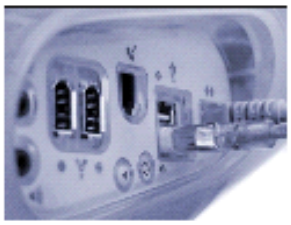
Please quote as: Gebauer, L.; Kroschwald, S. & Wicker, M. (2015): Anforderungsmuster zur Förderung der Rechtmäßigkeit und Rechtsverträglichkeit von Cloud Computing-Diensten. In: Technical Reports - Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG) , Ausgabe/Number: 3, Verlag/Publisher: Kassel University Press (ISBN: 978-3-86219-577-0). Erscheinungsjahr/Year: 2015.

Technical Reports 3

Wissenschaftliches Zentrum für Informationstechnik-Gestaltung


Lysann Gebauer, Steffen Kroschwald,
Magda Wicker

Anforderungsmuster zur Förderung der Rechtmäßigkeit und Rechtsverträglichkeit von Cloud Computing-Diensten

kassel university press

ITeG Technical Reports

Band 3

Herausgegeben vom
Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG)
an der Universität Kassel

Universität Kassel
ITeG Wissenschaftliches Zentrum
für Informationstechnik-Gestaltung
Pfannkuchstraße 1
D-34121 Kassel

Anforderungsmuster zur Förderung der Rechtmäßigkeit und Rechtsverträglichkeit von Cloud Computing-Diensten

Lysann Gebauer, Steffen Kroschwald, Magda Wicker

kassel
university
press

Fachgebietsleiter:

Prof. Dr. Jan Marco Leimeister
Fachgebiet Wirtschaftsinformatik

Prof. Dr. Alexander Roßnagel
Fachgebiet Öffentliches Recht

Autoren:

Lysann Gebauer
Steffen Kroschwald
Magda Wicker

Der Beitrag wurde im Rahmen des Projekts Value4Cloud (Förderkennzeichen: 01MD11044) erarbeitet und mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen des Technologieprogramms Trusted Cloud gefördert. Weiterführende Informationen zum Projekt Value4Cloud finden Sie unter: www.value4cloud.de.

Projektbeteiligte Value4Cloud:

Fortiss GmbH, An-Institut der TU München, Prof. Dr. Helmut Krcmar
Universität Kassel, Wissenschaftliches Zentrum ITeG, Prof. Dr. Alexander Roßnagel
Universität Kassel, Wissenschaftliches Zentrum ITeG, Prof. Dr. Jan Marco Leimeister
Universität zu Köln, Prof. Dr. Ali Sunyaev
gate (Garchinger Technologie- und Gründerzentrum GmbH)
SpaceNet AG

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar

ISBN: 978-3-86219-577-0
URN: URN: http://nbn-resolving.de/urn:nbn:de:0002-35770

Vorwort der Herausgeber

Dies ist der dritte Beitrag, der im Rahmen der Serie „ITeG Technical Reports“ erscheint. Das Wissenschaftliche Zentrum für Informationstechnik-Gestaltung (ITeG) ist eine Forschungseinrichtung der Universität Kassel. Es widmet sich der interdisziplinären Gestaltung gesellschaftlich wünschenswerter Informations- und Kommunikationstechnik aus einer soziotechnischen Perspektive. Mit der Bündelung von Kompetenzen aus Informatik, Ergonomie, Technikrecht, Wirtschaftsinformatik und Wirtschaftspsychologie ist das ITeG ein auf die nachhaltige Stärkung des Forschungsprofils der Universität Kassel ausgerichteter Forschungsverbund.

Ein Vorhaben am ITeG war das interdisziplinäre Projekt „Vaue4Cloud“, an dem die Fachgebiete Wirtschafsinformatik und Öffentliches Recht beteiligt waren. Ziel des Projektes war die Entwicklung marktunterstützender Mehrwertdienste zur Förderung von Vertrauen, Rechtsverträglichkeit, Qualität und Nutzung von Cloud Computing-Diensten für den Mittelstand.

Das Projekt „Value4Cloud“ wurde im Rahmen des Technologieprogramms „Trusted Cloud“ vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert, das die Entwicklung und Erprobung von innovativen, sicheren und rechtskonformen Cloud Computing-Diensten zum Ziel hat. Das Technologieprogramm „Trusted Cloud“ ist Teil des Aktionsprogramms Cloud Computing, das das BMWi im Oktober 2010 gemeinsam mit Partnern aus Wirtschaft und Wissenschaft gestartet hat.

Um die Akzeptanz und das Vertrauen in Cloud Computing-Dienste zu stärken, war ein Ziel der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) nicht nur die rechtlichen Voraussetzungen an Cloud Computing zu untersuchen, sondern darüber hinaus konkrete Vorschläge für eine bestmögliche rechtskonforme Gestaltung und Nutzung von Cloud Computing-Diensten zu erarbeiten. An dieses Ziel anknüpfend verfügt die Wirtschaftsinformatik über den Ansatz zur Entwicklung von Anforderungsmustern, der es ermöglicht den Entwicklungs- und Gestaltungsprozess von Informationssystemen systematisch zu unterstützen. Diese sogenannten Anforderungsmuster adressieren wiederkehrende Anforderungen oder Probleme und zeigen technische Gestaltungsmöglichkeiten zu deren Lösung im konkreten Einzelfall auf.

Das Ziel des vorliegenden Beitrages war es daher, aus den rechtlichen Ergebnissen der Rechtmäßigkeit und Rechtsverträglichkeit des Cloud Computings unter Verwendung des Ansatzes der Wirtschaftsinformatik interdisziplinär Anforderungsmuster zur Förderung rechtmäßiger und darüber hinaus rechtsverträglicher Cloud Computing-Dienste zu entwickeln.

Wir wünschen Ihnen eine spannende Lektüre.

Prof. Dr. Jan Marco Leimeister und Prof. Dr. Alexander Roßnagel

Inhalt

Kurzzusammenfassung

Die zurückhaltende Nutzung von Cloud Computing-Diensten wird in zahlreichen Forschungsarbeiten auf ein mangelndes Vertrauen der Kunden in die Technik und die Anbieter zurückgeführt. Die Vertrauenswürdigkeit von Informationssystemen und IT-Anbietern hängt unter anderem davon ab, inwiefern Systeme dem geltenden Recht entsprechen, dieses berücksichtigen oder den Nutzer bei der Einhaltung rechtlicher Vorgaben unterstützen. Durch die Gestaltung von rechtmäßigen sowie rechtsverträglichen Cloud Computing-Diensten können Anbieter somit auch zur Förderung der Nutzungsbereitschaft von Kunden beitragen.

Um Anbieter bei dieser Aufgabe zu unterstützen, werden in der Wirtschaftsinformatik sogenannte Anforderungsmuster verwendet. Ziel des Beitrages ist es, Anforderungsmuster zur rechtmäßigen und rechtsverträglichen Gestaltung von Cloud Computing-Diensten zu entwickeln. Dazu wurden gemeinsam mit juristischen Experten und Anforderungsanalysten interdisziplinäre Workshops durchgeführt. Im vorliegenden Beitrag werden 24 Anforderungsmuster zur rechtmäßigen und rechtsverträglichen Gestaltung von Cloud Computing-Diensten dargestellt und erläutert.

1 Einleitung und Motivation

Die vergangenen vier Jahre in Folge war Cloud Computing gemäß der jährlich durchgeführten BITKOM-Umfrage „*IT Trends das Jahres*“ das wichtigste Thema in der IKT-Branche (BITKOM 2010, 2011, 2012, 2013). Cloud Computing wird gehandelt als „*long-held dream of computing as a utility*“ (Armbrust et al. 2010, S. 50), der sich endlich bewahrheitet. Es bietet Unternehmen eine Möglichkeit, hohe Wartungskosten zu senken, die Auslastung und Nutzung der Hardware-Ressourcen zu optimieren, den internen Energieverbrauch zu verringern sowie agiler auf geänderte Geschäftsanforderungen zu reagieren (IDC 2011). Dennoch zeigen Studien und Umfragen, dass Cloud Computing im B2B-Bereich eher zurückhaltend genutzt wird (Golkowsky/Vehlow 2011; IDC 2011). Vor allem der Mittelstand hat noch enormen Aufholbedarf (BITKOM 2014).

