CHRISTIAN SCHRÖDER / NILS CHRISTIAN HAAG

Neue Anforderungen an Cloud Computing für die Praxis

Zusammenfassung und erste Bewertung der „Orientierungshilfe – Cloud Computing"

Internationale Clouds
Technische und organisatorische Anforderungen
Vertragsgestaltung von Cloud-Diensten
Outsourcing
Mindestanforderungen

■ Die Datenschutzbeauftragten des Bundes und der Länder haben am 28./29.9.2011 auf der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine „Orientierungshilfe – Cloud Computing" verabschiedet, die die aus Sicht der Datenschutzbeauftragten wichtigsten Risiken bei der Datenverarbeitung in Clouds aufzeigt, Anforderungen an die vertragliche Ausgestaltung von Cloud-Diensten stellt und Empfehlungen zu den technischen und organisatorischen Anforderungen gibt. Da diese Orientierungshilfe die derzeitige Sicht der Aufsichtsbehörden für den privaten Bereich wiedergibt und die Nutzung von Clouds bisher rechtlich weitgehend unklar war, ist die Orientierungshilfe für die Praxis von herausgehobener Bedeutung. Der Schwerpunkt des Beitrags liegt daher zunächst in der zusammenfassenden Erläuterung der Orientierungshilfe und enthält eine erste kritische Bewertung.

■ On September 28/29, 2011, at the 82nd Conference of Data Protection Officers of the Federation and the Federal States, the Data Protection Officers of the Federation and the Federal States passed an "Orientation Help – Cloud Computing", which from the Data Protection Officers' point of view demonstrates the major risks of data processing in clouds, sets requirements for the contractual set-up of cloud services and gives recommendations regarding the technical and organizational requirements. As this Orientation Help details the current supervisory authorities' view for the private sector and up until now the usage of clouds was mainly unclear from a legal perspective, the Orientation Help is of immense importance for practice. Thus, the emphasis of this article is in the summary explanation of the Orientation Help and contains a first critical assessment.

I. Einleitung

Auf der *82. Konferenz der Deutschen Datenschutzbeauftragten des Bundes und der Länder* haben die *Arbeitskreise Technik und Medien* eine Orientierungshilfe zum Cloud Computing – Stand 1.0 vorgestellt, die nachfolgend auf der *Konferenz* von den Teilnehmern verabschiedet wurde.[1] Nach dem Verständnis der öffentlichen Datenschutzbeauftragten richtet sich die Orientierungshilfe an Entscheidungsträger sowie betriebliche und örtliche Datenschutzbeauftragte und soll Anforderungen an die vertragliche Gestaltung von Cloud-Diensten sowie technische und organisatorische Risiken aufzeigen, aber bezüglich Letzterer auch mögliche Maßnahmen nennen, mit denen den vorgenannten Risiken datenschutzgerecht begegnet werden kann. Die *Datenschutzbeauftragten des Bundes und der Länder* betonen dabei zwar einerseits deutlich die wirtschaftlichen Vorteile der Nutzung von Clouds und empfehlen sogar öffentlichen Stellen ihre Nutzung, andererseits werden aber teilweise Anforderungen an Cloud-Diensteanbieter festgehalten, die weit über die Anforderungen des § 11 BDSG hinausgehen. Auch bleiben manche für die Praxis wichtigen Fragen wie z.B. die der Zulässigkeit von Clouds von US-amerikanischen Anbietern unbeantwortet.

Da diese Orientierungshilfe die derzeitige Sicht der Aufsichtsbehörden für den privaten Bereich wiedergibt und die Nutzung von Clouds bisher rechtlich weitgehend unklar war, ist die Orientierungshilfe für die Praxis von herausgehobener Bedeutung. Der Schwerpunkt des Beitrags liegt daher zunächst in der zusammenfassenden Erläuterung der Orientierungshilfe und enthält eine erste kritische Bewertung.[2]

II. Neue Anforderungen an Clouds

1. Vorteile der Nutzung von Cloud-Dienstleistungen und Terminologie

Nach der Orientierungshilfe versteht man unter Cloud Computing eine „Datenverarbeitung in der Wolke", eine über Netze angeschlossene Rechnerlandschaft, in welche die eigene Datenverarbeitung ausgelagert wird.[3] Dabei können sich die i.R.e. Cloud erbrachten externen IT-Dienstleistungen auf Anwendungen, Plattformen für Anwendungsentwicklungen und -betrieb sowie auf die Basis-Infrastruktur beziehen.[4] Die wichtigsten drei Begriffe für Organisationsformen von Cloud Services sind:

- „Software as a Service" (SaaS),
- „Platform as a Service" (PaaS) und
- „Infrastructure as a Service" (IaaS).

Ferner unterscheidet die Orientierungshilfe zwischen „Public Clouds", „Private Clouds", „Community Clouds" und „Hybrid Clouds". Da das Verständnis dieser Begriffe insbesondere für die Erläuterung der technischen und organisatorischen Anforderungen an Clouds notwendig ist, definiert die Orientierungshilfe die wichtigsten Begriffe wie folgt:

■ Stellt der Cloud-Anbieter virtualisierte Komponenten zur Datenverarbeitung, zum Datentransport oder zur Datenspeicherung zur Verfügung, bei denen die Anwender nahezu beliebige Anwendungsprogramme und Betriebssysteme einsetzen können, handelt es sich um ein „Infrastructure as a Service"(IaaS)-Angebot.

■ Diskutieren Sie dieses Thema auch in der ZD-Community unter: https://community.beck.de

1 Orientierungshilfe – Cloud Computing, abrufbar unter: http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf.

2 Ein besonderer Dank gilt *Maximilian Ahrens* (CPO der Zimory GmbH, Berlin) für seine Hinweise zu technischen und praktischen Aspekten.

3 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 4; Verweis auf *Weichert*, DuD 2010, 679.

4 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 4.

