftraggebers bedarf. Dadurch soll verhindert werden,

---

205 *Gola/ Schomerus, (Hrsg.),* BDSG, § 9 Rn. 28; *Ernestus,* in: Simitis (Hrsg.), BDSG 2011, § 9 Rn. 159.

206 *Bedner,* Cloud Computing, S. 171 f.

207 *Gola/ Schomerus, (Hrsg.),* BDSG, § 9 Rn. 29.

208 *Ernestus,* in: Simitis (Hrsg.), BDSG 2011, § 9 Rn. 161; *Roth,* ITRB 2010, 60 (63); *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 9 Rn. 55.

209 *Bedner,* Cloud Computing, S. 172.

dass das begründete Datenschutzniveau zwischen Auftraggeber und Auftragnehmer unterlaufen wird.[210]

Die Klärung der Unterauftragsverhältnisse ist im Rahmen des Cloud Computings von hoher Bedeutung, da es zu diesem Geschäftsmodell gehört, Unterauftragnehmer einzuschalten. Die Zulässigkeit der Unterbeauftragung gem. § 11 Abs. 2 S. 2 Nr. 6 BDSG regelt jedoch nur den Fall, in dem sowohl der Cloudanbieter als auch die Unterauftragnehmer mit ihren Rechenzentren in einem EU-Staat ansässig sind, da nach dem Bundesdatenschutzgesetz eine privilegierte Auftragsdatenverarbeitung gem. § 11 BDSG nur innerhalb der EU stattfinden kann.[211] Sollen Unterauftragnehmer aus einem Drittstaat eingebunden werden, verhält sich die Vergabe von Unterauftragsverhältnissen schwieriger, da sie nicht auf Basis des § 11 BDSG vorgenommen werden kann und bei den dafür zur Verfügung stehenden Instrumenten danach zu differenzieren ist, wo sich der vorgeschaltete Cloudanbieter und seine Rechenzentren befinden. Auf diese Fallgruppen soll an späterer Stelle eingegangen werden.[212]

Im Fall A, in dem sich sowohl der Cloudanbieter als auch die nachgeschalteten Unterauftragnehmer mit ihren Rechenzentren in EU-Staaten befinden, verlangt der Wortlaut des § 11 Abs. 2 S. 2 Nr. 6 BDSG, dass nur die Frage der grundsätzlichen Berechtigung zur Begründung von Unterauftragsverhältnissen zu regeln ist, nicht jedoch dass der einzelne Unterauftragnehmer näher spezifiziert werden braucht, sodass im Voraus nur das Ob und das Wie einer Unterbeauftragung festzulegen sind.[213] Da auch beim Einsatz von Unterauftragnehmern, die datenschutzrechtliche Verantwortung gegenüber dem Betroffenen beim Auftraggeber verbleibt,[214] ist es für diesen sinnvoll, sich einen Zu-

---

210 *Walz,* in: Simitis (Hrsg.), BDSG 2006, § 11 Rn. 52.

211 *Kahler,* RDV 2012 167 (167 f.); *Reindl,* in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 445.

212 Vgl. Kapitel 5.5.

213 *Gabel,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 11 Rn. 47; *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 105; *Gola/ Schomerus (Hrsg.),* BDSG, § 11 Rn. 18e.

214 *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 106.

stimmungsvorbehalt vor der Inanspruchnahme eines konkreten Unterauftragnehmers zusichern zu lassen, um diesen überprüfen und gegebenenfalls ablehnen zu können.[215] In jedem Fall sollte der Cloudnutzer im eigenen Interesse, den Cloudanbieter bei der Auswahl der Unterauftragnehmer nicht frei gewähren lassen und sich nicht darauf einlassen, dass der Cloudanbieter nicht näher spezifizierte Unterauftragnehmer beispielsweise dann einschalten kann, wenn seine eigenen Server ausgelastet sind.[216] Jedoch dürfte es der Cloudnutzer in der Praxis schwer haben, einen generellen Zustimmungsvorbehalt gegenüber großen Anbietern von Public Clouds durchzusetzen, da diese Anbieter dann nur zur Einschaltung von Unterauftragnehmern befugt wären, nachdem alle Cloudnutzer den Unterauftragnehmern zugestimmt hätten, schließlich ist es dem Prinzip der Public Clouds immanent, dass sich die Nutzer die physischen Ressourcen teilen.[217]

In der Literatur wird daher die Klassifizierung und Kategorisierung von Unterauftragnehmern vorgeschlagen. So sollen bestimmte Kategorien von Unterauftragnehmern unter Zustimmungsvorbehalt gestellt werden, während bei anderen Kategorien auf einen Zustimmungsvorbehalt verzichtet wird oder sie generell genehmigt werden können, wenn der Unterauftragnehmer bestimmte vertraglich vereinbarte Voraussetzungen erfüllt.[218] In jedem Fall darf der Cloudnutzer über die Einsetzung von Unterauftragnehmern nicht im Unklaren gelassen werden. Zur Förderung der Transparenz wird vorgeschlagen, dass der Cloudanbieter eine online zugängliche Liste von Unterauftragnehmern mit Namen und Kurzbeschreibung ihres Beitrags zur Erbringung des Cloudservices führen könne, auf die der Cloudnutzer

---

215 *Bedner,* Cloud Computing, S. 142.

216 *Söbbing,* ITRB 2010, 36 (38).

217 *Eckhardt,* in: Köhler/ Schute (Hrsg.), Cloud Computing, S. 188; *Bedner,* Cloud Computing, S. 142.

218 *Eckhardt,* Information Management und Consulting, 4/2010, 55 (60); *EuroCloud Deutschland_eco e.V.,* Leitfaden Cloud Computing, S. 16, abrufbar unter: http://www.cloudmacher.de/index.php/download_file/224/99/., Stand: 7.6.2014

zugreifen kann und über deren Änderung er per E-Mail informiert wird.[219]

Sicherlich schränkt ein derartiges Vorgehen die Flexibilität des Cloudanbieters ein, da die Erbringung der Cloudservices nur unter der Zuhilfenahme von Unterauftragnehmern erfolgen kann, die der Cloudnutzer in welcher Weise auch immer abgesegnet hat. Jedoch kann davon ausgegangen werden, dass es ein seriöser Cloudanbieter nachvollziehen können wird, wenn ihm der Cloudnutzer aufgrund seiner datenschutzrechtlichen Verantwortung nicht völlig freie Hand bei der Auswahl der Unterauftragnehmer lässt, auch wenn es im Interesse des Cloudanbieters selbst sein dürfte, nur seriöse Unterauftragnehmer einzusetzen, weil auch er an einer reibungslosen Leistungserbringung interessiert ist und es seinem Ruf schadet, wenn bekannt wird, dass es im schlimmsten Fall zu einem Datenverlust gekommen ist, weil der Cloudanbieter eigenmächtig dubiose Unterauftragnehmer eingesetzt hat.

Im Ergebnis muss sichergestellt werden, dass die Einschaltung von Unterauftragnehmern nicht zu einer Herabsetzung des Datenschutzniveaus führt, weshalb zu gewährleisten ist, dass auch der Unterauftragnehmer alle Bestimmungen einhält, die zwischen dem Cloudnutzer und dem Cloudanbieter vereinbart worden sind. Auch für Unterauftragnehmer gelten daher die Weisungsgebundenheit und die Pflicht zur Einhaltung derselben Datensicherheitsstandards, die auch für den Cloudanbieter gelten.[220] Wie bereits geschildert, ist es aufgrund der häufig in standardisierter Form angebotenen Cloudservices, für den Cloudnutzer schwer, Weisungen gegenüber dem Cloudanbieter selbst durchzusetzen. Die Weisungserteilung an einen Unterauftragnehmer gestaltet sich noch schwieriger, da zwischen beiden, außer im Fall eines Vertrags zu Gunsten des Cloudnutzers, keine Vertragsbeziehung besteht und der Cloudnutzer nur Weisungen gegenüber dem Cloudanbieter und nicht auch gegenüber dem Unterauftragneh-

---

219 *EuroCloud Deutschland_eco e.V.*, Leitfaden Cloud Computing, S. 16.

220 *Niemann/ Hennrich,* CR 2010, 686 (691).

mer erteilen kann, sodass dem Cloudanbieter die Aufgabe zukommt, die Weisungen des Cloudnutzers gegenüber dem Unterauftragnehmer weiterzugeben und ihre Einhaltung sicherzustellen.[221] Dieses Problem stellt sich für den Cloudnutzer auch bei der Ausübung von Kontrollrechten gegenüber den Unterauftragnehmern.

4.2.5 Zwischenfazit zur Auftragsdatenverarbeitung

Zusammenfassend lässt sich festhalten, dass das Auftragsdatenverarbeitungsprivileg zwar grundsätzlich in Frage kommt, jedoch der Cloudnutzer im Regelfall die umfangreichen gesetzlichen Vorgaben in §§ 9, 11 Abs. 2 BDSG i.V.m. Anlage 1 zu § 9 BDSG beim Cloudanbieter und dessen Unterauftragnehmern nicht selbst erfüllen können wird. Dies liegt vordergründig daran, dass die Regelungen der Auftragsdatenverarbeitung auf klassische IT-Outsourcing-Projekte mit langen Vertragsdauern und großen wirtschaftlichen Volumen ausgelegt sind und nicht auf neue Formen der Datenverarbeitung wie dem Cloud Computing, wo externe oftmals standardisierte Dienstleistungen auch kurzfristig oder in geringem Umfang nachgefragt werden.[222] Da die Nutzung von Cloudservices mit minimalem Managementaufwand realisierbar sein soll, erscheinen die Anforderungen an einen Auftragsdatenverarbeitungsvertrag, insbesondere hinsichtlich der Auswahl- und Kontrollpflichten als unpassend. Mittelfristig wäre es wünschenswert, wenn die Regelungen zur Auftragsdatenverarbeitung derart reformiert werden würden, dass das materielle Datenschutzniveau zwar nicht abgesenkt würde, sich die gesetzlichen Anforderungen jedoch auch bei modernen Formen der Datenverarbeitung wie dem Cloud Computing einfacher realisieren ließen.[223] Solange eine derartige Reform jedoch nicht vollzogen worden ist, muss den derzeit geltenden gesetzlichen Anforderungen entsprochen werden. Eine

---

221 *Plath,* in: ders. (Hrsg.), BDSG Kommentar, § 11 Rn. 106; *Bierekoven,* in: Bartsch/ Briner (Hrsg.), DGRI Jahrbuch 2010, S. 113.

222 *Trusted Cloud,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 6 f., abrufbar unter: http://www.trusted-cloud.de/documents/Datenschutzrechtliche-Loesungen-fuer-Cloud-Computing.pdf, Stand: 7.6.2014; *Bergt,* DuD 2013, 796 (799).

223 *Trusted Cloud,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 8.

Möglichkeit, um den Anforderungen hinsichtlich der Auswahl- und Kontrollpflichten entsprechen zu können, besteht darin, dass sich die Cloudanbieter und Unterauftragnehmer durch unabhängige Stellen auditieren und zertifizieren lassen.

In der Praxis sind viele Cloudanbieter zertifiziert, auch weil eine Zertifizierung für das Vertrauen der Nutzer in die Geschäftstätigkeit des Anbieters förderlich ist. Google verfügt beispielsweise über eine ISO 27001-Zertizierung für seinen Cloudservice Google Apps.[224] Auch die Cloudservices von Amazon und Microsoft sind ISO 27001-zertifiziert.[225] Diese Zertifizierung betrifft die IT-Sicherheit und wird auf Basis eines Audit-Reports von BSI-zertifizierten Auditoren durchgeführt. Das Zertifikat besagt jedoch nicht, dass die Datenverarbeitung datenschutzkonform im Sinne des § 9 BDSG abläuft, da es zwar viele Anforderungen des § 9 BDSG bezüglich der Datensicherheit abdeckt, jedoch nicht alle datenschutzrechtlich relevanten Aspekte wie beispielsweise das Trennungsgebot, die Auftragskontrolle oder die Eingabekontrolle erfasst.[226] Ebenfalls wird nicht geprüft, ob Regelungen bestehen, wie mit den Daten am Ende des Vertragsverhältnisses umgegangen wird,[227] sodass dieses Zertifikat hinsichtlich der Einhaltung des Datenschutzes wenig Aussagekraft besitzt.

Mit der Zertifizierung EuroCloud Star Audit SaaS haben Cloudanbieter, die SaaS-Services anbieten, die Möglichkeit sich auf Basis der ver-

---

224 *Ihlenfeld,* Google erhält ISO-27001-Zertifizierung für Google Apps, abrufbar unter: http://www.golem.de/news/cloud-computing-google-erhaelt-iso-27001-zertifizierung-fuer-google-apps-1205-92099.html, Stand: 7.6.2014

225 *Microsoft,* Datenschutz und Datensicherheit in der Microsoft Cloud, abrufbar unter: http://www.microsoft.com/de-de/kmu/Themen/Seiten/datensicherheit-datenschutz-cloud-rainer-stropek.aspx, Stand: 7.6.2014; *Amazon,* AWS-Sicherheits- und Compliance-Zentrum, abrufbar unter: http://aws.amazon.com/de/security/, Stand: 7.6.2014

226 *Gerlach,* Zertifizierungen für Cloud-Computing-Systeme und SaaS: Datenschutz und Compliance, abrufbar unter: http://www.it-rechts-praxis.de/meldungen/Zertifizierungen-fuer-Cloud-Computing-Systeme-und-SaaS-Datenschutz-und-Compliance-186, Stand: 7.6.2014

227 *Financial Times Deutschland,* Cloud-Zertifikate als Entscheidungshilfe, abrufbar unter: http://www.ftd.de/it-medien/:guetesiegel-cloud-zertifikate-als-entscheidungshilfe/70105762.html, Stand: 7.6.2014

traglichen Regelungen mit dem jeweiligen Cloudnutzer zertifizieren zu lassen.[228] Die Zertifizierung umfasst unterschiedliche Kategorien und es werden auch Datenschutzbestimmungen und Vertragsinhalte bezüglich der Auftragsdatenverarbeitung geprüft, die mit maximal 5 Sternen bewertet werden.[229] Die Zertifizierung selbst wird mit den Mitteln eines detaillierten Fragebogens, der Vorlage von Nachweisen, Vor-Ort-Audits und Rechenzentrumsbesichtigungen durchgeführt und bezieht auch die an der Serviceerbringung beteiligten Unterauftragnehmer mit ein.[230] Bisher haben sich nur wenige SaaS-Anbieter derart zertifizieren lassen, was wohl auch daran liegt, dass das Zertifikat vergleichsweise neu am Markt ist.[231] Die Zukunft wird zeigen, ob sich das EuroCloud Star Audit SaaS in der Praxis etablieren können wird. Positiv ist in jedem Fall, dass überhaupt ein Zertifikat entwickelt worden ist, das sich mit den cloudspezifischen Herausforderungen auseinander setzt und diese bewertet. Seit 2011 gibt es das EuroCloud Star Audit auch für die Cloudservices IaaS und PaaS.[232] Positiv am EuroCloud Star Audit ist ebenfalls, dass verschiedene Prüftiefen gewählt werden können. Dies macht Sinn, da die Anforderungen im Einzelfall an das jeweilige Schutzerfordernis der Daten angepasst werden können und sich die unterschiedlichen Prüftiefen auch bei den Kosten der Zertifizierung bemerkbar machen dürften, was für Kunden, die nur eine geringe Prüftiefe benötigen, einen Vorteil darstellt.

Insgesamt ist die Einführung und Fortentwicklung von cloudspezifischen Zertifikaten zu begrüßen, weil Zertifikate zum einen den Cloudnutzern die Erfüllung der gesetzlichen Anforderungen an die Auftragsdatenverarbeitung ermöglichen oder zumindest erleichtern

---

228 *Giebichenstein/ Weiss,* DuD 2011, 338 (339).

229 *EuroCloud Deutschland_eco e.V.,* Das Gütesiegel für die Cloud: EuroCloud Star Audit SaaS, abrufbar unter: http://www.saas-audit.de/files/2011/01/EuroCloud-Star-Audit-SaaS-PK-.pdf, Stand: 7.6.2014; *Giebichenstein,* BB 2011, 2218 (2223).

230 *Giebichenstein/ Weiss,* DuD 2011, 338 (339).

231 *Financial Times Deutschland,* Cloud-Zertifikate als Entscheidungshilfe, abrufbar unter: http://www.ftd.de/it-medien/:guetesiegel-cloud-zertifikate-als-entscheidungshilfe/70105762.html, Stand: 7.6.2014

232 *Weiss,* DuD 2014, 170 (173).

und dadurch möglicherweise zu einer höheren Nachfrage nach Cloudservices führen. Zum anderen werden auch die Cloudanbieter nicht stärker belastet, da sie aus Gründen der Effizienz ohnehin ein einheitliches Schutzniveau anstreben[233] und eine Vor-Ort-Prüfung der Rechenzentren durch unabhängige Prüfer zum Zwecke einer Zertifizierung sicherlich eher in ihrem Interesse sein dürfte als eine durch verschiedene Cloudnutzer im Einzelnen. Wie in der Literatur vorgeschlagen,[234] wäre es für die Zukunft sicherlich von Vorteil, wenn die Prüfkriterien für die Erteilung von Zertifikaten auf gesetzlicher Grundlage zumindest europaweit einheitlich festgesetzt werden würden, damit nicht jede zertifizierende Stelle eigene Prüfkriterien entwickelt und der Cloudnutzer den Überblick verliert, weil sich am Markt eine Vielzahl an Zertifizierungsanbietern mit unterschiedlichen Prüfkriterien befinden und der Cloudnutzer gar nicht abschätzen kann, welchen er auswählen soll, um seinen gesetzlichen Pflichten nachzukommen. Um zu verhindern, dass dem Zertifizierungsanbieter selbst die fachliche und persönliche Eignung zur Zertifikatserteilung fehlt, sollte er einer gesetzlich vorgeschriebenen Überprüfung unterzogen werden. Die Anforderungen an eine solche Akkreditierung des Zertifizierungsanbieters sollten auf europäischer Ebene einheitlich sein.[235] Wie beim EuroCloud Star Audit SaaS bereits umgesetzt, sollten die Zertifikate der Zukunft unterschiedliche Prüftiefen und -weiten bieten, da der Bedarf der Kunden unterschiedlich ausfallen dürfte. Sind solche Zertifizierungen am Markt verfügbar, kann auch über die Entwicklung spezifischer Zertifikate wie beispielsweise für die Auslagerung der Verarbeitung von Gesundheitsdaten in die Cloud nachgedacht werden, die in der Literatur ebenfalls gefordert werden.[236] Inzwischen hat auch die EU-Kommission den Nutzen von Zertifizierungen im Rahmen des Cloud Computings erkannt und möchte die Entwicklung EU-weiter freiwilliger Zertifizierungsprogramme im Bereich

233 *Trusted Cloud,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 14.
234 *Trusted Cloud,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 15.
235 *Trusted Cloud,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 15.
236 *Trusted Cloud,* Datenschutzrechtliche Lösungen für Cloud Computing, S. 14.

des Cloud Computings unterstützen.[237] Das Ergebnis dieser Unterstützung bleibt abzuwarten.

[237] *Europäische Kommission,* Freisetzung des Cloud-Computing-Potentials in Europa, S. 12.

5 Zulässigkeit der Datenübermittlung ins außereuropäische Ausland

Wie schon mehrfach erwähnt, ist es im Rahmen des Cloud Computings typisch, dass sich die Server der Cloudanbieter und der Unterauftragnehmer an unterschiedlichen Standorten in der Welt befinden und die Daten der Nutzer hin und her geschoben werden, um die Flexibilität der Angebote voll ausnutzen zu können.[238]

Grundsätzlich können auch internationale cloudbasierte Datentransfers auf einem Auftragsverhältnis beruhen, jedoch schließt das Bundesdatenschutzgesetz für Deutschland die Möglichkeit der Auftragsdatenverarbeitung in außereuropäischen Staaten, sogenannten Drittstaaten, aus.[239] Die privilegierende Wirkung des § 11 BDSG greift nur, wenn der internationale Datentransfer gem. § 3 Abs. 8 S. 3 BDSG eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag durch Stellen in EU-Staaten zum Gegenstand hat. Sind Stellen aus Drittstaaten involviert, handelt es sich somit um eine Auftragsdatenverarbeitung, die rechtlich als Übermittlung im Sinne des § 3 Abs. 4 Nr. 3 BDSG zu qualifizieren ist.[240]

Teilweise wird in der Literatur die Begrenzung der Auftragsdatenverarbeitung gem. § 11 BDSG auf EU-Staaten als europarechtswidrig empfunden und eine Gleichstellung zwischen sicheren Drittstaaten und EU-Staaten gefordert.[241] Begründet wird diese Ansicht mit den Erwägungen in den Adäquanzentscheidungen über die Angemessenheit von Datenschutzniveaus in Drittstaaten. Erwägungsgrund 4 der Adäquanzentscheidung für die Schweiz besagt, dass sicheren Drittstaaten nicht willkürlich oder ungerechtfertigt diskriminierend begegnet werden darf und die Übermittlung in solche Staaten gem. Erwä-

---

238 *Opfermann*, ZEuS 2012, 121 (139 f.).

239 *Kahler*, RDV 2012 167 (167 f.); *Reindl*, in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 445.

240 *Schmidt-Bens*, Cloud Computing, S. 42; *Kahler*, RDV 2012, 167 (167); *Grützmacher*, ITRB 2007, 183 (187).

241 *Erd*, DuD 2011, 275 (275 f.); *Giesen*, CR 2007, 543 (546).

gungsgrund 2 ohne zusätzliche Garantien erfolgen können muss.[242] Daraus wird geschlussfolgert, dass die Übermittlung personenbezogener Daten an Stellen in sicheren Drittstaaten unter denselben Voraussetzungen möglich sein muss wie an Stellen in der EU.[243] Andere Stimmen in der Literatur gehen im Fall der außereuropäischen Auftragsverarbeitung von einer planwidrigen Regelungslücke aus und sprechen sich daher für eine analoge Anwendung der §§ 3 Abs. 8 S. 3, 11 BDSG aus.[244] Ihrer Meinung nach dürfe § 3 Abs. 8 S. 3 BDSG nicht als abschließende Regelung in Bezug auf die Auftragsdatenverarbeitung nach § 11 BDSG verstanden werden, da auch die EU-Datenschutz-Richtlinie den Begriff des Auftragsverarbeiters nicht auf den Geltungsbereich der Richtlinie begrenze, sondern vielmehr auch eine privilegierte außereuropäische Auftragsdatenverarbeitung vorsehe, wenn der Drittstaat sicher sei oder ausreichende Garantien beispielsweise in Form von Vertragsklauseln vereinbart würden.[245] Aus diesem Grund dürften außereuropäische Auftragsdatenverarbeiter auch nicht als Dritte im Sinne des Bundesdatenschutzgesetzes angesehen werden.[246] Die Gegenmeinung spricht sich gegen eine Ausweitung des Anwendungsbereichs von § 11 BDSG auf die außereuropäische Auftragsdatenverarbeitung aus und argumentiert, dass eine Ausweitung nicht mit der Systematik des Gesetzes vereinbar sei, da die Interessenlagen, die zu der Privilegierung des § 11 BDSG für den europäischen Bereich führten, nicht mit denen bei einer außereuropäischen Auftragsdatenverarbeitung vergleichbar seien. Weiterhin entspräche

---

242 *Europäische Kommission,* Entscheidung 2000/518/EG der Kommission vom 26. Juli 2000 gem. der RL 95/46/EG des Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, S. 1, abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0001:0003:DE:PDF, Stand: 7.6.2014

243 *Erd,* DuD 2011, 275 (276).

244 *Nielen/ Thum,* K&R 2006, 171 (174).

