Cloud Computing in der anwaltlichen Beratungspraxis

RA Dirk Reintzsch, Köln*

I. Einleitung

Cloud Computing ist derzeit eines der zentralen Themen im Bereich der Informationstechnologie, wobei sich eine allgemeingültige Definition des Cloud Computing bislang noch nicht herausgebildet hat und die anzutreffenden Begriffsverständnisse in den Einzelheiten teils voneinander abweichen.[1] Aus unternehmerischer Sicht lässt sich Cloud Computing wohl am treffendsten als besondere Form des IT-Outcourcing beschreiben, bei dem IT-Service Leistungen auf einen (externen) Dienstleister ausgelagert werden. Statt eigene IT Ressourcen in Form von Hard- und Software zu beschaffen und zu betreiben, beziehen Unternehmen IT-Leistungen aus der Cloud (d.h. zumeist über das Internet). Anders als beim klassischen IT-Outsourcing hält der Dienstleister die IT-Infrastruktur allerdings nicht nur für einen, sondern für eine Vielzahl von (potentiellen) Kunden vor. Dies erlaubt Skaleneffekte, setzt jedoch auch eine gewisse Standardisierung voraus. Cloud Computing Angebote basieren auf dem Einsatz virtueller Systeme, die unabhängig von der konkreten Hardware je nach Nachfrage konfiguriert und zur Verfügung gestellt werden können. Hierdurch werden ein bedarfsgerechter Bezug und eine verbrauchsabhängige Abrechnung der Serviceleistungen ermöglicht, d.h. der Kunde muss nur für das bezahlen, was er auch tatsächlich genutzt hat.[2] Als gängige Erscheinungsformen von Cloud Computing haben sich insbesondere „Infrastructure as a Service" (IaaS), „Plattform as a Service" (PaaS) und „Software as a Service" (SaaS) etabliert, im Rahmen derer der Cloud Anbieter dem Kunden Rechen- und Speicherleistung (IaaS), eine Plattform, z.B. zur Entwicklung von Software (PaaS) oder eine auf seinen Servern vorinstallierte Softwareanwendung über das Internet zur Nutzung bereitstellt (SaaS).[3]

Trotz der hohen medialen Aufmerksamkeit, die der Thematik Cloud Computing seit einiger Zeit zuteil wird und der vielen unbestreitbaren Vorteile, welche die Technologie bereit hält (neben dem aus der verbrauchsabhängigen Abrechenbarkeit resultierenden Kosteneinsparpotential sei exemplarisch nur die steigende Agilität aufgrund der Ermöglichung einer ortsungebundenen IT-Nutzung genannt), haben insbesondere deutsche Unternehmen diese bislang erwiesenermaßen nur recht zögerlich zum Bestandteil ihrer IT-Strategie gemacht.[4] Als Hauptgrund wurden Bedenken im Hinblick auf die Sicherheit der in die Cloud eingestellten Informationen und Daten ausgemacht. Einer Vielzahl von IT-Verantwortlichen fehlt es ganz offenbar noch am dem erforderlichen Vertrauen in die Cloud Anbieter, weshalb sie lieber davon absehen, ihre mitunter sehr sensiblen unternehmensbezogenen Daten in die Cloud zu verlagern. Nichtsdestotrotz gibt es auch schon heute viele Unternehmen, die den Schritt in die Cloud wagen und insofern rechtlichen Beratungsbedarf anmelden.

Aus anwaltlicher Sicht teilt sich die Beratung in zwei Bereiche. Zum einen gilt es, den Mandanten auf zwingende Gesetze hinzuweisen, die bei dem Bezug von Cloud Leistungen zu beachten sind. Dies können Vorschriften aus dem Steuerrecht sein, sofern steuerlich relevante Daten in der Cloud verarbeitet werden sollen. Wollen Banken und Versicherungen wesentliche Leistungen aus der Cloud beziehen, sind die Voraussetzungen des Aufsichtsrechts zu beachten. Vor allem aber ist das Datenschutzrecht zu beachten, da Datenverarbeitungen in der Cloud fast immer auch personenbezogene Daten betreffen.

Neben der Beratung zu diesen zwingenden Vorschriften besteht die anwaltliche Aufgabe darin, bei der Gestaltung des Vertrages zwischen Cloud Anbieter und Kunden zu beraten.[5] Hier geht es in erster Linie um eine angemessene Verteilung von Risiko und Chance, z.B. bei den Themen

* Der Autor ist Rechtsanwalt bei Oppenhoff & Partner in Köln.

