CHRISTIAN SCHRÖDER / NILS CHRISTIAN HAAG

Stellungnahme der Art. 29-Datenschutzgruppe zum Cloud Computing

Cloud-Dienstleistung
Kriterienkatalog
Internationale Clouds
Technische und organisatorische Anforderungen
Vertragsgestaltung

Gibt es neue datenschutzrechtliche Anforderungen für Cloud Computing?

■ Nach der Orientierungshilfe zum Cloud Computing der deutschen Aufsichtsbehörden sowie dem Sopot-Memorandum der Berlin Group hat nun die Art. 29-Datenschutzgruppe ihre Vorgaben zur datenschutzgerechten Nutzung von Cloud Computing (WP 196) formuliert. Die Art. 29-Datenschutzgruppe orientiert sich dabei stark an den bisherigen Stellungnahmen, fügt ergänzende Anforderungen hinzu und zeigt insbesondere zu Zertifizierungen und Audits etwas mehr Mut als die bisherigen Stellungnahmen. Insgesamt wird nun auf europäischer Ebene langsam ein einheitlicher Standard für datenschutzgerechte Cloud-Lösungen erkennbar. Die Stellungnahme der Art. 29-Datenschutzgruppe ist daher ein weiterer wichtiger Schritt hin zu mehr Rechtssicherheit und ihre Kenntnis ein Muss für sämtliche mit Cloud-Dienstleistungen befassten Stellen und Berater.

■ After the orientation aid regarding cloud computing by the German supervisory authorities, as well as the Sopot-memorandum by the Berlin Group, the Art. 29-Data Protection Group now worded its requirements on the data protection compliant use of cloud computing (WP 196). In this, the Art. 29-Data Protection Group has strongly aligned itself with the hitherto statements, added supplementary requirements and, in particular, shows a bit more courage in regards to certifications and audits than the hitherto statements. In sum, slowly a uniform standard for data protection compliant cloud solutions is becoming discernible on a European level. Thus, the statement by the Art. 29-Data Protection Group is an important further step towards more legal certainty and the knowledge thereof is imperative for all agencies and advisors dealing with cloud services.

I. Einleitung

Anhand der zahlreichen Beiträge zur datenschutzgerechten Nutzung von Cloud Computing, die nicht nur von Beratern und der Lehre, sondern zunehmend auch von Aufsichtsbehörden veröffentlicht werden, lässt sich die Brisanz des Themas unschwer erkennen. Unternehmen lagern immer mehr Datenverarbeitungen „in die Cloud" zu externen Dienstleistern aus. Nach Prognosen der *Experton Group* wächst der Cloud-Markt in Deutschland auch im Jahr 2012 weiterhin stark.[1] Nach einer Umfrage des Branchenverbands *BITKOM* im März 2012 nutzt bereits jedes vierte Unternehmen in Deutschland Cloud Computing.[2] Die Gründe hierfür liegen nicht nur in der erhofften Kosteneinsparung, sondern finden sich auch in den technischen Vorteilen von Cloud-Diensten, wie z.B. der hohen Verfügbarkeit der Daten unabhängig vom Endgerät. Aus datenschutzrechtlicher Sicht liegen die damit einhergehenden Risiken für die Daten auf Grund von Kontrollverlust und fehlender Transparenz auf der Hand.

Dieser Unsicherheit nahmen sich zunächst die deutschen Aufsichtsbehörden im September 2011 an und veröffentlichten die „Orientierungshilfe zum Cloud Computing".[3] Diese bot mit praxisorientierten Vorschlägen eine gute Ausgangsbasis für deutsche Cloud-Nutzer.[4] Im April 2012 veröffentlichte dann die *International Working Group on Data Protection in Telecommunications* (*Berlin Group*) Best Business-Empfehlungen zum datenschutzgerechten Cloud Computing.[5]

Inhaltlich decken sich die Empfehlungen weitgehend mit den Anforderungen des europäischen Datenschutzrechts. Besonders positiv war die Schwerpunktsetzung der *Berlin Group* zu Gunsten technischer Lösungen zur Verbesserung des Datenschutzes.[6]

Nachdem nun auf deutscher und (teilweise) internationaler Ebene Anforderungen an datenschutzgerechtes Cloud Computing formuliert worden sind, durfte eine Stellungnahme der *Art. 29-Datenschutzgruppe* für die europäische Ebene nicht fehlen.

Aus Sicht deutscher Rechtsanwender dürften daher nun alle wesentlichen sie betreffenden Aufsichtsbehörden Stellungnahmen verfasst haben und es stellt sich die Frage, ob die europäischen Aufsichtsbehörden die teilweise sehr hohen Anforderungen der deutschen Aufsichtsbehörden an Cloud Computing teilen oder gar weitere Anforderungen formulieren.

Die Verfasser dieses Beitrags fassen daher in ihrem nun dritten Beitrag zu den aufsichtsbehördlichen Anforderungen an Cloud Computing die wesentlichen Ergebnisse der Stellungnahme der *Art. 29-Datenschutzgruppe* zusammen und zeigen auf, an welchen Stellen die *Art. 29-Datenschutzgruppe* von den bisherigen Stellungnahmen abweicht.

1 Cloud Marktzahlen, vgl. http://www.experton-group.de/consulting/cloud-computing-programme/ict-anwender/cloud-marktzahlen.html.
2 PM des *BITKOM* v. 7.3.2012, „Jedes vierte Unternehmen benutzt bereits Cloud Computing", http://www.bitkom.org/de/presse/8477_71446.aspx.
3 Orientierungshilfe – Cloud Computing, Stand 26.9.2011, http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf (im Folgenden: Orientierungshilfe Cloud Computing).
4 Besprechung und Bewertung der Orientierungshilfe bei *Schröder/Haag*, ZD 2011, 147 ff.
5 Working Paper on Cloud Computing – Privacy and data protection issues – „Sopot Memorandum" – 51st Meeting, 23–24 April, Sopot (Poland), die deutsche Übersetzung ist abrufbar unter: http://www.datenschutz-berlin.de/attachments/882/675.44.10.pdf?1340178180 (im Folgenden: Sopot Memorandum).
6 Ausführliche Darstellung und Bewertung bei *Schröder/Haag*, ZD 2012, 362 ff.