Forschungsarbeiten zeigen, dass eine Zurückhaltung bei der Akzeptanz und Nutzung neuer Technologien sowohl auf einen Mangel an Vertrauen (z. B. Gefen et al. 2003; Söllner/Leimeister 2012) als auch auf die Wahrnehmung von Risiken (z. B. Featherman/Pavlou 2003; Luo et al. 2010) zurückzuführen ist. Dabei wirkt sich das Maß an entgegengebrachten Vertrauen positiv aus auf die Bereitschaft, Risiken einzugehen (z. B. Glover/Benbasat 2010). Auch im Zuge der Akzeptanz und Nutzung von Cloud Computing-Diensten bestehen Hemmnisse seitens der (potentiellen) Kunden (z. B. Armbrust et al. 2010; Ackermann et al. 2011; Gebauer et al. 2012; Marston et al. 2011), wobei die Einschätzung der Vertrauenswürdigkeit als ein erfolgskritischer Faktor bei der Auswahl des Cloud-Anbieters gesehen wird (Repschlaeger et al. 2012).

Um sowohl die Akzeptanz als auch die Nutzung von Cloud Computing zu erhöhen, sollten daher die Anbieter von Cloud Computing-Diensten die Nutzungshemmnisse der (potentiellen) Kunden bestmöglich adressieren und gleichzeitig Maßnahmen zur Förderung der Vertrauenswürdigkeit einsetzen. Die Vertrauenswürdigkeit von Informationssystemen und dessen Anbietern wird dabei durch diverse Faktoren bestimmt. Die Vertrauenswürdigkeit des Anbieters ist abhängig von dessen wahrgenommener Fähigkeit, Wohlwollen und Integrität (Söllner et al. 2013; Mayer et al. 1995). Die Einschätzung der Vertrauenswürdigkeit des Informationssystems ist abhängig von der Performanz, der Zweckklarheit und der Prozessnachvollziehbarkeit (Söllner et al. 2012a; Söllner et al. 2012b).

Ein wesentliches Hemmnis der Kunden Cloud Computing-Dienste zu nutzen, sind jedoch die bestehenden rechtlichen Unsicherheiten (Gebauer et al. 2012; Trusted Cloud AG Rechtstrahmen des Cloud Computing 2012). Dies spiegelt sich darin wieder, dass bestehende Gesetze zu Datenschutz und Datensicherheit das noch verhältnismäßig junge Cloud Computing nicht explizit regeln, oder dass für das grenzüberschreitende Cloud Computing unterschiedliche, zum Teil gegensätzliche Regelungswelten aufeinandertreffen (Kroschwald

2013a). Gerade die Frage der Zulässigkeit der Cloud-Nutzung, aber auch der Datenzugriff durch Dritte, straf- und haftungsrechtliche Fragen, etwa bei Verfügbarkeitsverlust oder Datenverlust beim Anbieterwechsel oder sogar -bankrott, sorgen für Rechtsunsicherheit auf Seiten der Nutzer. Forschungsarbeiten (für den Berufsgeheimnisschutz etwa Kroschwald/Wicker 2012a) zeigen, dass das Vertrauen in das Informationssystem und dessen Anbieter gefördert werden kann, wenn Anbieter ihre Systeme rechtskonform und darüber hinaus auch rechtsverträglich gestalten (Hoffmann 2014; Jandt 2008).

Dementsprechend sollten bereits während der Systementwicklung Anforderungen an eine rechtmäßige und rechtsverträgliche Gestaltung von Cloud Computing-Diensten berücksichtigt werden. Auch wenn dies also eine wichtige Herausforderung der Anforderungserhebung (Otto/Anton 2007; Kiyavitskaya et al. 2008) ist, so verfügen oftmals weder Entwickler von Informationssystemen noch Anforderungsanalysten über ausreichend juristisches Wissen und Kenntnisse, um eine entsprechende rechtliche Begutachtung durchzuführen. Daher sollten rechtliche Anforderungen von Juristen analysiert und in den Entwicklungsprozess eingebracht werden (Kiyavitskaya et al. 2008).

Der folgende Beitrag basiert auf der Zusammenarbeit zwischen den Rechtswissenschaften und der Systementwicklung und geht dem Ziel nach, Anforderungsmuster zur Förderung der Rechtmäßigkeit und Rechtsverträglichkeit von Cloud Computing-Diensten zu entwickeln. Zur Erreichung dieses Ziels wurden interdisziplinäre Workshops mit Rechtswissenschaftler und Anforderungsanalysten, die jeweils zusätzlich über fundierte Kenntnisse im Bereich Cloud Computing verfügen, durchgeführt. Die entwickelten Anforderungsmuster sollen Anbieter von Cloud Computing-Diensten dabei unterstützen, ihre Dienste rechtmäßig und darüber hinaus rechtsverträglich zu gestalten und anzubieten.

Nach einer Erläuterung des Vorgehens (Kapitel 2) folgt die Erklärung begrifflicher Grundlagen (Kapitel 3). Anschließend werden die Ergebnisse, 24 Anforderungsmuster zur Förderung der Rechtmäßigkeit und Rechtsverträglichkeit von Cloud Computing-Diensten, dargestellt und erläutert (Kapitel 4). Da der Beitrag keinen Anspruch auf die Vollständigkeit sämtlicher Anforderungsmuster erhebt, soll mit Hilfe eines Ausblicks auf zukünftigen Forschungsbedarf ausreichend Raum für Diskussionen bleiben (Kapitel 5).

2 Vorgehen

Um Anforderungsmuster zur Förderung der Rechtmäßigkeit und Rechtsverträglichkeit von Cloud Computing-Diensten zu entwickeln, wurden zwei interdisziplinäre Workshops durchgeführt. An den Workshops haben drei Wissenschaftler aus der Wirtschaftsinformatik und zwei Rechtswissenschaftler teilgenommen, die jeweils auch über umfangreiche Kenntnisse zum Thema Cloud Computing verfügen.

Der interdisziplinäre Diskurs wurde unter Verwendung von Collaboration Engineering-Methoden (CE-Methoden) ausgestaltet (Leimeister 2014). Collaboration Engineering ist ein systematischer Ansatz zur Entwicklung und Umsetzung von Zusammenarbeitsprozessen, um hochwertige, wiederkehrende Aufgaben zu erfüllen. Ziel ist insbesondere, die Effizienz und Effektivität der an der Zusammenarbeit beteiligten Akteure zu verbessern sowie qualitativ hochwertige Ergebnisse zu erzielen (Leimeister 2014). Kombiniert mit dem Einsatz von Informationstechnologien eröffnet die Anwendung von CE-Methoden neue und innovative Möglichkeiten, Zusammenarbeitsprozesse in heterogenen Teams auszugestalten (Leimeister 2014). Heterogene Teams bestehen meist aus Teilnehmern unterschiedlicher fachlicher Disziplinen und kennzeichnen sich durch einen breit gefächerten Wissenshintergrund. Hoffmann et al. (2013) zeigen, dass es für die erfolgreiche Systementwicklung von Bedeutung ist, ein gegenseitiges und gemeinsames Begriffsverständnis zwischen den Mitgliedern einer solchen Arbeitsgruppe zu schaffen. Die Herstellung eines gemeinsamen Verständnisses (Engl.: *shared understanding*) stärkt dabei die Leistungsfähigkeit solcher heterogenen Gruppen (Bittner/Leimeister 2014, 2013; Hoffmann et al. 2013).

Im ersten Workshop wurden zunächst die begrifflichen Grundlagen als auch das Anliegen sowie der Zweck der Zusammenarbeit besprochen, um eine gemeinsame Arbeitsgrundlage für die folgende interdisziplinäre Zusammenarbeit zu schaffen. Anschließend wurden bereits in der Forschung existierende Anforderungsmuster zur rechtsverträglichen Gestaltung von soziotechnischen Systemen (Hoffmann 2014) vorgestellt, um aufbauend darauf Anforderungsmuster zur Rechtmäßigkeit und Rechtsverträglichkeit von Cloud Computing-Diensten zu entwickeln. Im dritten Schritt wurden diese Muster mit Hilfe der Anwendung *Thinktank*[1], einem Gruppenprozesse-Unterstützungssystem, kommentiert. Schließlich wurde aufbauend auf den im dritten Schritt erarbeiteten Kommentaren die Übertragbarkeit dieser Muster auf cloud-basierte Dienste in der Gruppe diskutiert. Dieser interdisziplinäre Austausch hat zu dem Ergebnis geführt, dass die Inhalte als auch die Kategorien der zu Grunde gelegten Anforderungsmuster an die Besonderheiten von Cloud Computing-Diensten angepasst wurden.