1 Vgl. zur Definition des Begriffs „Cloud Computing": Nägele/Jacobs, ZUM 2010, 281; *Wagner/Blaufuß*, BB 2012, 175.

2 *Nägele/Jacobs* (ZUM 2010, 281) sprechen in diesem Zusammenhang von einem „Paradigmenwechsel".
Auf technischer Ebene wird dies realisiert, indem die Anbieter solcher Leistungen große Rechenzentren errichten, auf deren (unzähligen) Computern beispielsweise die betreffende Software ausgeführt wird oder der Speicherplatz in Form von Festplatten tatsächlich vorhanden ist. Der einzelne Nutzer bekommt die Leistungen dann über das Internet, meist über den Browser, zur Verfügung gestellt. Dabei läuft die Software, deren Ergebnisse er angezeigt bekommt, nicht auf einem bestimmten Rechner, sondern verteilt auf alle vorhandenen Maschinen, je nachdem, welche gerade die notwendigen Ressourcen frei hat. Die dazu benutzte Technik nennt man „Virtualisierung", weil den Nutzern keine echten physischen Computer exklusiv zur Verfügung stehen, sondern virtuelle Maschinen mit soviel Ressourcen, wie eben gerade benötigt werden.

3 Vgl. zu den unterschiedlichen Erscheinungsformen von Cloud Computing: *Bierekoven*, ITRB 2010, 42 (42/43).

4 So das Ergebnis einer von Deloitte und BITKOM durchgeführten Umfrage.
http://www.deloitte.com/assets/Dcom-Germany/Local%20Assets/Documents/12_TMT/2010/DE_TMT_Cloud_Computing_19012011.pdf, Abruf v. 01.02.2013.

5 Vgl. auch *Niemann/Paul*, K&R 2009, S. 444 (445).

Haftung, Kündigung oder Exit, d.h. Rückführung oder Überleitung der Leistungsverantwortung bei Vertragsende. Bei urheberrechtlich relevanten Vorgängen des Cloud Computing wie der Nutzung von Software im Rahmen von SaaS muss außerdem sichergestellt werden, dass dem Kunden die für die Nutzung erforderlichen Rechte vertraglich eingeräumt werden und der Cloud Anbieter zu einer entsprechenden Rechtseinräumung überhaupt berechtigt ist.

Dieser Beitrag gibt einen kursorischen Überblick über einige der wesentlichen datenschutz- und urheberrechtlichen Aspekte des Cloud Computing, die es in der anwaltlichen Beratungspraxis zu berücksichtigen gilt.

II. Datenschutzrechtliche Aspekte des Cloud Computing

1. Grundsätzliche datenschutzrechtliche Zulässigkeit

Während die datenschutzrechtliche Zulässigkeit von Cloud Computing von einigen Autoren zunächst grundlegend angezweifelt wurde, herrscht mittlerweile – insbesondere bei den für die Rechtspraxis maßgeblichen Datenschutzbehörden[6] – die Auffassung vor, dass sich Cloud Computing auch insofern rechtskonform ausgestalten lässt.

2. Datenschutzrechtliche Qualifikation des Vertragsverhältnisses

Cloud Computing wird überwiegend als Auftragsdatenverarbeitung im Sinne von § 11 BDSG eingestuft, im Rahmen derer der Cloud Anbieter die fraglichen personenbezogenen Daten im Auftrag des Kunden verarbeitet.[7] Während die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gemäß § 4 I BDSG grundsätzlich nur unter der Voraussetzung zulässig ist, dass der Betroffene hierin einwilligt oder der Verarbeitungsvorgang von einer gesetzlichen Erlaubnisnorm gedeckt ist, besteht die Besonderheit einer Auftragsdatenverarbeitung darin, dass der weisungsabhängige Auftragnehmer gewissermaßen als verlängerter Arm des Auftraggebers fungiert, weshalb eine zu rechtfertigende Übermittlung zwischen beiden Stellen gewöhnlich nicht stattfindet.[8] Stattdessen sind die Voraussetzungen des § 11 BDSG einzuhalten, d.h. insbesondere ein schriftlicher Vertrag abzuschließen, in dem vom Gesetz definierte Aspekte zu regeln sind.