II. Stellungnahme 05/2012 der Art. 29-Datenschutzgruppe (WP 196)

Kurz nach Erscheinen der Empfehlungen der *Berlin Group* und unter ausdrücklichem Verweis auf deren Empfehlungen veröffentlichte die *Art. 29-Datenschutzgruppe* am 1.7.2012 die Stellungnahme 05/2012 zum Cloud Computing (WP 196).[7] Das Ziel dieser Stellungnahme sei, den Anbietern und Anwendern von Cloud-Diensten eine Hilfestellung zu geben, wie sie die Anforderungen der Europäischen Datenschutzrichtlinie 95/46/EG (DS-RL) beim Cloud Computing einhalten können.[8] Erfreulicherweise beginnt die *Art. 29-Datenschutzgruppe* ihre Stellungnahme mit einem klaren Bekenntnis zu den möglichen Vorteilen von Cloud Computing, die gerade auch im Datenschutz liegen. So betont die *Art. 29-Datenschutzgruppe* bereits in der Einleitung ausdrücklich, dass Cloud-Dienstleistungen gerade für kleine und mittlere Unternehmen in technischer und organisatorischer Hinsicht ein Sicherheitsniveau zum Schutz der Daten anbieten können, welches sich kleine und mittlere Unternehmen ansonsten häufig nicht leisten könnten.[9] Allerdings legt die *Art. 29-Datenschutzgruppe* besonderes Augenmerk auf „Mangelnde Kontrollmöglichkeiten" (lack of control) und „Mangelnde Transparenz" (lack of transparency). Diese beiden Bereiche müssten durch hinreichende technische und organisatorische Sicherheitsmaßnahmen sowie vertragliche Vereinbarungen abgedeckt werden.

III. Datenschutzrechtliche Rahmenbedingungen

Die Stellungnahme WP 196 beginnt nach der Einleitung zunächst mit dem Hinweis auf ihre rechtlichen Grundlagen, die DS-RL sowie die E-Privacy-RL 2002/58/EG, die von der sog. Cookie-RL 2009/136/EG ergänzt worden ist. Vor einer Erläuterung der sich daraus ableitenden rechtlichen Anforderungen befasst sich die *Art. 29-Datenschutzgruppe* zunächst mit der örtlichen Anwendbarkeit dieser Vorgaben und der rechtlichen Einordnung von Cloud-Anbieter und -Anwender i.S.e. Auftragsdatenverarbeitung.

1. Anwendbares Recht

Die Anwendbarkeit des europäischen Datenschutzrechts ergibt sich aus Art. 4 der DS-RL. Die *Art. 29-Datenschutzgruppe* differenziert dementsprechend bei Cloud-Dienstleistungen zwischen den zwei nachfolgenden möglichen Anwendungsfällen:[10]

- Im ersten Fall der Anwendbarkeit europäischen Datenschutzrechts befindet sich der Sitz der verantwortlichen Stelle, also in der Regel der des Cloud-Anwenders, im Geltungsbereich der DS-RL. Anwendbar ist dann das die Europäische DS-RL umsetzende nationale Datenschutzrecht desjenigen Mitgliedstaats, in dem sich der Sitz des Cloud-Anwenders befindet. Verfügt das Unternehmen über Niederlassungen in mehreren Mitgliedstaaten, sind auch deren nationale Datenschutzbestimmungen zu berücksichtigen (Niederlassungsprinzip, vgl. § 1 Abs. 5 Satz 1 BDSG).
- Nach Ansicht der *Art. 29-Datenschutzgruppe* kann aber auch bereits der Ort der physischen Datenverarbeitung europäisches Datenschutzrecht zur Anwendung bringen. So kann z.B. allein ein Server eines Cloud-Anbieters im Geltungsbereich der DS-RL europäisches Datenschutzrecht zur Anwendung bringen. Nicht als Datenverarbeitung in diesem Sinne ist die bloße Durchleitung von Daten zu verstehen.[11]
- Die zweite Variante, bei der innereuropäische Datenverarbeitungsanlagen des Cloud-Anbieters bereits zur Anwendbarkeit europäischen Datenschutzrechts führen, dürfte für viele außereuropäische Cloud-Anwender überraschend sein. Dabei dürfte es sich um kein seltenes Szenario handeln, da beim Cloud Computing in der Regel eine Vielzahl breit gestreuter Ressourcen genutzt wird, von denen sich nur eine im europäischen Rechtsraum befinden muss. Grundlage für die Anwendung des europäischen Rechts ist Art. 4 Abs. 1 lit. c der DS-RL. Mit dieser Regelung soll verhindert werden, dass sich verantwortliche Stellen durch die Verlagerung ihres Standorts den europäischen Datenschutzregelungen entziehen.[12] Von diesem Schutzzweck ausgehend ist es jedoch kaum nachvollziehbar, wenn z.B. ein US-Unternehmen, welches ausschließlich Daten von in den USA lebenden Personen verarbeitet, europäisches Datenschutzrecht beachten soll, nur weil es sich eines Dienstleisters in Europa bedient. Auch für europäische Cloud-Diensteanbieter dürfte eine solch unkritische, weite Anwendung europäischen Datenschutzrechts einen erheblichen Wettbewerbsnachteil darstellen, wenn sie personenbezogene Daten aus Jurisdiktionen außerhalb der EU bzw. des Europäischen Wirtschaftsraums verarbeiten. Sie müssten trotz Unkenntnis über die Zwecke bei Erhebung der Daten im außereuropäischen Ausland nun das gesamte europäische Datenschutzrecht beachten und erlitten dadurch gegenüber außereuropäischen Dienstleistern einen deutlichen Nachteil. Dementsprechend hält auch der *Düsseldorfer Kreis* als Gremium der deutschen Aufsichtsbehörden eine „Relativierung" des ausgedehnten Anwendungsbereichs des BDSG in diesem Fall für möglich.[13] Danach ist es zumindest denkbar, dass die DS-RL in Art. 4 Abs. 1 lit. c einen „EU/EWR-Bezug" der Daten stillschweigend unterstellt habe, sodass man durch teleologische Reduktion zu einer verringerten Anwendung europäischen Datenschutzrechts käme, sofern keine EU-Bürger zu den Betroffenen gehören. Den Auftragnehmer in der EU/EWR träfen daher nur die Anforderungen zur technischen und organisatorischen Datensicherheit. Er sei nicht zur Prüfung der materiellen Vereinbarkeit der Datenverarbeitung mit dem BDSG verpflichtet.[14] Die *Art. 29-Datenschutzgruppe* erörtert in ihrer Stellungnahme die Frage einer begrenzten Anwendbarkeit des europäischen Datenschutzrechts nicht. Insofern bleibt zu hoffen, dass sie sich der von den deutschen Aufsichtsbehörden vorgeschlagenen pragmatischen Lösung anschließen würde.