Im Nachgang an den ersten Workshop wurden die Ergebnisse in Form von adaptierten Anforderungsmustern schriftlich festgehalten. Diese Übersicht diente dann als Ausgangslage für den zweiten Workshop, in dem die erarbeiteten Anforderungsmuster zur Förderung der Rechtmäßigkeit und Rechtsverträglichkeit von allen Teilnehmern erneut kritisch geprüft und gegebenenfalls überarbeitet wurden. Zudem wurden weitere Merkmale diskutiert. Nach dem zweiten Workshop war eine ausreichende Grundlage geschaffen wurden, sodass die erarbeiteten Ergebnisse zum kritischen Überprüfen an die jeweiligen Fachexperten weiter gegebenen wurden und somit noch einige schriftliche Überarbeitungs- und Abstimmungsrunden erfuhren.

[1] www.thinktank.net

3 Begriffliche Grundlagen

Vor dem Hintergrund des Zwecks der interdisziplinären Zusammenarbeit wurden folgende Begriffe vorab definiert: Cloud Computing, Anforderungen, Anforderungsmuster, Rechtmäßigkeit, Rechtsverträglichkeit und rechtsverträgliche Technikgestaltung (Hammer et al. 1993; Roßnagel 2008, 1997). Ziel der anfänglichen Begriffsdefinition war es, ein gemeinsames Verständnis zwischen den Experten unterschiedlicher wissenschaftlicher Disziplinen und somit einen gemeinsamen Begriffsapparat zu schaffen.

3.1 Cloud Computing

Entsprechend der wirtschaftswissenschaftlichen Dienstleistungstypologie nach Leimeister (2012) ist Cloud Computing eine elektronische Dienstleistung, die sich durch einen hohen IT-Einsatz auszeichnet. Diese Dienstleistung kann dabei sowohl als reine IT-Dienstleistung ohne Personaleinsatz als auch als IT-unterstützte Dienstleistung angeboten werden, bei der neben der Technik auch Personal eingesetzt wird, um eine Leistung zu erbringen. Diese beiden Typen cloud-basierter Dienstleistungen werden im Nachfolgenden stets als „Cloud Computing-Dienste“ zusammengefasst, da es im Einzelfall schwer festzustellen ist, ob der Cloud-Anbieter für die Bereitstellung neben technischen Ressourcen auch Personal einsetzt.

Im Rahmen des Workshops wurde Cloud Computing wie folgt definiert und somit eingegrenzt:

> „*Cloud Computing ist ein auf Virtualisierung basierendes IT-Bereitstellungsmodell, bei dem Ressourcen sowohl in Form von Infrastruktur als auch Anwendungen und Daten als verteilter Dienst über das Internet durch einen oder mehrere Leistungserbringer bereitgestellt werden. Diese Dienste sind nach Bedarf flexibel skalierbar und können verbrauchsabhängig abgerechnet werden.*“ (Böhm et al. 2009, S. 8).

Ausschlaggebend für die Qualifizierung einer IT-Dienstleistung als Cloud Computing-Dienst ist demnach nicht die Form der Leistungserbringung (z. B. die technische und organisatorische Umsetzung der Leistungserstellung), sondern die Form der Bereitstellung der IT-Dienstleistung.

3.2 Rechtmäßigkeit und Rechtsverträglichkeit

Unter Rechtmäßigkeit wird die Einhaltung gesetzlicher Vorschriften verstanden. Anforderungsmuster zur Einhaltung der Rechtmäßigkeit umfassen „Muss“-Anforderungen, ohne deren Einhaltung ein Rechtsverstoß vorläge, der Sanktionen beim Nutzer oder Anbieter auslösen würde.

Unter Rechtsverträglichkeit wird darüber hinausgehend die optimale Berücksichtigung sozialer Regelungsziele verstanden, d.h. Anforderungsmuster zur Schaffung von Rechtsverträglichkeit umfassen „Kann"-Anforderungen, die die rechtlichen Vorgaben über das Mindestmaß der Rechtmäßigkeit hinaus erfüllen. Das Konzept der Rechtsverträglichkeit geht somit über das Konzept der Rechtmäßigkeit hinaus, indem es nicht nur eine minimale, sondern eine optimale Umsetzung rechtlicher Regelungsansätze angestrebt.

Im Rahmen der rechtmäßigen und rechtsverträglichen Technikgestaltung werden zunächst Rechtsvorschriften ausgewertet, die unmittelbare oder mittelbare rechtliche Anforderungen in Bezug auf die zu gestaltende Technik enthalten (z. B. Signaturgesetz, Datenschutzgesetz). Durch die rechtmäßige Technikgestaltung wird damit sichergestellt, dass das Angebot und die Nutzung des Cloud Computing-Dienstes den Mindestanforderungen aus dem geltenden Recht entsprechen. Eine rechtsverträgliche Technikgestaltung hingegen bewirkt, dass die Nutzung und das Anbieten von technischen Applikationen das Ziel der rechtlichen Standards optimal umsetzt und deren Zweck fördert (Hammer et al. 1993; Roßnagel 1997, 2008). Zweck und Ziel gesetzlicher Regelungen ergeben sich dabei häufig nicht aus den jeweiligen Fachgesetzen, sondern vielmehr aus verfassungsrechtlichen Vorgaben und Schutzgütern.

3.3 Anforderungen und Anforderungsmuster

Der Standard IEEE 610.12-1990 (IEEE 1990) definiert den Begriff „Anforderung" (Engl.: *Requirement*) wie folgt:

> „*Eine Anforderung ist:*
>
> *(1) Eine Bedingung oder Eigenschaft, die ein System oder eine Person benötigt, um ein Problem zu lösen oder ein Ziel zu erreichen.*
>
> *(2) Eine Bedingung oder Eigenschaft, die ein System oder eine Systemkomponente aufweisen muss, um einen Vertrag zu erfüllen oder einem Standard, einer Spezifikation oder einem anderen formell aufgelegten Dokument zu genügen.*
>
> (3) *Eine dokumentierte Repräsentation einer Bedingung oder Eigenschaft wie in (1) oder (2) definiert.*" (Pohl 2007, S. 13).

Anforderungen an Cloud Computing-Dienste sind folglich unter anderem die technische und organisatorischen Leistungsmerkmale des (zu entwickelnden) Dienstes oder des Anbieters. Jede Anforderung sollte je nur eine Bedingung oder Eigenschaft beinhalten, die vom cloud-basierten Dienst zu erfüllen ist. Die konkrete Umsetzung, also etwa eine bestimmte technische Lösung im Rahmen des cloud-basierten Dienstes, ist dabei jedoch nicht Teil einer Anforderung. Somit beschreibt eine Anforderung den Problemraum, nicht aber den Lösungsraum.

Anforderungsmuster sind grafisch-tabellarische Vorlagen, die den Anforderungsanalysten Unterstützung für wiederkehrende Anforderungen bieten. Die Anforderungsmuster beinhalten Vorlagen für die Anforderungsbeschreibung und andere relevante Informationen in tabellarischer Form (Durán Toro et al. 1999).

