CHRISTIAN SCHRÖDER / NILS CHRISTIAN HAAG

Internationale Anforderungen an Cloud Computing

Zusammenfassung und Bewertung der Best Business-Empfehlungen der Berlin Group

Cloud-Dienstleistung
Kriterienkatalog
Internationale Clouds
Technische und organisatorische Anforderungen
Vertragsgestaltung

■ Die International Working Group on Data Protection in Telecommunications (Berlin Group) hat in einer am 24.4.2012 veröffentlichten Stellungnahme „Sopot Memorandum" Empfehlungen für die datenschutzgerechte Nutzung von Cloud-Dienstleistungen gegeben. Diese erste internationale Stellungnahme zu Datenschutz und Cloud-Dienstleistungen wurde von Vertretern von Datenschutzbehörden aus 21 Ländern unterstützt und ist daher ein für die internationale Praxis bedeutsamer Kriterienkatalog für Cloud-Dienstleistungen. Der Schwerpunkt der Empfehlungen liegt im technischen Datenschutz, dabei insbesondere bei der Protokollierung von Datenverarbeitungsorten, sowie der vertraglichen Gestaltung. Der Artikel gibt eine erste Zusammenfassung und kritische Analyse der Vorschläge.

■ The International Working Group on Data Protection in Telecommunications (Berlin Group) published on April 24, 2012 a working paper called „Sopot Memorandum" which sets out recommendations of how to use cloud-computing services in compliance with applicable privacy laws. This first international working paper on privacy and cloud-computing services is supported by 21 international data protection authorities and is therefore understood to be the first important international guidance on cloud-computing services. The main recommendations of the working paper concern technical data protection, in particular the logging of all data processing locations, as well as guidance on the content of the cloud-services agreements. This article gives a first summary and critical analysis of the published recommendations.

I. Einleitung

Die *International Working Group on Data Protection in Telecommunications* (im Folgenden: *Berlin Group*) hat im April 2012 ein Arbeitspapier zu den datenschutzrechtlichen Anforderungen beim Cloud Computing veröffentlicht.[1] Die Kurzbezeichnung der *Berlin Group* geht auf den *Berliner Datenschutzbeauftragten* zurück, der die Arbeitsgruppe bereits 1983 ins Leben rief und seitdem ihren Vorsitz innehat.[2] Die *Gruppe* veröffentlicht regelmäßig Empfehlungen für Verbesserungen des Datenschutzes im TK-Bereich; in den vergangenen 15 Jahren stand der Schutz der Privatsphäre im Internet im Vordergrund. Organisatorisch gehört die *Berlin Group* als Arbeitsgruppe zur *Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre*, bei der sich Aufsichtsbehörden aus aller Welt jährlich treffen. Es handelt sich somit bei dem hier behandelten Papier um eine Empfehlung internationaler Aufsichtsbehörden aus nicht allein europäischer, sondern globaler Perspektive.

Bereits im September 2011 hatte die *Konferenz der Datenschutzbeauftragten des Bundes und der Länder* eine Orientierungshilfe zum Cloud Computing vorgestellt.[3] Die Orientierungshilfe der deutschen Aufsichtsbehörden ist jedoch etwas umfangreicher und enthält ebenfalls hilfreiche Ansätze für den datenschutzkonformen Einsatz von Cloud-Lösungen.[4]

Das nun von der internationalen *Berlin Group* veröffentlichte „Working Paper on Cloud Computing – Privacy and data protection issues – „Sopot Memorandum" (im Folgenden: Working Paper) ist nach dem Ort der letzten Tagung im polnischen Sopot benannt. Dort wurde das Memorandum am 24.4.2012 von Vertretern der Datenschutzbehörden aus 21 Ländern verabschiedet und versteht sich als erster auf internationaler Ebene beschlossener Kriterienkatalog, der datenschutzrechtliche Anforderungen an das Cloud Computing beschreibt.[5] Da Cloud-Angebote fast immer grenzüberschreitende Systeme darstellen, ist ein sol-

1 Working Paper on Cloud Computing – Privacy and data protection issues – „Sopot Memorandum" – 51st meeting, 23-24 April 2012, Sopot (Poland), abrufbar unter: http://datenschutz-berlin.de/content/nachrichten/datenschutznachrichten/27-april-2012; eine deutsche Fassung war zum Zeitpunkt der Erstellung dieses Beitrags lediglich angekündigt.

2 Informationen über und weitere Veröffentlichungen der *Arbeitsgruppe* unter: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt.

3 Orientierungshilfe – Cloud Computing, Stand 26.9.2011, http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf.

4 Eine ausführliche Darstellung und Bewertung bei *Schröder/Haag*, ZD 2011, 147 ff.

5 PM des *Berliner Datenschutzbeauftragten* v. 27.4.2012, abrufbar unter: http://datenschutz-berlin.de/attachments/872/Pressemitteilung_Cloud_Computing.pdf.

cher Vorstoß auf internationaler Ebene ebenso sehr zu begrüßen wie zu beachten. Die *Berlin Group* veröffentlicht jedoch keine Liste ihrer Mitglieder, ferner ist unklar, welche ihrer Mitglieder das Sopot Memorandum unterstützen. Insofern kann die Bedeutung des Memorandums nicht abschließend bewertet werden.