2. Rechtliche Einordnung von Anbieter und Anwender

Die *Art. 29-Datenschutzgruppe* betrachtet die Festlegung der Verantwortlichkeit für Datenverarbeitungen in der Cloud als eine der wichtigsten Regelungsaspekte. Insbesondere beim Cloud Computing bestehe oft auf Grund der Vielzahl beteiligter Unternehmen die Gefahr, dass sich niemand in der Verantwortung sieht.

Da in der Regel allein der Cloud-Anwender Zweck und Umfang der Datenverarbeitungen bestimmt, übernehme er die Funktion eines Auftraggebers und müsse daher die Verantwortung für

---

7 Bisher nur auf Englisch verfügbar: *Article 29 Data Protection Working Party*, Opinion 05/2012 on Cloud Computing (WP 196), adopted July 1st 2012, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (im Folgenden: WP 196).

8 WP 196 (o. Fußn. 7), S. 4.

9 WP 196 (o. Fußn. 7), S. 4; s.a. ähnlichen Hinweis in Sopot Memorandum (o. Fußn. 5), S. 3 ff.; *Schröder/Haag*, ZD 2012, 362, 363.

10 Ausführlicher zur Anwendbarkeit der europäischen Datenschutzregelungen ist die Stellungnahme der *Art. 29-Datenschutzgruppe* 8/2010 (WP 179).

11 Dies folgt aus Art. 4 Abs. 1 lit. c der Europäischen DS-RL 95/46/EG.

12 Vgl. Erwägungsgrund 18 der Europäischen DS-RL 95/46/EG.

13 *Düsseldorfer Kreis*, Handreichung zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung v. 19.4.2007, S. 17 (im Folgenden: Fallgruppen Internationale Auftragsdatenverarbeitung), abrufbar unter: http://www.datenschutz-berlin.de/content/themen-a-z/internationaler-datenverkehr/internationale-auftragsdatenverarbeitung.

14 Fallgruppen Internationale Auftragsdatenverarbeitung (o. Fußn. 13), S. 16, Beispiel H.

die datenschutzgerechte Verarbeitung personenbezogener Daten in der Cloud tragen. Der Cloud-Anbieter sei hingegen im Regelfall weisungsgebundener Dienstleister, also Auftragnehmer. Dies führe dazu, dass regelmäßig von einer klassischen Auftragsdatenverarbeitung i.S.d. Art. 17 der DS-RL (in Deutschland durch § 11 BDSG umgesetzt) auszugehen sei. In diesem Regelfall ist also der Cloud-Anwender allein für die Einhaltung datenschutzrechtlicher Bestimmungen verantwortlich. Die *Art. 29-Datenschutzgruppe* betont, dass dies auch für die häufig anzutreffende Konstellation gilt, in denen ein kleineres Unternehmen die Cloud-Dienste eines großen Anbieters wie *Apple*, *Microsoft* oder *Amazon* in Anspruch nimmt. Auch wenn der Anwender hier keine Möglichkeit zur Verhandlung individueller Vereinbarungen habe, könne ihm stets zugemutet werden, einen Anbieter zu wählen, der ein datenschutzkonformes Angebot bereithält.

Bemerkenswert sind die Erwägungen der *Art. 29-Datenschutzgruppe*, wonach in Einzelfällen auch der Cloud-Anbieter neben dem Cloud-Anwender verantwortliche Stelle sein kann.[15] Ein solcher Fall läge vor, wenn der Cloud-Anbieter ein eigenes Interesse an der Verwendung der Daten hätte, welches über die bloße Erfüllung seines Auftrags hinausgeht. Denkbar wäre z.B., dass ein Anbieter einem Internetportal eine cloud-basierte Software zur Auswertung von Nutzerdaten zur Verfügung stellt und die Daten dieser Nutzer auch für eigene Marketingzwecke nutzen möchte. Ohne wirksame Einwilligung wäre eine solche Konstellation jedoch kaum in zulässiger Weise durchführbar. Somit wird es in den meisten Fällen bei der alleinigen rechtlichen Verantwortlichkeit des Cloud-Anwenders und damit bei einer klassischen Auftragsdatenverarbeitung bleiben.

IV. Vertragliche Gestaltung

Aus der datenschutzrechtlichen Einordnung von Cloud-Dienstleistungen als Auftragsdatenverarbeitung folge, dass Cloud-Diensteanbieter mit den Cloud-Abnehmern (nachfolgend auch „Auftraggeber" genannt) grundsätzlich schriftliche Verträge abschließen müssten, die im Wesentlichen nicht nur die Weisungsgebundenheit des Dienstleisters in Bezug auf die Verarbeitung personenbezogener Daten, sondern auch die technischen und organisatorischen Sicherheitsmaßnahmen festlegen müssen. Eine schriftliche Vereinbarung sei nicht erforderlich, wenn vergleichbare Formen genutzt werden (diese Alternative wird leider nicht weiter erläutert). Ferner folge aus der Auftragsdatenverarbeitung, dass der Kunde als Auftraggeber ungeachtet seiner Größe den Cloud-Anbieter kontrollieren und die Cloud-Verträge diese Kontrollen auch entsprechend vorsehen müssen.[16]

Im Einzelnen:

- Die Datenverarbeitungen sollen in Service Level Agreements (SLA) genau definiert werden und Vertragsstrafen sollen die vertrags- bzw. weisungswidrige Verarbeitung von Daten sanktionieren.
- Die technischen und organisatorischen Sicherheitsanforderungen sind detailliert festzulegen.
- Der Vertrag muss eine Beschreibung der Art der Datenverarbeitung nebst Zweck, Dauer der Datenverarbeitung sowie den verarbeiteten Datenkategorien enthalten.
- Die Bedingungen für die Rückgabe bzw. sichere Löschung der Daten müssen geregelt werden.
- Der Cloud-Diensteanbieter muss sich und seine Mitarbeiter zur Verschwiegenheit über die ihm anvertrauten Daten verpflichten.
- Der Cloud-Diensteanbieter muss sich zur Unterstützung bei Geltendmachung von Auskunfts-, Berichtigungs- oder Löschungsansprüchen verpflichten.
- Der Cloud-Diensteanbieter muss über sämtliche Unterauftragsnehmer mit genauer Beschreibung der Art der outgesourcten Dienstleistungen, der Besonderheiten der derzeitigen oder zukünftig möglichen Unterauftragsnehmer informieren. Ferner muss vertraglich garantiert werden, dass sich die Unterauftragnehmer zur Einhaltung der sich aus der DS-RL ergebenden Vorgaben verpflichtet haben. Eine Möglichkeit, diese Anforderungen umzusetzen, ergebe sich für Datenverarbeitungen außerhalb der EU/des EWR aus dem 2010 veröffentlichten EU-Standardvertrag zur Auftragsdatenverarbeitung.[17] Sofern für die Unterbeauftragung nicht eine ausdrückliche Einwilligung des Auftraggebers erforderlich ist – die pauschal erteilt werden kann –, muss der Auftraggeber zumindest die Möglichkeit haben, den Änderungen widersprechen oder den Vertrag kündigen zu können.[18] Ein Cloud-Dienstleistungsvertrag muss daher vorsehen, dass Unterauftragnehmer nur auf Basis eigener Verträge beauftragt werden dürfen, die die Vorgaben des Hauptvertrags übernehmen und sicherstellen, dass der Auftraggeber seine Rechte nicht nur gegenüber dem Cloud-Diensteanbieter, sondern auch gegenüber allen Unterauftragnehmern durchsetzen kann. Diese Anforderung kann z.B. durch Verträge mit drittbegünstigenden Regelungen oder auch durch Abschluss gesonderter Verträge zwischen dem Kunden und den Unterauftragnehmern umgesetzt werden. Als Alternative bietet sich an, dass der Cloud-Diensteanbieter ausdrücklich für sämtliche vertragswidrigen Verarbeitungen von personenbezogenen Daten durch seine Unterauftragnehmer haftet.[19]
- Der Cloud-Diensteanbieter muss den Auftraggeber bei unbefugter Weitergabe von Daten an Dritte/Verlust von Daten (Security Breach) sowie über alle möglichen Verarbeitungsstandorte informieren.
- Die Rechte des Auftraggebers zur Überwachung des Cloud-Diensteanbieters müssen geregelt werden.
- Der Cloud-Diensteanbieter muss den Auftraggeber über jede beabsichtigte wesentliche Änderung der Cloud-Dienstleistungen informieren.
- Der Cloud-Diensteanbieter muss sämtliche Verarbeitungsschritte und Verarbeitungsorte automatisch protokollieren, um dem Auftraggeber die Überwachung des Cloud-Diensteanbieters bzw. seiner Unterauftragnehmer zu ermöglichen.[20]
- Ferner soll sich der Cloud-Diensteanbieter zur Information über sämtliche rechtsverbindlichen Auskunftsersuchen von Sicherheitsbehörden verpflichten, sofern diese Pflicht nicht gegen anwendbares Recht verstößt.
- Schließlich soll der Cloud-Diensteanbieter ausdrücklich bestätigen, dass er und seine Unterauftragnehmer sämtliche nationalen und internationalen rechtlichen Anforderungen an Cloud-Computing einhalten werden.

Den mit den Anforderungen des § 11 BDSG vertrauten Leser werden die meisten der vorgenannten Anforderungen nicht erstaunen. Auch ansonsten bringt die *Art. 29-Datenschutzgruppe* keine neuen Ansätze, die von den bisher bereits von den deutschen Aufsichtsbehörden formulierten Anforderungen abweichen. Bedauerlicherweise verlangt die *Art. 29-Datenschutzgruppe* wie auch die deutschen Aufsichtsbehörden, dass der Auftraggeber über sämtliche Standorte der Verarbeitung informiert werden muss. Nur hierdurch könne nachvollzogen werden, ob Daten z.B. die EU bzw. den Europäischen Wirtschafts-

15 WP 196 (o. Fußn. 7), S. 8.
16 WP 196 (o. Fußn. 7), S. 7 und 12 ff.
17 WP 196 (o. Fußn. 7), S. 9 f. unter Verweis auf FAQ II.5 des WP 176.
18 WP 196 (o. Fußn. 7), S. 10 und 20; s. hierzu auch Sopot Memorandum (o. Fußn. 5), S. 4; Anforderungen des *Unabhängigen Landesdatenschutzzentrums* „EuroPriSeÒ – Das Europäische Datenschutz-Gütesiegel Datenschutzrechtliche Anforderungen an Cloud Computing", S. 4.
19 WP 196 (o. Fußn. 7), S. 10
20 WP 196 (o. Fußn. 7), S. 11 und 13.

raum verlassen.[21] Warum hierfür eine Information darüber, dass die Standorte z.B. innerhalb der EU liegen, nicht ausreichen soll, bleibt offen.[22] Auch ist nicht nachvollziehbar, warum Cloud-Diensteanbietern im Unterschied zu einfachen Auftragsdatenverarbeitern eine erhöhte Bereitschaft zum Vertragsbruch unterstellt wird, denn nur diese sollen sich unter Vertragsstrafe zur Einhaltung der vertraglichen Regelungen verpflichten.[23]

Ein im Unterschied zur deutschen Informationspflicht wichtiger Punkt ist allerdings, dass die *Art. 29-Datenschutzgruppe* nun empfiehlt, die Betroffenen nicht nur über die verantwortliche Stelle, sondern darüber hinausgehend auch über den Cloud-Diensteanbieter bzw. sogar sämtliche Unterauftragnehmer zu informieren.[24]

V. Technische und organisatorische Maßnahmen

Bei der Feststellung der Anforderungen an den technischen Datenschutz differenziert die *Art. 29-Datenschutzgruppe* nach Schutzzielen wie Verfügbarkeit, Integrität, Vertraulichkeit und Nachweisbarkeit (Accountability). Welche Maßnahmen zur Erreichung dieser Ziele beim Cloud Computing jeweils getroffen werden müssen, schildert die Stellungnahme WP 196 leider – wenn überhaupt – nur sehr knapp. Konkretere Empfehlungen hierzu finden sich in einem Eckpunktepapier des *BSI* zur Informationssicherheit beim Cloud Computing.[25] Aber auch in den anderen Veröffentlichungen der Aufsichtsbehörden finden sich z.T. ausführlichere Vorschläge. Die nachfolgenden Regelungspunkte fassen diese Empfehlungen in der Reihenfolge zusammen, wie sie die Anlage zu § 9 BDSG vorgibt und wie sie regelmäßig in Vereinbarungen zur Auftragsdatenverarbeitung nach § 11 BDSG zu finden sind und in der Praxis abgeprüft werden.