3. Datenverarbeitung im Drittland (außerhalb der EU und des EWR)

Auftraggeber und Auftragnehmer können gemäß § 3 VIII 3 BDSG aber nur dann als Einheit betrachtet werden, wenn der Cloud Anbieter die Daten in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) verarbeitet. Da die Daten im Rahmen von Cloud Computing aber häufig auf weltweit verstreuten Serverfarmen abgelegt werden, gelangt die Privilegierungswirkung der Auftragsdatenverarbeitung nicht immer unmittelbar zur Anwendung. In diesem Fall liegt also eine Übermittlung von Daten vor, die aber nach § 28 BDSG zulässig sein kann. Probleme bestehen aber immer dann, wenn die Beteiligten auf die Privilegierungswirkung der Auftragsdatenverarbeitung angewiesen sind, etwa weil eine Verarbeitung besonderer Arten personenbezogener Daten im Sinne von § 3 IX BDSG in Rede steht (u.a. Angaben über religiöse Überzeugungen und die Gesundheit), die wegen ihrer gesteigerten Schutzbedürftigkeit ohne Einwilligung der Betroffenen kraft Gesetzes nur unter sehr restriktiven Anforderungen zulässig ist. Ist die beabsichtigte Datenverarbeitung in entsprechend gelagerten Fällen – zu denken wäre etwa an eine Arbeitnehmerdatenbank, z.B. mit Angaben zur Gesundheit oder Religion der Arbeitnehmer – nicht von den gesetzlichen Erlaubnisnormen gedeckt und auch eine Einholung von Einwilligungen der Betroffenen nicht möglich oder praktikabel, bestehen mehrere Möglichkeiten: Es kann mit dem Cloud Anbieter vereinbart und in den abzuschließenden Vertrag aufgenommen werden, dass die Verarbeitung der personenbezogenen Daten insgesamt oder zumindest die Verarbeitung der nach dem Gesetz als besonders sensitiv eingeschätzten Daten ausschließlich auf dem Gebiet der EU bzw. im EWR erfolgen darf.[9] Ist dies nicht möglich bzw. verhandelbar, ist entweder durch technische und organisatorische Maßnahmen sicherzustellen,

---

[6] Dies lässt sich mittelbar etwa der „Orientierungshilfe – Cloud Computing" der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26.09.2011entnehmen. http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf, Abruf v. 01.02.2013.

[7] Ob dies tatsächlich zutrifft, hängt unter anderem davon ab, ob der Kunde faktisch und rechtlich Herr der Daten bleibt, d.h. die Entscheidungshoheit über den Umgang mit diesen behält. Zweifelhaft kann allerdings bereits die Frage sein, ob deutsches Datenschutzrecht überhaupt zur Anwendung gelangt. Ausgangspunkt der Betrachtung ist in der Praxis die Frage, wo die verantwortliche Stelle ihren Sitz hat. Bei einer Auftragsdatenverarbeitung ist verantwortliche Stelle gemäß § 3 VII BDSG der Auftraggeber, weshalb auf den Kunden (und nicht den Cloud Anbieter als Auftragnehmer) abzustellen ist: Sitzt der Kunde in Deutschland, ist deutsches Datenschutzrecht zu beachten. Sitzt der Kunde in einem anderen Mitglieds- bzw. Vertragsstaat der EU bzw. des EWR, kommt gemäß § 1 V 1 BDSG grundsätzlich nicht deutsches Datenschutzrecht, sondern das Datenschutzrecht seines Sitzlandes zur Anwendung (sog. Sitzprinzip). Sitzt der Kunde in einem Drittland (weder Mitgliedsstaat der EU noch Vertragsstaat des EWR), ist deutsches Datenschutzrecht nach § 1 V 2 BDSG nur dann anwendbar, wenn sich der datenschutzrechtlich relevante Vorgang – die Datenverarbeitung in der Cloud – auf deutschem Boden vollzieht. Im letztgenannten Fall kommt es mit anderen Worten nicht mehr auf den Sitz des Kunden, sondern auf den Ort der Datenverarbeitung an (sog. Territorialitätsprinzip). Diese Feststellung kann im Rahmen von Cloud Computing aber erhebliche Schwierigkeiten bereiten, weil die Daten nicht selten auf wechselnden, weltweit verstreuten Serverfarmen abgelegt werden und unter Umständen auch für den Cloud Anbieter nicht ohne weiteres feststellbar ist, wann sich die diese wo befinden. Vgl. eingehender zur Thematik des anwendbaren Datenschutzrechts: *Nägele/Jacobs*, ZUM 2010, 281 (289/290).

[8] Vgl. *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 11 Rn. 3 u. 4.