II. Ausgangspunkt und Zielsetzung

Das Working Paper beginnt mit einer Erläuterung der Voraussetzungen für die nachfolgend beschriebenen Anforderungen an Cloud Computing.[6] Insofern hält das Working Paper zunächst fest, dass es mangels Praxisrelevanz keine Anforderungen für Cloud-Konstellationen beschreibt, bei denen sich Cloud-Anbieter und -Anwender sowie sämtliche Datenverarbeitungen innerhalb einer Jurisdiktion befinden. Ebenso ist das Working Paper weniger relevant für Cloud-Angebote, bei denen der Nutzer die volle Kontrolle über seine Daten behält. Vielmehr nimmt das Working Paper die typische Ausgangssituation in den Fokus seiner Betrachtung, bei der ein Unternehmen oder eine Behörde einen bestehenden Prozess in eine Cloud outsourcen möchte und dabei auf das Angebot eines international tätigen Dienstleisters zurückgreift.

Um einen klar definierten Ausgangspunkt für eine Auseinandersetzung mit dem Cloud Computing zu finden, zitiert das Working Paper eine Definition der US-amerikanischen Behörde für Standardisierungen, dem *National Institute of Standards and Technology* (*NIST*), die leicht verkürzt lautet:[7] „Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Die Begrenzung des Anwendungsbereichs der im Working Paper formulierten Anforderungen ist begrüßenswert, da unter *Cloud Computing* oft sehr unterschiedliche Dienstleistungen verstanden werden und die technische Entwicklung zudem rasch voranschreitet.[8] Da nicht nur technische Definitionen, sondern auch die datenschutzrechtlichen Anforderungen beim Cloud Computing noch unklar sind, ist es das erklärte Ziel des Working Papers, durch konkrete Empfehlungen mehr Sicherheit in Bezug auf die Einhaltung datenschutzrechtlicher Vorgaben zu schaffen.

Vor der Darstellung dieser konkreten Empfehlungen zählt das Working Paper relativ ungeordnet einige Besonderheiten des Cloud Computing auf, die man als Hauptursachen für die Schwierigkeit der Einhaltung datenschutzrechtlicher Vorgaben ausgemacht hat.[9]

- Es gibt vielfältige und laufend neue Ausprägungen von Cloud-Dienstleistungen (insofern lassen sich kaum standardisierte Lösungsvorschläge entwickeln);
- die globale Ausbreitung vieler Systeme erschwert die Durchsetzung nationaler datenschutzrechtlicher Regelungen;[10]
- der Cloud-Anwender kann kaum sicherstellen, dass er über unbefugte Datenweitergabe/Datenverlust (Security Breaches) oder eine mangelnde Verfügbarkeit von Daten informiert wird;
- es besteht oft mangelnde Transparenz im Hinblick auf genutzte Ressourcen und die Einhaltung vereinbarter Prozesse und
- datenschutzrechtliche Sicherungsmaßnahmen verursachen Kosten und stehen den wirtschaftlichen Interessen des Cloud-Anbieters (Senkung der Investitionskosten) und des Cloud-Anwenders (Kostenreduzierung durch Outsourcing) entgegen.

Wesentliche Folge ist regelmäßig der Verlust der Kontrolle des Cloud-Anwenders über die Datenverarbeitungen in der Cloud und die damit einhergehenden Risiken für die Betroffenen, deren Daten in der Cloud verarbeitet werden. Die Rechte der Betroffenen können oft nicht mehr durchgesetzt werden, da die datenverarbeitenden Stellen (z.B. auch Unterauftragnehmer) nicht bekannt oder an Standorten ansässig sind, die keine effektive Rechtsdurchsetzung gewährleisten.

III. Empfehlungen der Berlin Group

Kernstück des Working Papers der *Berlin Group* ist eine Auflistung von Empfehlungen, die bei der Nutzung von Clouds helfen soll, die vorgenannten Risiken zu minimieren. Nach allgemeinen Empfehlungen (1.) folgt eine nummerierte, jedoch nicht weiter strukturierte Aufzählung konkreter „best practice"-Maßnahmen (2.).[11] Die *Berlin Group* weist darauf hin, dass die dargestellten Empfehlungen und Maßnahmen nicht den Anspruch auf Vollständigkeit erheben.

1. Allgemeine Empfehlungen

In den „general recommendations" finden sich Grundprinzipien, die beim Cloud Computing aus datenschutzrechtlicher Perspektive stets berücksichtigt werden sollen. Danach müssen Unternehmen und Behörden darauf achten, dass sich ihre Datenschutzstandards infolge der Auslagerung in die Cloud generell nicht verschlechtern.

Diese Forderung hat auf Grund der geschilderten Risiken sicherlich ihre Berechtigung. Allerdings ist sie für den Cloud-Anwender wegen ihrer Pauschalität schwer umzusetzen. Zu begrüßen ist, dass die *Berlin Group* offenbar die Auffassung vertritt, dass Cloud-Lösungen trotz der Cloud-immanenten Risiken nicht zu einer Verschlechterung des Datenschutzstandards führen müssen. Offenbar ist die *Berlin Group* der Ansicht, dass bei Umsetzung ihrer Empfehlungen Cloud-Lösungen im Vergleich zu von der verantwortlichen Stelle selbst zur Verfügung gestellten Systemen durchaus Vorteile für die Datensicherheit bringen können. Hierdurch wird im Rahmen einer Abwägung des Gesamtrisikos die durch die Verlagerung bedingte reduzierte Kontrollmöglichkeit datenschutzrechtlich vertretbar. Nachvollziehbar ist dies z.B., wenn Daten in einer professionell administrierten Cloud-Umgebung u.U. deutlich besseren Schutz erhalten, als es z.B. in einer weniger professionell aufgestellten IT-Infrastruktur eines mittelständischen Unternehmens wirtschaftlich vertretbar wäre.[12]

