PRIVACY TOPICS

Matthis Grenzer

Niklas Heitmüller

Die Autoren sind wissenschaftliche Mitarbeiter und Doktoranden bei Prof. Dr. Gerald Spindler, Georg-August-Universität Göttingen. Der Beitrag wurde im Rahmen des Forschungsprojektes „PRACTICE: Privacy-Preserving Computation in the Cloud" verfasst.

Zur Problematik des Personenbezuges beim Cloud Computing

Welche Bedeutung hat der Personenbezug von Daten für Cloud Computing und wonach beurteilt er sich?

Matthis Grenzer und *Niklas Heitmüller*

Dass sich hinter dem (Sammel-)Begriff „Cloud Computing" eine Vielzahl verschiedener Technologien verbirgt, ist mittlerweile auch denen bekannt, die keine IT-Experten sind. Auch dass sich rechtliche – insbesondere datenschutzrechtliche – Schwierigkeiten ergeben können, wenn Cloud Computing eingesetzt wird, ist nicht neu. Dieser Beitrag soll einen Überblick darüber bieten, welche datenschutzrechtlichen Problematiken sich bei unterschiedlichen Anwendungsmöglichkeiten von Cloud Computing ergeben. Es sollen dann Ansätze aufgezeigt werden, um diesen Problematiken datenschutzkonform zu begegnen. Insbesondere entscheidend für die Anwendbarkeit des Datenschutzrechts ist das Merkmal des Personenbezugs des verarbeiteten Datums, auf dem der Schwerpunkt des Beitrags liegt. Es werden unterschiedliche Ansätze dazu vertreten, unter welchen Umständen Daten personenbezogen sind, insbesondere wenn sie pseudonymisiert oder verschlüsselt wurden. Dieser Beitrag bietet einen Überblick zu den vertretenen Ansichten und systematisiert diese, um letztlich Voraussetzungen auszuarbeiten, unter denen beim Cloud Computing ein Personenbezug von Daten nicht vorliegt. Dabei wird im Schwerpunkt die Rechtslage de lege lata gemäß dem BDSG und der Datenschutzrichtlinie 46/95/EG (DSRL) berücksichtigt als auch ein Ausblick auf die Rechtslage de lege ferenda gemäß dem Vorschlag des EU-Parlaments für eine Datenschutz-Grundverordnung gegeben.

I. Anwendungsmöglichkeiten von Cloud Computing

Cloud Computing bietet die Möglichkeit, leistungsstarke IT-Ressourcen zu nutzen, ohne sie selbst betreiben zu müssen. Vielmehr bezieht der Nutzer diese „aus dem Internet", wo sie, bildlich gesprochen, über ihm schwebend „in einer Wolke" angeboten werden. Dies bietet dem Nutzer finanzielle Vorteile, da er nur für den tatsächlichen Gebrauch des Cloud-Angebots zahlt, die daran hängenden Kosten für Anschaffung und Wartung aber nicht dauerhaft trägt. Die Dienste stehen dennoch „on-demand" zur Verfügung. Ermöglicht wird dies durch die Trennung von Soft- und Hardware mittels Virtualisierung. Vielen nur virtuell existenten Rechnern („virtual machines" – VMs) werden durch eine Steuerungssoftware physische Ressourcen zugewiesen. Neben Betriebssystemen können auch Speicherplatz, Netzwerke oder Anwendungen virtualisiert werden. Je nachdem, welche Belastung der Nutzer dem Cloud-Service gerade abverlangt, kann ihm flexibel und automatisiert mehr oder auch weniger Infrastruktur zur Verfügung gestellt werden. Dem Cloud-Service liegt entweder ein einzelner Server oder möglicherweise auch eine ganze Serverfarm zugrunde, deren Server in unterschiedlichen Nationen belegen sein können.[2]

1 The research leading to these results has received funding from the European Union Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-609611 (PRACTICE).

2 Ausführlich zur Funktionsweise von Cloud Computing: *Giedke,* Cloud Computing, 2013, S. 27–81; *Millard,* Cloud Computing Law, 2013, S. 3 ff.; *Baun/Kunze/Nimis/Tai,* Cloud Computing, 2009, S. 1–37; *Nägele*, ZUM 2010, 281; *Lehmann/Giedke*, CR 2013, 608.