Die im Rahmen der Workshops entwickelten Anforderungsmuster bestehen aus folgenden Kategorien, wobei die Kategorien „Perspektiven“ und „Datenarten“ die Folge der Besonderheiten im Cloud Computing-Umfeld darstellen:

- **Name:** Jedes Anforderungsmuster wird durch einen eindeutigen Namen benannt. Dieser ist so zu wählen, dass er das Anforderungsmuster prägnant bezeichnet.
- **Ziel:** In jedem Anforderungsmuster wird ein Ziel benannt, welches die Applikation erfüllt, wenn die Anforderung umgesetzt wurde. Das Ziel ist entsprechend der allgemeinen Mustereigenschaften der Problemteil und dient bei der Anwendung als Entscheidungshilfe für die Auswahl relevanter Anforderungsmuster für eine konkrete Applikation.
- **Standardisierte Anforderung:** Die standardisierte Anforderung entspricht einer Anforderung, die direkt in eine Anforderungsspezifikation übernommen werden kann. Sie ist so formuliert, dass sie die Erreichung des Ziels einfordert.
- **Hinweise:** Wenn die Anforderung spezielle Aktivitäten von Experten notwendig macht, so werden diese in Form von Handlungsimplikationen als Hinweise angegeben.
- **Perspektiven:** Die Analyse der rechtlichen Lage im Cloud Computing-Umfeld ergab, dass es von wesentlicher Bedeutung ist, verschiedene rechtliche Perspektiven zu unterscheiden. Zum einen ist es wichtig zu unterscheiden, ob die rechtliche Verantwortlichkeit für einen Vorgang vom Cloud-Anbieter oder vom Cloud-Nutzer zu tragen ist (Kroschwald 2013a, S. 388 ff.). Zum anderen ist es wichtig zu unterscheiden, ob das Anforderungsmuster zur Einhaltung von Rechtmäßigkeit oder zur Schaffung von Rechtsverträglichkeit beiträgt. Da die Anforderungsmuster jedoch nur an den Cloud Computing-Anbieter adressiert sind und dieser dabei unterstützt werden soll, die Vertrauenswürdigkeit seines Dienstes durch eine rechtmäßige und rechtsverträgliche Gestaltung zu fördern, wird auch die rechtliche Verantwortlichkeit des Nutzers nur aus der Perspektive des Cloud-Anbieters betrachtet. Das bedeutet, die Anforderungsmuster beschreiben Anforderungen an den Anbieter, die dieser umsetzen kann, um die Nutzer bei der rechtmäßigen als auch der rechtsverträglichen Nutzung zu unterstützen. Erfüllt ein Cloud-Anbieter die hierunter gennannten Anforderungen und unterstützt den Cloud Computing-Nutzer in einer rechtmäßigen und rechtsverträglichen Nutzung, obgleich er rechtlich dazu nicht verpflichtet wäre, trägt er folglich zu einer insgesamt rechtsverträglicheren Gestaltung des Cloud Computing-Dienstes bei.

  Daraus ergeben sich folgende Unterteilungen:

  - **Rechtmäßigkeit auf Seiten des Anbieters:** Diese Kategorie umfasst Anforderungsmuster, die dazu dienen, das rechtmäßige Verhalten der Cloud-Anbieter zu

unterstützen und sich damit die Frage zu stellen: „*Was muss der Cloud-Anbieter tun, damit das Anbieten des Dienstes rechtmäßig ist?*“. Das Ergebnis stellen Anforderungen an den Cloud-Anbieter dar, die dieser erfüllen sollte, damit das Anbieten des Cloud Computing-Dienstes für ihn rechtmäßig ist.

- **Rechtmäßigkeit auf Seiten des Nutzers:** Diese Kategorie umfasst Anforderungsmuster, die dazu dienen, das rechtmäßige Verhalten der Cloud-Nutzer durch Maßnahmen des Anbieters zu unterstützen und sich damit die Frage zu stellen: „*Was kann der Cloud-Anbieter tun, damit sich die Cloud-Nutzer bei der Nutzung des Dienstes rechtmäßig verhalten und dementsprechend nicht gegen geltendes Recht verstoßen?*“. Als Resultat ergeben sich Anforderungen an den Cloud-Anbieter, die dieser adressieren kann, damit sich der Kunde bei der Nutzung der Cloud Computing-Applikation rechtmäßig verhalten kann. Eine Umsetzung dieser Anforderungen würde somit die Rechtsverträglichkeit des Cloud Computing-Dienstes insgesamt fördern.
- **Rechtsverträglichkeit auf Seiten des Nutzers:** Diese Kategorie umfasst Anforderungsmuster, die dazu dienen, über die Rechtmäßigkeit hinaus eine rechtsverträgliche Nutzung der Cloud Computing-Nutzer durch Maßnahmen des Cloud-Anbieters zu unterstützen und sich damit die Frage zu stellen: „*Was kann der Cloud-Anbieter tun, damit sich die Cloud-Nutzer bei der Nutzung des Dienstes rechtsverträglicher verhalten?*“. Im Ergebnis ergeben sich Anforderungen an den Cloud-Anbieter, die dieser adressieren kann, damit sich der Kunde bei der Nutzung der Cloud Computing-Applikation über die Vorgaben seiner Rechtmäßigkeit hinaus „rechtsverträglich“ verhalten kann. Eine Umsetzung dieser Anforderungen würde somit ebenfalls die Rechtsverträglichkeit des Cloud Computing-Dienstes insgesamt fördern.

- **Datenart:** Aufgrund der Diversität von cloud-basierten Diensten und der damit variierenden Art und Weise hinsichtlich der Datenverarbeitung, müssen verschiedene Datenarten unterschieden werden. In Abhängigkeit von der Datenart (Boos et al. 2013) können sich unterschiedliche rechtliche Anforderungen ergeben. Folgende Datenarten müssen im Cloud Computing-Umfeld unterschieden werden:
  - **Bestandsdaten (im Sinne des TMG):** Bestandsdaten im Sinne des Telemediengesetzes (TMG) sind Daten, die der Cloud-Anbieter benötigt, um dem Cloud-Nutzer die cloud-basierte Applikation zur Verfügung zu stellen (z. B. Daten im Zuge des Vertragsabschlusses wie Name, Adresse, Zahlungsdaten, etc.).
  - **Nutzungsdaten:** Nutzungsdaten sind Daten, die der Cloud-Anbieter im Rahmen der Dienstbereitstellung, -erbringung oder zur Abrechnung benötigt (z. B. Datumsstempel, Nutzungszeiten, Nutzungsdauer, GPS-Daten, IP-Adressen, etc.).
  - **Inhaltsdaten:** Inhaltsdaten sind Daten, die den Gegenstand der cloud-basierten Dienstnutzung betreffen – also Daten, die der Cloud-Nutzer in eine Cloud zum

Zwecke der Speicherung oder Verarbeitung an den Cloud-Anbieter überträgt oder die über die cloud-basierte Applikation verwaltet werden (z. B. Inhalte, auch solche über betroffene Dritte).

Aufbauend auf der Grundlage wurden nun die Anforderungsmuster zur Förderung der rechtmäßigen und rechtsverträglichen Gestaltung von Cloud Computing-Diensten erarbeitet.

4 Ergebnisse

Insgesamt wurden 24 Anforderungsmuster zur Förderung der Rechtmäßigkeit und der Rechtsverträglichkeit von Cloud Computing-Diensten entwickelt. Zur Umsetzung dieser Anforderungsmuster ist stets der Cloud-Anbieter adressiert, um den Cloud Computing-Dienst rechtmäßiger als auch rechtsverträglicher gestalten zu können. Dabei werden drei verschiedene Perspektiven eingenommen:

Zum Ersten die Pflichten des Cloud-Anbieters, das heißt, welche Anforderungen sollte der Cloud Computing-Dienst erfüllen, sodass das Anbieten dieses Dienstes rechtmäßig ist (Kapitel 4.1 „Anforderungsmuster zur Förderung der Rechtmäßigkeit des Cloud-Anbieters“). Diese Anforderungsmuster adressieren daher die Rechtmäßigkeit der Cloud-Anbieter.

Zum Zweiten wird die Perspektive eingenommen, welchen rechtlichen Pflichten die Cloud-Nutzer grundsätzlich unterliegen. Da aber im Fokus dieser Arbeit Anforderungen an den Cloud-Anbieter stehen, zeigen die entwickelten Anforderungsmuster auf, wie der Cloud-Anbieter die Cloud-Nutzer dabei unterstützen kann, dass diese sich rechtmäßig verhalten (Kapitel 4.2.1 „Anforderungsmuster zur Förderung der rechtmäßigen Nutzung des Cloud Computing-Angebots“).