Die weiteren allgemeinen Empfehlungen richten sich jeweils an bestimmte Adressaten:

- Cloud-Anwender müssen vor der Entscheidung für eine Cloud-Lösung erforderliche Risikoanalysen durchgeführt haben;
- Cloud-Anbieter müssen ihre Systeme im Hinblick auf mehr Transparenz und Datensicherheit laufend verbessern;
- die Forschung, unabhängige Zertifizierungsstellen und Standardisierungsverfahren sind stärker zu fördern und
- die Gesetzgeber müssen Regelungen schaffen, die den Einsatz internationaler Cloud-Lösungen erlauben und gleichzeitig die erforderlichen Datenschutzanforderungen festlegen.

Diese sehr allgemein gehaltenen Anforderungen werden in den nachfolgenden „best practice"-Empfehlungen näher konkretisiert.

---

6 Working Paper (o. Fußn. 1), S. 1.
7 Working Paper (o. Fußn. 1), S. 1 mit Verweis auf *NIST*, Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, Page 3.
8 Working Paper (o. Fußn. 1), S. 2 und 6 (background).
9 Working Paper (o. Fußn. 1), S. 2 f.
10 Dazu auch Working Paper (o. Fußn. 1), S. 7 Ziff. 38 (background).
11 Working Paper (o. Fußn. 1), S. 3 ff.
12 Vgl. Interview mit BITKOM-Präsident *Kempf*, DIE WELT v. 16.5.2012, Sonderausgabe Cloud Computing, S. I.

2. Konkrete „best practice"-Empfehlungen

Unter der Überschrift „Additional guidance on best practices" finden sich 27 durchnummerierte Absätze im Working Paper, die von weiteren 17 Absätzen mit Begründungen zu den Empfehlungen gefolgt werden.[13] Bemerkenswert ist dabei schon die Nutzung des Begriffs „best practice", der praktikable und wirtschaftlich vertretbare Lösungsansätze erwarten lässt. Hieran zeigt sich deutlich, dass das Working Paper keinen dogmatischen, sondern einen pragmatischen und lösungsorientierten Ansatz verfolgt. Dies ist für Aufsichtsbehörden ein schwieriger, aber gleichwohl im Sinne des Datenschutzes sehr begrüßenswerter Paradigmenwechsel. Er ist offenbar dadurch bedingt, dass es für Cloud-Lösungen keine speziellen rechtlichen Rahmenbedingungen gibt, die weltweit einheitliche und klare Vorgaben geben.

Die im Working Paper nachfolgende Auflistung der einzelnen Empfehlungen und Hintergründe (background information) wirkt jedoch wenig strukturiert und ist daher etwas schwer zugänglich. Vermutlich liegt dies daran, dass das Papier unmittelbar im Anschluss an die Tagung der *Berlin Group* verfasst wurde. Um eine bessere Übersicht über die einzelnen Empfehlungen zu gewinnen, wurden die einzelnen Punkte nachfolgend unter Beibehaltung der vorgegebenen Struktur von den Autoren selbst gewählten Überschriften zugeordnet.

Die *Berlin Group* ordnet ihre Empfehlungen im Wesentlichen den fünf Bereichen „Transparenz", „Technischer Datenschutz", „Vertragsgestaltung", „Pflichten des Cloud-Anbieters" und „Audits" zu und beginnt zunächst mit der Empfehlung einer schrittweisen Vorgehensweise bei der Einführung von Cloud-Lösungen.

a) Schrittweise Implementierung von Cloud-Lösungen

Die ersten beiden Empfehlungen betreffen den Prozess der Entscheidung für oder gegen die Auslagerung eines bestimmten Verfahrens in die Cloud. Die *Berlin Group* empfiehlt grundsätzlich, Cloud-Lösungen zunächst zu Testzwecken ausschließlich für die Verarbeitung nicht-sensitiver Daten bzw. nicht-vertraulicher Informationen zu nutzen. Sobald später auch sensitive Daten in einer Cloud-Anwendung verarbeitet werden sollen, sind erweiterte Sicherheitsvorkehrungen zu treffen. Das Working Paper weist in einer Fußnote darauf hin, dass es in den verschiedenen Rechtskreisen ein unterschiedliches Verständnis dazu gibt, welche Daten als sensitiv einzustufen sind und welche Anforderungen für eine Verarbeitung solcher Daten gelten.[14]

Die schrittweise Einführung einer Cloud-Lösung stellt eine gute Möglichkeit dar, um Funktionalitäten wie systemseitige Protokollierungen mit vermindertem Risiko zu testen. Ohnehin muss vor jeder Überlegung, ein bestimmtes Verfahren in die Cloud auszulagern, auch aus datenschutzrechtlicher Sicht geprüft werden, ob es ein passendes Angebot hierfür gibt. Aus rein datenschutzrechtlicher Sicht vergrößern sich die Bedenken gegen eine Cloud-Lösung, je sensitiver bzw. vertraulicher die betroffenen Daten sind. Dies spiegelt sich auch auf der Kostenseite wider: Je sensitiver die Daten, desto größer werden der Aufwand und damit auch die Kosten zur Absicherung dieser Daten. Andererseits sollte diese Empfehlung nicht als zwingend verstanden werden. So ist beispielsweise bei der Verlagerung voll verschlüsselter Daten (mehr hierzu nachfolgend unter c)), bei denen ausschließlich der Cloud-Anwender die Schlüssel für die Entschlüsselung hat, eine vergleichbare Vorsicht nicht zwingend geboten. Das Risiko zeitweiser oder dauerhaft fehlender Verfügbarkeit bzw. sogar Löschung von Daten kann überdies durch vergleichsweise günstige und unter vollständiger Kontrolle des Cloud-Anwenders stehende Backup-Lösungen minimiert werden.