Eine standardisierte, einheitliche Definition davon, was „Cloud Computing" ist, gibt es noch nicht, jedoch kann es in drei Arten von Technologien unterteilt werden:[3] Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS). Bei reiner IaaS stellt der Anbieter (Provider) dem Nutzer grundlegende Ressourcen in Form von Hardware, wie Speicherkapazitäten, Netzwerke und Rechenleistung zur Verfügung. Der Nutzer muss selbst ein Betriebssystem und die Software, die er nutzen möchte, installieren.[4] Das bedeutet aber nicht, dass der IaaS-Provider zwangsweise selbst die Hardware betreibt, welche letztlich dem Nutzer zur Verfügung gestellt wird. Es ist ebenso denkbar, dass er die Server durch Dritte betreiben lässt oder seinerseits ein IaaS-Angebot nutzt.[5] Beispiele dafür sind Amazons „Amazon Web Services" oder GoGrids „GoGrid", die das Hosting virtueller Anwendungen und Datenspeicherung ermöglichen sowie Microsofts „SQL Server", der Datenspeicherung und Suchanfragen ermöglicht.[6] Bei PaaS wird dem Nutzer eine cloudbasierte Programmierumgebung angeboten, die er nutzen kann, um z. B. eigene Software zu entwickeln. Er hat dabei keinen Einfluss auf die Infrastruktur, auf die sich die Programmierumgebung stützt. Cloud-Plattformen können daher als eine besondere Form des Hostings bezeichnet werden.[7] Mit dem PaaS-Angebot „Heroku" werden beispielsweise viele Apps für Apples „iPhone" oder für das soziale Netzwerk „Facebook" entwickelt.[8] Soll keine eigene Software implementiert werden, sondern bereits in einer Cloud bestehende Software lediglich genutzt werden, handelt es sich um SaaS. Auf die Software kann dann mittels eines Interfaces wie einem Web-Browser zugegriffen werden und die Nutzung der Software ist von jedem Gerät möglich, das ein solches Interface besitzt.[9] Ein sehr prominentes Beispiel dafür ist sicherlich „Facebook", aber auch „Dropbox", „PayPal", Googles „Google Drive" oder Apples „iCloud" sind SaaS-Angebote. Cloud Computing lässt sich auch wissenschaftlich nutzen. So ermöglicht es die Software „Sharemind" beispielsweise, statistische Datensätze cloud-basiert so auszuwerten, dass der Wissenschaftler die Ausgangsdaten selbst nicht kennen muss. Dies ist dann von Vorteil, wenn es sich um sensible Daten handelt. Durch sog. „Secret Sharing" bietet dies auch einen hohen Grad an Datensicherheit.[10] Eine scharfe Abgrenzung zwischen diesen verschiedenen Arten von Cloud Computing ist praktisch aber nur schwer möglich, da es vorkommt, dass ein Cloud-Angebot selbst auf einer Cloud-Umgebung ausgeführt wird. So läuft beispielsweise die SaaS-Software „Dropbox" und auch das PaaS-Angebot „Heroku" auf Amazons IaaS „Amazon Web Services". Google bietet mit seiner „Google App Engine" eine PaaS an, die das Entwickeln und Hosten von Software ermöglicht, welche selbst wiederum als SaaS angeboten werden kann.[11] Ob ein Cloud-Service auf einem anderen Cloud-Service beruht, ist für den Endnutzer u. U. nicht ersichtlich. Gemeinsam ist allen drei Modellen, dass der Nutzer des Services selbst nur einen Internetzugang benötigt und auf die jeweiligen Ressourcen, die ihm der Anbieter zur Verfügung stellt, mittels des Internets zugreifen kann. Diese Unterscheidung zwischen verschiedenen Arten des Cloud Computing folgt einem technischen Ansatz und sagt grundsätzlich noch nicht viel darüber aus, ob ein bestimmter Cloud-Dienst aus Sicht des Datenschutzrechts Probleme aufwirft oder nicht. Cloud-Dienste lassen sich aber nicht nur technisch nach der Art der angebotenen Services kategorisieren, sondern auch organisatorisch.[12] Es kann zwischen Public-, Private-, Community oder Hybrid-Cloud-Diensten unterschieden werden. In einer Public-Cloud gehören die Nutzer und der Anbieter der Cloud nicht derselben Organisation an. Mittels eines Web-Portals wird der Dienst durch den Provider den verschiedensten Nutzern zugänglich gemacht. Bei einer Private-Cloud wird die gesamte Cloud-Infrastruktur von einer einzigen Organisation benutzt, auch wenn sie nicht notwendigerweise von nur einer Organisation betrieben werden muss. Einen Mittelweg stellt die Community-Cloud dar, deren Nutzer einer bestimmten abgrenzbaren Gruppe angehören, die die gleichen Ziele verfolgen. Provider eines solchen Cloud-Dienstes können ein Dritter oder einer oder mehrere der Nutzer sein. Als Mischform besteht die Hybrid-Cloud, bei der zwei oder mehrere dieser Organisationsmodelle kombiniert werden.[13] So könnten beispielsweise unbedenkliche Datenverarbeitungsvorgänge in einer Public-Cloud ausgeführt werden, während ein firmen- oder behördeninterner Private-Cloud-Dienst für datenschutzkritische Anwendungen benutzt wird.