[9] Die vertragliche Festlegung des physischen Standorts der Daten ist grundsätzlich ratsam, weil das Vorliegen einer Auftragsdatenverarbeitung im Sinne von § 11 BDSG unter anderem voraussetzt, dass der Kunde die Entscheidungshoheit über die wesentlichen Schritte

dass es nicht zu einer Übermittlung von besonderen Arten personenbezogener Daten kommt oder in letzter Konsequenz auch gänzlich vom Gang in die Cloud (zumindest über den jeweiligen Cloud Anbieter) abzusehen (wenn sich das Anfallen derartiger Daten nicht vermeiden lässt).

Ob die Daten innerhalb oder außerhalb der EU bzw. des EWR abgelegt werden, ist allerdings nicht nur für das Eingreifen der Privilegierungswirkung der Auftragsdatenverarbeitung von Belang. Der physische Standort der Daten ist vielmehr auch insofern von Bedeutung, als die Übermittlung von personenbezogenen Daten an einen Auftragsverarbeiter im Drittland gemäß §§ 4b, 4c BDSG überhaupt nur erfolgen darf, wenn bei diesem ein angemessenes Datenschutzniveau gewährleistet ist.[10] Dies lässt sich insbesondere dadurch herstellen, dass sich Cloud Anbieter und Kunde auf die Geltung der von der Europäischen Kommission ausgearbeiteten Standardvertragsklauseln für Auftragsverarbeiter verständigen, die hierfür unverändert in den abzuschließenden Cloud Vertrag zu implementieren sind. Soll der Cloud Anbieter als Teil einer international agierenden Konzerngesellschaft für andere Konzerngesellschaften eine interne Cloud betreiben, kommt daneben auch die Inkraftsetzung verbindlicher Unternehmensregelungen (sog. Binding Corporate Rules) in Betracht. Für in den USA ansässige Unternehmen hat die Europäische Kommission mit dem Handelsministerium der USA insofern eine Vereinbarung zu den Grundsätzen des sicheren Hafens (Safe Harbour-Abkommen) getroffen. Hiernach wird bei US-amerikanischen Unternehmen, die sich gegenüber der zuständigen US-Behörde bestimmten Datenschutzprinzipien – den sog. Safe Harbour Prinzipien – unterwerfen, ein angemessenes Datenschutzniveau angenommen.[11]

4. Form und Inhalt des Auftragsdatenverarbeitungsvertrags

Über diese aufgeführten, bei Cloud Computing aufgrund des gewöhnlich stattfindenden grenzüberschreitenden Datenverkehrs besonders relevanten Aspekte hinaus gilt es zu berücksichtigen, dass der Auftrag gemäß § 11 II 2 BDSG schriftlich zu erteilen ist, zumal der Einhaltung dieses Schriftformerfordernisses in der Literatur teils konstitutive Wirkung beigemessen wird, d.h. bei Nichtbeachtung keine wirksame Auftragsdatenverarbeitung vorliegen soll.[12]

Inhaltlich muss die Vereinbarung den in § 11 II BDSG aufgestellten Mindestanforderungen genügen, wobei sich insbesondere aus Sicht des Kunden die Aufnahme weiterer, cloud-spezifischer Bestimmungen empfiehlt: Dies vornehmlich deshalb, weil er als Auftraggeber für die Einhaltung der datenschutzrechtlichen Bestimmungen im Rahmen der Datenverarbeitung verantwortlich bleibt und bei Erfüllung der ihn treffenden Pflichten häufig in besonderem Maße auf die Mitwirkung des Cloud Anbieters angewiesen ist. So wird er etwa der sich aus § 35 BDSG unter Umständen ergebenden Verpflichtung zur Berichtigung, Löschung und Sperrung von Daten aufgrund seines in aller Regel nur sehr eingeschränkten Zugriffs auf die Systeme des Cloud Anbieters nur mit dessen Unterstützung nachkommen können. Daher bietet es sich an, die in den Vertrag nach § 11 II 2 Nr. 9 BDSG ohnehin aufzunehmenden Weisungsbefugnisse, die sich der Kunde vorbehält, möglichst konkret zu fassen und – sofern verhandelbar – zusätzlich mit einer Vertragsstrafenregelung für den Fall der Nichtbeachtung zu versehen, um gegenüber dem Cloud Anbieter ein wirksames Druckmittel zu haben.[13] Ferner ist es insbesondere ratsam, in den Vertrag so genannte Exit-Regelungen aufzunehmen, die festlegen, wie mit den in der Cloud abgelagerten Daten bei einem vorzeitigen Vertragsende zu verfahren ist, sprich unter welchen Voraussetzungen (Kosten etc.), wann (nämlich nicht erst bei Vertragsende) und wie (insbesondere in welchem Dateiformat) diese dem Kunden wieder verfügbar gemacht werden.[14]