- Bei einer „Platform as a Service" (PaaS) stellt der Anbieter eine Plattform zur Verfügung, bei der er Vorgaben zu den verwendeten Programmiersprachen und Schnittstellen zu Datenspeichern, Netzwerken und Datenverarbeitungssystemen der Cloud macht. Der Cloud-Anwender hat keine Möglichkeit, administrativ oder kontrollierend auf die zur Bereitstellung des Dienstes genutzte Infrastruktur zuzugreifen.
- Häufig stellt der Anbieter auch bereits ganze Anwendungen zur Verfügung – „Software as a Service" (SaaS), auf die üblicherweise über das Internet zugegriffen werden kann. Diese Anwendungen können regelmäßig nur im geringen Umfang an die Bedürfnisse des Anwenders angepasst werden. Ferner hat der Cloud-Anwender wie bei PaaS keine Möglichkeit, auf die zur Bereitstellung des Dienstes genutzte Infrastruktur administrativ oder kontrollierend zuzugreifen.

Während i.R.e. „Public Cloud" IT-Dienstleistungen durch einen Anbieter (z.B. von *Amazon*, *Apple*, *Google*, *Microsoft*, *Telekom* u.a.) für eine beliebige Zahl von Cloud-Anwendern angeboten werden,[5] werden die IT-Dienstleistungen bei „Private Clouds" ausschließlich innerhalb einer Institution oder innerhalb eines Unternehmensbereichs einer verantwortlichen Stelle angeboten. Insofern gehören bei „Private Clouds" Cloud-Anwender und Cloud-Anbieter der gleichen verantwortlichen Stelle an.[6] Bei einer „Community Cloud" schließen sich zwei oder drei Cloud-Anbieter aus „Private Clouds" zusammen, um für einen definierten Kundenkreis IT-Dienstleistungen zu erbringen. Wie schon aus dem Wort hervorgeht, stellen „Hybrid Clouds" eine Mischform aus Public, Private oder Community Clouds dar.

Die Orientierungshilfe betont nachfolgend insbesondere die erheblichen wirtschaftlichen Vorteile, die für die Nutzung von Cloud-Dienstleistungen sprechen: Clouds bieten die Möglichkeit, je nach aktuellem und ggf. kurzfristigem Bedarf flexibel Rechenkapazitäten zu buchen, zu nutzen bzw. stillzulegen. Cloud-Dienstleistungen können relativ einfach in Anspruch genommen werden, es erfolgt eine abhängige Bezahlung. Ein großer Vorteil aber ist, dass bei Clouds Geschäftsanwendungen ohne jede geografische Beschränkung verfügbar sind.

2. Datenschutzrechtliche Besonderheiten von Clouds

Ohne Eingehen auf die territoriale Anwendbarkeit des BDSG hält die Orientierungshilfe fest, dass Clouds, über die personenbezogene Daten erhoben, verarbeitet oder genutzt werden, den Anforderungen des BDSG unterliegen. Die Orientierungshilfe weist darauf hin, dass sich für öffentliche Stellen entsprechende Regelungen in den Landesdatenschutzgesetzen finden, und erwähnt die Anforderungen nach § 80 SGB X, beschränkt sich aber im Nachfolgenden auf die Darstellung der Anforderungen nach dem BDSG.

Vor Beschreibung der einzelnen vertraglichen und technisch-organisatorischen Umsetzungsanforderungen fasst die Orientierungshilfe zunächst die aus ihrer Sicht für Datenverarbeitung in der Cloud bestehenden datenschutzrechtlichen Besonderheiten wie folgt zusammen:

a) Besondere Gefährdung für anonymisierte Dateien

Nach der Orientierungshilfe bergen Clouds die besondere Gefahr, dass anonyme Daten durch Zusatzwissen des Cloud-Anbieters oder anderer Nutzer re-identifizierbar werden.[7] Diesem auch von *Weichert* geäußerten Hinweis[8] liegt ein objektives und damit sehr weites Verständnis der Personenbeziehbarkeit von Daten zu Grunde. Versteht man die Personenbeziehbarkeit eines Datums hingegen mit der h.M. relativ,[9] ist zu berücksichtigen, dass der Cloud-Anbieter (Auftragsdatenverarbeiter) die Vorgaben des § 11 BDSG, insbesondere auch die der Trennung von Daten, zu beachten hat. Er darf daher gerade nicht sein von einem Nutzer gewonnenes Zusatzwissen mit Daten anderer Nutzer zusammenführen. Abgesehen davon, dass gerade bei unstrukturierten Datenbanken ein solcher Austausch auch selten praktisch möglich wäre, ist folglich das Zusatzwissen des Cloud-Anbieters aus rechtlichen Gründen dem Cloud-Anwender nicht zuzuordnen. Die aus dessen Sicht anonymen Daten bleiben auch dann anonym, wenn andere Anwender der Cloud oder der Cloud-Anbieter selbst über Zusatzwissen verfügen, welches das Datum einer Person zuordnen könnte. Die Orientierungshilfe hat an dieser Stelle leider auch die für die Praxis zunehmend interessante Frage nicht aufgegriffen, ob eine hohe Verschlüsselung der Daten, bei der ausschließlich der Anwender den Schlüssel hat, zu einer Anonymisierung der Daten führt (hierzu ausführlicher in II. 6. e)).

b) Gewährleistung der Rechtmäßigkeit der Datenverarbeitung

Neben der besonderen vertraglichen Einbindung sämtlicher an der Dienstleistung Beteiligter muss die verantwortliche Stelle die Rechtmäßigkeit der Datenverarbeitung sicherstellen und dabei insbesondere gewährleisten, dass die Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung und Löschung nach §§ 34 und 35 BDSG beachtet werden. Bei internationalen Clouds finden zudem die Vorgaben der §§ 4b und 4c BDSG Anwendung, wonach grundsätzlich ein dem europäischen Datenschutzrecht vergleichbarer Standard zu gewährleisten ist (hierzu mehr unter II. 4. und II. 5.).

c) Technische und organisatorische Maßnahmen

Schließlich sind aus technischer und organisatorischer Sicht besondere Vorkehrungen für die Löschung und Trennung von Daten sowie für die Sicherstellung von Transparenz, Integrität und Revisionsfähigkeit der Daten zu treffen (hierzu mehr unter II. 6.).