Anhand der Organisationsstruktur eines Cloud-Dienstes können datenschutzrechtliche Problematiken besser bewertet werden, als wenn lediglich danach unterschieden wird, was das Angebot technisch umfasst. Wenn derjenige, der für die Daten verantwortlich ist, diese aus der Hand geben muss, um den Cloud-Dienst nutzen zu können, muss dies datenschutzrechtlich zulässig sein. Dies kann beim Cloud Computing aus verschiedenen Gründen fraglich sein. Für die datenschutzrechtliche Bewertung kommt es also darauf an, ob bzw. zwischen welchen Beteiligten die Daten transferiert werden. Noch viel entscheidender ist allerdings die Frage nach der Qualität der verarbeiteten Daten: Das gesamte Regelungsregime das Datenschutzrechts gilt ausschließlich für personenbezogene Daten. Besteht kein Personenbezug, ist der sachliche Anwendungsbereich des BDSG schon nicht eröffnet.

II. Datenschutzrechtliche Probleme beim Cloud Computing

Im Folgenden soll überblicksartig aufgezeigt werden, warum es für Anbieter wie Nutzer von Cloud-Diensten so entscheidend sein kann, ob das Datenschutzrecht auf ihre Tätigkeiten anwendbar ist oder nicht. Das europäische Datenschutzrecht folgt dem Prinzip

3 *Baun/Kunze/Nimis/Tai,* Cloud Computing, 2009, S. 1.
4 *Cloud Standards Customer Council,* Practical Guide to Cloud Computing Version 1.0, S. 7, abrufbar unter: http://www.cloudstandardscustomer council.org/2011_Practical_Guide_to_Cloud%20Computing.pdf.
5 *Millard,* Cloud Computing Law, 2013, S. 14.
6 Siehe: http://aws.amazon.com/de/; http://www.gogrid.com/cloud-platform; http://www.microsoft.com/de-de/server-cloud/products/sql-server/default.aspx; *Millard,* Cloud Computing Law, 2013, S. 41.
7 *Cloud Standards Customer Council,* Practical Guide to Cloud Computing Version 1.0, S. 7.
8 Https://www.heroku.com/; http://success.heroku.com/cardinal_blue; *Millard,* Cloud Computing Law, 2013, S. 16.
9 *Cloud Standards Customer Council,* Practical Guide to Cloud Computing Version 1.0, S. 7; *Hon/Millard/Walden,* The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part. 1, S. 6.
10 *Bogdanov,* Sharemind: programmable secure computations with practical applications, 2013, S. 30 ff.
11 *Millard,* Cloud Computing Law, 2013, S. 15 f.
12 *Baun/Kunze/Nimis/Tai,* Cloud Computing, 2009, S. 25.
13 Bzgl. der Definitionen von Public-, Private-, Community- und Hybrid-Clouds siehe: *Mell/Grance,* The NIST Definition of Cloud Computing, S. 3, abrufbar unter: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, wobei jedoch eine einheitliche, allgemeingültige Definition dieser Begriffe noch nicht existiert.

des Verbots mit Erlaubnisvorbehalt:[14] Personenbezogene Daten dürfen gemäß Art 7 lit. a der DSRL und § 4 Abs. 1 BDSG nur dann verarbeitet werden, wenn der Betroffene (derjenige, auf den sich die Daten beziehen) dafür seine Einwilligung erteilt hat oder eine ausdrückliche gesetzliche Erlaubnisnorm besteht. Neben diesem Erfordernis bestehen weitere datenschutzrechtliche Pflichten des für die Verarbeitung Verantwortlichen, die den datenschutzkonformen Einsatz von Cloud Computing erschweren können. Die Definition des Verarbeitens im europäischen Datenschutzrecht (Art 2 lit. b DSRL bzw. § 3 Abs. 4 BDSG) ist enorm weit gefasst, sodass jede Datenübermittlung, jedes Speichern von Daten und jedes Verändern von personenbezogenen Daten in der Cloud datenschutzrechtskonform erfolgen muss.