b) Transparenz durch Protokollierungen der Datenverarbeitungen

Die Empfehlungen in den Ziffern 3-5, 9, 22 und 23 greifen einen der wichtigsten Punkte beim Cloud Computing aus datenschutzrechtlicher Sicht auf:[15] Die Schaffung von Transparenz im Hinblick auf die erfolgenden Datenverarbeitungen. Zunächst wird eine lückenlose Protokollierung der Orte der physischen Datenverarbeitungen verlangt. Demnach muss dem Cloud-Anwender und ggf. auch der zuständigen Aufsichtsbehörde offen gelegt werden können, welche Daten auf welchen Servern wann verarbeitet worden sind. Dies setzt eine dauerhafte, automatisierte Protokollierung der Datenverarbeitungen durch den Cloud-Anbieter voraus. Dementsprechend muss protokolliert werden, wenn Daten durch den Cloud-Anbieter oder etwaige Unterauftragnehmer kopiert oder gelöscht worden sind. Dies umfasst auch die Erstellung von Backups. Schließlich sind auch alle sonstigen Nutzungen der Daten vom Cloud-Anbieter und seinen Unterauftragnehmern zu loggen. Die Logfiles müssen für den Cloud-Anwender leicht zugänglich und gut verständlich sein. Der Cloud-Anbieter ist dafür verantwortlich, die automatisiert erstellten Logfiles vor nachträglicher Manipulation zu schützen (Datenintegrität).

Solche automatisiert erstellten, nicht kompromittierbaren Protokolldateien sind das wichtigste Instrument für die Kontrolle der Datenverarbeitungen des Cloud-Anbieters bzw. seiner Unterauftragnehmer. Die Erfassung der Orte der physischen Datenverarbeitungen spielt dabei eine besonders große Rolle, da diese beim Cloud Computing sonst kaum überschaubar sind.[16] Ferner kann erst über eine solche Protokollierung nachvollziehbar gemacht werden, ob sich der Cloud-Anbieter an vertraglich zugesicherte Vorgaben bezüglich der Begrenzung der Cloud auf bestimmte Jurisdiktionen gehalten hat. Der Cloud-Anwender solle darüber hinaus eigene Prozesse einführen, die eine regelmäßige, stichprobenartige Kontrolle der Protokolle vorsehen. Ob ein kleines oder mittelgroßes Unternehmen allerdings diesen empfohlenen Kontrollaufwand gewährleisten kann, mag bezweifelt werden. Insofern sollte hier verstärkt, wie auch von der *Berlin Group* unterstützt, auf unabhängige Auditoren zurückgegriffen werden können.

Darüber hinaus soll der Cloud-Anbieter auch eine Liste sämtlicher Unterauftragnehmer sowie eine Beschreibung der von den Unterauftragnehmern durchgeführten Datenverarbeitungen vorhalten.

c) Technischer Datenschutz

In den Ziffern 6 bis 8 verlangt das Working Paper die Einrichtung bestimmter technischer Schutzmaßnahmen.[17]

■ Technische Verhinderung unzulässiger Datentransfers

Mit Blick auf die weitere technische Entwicklung und die Zugriffsmöglichkeiten ausländischer Sicherheitsbehörden fordert das Working Paper die Schaffung eines Verfahrens, das unbefugte Datenübermittlungen in Drittstaaten ohne angemessenes Datenschutzniveau auf technischem Wege ausschließen kann.

Unklar bleibt jedoch, ob der Cloud-Anbieter diese technischen Begrenzungen bereits jetzt anbieten muss oder die *Berlin Group* lediglich eine Entwicklung solcher Maßnahmen anregt. So heißt es einerseits in Ziffer 6, dass derartige technische Schutzmaß-

13 Working Paper (o. Fußn. 1), S. 3 ff.
14 Über § 3 Abs. 9 BDSG hinausgehend bestimmt z.B. Art. 9 Abs. 1 des Entwurfs der EU-DS-GVO auch genetische Daten und solche über Strafurteile als besondere personenbezogene Daten.
15 Working Paper (o. Fußn. 1), S. 3 f. und S. 7, Ziff. 36 f. (background).
16 Working Paper (o. Fußn. 1), S. 7, Ziff. 34 (background).
17 Working Paper (o. Fußn. 1), S. 4.

nahmen „entwickelt werden sollten", in Ziffer 11 wird jedoch bereits verlangt, dass technische Maßnahmen gewährleisten, dass die Daten nur an den mit dem Anwender vereinbarten Orten verarbeitet werden können. Zwar handelt es sich hierbei um eine relativ vage formulierte Maßnahme, deren konkrete Umsetzbarkeit fraglich erscheint. Angesichts der derzeitigen Diskussion über die Nutzbarkeit von US-Cloud-Anbietern wegen der Zugriffsmöglichkeiten von US-Behörden nach dem US Patriot Act[18] erscheint eine technische Lösung jedoch durchaus interessant. Immerhin werden die teilweise geforderten vertraglichen Lösungen wohl kaum einen Zugriff von US-Behörden verhindern können.[19] Ungeachtet einer solchen technischen Lösung fordert die *Berlin Group* in ihrem Working Paper eine international verbindliche Vereinbarung, die den Zugriff ausländischer Sicherheitsbehörden auf Daten, die außerhalb ihrer territorialen Zuständigkeit verarbeitet werden, regelt.[20]