5. Kontrollpflicht des Kunden gemäß § 11 II 4 BDSG

In verfahrenstechnischer Hinsicht stellt sich die Vorschrift von § 11 II 4 BDSG als problematisch dar, der zufolge der Auftraggeber – der Kunde – die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen (diese sind gemäß § 11 II 2 Nr. 3 BDSG in dem abzuschließenden Vertrag über die Auftragsdatenverarbeitung im Einzelnen festzulegen) durch den Auftragnehmer – den Cloud Anbieter – vor Auftragsbeginn und sodann regelmäßig zu kontrollieren hat. Schließt man hieraus auf die Verpflichtung zu einer persönlichen Vorortkontrolle, ist diese dem Kunden in der Regel kaum sinnvoll möglich. Auch ansonsten werden viele Kunden überhaupt nicht über das Know-how verfügen, derartige Kontrollen durchzuführen. Im Übrigen wird der Cloud Anbieter auch nicht immer ohne weiteres Auskunft geben können, wo sich die Daten genau befinden.[15] Nach wohl überwiegender, insbesondere auch von einer Datenschutzbehörde[16] schon geteilten Auffassung kann an die Stelle einer eigenen Überprüfung allerdings

der Datenverarbeitung hat, was sich dann auch im Hinblick auf den Ort der Datenverarbeitung dokumentieren lässt.

10 Vgl. hierzu auch *Wagner/Blaufuß*, BB 2012, 1751 (1752).

11 Den deutschen Datenschutzbehörden zufolge soll hierfür die bloße Zertifizierung des Unternehmens als Safe Harbour allerdings nicht mehr ausreichend sein. Die datenexportierende Stelle muss vielmehr unter anderem prüfen, ob das Zertifikat noch gültig ist (vgl. Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 28./29. April 2010. https://www.datenschutzzentrum.de/internationaler-datenverkehr/Beschluss_28_29_04_10neu.pdf, Abruf v. 01.02.2013).

12 So etwa *Gola/Schomerus*, (Fn. 8), § 11 Rdnr. 17; *Petri*, in: Simitis, BDSG, 7. Aufl. 2011, § 11 Rn. 64; *Wedde*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 11 Rn. 32; a.A. aber etwa *Gabel*, in; Taeger/Gabel, BDSG, § 11 BDSG Rn. 54.

13 So die Empfehlung der Datenschutzbehörden (vgl. Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26.09.2011unter Ziffer 3.3. http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf, Abruf v. 01.02.2013).

14 Vgl. zu dieser Thematik auch *Pohle/Ammann*, CR 2009, 273 (277).

15 *Pohle/Ammann*, CR 2009, 273 (277).

16 Bayerisches Landesamt für Datenschutz, 4. Tätigkeitsbericht 2009/2010, Ziffer 5.1.2. http://www.lda.bayern.de/lda/datenschutzauf-

auch das Testat eines unabhängigen Dritten treten, welcher die Kontrolle im Auftrag des Kunden durchführt.[17] Wenngleich somit eigentlich eine Lösung angedeutet ist, bleiben doch viele Fragen offen (etwa welche Anforderungen genau an das Testat zu stellen sind und welche Rechtsfolgen sich hieraus ergeben). Letztlich bleibt es dem Gesetzgeber vorbehalten, durch eine ausdrückliche gesetzliche Regelung für Rechtssicherheit zu sorgen.[18]

III. Urheberrechtliche Aspekte des Cloud Computing[19]

1. Urheberrechtliche Relevanz von SaaS

Soll Gegenstand der vertraglichen Vereinbarung zwischen Cloud Anbieter und Kunde die Nutzung von Software über die Cloud sein, handelt es sich in aller Regel um einen urheberrechtlich relevanten Vorgang, weil Software – genauer gesagt der Quell- und Objektcode in seiner konkreten Gestalt – nach Maßgabe der §§ 69a ff. UrhG urheberrechtlich geschützt ist.[20]