1. Die Einwilligung

Auf den ersten Blick erscheint es nicht schwer, dem Verbot mit Erlaubnisvorbehalt gerecht zu werden, wenn personenbezogene Daten in einer Cloud verarbeitet werden sollen. Warum ist es schwierig, eine Einwilligung des Betroffenen einzuholen? Im Gegensatz zur Datenverarbeitung aufgrund gesetzlicher Erlaubnistatbestände können, wenn eine Einwilligung erfolgt ist, Daten ohne Verhältnismäßigkeitserwägungen verarbeitet werden.[15] Allein der Umstand, dass sich durch Cloud Computing eine Kostenersparnis ergibt, vermag eine solche Interessenabwägung wohl nur in Extremfällen zu Gunsten des Verantwortlichen ausfallen zu lassen.[16] Als Erlaubnistatbestand spielt die Einwilligung deshalb eine „überragende Rolle" als „zentraler Baustein" im gesamten Datenschutzrecht.[17]

Die Einwilligung muss immer durch denjenigen erfolgen, den die personenbezogenen Daten betreffen. Dies kann beim Cloud Computing der Cloud-Nutzer selbst sein, muss es aber nicht. Denkbar ist auch, dass eine Firma beispielsweise Kundendaten mittels Cloud Computings verarbeiten möchte.[18] In diesem Falle müsste vor der Datenverarbeitung von jedem Kunden die grundsätzlich schriftliche Einwilligung eingeholt werden. Für bereits bestehende Geschäftsbeziehungen kommt in der Praxis ein effektives, nachträgliches Einholen einer Einwilligung kaum in Betracht.[19] Das bloße Informieren eines Kunden über die Verarbeitung in der Cloud ist nämlich nicht für eine Einwilligung i. S. d. § 4a BDSG ausreichend, vielmehr muss der Betroffene aktiv werden und seinerseits eine – zumindest konkludente – Erklärung abgeben.[20] Dass aber tatsächlich alle Personen, deren Daten von nun an cloud-basiert verarbeitet werden sollen, tatsächlich antworten und ihre Einwilligung erteilen, ist unwahrscheinlich.

Selbst wenn der Cloud-User selbst der Betroffene der Datenverarbeitung in der Cloud ist (wie beispielsweise bei der Nutzung von „Dropbox" oder E-Mail-Diensten wie „GMail"), ist eine wirksame Einwilligung u. U. nur schwer zu erhalten. Damit die Einwilligung wirksam ist, muss der Verantwortliche seinen Informationspflichten gegenüber dem Betroffenen gemäß § 4a Abs. 1 S. 2 BDSG nachkommen („informed consent").[21] Vor der Einwilligung ist der Betroffene über Zweck und Umfang der Datenverarbeitung zu informieren, ihm sind die näheren Umstände der Datenverarbeitung deutlich zu machen. Dies umfasst auch etwaige Empfänger der Daten.[22] Darüber ausreichend zu informieren kann schwierig sein, wenn beispielsweise ein SaaS Cloud-Provider seinen Service selbst auf einer IaaS Cloud betreibt. Insbesondere bei großen Public-Clouds lässt sich u. U. vor der Verarbeitung der Daten allerdings nicht mit Sicherheit sagen, auf welchem (der möglicherweise vielen) Server ein Datum letztlich gespeichert wird und in welchem Land dieser Server stehen wird. Eine automatisierte Steuerungssoftware des Cloud-Anbieters könnte das selbstständig entscheiden und es hinge dann von der jeweiligen Inanspruchnahme der Cloud und der damit verbundenen Auslastung der physischen Ressourcen ab.[23] Dem Betroffenen muss aber klar sein, wo auf der Welt seine Daten gespeichert werden, insbesondere wenn die Speicherung außerhalb des EU/EWG Raums stattfinden soll.[24] Den Betroffenen vor seiner Einwilligung ausreichend aufzuklären, gestaltet sich beim Cloud Computing also schwierig. Ein pauschaler Hinweis auf die Nutzung von Cloud Computing ist jedenfalls nicht ausreichend. Der für den Verantwortlichen normalerweise vorteilhafte und im Datenschutzrecht zentrale Erlaubnistatbestand der Einwilligung ist im Cloud Computing nicht die optimale Rechtfertigung für die Datenverarbeitung.[25]