Im Zuge der dritten Perspektive wird darüber hinaus betrachtet, welchen Anforderungen der Cloud-Anbieter nachkommen könnte, sodass sich die Cloud-Nutzer noch rechtsverträglicher verhalten (Kapitel 4.2.2 „Anforderungsmuster zur Förderung der rechtsverträglichen Nutzung des Cloud Computing-Angebots“).

Da es sich bei den Anforderungen zur Förderung der Rechtmäßigkeit und der Rechtsverträglichkeit der Cloud-Nutzer nicht um die Pflichten des Cloud-Anbieters handelt, führt eine Umsetzung dieser beiden zuletzt genannten Anforderungen zur Förderung der Rechtsverträglichkeit des Cloud Computing-Angebots insgesamt.

4.1 Anforderungsmuster zur Förderung der Rechtmäßigkeit des Cloud-Anbieters

4.1.1 Keine Kenntnisnahme der Daten durch den Cloud-Anbieter außerhalb der Weisung des Cloud-Nutzers

Der Cloud-Anbieter ist datenschutzrechtlich in der Regel Auftragnehmer im Sinne des § 11 Bundesdatenschutzgesetz (BDSG). In dieser Funktion ist er weisungsabhängig und hat keine eigene Verfügungsmacht über die Daten (Inhaltsdaten). Weist der Cloud-Nutzer ihn an, persönlich keine Kenntnis von den Daten zu nehmen, so verstößt der Cloud-Anbieter mit Kenntnisnahme nicht nur gegen den datenschutzrechtlichen Auftrag, sondern wird für diesen Datenumgang selbst verantwortliche Stelle im Sinne des Datenschutzgesetzes. Für einen solchen eigenständigen Datenumgang verfügt der Cloud-Anbieter aber regelmäßig über keine gesetzliche Erlaubnis oder Einwilligung des Betroffenen (Kroschwald/Wicker 2014).

Darüber hinaus kann die unbefugte Kenntnisnahme der Daten auch den strafrechtlichen Tatbestand des Ausspähens von Daten gemäß § 202a Strafgesetzbuch (StGB) erfüllen.

Anforderungsmuster: Keine Kenntnisnahme der Daten durch den Cloud-Anbieter ohne Befugnis	
Ziel:	Der Cloud-Anbieter hat keine Möglichkeit, unberechtigt Kenntnis vom Inhalt der Daten des Cloud-Nutzers zu nehmen.
Standardisierte Anforderung:	Der Cloud-Anbieter hat keine Möglichkeit des Zugriffs auf unverschlüsselte Daten.
Hinweis:	Eine Ausnahme liegt vor, wenn der der Cloud-Anbieter über eine Einwilligung des Cloud-Nutzers zur Kenntnisnahme verfügt.
Perspektive:	Anbieter und Rechtmäßigkeit
Datenart:	Inhaltsdaten

4.1.2 Bestands- und Nutzungsdaten enthalten keine personenbezogenen Daten

Cloud-Dienste sind regelmäßig Telemediendienste im Sinne des Telemediengesetzes (TMG). Bei der Buchung eines Cloud-Dienstes werden vom Cloud-Anbieter häufig Bestandsdaten (im Sinne des TMG) wie Name und Anschrift abgefragt und später während der Nutzung weitere Nutzungsdaten wie die IP-Adresse erhoben (Boos et al. 2013). Nach § 13 Abs. 6 TMG hat der Dienste-Anbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren. Soweit Bestands- und / oder Nutzungsdaten folglich nicht zwingend als personenbezogene Daten erforderlich sind und die Dienstbereitstellung und Erbringung einen Personenbezug nicht erfordert (etwa bei kostenfreien Diensten, die nicht abgerechnet werden müssen oder solchen Diensten, die auch anonym bezahlt werden können), sind Daten nur anonym oder pseudonym zu erheben, zu verarbeiten und zu nutzen.

Anforderungsmuster: Bestands- und Nutzungsdaten enthalten keine personenbezogenen Daten	
Ziel:	Der Benutzer kann die Cloud-Applikation pseudonym nutzen.
Standardisierte Anforderung:	Die Cloud-Applikation soll keine Nutzungs- und Bestandsdaten erheben und verarbeiten, soweit diese nicht zwingend erforderlich sind.
Hinweis:	Die Cloud-Applikation erlaubt deren Anwendung durch den Cloud-Nutzer mit einem minimalen Maß an Nutzungs- und Bestandsdaten. Falls Nutzungs- und Bestandsdaten erforderlich sind, dann sollten diese pseudonymisiert verarbeitet werden.
Perspektive:	Anbieter und Rechtmäßigkeit
Datenart:	Bestandsdaten und Nutzungsdaten

4.1.3 Schutz der Bestands- und Nutzungsdaten vor Zugriffen unbefugter Dritter

Anders als bei Inhaltsdaten ist es erforderlich, dass der Cloud-Anbieter Bestands- und Nutzungsdaten zur Kenntnis nimmt. Nur so kann er seinen Dienst erbringen und abrechnen – andernfalls wäre eine Verarbeitung von Bestands- und Nutzungsdaten ohnehin nicht zulässig.

Eine Übermittlung von Bestands- und Nutzungsdaten an Dritte ist, mit Ausnahme der strafprozessualen Bestandsdatenauskunft (Wicker 2014) im Telemediengesetz grundsätzlich nicht vorgesehen. Der Cloud-Anbieter muss vielmehr, die bei ihm gespeicherten Bestands- und Nutzungsdaten des Cloud-Nutzers vor dem Zugriff unbefugter Dritter schützen. Technische und organisatorische Maßnahmen hierfür ergeben sich beispielsweise aus § 13 Abs. 4 ff. TMG sowie aus § 9 BDSG und der Anlage zu § 9 BDSG.

Anforderungsmuster: Schutz der Bestands- und Nutzungsdaten vor Zugriffen unbefugter Dritter	
Ziel:	Schutz der Bestands- und Nutzungsdaten vor Zugriffen von unbefugten Dritten.
Standardisierte Anforderung:	Die Cloud-Applikation soll sicherstellen, dass niemand unbefugt einen Bezug zwischen den Benutzern und ihren Bestands- und Nutzungsdaten herstellen kann.
Hinweis:	Als unbefugte Dritte gelten auch die Mitarbeiter des Cloud-Anbieters.
Perspektive:	Anbieter und Rechtmäßigkeit
Datenart:	Bestandsdaten und Nutzungsdaten

4.1.4 Schutz der Inhaltsdaten vor Zugriffen unbefugter Dritter

Der Cloud-Anbieter ist verpflichtet, für Datensicherheit zu sorgen. Er muss technisch sicherstellen, dass die Daten, insbesondere soweit sie betroffene Dritte betreffen, nicht durch ihn oder Dritte zur Kenntnis genommen werden können.

Anforderungsmuster: Schutz der Inhaltsdaten vor Zugriffen unbefugter Dritter	
Ziel:	Der Cloud-Anbieter schützt die gespeicherten Daten vor Kenntnisnahme durch Dritte.
Standardisierte Anforderung:	Der Cloud-Anbieter verhindert die Kenntnisnahme der Daten durch unbefugte Dritte.
Hinweis:	Der Cloud-Anbieter handelt wie ein verlängerter Arm des Cloud-Nutzers.
Perspektive:	Anbieter und Rechtmäßigkeit
Datenart:	Inhaltsdaten

4.1.5 Einhaltung der Weisungen des Cloud-Nutzers

Als Auftragnehmer einer Auftragsdatenverarbeitung ist der Cloud-Anbieter gemäß § 11 BDSG dem Cloud-Nutzer gegenüber weisungsabhängig. Er verfügt über keine eigene Verfügungsmacht über die Daten und hat seine Datenverarbeitung sowie die technischen und organisatorischen Maßnahmen an den Vorgaben des Cloud-Nutzers aus dem Auftragsdatenverarbeitungsvertrag sowie an den regelmäßigen Einzelweisungen auszurichten (siehe hierzu Kroschwald 2013a, S. 388 ff.). Er ist nicht befugt, die Daten zu eigenen Zwecken zu verarbeiten, weiter zu übermitteln oder ohne Grund einzusehen.