3. Cloud-Anwender ist verantwortliche Stelle

Nach der Orientierungshilfe handelt es sich bei der Verarbeitung von personenbezogenen Daten über Cloud-Dienste regelmäßig um eine Auftragsverarbeitung i.S.d. § 11 BDSG bzw. bei internationalen Sachverhalten um eine Übermittlung i.S.d. § 28 Abs. 1 Nr. 2 BDSG. Diese Einstufung von Cloud-Dienstleistungen als Auftragsdatenverarbeitung entspricht dem allgemeinen Verständnis.[10] Hiernach ist grundsätzlich der Auftraggeber der Cloud-Dienste, der Cloud-Anwender, die verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG; der Cloud-Anbieter ist Auftragnehmer, der die Daten nur nach Weisung des Cloud-Anwenders verarbeiten darf.

4. Allgemeine Vorgaben für die Vertragsgestaltung

a) Umsetzung der Anforderungen nach § 11 Abs. 2 Satz 2 BDSG

Bei einer Auftragsdatenverarbeitung gelten die Vorgaben des § 11 BDSG. Der Cloud-Anwender muss daher mit dem Cloud-Anbieter einen schriftlichen Vertrag abschließen, der sämtliche

5 Vgl. *Weichert*, DuD 2010, 679, 680.

6 *Weichert*, DuD 2010, 679, 680 weist darauf hin, dass auch Clouds innerhalb eines Konzerns, d.h. verschiedener verantwortlicher Stellen als „Private Clouds" bezeichnet werden.

7 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 5.

8 *Weichert*, DuD 2010, 679, 681.

9 *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rdnr. 26; *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rdnr. 10 m.w.Nw.

10 *Petri*, in: Simitis (o. Fußn. 9), § 11 Rdnr. 30; *Gola/Schomerus* (o. Fußn. 9), § 11 Rdnr. 8; *Schulz*, MMR 2010, 75, 78; *Weichert*, DuD 2010, 679, 682; *Schuster/Reichl*, CR 2010, 38, 41; *Niemann/Paul*, K&R 2009, 444, 449; *Heidrich/Wegener*, MMR 2010, 803, 806.

Anforderungen des § 11 Abs. 2 BDSG erfüllt. Ein Verstoß gegen diese Verpflichtungen ist gem. § 43 Abs. 1 Nr. 2b BDSG bußgeldbewehrt. § 11 Abs. 2 Satz 2 führt zehn Mindestanforderungen an den Inhalt einer Auftragsvereinbarung auf, die in der Orientierungshilfe nicht sämtlich wiederholt werden. Die Orientierungshilfe verweist hierzu auf die Mustervereinbarungen zur Auftragsdatenverarbeitung des *Hessischen Datenschutzbeauftragten*.[11] Allerdings konkretisiert die Orientierungshilfe die vertraglichen Anforderungen für Cloud-Dienste wie folgt:

- Zu den nach § 11 Abs. 2 Satz 2 Nr. 4 BDSG vertraglich zu regelnden Rechten zur Berichtigung, Löschung und Sperrung verweist die Orientierungshilfe auf ihre Empfehlungen zu technischen und organisatorischen Maßnahmen. Abgesehen von den Hinweisen zu den bei Clouds im Zusammenhang mit einer Löschung bestehenden Risiken finden sich in der Orientierungshilfe nachfolgend jedoch keine Lösungsvorschläge. Für den Anwender bleibt daher offen, wie er über pauschale vertragliche Verpflichtungen zur Einhaltung der vorgenannten Rechte hinausgehend die Umsetzung derselben regeln soll.
- Die Orientierungshilfe verweist ferner auf die in der Praxis bei Cloud-Dienstleistungen schwierig zu gewährleistende Transparenz von Unterbeauftragungen. Unterbeauftragungen können im Einzelfall je nach abgefragter Rechenkapazität kurzfristig erfolgen. Zur Lösung dieses Problems verlangt die Orientierungshilfe unter Bezugnahme auf die Anforderung des § 11 Abs. 2 Satz 2 Nr. 6 BDSG, dass der Cloud-Anbieter vertraglich verpflichtet wird, sämtliche Unteranbieter abschließend gegenüber dem Cloud-Anwender zu benennen und die für § 11 Abs. 2 BDSG relevanten Inhalte offenzulegen.[12] Diese Anforderung geht über das bisherige Verständnis des § 11 Abs. 2 Satz 2 Nr. 6 BDSG deutlich hinaus, wonach lediglich geklärt werden muss, ob und unter welchen Bedingungen Datenverarbeitungen im Unterauftragsverhältnis zulässig sind.[13] Eine Offenlegung sämtlicher Unterauftragsverhältnisse, und sogar bei Abschluss des Hauptvertrags abschließende Festlegung, ist nicht zwingend notwendig.[14]
- Die Orientierungshilfe fordert zudem, dass der Cloud-Anwender zu Beginn über sämtliche möglichen Verarbeitungsorte vorab informiert wird.[15] Leider begründet die Orientierungshilfe diese Anforderung nicht. Es erscheint jedoch schwer nachvollziehbar, dass die Kenntnis, dass Daten nicht nur in Stuttgart, sondern auch in Paris und Frankfurt verarbeitet werden können, dem Cloud-Anwender eine bessere Kontrollmöglichkeit gibt. Dies kann allenfalls für Audits eine Rolle spielen. Insofern sollte genügen, dass der Cloud-Anbieter verpflichtet wird, auf Anfrage die jeweils aktuell genutzten Standorte mitzuteilen.
- Darüber hinaus unterstellt die Orientierungshilfe bei Cloud-Anbietern grundsätzlich ein höheres Risiko eines auftragswidrigen Umgangs mit personenbezogenen Daten. Diesem Risiko könne insbesondere dadurch entgegengewirkt werden, dass eine weisungswidrige Datenverarbeitung unter Vertragsstrafe gestellt wird.[16] Warum gerade Cloud-Anbieter zur weisungswidrigen Datenverarbeitung neigen sollen, lässt die Orientierungshilfe offen. Die Unterstellung dürfte daher für Cloud-Diensteanbieter schwer nachvollziehbar sein. Insofern ist zweifelhaft, ob Anbieter die ebenfalls über die Anforderungen des § 11 BDSG hinausgehende Forderung nach Absicherung durch Vertragsstrafen akzeptieren werden. Da die Orientierungshilfe andererseits bestätigt,[17] dass für den Anwender einer Cloud-Dienstleistung kaum eine Möglichkeit zur Kontrolle der Anbieter besteht, dürfte zudem der mit der Vertragsstrafe erhoffte Vorteil ungewiss sein (weitere vertragliche Regelungen insbesondere zur technischen und organisatorischen Datensicherheit vgl. unter II. 6.).