Sichere Löschung

Als weitere technische Schutzmaßnahme verlangt das Working Paper die Möglichkeit der effektiven und sicheren Löschung von Daten in der Cloud. Ein einfaches Löschen, bei dem lediglich die bisher verwendeten Speicherbereiche freigegeben werden („dereference") und ein Überschreiben erst durch erneute Nutzung erfolgt, reiche nicht aus, wenn der neue Nutzer die Möglichkeit des Zugriffs auf die noch nicht überschriebenen Bereiche haben könnte.[21] Eine Lösungsmöglichkeit wäre hier z.B. die sichere Löschung durch Überschreiben mit zufällig erzeugten Daten.

Hervorzuheben und zu begrüßen ist hier der maßvolle Ansatz der *Berlin Group*, qualifizierte Löschungsprozesse nur in den Fällen zu verlangen, in denen die Gefahr des Zugriffs durch den nachfolgenden Nutzer der Cloud-Ressource besteht. Denn aufwendigere Löschungsprozesse benötigen immer auch ein Mehr an Rechenleistung und -zeit und mindern damit gleichzeitig die Leistungsfähigkeit des Systems. Es muss also zunächst für das konkrete Cloud-Angebot geprüft werden, ob eine Zugriffsmöglichkeit für einen nachfolgenden Cloud-Anwender gegeben ist, wie es z.B. bei der generellen Bereitstellung von Speicherplatz der Fall wäre. Erst dann müssen qualifizierte Löschungsverfahren eingesetzt werden. Einen Überblick über verschiedene Methoden der Löschung von Daten bietet der IT-Grundschutz-Katalog des *BSI*.[22]

Verschlüsselung

Auf den technischen Schutz der Daten durch Verschlüsselung geht das Working Paper erfreulicherweise etwas ausführlicher ein.[23] Danach müssen personenbezogene Daten sowohl auf den Übertragungswegen als auch bei der Speicherung mit anerkannten Methoden verschlüsselt sein. Die Schlüssel selbst müssen über eine zeitgemäße Qualität (Länge) verfügen und dürfen nur dem Cloud-Anwender und dem Cloud-Anbieter bekannt sein. Der Cloud-Anbieter muss dabei jedem seiner Kunden eigene Schlüssel zur Verfügung stellen, damit nicht ein Cloud-Anwender die Daten eines anderen entschlüsseln und auf dieselben dann Zugriff haben kann (Umsetzung des Prinzips der Datentrennung). Darüber hinaus müssen die Verarbeitungen der Daten in unverschlüsselter Form so gering wie möglich gehalten werden. Schließlich äußert das Working Paper noch zwei Wünsche an die weitere technische Entwicklung im Bereich der Verschlüsselung: Zunächst werden Rendering-Methoden genannt, die die vom Cloud-Anwender verarbeiteten Daten für den Cloud-Anbieter von Anfang bis Ende unleserlich machen. Als Beispiel wird das deutsche „Sealed Cloud"-Angebot angeführt.[24] Ebenfalls wünschenswert sei die Entwicklung einer technischen Methode, die dem Cloud-Anwender eine Entziehung der Schlüssel des Anbieters für den Fall einer unbefugten Verarbeitung der Daten ermöglicht (eine Art Notbremse).

Die Entwicklung und der Einsatz verschiedener Verschlüsselungstechniken, wie sie das Working Paper hier andeutet, gehören zu den vielversprechendsten Ansätzen beim Ziel des datenschutzkonformen Cloud Computings und sollten deshalb mit hoher Priorität weiter verfolgt werden. Denn auf Grund der oft großen Anzahl beteiligter Unternehmen und Standorte auf Anbieterseite ist die Einhaltung vertraglich zugesicherter (organisatorischer) Maßnahmen meist schwer kontrollierbar, sodass technische Schutzmaßnahmen – wie z.B. durch Verschlüsselung – ein deutlich höheres Maß an Sicherheit versprechen. Wertvolle Best-Practice-Empfehlungen zur Verschlüsselung und zum Schlüsselmanagement finden sich in einem Eckpunktepapier des *BSI*.[25]

Welche Verschlüsselungslösungen für eine konkrete Cloud-Lösung in Betracht kommen, richtet sich vor allem nach der Art des Angebots. Stellt der Anbieter beispielsweise nur IT-Infrastrukturen zur Verfügung (IaaS)[26] und benötigt dabei keine eigenen Datenzugriffe, empfiehlt sich eine Vollverschlüsselung der Daten durch den Anwender, ohne Entschlüsselungsmöglichkeit auf Seiten des Anbieters. Bei der Prüfung der datenschutzrechtlichen Anforderungen kann in dieser Konstellation sogar durchaus hinterfragt werden, ob der Cloud-Anbieter überhaupt noch personenbezogene Daten im Auftrag verarbeitet.[27] Die Stellungnahme der *Art. 29-Datenschutzgruppe* im WP 136 lässt sich jedenfalls in diesem Sinne verstehen[28] und es wäre wünschenswert, wenn auch die deutschen Aufsichtsbehörden diesbezüglich ihre teilweise sehr restriktiven Positionen überdenken.