245 *Nielen/ Thum,* K&R 2006, 171 (174); *Räther,* DuD 2005, 461 (465); *BITKOM/ VOICE,* Empfehlungen für den Cloud Computing-Standort Deutschland, S. 12, abrufbar unter: http://www.bitkom.org/files/documents/cloud_computing_standort.pdf, Stand: 7.6.2014

246 *Nielen/ Thum,* K&R 2006, 171 (176).

eine Ausweitung nicht dem Willen des Gesetzgebers, da dieser im Rahmen der Reform des Bundesdatenschutzgesetzes im Jahr 2009 die Möglichkeit gehabt hätte, den Anwendungsbereich des § 11 BDSG auch auf die außereuropäische Auftragsdatenverarbeitung auszuweiten, dies jedoch nicht getan hätte.[247]

Sicherlich würde eine Ausweitung des § 11 BDSG auf die außereuropäische Auftragsdatenverarbeitung auch im Rahmen des Cloud Computings eine Erleichterung bedeuten, jedoch stellen die Regelungen im Bundesdatenschutzgesetz geltendes Recht dar, sodass die Definition des Dritten in § 3 Abs. 8 S. 3 BDSG nicht einfach übergangen werden darf. Dem Argument, dass die deutsche Regelung europarechtswidrig sei, kann entgegen gehalten werden, dass den Mitgliedsstaaten bei der Umsetzung von Richtlinien ein gewisser Umsetzungsspielraum zusteht und keine Fälle bekannt sind, in denen die geltende Rechtslage von europäischer Seite gerügt worden ist, sodass man davon ausgehen muss, dass die Privilegierung des § 11 BDSG nur für die innereuropäische Auftragsverarbeitung gilt und die Zulässigkeit jeder außereuropäischen Auftragsdatenverarbeitung im Sinne einer Übermittlung anhand der Vorgaben in §§ 4b, 4c BDSG zu prüfen ist.

Die Zulässigkeit einer Datenübermittlung in Drittstaaten erfolgt im Rahmen einer zweistufigen Prüfung. Auf der ersten Stufe ist zu prüfen, ob die Datenübermittlung nach den allgemeinen Grundsätzen des Bundesdatenschutzgesetzes zulässig ist. Diese ist gem. § 4 Abs. 1 BDSG zulässig, wenn eine Rechtsvorschrift es erlaubt oder eine Einwilligung des Betroffenen vorliegt.[248] Wie in Kapitel 4.1. geschildert, ist die Einwilligung schon bei der innereuropäischen cloudbasierten Datenverarbeitung keine praktikable Legitimationsgrundlage, sodass sie bei der internationalen cloudbasierten Datenverarbeitung erst recht als nicht praktikabel angesehen werden kann und daher auch nicht weiter betrachtet wird. Somit kommen als Erlaubnisnormen grundsätzlich die Regelungen des § 28 BDSG in Betracht, die

247 *Wybitul/ Patzak,* RDV 2011, 11 (17).
248 *Wybitul/ Patzak,* RDV 2011, 11 (12).

auf der ersten Stufe zu prüfen sind. Auf der zweiten Stufe sind die in §§ 4b und 4c BDSG verankerten Vorgaben zu prüfen.[249]

5.1 Zulässigkeitsprüfung auf der ersten Stufe

§ 28 Abs. 1 S. 1 BDSG behandelt die Verwendung von Daten für eigene Geschäftszwecke. Gemeint sind damit Datenverarbeitungen, die als Hilfsmittel zur Erfüllung bestimmter anderer Zwecke der datenverarbeitenden Stelle erfolgen. Die Datenverarbeitung selbst bildet demnach nicht das geschäftliche Interesse, sondern dient nur als Mittel zum Zweck.[250] Man kann davon ausgehen, dass die Übertragung von Daten in die Cloud in den meisten Fällen unter § 28 Abs. 1 S. 1 BDSG fallen dürfte und demnach als eigener Geschäftszweck angesehen werden kann.[251] So geht es dem Cloudnutzer beispielsweise bei der Nutzung von IaaS nicht darum, dass seine Daten beim Cloudanbieter gespeichert werden, sondern darum, dass er selbst keine großen Datenspeicher betreiben muss und dadurch Kosten einsparen kann.

Gemäß § 28 Abs. 1 S. 1 BDSG kann eine Übermittlung personenbezogener Daten zu eigenen Geschäftszwecken zulässig sein, wenn dies zur Erfüllung eines Schuldverhältnisses zwischen der übermittelnden Stelle, demnach dem Cloudnutzer und dem Betroffenen erforderlich ist (Nr. 1), die Daten allgemein zugänglich sind (Nr. 3) oder eine Übermittlung der Daten nicht dem schutzwürdigen Interesse des Betroffenen entgegensteht (Nr. 2).

Gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG kann eine Übermittlung personenbezogener Daten zu eigenen Geschäftszwecken zulässig sein, wenn dies zur Erfüllung eines Schuldverhältnisses zwischen dem Cloudnutzer und dem Betroffenen erforderlich ist. In der Regel sind jedoch keine unmittelbaren vertraglichen Regelungen zwischen dem Cloudnutzer und dem Betroffenem hinsichtlich der Übermittlung personenbezogener Daten des Betroffenen in eine Cloud getroffen worden, sodass die-

249 *Wybitul/ Patzak,* RDV 2011, 11 (13); *Grützmacher,* ITRB 2007, 183 (187).
250 *Gola/ Schomerus (Hrsg.),* BDSG, § 28 Rn. 4.
251 *Opfermann,* ZEuS 2012, 121 (138).

se Erlaubnisnorm ausscheidet.[252] Ebenso werden die personenbezogenen Daten, die übermittelt werden sollen nicht allgemein zugänglich sein wie es § 28 Abs. 1 S. 1 Nr. 3 BDSG vorsieht, sodass meist nur § 28 Abs. 1 S. 1 Nr. 2 BDSG als Erlaubnisnorm in Frage kommen wird.

§ 28 Abs. 1 S. 1 Nr. 2 BDSG gestattet die Datenübermittlung, wenn diese zur Wahrung berechtigter Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdigen Interessen der Betroffenen am Ausschluss der Übermittlung bestehen und diese das Übermittlungsinteresse überwiegen. Die Auslegung der „Erforderlichkeit" besteht aus einer datenschutzrechtlichen Verhältnismäßigkeitsprüfung, nach der die Übermittlung dann erlaubt ist, wenn sie zur Verwirklichung eines berechtigten Interesses des Unternehmens geeignet, erforderlich und angemessen ist.[253] Zunächst muss die Übermittlung geeignet sein, um das berechtigte Interesse erfüllen zu können. Dieses kann jedes von der Rechtsordnung gebilligte Interesse sein und demnach auch rein wirtschaftliche Ziele verfolgen.[254] Der Hauptgrund Cloudservices zu nutzen, liegt in der Einsparung von Kosten, jedoch ist die Kosteneinsparung nicht der einzige Grund, denn Cloudservices können für den Cloudnutzer auch ein Mittel sein, um die Wettbewerbsfähigkeit zu stärken,[255] die Flexibilität der Datenverfügbarkeit zu steigern oder auch eine Möglichkeit, nicht in neue Technik investieren zu müssen.[256] Die Geeignetheit kann damit als erfüllt angesehen werden.

Die Datenübermittlung muss jedoch auch erforderlich sein, um den angestrebten Zweck zu erreichen. Der zur Wahrung berechtigter Interessen des Unternehmens dienende Zweck darf nicht durch ein milderes Mittel ebenso gut verwirklicht werden können.[257] An der Erforder-

---

252 *Weichert,* DuD 2010, 679 (683); *Bedner,* Cloud Computing, S. 236; *Opfermann,* ZEuS 2012, 121 (138).
253 *Wybitul/ Patzak,* RDV 2011, 11 (12).
254 *Gola/ Schomerus, (Hrsg.),* BDSG, § 28 Rn. 24; *Nielen/ Thum,* K&R 2006, 171 (173).
255 *Niemann/ Paul,* K&R 2009, 444 (449).
256 *Gaul/ Koehler,* BB 2011, 2229 (2232).
257 *Wybitul/ Patzak,* RDV 2011, 11 (13).

lichkeit fehlt es beispielsweise dann, wenn auch die Übermittlung anonymisierter und pseudonymisierter Daten ausreichen würde,[258] was im Falle des Cloud Computings meist jedoch nicht der Fall sein dürfte, da es im Moment, wie bereits geschildert, keine marktfähige Verschlüsselungsmethode gibt, die eine Verarbeitung verschlüsselter Daten in der Cloud ermöglicht. Bei der Datenübermittlung an internationale Clouds wird es meist an der Erforderlichkeit mangeln, da zunehmend auch rein europäische Cloudservices angeboten werden. Diese werden die meisten Bedürfnisse der Cloudnutzer befriedigen können, sodass es nicht zwingend erforderlich ist, Cloudservices außerhalb von EU-Staaten zu nutzen, denn die Tatsache allein, dass internationale Cloudservices kostengünstiger sind, soll für die Erforderlichkeit der Datenübermittlung in einen Drittstaat nicht genügen.[259] Allenfalls in den Fällen, in denen es keine adäquaten europäischen Clouds am Markt gibt, kann von einer Erforderlichkeit zur Wahrung berechtigter Interessen ausgegangen werden.[260] In den Fällen, in denen von einer Erforderlichkeit ausgegangen werden kann, ist weiter zu prüfen, ob die Übermittlung nicht deshalb zu unterbleiben hat, weil ein Grund zu der Annahme besteht, dass die schutzwürdigen Interessen des Betroffen an einer Übermittlung in eine internationale Cloud überwiegen. In diesem Fall hat gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG eine Abwägung zwischen den wirtschaftlichen Interessen des Cloudnutzers und den Persönlichkeitsrechten der Betroffenen, im Falle des Cloud Computings beispielsweise die der Arbeitnehmer und Kunden, stattzufinden. Der Cloudnutzer muss eine hypothetische Prüfung vornehmen und dabei objektiv entscheiden, ob er die Datenübermittlung vornimmt oder ob er die Persönlichkeitsrechte der Betroffenen als überwiegend einstuft.[261]

---

258 *Taeger,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 28 Rn. 59.

259 *Weichert,* DuD 2010, 679 (683).

260 *Bedner,* Cloud Computing, S. 236.

261 *Wybitul/ Patzak,* RDV 2011, 11 (13); *Taeger,* in: Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, § 28 Rn. 62 ff.

Zugunsten des Betroffenen ist anzuführen, dass dieser meist keine Kenntnis über Art und Umfang der Inanspruchnahme der Cloudservices durch den Cloudnutzer hat und auch nicht weiß, ob der Cloudanbieter und seine Unterauftragnehmer vertrauenswürdig sind, sodass davon ausgegangen werden kann, dass die schutzwürdigen Interessen des Betroffenen einer Datenübermittlung an einen Cloudanbieter grundsätzlich entgegenstehen.[262] Im Ergebnis wird die Datenübermittlung an internationale Clouds in den meisten Fällen somit unzulässig sein.[263] Ein seltener Fall von Zulässigkeit kann angenommen werden, wenn es keine adäquaten europäischen Clouds am Markt gibt und den berechtigten Interessen des Cloudnutzers an der Datenübermittlung der Vorzug gegeben werden kann, wobei es hierbei immer auf den Einzelfall ankommt. Teilweise wird die Auslagerung in eine Cloud auch im Sinne des § 28 Abs. 1 S. 1. Nr. 2 BDSG als gerechtfertigt angesehen, wenn der Cloudanbieter in ähnlicher Weise vertraglich verpflichtet ist wie im Rahmen des § 11 BDSG und dieser Rechtsnorm gleichwertige Sicherheitsmaßnahmen trifft.[264] Die nachfolgenden Ausführungen zur Angemessenheit des Datenschutzniveaus und den Ausnahmen gem. § 4c BDSG sind nur zu prüfen, wenn die bisher genannten Voraussetzungen erfüllt worden sind.

5.2 Zulässigkeitsprüfung auf der zweiten Stufe

Internationale Datenübermittlungen sind gem. § 4b Abs. 2 S. 2 BDSG grundsätzlich verboten, wenn der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Das schutzwürdige Interesse des Betroffenen gem. § 4b Abs. 2 S. 2 BDSG wird insbesondere dann als nicht gewahrt angesehen, wenn kein angemessenes Datenschutzniveau beim Datenempfänger gewährleistet ist.

Das Datenschutzniveau gilt als angemessen, wenn es dem in Deutschland geltenden Datenschutzrecht entspricht und der Betroffene durch

---

262 *Schmidt-Bens*, Cloud Computing, S. 41.

263 *Redeker*, IT-Recht, Rn. 957; *Weichert*, DuD 2010, 679 (686).

264 *Conrad/ Hausen*, in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 2 Rn. 317.

die Übermittlung seiner personenbezogenen Daten in den Drittstaat keine Nachteile hinsichtlich seiner Datenschutzposition zu befürchten hat. Das Datenschutzniveau beim Datenempfänger muss dem deutschen Datenschutzrecht jedoch nicht gleichwertig sein.[265] Vielmehr wird es dann als angemessen und ausreichend angesehen, wenn die schutzwürdigen Interessen des Betroffenen bei der Verarbeitung seiner personenbezogenen Daten durch Normen geschützt sind, die im Wesentlichen dem Kernbestand der Schutzprinzipien der EU-Datenschutz-Richtlinie entsprechen. Als zulässig werden Abstriche bei einzelnen Schutzinstrumenten sowie Minderungen des Schutzniveaus im Ganzen akzeptiert, ohne dass gleich von einem unangemessenen Datenschutzniveau ausgegangen wird.[266]

Die Feststellung, ob ein angemessenes Datenschutzniveau vorliegt, liegt meist in der Verantwortung der übermittelnden Stelle, wobei in den überwiegenden Fällen die Konsultation einer Aufsichtsbehörde nötig sein dürfte, weil die Prüfung häufig sehr umfangreich ausfällt. Für die Ermittlung, ob ein angemessenes Datenschutzniveau vorliegt, sind insbesondere die Datenschutzvorschriften des Drittstaates heranzuziehen, sowie die Maßnahmen, mit denen diese Vorschriften durchgesetzt werden können.[267] Gemäß Art. 25 Abs. 2 EU-DSRL und § 4b Abs. 3 BDSG werden bei der Bestimmung der Angemessenheit des Schutzniveaus alle Umstände beurteilt, die bei einer Datenübermittlung Bedeutung haben.[268] Zur Bestimmung des Datenschutzniveaus können gem. § 4b Abs. 3 BDSG insbesondere die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den Datenempfänger geltenden Rechtsnormen, sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden. Die Gefährdung der Interessen des Betroffenen fällt umso größer aus, je sensibler die Daten sind und je umfangreicher der Zweck ist, für den sie verar-

---

265 *Gola / Schomerus (Hrsg.),* BDSG, § 4b Rn. 12.
266 *Gola/ Schomerus,* BDSG, § 4b Rn. 12; *Simitis,* in: ders. (Hrsg.), BDSG 2011, § 4b Rn. 52.
267 *Opfermann,* ZEuS 2012, 121 (142).
268 *Marnau/ Schlehahn,* DuD 2011, 311 (312).

beitet werden. Zudem ist die Gefahr möglicher Persönlichkeitsrechtsverletzungen größer, wenn die personenbezogenen Daten länger verarbeitet werden, die Daten mehrere Stellen durchlaufen und das Datenschutzrecht des Drittstaates wenige Durchsetzungsmechanismen bietet.[269]

5.2.1 Sichere Drittstaaten gem. Adäquanzentscheidung

Für einige Länder hat die EU-Kommission gem. Art. 25 Abs. 6 EU-DSRL durch eine Adäquanzentscheidung ein angemessenes Datenschutzniveau im Sinne des Art. 25 Abs. 2 DSRL festgestellt. Zu den Ländern mit angemessenem Datenschutzniveau zählen Andorra, Argentinien, Australien, Israel, Kanada für den nicht-öffentlichen Bereich, die Schweiz, die Färöer-Inseln, Guernsey, Isle of Man, Jersey, Neuseeland und das Safe-Harbor-System der USA.[270] Da eine Beurteilung des Datenschutzniveaus durch die EU-Kommission erfolgt ist, darf die verantwortliche Stelle in diesen Fällen keine eigene Beurteilung des Datenschutzniveaus mehr durchführen.[271] Es sei nochmals erwähnt, dass Stellen, die ihren Sitz in Ländern haben, denen die EU-Kommission gem. Art. 25 Abs. 6 DS-RL ein angemessenes Datenschutzniveau bescheinigt hat, dennoch als Dritte i.S.d. § 3 Abs. 8 S. 3 BDSG gelten.

5.2.2 Safe Harbor gelistete Unternehmen

Aus EU-Sicht werden die USA im Hinblick auf das dort herrschende Datenschutzniveau zum gegenwärtigen Zeitpunkt als unsicherer Drittstaat angesehen.[272] Die Gründe dafür liegen in einem fehlenden Normgefüge eines einheitlichen Datenschutzrechts, der Tatsache, dass Datenschutzgesetze von unterschiedlichen Stellen erlassen werden

---

269 *Opfermann*, ZEuS 2012, 121 (142).

270 *Europäische Kommission*, Pressemitteilung IP/12/1403 vom 19.12.2012, abrufbar unter: http://europa.eu/rapid/press-release_IP-12-1403_de.htm, Stand: 7.6.2014

271 *Busche*, in: Taeger/Wiebe (Hrsg.), Inside the cloud , S. 63.

272 *Deutlmoser/ Filip*, ZD-Beilage 6/2012, S. 9; *Spies*, MMR 2007, Heft 7, V (VI); *Wybitul/ Patzak*, RDV 2011, 11 (13); *Räther*, DuD 2005, 461 (463).

und dass auf freiwillige Selbstregulierungen der Wirtschaft gesetzt wird.[273]

Eine solche Selbstregulierungsmaßnahme stellt auch die Safe Harbor Zertifizierung für amerikanische Unternehmen dar. Am 26. Juli 2000 haben die EU-Kommission und das amerikanische Department of Commerce das Safe Harbor Abkommen geschlossen, um den Datentransfer zwischen der EU und den USA zu fördern und die Handelsbeziehungen zu stärken.[274] Das Resultat des Abkommens ist, dass amerikanischen Unternehmen ein angemessenes Datenschutzniveau bescheinigt wird, wenn sie sich den Safe Harbor Grundsätzen der amerikanischen Federal Trade Commission (FTC) unterstellen und sich verpflichten, diese einzuhalten.[275]

5.2.2.1 Grundsätze der Safe Harbor Zertifizierung

Den Kern der Safe Harbor Zertifizierung bilden die sieben Grundsätze, die im Folgenden kurz dargestellt werden sollen: Der Grundsatz der Informationspflicht verlangt, dass Betroffene vor der Erhebung ihrer Daten über den Zweck der Erhebung und Verwendung zu informieren sind und sie Kenntnis darüber verlangen können, an welche Kategorien von Dritten ihre Daten weitergegeben werden dürfen und welche Mittel ihnen zur Verfügung stehen, um die Verwendung und Weitergabe ihrer Daten einzuschränken.

Der Grundsatz der Wahlmöglichkeit sieht vor, dass dem Betroffenen bei der Erhebung, Verarbeitung und Übermittlung seiner personenbezogenen Daten die Möglichkeit eingeräumt werden muss, dieser zu

---

273 *Schmidt/ Bens,* Cloud Computing, S. 46; *Söbbing,* in: Leible/ Sosnitza (Hrsg.), Onlinerecht 2.0, S. 65.

274 *Europäische Kommission,* Entscheidung der Kommission vom 26. Juli 2000 gem. der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglich „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, S. 4, abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF, Stand: 7.6.2014

275 *Marnau/ Schlehahn,* DuD 2011, 311 (312).

widersprechen. Dies gilt auch für den Fall, in dem Daten für einen anderen als den ursprünglich vorgesehenen Fall genutzt werden sollen.

Der dritte Grundsatz der Weitergabe sieht vor, dass eine Datenübermittlung an Dritte nur unter Wahrung des ersten und zweiten Grundsatzes erfolgen darf. Bei Datenübermittlungen an Dritte, die im Auftrag und auf Weisung der übermittelnden Stelle arbeiten, muss der Dritte mindestens das Schutzmaß für personenbezogene Daten bieten, das den Grundsätzen des sicheren Hafens entspricht. Der Grundsatz der Sicherheit verlangt von den Stellen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, dass sie angemessene Sicherheitsvorkehrungen zu treffen haben, um die Daten vor Verlust, Missbrauch oder unbefugter Kenntnisnahme, Veränderung oder Zerstörung zu schützen.

Der Grundsatz der Datenintegrität beinhalten die Erheblichkeit der Daten für den beabsichtigten Verwendungszweck. Die Verarbeitung personenbezogener Daten, die mit dem eigentlichen oder dem später genehmigten Zweck nicht vereinbar ist, ist untersagt. Die datenverarbeitende Stelle hat die Daten hinreichend zuverlässig, genau, vollständig und aktuell zu halten.

Der Grundsatz des Auskunftsrechts bedeutet, dass Betroffene Zugang zu den personenbezogenen Daten erhalten müssen, die die datenverarbeitende Stelle über sie besitzt. Weiterhin muss dem Betroffenen das Recht zugestanden werden, seine Daten ändern oder löschen zu lassen, wenn diese fehlerhaft sind. Diese Möglichkeit soll nur dann nicht bestehen, wenn die Gewährung des Zugangs mit unverhältnismäßigen Kosten oder Belastungen verbunden ist.

Das siebte Prinzip dient der Durchsetzung der zuvor genannten Grundsätze. Um eine Umsetzung gewährleisten zu können, sind effektive Maßnahmen zu installieren. Diese sollen zum einen Verfahren umfassen, die den Umgang mit Beschwerden und gegebenenfalls Schadensersatzansprüchen von Betroffenen regeln und zum anderen Kontrollmaßnahmen beinhalten, mit denen nachgeprüft werden kann,

ob die behaupteten Datenschutzmaßnahmen der Unternehmen richtig sind und auch durchgeführt werden. Das Prinzip der Durchsetzung bedeutet weiterhin, dass geregelt sein muss, wie Unternehmen zu sanktionieren sind, wenn sie die Einhaltung der Grundsätzen zwar erklärt, sich aber nicht daran gehalten haben.

Im Rahmen der Safe Harbor Zertifizierung haben zudem die ergänzenden Frequently Asked Questions (FAQ) des US-Handelsministeriums verbindlichen Charakter für die Unternehmen. Sie dienen der Konkretisierung der Grundsätze und geben Anwendungshinweise.[276] Ein US-Unternehmen erhält die Safe Harbor Zertifizierung entweder dadurch, dass es sich einem vom Privatsektor entwickelten Datenschutzprogramm anschließt, dass die Safe Harbor Grundsätze berücksichtigt oder eigene Maßnahmen zum Schutz personenbezogener Daten ergreift und eine selbstbindende Datenschutzerklärung abgibt. Sobald sich das US-Unternehmen gegenüber der FTC zur Einhaltung der Safe Harbor Grundsätze verpflichtet und hierzu eine Erklärung abgibt, wird es in die Safe Harbor Liste aufgenommen, die im Internet öffentlich abrufbar ist.[277]

5.2.2.2 Defizite der Selbstzertifizierung

Möchten Cloudanbieter personenbezogene Daten ihrer europäischen Kunden auch in Rechenzentren in den USA verarbeiten lassen, haben sie die Möglichkeit, sich dem Safe Harbor Abkommen zu unterwerfen, wenn sie nicht zu den Branchen zählen, die nicht unter die Gerichtbarkeit des FTC fallen und somit vom Safe Harbor Abkommen ausgenommen sind. Ausgeschlossen sind gem. der Ausnahmeregelungen des Abschnitts 5 des Abkommens Finanzinstitute, einschließlich Banken, Spar- und Darlehenskassen, sowie Kreditgenossenschaften, Betreiber öffentlicher Kommunikationsnetze, zwischenstaatlich tätige Transportunternehmer, Luftverkehrsunternehmen und Vieh- und

---

276 *Marnau/ Schlehahn,* DuD 2011, 311 (312); *Söbbing,* in: Leible/ Sosnitza (Hrsg.), Onlinerecht 2.0, S. 65.