2. Nutzungshandlungen des Cloud Anbieters

Das ausschließliche Recht, das urheberrechtlich geschützte Werk zu verwerten, liegt gemäß § 15 I UrhG zunächst beim Urheber selbst, also bei der natürlichen Person, welche den Softwarecode programmiert hat. Bei angestellten Programmierern gehen die Verwertungsrechte gemäß § 69b UrhG automatisch auf den Arbeitgeber über. Ist der Cloud Anbieter nicht selbst Inhaber der Verwertungsrechte an der vertragsgegenständlichen Softwareanwendung, muss er sich vom Rechteinhaber die für sein Geschäftsmodell benötigten Nutzungsrechte einräumen lassen. Der Umfang der benötigten Rechte bemisst sich hierbei danach, welche relevanten Nutzungshandlungen stattfinden bzw. stattfinden sollen. In § 69c UrhG werden als mögliche Nutzungshandlungen von Software das Vervielfältigen, Umarbeiten, Verbreiten und die öffentliche Wiedergabe einschließlich der öffentlichen Zugänglichmachung genannt. Diese Aufzählung ist allerdings nicht abschließend zu verstehen. Es kommen – wie sich der Vorschrift von § 31a UrhG entnehmen lässt – vielmehr auch weitere, gesetzlich (noch) nicht normierte Nutzungsarten in Betracht.

a) Nutzungsrecht für Installation und Ablaufen lassen

Um die Softwareanwendung zur Nutzung bereit zu stellen, muss der Cloud Anbieter diese zunächst auf seiner IT-Infrastruktur installieren und anschließend auf seinen Systemen ablaufen lassen. Da die Software bzw. Bestandteile derselben im Rahmen der Installation gespeichert werden, sind die Anforderungen an eine Vervielfältigung im Rechtsinne erfüllt.[21] Das Ablaufen lassen von Software setzt in aller Regel eine zumindest vorübergehende Speicherung im Arbeitsspeicher des betreffenden Rechners voraus, weshalb es insofern zu einer weiteren Vervielfältigungshandlung kommt. Der Cloud Anbieter benötigt daher für beide Vorgänge ein Vervielfältigungsrecht.

b) Nutzungsrecht für die Bereitstellung zur Nutzung

Während Vervielfältigungen anlässlich von Installation und Ablaufen lassen charakteristische Vorgänge im Zusammenhang mit der Nutzung von Software sind, die auch bei einer herkömmlichen Nutzung von Software im eigenen Betrieb des Unternehmens stattfinden, stellt sich speziell für das Cloud Computing bzw. genauer gesagt für die Erscheinungsform SaaS die Frage, wie die gewöhnlich an eine unbestimmte Anzahl von Personen gerichtete Nutzungsbereitstellung der Software über das Internet urheberrechtlich zu bewerten ist.

Begrifflich naheliegend erscheint es, den Vorgang als gemäß § 69c Nr. 4 UrhG zustimmungsbedürftige öffentliche Zugänglichmachung einzustufen. Das Öffentlichkeitserfordernis wird gewöhnlich in der Tat auch erfüllt sein.[22]

Ob es auch zu einer Zugänglichmachung der fraglichen Softwareanwendung kommt, wird allerdings kontrovers beurteilt.[23] Während die wohl herrschende Meinung[24] eine öffentliche Zugänglichmachung für einschlägig erachtet, nimmt eine in der Literatur vertretene Auffassung[25] den konträren Standpunkt ein. Sie verneint eine öffentliche

sicht/lda_daten/dsa_Taetigkeitsbericht_2010.pdf, Abruf v. 01.02.2013.

17 Vgl. *Gola/Schomerus*, (Fn. 8), § 11 Rdnr. 21; *Petri*, (Fn. 12), § 11 Rn. 59, *Wedde*, (Fn. 12), § 11 Rn. 57.

18 Vgl. zu diesem Aspekt auch die eingehenden Ausführungen im rechtspolitischen Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing" der Arbeitsgruppe „Rechtsrahmen des Cloud Computing" im Kompetenzzentrum Trusted Cloud. http://www.trusted-cloud.de/documents/Datenschutzrechtliche-Loesungen-fuer-Cloud-Computing.pdf, Abruf v. 01.02.2013.

19 Die nachfolgenden Ausführungen gehen auf das Arbeitspapier „Lizenzierungsbedarf beim Cloud Computing" der Arbeitsgruppe „Rechtsrahmen des Cloud Computing" im Kompetenzzentrum Trusted Cloud zurück, an dessen Erstellung der Autor beteiligt war. http://www.trusted-cloud.de/documents/121102_Thesenpapier_Lizenzen_03.pdf, Abruf v. 01.02.2013.