b) Umsetzung der Anforderungen nach § 11 Abs. 2 Satz 4 BDSG

Nach § 11 Abs. 2 Satz 4 BDSG muss sich der Auftraggeber vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen. Diese Kontrolle ist nach Satz 5 zu dokumentieren. Auch ein Verstoß gegen diese Verpflichtung ist nach § 43 Abs. 1 Nr. 2b BDSG bußgeldbewehrt. Angesichts der regelmäßig faktischen Unmöglichkeit, dieser Verpflichtung nachzukommen, ist positiv zu bewerten, dass die Orientierungshilfe das Einholen von Zertifizierungen durch unabhängige Prüfer empfiehlt.[18] Auch soll der Auftragsdatenverarbeiter vertraglich dazu verpflichtet werden, entsprechende Zertifizierungen bei seinen Unterauftragsdatenverarbeitern einzuholen und dem Anwender auf Verlangen vorhandene Nachweise vorzulegen. Aus Sicht der Praxis bedauerlich ist aber, dass sich die Orientierungshilfe nicht der Ansicht von *Weichert*[19] anschließt und selbst bei positiver Zertifizierung von einem Fortbestehen der Prüfpflichten des Anbieters ausgeht.[20] Mit dem Hinweis auf fortbestehende Verpflichtungen entfällt aber ein starker Anreiz für den Diensteanbieter, sich extern kostenintensiv zertifizieren zu lassen. Ferner bleibt offen, welche Maßnahmen der Anwender über die Abfrage der Zertifizierung hinaus durchführen könnte, um seiner Kontroll- und Überwachungspflicht nachzukommen. Im Ergebnis bleibt leider eine hohe Rechtsunsicherheit bezüglich der Erfüllung von Kontrollpflichten.[21]

c) Gewährleistung der Betroffenenrechte

Wie schon hinsichtlich der weisungsgemäßen Verarbeitung im Allgemeinen sollen Vertragsstrafenregelungen auch die Gewährleistung der Betroffenenrechte auf Auskunft, Löschung, Berichtigung und Sperrung sicherstellen. Entsprechende Rechte sollten auch gegenüber Unterauftragnehmern geregelt werden. Handelt es sich bei einem Cloud-Diensteanbieter nicht um ein bereits als seriös bekanntes Unternehmen, erscheint eine Vertragsstrafenregelung in der Tat als eine interessengerechte Möglichkeit zur Durchsetzung dieser Rechte.

5. Vertragsgestaltung bei internationalen Clouds

a) Zusätzliche Anforderungen bei Clouds außerhalb der EU/des EWR

Bei Cloud-Anbietern mit Standorten außerhalb der EU/des EWR ist gem. §§ 4b, 4c BDSG grundsätzlich ein dem europäischen Datenschutz vergleichbares Schutzniveau zu gewährleisten. Dies kann z.B. durch Abschluss der sog. Standardvertragsklauseln oder auch Binding Corporate Rules, vgl. § 4c Abs. 2 BDSG, geschaffen werden. Bei in den USA ansässigen Anbietern kann auch über das sog. „Safe Harbor Program" ein hinreichendes Schutzniveau gewährleistet werden. Bezüglich Safe Harbor-zertifizierter Anbieter erinnert die Orientierungshilfe an die bereits

11 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 8 unter Hinweis auf http://www.datenschutz.hessen.de/mustervereinbarung_auftrag.htm.
12 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 8, 20.
13 Keine weitergehenden Forderungen festhaltend *Petri*, in: Simitis (o. Fußn. 9), § 11 Rdnr. 30; *Gola/Schomerus* (o. Fußn. 9), § 11 Rdnr. 8; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 11 Rdnr. 44.
14 Auch darauf hinweisend, dass eine Offenlegung sämtlicher Unterauftragsverhältnisse häufig nicht möglich ist, *Schuster/Reichl*, CR 2010, 38, 42.
15 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 10.
16 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 8.
17 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 16.
18 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 9, 21; zur Auswahl zertifizierter Cloud-Anbieter *Giebichenstein/Weiss*, DuD 2011, 338 ff.
19 Für keine weitergehenden Kontrollpflichten *Weichert*, DuD 2010, 679, 683; aufgegriffen von *Heidrich/Wegener*, MMR 2010, 803, 806.
20 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 9.
21 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 9.

2010 allgemein zu Safe Harbor-zertifizierten Auftragsdatenverarbeitern veröffentlichten Anforderungen.[22]

Die Orientierungshilfe weist insbesondere auf die Möglichkeit hin, dass Cloud-Anbieter das erforderliche vergleichbare Schutzniveau durch Abschluss der von der *EU-Kommission* angenommenen Standardvertragsklauseln für Auftragsdatenverarbeiter sichern können.[23] Dabei greift die Orientierungshilfe die bereits zuvor von verschiedenen Aufsichtsbehörden geäußerte und in der Literatur umstrittene Ansicht auf,[24] wonach selbst bei Anwendung der Standardvertragsklauseln für Auftragsdatenverarbeiter die Anforderungen des § 11 BDSG analog anzuwenden und vollständig umzusetzen sind.[25] Dementsprechend ist nun sicherzustellen, dass zumindest über ergänzende Vereinbarungen in den Anlagen zu den Standardvertragsklauseln sämtliche Anforderungen des § 11 BDSG erfüllt sind.