Aber auch bei erforderlichen Datenzugriffen durch den Anbieter, wie z.B. bei Softwarelösungen in der Cloud (SaaS),[29] sind Verschlüsselungsmaßnahmen als effektive Schutzmaßnahmen in Betracht zu ziehen. Neben dem vom Working Paper genannten „Sealed Cloud"-Angebot gibt es auch andere anpassbare Lösungen, die insbesondere vor der in der Praxis bedeutsamen Gefahr des Insider-Angriffs schützen können.[30] Empfohlen werden z.B. der Einsatz von Hardware-Token für die Entschlüsselung durch Mitarbeiter des Anbieters und die fragmentierte Speicherung von Datenbanken in der Cloud, bei der die einzelnen Teile auf verschiedene Serverstandorte verteilt werden.[31]

18 *Weichert*, „Advanced Topics in European Privacy, Privacy and Data Protection – A Conflict between the US and Europe", abrufbar unter: https://www.datenschutzzentrum.de/vortraege/20120307-weichert-conflict-us-europe.html.
19 S. hierzu *Becker/Nikolaeva*, CR 2012, 170, 175 f.
20 Working Paper (o. Fußn. 1), S. 9, Fußn. 16.
21 Working Paper (o. Fußn. 1), S. 4, Ziff. 7 und Fußn. 11.
22 *Bundesamt für Sicherheit in der Informationstechnik* (*BSI*), IT-Grundschutz-Katalog, Maßnahme M 2.433, abrufbar unter: https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02433.html.
23 Working Paper (o. Fußn. 1), S. 4, Ziff. 8.
24 Informationen zu diesem Angebot abrufbar unter: http://www.sealedcloud.de.
25 *Bundesamt für Sicherheit in der Informationstechnik* (*BSI*), Sicherheitsempfehlungen für Cloud Computing Anbieter, S. 39 ff., abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf.
26 IaaS steht für „Infrastructure as a Service", wie z.B. das EC2-Angebot von *Amazon*, bei dem ganze virtuelle Systeme gemietet werden können.
27 Hierzu bereits ausführlicher *Schröder/Haag*, ZD 2011, 147, 152 m.w.Nw.; außerdem *Stiemerling/Hartung*, CR 2012, 60, 62.
28 S. Beispiel 17 auf S. 18 und 19 des WP 136 der *Artikel-29 Datenschutzgruppe*, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf.
29 SaaS steht für „Software as a Service", wie z.B. die Büroanwendungen „Google Docs" oder „Office 365" von Microsoft.
30 Nach einer US-Studie gehen ca. ein Drittel aller Angriffe auf IT-Systeme, bei denen ein Schaden entsteht und der Angreifer identifiziert werden kann, von eigenen (z.B. unzufriedenen) Mitarbeitern aus, abrufbar unter: http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymatters200702.cfm.
31 *Achenbach/Gabel/Huber*, MimoSecco: A Middleware for Secure Cloud Storage, in: *Frey/Fukuda/Rock*, Improving Complex Systems Today, London 2011, abrufbar unter: http://books.google.de/books?id=06jEWTS3uiUC.

Microsoft forscht daneben an einem Algorithmus, der Datenverarbeitungen durch den SaaS-Anbieter ermöglicht, ohne dass dieser die enthaltenen (personenbezogenen) Daten entschlüsseln muss.[32]

d) Vertragsgestaltung

Neben den erwähnten technischen Maßnahmen legt die *Berlin Group* besonderen Wert auf eine klare und im Vergleich zur bisherigen Praxis deutlich detailliertere und für den Cloud-Anwender verbesserte Vertragsgestaltung. So bemängelt die *Berlin Group* vor allem, dass der Cloud-Dienstemarkt derzeit durch wenige Anbieter geprägt sei, die bisher geringes Interesse an einer Transparenz ihrer Dienstleistungen gezeigt hätten. Dies führe zu einem erheblichen Informationsdefizit der Anwender, welches ihnen eine ausreichende Risikobewertung kaum ermöglicht.

Ähnlich wie schon die Orientierungshilfe Cloud Computing der deutschen Aufsichtsbehörden[33] verlangt daher auch die *Berlin Group* eine vertraglich abgesicherte, deutlich verbesserte Transparenz. Nach den Ziffern 10 bis 13 des Working Papers soll diese u.a. durch eine abschließende Auflistung aller Standorte, an denen Daten durch den Cloud-Anbieter oder dessen Unterauftragnehmer physisch verarbeitet werden können (einschließlich Backups), gewährleistet werden. Ebenso sei vertraglich festzulegen, dass Daten unter keinen Umständen an nicht gelistete Standorte gelangen dürfen. Darüber hinaus soll der Cloud-Anwender jederzeit die Möglichkeit haben, sämtliche Verarbeitungsorte zu besichtigen und Zugriffe auf sämtliche Informationen zu haben, die er – nach seinem Ermessen – für notwendig hält, um die Einhaltung der Vereinbarung prüfen zu können.[34] In den Verträgen soll ferner ein Recht vorgesehen sein, dass anerkannte Auditoren entweder Teile oder die gesamte Datenverarbeitung prüfen können.