277 *Schmidt-Bens,* Cloud Computing, S. 49; *Marnau/ Schlehahn,* DuD 2011, 311 (313).

Fleischhändler bzw. Fleischwarenproduzenten. Auch Firmen der Versicherungswirtschaft können durch bundesstaatliche Regelungen der Gerichtsbarkeit der FTC entzogen sein. Sieht man von diesen Ausnahmeregelungen ab, zeigt sich, dass viele amerikanische Unternehmen nach dem Safe Harbor Abkommen zertifiziert sind und auch viele bekannte Cloudanbieter wie Amazon, Microsoft, Google oder Salesforce über eine solche Zertifizierung verfügen.[278]

In der Literatur wird jedoch vermehrt der Ruf laut, dass entgegen der ursprünglichen Intention, die Safe Harbor Zertifizierung keine hinreichende Garantie für einen nach europäischen Maßstäben angemessenen Umgang mit personenbezogenen Daten beim Cloudanbieter und seinen Unterauftragnehmern darstellt.[279] Die Frage, ob eine Verbringung personenbezogener Daten an Safe Harbor zertifizierte Unternehmen rechtssicher ist, wurde jedoch bislang höchstrichterlich nicht entschieden.[280] Dass die Safe Harbor Zertifizierung einen unzureichenden Schutz personenbezogener Daten bietet, wird unter anderem auf eine unzureichende Kontrolle bei der Erfüllung der Zertifizierungsanforderungen zurückgeführt. Weiterhin werden erhebliche Defizite in Bezug auf die ursprünglich intendierten Grundsätze des Abkommens bemängelt. Beanstandet wird auch, dass sich die Safe Harbor Zertifizierung der US-Unternehmen häufig nicht auf alle Arten von Daten erstrecke und die von der Zertifizierung erfassten Datenkategorien auch nicht aus der Datenschutzerklärung des Unternehmens, sondern nur aus dem Selbstzertifizierungseintrag selbst herauslesbar seien.[281] Dies erschwere es dem Nutzer, sich Kenntnis über die entsprechenden Datenkategorien zu verschaffen und könne auch die Wahl der in Frage kommenden Cloudanbieter einschränken, wenn unterschiedliche Datenkategorien ausgelagert werden sollen,[282] was nicht

---

278 *Marnau/ Schlehahn,* DuD 2011, 311 (312).

279 *Marnau/ Schlehahn,* DuD 2011, 311 (313); *Kühling/ Biendl,* CR 2014, 150 (153).

280 *Wagner/ Blaufuß,* BB 2012, 1751 (1752).

281 *Busche,* in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 66; *Marnau/ Schlehahn,* DuD 2011, 311 (313).

282 *Marnau/ Schlehahn,* DuD 2011, 311 (313).

selten der Fall sein dürfte, insbesondere wenn die Cloud als Datenspeicher im Rahmen des IaaS genutzt werden soll. Beispielhaft sei erwähnt, dass sich die Zertifizierung bei salesforce nicht auf offline übermittelte Daten bezieht und sich bei Amazon nicht auf Personaldaten erstreckt.[283]

Als expliziter Kritikpunkt werden zudem die wage gehaltenen inhaltlichen Vorgaben der unternehmensinternen Datenschutzerklärungen genannt, die dazu führen würden, dass die Datenschutzerklärungen der Unternehmen im Unternehmensvergleich stark voneinander abwichen. Zudem sorgten auch die FAQ des US-Handelsministeriums dafür, dass die Grundsätze des Safe Harbor Abkommens aufgeweicht würden, was zu Lasten der Durchsetzung der an sich in den Grundsätzen klar geregelten Betroffenenrechte ginge. So verzichte beispielsweise Amazon auf die Benachrichtigung der Betroffenen über die Erhebung der Daten und den Zweck der Verarbeitung und belasse die Betroffenen hinsichtlich des Speicherorts der Daten im Unklaren; weiterhin benenne es die zugriffsberechtigten Stellen nicht. Kritisiert wird auch, dass dem Grundsatz der Wahlfreiheit nicht genügend entsprochen werde, da der Nutzer, wenn er die Leistung des Unternehmens beanspruchen möchte, einzig die Möglichkeit habe, der Datenverarbeitung vollständig zuzustimmen oder vollständig auf die Nutzung des Cloudservices zu verzichten. Ähnliches soll für die Datenschutzerklärungen anderer amerikanischer Unternehmen gelten. [284]

Inzwischen sind mehrere Studien veröffentlicht worden, die auf Unzulänglichkeiten beim Vollzug des Safe Harbor Abkommens hinweisen.[285] Eine Studie offenbarte, dass nur 3% der Unternehmen, die nach

---

283 *Marnau/ Schlehahn,* DuD 2011, 311 (313).

284 *Marnau/ Schlehahn,* DuD 2011, 311 (313).

285 *Connolly,* Safe Harbor – Fact or Fiction, abrufbar unter: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf, Stand: 7.6.2014; *Dhont/ Pérez Asinari/ Poullet,* Safe Harbor Decision Implementation Study, abrufbar unter: http://www.informatik.fh-gelsenkirchen.de/fileadmin/fb5/Paul/IGEA/Literatur/safe-harbour-2004_en.pdf, Stand: 7.6.2014

der Safe Harbor Liste über eine gültige Zertifizierung verfügten, auch tatsächlich alle Grundsätze der Zertifizierung einhielten.[286] Weiterhin wird bemängelt, dass die Einhaltung der Grundsätze kaum durchsetzbar sei, da die FTC ihre Aufsichts- und Eingriffsbefugnisse nur nutze, wenn es um falsche Angaben hinsichtlich der Zertifizierung oder um die Übereinstimmung mit den Grundsätzen gehe und auch dort nicht alle ihr zustehenden Befugnisse ausnutze, sodass Unternehmen keine gravierenden Rechtsfolgen zu befürchten hätten, wenn sie gegen die Vorgaben des Abkommens verstießen.[287] Probleme täten sich in der Praxis auch bei der unabhängigen Schlichtungsstelle auf, die es im Rahmen des Grundsatzes der Durchsetzung zu benennen gelte. Viele zertifizierte Unternehmen benennen die American Arbitration Association oder den Judical Arbitration Mediation Service, deren Schlichtungsbemühungen jedoch hohe Kosten verursachen und es dem Betroffenen daher schwer machen, gegen Verstöße vorzugehen.[288]

Im April 2010 hat der Düsseldorfer Kreis als Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich verkündet, dass es nach seiner Einschätzung für datenexportierende Unternehmen nicht hinreichend sei, wenn sie sich allein auf eine Safe Harbor Zertifizierung ihrer Datenempfänger verließen.[289] Daher bestünden für deutsche Unternehmen trotz der Angabe einer Safe Harbor Zertifizierung beim Datenempfänger gewisse Prüfpflichten. Diese erstrecken sich zum einen darauf, dass das deutsche Unternehmen zu prüfen habe, ob eine bestehende Zertifizierung gültig sei. Zertifizierungen, die vor mehr als sieben Jahren ausgestellt worden sind, sollen als nicht mehr gültig betrachtet werden. Zum anderen sol-

---

286 *Connolly*, Safe Harbor – Fact or Fiction, S. 8.

287 *Marnau/ Schlehahn*, DuD 2011, 311 (314).

288 *Marnau/ Schlehahn*, DuD 2011, 311 (314).

289 *Düsseldorfer Kreis*, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover, S. 1, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf;jsessionid=222DCBF4F6DAC479E12B20C3FA7FB035.1_cid354?__blob=publicationFile, Stand: 7.6.2014

len deutsche Unternehmen einen Nachweis darüber einfordern, dass das zertifizierte Unternehmen seinen Informationspflichten gegenüber den Betroffenen nachkommt. Die Erfüllung der Prüfkriterien sei zu Nachweiszwecken zu protokollieren. Könne das datenexportierende Unternehmen Zweifel an einer Safe Harbor Zertifizierung nicht vollständig ausräumen, empfiehlt der Düsseldorfer Kreis die Verwendung von EU-Standardvertragsklauseln oder eine Selbstbindung des Datenempfängers durch Binding Corporate Rules.[290] Für datenexportierenden Unternehmen hat der Beschluss des Düsseldorfer Kreises weitreichende Folgen, die die Datenweitergabe erschweren, weil die Prüf- und Dokumentationspflichten zusätzlichen Aufwand und weitere Kosten darstellen und Datenempfänger aus den USA somit faktisch denen aus den übrigen Drittstaaten ohne angemessenes Datenschutzniveau gleichgestellt werden.[291]

5.2.2.3 Konsequenzen für das Cloud Computing

Die Vollzugsdefizite bei der Durchsetzung einer dem Safe Harbor Abkommen entsprechenden Zertifizierung und die Reaktionen des Düsseldorfer Kreises darauf haben auch Auswirkungen auf die Nutzung von Cloudservices von US-Cloudanbietern und Unterauftragnehmern. Reicht eine Safe Harbor Zertifizierung allein nun nicht mehr aus, um ein angemessenes Datenschutzniveau zu garantieren, wäre eine Datenübermittlung an einen amerikanischen Cloudanbieter und Unterauftragnehmer nur nach Maßgabe der §§ 4b, 4c BDSG möglich.[292]

Der Beschluss des Düsseldorfer Kreises bedeutet für den Cloudnutzer, dass dieser fortan zu beurteilen hat, ob der Cloudanbieter zumindest über eine gültige Safe Harbor Zertifizierung verfügt und ob er seinen Informationspflichten nachkommt. Eine solche Prüfung muss auch für nachgeschaltete Unterauftragnehmer vorgenommen werden. In der Literatur wird zum Teil sogar die Auffassung vertreten, dass in Anbe-

---

290 *Düsseldorfer Kreis,* Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover, S. 2.

291 *Marnau/ Schlehahn,* DuD 2011, 311 (315); *Schmidt/ Bens,* Cloud Computing, S. 52.

292 *Marnau/ Schlehahn,* DuD 2011, 311 (315).

tracht der zahlreichen Auffälligkeiten im Rahmen der Safe Harbor Zertifizierung der Cloudnutzer sogar die Umsetzung aller sieben Grundsätze des Abkommens zu überprüfen und zu dokumentieren habe. Dies betreffe auch die relevanten Datenkategorien, die Prüfung der Datensicherheitsmaßnahmen und die Frage der Datenweitergabe an Dritte.[293]

Kann ein angemessenes Datenschutzniveau beim Cloudanbieter angenommen werden, ist zu prüfen, ob der Nutzung des Cloudservices nicht schutzwürdige Interessen des Betroffenen nach § 4b Abs. 2 S. 2 BDSG entgegenstehen.[294] Dies ist bereits an anderer Stelle erläutert worden.[295] Stellt der Cloudnutzer fest, dass das US-Unternehmen über kein angemessenes Datenschutzniveau verfügt, so ist die Nutzung von Cloudservices für personenbezogene Daten nur möglich, wenn einer der gesetzlichen Ausnahmetatbestände des § 4c Abs. 1 S. 1 BDSG greift[296] oder die zuständige Aufsichtsbehörde eine Ausnahmegenehmigung nach § 4c Abs. 2 S. 1 BDSG erteilt. Diese wird jedoch nur dann erteilt, wenn ausreichende Garantien zum Schutz von Persönlichkeitsrechten beispielsweise in Form von Vertragsklauseln oder verbindlichen Unternehmensregelungen nachgewiesen werden. In diesem Zusammenhang stellt sich jedoch die Frage, ob amerikanische Unternehmen, die über eine Safe Harbor Zertifizierung verfügen und daher davon ausgehen, ein angemessenes Datenschutzniveau zu gewährleisten, sich auf Verhandlungen mit dem Cloudnutzer über weitere Garantien zum Schutz von Persönlichkeitsrechten einlassen werden.

Nach Bekanntwerden des PRISM-Überwachungsskandals hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder

---

293 *Marnau/ Schlehahn,* DuD 2011, 311 (315).

294 *Räther/ Seitz,* MMR 2002, 425 (426); *Weichert,* DuD 2010, 679 (687); *Marnau/ Schlehahn,* DuD 2011, 311 (315).

295 Näheres dazu in Kapitel 5.2.

296 Näheres dazu in Kapitel 5.3.

am 24.07.2013 eine Pressemitteilung abgegeben.[297] In dieser Erklärung teilen die Datenschutzaufsichtsbehörden mit, dass sie keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten erteilen und nachprüfen werden, ob bestehende Datenübermittlungen auf Grundlage des Safe Harbor-Abkommens ausgesetzt werden sollen. In der Literatur sind inzwischen Zweifel geäußert worden, ob die Kompetenz der deutschen Aufsichtsbehörden ausreiche, um eine datenschutzrechtliche Rechtfertigung zur Datenübermittlung entfallen zu lassen, die wie beim Safe Harbor-Abkommen auf Basis einer Entscheidung der EU-Kommission beruht.[298] Zwar werde in Art. 3 1 Safe Harbor-Abkommen auch nationalen Behörden eingeräumt, die Datenübermittlung bei Verstößen gegen die Grundsätze des Abkommens unter bestimmten Voraussetzungen auszusetzen. Jedoch müsse bedacht werden, dass das Safe Harbor Abkommen gerade nicht den Zugriff von Sicherheitsbehörden auf die übermittelten Daten ausschließe, sondern diesen ausweislich des Anhang I der Entscheidung über die Grundsätze des sicheren Hafens zum Datenschutz für die dort bestimmten Zwecke wie beispielsweise aus Gründen der nationalen Sicherheit zulasse.[299] Aus diesem Grund wird in der Literatur teilweise die Meinung vertreten, dass die im Rahmen von PRISM durchgeführten Überwachungsmaßnahmen im Einklang mit dem Safe Harbor-Abkommen stünden.[300]

Es kann jedoch angezweifelt werden, dass die EU-Kommission beim Abschluss der Verhandlungen zum Safe Harbor-Abkommen derart umfassende Datenerhebungen, und -verarbeitung personenbezogener Daten als durch das Abkommen gedeckt angesehen hätte, wenn es um

---

297 *Konferenz der Datenschutzbeauftragten des Bundes und der Länder,* Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten, abrufbar unter: http://www.datenschutz-berlin.de/attachments/970/Presseerkl__rung_Safe_Harbor-2.pdf?1374663105, Stand: 7.6.2014.

298 *Voigt,* Datenübermittlung in die USA ab sofort rechtswidrig?, abrufbar unter: http://www.datenschutzkongress.de/lp/2014/P1106112_newsletter.pdf, Stand: 7.6.2014; *Spies,* ZD 2013, 535 (536)

299 *Spies,* ZD 2013, 535 (536).

300 *Schuppert/von Reden,* ZD 2013, 210 (212).

diese gewusst hätte. Im November 2013 hat die EU-Kommission das MEMO „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA – Häufig gestellte Fragen“[301] veröffentlicht. Dort spricht sie sich für die Beibehaltung des Abkommens aus und gibt 13 Empfehlungen ab, durch die das Abkommen besser funktionieren solle. Im Bereich der Transparenz empfiehlt die EU-Kommission eine Regelung, nach der die zertifizierten Unternehmen neben ihren eigenen Datenschutzrichtlinien auch die Datenschutzbestimmungen veröffentlichen sollen, die sie in Verträgen mit ihren Unterauftragnehmern vereinbart haben. Diese Regelung würde sich insbesondere an Cloudanbieter und ihre Unterauftragnehmer richten. Weiterhin fordert die EU-Kommission Angaben in den Datenschutzrichtlinien der zertifizierten Unternehmen, aus denen hervorgehen soll, inwieweit es das US-Recht US-Behörden gestatte, die im Rahmen des Abkommens übermittelten Daten zu sammeln und zu verarbeiten. Aus den Datenschutzbestimmungen soll zudem hervorgehen, zu welchen Zwecken Ausnahmen von den Grundsätzen des Abkommens angewandt werden. Ausnahmen zum Zwecke der nationalen Sicherheit sollen nur dann zur Anwendung gelangen, wenn dies unbedingt notwendig beziehungsweise angemessen ist. Inwieweit sich die USA auf die Forderungen der EU-Kommission einlassen werden, ist abzuwarten. Die EU-Kommission hat den US-Behörden bis zum Sommer 2014 Zeit eingeräumt, geeignete Lösungen zu finden.

5.2.2.4 USA Patriot Act

Da viele Cloudanbieter und Unterauftragnehmer in den USA ansässig sind, soll im Folgenden kurz der USA Patriot Act[302] vorgestellt werden, der US-Ermittlungsbehörden und Geheimdiensten starke Zu-

---

301 *Europäische Kommission,* Widerherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA – Häufig gestellte Fragen, abrufbar unter: http://europa.eu/rapid/press-release_MEMO-13-1059_de.htm, Stand: 07.05.2014.

302 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, abrufbar unter: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf, Stand: 7.6.2014

griffsrechte auf bei amerikanischen Unternehmen lagernde Daten einräumt und somit auch für deutsche Unternehmen als Cloudnutzer eine hohe Bedeutung erlangt.

Aufgrund der Terroranschläge vom 11.9.2011 hat der US-Kongress den USA Patriot Act erlassen. Dieser stellt kein eigenständiges Gesetzeswerk, sondern ein Änderungsgesetz dar, das mehrere Bestimmungen des US Code ändert. Dem USA Patriot Act zufolge dürfen US-Ermittlungsbehörden und Geheimdienste auf Datenbestände amerikanischer Unternehmen zugreifen, wenn ein Terrorverdacht besteht. Dies gilt auch für Server, die einem amerikanischen Unternehmen gehören, jedoch außerhalb der USA gelegen sind.[303] Durch den Erlass eines National Security Letters von US-Behörden werden Unternehmen, ohne dass es notwendigerweise der Einschaltung eines US-Gerichts bedarf, zur Herausgabe verpflichtet.[304] Der Adressat des National Security Letters kann zudem verpflichtet werden, über den Sachverhalt Stillschweigen zu wahren.[305] Diese weitreichenden Befugnisse nach US-Recht sind folgenreich für amerikanische Cloudanbieter und Unterauftragnehmer, die auch auf dem europäischen Markt aktiv sind. Sie haben viele deutsche Unternehmen gegenüber Cloudservices amerikanischer Anbieter skeptisch werden lassen, da ein Zugriff durch US-Behörden nicht unterbunden werden kann und amerikanische Anbieter teilweise offen verkündet haben, dass sie zur Herausgabe der bei ihnen gespeicherten Daten an die USA bereit seien, wenn sie hierzu aufgefordert werden würden.[306]

---

303 *Spies,* MMR 2009, Heft 5, XI (XI); *Opfermann,* ZEuS 2012, 121 (148); *Becker/ Nikolaeva,* CR 2012, 170 (170).

304 *Becker/ Nikolaeva,* CR 2012, 170 (171); *Böken,* Patriot Act und Cloud Computing, abrufbar unter: http://www.heise.de/ix/artikel/Zugriff-auf-Zuruf-1394430.html, Stand: 7.6.2014; *Hansen,* DuD 2012, 407 (410).

305 *Becker/ Nikolaeva,* CR 2012, 170 (171).

306 *Sawall,* Europäische Cloud-Daten nicht vor US-Zugriff sicher, abrufbar unter: http://www.golem.de/1106/84620.html, Stand: 7.6.2014; *Böken,* Patriot Act und Cloud Computing, abrufbar unter: http://www.heise.de/ix/artikel/Zugriff-auf-Zuruf-1394430.html, Stand: 7.6.2014

Die Ankündigung der US-Anbieter ist jedoch auch verständlich, da sobald ein National Security Letter gegen das Unternehmen erlassen wird, es nur die Möglichkeit hat, sich diesem Erlass zu widersetzen und somit gegen US-Recht zu verstoßen oder gegen deutsches Recht, indem es dem Erlass Folge leistet. Das Risiko einer unzulässigen Datenübermittlung besteht bei jedem amerikanischen Cloudanbieter und Unterauftragnehmer und lässt sich weder durch die Begründung eines Sitzes in Europa, noch durch die Errichtung einer europäischen Availability Zone eindämmen.[307] Obwohl dieses Problem auf europäischer Ebene wahrgenommen wird,[308] gibt es derzeit keine Lösung.

Solange keine Lösung gefunden worden ist, haben Cloudnutzer daher nur die Möglichkeit, Server von US-Cloudanbietern und Unterauftragnehmer zu nutzen und mögliche Zugriffe von US-Behörden zu akzeptieren oder ganz auf US-Clouds zu verzichten und ausschließlich europäische Anbieter zu nutzen, wobei Flexibilitäts- und Kostenvorteile schwinden könnten. Die dritte Möglichkeit besteht darin, auf den Servern europäischer Anbieter, Services von US-Anbietern zu nutzen, da sich das Zugriffsrecht der US-Behörden nur auf die Server der US-Anbieter bezieht.[309] Dies ist grundsätzlich möglich, da es auch Cloudanbieter auf dem Markt gibt, die ohne eigene Server Cloudservices anbieten, jedoch verkomplizieren sich die Verhältnisse mit jedem weiteren Unterauftragnehmer. Zudem sind die kostengünstigsten und größten Cloudanbieter aus den USA und verfügen über eigene Server, sodass es nicht einleuchtet, was diese Anbieter veranlassen könnte, statt vorhandener eigener Server die europäischer Anbieter zu nutzen.

Weiterhin sei erwähnt, dass der USA Patriot Act auch das Safe Harbor-Abkommen berührt, weil ein derart zertifiziertes Unternehmen nicht garantieren kann, dass es die bei ihm gespeicherten Daten vor

---

307 *Becker/Nikolaeva,* CR 2012, 170 (175); *Hansen,* DuD 2012, 407 (410).