1. Zutrittskontrolle

Die Zutrittskontrolle dient der Verhinderung des physischen Zutritts unbefugter Personen zu Datenverarbeitungsanlagen. Der Cloud-Anbieter muss darlegen, durch welche konkreten Maßnahmen er diese Anforderung an den einzelnen Verarbeitungsorten erfüllt. Da es für den Cloud-Anwender in der Regel kaum möglich sein wird, die Umsetzung an sämtlichen Standorten zu überprüfen, bietet sich insbesondere hierfür der Einsatz unabhängiger Auditoren bzw. die Heranziehung von Zertifizierungen an.[26]

2. Zugangskontrolle

Um Vertraulichkeit und Integrität der Daten in der Cloud zu schützen, ist unbefugten Personen der Zugang zu den Systemen zu verwehren. Hierfür sind Authentifizierungs- und Verschlüsselungsverfahren einzusetzen.[27] Bei Cloud-Anwendungen ist insbesondere auf die Absicherung der APIs zu achten, die Schnittstellen zu anderen Anwendungen und damit auch Angriffsflächen für Angriffe bieten.[28] Nach den Vorgaben der *Art. 29-Datenschutzgruppe* muss jeder Benutzer auch über einen eigenen Authentifizierungsschlüssel (z.B. Passwort) verfügen, damit ihm seine Aktionen zugeordnet werden können (s.u. V. 5. Eingabekontrolle).[29] Die Verwendung sicherer Passwörter sei hierfür unerlässlich, besser wäre der Einsatz von Hardware-Token zur Authentifizierung. Insider-Angriffe durch einzelne Mitarbeiter beim Cloud-Anbieter oder einem seiner Unterauftragnehmer, die über die erforderlichen Zugangsberechtigungen verfügen, könnten zudem durch eine fragmentierte Speicherung der Daten bei verschiedenen Unterauftragnehmern erreicht werden.[30]

Cloudspezifische Risiken treten zudem häufig auf Grund unzureichender Überwachung und Wartung der Systeme durch den Cloud-Anbieter auf. So könnten z.B. gravierende Sicherheitslücken durch mangelndes „Patching" entstehen.[31] Um unberechtigten Zugang durch Ausnutzung dieser Sicherheitslücken zu verhindern, seien die erforderlichen Maßnahmen des Anbieters zur Systempflege festzulegen und zu kontrollieren.

Dem Einsatz von Verschlüsselungstechniken misst die Stellungnahme der *Art. 29-Datenschutzgruppe* erfreulicherweise eine hohe Bedeutung zu. Verschlüsselung könne einen wesentlichen Beitrag zum Schutz der Vertraulichkeit der Daten in der Cloud leisten, sofern diese richtig eingesetzt wird.[32] Nach Möglichkeit sollten personenbezogene Daten zu jedem Zeitpunkt verschlüsselt sein, sowohl bei Übermittlungen als auch bei der Speicherung. Konkretere Vorschläge zur Umsetzung nennt die *Art. 29-Datenschutzgruppe* allerdings nicht. Zumindest hebt sie noch einen wichtigen Punkt hervor: Gerade weil die Verschlüsselung ein wichtiges Instrument zum Schutz der Daten in der Cloud darstelle, sei dem Schlüsselmanagement besondere Aufmerksamkeit zu schenken. Hierfür müsse geregelt sein, wer die Schlüssel besitzt und wie diese vor unbefugtem Zugriff und Verlust geschützt sind. Gehen die Schlüssel verloren, droht ein vollständiger Datenverlust.[33] Auch zum Schlüsselmanagement finden sich im Eckpunktepapier des *BSI* wertvolle Hinweise.[34]

3. Zugriffskontrolle

Verschlüsselungstechniken sind auch für die Zugriffskontrolle von Bedeutung, bei der es um die individuelle Verwaltung von Zugriffsberechtigungen geht. Neben einer erforderlichen organisatorischen Regelung in Berechtigungskonzepten, wer auf Seiten von Cloud-Anwender und Cloud-Anbieter welche Zugriffsrechte bekommen soll, kann die Berechtigungsvergabe auch über Verschlüsselungsmaßnahmen auf technischem Wege abgesichert werden. Sofern der Cloud-Anbieter für die Durchführung seines Auftrags keinen Zugriff auf personenbezogene Daten benötigt, wie es bei der bloßen Bereitstellung von IT-Infrastruktur (IaaS) in der Regel der Fall ist, empfiehlt die *Art. 29-Datenschutzgruppe* dem Cloud-Anwender eine Verschlüsselung der Daten, bevor er diese in die Cloud übermittelt.[35] Unter der Prämisse einer ausreichenden Schlüsselqualität spricht in diesem Fall vieles dafür, dass der Cloud-Anbieter mangels Zugriffsmöglichkeit keine personenbezogenen Daten im Auftrag verarbeitet.[36] Auch die *Art. 29-Datenschutzgruppe* hat in einer anderen Stellungnahme (WP 136) bereits zu dieser Auffassung tendiert, während die deutschen Aufsichtsbehörden einen Personenbezug erst ausschließen wollen, wenn dieser von niemandem mehr hergestellt werden kann.[37] Bei der Berechtigungsvergabe

21 WP 196 (o. Fußn. 7), S. 11 und Fußn. 18.
22 S. bisherige Kritik bei *Schröder/Haag*, ZD 2012, 362, 367.
23 WP 196 (o. Fußn. 7), S. 7 ff.; bereits bei der Stellungnahme der deutschen Aufsichtsbehörden kritisiert, s. *Schröder/Haag*, ZD 2011, 147, 149.
24 WP 196 (o. Fußn. 7), S. 6.
25 *Bundesamt für Sicherheit in der Informationstechnik* (*BSI*), Sicherheitsempfehlungen für Cloud Computing-Anbieter, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf.
26 *Schröder/Haag*, ZD 2012, 362, 364.
27 So verweist auch die Anl. zu § 9 BDSG in Satz 3 explizit auf die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungstechniken.
28 Ausführlicher hierzu *Schröder/Haag*, ZD 2011, 147, 151.
29 WP 196 (o. Fußn. 7), S. 15 (Integrity).
30 Hierzu bereits *Schröder/Haag*, ZD 2012, 362, 365 m.w.Nw.
31 *Schröder/Haag*, ZD 2011, 147, 151 m. Hinw. auf *Münch/Doubrava/Essoh*, DuD 2011, 322, 323 ff.
32 WP 196 (o. Fußn. 7), S. 15 (Confidentiality).
33 Dazu bereits *Schröder/Haag*, ZD 2011, 147, 152.
34 *BSI* (o. Fußn. 25), S. 39 ff.
35 WP 196 (o. Fußn. 7), S. 15 (Confidentiality).
36 Hierzu bereits *Schröder/Haag*, ZD 2011, 147, 152 m.w.Nw.; *Stiemerling/Hartung*, CR 2012, 60, 62.
37 S. Nachweise in *Stiemerling/Hartung*, CR 2012, 60, 62; *Schröder/Haag*, ZD 2012, 362, 365 m. Verw. auf WP 136 der *Art. 29-Datenschutzgruppe*, S. 18 f. (Beispiel 17), abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf.