Anforderungsmuster: Einhaltung der Weisungen des Auftragnehmers	
Ziel:	Der Cloud-Anbieter ist an die Weisung und Kontrolle des Cloud-Nutzers gebunden.
Standardisierte Anforderung:	Der Cloud-Anbieter verarbeitet Daten ausschließlich nach den Vorgaben des Cloud-Nutzers.
Hinweis:	Der Cloud-Anbieter handelt wie ein verlängerter Arm des Cloud-Nutzers.
Perspektive:	Anbieter und Rechtmäßigkeit
Datenart:	Bestandsdaten, Nutzungsdaten und Inhaltsdaten

4.1.6 Einsichtnahme in gespeicherte Daten

Der Cloud-Anbieter als Auftragnehmer ist nach § 11 Abs. 2 Satz 2 Nr. 7 BDSG zur Duldung und Mitwirkung zu verpflichten. Hierzu gehört auch die Transparenz gegenüber dem Cloud-Nutzer als Auftraggeber (Zu den Pflichten des Auftraggebers Petri, in: Simitis 2014 § 11 BDSG Rn. 85 ff.).

Soweit der Cloud-Anbieter darüber hinaus selbst als verantwortliche Stelle Daten erhebt und verarbeitet, ist er im Übrigen dem Cloud-Nutzer als Betroffenen zur Benachrichtigung und Auskunft nach § 4 Abs. 3 BDSG sowie §§ 34 und 35 BDSG verpflichtet (Scholz/Sokol, in: Simitis 2014 § 4 BDSG Rn. 39 ff.).

Anforderungsmuster: Einsichtnahme in gespeicherte Daten	
Ziel:	Der Cloud-Anbieter ist verpflichtet dem Cloud-Nutzer die Einsichtnahme in die gespeicherten personenbezogenen Daten zu ermöglichen.
Standardisierte Anforderung:	Der Cloud-Anbieter ist verpflichtet dem Cloud-Nutzer bei Bedarf Auskunft über die gespeicherten personenbezogenen Daten zu geben.
Hinweis:	Auch über das gesetzlich geforderte Maß könnte dem Nutzer zum Zwecke der Rechtsverträglichkeit eine Funktion angeboten werden, mit der er zu jeder Zeit und ohne Anfrage die durch den Anbieter gespeicherten personenbezogenen Daten abrufen kann.
Perspektive:	Anbieter und Rechtmäßigkeit
Datenart:	Bestandsdaten und Nutzungsdaten

4.1.7 Änderung personenbezogener Nutzerdaten

Der Cloud-Anbieter ist gemäß § 35 Abs. 1 Satz 1 BDSG verpflichtet, personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Um die Richtigkeit seiner personenbezogenen Daten festzustellen, ist der Cloud-Nutzer zunächst darauf angewiesen, die beim Cloud-Anbieter gespeicherten Daten in Erfahrung zu bringen. Erst in einem zweiten Schritt könnte ein Berichtigungsverlangen an den Cloud-Anbieter gerichtet werden.

Soweit allerdings der Cloud-Nutzer die Möglichkeit erhält, seine gespeicherten personenbezogen Daten einzusehen und selbst notwendige Veränderungen vorzunehmen, wird sowohl die Notwendigkeit des Handelns des Cloud-Anbieters reduziert als auch das Zuverlässigkeit einer zügigen Datenkorrektur ermöglicht.

Anforderungsmuster: Änderung personenbezogener Nutzerdaten ermöglichen	
Ziel:	Der Cloud-Nutzer kann seine gespeicherten personenbezogenen Daten ändern.
Standardisierte Anforderung:	Die Cloud-Applikation soll es den Cloud-Nutzern ermöglichen, ihre gespeicherten personenbezogenen Daten zu ändern.
Hinweis:	1) Die verantwortliche Stelle muss die Möglichkeit haben, die Änderungen sicherzustellen. 2) Löschen ist eine Form von Ändern.
Perspektive:	Anbieter und Rechtmäßigkeit
Datenart:	Bestandsdaten und Nutzungsdaten

4.1.8 Löschung personenbezogener Nutzerdaten durch den Nutzer

§ 35 Abs. 2 Satz 1 BDSG verlangt, dass personenbezogene Daten unter bestimmten Voraussetzungen zu löschen sind. Entsprechende Gründe sind nach § 35 Abs. 2 Satz 2 BDSG beispielsweise die unzulässige Speicherung der betroffenen Daten, das Vorliegen von besonders sensitiven Daten, die Erfüllung des Zwecks, der eine Speicherung gerechtfertigt hat, sowie nach Ablauf einer bestimmten Zeitspanne in bestimmten Fällen.

Der Anspruch auf Löschung kann dabei auch mit der Möglichkeit des Cloud-Anbieters hinsichtlich der Dienstbereitstellung kollidieren, soweit die Dienstbereitstellung nach der Löschung nicht mehr möglich ist.

Anforderungsmuster: Löschung der personenbezogenen Daten durch den Nutzer ermöglichen	
Ziel:	Der Cloud-Nutzer kann seine gespeicherten personenbezogenen Daten löschen.
Standardisierte Anforderung:	Die Cloud-Applikation soll den Cloud-Nutzern ermöglichen, ihre gespeicherten personenbezogenen Daten zu löschen.
Hinweis:	Der Cloud-Nutzer muss die Möglichkeit haben, die physische Löschung sicherzustellen.
Perspektive:	Anbieter und Rechtmäßigkeit
Datenart:	Bestandsdaten und Nutzungsdaten

4.1.9 Löschung nicht mehr benötigter personenbezogener Nutzerdaten

§ 35 Abs. 2 Satz 1 BDSG verlangt, dass personenbezogene Daten unter bestimmten Voraussetzungen zu löschen sind. Insbesondere die Löschung von Daten, deren Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, ist gemäß § 35 Abs. 2 Satz 1 Nr. 2 BDSG vorgeschrieben (hierzu Dix, in: Simitis 2014 § 35 BDSG Rn. 19 ff.).

In solchen Konstellationen kann der Cloud-Anbieter die Löschung selbst viel effizienter umsetzen, als dies der Cloud-Nutzer kann. Der Cloud-Nutzer kann beispielsweise selbst nicht ohne weiteres beurteilen, inwieweit sich der Zweck erledigt hat. Eine automatische Löschung ist deshalb zu bevorzugen.

Anforderungsmuster: Löschung nicht mehr benötigter personenbezogener Nutzerdaten	
Ziel:	Die Cloud-Applikation löscht erhobene, personenbezogene Nutzerdaten, wenn diese nicht mehr benötigt werden.
Standardisierte Anforderung:	Die Cloud-Applikation soll personenbezogene Daten löschen, die für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden.
Hinweis:	1) Nur personenbezogene Daten aufbewahren, die für die Funktionalität der Applikation wieder benötigt werden. 2) Sicherstellung einer echten Löschung (Überschreibung). 3) Aufbewahrungspflichten für Daten beachten. Beispiel: Im Falle einer Adressänderung, stellt der Cloud-Anbieter sicher, dass die alte Adresse vollständig gelöscht wird, sobald diese nicht mehr benötigt wird.
Perspektive:	Anbieter und Rechtmäßigkeit
Datenart:	Bestandsdaten und Nutzungsdaten

4.2 Anforderungsmuster zur Förderung der Rechtsverträglichkeit des Cloud-Anbieters

4.2.1 Anforderungsmuster zur Förderung der rechtmäßigen Nutzung des Cloud Computing-Angebots

4.2.1.1 Vertrag zur Auftragsdatenverarbeitung anbieten

Nach § 11 Abs. 2 Satz 2 BDSG ist der Cloud-Nutzer als Auftraggeber verpflichtet, dem Cloud-Anbieter gegenüber einen schriftlichen Auftrag über die Auftragsdatenverarbeitung zu erteilen. Nach dem gesetzlichen Leitbild geht die Initiative hierzu vom Cloud-Nutzer aus, der Cloud-Anbieter kann den Cloud-Nutzer bei der Erfüllung seiner Pflicht zur Erteilung des Auftrags nach den Vorgaben des § 11 Abs. 2 Satz 2 BDSG auch unterstützen, indem er selbst einen Vertragstext vorformuliert und dem Cloud-Nutzer zur Vereinbarung anbietet.