308 *Gehring,* EU-Parlamentarier besorgt über US-Zugriff auf Cloud-Daten, abrufbar unter: http://www.golem.de/1107/84763.html, Stand: 7.6.2014

309 *Opfermann,* ZEuS 2012, 121 (148).

dem Zugriff amerikanischer Behörden und Geheimdiensten bewahren kann.[310]

5.3 Ausnahmen gem. §. 4c Abs. 1 BDSG

§ 4c BDSG erlaubt unter den dort aufgeführten Voraussetzungen auch die Übermittlung von Daten in Drittstaaten ohne angemessenes Datenschutzniveau, um gewöhnliche Routineaufgaben des täglichen Lebens zu erleichtern.[311] § 4c Abs. 1 S. 1 Nr. 1 BDSG gestattet die Übermittlung in Staaten ohne angemessenes Datenschutzniveau, wenn die Einwilligung des Betroffenen vorliegt. Wie bereits dargelegt, ist die Einwilligung im Rahmen des Cloud Computings keine praktikable Lösung. Beim internationalen Datentransfer kommt noch hinzu, dass der Betroffene ausdrücklich auf das geringere Datenschutzniveau hingewiesen werden muss.[312] Zudem ist beim Erheben der Daten der Aspekt der außereuropäischen Übermittlung noch nicht abzusehen und das Einholen der Einwilligung daher erst nachträglich vor der Auslagerung in die Cloud möglich.[313]

§ 4c Abs. 1 S. 1 Nr. 2 BDSG regelt die Ausnahme, in der die Übermittlung für die Erfüllung eines Vertrags zwischen verantwortlicher Stelle und Betroffenem erforderlich ist. Häufig ist es jedoch selten vorab klar, dass die erhobenen Daten in eine Cloud verlagert werden sollen, sodass die spätere Übermittlung für das Vertragsverhältnis keine Rolle spielt.[314]

Gemäß § 4c Abs. 1 S. 1 Nr. 3 BDSG ist eine Übermittlung in einen Drittstaat ohne angemessenes Datenschutzniveau zulässig, wenn sie zum Abschluss oder zur Erfüllung eines Vertrags, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen worden ist, erforderlich ist. § 4c Abs. 1 S. 1 Nr. 3 BDSG

310 *Schweda,* ZD-aktuell 2012, 30109; *Bedner,* Cloud Computing, S. 304.
311 *Simitis,* in: ders. (Hrsg.), BDSG 2011, § 4c Rn. 1; *Schmidt-Bens,* Cloud Computing, S. 58.
312 *Simitis,* in: ders. (Hrsg.), BDSG 2011, § 4c Rn. 9.
313 *Bedner,* Cloud Computing, S. 240.
314 *Bedner,* Cloud Computing, S. 240.

greift damit Verträge auf, an denen der Betroffene zwar nicht beteiligt ist, von denen er aber begünstigt wird.[315] Fraglich ist daher, ob der Abschluss eines Vertrags zwischen dem Cloudnutzer und dem Cloudanbieter im Interesse des Betroffenen liegt. Es ist nicht ersichtlich, worin der Vorteil beim Betroffenen liegen soll, wenn seine Daten in eine internationale Cloud ausgelagert werden; vielmehr liegen die Vorteile der Cloudnutzung auf der Seite des Cloudnutzers, sodass § 4c Abs. 1 S. 1 Nr. 3 BDSG als Ausnahme für Cloudsachverhalte nicht eingreift. Die weiteren Ausnahmen des § 4c Abs. 1 S. 1 Nr. 4 bis 6 BDSG sind ebenfalls kaum auf Cloud Computing beziehbar, sodass die Ausnahmetatbestände des § 4c Abs. 1 S. 1 BDSG im Rahmen des Cloud Computings in den seltensten Fällen zur Übermittlung von personenbezogenen Daten in Drittstaaten ohne angemessenes Datenschutzniveau herangezogen werden können.[316]

5.4 Ausnahmen gem. § 4c Abs. 2 BDSG

Greift keine der bisher geschilderten Ausnahmen, so sind die genehmigungsbedürftigen Ausnahmen aus § 4c Abs. 2 S. 1 BDSG zu prüfen. Diese haben im Rahmen des Cloud Computings eine praxisrelevante Bedeutung und ermöglichen es, Defizit im Datenschutzniveau zu kompensieren.[317] § 4c Abs. 2 S. 1 BDSG regelt explizit, dass ausreichende Garantien zum Schutz des Persönlichkeitsrechts und der damit verbundenen Rechte insbesondere durch Vertragsklauseln oder verbindliche Unternehmensregelungen erzielt werden können. Die von der EU-Kommission beschlossenen EU-Standardvertragsklauseln haben in diesem Zusammenhang eine besondere Bedeutung, da sie als eine ausreichende Garantie gelten.[318] Da diese erwähnten Instrumente nicht auf alle Konstellationen anwendbar sind, soll im Folgenden zu-

315 *Simitis,* in: ders. (Hrsg.), BDSG 2011, § 4c Rn. 17; *Gola/ Schomerus (Hrsg.),* § 4c Rn. 6a.

316 *Bedner,* Cloud Computing, S. 240.

317 *Schulz,* in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 413; *Rittweger/ Schmidl,* DuD 2004, 617 (617); *Grapentin,* CR 2011, 102 (102); *Nielen/ Thum,* K&R 2006, 171 (172); *Schmidt-Bens,* Cloud Computing, S. 58.

318 *Gola/ Schomerus (Hrsg.),* BDSG, § 4c Rn. 12; *Roth,* in: Auer-Reinsdorff/ Conrad (Hrsg.), Beck´sches Mandats Handbuch IT-Recht, § 6 Rn. 198.

nächst eine Differenzierung danach erfolgen, wo die am Cloud Computing Beteiligten ansässig sind, um die Instrumente anschließend vorzustellen. Dabei wird unterstellt, dass die Cloudanbieter und Unterauftragnehmer auch ihre Rechenzentren am Ort des Unternehmenssitzes unterhalten.

5.5 Unterauftragsdatenverarbeitung in Drittstaaten

Wie darstellt, ist es bei der Erbringung von Cloudservices üblich, dass Cloudanbieter Verträge mit Unterauftragnehmern aus aller Welt schließen, sodass auch diese Zugang zu personenbezogenen Daten erhalten. Für die Zulässigkeit der Datenübermittlung an Unterauftragnehmer in Drittstaaten ist das Schutzniveau für personenbezogene Daten ebenfalls maßgeblich, sodass im Falle nicht sicherer Drittstaaten geschaut werden muss, mit welchen Instrumenten dieses hergestellt werden kann.

Inzwischen hat sich auch die Artikel-29-Datenschutzgruppe als unabhängiges europäisches Beratungsgremium auf Grundlage von Art. 29 EU-DSRL zur Unterauftragsverarbeitung in Drittstaaten geäußert.[319] Ihr kommt aufgrund ihrer Zusammensetzung aus Vertretern der nationalen Datenschutzbehörden, sowie aus europäischen Datenschutzbeauftragten und einem Vertreter der EU-Kommission eine starke Bedeutung im Bereich des Schutzes von Betroffenen bei der Verarbeitung ihrer personenbezogenen Daten zu, obwohl sie nur Stellungnahmen und Empfehlungen ausspricht, jedoch über keine legislativen Kompetenzen verfügt.[320] Ihrer Ansicht nach soll auch der Cloudanbieter bei der Unterauftragsverarbeitung in Drittstaaten, seine Tätigkeiten an Unterauftragnehmer nur auf Grundlage einer Einwilligung des Cloudnutzers auslagern dürfen, wobei diese auch zu Beginn des Vertragsverhältnisses zwischen Cloudnutzer und Cloudanbieter

---

319 *Artikel-29-Datenschutzgruppe,* WP 176, S. 6, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_de.pdf, Stand: 7.6.2014

320 *Grapentin,* CR 2009, 693 (696); *Büllesbach,* Transnationalität und Datenschutz, S. 67; *Schmidt-Bens,* Cloud Computing, S. 66.

generell erteilt werden könne.[321] Wenig überraschend ist die Forderung, nach der alle einschlägigen Verpflichtungen, die zwischen dem Cloudnutzer und dem Cloudanbieter bestehen, auch für eingeschaltete Unterauftragnehmer gelten sollen,[322] wobei insbesondere sichergestellt werden soll, dass sich alle Unterauftragnehmer bei der Durchführung der Verarbeitung den Weisungen des Cloudnutzers unterwerfen. Eine klare Zuordnung der Verpflichtungen und Verbindlichkeiten soll verhindern, dass sich Cloudanbieter und Unterauftragnehmer ihrer Verantwortung entziehen und Fehlverhalten nicht mehr kontrolliert und zugeordnet werden kann. [323]

Ein mögliches Instrument zur Regelung dieser Verpflichtungen bei der Datenweitergabe an Unterauftragnehmer sieht die Artikel-29-Datenschutzgruppe in den EU-Standardvertragsklauseln 2010/87/EU (Standardvertragsklauseln) vom 5.2.2010.[324] Dabei wird jedoch nicht darauf eingegangen, dass diese nicht in jedem Fall anwendbar sind und daher danach differenziert werden muss, wo Cloudanbieter und Unterauftragnehmer ansässig sind. Eine derartige Differenzierung soll nun vorgenommen werden. Wie schon einleitend dargestellt, ergeben sich aus der Sicht eines deutschen Unternehmens als Cloudnutzer vier Fälle, aus denen hervorgeht, wo Cloudanbieter und Unterauftragnehmer ansässig sein können. Diese können der nachfolgenden Tabelle 1 entnommen werden.

---

321 *Artikel-29-Datenschutzgruppe*, WP 176, S. 6, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_de.pdf, Stand: 7.6.2014

322 *Artikel-29-Datenschutzgruppe*, WP 196, S. 11.

323 *Artikel-29-Datenschutzgruppe*, WP 169, S. 29, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf, Stand: 7.6.2014

324 *Artikel-29-Datenschutzgruppe*, WP 196, S. 12.

	Cloudnutzer	Cloudanbieter	Unterauftrag-nehmer
Fall A	Deutschland	EU	EU
Fall B	Deutschland	Drittstaat	Drittstaat
Fall C	Deutschland	EU	Drittstaat
Fall D	Deutschland	Drittstaat	EU

Tabelle 2: Ansässigkeit der am Cloud Computing Beteiligten

Nachfolgend soll dargelegt werden, welche Regelungsmöglichkeiten in den unterschiedlichen Fällen bestehen. Da es bisher keine cloudspezifischen Regelungsinstrumente gibt, ist auf die allgemeinen zurückzugreifen und zu schauen, ob sich für das Cloud Computing Besonderheiten ergeben. Da Fall A bereits im Rahmen der Auftragsdatenverarbeitung gem. § 11 BDSG in Kapitel 4.2.4. behandelt worden ist, beschränkt sich die nachstehende Betrachtung auf die Fälle B-D.

5.5.1 Regelungsmöglichkeiten im Fall B

Wie Tabelle 1 entnommen werden kann, befinden sich im Fall B sowohl der Cloudanbieter als auch der Unterauftragnehmer mit ihren Rechenzentren in einem Drittstaat. Dieser Fall soll durch die Standardvertragsklauseln regelbar sein. Durch den Beschluss der EU-Kommission vom 5.2.2010[325] sind die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in

[325] *Europäische Kommission,* Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern, abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF, Stand: 7.6.2014

Drittstaaten in Kraft, die ab dem 15.5.2010 für alle neu abzuschließenden Auftragsdatenverarbeitungsverträge Geltung erlangen. Zu beachten ist, dass der Begriff „Auftragsverarbeiter" im Sinne des Art. 2 lit. e) EU-DSRL zu verstehen ist, da wie bereits geschildert, § 3 Abs. 8 S. 3 BDSG die Auftragsdatenverarbeitung nach Maßgabe des § 11 BDSG in Drittstaaten nicht vorsieht und alle Auftragsverarbeiter mit Sitz in einem Drittstaat als Dritte ansieht.[326]

Die Standardvertragsklauseln 2010/87/EU haben die alten Standardvertragsklauseln vom 27.12.2001 abgelöst, die nicht mehr verwendet werden dürfen.[327] Nur alte Verträge, die vor dem 15.5.2010 geschlossen worden sind, können so lange fortbestehen bleiben wie die Übermittlung und die Datenverarbeitung durch den Auftragsverarbeiter unverändert erfolgt. Werden neue Arten von Daten wie z.B. neben Kundendaten auch Lieferantendaten übertragen, soll eine Unterauftragsvergabe erfolgen oder die Daten für weitergehende Zwecke verarbeitet werden, so muss die Vertragsbeziehung auf die neuen Standardvertragsklauseln umgestellt werden.[328]

Die Standardvertragsklauseln werden als gesonderter Vertrag neben dem eigentlichen Dienstleistungsvertrag über die Erbringung der Leistung geschlossen und regeln die Rechte und Pflichten der Parteien im Umgang mit personenbezogenen Daten. Sie haben vollständig und unverändert übernommen zu werden, um ihre Genehmigungsfreiheit durch die Aufsichtsbehörde nicht zu verlieren.[329] Da sich die Standardvertragsklauseln gem. Erwägungsgrund 4 des Kommissionsbeschlusses nur auf datenschutzrechtliche Fragen beziehen sollen, können von den Parteien auch weitere geschäftsbezogene Klauseln in den

---

326 *Grapentin,* CR 2011, 102 (104); *Wybitul/ Patzak,* RDV 2011, 11 (12); *Hoeren,* RDV 2012, 271 (272).

327 *Hladik,* DSB 3/2010, S. 7.

328 *Eul/ Eul,* Datenschutz International, S. 82; *Helbing,* Standardvertragsklauseln und Auftragsverarbeiter, 3., abrufbar unter: http://www.saasmagazin.de/schwerpunkte/schwerpunkte-2009/crm-loesungen-in-der-cloud-saas-crm/dr-helbing-sp-crm090712.html, Stand: 7.6.2014; *Wybitul/ Patzak*, RDV 2011, 11 (15).

329 *Schmidt-Bens,* Cloud Computing, S. 61; *Wybitul/ Patzak,* RDV 2011, 11 (15); *Hoeren,* RDV 2012, 271 (274).

Vertrag aufgenommen werden, sofern sie nicht im Widerspruch zu den Standardvertragsklauseln stehen. Der zugrunde liegende Dienstleistungsvertrag hat dann auf die Nutzung der Standardklauseln hin überprüft und entsprechend angeglichen zu werden.[330]

Eine wichtige Regelung in den Standardvertragsklauseln betrifft die Möglichkeit der Unterauftragsvergabe, sodass diese Klauseln auch im Rahmen des Clouds Computings interessant sein könnten, um die komplexen Geflechte zwischen Cloudanbietern und Unterauftragnehmern rechtlich anzugehen. Gemäß Art. 2 des Kommissionsbeschlusses gelten die Standardvertragsklauseln „für die Übermittlung personenbezogener Daten durch für die Verarbeitung Verantwortliche, die in der EU niedergelassen sind, an Empfänger außerhalb der EU, die ausschließlich als Auftragsverarbeiter fungieren." Dem Wortlaut nach finden die Standardvertragsklauseln demnach keine Anwendung, wenn nur der Unterauftragnehmer in einem Drittstaat ansässig ist, sich der Auftragsverarbeiter jedoch in einem EU-Staat befindet.[331]

Nach der Terminologie ist der Datenexporteur gem. Art. 3 c) des Kommissionsbeschlusses der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt. Im Anwendungsfall des Cloud Computings ist dies der Cloudnutzer. Datenimporteur ist gem. Art. 3 d) des Kommissionsbeschlusses der in einem Drittstaat niedergelassene Auftragsverarbeiter, der die personenbezogenen Daten vom Datenexporteur übermittelt bekommt und diese in dessen Auftrag und auf dessen Weisungen hin verarbeitet. Der Datenimporteur darf weiterhin nicht aus einem Drittstaat kommen, das gem. Art. 25 Abs. 1 EU-DSRL ein angemessenes Datenschutzniveau bietet. Im Anwendungsfall des Cloud Computings ist dies der Cloudanbieter. Gemäß Art. 3 e) des Kommissionsbeschlusses ist ein Unterauftragsverarbeiter ein Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenim-

330 *Helbing*, Standardvertragsklauseln und Auftragsverarbeiter, 1c.
331 *Lensdorf*, CR 2010, 735 (737).

porteurs tätig ist. Dieser ist im Fall des Cloud Computings der Unterauftragnehmer. Somit decken die Standardvertragsklauseln den momentan gängigsten Fall der Nutzung von Cloudservices ab. Schließlich sind die meisten Cloudanbieter in den USA ansässig und beauftragen ihrerseits wiederrum Unterauftragnehmer, die ebenfalls häufig außerhalb der EU ansässig sind.[332]

Klausel 11 der Standardvertragsklauseln regelt die Unterauftragsvergabe. Damit sichergestellt werden kann, dass die übermittelten personenbezogenen Daten auch beim Datentransfer an einen Unterauftragsverarbeiter geschützt sind, ist die Unterauftragsvergabe nur unter strengen Voraussetzungen gestattet.[333] Zu einem muss der Cloudnutzer gem. Klausel 11 Abs. 1 S. 1 der Vergabe des Unterauftrags im Voraus schriftlich zustimmen. Zum anderen hat er gem. Klausel 11 Abs. 4 ein Verzeichnis über sämtliche Verträge mit Unterauftragnehmern zu führen und hat dieses mindestens einmal im Jahr zu aktualisieren. Dieses Verzeichnis muss er seiner zuständigen Aufsichtsbehörde bereitstellen. Der Unterauftrag hat im Wege einer schriftlichen Vereinbarung zu erfolgen, die dem Unterauftragnehmer nach den Vorgaben der Klausel 11 Abs. 1 S. 2 dieselben Pflichten auferlegt, die auch den Cloudanbieter nach dem Vertrag mit dem Cloudnutzer treffen. Der Cloudanbieter bleibt gegenüber dem Cloudnutzer für die eigene Datenverarbeitung und auch für die des Unterauftragnehmers gem. Klausel 11 Abs. 1 S. 3 voll verantwortlich. Weiterhin hat der Vertrag über die Unterbeauftragung eine Drittbegünstigungsklausel zu enthalten, die dem Betroffenen die subsidiäre Geltendmachung von Schadensersatzansprüchen gegenüber dem Unterauftragnehmer einräumt, wenn das Unternehmen des Cloudanbieters selbst nicht mehr besteht oder zahlungsunfähig ist. Diese Haftpflicht ist auf die Verarbeitungstätigkeiten des Unterauftragnehmers nach den Vertragsklauseln beschränkt.[334]

---

332 *Bedner*, Cloud Computing, S. 244.
333 *Moos*, CR 2010, 281 (283).
334 *Moos*, CR 2010, 281 (284)

Für Datenverarbeitungen durch den Unterauftragnehmer findet gem. § 11 Abs. 3 BDSG zwingend das für den Cloudnutzer geltende Datenschutzrecht Anwendung. Dies gilt auch für die Datenverarbeitungen durch den Cloudanbieter. Nutzen in Deutschland ansässige Unternehmen Cloudservices, hat dies für die betroffenen Kunden, Mitarbeiter und Lieferanten den Vorteil, dass unabhängig vom physischen Aufenthaltsort ihrer Daten in jedem Fall deutsches Datenschutzrecht Anwendung findet, das ein sehr hohes Datenschutzniveau aufweist. Für Unterauftragnehmer bedeutet dies, dass sie eine Vielzahl nationaler Datenschutzbestimmungen zu beachten haben, wenn sie für mehrere, in verschiedenen Mitgliedsstaaten der EU niedergelassene Cloudnutzer tätig sind, was für sie einen Nachteil bedeutet.[335]

Darüber hinaus gibt es außerhalb der Klausel 11 zusätzliche Regelungen bezüglich der Unterauftragsvergabe. Der Cloudanbieter muss den Cloudnutzer gem. Klausel 5 lit. h. vor der Unterauftragsvergabe benachrichtigen und dessen schriftliche Einwilligung einholen. Ebenso wie nach Maßgabe des § 11 BDSG, wird auch hier davon ausgegangen, dass ein Unterauftrag nicht in jedem Einzelfall genehmigt werden muss, sondern es der Cloudnutzer selbst entscheiden können soll, ob er eine generelle vorherige Zustimmung erteilt oder jedem einzelnen Unterauftrag zustimmen möchte.[336] Eine generelle vorherige Zustimmung, bei der die Bedingungen für die Unterauftragsvergabe eindeutig und unabdingbar festgelegt sind, bietet auch im Rahmen des Cloud Computings Vorteile, da die Vergabe von Unteraufträgen aufgrund technischer Erfordernisse auch kurzfristig bewerkstelligt werden kann und zugleich keine Einbußen für die Datenschutzpositionen der Betroffenen befürchtet werden müssen. Ein Problem dürften Freibriefe darstellen, die eine Unterauftragsvergabe an beliebige Unterauftragnehmer erlauben, da die Erfordernisse an die informierte Einwilli-

335 *Moos,* CR 2010, 281 (284).
336 *Artikel-29-Datenschutzgruppe,* WP 176, S. 6.

gungserteilung in diesem Fall als unterlaufen angesehen werden könnten.[337]

Eine weitere Pflicht trifft den Cloudanbieter gem. Klausel 5 lit. j des Kommissionsbeschlusses. Danach hat er dem Cloudnutzer unverzüglich eine Kopie des Unterauftrags zuzuschicken, aus der hervorzugehen hat, dass dem Unterauftragnehmer die gleichen Pflichten auferlegt worden sind, die auch nach den Vertragsklauseln für ihn selbst gelten. Nach Auffassung der Artikel-29-Datenschutzgruppe sind nicht alle Unterlagen über die Unterauftragsvergabe zu übermitteln, sondern nur diejenigen, die vertragliche Vereinbarungen zum Datenschutz und zu Sicherheitsmaßnahmen enthalten.[338] Diese Anforderung und jene, nach der der Cloudnutzer ein Verzeichnis über sämtliche Unteraufträge zu führen hat, bedeutet für beide Parteien einen zusätzlichen administrativen Aufwand, wobei diese Vorgaben sicherlich den positiven Effekt haben dürften, dass Unteraufträge auch tatsächlich im Einklang mit den Standardvertragsklauseln geschlossen werden.[339] Der Cloudnutzer muss dem Betroffenen zudem auf dessen Anfrage hin gem. Klausel 4 lit. h eine Kopie der Unterauftragsverarbeitungsverträge zur Verfügung stellen, die gegebenenfalls um Anhang 2 und sogenannte Geschäftsinformationen gekürzt werden können. Die für den Cloudnutzer zuständige Datenschutzbehörde kann gem. Klauseln 8 Abs. 2 in gleichem Maße und zu gleichen Bedingungen wie beim Cloudnutzer, auch beim Cloudanbieter und seinen Unterauftragnehmern Prüfungen vornehmen. Bei Cloudnutzern aus unterschiedlichen EU-Staaten können es der Cloudanbieter und seine Unterauftragnehmer somit mit einer Vielzahl von Aufsichtsbehörden zu tun bekommen.

Die Standardvertragsklauseln sind auch für das Cloud Computing ein Fortschritt, da sich mit ihnen der in der Praxis wichtige Fall regeln lässt, in dem ein deutsches Unternehmen als Cloudnutzer einen

337 *Artikel-29-Datenschutzgruppe,* WP 176, S. 6.
338 *Artikel-29-Datenschutzgruppe,* WP 176, S. 6.
339 *Moos,* CR 2010, 281 (284); *Wybitul/ Patzak,* RDV 2011, 11 (16).

Cloudservice nutzt, der durch einen in einem Drittstaat ansässigen Cloudanbieter unter Zuhilfenahme von Ressourcen weiterer in Drittstaaten ansässiger Unterauftragnehmer erbracht wird.

In der Literatur wird die Tatsache bedauert, dass die Standardvertragsklauseln eine Unterbeauftragung nur erlauben, wenn diese auf Basis der Standardvertragsklauseln selbst erfolgt und keine Verknüpfung zu Unternehmensregelungen im Sinne von Binding Corporate Rules (BCR) oder zu Safe Harbor Zertifizierungen vorgesehen ist. Es wird bemängelt, dass eine Unterbeauftragung nicht auf Basis von BCR oder einer Safe Harbor Zertifizierung erfolgen kann, ohne dass die Verpflichtungen aus den Standardvertragsklauseln 1:1 auch für die Unterauftragnehmer zu gelten haben.[340] Pauschal kann dieser Kritik im Hinblick auf die Safe Harbor Zertifizierung nicht beigepflichtet werden, allerdings hat der Düsseldorfer Kreis dem Cloudnutzer Prüf- und Dokumentationspflichten auferlegt, die ihn dazu zwingen, sich mit der Safe Harbor Zertifizierung und dem damit garantierten Datenschutzniveau auseinanderzusetzen. Sollte der Cloudnutzer nach sorgfältiger Prüfung feststellen, dass das Datenschutzniveau aus der Safe Harbor Zertifizierung mit dem in den Standardvertragsklauseln deckungsgleich ist, spricht grundsätzlich nichts dagegen, beide Instrumente zu verknüpfen und somit eine im Vergleich zu den Standardvertragsklauseln flexiblere Regelung zur Unterauftragsvergabe zuzulassen.