Da die Orientierungshilfe jedoch nicht von einer automatischen Privilegierung der Auftragsdatenverarbeitung im außereuropäischen Ausland ausgeht, sondern grundsätzlich eine Interessenabwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG verlangt, können in solchen Clouds sensitive Daten (besondere Arten personenbezogener Daten gem. § 3 Abs. 9 BDSG) in der Regel nicht verarbeitet werden. Die für sensitive Daten in § 28 Abs. 6 BDSG festgehaltenen Anforderungen sind bei Clouds regelmäßig nicht einschlägig.

Wenngleich diese Einschränkung in Bezug auf sensitive Daten die Nutzung von außereuropäischen Clouds begrenzt, ist dem Hinweis der Orientierungshilfe angesichts der bisherigen Kritik gegen Clouds außerhalb der EU bzw. des EWR auch etwas Positives abzugewinnen: Offensichtlich halten die Aufsichtsbehörden nun die Nutzung von außereuropäischen Clouds für grundsätzlich zulässig.

b) Zulässigkeit von europäischen Clouds von US-Anbietern

Angesichts der Vielzahl der rechtlichen Probleme von Clouds ist es vielleicht verständlich, gleichwohl schade, dass das Thema der Zulässigkeit von europäischen Clouds durch US-Anbieter nicht angesprochen wurde. *Microsoft* hatte bei der Vorstellung seines Cloud-Officepakets im Juni 2011 bestätigt, dass es auf Anfrage von US-Sicherheitsbehörden an diese möglicherweise auch ohne Information der Kunden Daten herausgeben würde, die in Rechenzentren in Europa gespeichert sind.[26] Diese Mitteilung stieß zumindest im *Europäischen Justizministerium* sowie bei Mitgliedern des *Europäischen Parlaments* auf Unmut.[27] Hierzu sollte möglichst schnell eine praxistaugliche Lösung gefunden werden. Die Lösung dieses Problems sollte jedenfalls nicht darin liegen, dass europäische Clouds in die USA verlegt werden, um dann den Bestimmungen des Safe Harbor Programs und den Standardvertragsklauseln entsprechend rechtmäßig dem Zugriff der US-Behörden zu unterliegen.[28]

6. Technische und organisatorische Aspekte

Nach einer allgemeinen Abhandlung der Ziele und Risiken aus der Perspektive der IT-Sicherheit erläutert die Orientierungshilfe jeweils gesondert für die Cloud-Modelle IaaS, PaaS und SaaS, welche spezifischen Risiken bestehen und wie diesen mit technisch-organisatorischen Maßnahmen begegnet werden kann.

a) Ziele und Risiken

Vor einer ausführlichen Beschreibung der Risiken zählt der Text kurz die wesentlichen Schutzziele auf, die für eine ausreichende technische Absicherung der personenbezogenen Daten anzustreben sind:[29]

- Verfügbarkeit: Daten stehen stets zeit- und verarbeitungsgerecht zur Verfügung;
- Vertraulichkeit: Zugriffs- und Verarbeitungsrechte nur für befugte Personen;
- Integrität: Daten bleiben unversehrt, vollständig und aktuell;
- Revisionssicherheit: Protokollierung einzelner Datenverarbeitungen;
- Transparenz: Protokollierung der Verarbeitungsprozesse.

Im Anschluss werden Bedrohungen beschrieben, die auf die technischen Besonderheiten des Cloud Computings zurückzuführen sind.[30] Kernprobleme seien hier die räumliche Trennung zwischen Anwender und Server-Standorten und die häufig fehlende Kenntnis darüber, auf welchen Systemen sich die Daten in einem bestimmten Zeitpunkt befinden. Hierdurch werde eine kontrollierte Protokollierung sämtlicher Verarbeitungen und eine überprüfbare Löschung der Daten erschwert. Im Vergleich zu anderen Outsourcing-Lösungen werde die Gefahr des Kontrollverlusts beim Cloud Computing dadurch vergrößert, dass Daten über leistungsfähige Breitbandverbindungen transferiert und fragmentiert gespeichert werden. Schließlich würde die kurzfristige Verfügbarkeit von Cloud-Angeboten dazu führen, dass diese voreilig, also ohne ausreichende rechtliche und technische Überprüfung, eingesetzt werden.

Nach den cloudspezifischen Risiken erläutert die Orientierungshilfe allgemeine Bedrohungen, die für sämtliche IT-Systeme gelten.[31] Stichpunktartig genannt werden u.a. fahrlässiges oder vorsätzliches Fehlverhalten von eigenen oder externen Mitarbeitern, Angriffe von außen, Sicherheitslücken auf den Übertragungswegen, Systemausfälle auf Grund mangelhafter Sicherheitskonzepte, Missbrauch von Sicherungskopien und mangelhafte Löschung von Daten. Einige dieser Risiken seien in einer Cloud-Umgebung besonders hoch: Die flexible Verteilung der Ressourcen gefährde die Trennung der Daten verschiedener Cloud-Anwender. Mangelnde Transparenz führe dazu, dass der Cloud-Anwender die Kontrolle u.a. über Zugriffe von innen oder außen, Sicherheitsvorkehrungen am Ort der Server und die Beauftragung von Subauftragnehmern verliere. Dementsprechend sei auch die Verfügbarkeit der Daten in der Cloud gefährdet, weil man als Cloud-Anwender die Durchführung der hierfür erforderlichen Maßnahmen aus der Hand gebe.