Vertragliche Vereinbarungen sollen zudem sicherstellen, dass die Betroffenen ihre Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung der Daten jederzeit ausüben können. Schließlich soll vertraglich vereinbart sein, dass der Cloud-Anwender und bzw. oder die Aufsichtsbehörde unverzüglich über unbefugte Weitergabe von Daten an Dritte/Verlust von Daten (Security Breach) informiert werden, sodass Maßnahmen zum Abwenden weiteren Schadens getroffen werden können.

Den deutschen bzw. europäischen Rechtsanwender mögen diese Vorgaben zunächst nicht sehr erstaunen, da sie sich weitgehend an dem europäischen bzw. deutschen Konzept einer Auftragsdatenverarbeitung[35] orientieren und lediglich vereinzelt darüber hinausgehende cloud-spezifische Anforderungen formulieren. Berücksichtigt man jedoch, dass es sich bei der *Berlin Group* nicht um ein Treffen ausschließlich europäischer Aufsichtsbehörden handelt, überrascht die sehr starke Anlehnung des Working Papers an die europäischen Datenschutzvorgaben.

Ingesamt erscheinen die Vorgaben für die vertragliche Gestaltung umsetzbar, wenn auch im Einzelnen sicher noch etwas überarbeitungsbedürftig. So wird z.B. ein Cloud-Anbieter kaum die Anforderung umsetzen können, den Anwendern vertraglich Zugang zu sämtlichen Informationen zuzusichern, die diese – nach ihrem eigenen Ermessen – für die Prüfung der Einhaltung der vertraglichen Verpflichtungen für notwendig halten.

Ferner übernimmt das Working Paper leider auch die bereits von den deutschen Aufsichtsbehörden in der Orientierungshilfe Cloud-Computing enthaltene Forderung, der Cloud-Anbieter müsse vorab über sämtliche Datenverarbeitungsorte und Unterauftragnehmer informieren.[36] Einerseits wird diese Anforderung nicht der dynamischen Entwicklung von Cloud-Dienstleistungen gerecht. Andererseits ist auch der hiervon erhoffte Vorteil für den Datenschutz nicht ersichtlich. Für die Risikobewertung dürfte es keinen Unterschied machen, ob die Datenverarbeitung innerhalb einer vertraglich klar vereinbarten Jurisdiktion, aber an unterschiedlichen und wechselnden Orten stattfindet. Eigentlich sollte hier die vertragliche Zusicherung der Jurisdiktionen sowie die von der *Berlin Group* ebenfalls geforderte Zurverfügungstellung der Log-Files genügen, um ggf. schnell Audits durchführen zu können.[37]

Neben der Zusicherung der Verarbeitungsorte verlangt das Working Paper noch die unmissverständliche vertragliche Festlegung der Weisungsgebundenheit des Cloud-Anbieters und der Zweckbindung der Datenverarbeitung. Für die Praxis ist dabei der in diesem Rahmen gegebene Hinweis interessant, dass der Cloud-Anbieter durchaus einseitig Änderungen des Vertrags vornehmen darf (Ziffer 12, aber in Widerspruch zur Anforderung in Ziffer 24). Allerdings müsse dann sichergestellt sein, dass diese Änderungen nicht nur dem Vertragspartner bekanntgegeben werden müssen, sondern dass auch jede Änderung (z.B. der Orte) zu einem sofortigen Kündigungsrecht des Cloud-Anwenders führt.[38] Grundsätzlich erscheint diese Änderungsmöglichkeit durchaus sachgerecht. Allerdings sollte in der Praxis das Kündigungsrecht nicht bereits dann eingreifen, wenn Änderungen vorgenommen werden, die materiell nicht zu einer veränderten Risikobewertung führen. Beispielsweise kann ein Austausch des Verarbeitungsorts von München nach Düsseldorf allein nicht zu einer veränderten Risikobewertung führen und sollte damit kein Kündigungsrecht begründen.

Zudem müssen effektive Kontrollmaßnahmen definiert werden, um die Einhaltung vertraglicher Regelungen sicherzustellen. Hierfür sind die bereits dargestellten technischen Schutzmaßnahmen, wie etwa die Erstellung von Protokollen, vertraglich festzulegen. Diese bieten eine wirksamere Kontrollmöglichkeit als die vorgeschlagene Vereinbarung einer Vertragsstrafe, da mit dieser allein noch keine Verstöße aufgedeckt werden können und sie für den Cloud-Anbieter meist nicht annehmbar ist.[39] Schließlich müssen deutsche Cloud-Anwender selbstverständlich auch die Regelungen aus § 11 Abs. 2 i.V.m. § 9 BDSG beachten bzw. im Falle der Datenverarbeitung in Drittstaaten die Vorgaben der §§ 4b, 4c BDSG.

e) Pflichten des Cloud-Anwenders

Neben der Pflicht zur hinreichenden Vertragsgestaltung treffen den Cloud-Anwender auch nach diesem internationalen Working Paper weitere sehr weitgehende Pflichten, vgl. Empfehlungen in Ziffern 16 bis 19. So soll der Cloud-Anwender vor Nutzung eines Cloud-Dienstes eine umfassende Risikobewertung vornehmen, die die spezifischen Bedingungen und Gegebenheiten der Datenverarbeitung berücksichtigt. Insbesondere sollen die Orte, an denen die Datenverarbeitung durch den Cloud-Anbieter und seine Unterauftragnehmer stattfindet, für die Einschätzung des mit der Cloud verbundenen Risikos für die Datenverarbeitung berücksichtigt werden. Diese Risikobewertung soll regelmäßig aktualisiert werden. Ferner soll der Cloud-Anbieter prüfen, ob er eine tatsächliche Exit-Option hat, die es ihm z.B. über einen Datentransfer ermöglicht, den Anbieter zu wechseln