Obwohl die Standardvertragsklauseln viele Regelungen enthalten, die § 11 BDSG entsprechen[341] und teilweise auch über diese hinausgehen,[342] fordern einige Aufsichtsbehörden, dass der Cloudnutzer neben der Vereinbarung der Standardvertragsklauseln, auch die Anforderungen aus § 11 Abs. 2 BDSG erfüllen und vertraglich abbilden muss, ohne dass jedoch die Erfüllung dieser Anforderungen zu einer Privile-

340 *Moos,* CR 2010, 281 (285).
341 *Eul/ Eul,* Datenschutz International, S. 83.
342 *Moos,* CR 2010, 281 (283).

gierung des Cloudanbieters führt.[343] Die Anforderungen aus § 11 Abs. 2 BDSG sollen beispielsweise in Regelungen in den Anlagen zum Standardvertrag oder in ergänzenden geschäftsbezogenen Klauseln abgebildet werden.[344] Die Forderung ist in ihrer Umsetzung jedoch problembehaftet. So ist beispielsweise ausgeführt worden, dass die Vor-Ort-Kontrolle im Rahmen von § 11 Abs. 2 S. 4 BDSG durch Datenschutz-Audits, Zertifizierungen oder Testate ersetzt werden kann und beim Cloud Computings auch ersetzt werden muss, weil eine Vor-Ort-Kontrolle in den meisten Fällen nicht durchführbar sein dürfte. Beim internationalen Cloud Computing werden die Cloudanbieter und Unterauftragnehmer jedoch Audits oder Zertifikate ausländischer Prüfer und Stellen vorlegen, ohne dass klar ist, ob diese den deutschen gleichwertig sind, sodass eine intensive Auseinandersetzung mit den vorgelegten Audits und Zertifikaten erfolgen und eine Gleichwertigkeit nachgewiesen werden muss.[345]

Unabhängig davon, ob man die zusätzliche Erfüllung der Anforderungen aus § 11 Abs. 2 BDSG befürwortet oder nicht, ist es für den Cloudnutzer aufgrund der bestehenden Rechtsunsicherheit wichtig, seine zuständige Aufsichtsbehörde um ihre Einschätzung anrufen.[346] Sollte sich die Aufsichtsbehörde für die zusätzliche Abbildung des § 11 Abs. 2 BDSG aussprechen, so muss dem Folge geleistet werden, wobei darauf zu achten ist, die zusätzlichen Anforderungen derart aufzunehmen, dass sie weder direkt noch indirekt die Standardvertragsklauseln einschränken.[347]

---

343 *Weichert*, DuD 2010, 679 (686).

344 *Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Orientierungshilfe – Cloud Computing, S. 10 f; *Schröder/ Haag*, ZD 2011, 147 (150).

345 *Bierekoven*, in: Bartsch/ Briner (Hrsg.), DGRI Jahrbuch 2010, S. 110.

346 *Schmidt-Bens*, Cloud Computing, S. 64.

347 *BITKOM/ VOICE*, Empfehlungen für den Cloud Computing-Standort Deutschland, S. 11

5.5.2 Regelungsmöglichkeiten im Fall C

Fraglich ist, wie im Fall C zu verfahren ist, wenn sich der Cloudanbieter in der EU befindet und erst der Unterauftragnehmer in einem unsicheren Drittstaat ansässig ist.

5.5.2.1 Analoge Anwendung der Standardvertragsklauseln

Fraglich ist, ob die Standardvertragsklauseln auch anwendbar sind, wenn ein in der EU niedergelassener Cloudnutzer einem ebenfalls in der EU niedergelassenen Cloudanbieter personenbezogene Daten übermittelt, der diese wiederrum an einen Unterauftragnehmer in einem Drittstaat transferiert. Die Artikel-29-Datenschutzgruppe verneint die Anwendung in diesem Fall und verweist auf den Erwägungsgrund 23 des Kommissionsbeschlusses, nach dem der Beschluss nur dann gelten solle, wenn sowohl der Cloudanbieter als auch der Unterauftragnehmer in einem Drittstaat ansässig sei und mit Verarbeitungstätigkeiten beauftragt werde. Begründet wird diese Ansicht mit der Definition des Datenimporteurs, der nach dem Kommissionsbeschluss außerhalb der EU niedergelassen zu sein habe. Weiterhin könne der in der EU niedergelassene Auftragsverarbeiter auch nicht als Datenexporteur im Sinne des Kommissionsbeschlusses angesehen werden, da dieser definitionsgemäß der für die Datenverarbeitung Verantwortliche sei. Darüber hinaus seien die Pflichten, die dem Datenimporteur im Kommissionsbeschluss auferlegt würden, für einen Auftragsverarbeiter aus einem EU-Staat nicht angemessen.[348] Dies gelte insbesondere für das anwendbare Datenschutzrecht, da nach dem Kommissionsbeschluss das Datenschutzrecht desjenigen Mitgliedsstaates Anwendung finde, in dem der Datenexporteur, demnach der Cloudnutzer, niedergelassen sei. Dies widerspreche den Vorgaben der EU-Datenschutz-Richtlinie und denen des Bundesdatenschutzgesetzes, nach denen bei Datenübermittlungen innerhalb der EU das Datenschutzrecht desjenigen Staates Anwendung finde, in dem die personenbezogenen Daten verarbeitet würden. Da die Vorgaben in den

[348] *Artikel-29-Datenschutzgruppe*, WP 176, S. 3.

Standardvertragsklauseln nicht modifiziert werden dürfen, scheidet ihre unmittelbare Anwendung somit für in der EU ansässige Cloudnutzer bei der Übermittlung personenbezogener Daten an Cloudanbieter aus EU-Staaten unter Einbeziehung weiterer Unterauftragnehmer aus Drittstaaten aus.

Da eine unmittelbare Anwendung der Standardvertragsklauseln ausscheidet, ist in der Literatur die analoge Anwendung der Standardvertragsklauseln diskutiert worden.[349] Für eine analoge Anwendung der Standardvertragsklauseln spricht, dass es keinen sachlichen Grund dafür gibt, Cloudanbieter aus Drittstaaten besser zu stellen als Cloudanbieter aus EU-Staaten. Eine analoge Anwendung würden sicherlich auch die Beteiligten im Rahmen des Cloud Computings begrüßen, weil sie anerkannte Regelungen darstellen und klare Vorgaben zur Unterbeauftragung enthalten.

Allerdings kann eine analoge Anwendung nur stattfinden, wenn eine planwidrige Regelungslücke vorliegt und die Interessenlagen im Fall B und Fall C als vergleichbar angesehen werden können. Eine planwidrige Regelungslücke liegt vor, wenn davon ausgegangen werden kann, dass der Gesetzgeber etwas nicht geregelt hat, was er aber erkennbar geregelt hätte, wenn er um die Regelungsbedürftigkeit wüsste.[350] Bereits im WP 161[351] hat die Artikel-29-Datenschutzgruppe über die damals im Entwurf vorliegenden Standardvertragsklauseln geäußert, dass diese aufgrund der expliziten Regelungen der Unterauftragsvergabe die Datenverarbeitung flexibilisierten, dieser Vorteil jedoch nicht für Auftragsverarbeiter aus EU-Staaten gelte, die Teile ihrer Datenverarbeitungen an Unterauftragnehmer in Drittstaaten übertragen möchten, wodurch europäischen Unternehmen Wettbewerbsnachteile entstehen würden, da sie größere verwaltungstechnische Hindernisse überwinden müssten als ihre Konkurrenten in Drittstaaten, um

349 *Lensdorf*, CR 2010, 735 (737).
350 *Lensdorf*, CR 2010, 735 (737).
351 *Artikel-29-Datenschutzgruppe*, WP 161, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp161_de.pdf, Stand: 7.6.2014

vergleichbare Leistungen anbieten zu können.[352] In diesem Zusammenhang forderte die Artikel-29-Datenschutzgruppe die EU-Kommission auf, ein neues Rechtsinstrument zu schaffen, das sich beispielsweise auch an den Standardvertragsklauseln orientieren könne.[353]

Es kann davon ausgegangen werden, dass die EU-Kommission spätestens seit der Stellungnahme im WP 161 um die Problematik wusste und eine Regelung des Falles C bewusst unterlassen hat, sodass nicht von einer planwidrigen Regelungslücke ausgegangen werden kann. Eine analoge Anwendung der Standardvertragsklauseln auf den Fall C ist somit nicht möglich.[354]

5.5.2.2 Alternative Vorschläge der Artikel-29-Datenschutzgruppe

Da eine analoge Anwendung der Standardvertragsklauseln im Fall C ausscheidet, stellt sich die Frage, wie in diesem Fall vorgegangen werden kann. Solange hierfür kein spezielles Instrument geschaffen worden ist, schlägt die Artikel-29-Datenschutzgruppe für die internationale Auftragsvergabe durch in der EU niedergelassene Auftragsverarbeiter an Unterauftragsverarbeiter in Drittstaaten drei Möglichkeiten vor.[355]

Der erste Vorschlag beinhaltet Direktverträge auf Basis der Standardvertragsklauseln zwischen dem in der EU niedergelassenen für die Verarbeitung Verantwortlichen, demnach dem Cloudnutzer und dem in einem Drittstaat ansässigen Unterauftragnehmer. Bei dieser Lösung würde der Unterauftragnehmer die Standardvertragsklauseln nicht als Unterauftragnehmer unterzeichnen, sondern als Datenimporteur im Sinne des Kommissionsbeschlusses. Der eigentliche Dienstleistungsvertrag über die Erbringung des Cloudservices zwischen dem Cloudnutzer und dem in der EU ansässigen Cloudanbieter hat nach

352 *Artikel-29-Datenschutzgruppe*, WP 161, S. 3.
353 *Artikel-29-Datenschutzgruppe*, WP 161, S. 3.
354 *Lensdorf*, CR 2010, 735 (738).
355 *Artikel-29-Datenschutzgruppe*, WP 176, S. 4.

diesem Vorschlag die Weisungen des Cloudnutzers gegenüber dem Cloudanbieter zu enthalten. Weiterhin hat er sämtlichen einschlägigen Bestimmungen aus Art. 16 und 17 EU-DSRL zu entsprechen.[356] Der eigentliche Dienstleistungsvertrag hat in Deutschland demnach den Vorgaben des § 11 BDSG zu entsprechen.

Dieser Lösungsvorschlag der Artikel-29-Datenschutzgruppe bietet auch im Rahmen des Cloud Computings eine Regelungsmöglichkeit für den Fall C, stößt jedoch auf praktische Probleme.[357] Für den Cloudnutzer ist es am bequemsten, einen Dienstleistungsvertrag mit dem Cloudanbieter einzugehen und sich einen Zustimmungsvorbehalt bei der Auswahl der Unterauftragnehmer zu sichern, anstatt mit jedem Unterauftragnehmer des Cloudanbieters selbst Verträge zu schließen. Der Cloudnutzer möchte die Cloudservices bequem und schnell nutzen können und möglichst nur einen Ansprechpartner auf der Seite des Cloudanbieters haben, sodass es nicht in seinem Sinn ist, Direktverträge mit den Unterauftragnehmern des Cloudanbieters zu schließen. Weiterhin wird es nicht in seinem Sinne sein, sich um die Auswahl der Unterauftragnehmer des Cloudanbieters zu kümmern, da er zum einen nicht weiß, welche Ressourcen der Cloudanbieter zur Erbringung des Cloudservices benötigt und zum anderen eine entsprechende Suche nach Unterauftragnehmer mit Aufwand und Kosten verbunden ist. Es ist leicht vorstellbar, dass dieser Aufwand sehr hoch werden kann, wenn es nicht um die Auswahl einiger weniger Unterauftragnehmer, sondern um eine Vielzahl an Unterauftragnehmern geht. Dies wird beim Cloud Computing regelmäßig der Fall sein. Es ist somit sehr aufwendig für den Cloudnutzer, die Unterauftragnehmer zu suchen und mit allen Unterauftragnehmern entsprechende Verträge zu schließen.

Aus diesen Gründen wird sich in der Praxis der Cloudanbieter selbst um die Auswahl der Unterauftragnehmer kümmern, da er auch am besten abschätzen können wird, welche Ressourcen er zur Erbringung

---

356 *Artikel-29-Datenschutzgruppe*, WP 176, S. 4.

357 *Bedner*, Cloud Computing, S. 245.

der von ihm angebotenen Cloudservices benötigt. Bei diesem Vorgehen besteht jedoch die Gefahr, dass der Cloudanbieter den Vertragsschluss mit dem Unterauftragnehmer verweigert und dadurch die Funktionsfähigkeit des Cloudservices in Gefahr gerät, wenn die Leistung des Unterauftragnehmers kritisch für die komplette Leistungserbringung ist.[358]

Der zweite Vorschlag der Artikel-29-Datenschutzgruppe[359] ähnelt dem ersten Vorschlag und bedeutet auf den Anwendungsfall des Cloud Computings übertragen, dass Cloudnutzer und Cloudanbieter eine Regelung im Dienstleistungsvertrag treffen, die den Cloudanbieter dazu berechtigt, im Namen des Cloudnutzers einen Vertrag auf Grundlage der Standardvertragsklauseln mit den einzelnen aus Drittstaaten stammenden Unterauftragnehmern zu schließen. Der Cloudnutzer ist demnach wie beim ersten Vorschlag als Datenexporteur und der Unterauftragnehmer als Datenimporteur i.S.d. Kommissionsbeschlusses tätig. Dieser Vorschlag wäre auch im Rahmen des Cloud Computings denkbar, da sich der Cloudnutzer zumindest nicht um die Vertragsabschlüsse mit den Unterauftragnehmern kümmern müsste, sondern dies vom Cloudanbieter im Namen des Cloudnutzers auf Basis der Standardvertragsklauseln erfolgen würde.[360] Jedoch bleibt zu bedenken, dass es nicht im Sinne aller Cloudnutzer sein dürfte, Cloudanbieter mit rechtsgeschäftlicher Vertretungsmacht auszustatten.

Der dritte Vorschlag sieht den Abschluss von Ad-hoc-Einzelfallverträgen vor. Die Artikel-29-Datenschutzgruppe verweist auf den zweiten Teil des Erwägungsgrundes 23 des Kommissionsbeschlusses über die Standardvertragsklauseln, nach dem es den Mitgliedsstaaten in dem Falle, in dem der Auftragsverarbeiter seinen Sitz in der EU habe und sich nur der Unterauftragnehmer in einem Drittstaat befinde, freistehe, ob sie die Tatsache berücksichtigten möchten,

358 *Bedner,* Cloud Computing, S. 245.
359 *Artikel-29-Datenschutzgruppe,* WP 176, S. 4.
360 *Bedner,* Cloud Computing, S. 246.

dass bei der Vergabe eines Verarbeitungsauftrags an einen solchen Unteraufragnehmer die in den Standardvertragsklauseln festzuschreibenden Grundsätze und Garantien mit dem Ziel zur Anwendung gebracht werden, die Rechte der von der Datenübermittlung zwecks Unterauftragsverarbeitung betroffenen Person angemessen zu schützen. Weiterhin weist die Artikel-29-Datenschutzgruppe darauf hin, dass ein derartiger Einzelvertrag die gleichen Prinzipien und Sicherheiten wie die Standardvertragsklauseln inklusive der Klausel 3 zur Drittbegünstigung enthalten müsse und für den Auftragsverarbeiter mit Sitz in der EU und den Unterauftragnehmer mit Sitz in einem Drittstaat dieselben Pflichten und Verantwortlichkeiten wie in den Standardvertragsklauseln gelten sollten. Hinsichtlich des Auftragsverarbeiters mit Sitz in der EU seien die Regelungen der EU-Datenschutz-Richtlinie zu beachten; weiterhin gelte hinsichtlich seiner zu ergreifenden technischen und sicherheitsrelevanten Maßnahmen das Recht seines Staates, während der in einem Drittstaat ansässige Unterauftragnehmer die Geltung des innerstaatlichen Rechts des für die Verarbeitung Verantwortlichen anzuerkennen habe.[361]

Dieser Lösungsvorschlag wäre auch im Rahmen des Cloud Computings möglich, allerdings hat er den Nachteil, dass die Standardvertragsklauseln nicht direkt zur Anwendung kommen, sondern ihre Prinzipien und Sicherheiten zur Herstellung eines angemessenen Datenschutzniveaus nur über entsprechende Regelungen in den Einzelverträgen Geltung erlangen. Die Einzelfallverträge bedürfen vor ihrer Anwendung einer Genehmigung durch die jeweilige Aufsichtsbehörde, sodass die eigentlichen Vorteile der Genehmigungsfreiheit und der einfachen Verwendung der Standardvertragsklauseln verloren gingen. Es besteht für den Cloudanbieter zwar die Möglichkeit, für jede Geschäftsbeziehung in der Kette die gleichen Verträge anzuwenden, sodass diese nur einmalig genehmigt werden bräuchten, nichts desto trotz sind diese Verträge erst einmal zu entwerfen und bei jeder Ab-

361 *Artikel-29-Datenschutzgruppe*, WP 176, S. 5; *Lensdorf*, CR 2010, 735 (739 f.).

weichung aufgrund individueller Vereinbarung erneut zur Genehmigung bei der jeweiligen Aufsichtsbehörde vorzulegen.[362]

Alle drei Lösungsvorschläge haben neben ihren spezifischen Unzulänglichkeiten, auch den Nachteil, dass bei der Vergabe von Unteraufträgen für jeden Unterauftrag ein gesonderter Vertrag abzuschließen wäre, was zu einer Vielzahl an Verträgen und zu einem hohen Verwaltungsaufwand führen dürfte.[363]

5.5.2.3 Processor Binding Corporate Rules

Eine weitere Möglichkeit, um die gem. § 4c Abs. 2 BDSG erforderlichen Garantien zum Schutz des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte nachzuweisen, bieten für konzernrechtlich mit ihren Unterauftragnehmern verbundene Cloudanbieter Binding Corporate Rules (BCR). Sie eigenen sich auch für Private Clouds in länderübergreifenden Konzernen.[364] BCR binden innerhalb einer internationalen Unternehmensgruppe alle Teilnehmer und sollen durch verbindliche Datenschutzstandards ein angemessenes Datenschutzniveau gewährleisten.[365]

Zwar finden BCR grundsätzlich keine ausdrückliche Erwähnung in der EU-Datenschutz-Richtlinie, jedoch sieht Art. 26 Abs. 2 EU-DSRL die Herstellung eines angemessenen Schutzniveaus im Wege von Vertragsklauseln vor, unter die auch die BCR zu zählen sind.[366] Im deutschen Recht sind diese ausdrücklich in § 4c Abs. 2 S. 1 HS. 2 BDSG erwähnt. Da das deutsche und europäische Datenschutzrecht kein Konzernprivileg beinhaltet, bietet die Etablierung von BCR eine Möglichkeit zum internen Datenaustausch innerhalb von Konzernen.[367] Der Vorteil der BCR ist, dass sie nicht nur interne Wirkung entfalten, son-

362 *Bedner*, Cloud Computing, S. 247.
363 *Filip*, ZD 2013, 51 (59).
364 *Karger/ Sarre*, in: Taeger/ Wiebe (Hrsg.), Inside the Cloud, S. 435; *Bierekoven*, in: Bartsch/ Briner (Hrsg.), DGRI Jahrbuch 2010, S. 118 f; *Weichert*, DuD 2010, 679 (686).
365 *Hoeren*, RDV 2012, 271 (274); *Grapentin*, CR 2009, 693 (693).
366 *Bedner*, Cloud Computing, S. 247; *Grapentin*, CR 2009, 693 (693 f.).
367 *Büllesbach*, Transnationalität und Datenschutz, S. 67; *Hoeren*, RDV 2012, 271 (271).

dern auch gegenüber dem Betroffenen als Garantiezusage gelten. Die an die BCR gebundenen Unternehmen verpflichten sich, die Daten des Betroffenen nach den in den BCR verankerten Grundsätzen zu behandeln, unabhängig davon, ob die Daten in der EU oder in einem Drittstaat verarbeitet werden.[368]

Im Juni 2012 sind die Processor BCR beschlossen worden.[369] Sie stellen interne Verhaltenskodizes zum Datenschutz und zur Datensicherheit dar, um den Transfer von personenbezogenen Daten außerhalb von EU-Staaten zwischen einem für die Verarbeitung Verantwortlichen und einem nach dessen Weisungen handelnden Auftragsverarbeiter in Übereinstimmung mit den Vorschriften der EU zum Datenschutz zu gestalten.[370] Sie können dem Dienstleistungsvertrags als Anhang beigefügt werden und sollen auch im Rahmen des Cloud Computings einsetzbar sein.[371] Processor BCR sollen es den Cloudanbietern ermöglichen, ihre Cloudservices auch gegenüber europäischen Cloudnutzern anzubieten, ohne hierbei ausschließlich Rechenzentren und Ressourcen innerhalb der EU nutzen oder komplexe individuelle Verträge mit jedem Unterauftragnehmer schließen zu müssen.[372] Die Processor BCR könnten sich somit zu einem Wettbewerbsvorteil für multinationale Cloudanbieter entwickeln.[373] Seit dem 1.1.2013 können die Processor BCR zur Genehmigung vorgelegt werden. Die wichtigsten Anforderungen und Kriterien für die Genehmigung, auch im Hinblick

---

368 *Büllesbach,* in: Klumpp et al. (Hrsg.), Medien, Ordnung und Innovation, S. 311.

369 *Artikel-29-Datenschutzgruppe,* WP 195, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_de.pdf, Stand: 7.6.2014

370 *Artikel-29-Datenschutzgrupp,* Pressemitteilung vom 21.12.2012, S. 1., abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20121221_pr_bcrs_en.pdf, Stand: 7.6.2014

371 *Artikel-29-Datenschutzgrupp,* Pressemitteilung vom 21.12.2012, S. 1; *Filip,* ZD 2013, 51 (59); *Artikel-29-Datenschutzgruppe,* WP 204, S. 5, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf, Stand: 7.6.2014; *Artikel-29-Datenschutzgruppe,* WP 196, S. 23.

372 *Marnau,* Could Processor BCR prove to be cloud-enabling in Europe?, abrufbar unter: http://www.tclouds-project.eu/index.php/tclouds-blog/blogger/listings/nmarnau, Stand: 7.6.2014

373 *Marnau,* Could Processor BCR prove to be cloud-enabling in Europe?

auf Unterbeauftragungen, sollen im Folgenden dargestellt und bewertet werden.

Die Vorgaben zur Unterauftragsverarbeitung regelt Genehmigungskriterium 6 vi) und vii). Nach Kriterium 6 vi) kann eine Verarbeitung durch Unterauftragnehmer, die der an die Processor BCR gebundenen Unternehmensgruppe angehören, erfolgen, wenn der für die Verarbeitung Verantwortliche, demnach der Cloudnutzer hierüber unterrichtet wurde und seine vorherige schriftliche Einwilligung erteilt hat. Demnach hat aus dem Dienstleistungsvertrag über die Erbringung des Cloudservices zwischen dem Cloudnutzer und dem Cloudanbieter als Auftragsverarbeiter hervorzugehen, ob eine generelle vorherige Einwilligung ausreichend ist oder ob eine separate Einwilligung für jede neue Unterverarbeitung erforderlich ist. Diese Regelung ist bereits aus den Standardvertragsklauseln bekannt. Im Fall der Erteilung einer generellen Einwilligung muss der Cloudnutzer über beabsichtigte Änderungen bei den Unterauftragnehmern informiert werden, damit er Einwände vortragen oder vom Vertrag zurückzutreten kann, bevor die Daten an einen neuen Unterauftragnehmer weitergeleitet werden. Auch die Weiterleitung personenbezogener Daten an externe Unteraufragnehmer der Unternehmensgruppe, die nicht an die Processor BCR gebunden sind, ist möglich. Sollen Unteraufträge an externe Unterauftragnehmer vergeben werden, so ist dies nur im Wege einer schriftlichen Vereinbarung zwischen ihm und dem an die Processor BCR gebundenen Cloudanbieter möglich, die dem externen Unterauftragsverarbeiter die gleichen Pflichten auferlegt, die auch für den Cloudanbieter nach den Regeln der Processor BCR und denen des Dienstleistungsvertrags gelten.