20 Urheberrechtlich relevante Vorgänge sind des Weiteren in Form des Up-und Downloads von urheberrechtlich geschützten Werken in die über die Cloud zur Nutzung bereit gestellte Software denkbar, vgl. Bisges, MMR 2012, 574 (575).

21 Vgl. auch *Bisges*, MMR 2012, 574 (575/576).

22 Dies gilt gewöhnlich selbst für den Fall, dass es sich nicht um eine Public Cloud, sondern um Private Cloud (wie etwa ein firmeneigenes Intranet) handelt, weil der Öffentlichkeitsbegriff in § 15 III UrhG sehr weit gefasst ist, vgl. hierzu *Bisges*, MMR 2012, 574 (576).

23 Einigkeit besteht allerdings wohl insofern, als es nicht darauf ankommt, ob die Software tatsächlich abgerufen bzw. ausgeführt wird (vgl. *Wiebe*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 19a UrhG Rn. 2).

24 Vgl. OLG *München* GRUR-RR 2009, 91 (91 f.); Bisges, MMR 2012, 574 (576); *Niemann/Paul*, K&R 2009, 444 (448); *Pohle/Ammann*, CR 2009, 273 (276); *Redeker*, IT-Recht, 5. Aufl. 2012, Abschnitt A) Rn. 70; *Spindler*, in: Loewenheim Urheberrecht Kommentar, 4. Aufl. 2010, vor §§ 69a ff. Rn. 69.

25 *Grützmacher*, CR 2011, 697 (705); *Nägele/Jacobs*, ZUM 2010, 281 (287); für den Fall, dass der Kunde im Rahmen der Nutzung der Softwarefunktionalitäten keine zustimmungsbedürftige Handlung vornimmt auch: Koch, ITRB 2011, 42 (43/44).

Zugänglichmachung unter Hinweis darauf, dass dem Kunden gerade nicht – wie es von § 69c Nr. 4 UrhG gefordert werde – die Software selbst, also der ablauffähige Code, sondern allein die Benutzeroberfläche des Computerprogramms übertragen und somit zugänglich gemacht werde.[26] Dies erscheint auf den ersten Blick zweifelhaft, da sich dem Gesetzeswortlaut keine Anhaltspunkte dafür entnehmen lassen, dass das Computerprogramm oder wesentliche Teile desselben für ein Zugänglichmachen im Sinne der Vorschrift im Quell- oder Objektcode abrufbar sein müssen. Unbestritten ist, dass es sich bei der grafischen Benutzeroberfläche eines Computerprogramms nicht um eine urheberrechtlich geschützte Ausdrucksform des Computerprogramms handelt.[27] Da „Zugänglichmachung" als das Eröffnen von Zugriff auf das betreffende Werk definiert wird,[28] lässt es sich daher zweifelsohne gut vertreten, in dem bloßen zum Abruf stellen der nicht zum Werk „Computerprogramm" gehörenden grafischen Benutzeroberfläche noch keine öffentliche Zugänglichmachung zu erblicken. Andererseits lassen sich auch gute Argumente für die gegenteilige Auffassung finden. So hat etwa das *OLG München* nicht zu Unrecht darauf verwiesen, „dass auch andere Werkarten (Theaterstücke, Musikwerke) in einer Weise der Öffentlichkeit zugänglich gemacht werden, ohne dass dieser das Werk selbst in körperlicher Form […] präsentiert wird."[29] Selbst wenn man das Verständnis teilt, dass keine öffentliche Zugänglichmachung vorliegt, wird man hieraus richtigerweise aber nicht etwa auf die urheberrechtliche Irrelevanz der Nutzungsbereitstellung der Software schließen können.[30] Der Cloud Anbieter dürfte hierfür dann vielmehr ein gesondertes, gesetzlich unbenanntes Nutzungsrechts – ein sog. Nutzungsrecht sui generis – benötigen.[31]