sei auch auf Anbieterseite darauf zu achten, dass niemand mehr Zugriffsrechte erhält, als es für die Erfüllung seiner Aufgaben erforderlich, dies gelte auch für Administratorenrechte.[38]

4. Weitergabekontrolle

Auch bei der Weitergabekontrolle seien Verschlüsselungstechniken zum Schutz der Daten einzusetzen. Die *Art. 29-Datenschutzgruppe* verlangt, sämtliche Übertragungswege zwischen Cloud-Anbieter und -Anwender sowie zwischen sonstigen physischen Verarbeitungsorten durch Verschlüsselung abzusichern. Dies gelte auch für Remote-Zugriffe bei Fernwartungen.[39] Aus Sicht eines Cloud-Anwenders solle bereits bei Vertragsschluss darauf geachtet werden, dass der Anbieter entsprechende Übertragungsprotokolle (wie TLS/SSL oder SSH) anbietet und auch einsetzt.

5. Eingabekontrolle

Nach Ansicht der *Art. 29-Datenschutzgruppe* sind fehlende Kontrolle und mangelnde Transparenz die Hauptursachen für Datenschutzverletzungen beim Cloud Computing. Für ausreichende Transparenz kann bereits im Vorfeld auf vertraglicher Ebene gesorgt werden, indem die zu treffenden Maßnahmen schriftlich fixiert werden. Eine effektive Kontrolle der tatsächlichen Umsetzung dieser Maßnahmen sei durch automatisch generierte Systemprotokolle möglich. So ist es nach der *Art. 29-Datenschutzgruppe* auch von größter Bedeutung, dass der Cloud-Anbieter seine Datenverarbeitungen umfassend automatisch protokolliert und diese Protokolle für vertrauenswürdige Kontrollen zur Verfügung stellt.[40] Daneben müsse er fundierte Nachweise für die Durchführung aller technisch-organisatorischen Maßnahmen erbringen, zu denen er sich vertraglich verpflichtet hat.

Konkretere Empfehlungen zur Umsetzung finden sich in dem Working Paper der *Berlin Group*.[41] Danach müssten Ort und Zeit der Datenverarbeitungen automatisch protokolliert werden, sodass der Cloud-Anwender jederzeit einsehen kann, an welchen Standorten seine Daten physisch verarbeitet werden. Auf einer detaillierteren Ebene müssten sämtliche Aktivitäten wie Datenänderungen, Backups oder Löschungen durch den Anbieter oder dessen Unterauftragnehmer automatisch geloggt werden. Die Logfiles seien ausreichend vor Manipulation zu schützen. Für eine Kontrolle durch stichprobenartige Einsichtnahme dieser Protokolle empfiehlt sich auf Grund des nicht zu unterschätzenden Aufwands auch hier die Hinzuziehung unabhängiger Auditoren.[42]

6. Verfügbarkeitskontrolle

Um die ständige Verfügbarkeit der Daten in der Cloud gewährleisten zu können, muss der Cloud-Anbieter nach der *Art. 29-Datenschutzgruppe* geprüft haben, ob bestimmte Ausfallrisiken bestehen und diesen ggf. mit angemessenen Sicherungsmaßnahmen begegnet sein.[43] In Betracht kämen redundante Spiegelungen der Systeme, Ersatzleitungen und weitere Backuplösungen. Bei Online-Anwendungen mit Webzugang bestehe zudem die Gefahr eines Systemausfalls auf Grund von DoS-Angriffen.[44] Praktikable Hinweise zur technischen Absicherung von Online-Anwendungen bieten z.B. die frei verfügbaren OWASP TOP 10.[45]

7. Trennungskontrolle

Ein Cloud-Dienst wird in der Regel von einer Vielzahl von Anwendern genutzt, sodass auf technischem Wege sichergestellt sein müsse, dass ein Anwender nicht auf die Daten eines anderen zugreifen kann.[46] Die Umsetzung erfordert die Einrichtung individueller Benutzer-Accounts für jeden Cloud-Anwender. Bei Infrastrukturdiensten (IaaS oder PaaS) erfolgt in der Regel eine Trennung durch die Einrichtung virtueller Server mit eigenen Adressbereichen.

8. Portabilität

Eine Portabilität der Daten kann für einen Cloud-Anwender Bedeutung erlangen, der seinen Anbieter wechseln und seine Daten vom einen ins andere System migrieren möchte. Die *Art. 29-Datenschutzgruppe* spricht deshalb die Empfehlung für Anwender aus, vor Inanspruchnahme eines Systems die Möglichkeiten einer Datenmigration zu überprüfen, um nicht aus faktischen Gründen an den Anbieter gebunden zu sein (sog. Lock-in).[47] Auch wenn diese Anforderung nicht für alle Cloud-Dienstleistungen relevant sein dürfte, sollte sie vor allem dann berücksichtigt werden, wenn komplexere Datenbanken in Cloud-Lösungen verarbeitet werden. Konkret ist auf die Verwendung standardisierter Datenformate und Schnittstellen zu achten.