Eine der wichtigsten Regelungen in den Processor BCR ist die Haftungsregelung. Gemäß Kriterium 1.5 muss festgelegt werden, dass die EU-Hauptniederlassung des Auftragsverarbeiters bzw. das in der EU haftende Mitglied des Auftragsverarbeiters die Haftung für Handlungen anderer Gruppenmitglieder außerhalb der EU, die an die BCR gebunden sind, übernimmt und für Verstöße externer Unterauftragsver-

arbeiter außerhalb der EU einsteht. Das haftende Mitglied muss sich auch dazu bereit erklären, Schadensersatz zu leisten und Verstößen gegen die Processor BCR abzuhelfen. Es muss akzeptieren, dass es so haftet, als hätte es selbst gegen die Regelungen der Processor BCR im Staat seiner Niederlassung verstoßen und nicht die Mitglieder der Unternehmensgruppe oder die externen Unterauftragsverarbeiter außerhalb der EU. Es kann sich nicht der Haftung entziehen, indem es behauptet, dass ein Unterauftragsverarbeiter den Pflichtverstoß begangen habe. Sofern kein Mitglied des an die Processor BCR gebundenen Auftragsverarbeiters in der EU ansässig ist, hat die außerhalb der EU befindliche Hauptniederlassung der Unternehmensgruppe diese Haftung zu übernehmen. Damit soll sichergestellt werden, dass der Betroffene bei Datenschutzverstößen außerhalb der EU so behandelt wird als wenn die Daten in der EU verarbeitet worden wären.[374] Das haftende Unternehmen muss im Genehmigungsantrag nachweisen können, dass es über ausreichende Mittel verfügt, um Schäden, die aus der Verletzung der Processor BCR entstanden sind, ersetzen zu können. Eine klare Haftungsregelung ist insbesondere beim Cloud Computings notwendig, da sich das Haftungsgeflecht mit zunehmender Anzahl an Unterauftragnehmern verkompliziert und eindeutige Haftungsregelungen nur im Sinne der Cloudnutzer und Betroffenen sein können.

Weiterhin hat der Auftragsverarbeiter nach Kriterium 1.3 sicherzustellen, dass Betroffenen als Drittbegünstigen für den Fall Durchsetzungsrechte eingeräumt werden, in dem sie nicht mehr in der Lage sind, Ansprüche gegen den für die Verarbeitung Verantwortlichen geltend zu machen, weil er faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist. Die Rechte der Betroffenen betreffen gerichtliche Rechtsbehelfe bei Verstößen gegen garantierte Rechte und Schadensersatzansprüche. Diese Regelung entspricht im Wesentlichen Klausel 3 der Standardvertragsklauseln.

---

374 *Grapentin*, CR 2011, 102 (104).

Durch die Processor BCR sind auch Kooperationspflichten im multinationalen Unternehmen zu etablieren. So haben sich gem. Kriterium 3.1 alle an die Processor BCR gebunden Mitglieder dazu zu verpflichten, mit der Datenschutzbehörde, die für den für die Verarbeitung Verantwortlichen zuständig ist, zusammenzuarbeiten und ihre Prüfungen zu erdulden, sowie ihre Mitteilungen hinsichtlich der Anwendung der Processor BCR zu befolgen. Im Zusammenhang mit Cloud Computing ist davon auszugehen, dass Cloudanbieter ihre Services nicht nur deutschen, sondern auch anderen europäischen Cloudnutzern anbieten werden. Für den Cloudanbieter bedeutet dies eine Kooperation und Auseinandersetzung mit unterschiedlichen Datenschutzbehörden, was mit erhöhten Kosten und einem erhöhten Personalbedarf einhergehen dürfte.

Die Verpflichtung zur Kooperation wird auch in der Verpflichtung zu BCR-Audits deutlich. Die BCR-Audits sind nach dem Genehmigungskriterium 2.3 durch interne oder externe akkreditierte Auditoren durchzuführen und haben sich auf alle Aspekte der BCR zu erstrecken. Das Ergebnis ist neben internen Stellen auch dem für die Verarbeitung Verantwortlichen und auf Antrag auch der für diesen zuständigen Datenschutzbehörde zugänglich zu machen. Hier wird deutlich, dass ein gewisses Maß an Standardisierung im Auditverfahren nötig ist, um die intensive Kooperation und Zusammenarbeit mit den unterschiedlichen Datenschutzbehörden umsetzen zu können.[375] Problematisch im Zusammenhang mit Cloud Computing könnte sich eine weitere Anforderung an das Auditverfahren gestalten, nach der Auftragsverarbeiter und Unterauftragnehmer verpflichtet sind, ihre „Datenverarbeitungseinrichtungen zur Prüfung derjenigen Datenverarbeitungstätigkeiten zur Verfügung zu stellen, die mit dem betreffenden, für die Verarbeitung Verantwortlichen zu tun haben," wenn dieser es verlangt. Dabei soll der für die Verarbeitung Verantwortliche selbst oder ein von ihm ausgewähltes unabhängiges Prüfgremium das Auditverfahren durchführen.

---

375 *Marnau,* Could Processor BCR prove to be cloud-enabling in Europe?

In der Literatur ist geäußert worden, dass sich Cloudanbieter häufig nicht auf Überprüfungen ihrer Datenverarbeitungseinrichtungen durch die Nutzer ihrer Services einlassen würden, weil sie um die Sicherheit ihrer Anlagen, die Datensicherheit und ihre Geschäftsgeheimnisse fürchteten und es daher bevorzugten, die genauen Standorte ihrer Rechenzentren geheim zu halten.[376] Vor diesem Hintergrund ist es fraglich, ob die Cloudanbieter und Unterauftragnehmer gewillt sind, die Anforderungen der Processor BCR hinsichtlich des Auditverfahrens zu erfüllen. Dem Cloudnutzer wird es bei großen multinationalen Cloudanbietern kaum möglich sein, solchen Prüfungen selbst nachzukommen, weshalb auch hier auf unabhängige und geprüfte Auditoren zurückgegriffen werden sollte.

Eine Pflicht zur Zusammenarbeit besteht für Auftragsverarbeiter und Unterauftragnehmer auch mit dem für die Verarbeitung Verantwortlichen. So soll das Vertragsverhältnis zwischen dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Unterauftragnehmern von Transparenz und Fairness gezeichnet sein. Ausdruck dessen kann sein, die Tätigkeiten der Unterauftragnehmer transparent zu machen, damit der für die Verarbeitung Verantwortliche die Betroffenen ordnungsgemäß unterrichten kann. Ein Transparenzproblem besteht in jedem Fall auch beim Cloud Computing, sodass es zu begrüßen ist, dass der Transparenzgedanke als Genehmigungskriterium auch in den Processor BCR Einklang gefunden hat.

Die Regelungen der Processor BCR haben im Rahmen des Cloud Computings für multinationale Cloudanbieter den Vorteil, dass sie überhaupt die Multilateralität regeln und die Beauftragung von Unterauftragnehmern, die in die Processor BCR eingebunden sind, vergleichsweise einfach gelöst werden kann. Auch ist es von Vorteil, dass einmal genehmigte Processor BCR genutzt werden können, ohne dass Schutzmaßnahmen und Bedingungen der Datenverarbeitung mit jedem Unterauftragnehmer neu auszuhandeln sind,[377] weil neue Mit-

376 *Niemann/ Hennrich,* CR 2010, 686 (690); *Bedner,* Cloud Computing, S. 50.
377 *Hladjik,* DSB 2013, S. 42.

glieder der Unternehmensgruppe, die als Unterauftragnehmer fungieren sollen, den Processor BCR einfach beitreten können. Die Kriterien, die vom Auftragsverarbeiter und den übrigen Gruppenmitgliedern erfüllt werden müssen, sind jedoch nicht zu unterschätzen. So ist es beispielsweise fraglich, ob kleinere Cloudanbieter die Anforderungen zur Haftung oder zum Bonitätsnachweis erfüllen können. Weiterhin bleibt die Frage ungelöst wie mit den Anforderungen des nationalen Rechts umzugehen ist, wenn die Cloudnutzer aus unterschiedlichen EU-Staaten kommen.

5.5.3 Regelungsmöglichkeiten im Fall D

Auch für den Fall D, in dem ein deutsches Unternehmen als Cloudnutzer einen Service von einem in einem Drittstaat ansässigen Cloudanbieter nutzt und sich dieser in der EU ansässiger Unterauftragnehmer zur Leistungserbringung gegenüber dem Nutzer bedient, existiert kein spezielles Instrument zur Regelung, sodass erneut auf die Handreichung des Düsseldorfer Kreises zur internationalen Auftragsdatenverarbeitung zurückzugreifen ist.

In diesem Fall wird neben dem Abschluss eines Dienstleistungsvertrags, auch der Abschluss des EU-Standardvertrags 2010/87/EU zwischen dem Cloudnutzer und dem Cloudanbieter im Drittstaat empfohlen. Da Zweck und Umfang der zulässigen Datenverarbeitung, sowie die einzuhaltenden Datensicherungsmaßnahmen bereits aus dem Vertrag zwischen Cloudnutzer und Cloudanbieter hervorgehen, soll der Unterauftragnehmer diesem Vertrag beitreten, nachdem der Cloudnutzer dem Unterauftragnehmer zugestimmt hat.[378]

Auch im Rahmen des Cloud Computings wäre dieser Lösungsweg möglich, jedoch besteht wie bei Beitritten zu bestehenden Verträgen generell das Problem, dass dem Unterauftragnehmer der gesamte Ver-

---

[378] *Düsseldorfer Kreis,* Fallgruppen der internationalen Auftragsdatenverarbeitung, S. 6, abrufbar unter: http://www.datenschutz-berlin.de/attachments/456/HandreichungApril2007.pdf?1208354740, Stand: 7.6.2014; *Eul/Eul,* Datenschutz International, S. 55.

trag, inklusive der Standardvertragsklauseln, offenzulegen ist.[379] Somit entsteht ein Spannungsfeld zwischen den Interessen des Unterauftragnehmers, der nicht nur die Standardvertragsklauseln, sondern den gesamten Vertrag sehen möchte, weil dieser noch weitere ihn betreffende Regelungen enthalten kann und den Interessen des Cloudnutzers und des Cloudanbieters, die nicht alle Einzelheiten des Dienstleistungsvertrags offenlegen möchten.

5.6 Zwischenfazit zur Datenübermittlung ins außereuropäische Ausland

Die Ausführungen haben gezeigt, dass die Nutzung internationaler Cloudservices einige datenschutzrechtliche Hürden bereithält. Die Schwierigkeiten fangen damit an, dass das Bundesdatenschutzgesetz keine privilegierte Auftragsdatenverarbeitung nach Maßgabe des § 11 BDSG bei Datenempfängern außerhalb der EU zulässt und daher immer eine Datenübermittlung im Sinne des § 3 Abs. 4 Nr. 3 BDSG vorliegt, die für ihre Zulässigkeit eines gesetzlichen Erlaubnistatbestandes bedarf. Es ist gezeigt worden, dass § 28 Abs. 1 S. 1 Nr. 2 BDSG nur bedingt als Erlaubnistatbestand im Rahmen des Cloud Computings in Frage kommt, da es in Anbetracht der zahlreichen Angebote rein europäischer Clouds, meist an der Erforderlichkeit der Nutzung einer internationalen Cloud fehlen wird und auch wenn diese bejaht wird, die Interessenabwägung häufig zugunsten des schutzwürdigen Persönlichkeitsrechts des Betroffenen ausfällt, sodass die Übermittlung zu unterbleiben hat. Sollte man in seltenen Fällen feststellen, dass die schutzwürdigen Interessen des Betroffenen nicht überwiegen, muss das Datenschutzniveau beim Cloudanbieter und dessen Unterauftragnehmern beurteilt werden.

Für viele Länder hat die EU-Kommission Adäquanzentscheidungen vorgelegt, jedoch fehlen hier IT-Nationen wie Indien oder China, die

---

379 *BITKOM*, Fallgruppen zur internationalen Auftragsdatenverarbeitung und abgestimmte Position der Aufsichtsbehörden, S. 6, abrufbar unter: http://www.bitkom.org/files/documents/BITKOM_Echo_Duesseldorfer_Kreis_Int__ADV.pdfStand: 7.6.2014

voraussichtlich auch am weltweiten Cloud Computing Markt verstärkt partizipieren werden, sodass die Adäquanzentscheidungen beim Cloud Computing nur bedingt weiterhelfen. Die Safe Harbor Zertifizierung hat für das Cloud Computing eine besondere Bedeutung, da US-Cloudanbieter sehr stark am Markt vertreten sind und überwiegend auch über eine Safe Harbor Zertifizierung verfügen. Jedoch schützt eine Safe Harbor Zertifizierung nicht vor dem Datenzugriff von US-Ermittlungsbehörden und Geheimdiensten auf Grundlage des USA Patriot Acts und durch die Feststellung des Düsseldorfer Kreises kommen auf den Cloudnutzer umfangreiche Prüfungs- und Dokumentationspflichten zu, die den „Wert" dieser Zertifizierung relativieren. Da auch die gesetzlichen Ausnahmetatbestände aus § 4c Abs. 1 S. 1 BDSG im Regelfall für das Cloud Computing nicht einschlägig sein werden, muss beim Cloudanbieter und Unterauftragnehmer in einem Drittstaat ein angemessenes Schutzniveau hergestellt werden. Hierzu kommen grundsätzlich die in § 4c Abs. 2 BDSG genannten Instrumente in Betracht.

Da beim Cloud Computing nicht nur der Cloudanbieter Zugang zu personenbezogenen Daten erhält, sondern auch die an der Erbringung des Cloudservices beteiligten Unterauftragnehmer, muss bei den zur Verfügung stehenden Instrumenten zur Herstellung eines angemessenen Schutzniveaus danach differenziert werden, wo Cloudanbieter und Unterauftragnehmer mit ihren Rechenzentren ansässig sind, um gegebenenfalls das passende Instrument auswählen zu können. Es ist gezeigt worden, dass im Fall B, der die häufigste Konstellation des Cloud Computings widerspiegelt, die Standardvertragsklauseln für Auftragsverarbeiter angewandt werden können und diese durch ihre detaillierte Regelung zur Unterauftragsvergabe auch einen durchaus gangbaren Weg darstellen. Die EU-Kommission hat zudem angekündigt, die Standardvertragsklauseln an die Belange des Cloud Computings anzupassen, wenn es die Praxis erforderlich machen sollte.[380]

---

[380] *Europäische Kommission,* Freisetzung des Cloud-Computing-Potentials in Europa, S. 15.

Die Regelungsmöglichkeiten im Fall C und D gestalten sich indes schwieriger, da keine spezifischen Instrumente zur Verfügung stehen und auch eine analoge Anwendung der Standardvertragsklauseln ausscheidet, sodass in den meisten Fällen nur nach den Vorschlägen der Artikel-29-Datenschutzgruppe verfahren werden kann, diese jedoch alle mit Nachteilen verbunden sind, sodass sich der Forderung nach einem für den Fall C einsetzbaren Instrument, ähnlich der Standardvertragsklauseln, angeschlossen werden kann.[381]

Das neu zu schaffende Instrument sollte die Unterauftragsvergabe ebenfalls von der Einwilligung des Cloudnutzers abhängig machen und dem Unterauftragnehmer die gleichen datenschutzrechtlichen Verpflichtungen auferlegen wie dem Cloudanbieter. Dem Cloudnutzer muss das Recht eingeräumt werden, die Einhaltung dieser Verpflichtungen mit technischen Mitteln oder unter Zuhilfenahme von Auditoren überprüfen zu dürfen. Letztendlich kann es nicht im Sinne des Europäischen Gesetzgebers sein, europäische Cloudanbieter, die Aufträge an Unternehmen in Drittstaaten vergeben wollen, mit komplizierten Vertragsgeflechten zu belasten, da Komplexität im Zweifel mit negativen Folgen für den Schutz personenbezogener Daten einhergeht[382] und es nicht ersichtlich ist, warum Cloudanbieter aus Drittstaaten die Standardvertragsklauseln nutzen können sollen und europäische Cloudanbieter nicht.

Für Cloudanbieter, die konzernrechtlich mit ihren Unterauftragnehmern verbunden sind, bietet sich die Implementierung von Processor BCR an, die hinsichtlich der Unterauftragsvergabe den Standardvertragsklauseln sehr ähnlich sind, jedoch noch weitergehende Anforderungen enthalten. So sehen die Processor BCR vor, dass Bonitätsnachweise erbracht werden müssen und ein Mitarbeiterstab zu bilden ist, der die Einhaltung der Processor BCR überwacht. Weiterhin sind die Mitarbeiter zur Anwendung der Processor BCR zu schulen. Derartige

---

381 So auch: *BITKOM/ VOICE,* Empfehlungen für den Cloud Computing-Standort Deutschland, S. 11; *Lensdorf,* CR 2010, 735 (737).

382 *Lensdorf,* CR 2010, 735 (740).

Anforderungen sind in den besagten Standardvertragsklauseln nicht enthalten. Aufgrund dieser Anforderungen und den strengeren Haftungsregelungen, wird es für kleinere Cloudanbieter schwierig sein, Processor BCR implementieren zu können. Für größere konzernrechtlich verbundene Cloudanbieter sind sie jedoch ein Fortschritt, der zu begrüßen ist, auch wenn es im Rahmen des Cloud Computings seltener der Fall sein dürfte, dass der Cloudanbieter und all seine Unterauftragnehmer derselben Unternehmensgruppe angehören.[383]

Gegenüber den Standardvertragsklauseln haben sie zudem den Vorteil, dass sie anhand der Kriterien individuell für die Unternehmensgruppe gestaltet werden können. Dies stellt jedoch auch einen Nachteil dar, da sie zunächst einmal von den zuständigen Behörden genehmigt werden müssen und sich dies als langwierig gestalten kann. Nichtsdestotrotz sind einmal genehmigte Processor BCR als Fortschritt zu werten, da sie als ausreichende Garantien zum Schutz von personenbezogenen Daten gelten und auch im gesamten Konzern standortunabhängig Anwendung finden, sodass ihre Anwendung in allen hier geschilderten Fällen möglich ist, sofern Cloudanbieter und Unterauftragnehmer konzernverbunden sind.

383 *Filip*, ZD 2013, 51 (59).

6 Regelungen im Entwurf zur Datenschutz-Grundverordnung

Im Folgenden soll der Entwurf zur Datenschutz-Grundverordnung (DS-GVO-E)[384] vom 25.01.2012 im Hinblick auf den Anwendungsfall des Cloud Computings betrachtet werden. Gemäß Erwägungsgrund 13 der DS-GVO-E soll der Schutz der natürlichen Personen technologieneutral bleiben, weshalb der Entwurf auch keine cloudspezifischen Regelungen enthält. Jedoch sind die vorgeschlagenen Regelungen des Entwurfs auch für das Cloud Computing als Querschnittsmaterie von hoher Bedeutung.[385] Gemäß Art. 88 Abs. 1 DS-GVO-E würde der Entwurf die bisherige EU-Datenschutz-Richtlinie aufheben.

Eine wichtige Neuerung enthalten die Regelungen über den räumlichen Anwendungsbereich in Art. 3 DS-GVO-E. Gemäß Art. 3 Abs. 2 lit. a DS-GVO-E sollen auch Verantwortliche außerhalb der EU erfasst werden, wenn ihre Datenverarbeitung dazu dient, in der EU ansässigen Personen Waren oder Dienstleistungen in der EU anzubieten. Im Zweipersonenverhältnis zwischen dem Cloudanbieter und dem Betroffenem selbst wird dies der Fall sein, wenn Cloudanbieter außerhalb der EU, ihre Angebote direkt an den europäischen Markt richten. Zu einer Anwendbarkeit des Entwurfs der Datenschutz-Grundverordnung für den außereuropäischen Cloudanbieter würde es jedoch nicht kommen, wenn beispielsweise ein deutsches Unternehmen die Daten seiner Kunden und Mitarbeiter in eine Cloud auslagert, da dieses Angebot nicht dazu dient, den betroffenen Kunden und Mitarbeitern Waren oder Dienstleistungen anzubieten.[386] Somit wird bei der Anwendbarkeit des Entwurfs der Datenschutz-

384 *Europäische Kommission,* Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF, Stand: 7.6.2014

385 *Hornung/ Sädtler,* CR 2012, 636 (639).

386 *Hornung/ Sädtler,* CR 2012, 636 (640).

Grundverordnung danach unterschieden, ob der Cloudnutzer der einzige von der Datenübermittlung Betroffene ist oder nicht.

6.1 Datenverarbeitung in Drittstaaten

Gemäß Art. 40 DS-GVO-E ist die Übermittlung von Daten an Drittstaaten zulässig, sofern der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter die Bestimmungen der Datenschutz-Grundverordnung einhalten. Eine Übermittlung an Drittstaaten kann nur stattfinden, wenn das Datenschutzniveau dort als angemessen angesehen werden kann. Liegt ein Angemessenheitsbeschluss gem. Art. 41 DS-GVO-E vor, so ist die Übermittlung zulässig. Ansonsten kann die Übermittlung aufgrund der in Art. 44 DS-GVO-E genannten Ausnahmen zulässig sein. In den meisten Anwendungsfällen des Cloud Computings kommen diese Ausnahmen jedoch nicht in Betracht, da die Vorteile des Cloud Computing, entsprechend § 4c Abs. 1 S. 1 Nr. 2 BDSG im deutschen Recht, auch im Falle des Art. 44 Abs. 1 lit. b DS-GVO-E nicht als „für die Erfüllung eines Vertrags erforderlich angesehen werden können."[387] Ebenso scheidet der Ausnahmetatbestand aus Art. 44 Abs. 1 lit. h DS-GVO-E aus, da die Übermittlungen im Rahmen des Cloud Computings regelmäßig einen häufigen oder massiven Umfang annehmen werden.[388] Eine weitere Möglichkeit, um ein adäquates Datenschutzniveau herzustellen, besteht auf der Grundlage geeigneter Garantien, zu denen gem. Art. 42 Abs. 2 a-d DS-GVO-E genehmigungsbedürftige BCR, von der EU-Kommission oder von Aufsichtsbehörden angenommene Standardschutzklauseln und Vertragsklauseln zählen.

Art. 43 DS-GVO-E sieht BCR für Unternehmensgruppen vor, deren Mitglieder entweder als verantwortliche Stellen agieren oder mit Auftragsverarbeitungen befasst sind. Somit greift der Entwurf der Datenschutz-Grundverordnung die von der Artikel-29-Datenschutzgruppe im WP 195 niedergelegte Ausweitung dieses Rechtsinstruments auf

---

387 *Hornung/ Sädtler*, CR 2012, 636 (643).
388 *Hornung/ Sädtler*, CR 2012, 636 (643).

Auftragsverarbeiter auf.[389] Es wird daher erwartet, dass die Bedeutung der Binding Corporate Rules in der Praxis deutlich zunehmen könnte.[390] Da BCR im Rahmen des Cloud Computings nur dann bedeutsam sind, wenn sowohl der Auftragsverarbeiter als auch die Unterauftragnehmer einer Unternehmensgruppe angehören und dies in der Praxis vergleichsweise selten der Fall sein dürfte, können sie das Problem des Drittstaatentransfers nicht komplett beseitigen.[391]

Neu in diesem Zusammenhang ist, dass Standarddatenschutzklauseln nun auch von Aufsichtsbehörden in einem Kohärenzverfahren nach Art. 57 ff. DS-GVO-E festgelegt und von der EU-Kommission für gültig erklärt werden können. Ob in Zukunft Standarddatenschutzklauseln erlassen werden, die anders als die EU-Standardvertragsklauseln 2010/87/EU alle Auftrags- und Unterauftragsverarbeiter erfassen und nicht nur den Fall, in dem beide Beteiligte im außereuropäischen Ausland ansässig sind, bleibt abzuwarten. Dahingehende Forderungen werden von der Wirtschaft verständlicherweise geäußert.[392] Es bleibt abzuwarten, welchen Anklang diese Instrumente in der Praxis finden werden, jedoch können positive Rückmeldungen aus der Wirtschaft verzeichnet werden. So bietet Microsoft mittlerweile für zwei seiner Cloudservices den Abschluss von Standardvertragsklauseln in Verbindung mit einer standardisierten Auftragsdatenverarbeitungsvereinbarung an.[393]

Gemäß Erwägungsgrund 79 DS-GVO-E bleiben internationale Abkommen zwischen der EU und Drittstaaten über die Übermittlung personenbezogener Daten von der Verordnung unberührt, sodass die Übermittlung in die USA an Safe Harbor zertifizierte Unternehmen

---

389 *Filip*, ZD 2013, 51 (59); *Lang*, K&R 2012, 145 (148).