Anforderungsmuster: Vertrag zur Auftragsdatenverarbeitung anbieten	
Ziel:	Sicherstellung, dass der Cloud-Nutzer seinen gesetzlichen Pflichten nachkommt. Der Cloud-Nutzer ist in der Pflicht mit dem Cloud-Anbieter einen ADV abzuschließen.
Standardisierte Anforderung:	Die Cloud-Applikation soll den Cloud-Nutzer auffordern, einen ADV mit dem Cloud-Anbieter abzuschließen.
Hinweis:	Werden die Verträge für eine Vielzahl von Fällen vorformuliert und einseitig gestellt, sind die Vorschriften zu Allgemeinen Geschäftsbedingungen zu beachten.
Perspektive:	Nutzer und Rechtmäßigkeit
Datenart:	Inhaltsdaten

4.2.1.2 Verarbeitung der Inhaltsdaten ausschließlich im gleichen Rechtsraum wie der Cloud-Nutzer

Eine Auftragsdatenverarbeitung ist nach § 3 Abs. 8 BDSG ausschließlich innerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) zulässig. Als verantwortliche Stelle sollte der Cloud-Nutzer als Auftraggeber bereits im Auftragsdatenverarbeitungsvertrag sowie durch Weisungen und vor allem durch Kontrollen sicherstellen, dass die Daten ausschließlich von europäischen Anbietern innerhalb der EU oder des EWR gespeichert und verarbeitet werden (hierzu Maier 2014, S. 58 ff.). Der Cloud-Anbieter kann den Cloud-Nutzer unterstützen, indem er das „europäische“ Cloud Computing garantiert und seine Garantie zusätzlich einer unabhängigen Kontrolle zuführt.

Anforderungsmuster: Verarbeitung der Inhaltsdaten ausschließlich im gleichen Rechtsraum wie der Cloud-Nutzer	
Ziel:	Der Cloud-Nutzer muss keine Übermittlung von Inhaltsdaten in Drittländer verantworten.
Standardisierte Anforderung:	Die Datenverarbeitung soll ausschließlich im gleichen Rechtsraum (hier: innerhalb der EU / des EWR) wie der Standort des Benutzers stattfinden, da dieser keine Inhalte im Ausland verwalten darf.
Hinweis:	Je „lokaler" die Verarbeitung der Inhaltsdaten in der Cloud erfolgt desto besser. Bevorzugt sollte die Verarbeitung der Inhaltsdaten in Deutschland, bei Bedarf europaweit, nicht jedoch weltweit erfolgen.
Perspektive:	Nutzer und Rechtmäßigkeit
Datenart:	Inhaltsdaten

4.2.1.3 Schaffung von Kontrollmöglichkeiten für den Cloud-Nutzer im Rahmen der Auftragsdatenverarbeitung

Als Auftraggeber einer Auftragsdatenverarbeitung ist der Cloud-Nutzer nach § 11 Abs. 2 Satz 4 BDSG verpflichtet, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis dieser Kontrolle ist zu dokumentieren.

Hierzu muss der Cloud-Nutzer seinen Cloud-Anbieter faktisch kontrollieren. Kontrollen sind in der Regel vor Ort und anhand von Unterlagen „selbst" durchzuführen. Die höchstpersönliche Vor-Ort-Kontrolle kann aber auch dadurch ersetzt werden, dass sich der Cloud-Nutzer vom Cloud-Anbieter ein Zertifikat eines seriösen Zertifizierungsanbieters vorlegen lässt, das die Einhaltung technischer und organisatorischer Maßnahmen beim Cloud-Anbieter bestätigt. Der Cloud-Anbieter kann den Cloud-Nutzer unterstützen, indem er unaufgefordert über den Dienst angemessene Zertifikate vorlegt (Trusted Cloud AG Rechtstrahmen des Cloud Computing 2012).

Anforderungsmuster: Schaffung von Kontrollmöglichkeiten für Cloud-Nutzer	
Ziel:	Der Cloud-Nutzer kann seinen Pflichten gemäß dem §11 BDSG nachkommen. Der Cloud-Nutzer muss den Cloud-Anbieter nach besten Wissen und Gewissen auswählen, kontrollieren (Kontrollmöglichkeiten) und anweisen (Weisungsmöglichkeiten) können.
Standardisierte Anforderung:	Der Cloud-Anbieter soll Kontroll- und Weisungsmöglichkeiten für den Cloud-Nutzer schaffen, um dessen vorgenommenen technischen und organisatorischen Maßnahmen im Rahmen des Cloud-Angebots zu überprüfen und anzuweisen.
Hinweis:	Verschiedene Umsetzungsmöglichkeiten, z. B. von gesetzlich geregelter Zertifizierung (Cloud-Anbieter sollte sicherstellen, dass die Cloud-Applikation unabhängige Zertifizierungsrichtlinien erfüllt) bis Zugang zum Rechenzentrum oder Bereitstellung gemäß dem Stand der Technik.
Perspektive:	Nutzer und Rechtmäßigkeit
Datenart:	Inhaltsdaten (mit Bezug zu Dritten)

4.2.1.4 Sicherstellung der Weitergabe der Anforderungen der Auftragsdatenverarbeitung an die vom Cloud-Anbieter beauftragten Subunternehmen

§ 11 Abs. 2 Satz 2 Nr. 7 BDSG sieht vor, dass im Vertrag zur Auftragsdatenverarbeitung (ADV) die Berechtigung zur Begründung von Unterauftragsverhältnissen geregelt wird. Da der Cloud-Nutzer als Auftraggeber für den gesamten Auftragsdatenverarbeitungsprozess verantwortlich ist, muss er sicherstellen, dass er auch über einen Unterauftragnehmer die Weisungs- und Kontrollmacht behält. Da dies jedoch nur indirekt über den Cloud-Anbieter als Auftragnehmer möglich ist, muss zwischen dem Cloud-Anbieter und dem Cloud-Nutzer vertraglich sichergestellt sein, dass der Auftragnehmer dem Unterauftragnehmer dieselben Weisungen weitergibt, die er selbst vom Auftraggeber erhält.

Der Cloud-Anbieter kann den Cloud-Nutzer in dieser Pflicht unterstützen, indem er – auch ohne im Konkreten dazu aufgefordert zu werden – von sich aus die Pflichten aus seinem Auftragsverhältnis weitergibt (Zur Unterbeauftragung beim Cloud Computing, Maier 2014, S. 35 ff.).

Anforderungsmuster: Sicherstellung der Weitergabe der Anforderungen der Auftragsdatenverarbeitung an die vom Cloud-Anbieter beauftragten Subunternehmen	
Ziel:	Sicherstellung, dass der Cloud-Nutzer seinen gesetzlichen Pflichten nachkommt. Der Cloud-Nutzer ist in der Pflicht sicherzustellen, dass die Anforderungen der Auftragsdatenverarbeitung auch an durch den Cloud-Anbieter beauftragte Subunternehmen weitergereicht und eingehalten werden.
Standardisierte Anforderung:	Die Cloud-Applikation soll den Cloud-Nutzer auffordern, dass dieser in der Pflicht ist sicherzustellen, dass die Weisungen aus der Auftragsdatenverarbeitung vom Cloud-Anbieter auch an von ihm beauftragte Subunternehmer weitergereicht werden.
Hinweis:	Es ist rechtsverträglicher wenn der Cloud-Anbieter auf den Cloud-Nutzer zugeht und diesen über den ADV darauf aufmerksam macht, dass er als Cloud-Anbieter verpflichtet ist, die vereinbarten Anforderungen der Auftragsdatenverarbeitung auch seine Subunterunternehmen weiterzureichen.
Perspektive:	Nutzer und Rechtmäßigkeit
Datenart:	Inhaltsdaten

4.2.1.5 Verwaltung von Inhaltsdaten betroffener Dritter

Als verantwortliche Stelle ist der Cloud-Nutzer verpflichtet, die Betroffenen über die Erhebung, Verarbeitung und Nutzung zu informieren (zu benachrichtigen) und bei Bedarf eine formelle Auskunft zu erteilen (§ 4 Abs. 3 BDSG, §§ 33, 34 BDSG, so z. B. Scholz/Sokol, in: Simitis 2014 § 4 BDSG Rn. 39 ff.). Weitere Betroffenenrechte, etwa auf Sperrung, Änderung und Löschung, sind ebenfalls zu berücksichtigen.