9. Sichere Löschung

Um die Vertraulichkeit der Daten auch nach einer Löschung gewährleisten zu können, empfiehlt die *Art. 29-Datenschutzgruppe* den Einsatz sicherer Löschverfahren durch mehrfaches Überschreiben oder spezielle Software-Tools.[48] Insbesondere bei Cloud-Diensten mit einer Vielzahl häufig wechselnder Anwender ist dies ein wichtiger Aspekt, um zu verhindern, dass die Daten eines vorherigen Anwenders von einem späteren eingesehen werden können. Sicherere Löschungsverfahren bremsen jedoch in der Regel die Performance eines Systems, sodass auf diese nur dann zurückgegriffen werden sollte, wenn die Vertraulichkeit der Daten sonst tatsächlich in Gefahr ist.[49] Hinweise zu sicheren Löschverfahren bietet der IT-Grundschutz-Katalog des *BSI*.[50]

10. Nachweisbarkeit (Accountability)

Schließlich setzt die *Art. 29-Datenschutzgruppe* recht detaillierte Anforderungen an die Nachweisbarkeit der Verarbeitungsschritte (Accountability). Es müsse jederzeit Nachweis darüber erbracht werden können, was welcher Anbieter wann und wie gemacht hat. Darüber hinaus müsse das Einhalten angemessener Maßnahmen zur Gewährleistung der Datenschutzgrundsätze nachweisbar sein. Hierzu zählen insbesondere technische und organisatorische Vorkehrungen, die es ermöglichen, Datenverarbeitungen zu identifizieren sowie Auskunftsersuchen zu beantworten, bzw. die Bestellung eines für die Überwachung des Datenschutzes Verantwortlichen.

VI. Zertifizierungen/Audits

Angesichts der insbesondere für kleine und mittlere Unternehmen fast unmöglichen Aufgabe, die Einhaltung der von den Cloud-Diensteanbietern zu treffenden technischen und organisatorischen Maßnahmen zu prüfen und zu überwachen, bietet es sich gerade beim Cloud Computing an, die Prüfung der Maßnahmen auf unabhängige Dienstleister zu übertragen. Diese

38 WP 196 (o. Fußn. 7), S. 16 (Isolation).
39 WP 196 (o. Fußn. 7), S. 15 (Confidentiality).
40 WP 196 (o. Fußn. 7), S. 16.
41 Sopot Memorandum (o. Fußn. 5), S. 3 f.
42 *Schröder/Haag*, ZD 2012, 362, 364.
43 WP 196 (o. Fußn. 7), S. 14 (Availability).
44 DoS steht für „Denial of Service" und meint die Nichtverfügbarkeit eines Systems. DoS-Angriffe führen diese durch eine Vielzahl automatisierter Anfragen herbei, die zu einer Überlastung des Systems führen.
45 The Open Web Application Security Project (OWASP), OWASP Top 10 – 2010, The Ten Most Critical Web Application Security Risks, abrufbar unter: www.owasp.org.
46 WP 196 (o. Fußn. 7), S. 15 f. (Isolation).
47 WP 196 (o. Fußn. 7), S. 16 (Portability).
48 WP 196 (o. Fußn. 7), S. 11 f. (Erasure of data).
49 Hierzu bereits *Schröder/Haag*, ZD 2012, 362, 365.
50 *BSI*, IT-Grundschutz-Katalog, Maßnahme M 2.433, abrufbar unter: https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02433.html.

können entweder im Auftrag des Cloud-Anbieters oder des Cloud-Anwenders (Auftraggeber) tätig werden und zertifizieren, ob der Cloud-Diensteanbieter die vereinbarten technischen und organisatorischen Maßnahmen tatsächlich einhält und ob diese den jeweils anwendbaren nationalen Anforderungen entsprechen. Die Zertifizierung durch Dritte wird von der *Art. 29-Datenschutzgruppe* nun ausdrücklich empfohlen.[51] Im Unterschied zu den bisherigen Stellungnahmen der deutschen Aufsichtsbehörden, wie auch der *Berlin Group*,[52] hält die *Art. 29-Datenschutzgruppe* sogar ausdrücklich fest, dass eine solche Prüfung bzw. Zertifizierung teilweise sogar aus technischen Gründen geboten sein kann, z.B. um durch Prüfungen jedes einzelnen Kunden bewirkte Risiken zu verhindern. Die Prüfungen durch Dritte sollen dann das Prüfrecht bzw. die Prüfpflicht des einzelnen Kunden ersetzen.[53]

VII. Internationale Datenverarbeitung

Schließlich erläutert die *Art. 29-Datenschutzgruppe*, wie Cloud-Dienstleistungen im außereuropäischen Ausland rechtssicher gestaltet werden können. In Bezug auf Dienstleistungen, die in den USA erbracht werden sollen, erwähnt die *Art. 29-Datenschutzgruppe* das Safe Harbor-Abkommen. Wie jedoch grundsätzlich bei Safe Harbor zertifizierten Empfängern dürfe sich der Auftraggeber als verantwortliche Stelle auch beim Cloud Computing nicht allein auf die eigene Erklärung der Zertifizierung nach Safe Harbor verlassen. Der Auftraggeber müsse die Zertifizierung nachprüfen und Nachweise dafür verlangen, dass die Grundsätze des Safe Harbor-Abkommens auch tatsächlich eingehalten werden.[54] Darüber hinaus sicherten die technischen und organisatorischen Sicherheitsanforderungen des Safe Harbor-Abkommens die spezifischen Gefahren des Cloud Computing nicht hinreichend, sodass hierüber hinausgehende Maßnahmen zum Schutz der Daten erforderlich seien. Grundsätzlich böten auch die Standardvertragsklauseln für Auftragsdatenverarbeitung bzw. Binding Corporate Rules hinreichende Sicherheit. Die *Art. 29-Datenschutzgruppe* weist jedoch zu Recht darauf hin, dass die rechtliche Situation für Cloud-Diensteanbieter, die in der EU bzw. dem EWR niedergelassen sind und Unterauftragnehmer außerhalb der EU/des EWR nutzen, komplexer ist. Solche Auftragsdatenverarbeiter können nach bisheriger Ansicht der Aufsichtsbehörden nicht unmittelbar Vertragspartner des EU-Standardvertrags für Auftragsdatenverarbeiter sein, da dieser von einem Auftragsdatenverarbeiter außerhalb der EU bzw. des EWR ausgeht.[55]