Als cloudspezifisches Risiko wird zu Recht die Beauftragung von Unterauftragnehmern hervorgehoben. Denn insbesondere für Anbieter von PaaS- und SaaS-Diensten ist es aus technischen Gründen attraktiv, Ressourcen bei anderen Anbietern hinzuzukaufen. Für den Anwender ist meist nicht erkennbar, ob auch die hinzugekauften Ressourcen entsprechend abgesichert werden. Bei der Löschung von Daten wird richtigerweise auf das praxisrelevante Problem eingegangen, dass Daten nicht nur sicher gelöscht, sondern auf Grund der flexiblen Nutzung von Ressourcen auch vor dem Zugriff nachfolgender Nutzer geschützt werden müssen. Dieses Problem ist jedoch bereits vom

22 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 11; Beschluss des *Düsseldorfer Kreises* v. 28./29.4.2010 in Hannover, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.html?nn=409242.

23 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 10; Beschluss der *Kommission* v. 5.2.2010 (2010/87/EU), K(2010) 593.

24 A.A. und ausf. zum Streitstand *Weber/Voigt*, ZD 2011, 74, 76.

25 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 11.

26 *Whittaker*, ZD-Net v. 28.6.2011, abrufbar unter: http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225.

27 *Barnitzke*, MMR-Aktuell 2011, 321103; „EU-Parlamentarier besorgt über US-Zugriff auf Cloud-Daten", abrufbar unter: http://www.golem.de/1107/84763.html.

28 Beschluss der *Kommission* v. 5.2.2010 (2010/87/EU), K(2010) 593, Art. 3, Fußn. 8; *U.S. Department of Commerce,* Safe Harbor Principles, July 21, 2000, abrufbar unter: http://export.gov/safeharbor/eu/eg_main_018475.asp.

29 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 13.

30 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 14.

31 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 15.

Hosting bekannt und wird in Hosting-Verträgen meist umfassend geregelt. Bei Cloud-Angeboten fehlen hingegen oft entsprechende Regelungen, sodass die cloudspezifische Besonderheit hier eher auf Vertragsebene zu sehen ist.

Nicht zuzustimmen ist der Orientierungshilfe darin, die kurzfristige Verfügbarkeit von Cloud-Services als Ursache für eine vorschnelle Inanspruchnahme anzuführen. Eine gründliche Prüfung vor der Einführung liegt zweifellos im Verantwortungsbereich des Anwenders. Derart sorglose Anwender, auf die hier angespielt wird, würden bei schlecht administrierten Inhouse-Lösungen größere Probleme bekommen als bei der Nutzung der meisten Cloud-Lösungen.

Als echtes cloudspezifisches Risiko sollten mögliche Sicherheitslücken in den APIs (application programming interface) herausgestellt werden. APIs sind die Software-Schnittstellen zwischen den Systemen von Anbieter und Anwender der Cloud. Hier ist unbedingt darauf zu achten, dass ein sicheres Authentifizierungsverfahren zur Zugangskontrolle und eine Verschlüsselung zur Übermittlungskontrolle genutzt werden. Von Bedeutung ist zudem die Gefahr des Zugriffs von staatlichen Stellen bei Verarbeitungen in Drittstaaten, die in der Orientierungshilfe kurz Erwähnung findet (s. hierzu bereits oben unter 5. b)). Die ebenfalls knapp angesprochenen Verfügbarkeitsprobleme sind in der Praxis vor allem dann von Relevanz, wenn die in der Cloud betriebene Software nicht auf die Architektur der unterliegenden Cloud angepasst wurde.[32]

b) Infrastructure as a Service (IaaS)

Zur Absicherung der Daten bei der Nutzung von IaaS-Angeboten empfiehlt die Orientierungshilfe, sich selbst vom Stand der IT-Sicherheit zu überzeugen.[33] Denn als Cloud-Anwender sei man darauf angewiesen, dass der Anbieter die ihm obliegenden IT-Sicherheitsmaßnahmen auch tatsächlich durchführt. Als Nachweis seien Zertifikate von unabhängigen Stellen am besten geeignet.

Da bei IaaS-Angeboten lediglich (virtualisierte) Hardware-Komponenten zur Verfügung gestellt werden, stehe die Absicherung dieser Hardware im Vordergrund. Danach sei diese vor Verlust (z.B. durch Diebstahl) und Ausfall zu schützen und es müssten Absicherungen durch Zugriffsbeschränkungen, Patchmanagement, Firewalls, Virenschutz und weitere Maßnahmen nach den Vorgaben von § 9 BDSG getroffen werden. In einem solchen Sicherheitskonzept müsse der Cloud-Operator (Cloud-Control) eine besondere Rolle einnehmen, da dieser die Vergabe der Ressourcen koordiniert.

Besonders schützenswert seien zudem die Kommunikationsverbindungen zwischen Anwender und Cloud-Ressource. Zum Schutz der Vertraulichkeit werden Ende-zu-Ende-Verschlüsselungen und Intrusion-Detection/Prevention-Systeme (IDS/IPS) zur Erkennung und Verhinderung von Angriffen empfohlen. Die Verfügbarkeit könne mit redundanten Leitungen gesichert werden. Einen weiteren Schwerpunkt legt die Orientierungshilfe auf die Absicherung der Virtualisierungssoftware: Diese sollte nach Möglichkeit zertifiziert sein. Benutzerrichtlinien und Berechtigungskonzepte sollten den Umgang mit den virtualisierten Systemen regeln. Dabei sei der Admin-Zugang besonders zu schützen, da dieser über öffentliche Netze erreichbar ist.