2. Auftragsdatenverarbeitung und Cloud Computing

Das Konzept der Auftragsdatenverarbeitung (in Art. 2 lit. d, Art. 17 Abs. 2, 3 der DSRL bzw. in § 3 Abs. 8 S. 3, § 11 BDSG geregelt) bietet die Möglichkeit, ohne Einwilligung des Betroffenen oder gesetzlichen Erlaubnistatbestand eine „Datenübermittlung" (nicht im Sinne des Datenschutzrechts, sondern im technischen Sinne) zwischen dem Verantwortlichen und dem Datenverarbeiter (dem Cloud-Provider) vorzunehmen.[26] Der tatsächliche Verarbeiter der Daten geht weisungsgebunden für den Verantwortlichen mit den Daten um. Der Auftragsdatenverarbeiter fungiert als „verlängerter Arm" und wird rechtlich als Einheit mit der Auftrag gebenden

14 Das europäische Datenschutzrecht beruht auf der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 v. 23. 11. 1995, S. 31 (DSRL), welche vollharmonisierende Wirkung hat, EuGH, Slg. 2003, I-12971 Rn. 96 – Bodil Lindquist = MMR 2004, 95 m. Anm. *Roßnagel*; *Vulin* ZD 2012, 414, 415 ff.; *EuGH*, Urt. v. 24. 11. 2011, C-468/10.

15 *Art. 29-Datenschutzgruppe,* Stellungnahme 15/2011 zur Definition von Einwilligung, WP 187, S. 7 f.; *Nägele/Jacobs,* ZUM 2010, 281, 290; *Rath/Rothe*, K&R 2013, 623, 624.

16 Vgl. *Nägele/Jacobs,* ZUM 2010, 281, 290, die eine Kostenersparnis gar nicht als Rechtfertigung anerkennen; *Spindler/Nink,* in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 28 BDSG, Rn. 6; *Hoeren,* in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 4.6, Rn. 31, der zwar auch wirtschaftliche Interessen erfasst sieht, das berechtigte Interesse aber nur bejaht, wenn ein Verzicht auf die Datenverarbeitung unzumutbar wäre; *Niemann/Paul*, K&R 2009, 444, 449, die eine Kostenersparnis durchaus als Rechtfertigungsgrund anerkennen.

17 *Spindler,* GRUR-Beilage 2014, 101, 102; *Spindler*, NJW-Beil. 2012, 98, 100; ausführlich zur Einwilligung: *Holznagel*/Sonntag, in: Roßnagel, Handbuch Datenschutzrecht, 2003, Kap. 4.8, Rn. 1 ff.

18 Ausführlich: *Brennscheidt,* Cloud Computing und Datenschutz, 2013, S. 150 ff.

19 *Rath/Rothe*, K&R 2013, 623, 624.

20 Vgl. Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4a Rn. 2; *Taeger,* in Taeger/Gabel, Kommentar zum BDSG, 2. Aufl. 2013, § 4a Rn. 41; die Möglichkeit einer konkludenten Einwilligung verneinend: *Simitis*, in: Simitis, BDSG, 7. Aufl. 2011, § 4a Rn. 78.

21 *Simitis,* in: Simitis, BDSG, § 4a Rn. 70.

22 *Nord/Manzel*, NJW 2010, 3756, 3757; *Taeger,* in: Taeger/Gabel, Kommentar zum BDSG, § 4a Rn. 30; i. E. wohl auch Gola/Schomerus, BDSG, § 4a Rn. 26, die darauf hinweisen, dass Unklarheiten bei der Einwilligung zu Lasten der verantwortlichen Stelle gehen; vgl. m. w. N. *Simitis,* in: Simitis, BDSG, § 4a Rn. 72, 77; *BITKOM*, Cloud Computing Leitfaden, S. 53, abrufbar unter http://www.bitkom.org/files/documents/BITKOM-Leitfaden-Cloud-Computing_Web.pdf.

23 *Millard,* Cloud Computing Law, 2013, S. 8 ff.; *Funke/Wittmann,* ZD 2013, 221, 222.

24 *Simitis,* in: Simitis, BDSG, § 4b Rn. 85 ff.

25 Vgl. *Art. 29-Datenschutzgruppe*, WP 187, S. 12.

26 Ausführlich dazu *Petri,* in: Simitis, BDSG, § 11; Gola/Schomerus, BDSG, § 11; *Giedke*, Cloud Computing, 2013, S. 218 ff.; *Gabel*, in: Taeger/Gabel, Kommentar zum BDSG, § 11 Rn. 2.