Aus Rechtsberatersicht stellt sich die Frage, wie mit dieser unsicheren Rechtslage umzugehen ist. Da eine höchstrichterliche Entscheidung (noch) nicht existiert, kann sich der Anwalt nicht einer der obigen Auffassungen anschließen und diese (allein) bei der Vertragsgestaltung berücksichtigen. Die Lösung kann bei Beratung eines Cloud Anbieters nur darin bestehen, sich in dem mit dem Rechteinhaber abzuschließenden Vertrag für die beabsichtigte Nutzungsbereitstellung der Software über die Cloud bis auf weiteres sowohl ein Recht zur öffentlichen Zugänglichmachung als auch ein Nutzungsrecht für die zur Verfügungsstellung mittels Cloud Computing (Nutzungsrecht *sui generis*) einräumen zu lassen. Während sich dies für das gesetzlich benannte Nutzungsrecht „öffentliche Zugänglichmachung" ohne größeren Aufwand bewerkstelligen lässt, geht mit der Aufnahme einer unbekannten Nutzungsart naturgemäß ein ungleich größerer vertragsgestalterischer Aufwand einher, zumal speziell im Urheberrecht eine exakte und ausdrückliche Benennung der zu übertragenden Rechte verlangt wird.[32] Bei Beratung eines (potentiellen) Kunden ist zu prüfen, ob der Anbieter über die benötigten Rechte verfügt, um dem Kunden die Software wie beabsichtigt über die Cloud zur Nutzung bereitstellen zu können. Der Kunde wird (abgesehen von Großtransaktionen, in deren Rahmen eine sog. Vendor Due Diligence stattfindet) allerdings in den wenigsten Fällen tatsächlich einmal Einblick in den zwischen Anbieter und Rechteinhaber geschlossenen Vertrag bekommen.

3. Nutzungshandlungen des Kunden

Für SaaS ist es charakteristisch, dass die Softwareanwendung ausschließlich auf den Rechnern des Cloud Anbieters installiert wird und dort abläuft, weshalb es insofern zu keiner Vervielfältigungshandlung durch den Kunden kommt.[33] Letzterer kann die Software aber häufig nur unter der Voraussetzung nutzen, dass er auf seinem Rechner zunächst ein Programm installiert, welches er bei Bedarf ablaufen lässt, um auf die Software zugreifen zu können (in Form sog. Clients und Apps etc.). Für die hiermit einhergehenden Vervielfältigungen dieses Programms benötigt der Kunde ein entsprechendes Nutzungsrecht. Sofern es sich hierbei nicht ohnehin um bei dem Kunden bereits vorhandene Standardprogramme handelt (wie etwa den Internetbrowser), ist bei der Vertragsgestaltung für eine entsprechende Rechtseinräumung Sorge zu tragen.

IV. Fazit

Cloud Computing ist ein weiteres Beispiel für die im IT-Bereich häufiger anzutreffende Problematik, dass die Rechtsentwicklung mit der rasanten technologischen Entwicklung nicht immer Schritt halten kann. Die führt zwangsläufig zu Rechtsunsicherheit, welche nicht nur einige Herausforderungen für die anwaltliche Beratungspraxis bereit hält, sondern wohl auch eine der Ursachen dafür ist, dass derzeit noch viele deutsche Unternehmen zögern, den Weg in die Cloud zu beschreiten. Zum Teil lässt sich dieser Rechtsunsicherheit – wie etwa im datenschutzrechtlichen Bereich bei der Kontrollpflicht des Auftraggebers gemäß § 11 II 4 BDSG – nur durch eine Anpassung der Rechtslage, sprich ein Tätigwerden des Gesetzgebers, effektiv begegnen. Häufig geht es – wie etwa bei den urheberrechtlichen Aspekten des Cloud Computing – auch „nur" um eine verbindliche Klärung der bestehenden Rechtslage, die in einigen relevanten Bereichen mittlerweile aber auch bereits angestoßen worden ist. Überhaupt lässt sich festhalten, dass trotz der bestehenden Probleme eine rechtskonforme Ausgestaltung des Cloud Computing Prozesses bei Wahrung anwaltlicher Vorsicht auch derzeit schon möglich ist.

---

[26] So *Grützmacher*, CR 2011, 697 (705); N*ägele/Jacobs*, ZUM 2010, 281 (287).

[27] Dies hat auch unlängst der *EuGH* bestätigt (GRUR 2011, 220).

[28] *Dreier/Schulze*, UrhG, 3. Aufl. 2008, § 19a Rn. 6.

[29] *OLG München* GRUR-RR 2009, 91.

[30] Dahingehend aber möglicherweise *Koch*, ITRB 2011, 42 (43/44).

[31] So explizit *Nägele/Jacobs*, ZUM 2010, 281 (288); womöglich auch *Grützmacher*, CR 2011, 697 (705), wonach der Cloud Anbieter zwar kein Recht zur öffentlichen Zugänglichmachung, wohl aber ein „weitergehendes" Vervielfältigungsrecht benötigen soll.

[32] Vgl. *Dreier/Schulze*, (Fn. 28), § 31 Rn. 110 ff.

[33] *Niemann/Paul*, K&R 2009, 444 (448).