390 *Hornung*, ZD 2012, 99 (102).

391 *Hornung/ Sädtler*, CR 2012, 636 (644).

392 *BITKOM/ VOICE*, Empfehlungen für den Cloud Computing-Standort Deutschland, S. 10.

393 *Microsoft*, CRM in der Cloud: Microsoft baut Führung beim Datenschutz weiter aus, http://www.microsoft.com/de-de/kmu/Produkte/Seiten/Microsoft-CRM-Online.aspx, Stand: 7.6.2014

wie bisher unter denselben Voraussetzungen möglich bleiben soll, was angesichts der dargestellten Mängel dieser Zertifizierung enttäuscht. Weiterhin enttäuschend ist, dass das Dilemma um Herausgabeverpflichtungen gegenüber US-Behörden im Rahmen des USA Patriot Acts bei Daten, die bei amerikanischen Cloudanbietern lagern in diesem Entwurf der Datenschutz-Grundverordnung nicht angegangen worden ist. Ein früher Entwurf[394] sah in Art. 42 Abs. 2 DS-GVO-E noch eine Genehmigungspflicht der eigenen Aufsichtsbehörde vor, wenn ausländische Gerichte oder Behörden die Offenlegung von Daten anordnen. Die Streichung dieser Regelung kann aus europäischer Sicht sicherlich als Rückschritt betrachtet werden.[395] Da der Entwurf die ursprünglich angedachte Regelung gar nicht mehr enthält, wäre es erfreulich gewesen, wenn der Entwurf zumindest eine Verpflichtung an ausländische Cloudanbieter, insbesondere aus den USA, vorsehen würde, ihre Kunden über die Offenbarungsanordnung zu informieren, da dies im Moment scheinbar nur geschieht, „wo immer es möglich ist."[396]

6.2 Auftragsdatenverarbeitung

Die wesentlichen Vorschriften zur Auftragsdatenverarbeitung finden sich in Art. 26 DS-GVO-E, der weitgehend den Inhalt eines Auftragsdatenverarbeitungsvertrags vorgibt. Eine Neuregelung bei Verstößen gegen den Auftragsdatenverarbeitungsvertrag sieht Art. 26 Abs. 4 DS-GVO-E vor, der in diesem Fall den Auftragsverarbeiter zum für die Verarbeitung Verantwortlichen erklärt. Im Übrigen entspricht Art. 26 DS-GVO-E weitgehend § 11 BDSG,[397] wobei bemängelt wird, dass Angaben zum Gegenstand und zur Dauer des Auftrags, zum

---

394 *European Commission,* Proposal for a General Data Protection Regulation, Version 56 (29.11.2011), abrufbar unter: http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf, Stand: 7.6.2014

395 *Hornung,* ZD 2012, 99 (102).

396 *Sawall,* Europäische Cloud-Daten nicht vor US-Zugriff sicher, abrufbar unter: http://www.golem.de/1106/84620.html, Stand: 7.6.2014

397 *Lang,* K&R 2012, 145 (149); *Hornung/ Sädtler,* CR 2012, 636 (640); *Wybitul/ Fladung,* BB 2012, 509 (512); *Deutlmoser/ Filip,* ZD-Beilage 6/12, S. 9

Umfang, zu Art und Zweck der Verarbeitung, zur Datenart und zum Kreis der Betroffenen nicht verlangt werden.[398]

Dem Cloudnutzer als dem für die Verarbeitung Verantwortlichen stehen gem. Art. 26 Abs. 2 lit. a DS-GVO-E auch weiterhin Weisungsbefugnisse zu und er hat sich gem. lit. h von der Einhaltung der Pflichten zu überzeugen. Zu der Frage, ob der Cloudnutzer zur Prüfung vor Ort verpflichtet ist, enthält der Datenschutz-Grundverordnungsentwurf keine Regelung. Da einer derartigen Pflicht jedoch in der Praxis, insbesondere gegenüber international operierenden Cloudanbietern ohnehin nicht nachgekommen werden kann, sollte sie auch nicht gefordert werden. Stattdessen sollte diesbezüglich auf zertifizierte Kontrollmechanismen gesetzt werden, die jedoch in Bezug auf die Auftragsdatenverarbeitung im Entwurf zur Datenschutz-Grundverordnung keine Erwähnung finden.[399]

Eine eigene Regelung bezüglich der Einschaltung von Subunternehmern findet sich in Art. 26 Abs. 2 d DS-GVO-E, der für die Einschaltung von Subunternehmern die vorherige Zustimmung des für die Verarbeitung Verantwortlichen, demnach des Cloudnutzers, voraussetzt. Dies gilt auch für die Datenverarbeitung in Unternehmensgruppen.[400] Wie bereits geschildert, ist die Frage der Unterbeauftragung auch in den EU-Standardvertragsklauseln 2010/87/EU sowie in den Processor BCR ähnlich geregelt. Ob die vorherige Zustimmung nach dem Entwurf der Datenschutz-Grundverordnung generell oder für jede einzelne Unterauftragsvergabe einzeln erteilt werden kann, wird nicht deutlich. In der Literatur wird die Meinung vertreten, dass zumindest die Unterauftragnehmer zu benennen sind, da ansonsten der

---

398 *GDD*, Stellungnahme zum Vorschlag für eine EU-Datenschutz-Grundverordnung, S. 12, abrufbar unter: https://www.gdd.de/nachrichten/arbeitshilfen/Stellungnahme%20DS-GVO-E%20endgx.pdf., Stand: 7.6.2014; *Nebel/ Richter*, ZD 2012, 407 (411).

399 *Hornung/ Sädtler*, CR 2012, 636 (643); *Borges*, DuD 2014, 165 (168).

400 *Lang*, K&R 2012, 145 (149).

durch Art. 26 Abs. 1 DS-GVO-E normierte Sorgfaltsmaßstab bei der Auswahl der Auftragsverarbeiter ausgehebelt werden würde.[401]

Den Auftragsverarbeiter treffen darüber hinaus noch weitere Pflichten. So haben sie gem. Art. 30 DS-GVO-E technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu treffen, gem. Art. 35 Abs. 1 DS-GVO-E einen Datenschutzbeauftragten zu benennen, sie sind gem. Art. 28 DS GVO-E zur Dokumentation verpflichtet und müssen gem. Art. 31 Abs. 2 DS-GVO-E über Datenpannen informieren.

6.3 Stand des Gesetzgebungsverfahrens

Nachdem der federführende LIBE-Ausschuss des EU-Parlaments im Oktober 2013 eine Kompromissfassung zum Entwurf der Datenschutz-Grundverordnung verabschiedet hatte, hat das EU-Parlament dieser Fassung am 12.03.2014 in erster Lesung zugestimmt.[402] Mit dieser Fassung tritt das EU-Parlament in die weiteren Verhandlungen, die nach der EU-Wahl im Rahmen des Trilog-Verfahrens zwischen dem EU-Parlament, dem Rat der europäischen Union und der EU-Kommission aufgenommen werden sollen.

Die Kompromissfassung des Datenschutz-Grundverordnungs-Entwurfs (DS-GVO-EK) enthält im Vergleich zur ursprünglichen, von der EU-Kommission vorgelegten Fassung, zahlreiche Änderungen, die auch für das Cloud Computing relevant werden würden, sodass diese kurz vorgestellt werden sollen.

Änderungen lassen sich bei den Regelungen zur Auftragsdatenverarbeitung feststellen. Wie auch schon im Kommissionsentwurf regelt Art. 26 DS-GVO-EK die Auftragsdatenverarbeitung und gibt eine Rei-

---

401 *Hornung/ Sädtler*, CR 2012, 636 (643).

402 *Europäisches Parlament,* Legislative Entschließung des Europäischen Parlaments vom 12. März zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung), P7_TA-PROV(2014)0212, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE, Stand: 7.6.2014.

he von Punkten vor, die zwischen Auftraggeber und Auftragsnehmer zu vereinbaren sind. Anders als in der ursprünglichen Fassung verlangt Art. 26 Abs. 2d DS-GVO-EK, dass der Einsatz von Unterauftragnehmern nicht nur von der Zustimmung des für die Verarbeitung Verantwortlichen abhängt, sondern dass auch die Bedingungen, unter denen diese eingesetzt werden dürfen, festzulegen sind. Dies gilt solange nichts anderes durch Rechtsvorschriften der Mitgliedsstaaten oder der EU bestimmt ist. Die vorherige Festlegung dieser Bedingungen kann sich beim Cloud Computing schwierig gestalten, da zu Anfang des Vertragsverhältnisses nicht immer vorhergesagt werden kann, ob und wie viele Unterauftragnehmer für die Erbringung des Cloudservices nötig sein werden.

Während der ursprüngliche Entwurf der EU-Kommission keine Regelung vorgesehen hatte, nach der sich der für die Verarbeitung Verantwortliche beim Auftragsverarbeiter ein Recht einräumen lassen musste, die Einhaltung der Regelungen des Art. 26 DS-GVO-EK vor Ort nachprüfen zu können, sieht Art. 26 Abs. 2h DS-GVO-EK genau dieses Recht vor. Es ist bereits erläutert worden, dass die Durchführung von Vor-Ort-Kontrollen aufgrund der Vielzahl der Beteiligten auf der Seite des Cloudanbieters und der verteilten Ressourcen beim Cloud Computing kaum handhabbar ist. Wird diese Regelung geltendes Recht, sind praktische Umsetzungsprobleme vorprogrammiert. Neu ist ebenfalls die Regelung in Art 26 Abs. 3a DS-GVO-EK, nach der die in Art. 26 Abs. 1 DS-GVO-EK geforderten „hinreichenden Garantien“ für die Zuverlässigkeit des Auftragsverarbeiters durch die Einhaltung von Verhaltenskodizes und das Durchlaufen von Zertifizierungsverfahren gem. Art 38 und 39 DS-GVO-EK nachgewiesen werden können. Für den Anwendungsfall des Cloud Computings wären derartige Nachweismöglichkeiten grundsätzlich positiv zu bewerten.

In der Kompromissfassung des EU-Parlaments haben auch Zertifizierungen eine ausführlichere Regelung erfahren. Art. 39 DS-GVO-EK regelt, dass jeder für die Verarbeitung Verantwortliche und Auftragsverarbeiter bei der zuständigen Aufsichtsbehörde eine Zertifizie-

rung beantragen kann, die die Übereinstimmung der durchgeführten Datenverarbeitungen mit den Regelungen der Datenschutz-Grundverordnung bestätigt. Wird diese Übereinstimmung einer Stelle bescheinigt, so soll diese ein europäisches Datenschutzsiegel tragen dürfen. Es ist vorgesehen, dass die Europäischen Aufsichtsbehörden und der Europäische Datenschutzausschuss im Rahmen des Kohärenzverfahrens zusammenarbeiten, um ein harmonisiertes Zertifizierungsverfahren zu gewährleisten. Im Rahmen des Cloud Computings ist die Notwendigkeit von einheitlichen europäischen Zertifikaten bereits festgestellt worden, sodass Art. 39 DS-GVO-EK grundsätzlich zu begrüßen ist. Vermissen lässt die Kompromissfassung des Verordnungsentwurfs allerdings konkrete Anforderungen und Kriterien für das Zertifizierungsverfahren sowie Bedingungen für die Akkreditierung der Prüfer, die von der EU-Kommission nach Anhörung unterschiedlicher Stellen im Rahmen eines delegierten Rechtsakts festgelegt werden sollen. Kritisiert wird ebenfalls, dass die Zertifizierung ausschließlich den Aufsichtsbehörden vorbehalten werden soll.[403]Abzuwarten bleibt wann diese Ankündigungsgesetzgebung tatsächlich ein einheitliches europäisches Datenschutzsiegel hervorbringen wird.

Eine Änderung hat auch Art. 43 DS-GVO-EK erfahren, der die Datenverarbeitung in Drittstaaten aufgrund von Binding Corporate Rules für Unternehmensgruppen regelt. Während der ursprüngliche Verordnungsvorschlag nur den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter einbezog, sieht. Art. 43 Abs. 1a DSGVO-EK nun vor, dass sich die verbindlichen unternehmensinternen Vorschriften auch auf externe Unterauftragnehmer beziehen können, denen im Rahmen des Cloud Computings eine wichtige Rolle zukommt.

Im Vergleich zum Kommissionsentwurf neu aufgenommen ist Art. 43a DS-GVO-EK. Art. 43a Abs. 1 DS-GVO-EK stellt klar, dass Gerichtsurteile und Entscheidungen von Verwaltungsbehörden aus Drittstaaten, die den für die Verarbeitung Verantwortliche oder den

403 *Borges,* DuD 2014, 165 (169).

Auftragsverarbeiter verpflichten, personenbezogene Daten weiterzugeben, nicht anerkannt werden. Art. 43a Abs. 2 DS-GVO-EK verpflichtet die besagten Stellen in diesem Fall, die zuständige Aufsichtsbehörde zu informieren und eine Genehmigung für die Datenübermittlung einzuholen. Die Aufnahme des Art. 43a DS-GVO-EK in den Verordnungsentwurf kann als Reaktion auf die PRISM-Enthüllungen gesehen werden und ist aus europäischer Sicht zu begrüßen.

7 Fazit

Zusammenfassend kann festgehalten werden, dass eine unkomplizierte und schnelle Nutzung von Cloudservices nicht einfach zu realisieren ist, sobald personenbezogene Daten mit der Cloud in Berührung kommen sollen. Die Einschränkungen bei der Nutzung sind einerseits darauf zurückzuführen, dass sich die Cloudanbieter gegenüber ihrer Nutzern sehr verschwiegen und intransparent geben und häufig nicht klar ist, welche Verfahren, Prozesse und Methoden der Cloudanbieter und seine Unterauftragnehmer nutzen, was es für den Nutzer schwierig macht, Datenschutzregelungen durchzusetzen.[404] Andererseits enthält das deutsche Recht keine cloudspezifischen Datenschutzregelungen, weshalb der Datentransfer in die Cloud nach den allgemeinen Regelungen des Bundesdatenschutzgesetzes legitimiert werden muss, was sich jedoch als schwierig gestaltet, da die Anforderungen, die beispielsweise an den Auftragsdatenverarbeitungsvertrag nach § 11 BDSG gestellt werden, nicht auf den Anwendungsfall des Cloud Computings zugeschnitten sind und sich daher nur auf Umwegen erfüllen lassen.

Aufgrund des dem Cloud Computing immanenten Prinzip der verteilten Orte der Datenverarbeitung und der Vielzahl der beteiligten Akteure auf der Seite des Cloudanbieters, ist es für den Nutzer kaum möglich zu kontrollieren, ob die zugesicherten Maßnahmen zum Datenschutz eingehalten worden sind. Einfacher wäre es daher, wenn es unabhängige cloudspezifische Zertifizierungen geben würde, die ein verlässliches Datenschutzniveau bescheinigen. Weiterhin wäre es wünschenswert, wenn die Entwicklung von Verschlüsselungstechnologien derart voranschreiten würde, dass nicht nur der Transport und die Speicherung in der Cloud verschlüsselt erfolgen könnten, sondern der Cloudnutzer die Daten vor dem Transport in die Cloud verschlüsseln und diese Daten auch verschlüsselt verarbeitet werden könnten.

---

[404] *International Working Group on Data Protection in Telecommunications,* WP on Cloud Computing – Privacy and data protection issues, S. 2.

Kann sichergestellt werden, dass nur der Cloudnutzer über den Schlüssel verfügt, unterfallen die Daten nicht mehr unter das Bundesdatenschutzgesetz, sodass auch die dort geltenden Anforderungen nicht mehr erfüllt werden brauchen.

Die Nutzung internationaler Cloudservices gestaltet sich noch schwieriger, da nach § 3 Abs. 8 S. 3 BDSG jede Auftragsdatenverarbeitung unter Beteiligung von außereuropäischen Datenempfängern als Übermittlung zu werten ist und deren Zulässigkeit das Bundesdatenschutzgesetz an strenge Anforderungen knüpft. Sowohl für die Nutzer als auch für die Cloudanbieter wäre es sicherlich wünschenswert, wenn die Auftragsdatenverarbeitung als solche auch unter Beteiligung von außereuropäischen Cloudanbietern und Unterauftragnehmern ermöglicht werden würde, wenn ein angemessenes Datenschutzniveau sichergestellt werden kann. Es ist daher von Nöten, dass der Gesetzgeber einen Rechtsrahmen schafft, der auch die Nutzung von internationalen Cloudservices ermöglicht und hierzu Anforderungen an den Datenschutz erlässt, die sich auch im Rahmen des Cloud Computings erfüllen lassen, da der Cloudnutzer sonst weiterhin bei personenbezogenen Daten faktisch keine Wahlfreiheit hat und auf innereuropäische Cloudservices zurückgreifen muss.

Es ist dargelegt worden, dass US-Cloudanbieter eine bedeutende Rolle am Cloud Computing Markt einnehmen und ein adäquates Datenschutzniveau häufig mit einer Safe Harbor Zertifizierung nachweisen, die aber bedeutende Vollzugsschwächen aufweist. Sollte an der Safe Harbor Zertifizierung festgehalten werden, so ist es unerlässlich, dass hier eine stärkere Kontrolle durch die zuständigen Kontrollbehörden erfolgt und Verstöße sanktioniert werden, damit sich der Cloudnutzer wirklich auf das verlassen kann, was die Zertifizierung verspricht. Dass die angesprochenen Empfehlungen der EU-Kommission zur Verbesserung des Safe Harbor-Abkommens tatsächlich von US-amerikanischer Seite unverändert angenommen werden, kann bezweifelt werden. Ein weiteres Problem im Zusammenhang mit amerikanischen Cloudanbietern sind die Zugriffsbefugnisse auf Grundlage des

USA Patriot Acts, die in den letzten Monaten durch das Bekanntwerden des Überwachungsprogramms PRISM für Diskussionen gesorgt haben.

Es ist davon auszugehen, dass die Enthüllungen um PRISM zu einem starken Vertrauensverlust gegenüber US-Cloudanbietern führen werden. Dies zeigt sich auch in einer Erklärung von Amazon, in der das Unternehmen klarstellt, dass seine Cloudservices Amazon Web Services (AWS) und Rackspace kein Teil von PRISM seien und dass man Kunden von AWS über Datenanfragen von Regierungsbehörden unterrichte und sie dabei unterstütze, gerichtlich gegen diese vorzugehen.[405]

Diese neu entfachte Diskussion zeigt, dass internationale Vereinbarungen notwendig sind, die festsetzen, dass ausländische Sicherheitsbehörden nicht das Recht haben, auf personenbezogene Daten zuzugreifen, die durch eine andere Rechtsordnung geschützt sind, ohne dass vorher geprüft wird, ob der Zugriff nach der betreffenden Rechtsordnung auch zulässig ist. Insofern ist Art. 43a DS-GVO-EK zu begrüßen, der Unternehmen dazu verpflichten würde, Zugriffsanforderungen von ausländischen Behörden, an die zuständige europäische Aufsichtsbehörde zu melden, die dann über die Zulässigkeit des Zugriffs entscheiden würde.

---

405 *Gohring,* Amazon Web Services: We'll go to court to fight gov't requests for data, abrufbar unter: http://www.itworld.com/cloud-computing/361679/amazon-web-services-we-ll-go-court-fight-gov-t-requests-data, Stand: 7.6.2014

Literatur

Amazon, AWS-Sicherheits- und Compliance-Zentrum, http://aws.amazon.com/de/security/, Zugriff am 7.6.2014.

Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf, Zugriff am 7.6.2014.

Arbitter, Peter/ Deutsch, Heiko/ Pracht, Thomas/ Reti, Martin, Cloud Computing – mehr als nur industrialisierte IT, in: Köhler-Schute, Christiana (Hrsg.), Cloud Computing: Neue Optionen für Unternehmen – Strategische Überlegungen, Konzepte und Lösungen, Beispiele aus der Praxis, Berlin 2011, 35-49.

Article 29 Data Protection Working Party, Explanatory Document on the Processor Binding Corporate Rules (WP 204), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf, Zugriff am 7.6.2014.

Artikel-29-Datenschutzgruppe, Arbeitsdokument 02/2012 mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter (WP 195), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_de.pdf, Zugriff am 7.6.2014.

Artikel-29-Datenschutzgruppe, Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU (WP 56), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_de.pdf., Zugriff am 7.6.2014.

Artikel-29-Datenschutzgruppe, Häufig gestellte Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardver-

tragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (WP 176), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_de.pdf, Zugriff am 7.6.2014.

Artikel-29-Datenschutzgruppe, Stellungnahme 05/2012 zum Cloud Computing (WP 196), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf, Zugriff am 7.6.2014.

Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" (WP 169), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf, Zugriff am 7.6.2014.

Artikel-29-Datenschutzgruppe, Stellungnahme 3/2009 über den Entwurf einer Entscheidung der Kommission zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (vom für die Datenverarbeitung Verantwortlichen zum Datenverarbeiter) (WP 161), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp161_de.pdf, Zugriff am 7.6.2014.

Auer-Reinsdorff, Astrid/ Conrad, Isabell (Hrsg.), Beck`sches Mandats Handbuch IT-Recht, München 2011.

Becker, Philipp/ Nikolaeva, Julia, Das Dilemma der Cloud-Anbieter zwischen US Patriot Act und BDSG – Zur Unmöglichkeit rechtskonformer Datenübermittlung für gleichzeitig in USA und Deutschland operierende Cloud-Anbieter, CR 2012, 170-176.

Beckereit, Frank, Quo vadis Virtualisierung – Infrastrukturen für die Private Cloud, in: Köhler-Schute, Christiana (Hrsg.), Cloud Computing: Neue Optionen für Unternehmen – Strategische Überlegungen, Konzepte und Lösungen, Beispiele aus der Praxis, Berlin 2011, 67-90.

Bedner, Mark, Cloud Computing – Technik, Sicherheit und rechtliche Gestaltung, Kassel 2013.

Bergt, Matthias, Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft, DuD 2013, 796-801.

Bierekoven, Christiane, Auftragsdatenverarbeitung in der Cloud, in: Bartsch, Michael/ Briner, Robert G. (Hrsg.), DGRI Jahrbuch 2010, Köln 2011, 95-122.

Bierekoven, Christiane, Lizenzierung in der Cloud, ITRB 2010, 42-44.

Birk, Dominik/ Wegener Christoph, Über den Wolken: Cloud Computing im Überblick, DuD 2010, 641-645.

BITKOM, Fallgruppen zur internationalen Auftragsdatenverarbeitung und abgestimmte Position der Aufsichtsbehörden – ein Echo des BITKOM, http://www.bitkom.org/files/documents/BITKOM_Echo_Duesseldorfer_Kreis_Int__ADV.pdf, Zugriff am 7.6.201.

BITKOM/ VOICE, Empfehlungen für den Cloud Computing-Standort Deutschland, http://www.bitkom.org/files/documents/cloud_computing_standort.pdf, Zugriff am 7.6.2014

Böken, Arnd, Patriot Act und Cloud Computing, http://www.heise.de/ix/artikel/Zugriff-auf-Zuruf-1394430.html, Zugriff am 7.6.2014.