Die in diesem Abschnitt aufgezählten Risiken und Empfehlungen decken sich weitestgehend mit denen beim einfachen Hosting (z.B. werden auch Server in Rechenzentren virtualisiert). Insofern wäre es wünschenswert, dass die Orientierungshilfe stärker auf cloudspezifische Probleme eingeht. So bleibt z.B. eine gefährliche Schwachstelle bei IaaS-Angeboten unberücksichtigt: Anders als beim Hosting wird bei IaaS-Diensten in der Regel nicht angeboten, die auf den virtualisierten Systemen laufenden Betriebssysteme zu überwachen und zu patchen. Hierdurch können eklatante Sicherheitslücken entstehen, die als besondere Gefahr bei IaaS-Angeboten unbedingt zu berücksichtigen sind.[34]

c) Platform as a Service (PaaS)

Bei einem PaaS-Angebot kann der Anwender eigene Anwendungen in einer zur Verfügung gestellten Laufzeitumgebung entwickeln und nutzen. Nach der Orientierungshilfe muss sich der Anwender vertraglich zusichern lassen, dass der Anbieter die Betreuung der bereitgestellten Infrastruktur ordnungsgemäß erfüllt.[35] Dies setze ein hohes Maß an Transparenz auf Seiten des Anbieters voraus. Der Anbieter müsse u.a. sämtliche Serverstandorte sowie alle Unterauftragnehmer und deren Standorte offenlegen. Da Vor-Ort-Kontrollen auf Grund der Vielzahl der betroffenen Unternehmen und Standorte kaum möglich sein dürften, seien Cloud-Anbieter zu bevorzugen, die sich regelmäßig von unabhängigen Stellen auditieren und zertifizieren lassen. Auch bezüglich der Gewährleistung der Verfügbarkeit von Daten in der Cloud empfiehlt die Orientierungshilfe entsprechend zertifizierte Rechenzentren. Ein besonderer Wert wird zudem darauf gelegt, dass die Daten portierbar sein müssten, sodass der Cloud-Anwender stets den Anbieter wechseln kann (z.B. bei dessen Insolvenz oder Unzuverlässigkeit). Um die Revisionssicherheit zu gewährleisten, müsse sich der Anwender entsprechende Einsichtsrechte vertraglich zusichern lassen.

Die von der Orientierungshilfe propagierte Zielsetzung, vom Anbieter umfangreiche Sicherheitsmaßnahmen zu verlangen, ist aus Anwendersicht zwar richtig, lässt sich von PaaS-Anbietern in der Praxis jedoch nur bedingt realisieren, da die vielen Anwender die bereitgestellte Plattform sehr unterschiedlich nutzen können. Anbieter können deshalb keine Umgebung schaffen, die optimale Sicherheitsbedingungen für sämtliche Nutzungsarten gewährt. Die Inanspruchnahme von PaaS-Diensten birgt deshalb grundsätzlich die größten Risiken für den Anwender. Auch wird es in der Praxis nicht möglich sein, den Anbieter dazu zu verpflichten, Änderungen in der bereitgestellten Umgebung nur mit Zustimmung des Anwenders vornehmen zu dürfen. Eine Weiterentwicklung ist ständig erforderlich und kann nicht vom Einverständnis einzelner Anwender abhängig gemacht werden. Auch hinsichtlich der Transparenz verlangt die Orientierungshilfe zu viel vom Anbieter: Eine Offenlegung sämtlicher Subunternehmer und deren Serverstandorte sollte aus Anwendersicht zwar angestrebt werden, geht jedoch bei neutraler Betrachtung über die gesetzlichen Anforderungen von § 11 Abs. 2 Satz 2 Nr. 6 BDSG hinaus (s. hierzu II. 4. a)).

d) Software as a Service (SaaS)

Bei ihren Empfehlungen zu SaaS-Diensten verweist die Orientierungshilfe zunächst auf die Ausführungen zu IaaS und PaaS.[36] Darüber hinaus müsse der Nutzer eines SaaS-Angebots darauf achten, dass der Anbieter seine zur Verfügung gestellten Anwendungen ausreichend absichert. Die Durchführung dieser Sicherungsmaßnahmen kann nur durch den Anbieter selbst erfolgen, weil dieser die administrative Hoheit bis in die Anwendungsebene hinein besitzt. Wichtigstes Schutzziel sei deshalb die Transparenz, die mit Hilfe ausführlicher Service-Level-Agreements (SLAs) geschaffen werden könne. Durch Abfrage um-

32 Ausf. zur Verfügbarkeit in der Cloud: *Vogels*, Eventually Consistent – Revisited, abrufbar unter: http://www.allthingsdistributed.com/2008/12/eventually_consistent.html.
33 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 17 f.
34 Vgl. Gefährdungsanalyse bei *Münch/Doubrava/Essoh*, DuD 2011, 322, 323 ff.
35 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 20.
36 Orientierungshilfe – Cloud Computing (o. Fußn. 1), S. 22.

fangreicher vertraglicher Zusicherungen zu Schutzmaßnahmen müsse der Anwender seiner datenschutzrechtlichen Verantwortung gerecht werden. Auch durch Vorlage entsprechender Dokumente, Protokolle oder Zertifikate könne der SaaS-Anbieter getroffene Maßnahmen nachweisen. Eine besondere Schwachstelle eines SaaS-Dienstes sei häufig der webbasierte Zugang. Deshalb sei insbesondere darauf zu achten, dass der Anbieter sein Webinterface angemessen gegen unbefugten Zugang schützt. Der Anwender müsse zudem sicherstellen, dass ein ausreichendes Authentifizierungsverfahren eingesetzt wird (Zugangskontrolle).

In der Praxis ist die hier vorgeschlagene Absicherung durch ausführliche SLAs oft nicht durchsetzbar, weil SaaS-Anbieter auf Grund der Vielzahl an Kunden nicht mit jedem individuelle Vereinbarungen treffen können, sondern meist nur verschiedene Standardverträge zur Verfügung stellen. Das aus technischer Sicht größte Risiko folgt – wie in der Orientierungshilfe angesprochen – aus der mangelnden Transparenz über die einzelnen Datenverarbeitungen: Diese kann vom Anbieter nicht umfassend gewährleistet werden, da er sie meist selbst nicht überblicken kann. Zusätzliche Risiken ergeben sich daraus, dass die Anbieter im Backend meist nur eine gemeinsame Datenstruktur verwenden. Anstatt „security by transparency" findet sich hier oft nur „security by obscurity" (Sicherheit durch Verschleierung).[37]

e) Verschlüsselung als Lösungsansatz

Bedauerlicherweise geht die Orientierungshilfe nicht vertieft auf die Möglichkeit ein, personenbezogene Daten in der Cloud mit Hilfe von Kryptografie zu schützen.[38] Wie bereits bei der Problematik einer möglichen Re-Identifizierung angesprochen (s. II. 2. a)), könnte die Verschlüsselung in Frage stellen, ob der Anbieter im Falle einer Verschlüsselung durch den Anwender überhaupt personenbezogene Daten (im Auftrag) verarbeitet. Eine solche Anonymisierung könnte dann eine Vielzahl von bei Clouds kaum umsetzbaren datenschutzrechtlichen Anforderungen vermeiden und zu einer erheblichen Verbesserung des effektiven Datenschutzes führen.