32 Datenanalyse von verschlüsselten Cloud-Daten, http://www.heise.de/newsticker/meldung/Datenanalyse-an-verschluesselten-Cloud-Daten-1324757.html.
33 Orientierungshilfe – Cloud Computing (o. Fußn. 3), S. 10.
34 Working Paper (o. Fußn. 1), Ziff. 14.
35 Zur Auftragsdatenverarbeitung bei Cloud Dienstleistungen *Winkelmann*, „Cloud Computing: Sicherheit und Datenschutz", Arbeitspapier für die Alcatel-Lucent Stiftung v. 22.11.2010, S. 21, abrufbar unter: http://www.stiftungaktuell.de/files/cloudcomputing_winkelmann.pdf.
36 Orientierungshilfe – Cloud Computing (o. Fußn. 3), S. 10.
37 S. *Schröder/Haag*, ZD 2011, 147, 149.
38 Working Paper (o. Fußn. 1), S. 4.
39 S. *Schröder/Haag*, ZD 2011, 147, 149.

oder ob er an diesen gebunden ist. Schließlich soll der Cloud-Anwender prüfen, ob er eine Kopie sämtlicher Daten außerhalb der Verfügungsgewalt des Anbieters benötigt. Falls dies für erforderlich gehalten wird, soll der Anwender sicherstellen, dass er diese Kopie auch ohne Mitwirkung des Cloud-Anbieters nutzen kann.

Aus europäischer Sicht nachvollziehbar ist der auch im Working Paper der *Berlin Group* vertretene Ansatz, dem Cloud-Anwender weitreichende Kontroll- und Risikobewertungspflichten aufzuerlegen.[40] Leider sind dies in der Praxis für den kleineren und mittleren Anwender jedoch wenig greifbare Vorgaben, die zudem häufig mangels eigenen Know-hows bzw. Personals nicht umsetzbar sind. Besser wäre es hier, dem Anwender konkrete Möglichkeiten aufzuzeigen, diesen Pflichten auch nachkommen zu können. Ein hilfreicher Ansatz wäre z.B. das Mitentwickeln und/oder Anerkennen von Sicherheits-Benchmarks, die dem Anwender einen Vergleich der Anbieter ermöglichen. Eine auf solchen Benchmarks erfolgte Auswahl des Cloud-Dienstanbieters könnte dann auch das Haftungsrisiko des Anwenders reduzieren.

Nicht nur für Cloud-Dienste sachgerecht erscheint aber die Empfehlung, sich vor Nutzung eines Cloud-Dienstes über eine Exit-Option zu informieren bzw. ggf. Kopien der Daten vorzuhalten.

f) Audits

Angesichts der Massenspeicherung von Daten verlangt das Working Paper, dass sich Cloud-Anbieter neben der Überwachung durch den Cloud-Anwender auch regelmäßig selbst der Prüfung von anerkannten und unabhängigen Auditoren auf Einhaltung der in diesem Working Paper genannten Maßnahmen unterstellen.

40 Aus der Verpflichtung als verantwortliche Stelle folgend, s. *Petri*, in: Simitis, BDSG, 7. Aufl. 2011, § 11 Rdnr. 30; *Schröder/Haag*, ZD 2011, 147, 148.

Schade ist bei diesem an sich sinnvollen Vorschlag jedoch erneut, dass sich der Cloud-Anwender nicht auf die Prüfung durch anerkannte und unabhängige Dritte verlassen können soll, obwohl diese im Zweifel weit bessere Prüfungsmöglichkeiten haben als der einzelne Cloud-Anwender.

IV. Bewertung und Ausblick

Das Working Paper der *Berlin Group* ist ein deutliches Zeichen dafür, dass die bisher aus allein europäischer Perspektive formulierten Anforderungen an Cloud-Computing offenbar zunehmend weltweit Akzeptanz finden. Wenngleich im Einzelnen noch nicht in Gänze überzeugend, können daher die in dem leider etwas schwer lesbaren Working Paper enthaltenen Vorgaben durchaus Maßstab für zukünftige Gestaltungen von Cloud-Diensten in vertraglicher und technischer Sicht werden. Das Working Paper hebt zu Recht die wirtschaftliche Bedeutung von Cloud-Lösungen hervor und setzt nachvollziehbare Schwerpunkte bei der Vertragsgestaltung und technischen Anforderungen. Dabei ist sehr zu begrüßen, dass offenbar der technische Datenschutz zukünftig noch mehr Gewicht erhält als bloße vertragliche Abreden. Letztlich lässt das Working Paper aber noch viel Raum für weitere Entwicklungen und Lösungsansätze insbesondere für die Regelung des Zugriffs ausländischer Sicherheitsbehörden.

Dr. Christian Schröder
ist Rechtsanwalt und Leiter des Fachbereichs IP/IT der BDO Legal Rechtsanwaltsgesellschaft mbH in Düsseldorf sowie Mitglied des Wissenschaftsbeirats der ZD.

Dr. Nils Christian Haag
ist Rechtsanwalt und als Consultant für Datenschutz und IT-Compliance bei der intersoft consulting services AG in Hamburg tätig.