Boos, Carina/ Kroschwald, Steffen/ Wicker Magda, Datenschutz bei Cloud Computing zwischen TKG, TMG und BDSG – Datenkategorien bei der Nutzung von Cloud-Diensten, ZD 2013, 205-209.

Borges, Georg, Cloud Computing und Datenschutz – Zertifizierung als Ausweg aus einem Dilemma, DuD 2014, 165-169.

Bradshaw, David/ Folco, Guiliana/ Cattaneo, Gabriella/ Kolding, Marianne, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf, Zugriff am 7.6.2014.

Brenner, Michael, Geheimnisträger – Vertrauliche Datenverarbeitung mit homomorpher Kryptografie, iX 2012, 120-124.

Büllesbach, Achim, Transnationalität und Datenschutz – Die Verbindlichkeit von Unternehmensregelungen, Frankfurt am Main 2008.

Büllesbach, Alfred, Können Konzernrichtlinien interkontinentale Bruchlinien im IT-Recht überwinden: Ist das Beispiel Datenschutz übertragbar?, in: Klumpp, Dieter/ Kubicek, Herbert/ Roßnagel, Alexander/ Schulz, Wolfgang (Hrsg.), Medien, Ordnung und Innovation, Berlin, Heidelberg 2006, 307-313.

Busche, Angela, Internationaler Datenverkehr und Bundesdatenschutzgesetz („BDSG"), in: Taeger, Jürgen/ Wiebe, Andreas (Hrsg.), Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Edewecht 2009, 63-77.

Connolly, Chris, Safe Harbor – Fact or Fiction, http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf, Zugriff am 7.6.2014.

Conrad, Isabell / Hausen, Dominik, Datenschutzrechtliche Aspekte von Data Loss Prevention und Cloud-Computing, in: Büchner, Wolfgang/ Briner, Robert G. (Hrsg.), DGRI Jahrbuch 2009, Köln 2010, 21-42.

Deutlmoser, Ralf / Filip, Alexander, Europäischer Datenschutz und US-amerikanische (e-)Discovery-Pflichten, ZD-Beilage 6/2012, 1-20.

Dhont, Jan / Pérez Asinari, Maria Veronica / Poullet, Yves, Safe Harbor Decision Implementation Study, http://www.informatik.fh-gelsenkirchen.de/fileadmin/fb5/Paul/IGEA/Literatur/safe-harbour-2004_en.pdf, Zugriff am 7.6.2014.

Düsseldorfer Kreis, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April in Hannover – Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierenden Unternehmen, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf;jsessionid=222DCBF4F6DAC479E12B20C3FA7FB035.1_cid354?__blob=publicationFile, Zugriff am 7.6.2014.

Düsseldorfer Kreis, Fallgruppen der internationalen Auftragsdatenverarbeitung – Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung, http://www.datenschutz-berlin.de/attachments/456/HandreichungApril2007.pdf?1208354740, Zugriff am 7.6.2014.

Eckhardt, Jens, Rechtliche Aspekte des Cloud Computings, in: Köhler-Schute, Christiana (Hrsg.), Cloud Computing: Neue Optionen für Unternehmen – Strategische Überlegungen, Konzepte und Lösungen, Beispiele aus der Praxis, Berlin 2011, 166-191.

Eckhardt, Jens, BDSG: Neuregelungen seit 01.09.2009, DuD 2009, 587-595.

Eckhardt, Jens, Cloud Computing – ein rechtlicher Überblick, Information Management und Consulting 4/2010, 55-61.

Engels, Thomas, Datenschutz in der Cloud – Ist hierbei immer eine Auftragsdatenverarbeitung anzunehmen?, K&R 2011, 548-551.

Erd, Reiner, Auftragsdatenverarbeitung in sicheren Drittstaaten – Plädoyer für eine Reform von § 3 Abs. 8 S. 3 BDSG, DuD 2011, 275-278.

Eul, Harald / Eul, Petra, Datenschutz international – Ein Praxisleitfaden für die Übermittlung von Kunden-, Mitarbeiter-, und Lieferantendaten, Heidelberg 2011.

EuroCloud Deutschland_eco e.V., Das Gütesiegel für die Cloud: EuroCloud Star Audit SaaS, http://www.saas-audit.de/files/2011/01/EuroCloud-Star-Audit-SaaS-PK-.pdf, Zugriff am 7.6.2014.

EuroCloud Deutschland_eco e.V., Leitfaden Cloud Computing – Recht, Datenschutz und Compliance, http://www.cloudmacher.de/index.php/download_file/224/99/., Zugriff am 7.6.2014.

Europäische Kommission, Freisetzung des Cloud Computing-Potentials in Europa, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:DE:PDF, Zugriff am 7.6.2014.

Europäische Kommission, Widerherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA – Häufig gestellte Fragen,

http://europa.eu/rapid/press-release_MEMO-13-1059_de.htm, Zugriff am 07.05.2014.

Filip, Alexander, Binding Corporate Rules (BCR) aus der Sicht einer Datenschutzaufsichtsbehörde, ZD 2013, 51-60.

Financial Times Deutschland, Cloud-Zertifikate als Entscheidungshilfe, http://www.ftd.de/it-medien/:guetesiegel-cloud-zertifikate-als-entscheidungshilfe/70105762.html, Zugriff am 7.6.2014.

Gaul, Björn / Koehler, Lisa-Marie, Mitarbeiterdaten in der Computer-Cloud: Datenschutzrechtliche Grenzen des Outsourcing, BB 2011, 2229-2236.

Gehring, Robert A., EU-Parlamentarier besorgt über US-Zugriff auf Cloud-Daten, http://www.golem.de/1107/84763.html, Zugriff am 7.6.2014.

Gerlach, Carsten, Zertifizierungen für Cloud-Computing-Systeme und SaaS: Datenschutz und Compliance, http://www.it-rechts-praxis.de/meldungen/Zertifizierungen-fuer-Cloud-Computing-Systeme-und-SaaS-Datenschutz-und-Compliance-186, Zugriff am 7.6.2014.

Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Stellungnahme zum Vorschlag für eine EU-Datenschutz-Grundverordnung, https://www.gdd.de/nachrichten/arbeitshilfen/Stellungnahme%20DS-GVO-E%20endgx.pdf., Zugriff am 7.6.2014.

Giebichenstein, Rüdiger, Chancen und Risiken beim Einsatz von Cloud Computing in der Rechnungslegung, BB 2011, 2218-2224.

Giebichenstein, Rüdiger / Weiss, Andreas, Zertifizierte Cloud durch das EuroCloud Star Audit SaaS – Ein Best Practice-Ansatz zur Auswahl eines vertrauenswürdigen Cloud-Anbieters, DuD 2011, 338-342.

Giesen, Thomas, Datenverarbeitung im Auftrag in Drittstaaten – eine misslungene Gesetzgebung, CR 2007, 543-548.

Gohring, Nancy, Amazon Web Services: We'll go to court to fight gov't requests for data, http://www.itworld.com/cloud-computing/361679/amazon-web-services-we-ll-go-court-fight-gov-t-requests-data, Zugriff am 7.6.2014.

Gola, Peter / Schomerus, Rudolf (Hrsg.), BDSG – Bundesdatenschutzgesetz Kommentar, 11. Auflage, München 2012.

Gola, Peter / Schomerus, Rudolf (Hrsg.), BDSG – Bundesdatenschutzgesetz Kommentar, 10. Auflage, München 2010.

Grapentin, Sabine, Datenschutz und Globalisierung – Binding Corporate Rules als Lösung?, CR 2009, 693-699.

Grappentin, Sabine, Haftung und anwendbares Recht im internationalen Datenverkehr – EU-Standardvertragsklauseln und Binding Corporate Rules, CR 2011, 102-107.

Grünwald, Andreas / Döpkens, Harm-Randolf, Cloud Control? – Regulierung von Cloud Computing-Angeboten, MMR 2011, 287-280.

Grützmacher, Malte, Datenschutz und Outsourcing, ITRB 2007, 183-187.

Hallermann, Ulrich, Wann müssen Auftragsdatenverarbeitungen vor Ort kontrolliert werden?, RDV 2012, 226-230.

Hansen, Marit, Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter, DuD 2012, 407-412.

Heibey, Hanns-Wilhelm, Datensicherung, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, 570-599.

Heidrich, Jörg / Wegener, Christoph, Cloud Computing und Datenschutz, MMR 2010, 803-807.

Helbing, Thomas, Standardvertragsklauseln und Auftragsverarbeiter, http://www.saasmagazin.de/schwerpunkte/schwerpunkte-2009/crm-loesungen-in-der-cloud-saas-crm/dr-helbing-sp-crm090712.html. Zugriff am 7.6.2014.

Hennrich, Thorsten, Compliance in Clouds – Datenschutz und Datensicherheit in Datenwolken, CR 2011, 546-552.

Hoeren, Thomas, Das neue BDSG und die Auftragsdatenverarbeitung, DuD 2010, 688-691.

Hoeren, Thomas, EU-Standardvertragsklauseln, BCR und Safe Harbor Principles – Instrumente für ein angemessenes Datenschutzniveau, RDV 2012, 271-277.

Hornung, Gerrit, Eine Datenschutz-Grundverordnung für Europa? – Licht und Schatten im Kommissionsentwurf vom 25.1.2012, ZD 2012, 99-106.

Hornung, Gerrit / Sädtler, Stephan, Europas Wolken – Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing, CR 2012, 638-645.

Ihlenfeld, Jens, Google erhält ISO-27001-Zertifizierung für Google Apps, http://www.golem.de/news/cloud-computing-google-erhaelt-iso-27001-zertifizierung-fuer-google-apps-1205-92099.html, Zugriff am 19.06.2013.

International Working Group on Data Protection in Telekommunications, Working Group on Cloud Computing – Privacy and data protection issues – „Sopot Memorandum", http://www.datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf., Zugriff am 7.6.2014.

Janisch, Fabian, Cloud Computing und Datenschutz, Norderstedt 2011.

Jotzko, Florian, Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?, MMR 2009, 232-237.

Kahler, Thomas, Auftragsdatenverarbeitung im Drittstaat: europarechtskonform! – Unmittelbare Anwendung der Datenschutzrichtlinie 95/46/EG in Deutschland, RDV 2012, 167-172.

Karger, Michael / Sarre, Frank, Wird Cloud Computing zu neuen juristischen Herausforderungen führen?, in: Taeger, Jürgen/ Wiebe, Andreas (Hrsg.), Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Edewecht 2009, 427-439.

Kiehne, Andre, Auf Wolken gebettet, nicht auf Sand gebaut: Cloud Services – Wie sich ihr Potential am besten erschließen lässt, in: Köhler-Schute, Christiana (Hrsg.), Cloud Computing: Neue Optionen für Unternehmen – Strategische Überlegungen, Konzepte und Lösungen, Beispiele aus der Praxis, Berlin 2011, 23-34.

Köhler, Markus / Arndt, Hans-Wolfgang / Fetzer, Thomas, Recht des Internet, 7. Auflage, Heidelberg 2011.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten, http://www.datenschutz-berlin.de/attachments/970/Presseerkl__rung_Safe_Harbor-2.pdf?1374663105, Zugriff am 7.6.2014.

Kramer, Philipp / Herrmann, Michael, Auftragsdatenverarbeitung – Zur Reichweite der Privilegierung durch den Tatbestand des § 11 Bundesdatenschutzgesetz, CR 2003, 938-941.

Kroschwald, Steffen, VERSCHLÜSSELTES CLOUD COMPUTING – Anwendung des Daten- und Geheimnisschutzrechts auf „betreibersichere" Clouds am Beispiel der „Sealed Cloud", in: Taeger, Jürgen (Hrsg.), Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter, Tagungsband Herbstakademie 2013, Band 1, Edewecht 2013, 289-308.

Kroschwald, Steffen, Verschlüsseltes Cloud Computing – Auswirkungen der Kryptografie auf den Personenbezug in der Cloud, ZD 2014, 75-80.

Lang, Markus, Reform des EU-Datenschutzrechts – Einheitliche Regelungen mit hohem Datenschutzniveau geplant, K&R 2012, 145-151.

Laue, Philip / Stiemerling, Oliver, Identitäts- und Zugriffsmanagement für Cloud Computing Anwendungen – Technisch-organisatorische Probleme, rechtliche Risiken und Lösungsansätze, DuD 2010, 692-697.

Lensdorf, Lars, Auftragsdatenverarbeitung in der EU/EWR und Unterauftragsdatenverarbeitung in Drittländern, CR 2010, 735-741.

Maisch, Michael Marc / Seidl, Alexander, Cloud Government: Rechtliche Herausforderungen beim Cloud Computing in der öffentlichen Verwaltung, VBIBW 2012, 7-12.

Marnau, Ninja, Could Processor BCR prove to be cloud-enabling in Europe?, http://www.tclouds.eu/index.php/tclouds-blog/entry/could-processor-bcr-prove-to-be-cloud-enabling-in-europe, Zugriff am 7.6.2014.

Marnau, Ninja / Schirmer, Norbert / Schlehan, Eva / Schunter, Matthias, TClouds – Herausforderungen und erste Schritte zur sicheren und datenschutzkonformen Cloud, DuD 2011, 333-337.

Marnau, Ninja / Schlehan, Eva, Cloud Computing und Safe Harbor, DuD 2011, 311-316.

Microsoft, CRM in der Cloud: Microsoft baut Führung beim Datenschutz weiter aus, http://www.microsoft.com/de-de/kmu/Produkte/Seiten/Microsoft-CRM-Online.aspx, Zugriff am 7.6.2014.

Microsoft, Datenschutz und Datensicherheit in der Microsoft Cloud, http://www.microsoft.com/de-de/kmu/Themen/Seiten/datensicherheit-datenschutz-cloud-rainer-stropek.aspx, Zugriff am 7.6.2014.

Moos, Flemming, Die EU-Standardvertragsklauseln für Auftragsverarbeiter 2010, CR 2010, 281-286.

Müglich, Andreas, Datenschutzrechtliche Anforderungen an die Vertragsgestaltung beim eShop-Hosting – Anspruch, Wirklichkeit und Vollzugsdefizit, CR 2009, 479-484.

Müthlein, Thomas, Abgrenzungsprobleme bei der Auftragsdatenverarbeitung, RDV 1993, 165-171.

Müthlein, Thomas, Probleme der Auftragsdatenverarbeitung für Auftraggeber und Auftragnehmer, RDV 1992, 63-74.

Nägele, Thomas / Jacobs, Sven, Rechtsfragen des Cloud Computing, ZUM 2010, 281-292.

National Institute of Standards and Technology (NIST), The NIST Definition of Cloud Computing, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, Zugriff am 7.6.2014.

Nebel, Maxi / Richter, Philipp, Datenschutz bei Internetdiensten nach der DS-GVO, ZD 2012, 407-413.

Nielen, Michael / Thum, Kai, Auftragsdatenverarbeitung durch Unternehmen im Nicht-EU-Ausland, K&R 2006, 171-176.

Niemann, Fabian / Hennrich, Thorsten, Kontrollen in den Wolken – Auftragsdatenverarbeitung in Zeiten des Cloud Computings, CR 2010, 686-692.

Niemann, Fabian / Paul, Jörg-Alexander, Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computings, K&R 2009, 444-453.

Paulus, Sachar, Standards für Trusted Clouds – Anforderungen an Standards und aktuelle Entwicklungen, DuD 2011, 317-321.

Pauly, Michael, Cloud Computing – Kronzeuge einer Zeitenwende, in: Köhler-Schute, Christiana (Hrsg.), Cloud Computing: Neue Optionen für Unternehmen – Strategische Überlegungen, Konzepte und Lösungen, Beispiele aus der Praxis, Berlin 2011, 15-22.

Plath, Kai-Uwe (Hrsg.), BDSG – Kommentar zum BDSG sowie den datenschutzrechtlichen Regelungen des TMG und des TKG, Köln 2013.

Pohle, Jan / Ammann, Thorsten, Software as a Service – auch rechtlich eine Evolution?, K&R 2009, 625-631.

PWC, Cloud Computing – Navigation in der Wolke, http://www.pwc.de/de_DE/de/prozessoptimierung/assets/evolution-in-der-wolke-reifegrad-der-cloud-services-steigt2.pdf, Zugriff am 7.6.2014.

Räther, Philipp C., Datenschutz und Outsourcing, DuD 2005, 461-466.

Räther, Philipp C. / Seitz, Nicolai, Übermittlung personenbezogener Daten in Drittstaaten – Angemessenheitsklausel, Safe Harbor und die Einwilligung, MMR 2002, 425-433.

Redeker, Helmut, IT-Recht, 5. Auflage, München 2012.

Reindl, Martin, Cloud Computing und Datenschutz, in: Taeger, Jürgen/ Wiebe, Andreas (Hrsg.), Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Edewecht 2009, 441-454.

Rittweger, Christoph / Schmidl, Michael, Einwirkung von Standardvertragsklauseln auf § 28 BDSG, DuD 2004, 617-620.

Roßnagel, Alexander / Scholz, Philip, Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721-731.

Roth, Birgit, Organisatorische und technische Maßnahmen zum Schutz personenbezogener Daten, ITRB 2010, 60-63.

Sawall, Achim, Europäische Cloud-Daten nicht vor US-Zugriff sicher, http://www.golem.de/1106/84620.html, Zugriff am 7.6.2014.

Schmidt-Bens, Johanna, Cloud Computing Technologien und Datenschutz, Edewecht 2012.

Schröder, Christian / Haag, Nils Christian, Neue Anforderungen an Cloud Computing für die Praxis – Zusammenfassung und erste Bewertung der „Orientierungshilfe – Cloud Computing", ZD 2011, 147-152.

Schultze-Melling, Jyn, Gedanken zum Umgang mit der Wolke, ITRB 2011, 239-240.

Schulz, Carsten, Rechtliche Aspekte des Cloud Computing im Überblick, in: Taeger, Jürgen/ Wiebe, Andreas (Hrsg.), Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Edewecht 2009, 403-418.

Schulz, Carsten / Rosenkranz, Timo, Cloud Computing – Bedarfsorientierte Nutzung von IT-Ressourcen, ITRB 2009, 232-236.

Schulz, Sönke E., Cloud Computing in der öffentlichen Verwaltung – Chancen – Risiken – Modelle, MMR 2010, 75-80.

Schuppert, Stefan / von Reden, Armgard, Einsatz internationaler Cloud-Anbieter: Entkräftung der Mythen, ZD 2013, 210-220.

Schuster, Fabian / Reichl, Wolfgang, Cloud Computing & SaaS: Was sind die wirklich neuen Fragen?, CR 2010, 38-43.

Schweda, Sebastian, Wolken über dem Rechtsstaat? – Recht und Technik des Cloud Computings in Verwaltung und Wirtschaft, ZD-aktuell 2012, 30109.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 6. Auflage, Baden-Baden 2006.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 7. Auflage, Baden-Baden 2011.

Simonite, Tom, Sicheres Computing für die Cloud, http://www.heise.de/tr/artikel/Sicheres-Computing-fuer-die-Cloud-1021071.html, Zugriff am 7.6.2014.

Söbbing, Thomas, Auswirkungen der BDSG-Novelle II auf Outsourcingprojekte, ITRB 2010, 36-39.

Söbbing, Thomas, Cloud Computing und Virtualisierung – Rechtliche Frage –, in: Leible, Stefan/ Sosnitza, Olaf (Hrsg.), Online-Recht 2.0: Alte Fragen – neue Antworten? Cloud Computing – Datenschutz – Urheberrecht – Haftung, Stuttgart 2011, S. 35-75.

Spies, Axel, Keine „Genehmigungen“ mehr zum USA-Datenexport nach Safe Harbor? – Übertragung personenbezogener Daten aus Deutschland in die USA, ZD 2011, 535-538.

Spies, Axel, USA: Cloud Computing – Schwarze Löcher im Datenschutzrecht, MMR 2009, Heft 5, XI-XII.

Spies, Axel, USA: Grenzüberschreitende elektronische Beweiserhebung (Discovery) vs. Datenschutz, MMR 2007, Heft 7, V-VII.

Spindler, Gerald / Schuster, Fabian (Hrsg.), Recht der elektronischen Medien, 2. Auflage, München 2011.

Splittgerber, Andreas / Rockstroh, Sebastian, Sicher durch die Cloud navigieren – Vertragsgestaltung beim Cloud Computing, BB 2011, 2179-2185.

Stögmüller, Thomas, Teil 5. Internationale Bezüge des IT-Rechts einschließlich Internationales Privatrecht, in: Leupold, Andreas/ Glossner, Silke (Hrsg.), Münchner Anwaltshandbuch IT-Recht, 2. Auflage, München 2011.

Sutschet, Holger, Auftragsdatenverarbeitung und Funktionsübertragung, RDV 2004, 97-104.

Taeger, Jürgen / Gabel, Detlev (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, Frankfurt am Main 2010.

Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing – Ein rechtspolitisches Thesenpapier der AG Rechtsrahmen des Cloud Computing, http://www.trusted-cloud.de/documents/Datenschutz rechtliche-Loesungen-fuer-Cloud-Computing.pdf, Zugriff am 7.6.2014.

Vander, Sascha, Auftragsdatenverarbeitung 2.0? – Neuregelungen der Datenschutznovelle II im Kontext von § 11 BDSG, K&R 2010, 292-298.

Voigt, Paul, Datenübermittlungen in die USA ab sofort rechtswidrig?, http://www.datenschutzkongress.de/lp/2014/P1106112_newsletter.pdf, Zugriff am 07.06.2013

Von Sponeck, Henning, Überlassung von RZ-Kapazität – ein Fall der Auftragsdatenverarbeitung?, CR 1992, 594-596.

Wächter, Michael, Rechtliche Grundstrukturen der Datenverarbeitung im Auftrag, CR 1991, 333-336.

Wagner, Axel-Michael / Blaufuß, Henning, Datenexport als juristische Herausforderung: Cloud Computing, BB 2012, 1751-1755.

Weichert, Thilo, Cloud Computing und Datenschutz, DuD 2010, 679-687.

Weiss, Andreas, EuroCloud Star Audit – Zertifizierung von Cloud Diensten, DuD 2014, 170-174.

Wronka, Georg, Zur Interessenlage bei der Auftragsdatenverarbeitung, RDV 2003, 132-135.

Wybitul, Tim / Fladung, Armin, EU-Datenschutz-Grundverordnung – Überblick und arbeitsrechtliche Betrachtung des Entwurfs, BB 2012, 509-515.

Wybitul, Tim / Patzak, Andrea, Neue Anforderungen beim grenzüberschreitenden Datenverkehr, RDV 2012, 11-18.

Die Nutzung online bereitgestellter Hard- und Software im Rahmen des Cloud Computings verspricht viele Vorzüge gegenüber dem traditionellen Bezug von IT. Der größte Vorteil wird in der flexiblen, skalierbaren und kostengünstigen Nutzung von Cloudservices gesehen. Dieser Kosten- und Flexibilitätsvorteil beruht vor allem auf der Architektur von Public Clouds. In der Wahrnehmung der Nutzer ist eine Public Cloud ein einzelnes System, tatsächlich setzt sich diese in der Regel jedoch aus vielen Servern und Rechenzentren zusammen, die über die ganze Welt verteilt sein können. Ohne die eingebundenen Ressourcen von Unterauftragnehmern ist die Erbringung von Cloudservices häufig gar nicht erst möglich.

Diese mitunter intransparenten Strukturen des Cloud Computings und die Vielzahl der an der Serviceerbringung beteiligten Akteure erschweren die Erfüllung datenschutzrechtlicher Vorgaben. Die vorliegende Arbeit untersucht aktuelle datenschutzrechtliche Herausforderungen bei der Nutzung von Cloudservices. Insbesondere wird dargestellt und bewertet, welche rechtlichen Instrumente zur Einbindung von Unterauftragnehmern zur Verfügung stehen.

ISBN 978-3-86219-834-4