So entfällt nach der immer stärker vordringenden Auffassung der Personenbezug eines Datums nicht nur dann, wenn eine Bestimmbarkeit absolut ausgeschlossen ist, sondern es ist auch darauf abzustellen, ob der jeweilige Verwender wie z.B. der Cloud-Anbieter über das nötige Zusatzwissen für eine Herstellung des Personenbezugs verfügt.[39] Um eine Herbeiführung des Personenbezugs sicher verhindern zu können, müssten jedoch eine Verschlüsselungslösung und ein Passwortmanagement von solcher Qualität eingesetzt werden, dass eine Herstellung des Personenbezugs für den Cloud-Anbieter praktisch ausgeschlossen ist.[40] In diesem Fall wäre von einer Anonymisierung der Daten auszugehen.[41] In weiterer Konsequenz wären die Vorgaben des BDSG für die Datenverarbeitungen des Cloud-Anbieters nicht zu berücksichtigen, da nicht anwendbar.[42]

Unabhängig von der Frage des Personenbezugs ist der Einsatz von Kryptografie jedenfalls eine wirkungsvolle Schutzmaßnahme für Daten in der Cloud. Die heutigen Methoden und Tools sind zwar noch relativ kostspielig und unflexibel; so kann insbesondere das Schlüsselmanagement Probleme bereiten: Ein unzureichendes Schlüsselmanagement trägt immer das Risiko des kompletten Datenverlusts in sich, da im Falle des Schlüsselverlusts die Daten nicht mehr entschlüsselt werden könnten. Dennoch sind praktikable Verschlüsselungslösungen technisch umsetzbar und müssten vielleicht auch durch gesetzliche Vorgaben stärker in den Vordergrund gerückt werden.

III. Bewertung und Ausblick

Die Orientierungshilfe zum Cloud Computing ist ein guter Start, Unternehmen bei der Nutzung von Clouds mehr Rechtssicherheit zu geben. Da die Orientierungshilfe aus Sicht der Aufsichtsbehörden zahlreiche Mindestanforderungen festlegt, sind Unternehmen gut beraten, die Orientierungshilfe gründlich zu studieren und möglichst vollständig umzusetzen. Die Orientierungshilfe setzt jedoch, teilweise sogar ohne jede Begründung, hohe Anforderungen an Cloud Computing, die weit über die gesetzlichen Anforderungen des § 11 BSDG hinausgehen. Ferner zeigt sie, wie z.B. bei der Forderung nach Zertifizierungen oder externen Auditierungen, praktisch gut verwertbare Ansätze, zaudert dann aber doch bei dem naheliegenden Schritt, dem Cloud-Anwender darüber hinaus keine weiteren selbstständigen Kontrollpflichten aufzuerlegen.

In den Ausführungen zu den technisch-organisatorischen Aspekten greift die Orientierungshilfe einige wichtige Punkte auf, verliert sich aber häufiger in zu allgemeinen Vorgaben zur IT-Sicherheit, die für jede Form des Outsourcings gelten und nicht auf Besonderheiten des Cloud Computings zurückzuführen sind. Hilfreicher wäre eine differenziertere Betrachtung, die konkreter auf die Probleme eingeht, die beim Cloud Computing im Vergleich zum externen Hosting entstehen und nicht im Vergleich zur Inhouse-Verarbeitung.

Insgesamt spricht die Orientierungshilfe viele wichtige Punkte an, die man durch eine detailliertere Betrachtung hilfreich ausbauen kann. Wie bereits der Titel der Orientierungshilfe: „Orientierungshilfe Cloud Computing Stand 1.0" andeutet, sind die Empfehlungen der Aufsichtsbehörden keinesfalls als endgültige und abschließende Bewertung zu verstehen, sondern als guter Ausgangspunkt für weitere, vertiefte Diskussionen. Dabei sollte insbesondere die Überlegung, personenbezogene Daten durch verschlüsselte Übertragung und Speicherung vor unbefugtem Zugriff zu schützen, in Zukunft ausführlicher behandelt werden.

Dr. Christian Schröder
ist Rechtsanwalt in der Kanzlei Hengeler Mueller in Düsseldorf und 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.

37 *Weichert*, Cloud Computing und Datenschutz, Kap. 10, abrufbar unter: https://www.datenschutzzentrum.de/cloud-computing/.

38 Orientierungshilfe – Cloud Computing (o. Fußn. 1): bei IaaS wird nur die Verschlüsselung der Kommunikationswege vorgeschlagen (S. 19), bei SaaS wird zumindest auch die verschlüsselte Speicherung kurz erwähnt (S. 23).

39 Zur Streitfrage *Dammann*, in: Simitis (o. Fußn. 9), § 3 Rdnr. 20 ff., der einen Personenbezug verneint, wenn das Risiko der Bestimmbarkeit praktisch irrelevant ist; vermittelnde Ansichten bei *Forgó/Krügel*, MMR 2010, 17, 18 ff.

40 *Spies*, MMR-Aktuell 2011, 313727 problematisiert die Nachweisbarkeit solcher Qualitätsstandards.

41 Befürwortend *Spies* (o. Fußn. 40) sowie *Heidrich/Wegener*, MMR 2010, 803, 807; eher ablehnend *Splittgerber/Rockstroh*, BB 2011, 2179, 2181.

42 Zur Kritik an diesem „Schwarz-Weiß-Prinzip" des BDSG *Schneider/Härting*, ZD 2011, 63, 64.