VIII. Zugriff auf Daten durch ausländische Sicherheitsbehörden

Schließlich nimmt die *Art. 29-Datenschutzgruppe* zu der Frage Stellung, ob außereuropäische Sicherheitsbehörden Zugriff auf Daten haben dürfen, die eine dem europäischen Datenschutzrecht unterliegende verantwortliche Stelle in einer Cloud verarbeiten lässt. Nach Auffassung der *Art. 29-Datenschutzgruppe* dürfen außereuropäische Sicherheitsbehörden in Clouds gespeicherte Daten europäischer Auftraggeber nur dann abfragen, wenn dieser Zugriff entweder auf spezielle internationale Abkommen oder allgemeine Rechtshilfeabkommen gestützt werden kann oder von einer nationalen europäischen Aufsichtsbehörde genehmigt wird.[56] Da sich der derzeit offenbar mögliche Zugriff von US-Sicherheitsbehörden auf Daten US-amerikanischer Cloud-Diensteanbieter nach dem US Patriot Act nicht auf internationale Abkommen stützen kann,[57] begegnen Cloud-Dienstleistungen US-amerikanischer Anbieter erheblichen datenschutzrechtlichen Bedenken.[58] Diese Bedenken dürften zudem nicht durch vertragliche Vereinbarungen mit den US-Anbietern ausräumbar sein, da privatrechtliche Vereinbarungen US-Sicherheitsgesetze nicht beschränken können.[59]

IX. Bewertung

Die eingangs gestellte Frage nach neuen Anforderungen für Cloud Computing kann mit „ja, aber nur wenig" gut beantwortet werden. Die Stellungnahme der *Art. 29-Datenschutzgruppe* greift die meisten schon von den deutschen Aufsichtsbehörden bzw. der *Berlin Group* im Sopot-Memorandum formulierten Anforderungen auf und fügt dankenswerterweise nur wenige weitere Vorgaben hinzu, wie z.B. die Informationspflicht gegenüber den Betroffenen über die Cloud-Diensteanbieter und ihrer Unterauftragnehmer.[60]

Leider hat es die *Art. 29-Datenschutzgruppe* jedoch nur an sehr wenigen Stellen geschafft, die schon sehr hohen Anforderungen der deutschen Aufsichtsbehörden bzw. der *Berlin Group* etwas flexibler zu gestalten. Insbesondere ist auch bedauerlich, dass die *Art. 29-Datenschutzgruppe* nun wie die deutschen Aufsichtsbehörden Cloud-Diensteanbieter unter den Generalverdacht stellen, eine erhöhte Bereitschaft zum Vertragsbruch zu haben, und daher die Absicherung ihrer Verpflichtungen durch Vertragsstrafen fordert.[61] Schade ist auch, dass sich die *Art. 29-Datenschutzgruppe* zu den technisch-organisatorischen Maßnahmen jeweils nur sehr knapp geäußert hat, die Verfolgung der allgemein anerkannten Schutzziele fordert, ohne aber konkrete Maßnahmen zur Umsetzung zu benennen. Hier finden sich in den Stellungnahmen anderer Aufsichtsbehörden z.T. detailliertere Ausführungen.

Sehr zu begrüßen ist jedoch der konsequente Schritt, nicht nur auf die Vorteile von Zertifizierungen bzw. Audits durch anerkannte Sachverständige zu verweisen, sondern ausdrücklich festzuhalten, dass diese das Haftungsrisiko des Auftraggebers deutlich reduzieren können.[62] Ebenfalls positiv ist die lang erwartete Stellungnahme zum US Patriot Act, wonach nun ausdrücklich festgehalten wird, dass Zugriffe von US-Sicherheitsbehörden entweder auf spezielle internationale Abkommen oder allgemeine Rechtshilfeabkommen gestützt werden müssen oder von einer nationalen europäischen Aufsichtsbehörde zu genehmigen sind.[63]

Darüber hinaus muss zukünftig wohl ein besonderes Augenmerk auf die weitere Entwicklung zur Anwendbarkeit des europäischen Datenschutzrechts gelegt werden. Die Festlegung der *Art. 29-Datenschutzgruppe*, wonach bereits ein Cloud-Server den Geltungsbereich der DS-RL und deren Recht zur Anwendung bringt, birgt Gefahren für die Wettbewerbsfähigkeit europäischer Cloud-Diensteanbieter. Es wäre sehr zu begrüßen, wenn sich die *Art. 29-Datenschutzgruppe* hier der Auffassung des *Düsseldorfers Kreises* anschließen könnte, der zumindest

---

51 WP 196 (o. Fußn. 7), S. 22.
52 S.a. Orientierungshilfe – Cloud Computing (o. Fußn. 3), S. 9 und 21; Sopot Memorandum (o. Fußn. 5), S. 5.
53 WP 196 (o. Fußn. 7), S. 22; unterstützend: *Simitis/Petri*, § 11 Rdnr. 59; *Weichert*, DuD 2010, 679, 683; *Heidrich/Wegener*, MMR 2010, 803, 806; *Schröder/Haag*, ZD 2011, 147, 152 m.w.Nw.; zur Auswahl zertifizierter Cloud-Anbieter *Giebichenstein/Weiss*, DuD 2011, 338 ff.
54 WP 196 (o. Fußn. 7), S. 17.
55 Instruktiv zum Rechtsstreitstand *Schmidl*, World Data Protection Report July 2012, 6, 10.
56 WP 196 (o. Fußn. 7), S. 23.
57 *Whittaker*, ZD-Net v. 28.6.2011, http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225.
58 *ULD*, PM v. 3.7.2011, https://www.datenschutz.de/news/alle/detail/?nid=4984; *Barnitzke*, MMR-Aktuell 2011, 321103; „EU-Parlamentarier besorgt über US-Zugriff auf Cloud-Daten", http://www.golem.de/1107/84763.html; ausf. hierzu *Schröder/Haag*, ZD 2011, 147, 152 m.w.Nw.
59 Vgl. *Schröder/Haag*, ZD 2012, 362, 365, unter Hinw. auf *Becker/Nikolaeva*, CR 2012, 170, 175 f.
60 WP 196 (o. Fußn. 7), S. 6.
61 S. Ziff. IV.
62 S.o. Ziffer VII und WP 196 (o. Fußn. 7), S. 22.
63 WP 196 (o. Fußn. 7), S. 23.

bei der Verarbeitung von außereuropäischen Daten nur eine sehr begrenzte Anwendung des materiellen europäischen Datenschutzrechts fordert. [64]

Positiv ist aber, dass sich nun auf europäischer Ebene langsam ein einheitlicher Standard für datenschutzgerechte Cloud-Lösungen durchsetzt, wenngleich all diese Empfehlungen sicher noch nicht das letzte Wort in einem doch sehr von der Dynamik der technischen Entwicklungen geprägten Rechtsgebiet darstellen.

64 Fallgruppen Internationale Auftragsdatenverarbeitung (o. Fußn. 13), S. 16, Beispiel H.

Dr. Christian Schröder
ist Rechtsanwalt bei der BDO Legal Rechtsanwaltsgesellschaft mbH 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.