Der Cloud-Anbieter kann den Cloud-Nutzer bei der Einhaltung seiner Pflichten gegenüber Betroffenen unterstützen, indem er den Cloud-Nutzer auf diese Pflichten hinweist und technische Mittel zur Verfügung stellt, mit denen der Cloud-Nutzer den Pflichten nachkommen

kann – etwa die automatisierte Benachrichtigung an Betroffene oder Werkzeuge zur eigenständigen Korrektur und Nachverfolgbarkeit von Informationen in der Cloud, die dem Betroffenen zur Verfügung gestellt werden.

Anforderungsmuster: Verwaltung von Inhaltsdaten betroffener Dritter	
Ziel:	Rechtliche Informiertheit des Cloud-Kunden hinsichtlich seiner Transparenzpflichten ggü. betroffenen Dritten.
Standardisierte Anforderung:	Die Cloud-Applikation soll Cloud-Nutzer auffordern, sich über dessen rechtliche Pflichten zur Benachrichtigung und Auskunft ggü. betroffenen Dritten zu informieren.
Hinweis:	Aufklärung des Cloud-Kunden durch den Cloud-Anbieter zum Umgang mit Inhaltsdaten, dass dieser betroffene Dritte über die Cloud-Nutzung und den Inhalt der verwalteten Inhaltsdaten informieren muss. Der Cloud-Anbieter informiert den Cloud-Nutzer, auch über weitere Pflichten gegenüber dem Betroffenen, etwa deren Recht, Daten zu ändern und zu löschen. Der Cloud-Anbieter eröffnet dem Cloud-Nutzer zur Umsetzung dieser Rechte und Pflichten technische Realisierungsmöglichkeiten.
Perspektive:	Nutzer und Rechtmäßigkeit
Datenart:	Inhaltsdaten

4.2.1.6 Zugriffsschutz für Daten

Gibt ein Cloud-Nutzer im Rahmen der Auftragsdatenverarbeitung Daten an einen Cloud-Anbieter weiter, ist der Cloud-Nutzer als verantwortliche Stelle verpflichtet, den technischen und organisatorischen Schutz sicherzustellen und die Sicherheit der Daten auch auf Seiten des Cloud-Anbieters zu schützen (Kroschwald 2013a, S. 388 ff.). Eine Ausnahme können strafprozessuale Ermittlungen gegen den Cloud-Nutzer darstellen, bei denen der Cloud-Anbieter zur Herausgabe der Daten an Strafverfolgungsbehörden verpflichtet sein kann (Wicker 2013a).

Ein wesentliches Mittel hierzu ist die nutzerseitige Verschlüsselung (hierzu Kroschwald 2014b, S. 75 ff.). Der Cloud-Anbieter kann den Cloud-Nutzer in seiner Verantwortung unterstützen, indem er den Cloud-Nutzer auf die Vorteile einer nutzerseitigen Verschlüsselung hinweist und ggf. entsprechende Tools bereithält. Sollen Daten nicht nur gespeichert, sondern auch verarbeitet werden, kann der Cloud-Anbieter einen Zugriffschutz durch eine sog. Datenversiegelung anbieten (hierzu Kroschwald 2014a, S. 18 ff.).

Anforderungsmuster: Zugriffsschutz für Daten	
Ziel:	Unbefugte können Daten in der Cloud weder ausspähen noch manipulieren.
Standardisierte Anforderung:	Die Cloud-Applikation soll den unberechtigten Zugriff auf gespeicherte Daten verhindern.
Hinweis:	Umsetzung durch die nutzerseitige Verschlüsselung oder Versiegelung der Daten.
Perspektive:	Nutzer und Rechtmäßigkeit
Datenart:	Inhaltsdaten

4.2.1.7 Zugriffsschutz während der Datenübertragung

Die technisch-organisatorische Datensicherheit gebietet nicht nur den Schutz der ruhenden Daten, etwa beim Cloud-Nutzer oder in der Cloud. Die Weitergabekontrolle nach Nr. 4 Anlage zu § 9 BDSG sieht vor, dass von der verantwortlichen Stelle Maßnahmen zu ergreifen sind, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zum Schutz der Datenübermittlung in und von der Cloud bieten sich beispielsweise Transportverschlüsselungen wie beispielsweise das SSL-Protokoll an. Der Cloud-Anbieter kann den Cloud-Nutzer in der Erfüllung dieser Vorgaben zur Transportsicherheit unterstützen, indem beispielsweise der Cloud-Dienst eine Übertragung vom und an den Cloud-Anbieter stets nur mit einer Transportverschlüsselung zulässt.

Anforderungsmuster: Zugriffsschutz während der Datenübertragung	
Ziel:	Der Cloud-Dienst verhindert die Manipulation und Ausspähung von Daten während der Datenübertragung.
Standardisierte Anforderung:	Der Cloud-Dienst ermöglicht nur Datenübertragungen, die vor unbefugtem Zugriff geschützt sind.
Hinweis:	Sicherstellung der Datenübertragungswege
Perspektive:	Nutzer und Rechtmäßigkeit
Datenart:	Bestandsdaten, Nutzungsdaten und Inhaltsdaten

4.2.1.8 Warnung von Berufsgeheimnisträgern

Nach § 203 StGB machen sich Angehörige bestimmter Berufsgruppen, darunter vor allem Rechtsanwälte und Ärzte, strafbar, wenn sie Geheimnisse aus dem Mandats- bzw. Behandlungsverhältnis offenbaren (Kroschwald/Wicker 2012b). In der Nutzung einer Cloud könnte solch eine strafbare Offenbarung liegen, indem zumindest dem Cloud-Anbieter die faktische Möglichkeit der Kenntnisnahme der Dateninhalte eingeräumt wird (Kroschwald/Wicker 2012a). Berufsgeheimnisträger dürfen Cloud-Angebote im Zuge der Ausübung ihrer beruflichen Rolle nicht verwenden. Der Cloud-Anbieter kann den Cloud-Nutzer unterstützen, indem er bereits bei Buchung des Dienstes abfragt, ob der Nutzer einer dieser Berufsgruppen ange-

hört und ggf. ausdrücklich auf die mögliche Strafbarkeit des Cloud-Nutzers hinweist. Auch könnte der Cloud-Anbieter davon absehen, spezielle Software (z. B. Anwaltssoftware), die sich an Berufsgeheimnisträger richtet, als Cloud-Dienst anzubieten.

Anforderungsmuster: Warnung von Berufsgeheimnisträgern	
Ziel:	Eine Straftat durch Berufsgeheimnisträger aufgrund einer Cloud-Nutzung nach § 203 StGB wird verhindert.
Standardisierte Anforderung:	Die Applikation soll Berufsgeheimnisträger vor der beruflichen Nutzung warnen und davon abraten, anvertraute Privatgeheimnisse nach § 203 StGB über einen Cloud-Dienst zu übertragen oder über eine Cloud-Applikation zu verwalten.
Hinweis:	Relevant nur für Personen in ihrer Eigenschaft als Berufsgeheimnisträger nach § 203 StGB – etwa beim Umgang mit Informationen von Mandanten oder Patienten; Privatgebrauch einer Cloud ist nicht betroffen.
Perspektive:	Nutzer und Rechtmäßigkeit
Datenart:	Inhaltsdaten (mit Bezug zu Dritten)

4.2.2 Anforderungsmuster zur Förderung der rechtsverträglichen Nutzung des Cloud Computing-Angebots

4.2.2.1 Inhaltsdaten enthalten keine personenbezogenen Daten von betroffenen Dritten

Beziehen sich Daten ausschließlich auf den Cloud-Nutzer, so verantwortet dieser den Umgang mit seinen Daten und deren Schicksal – etwa indem er die Einwilligung zur Datenverarbeitung auch zu anderen Zwecken erteilt.

Werden jedoch personenbezogene Daten Dritter in die Cloud übertragen, so erlangen diese Betroffenen häufig hiervon gar keine Kenntnis. Das Datenschutzrecht legt dann dem Cloud-Nutzer entsprechend strenge Informations- sowie Auftragsnehmerpflichten gegenüber diesen betroffenen Dritten, deren Daten nunmehr beim Cloud-Anbieter gespeichert sind, auf. Enthalten die in die Cloud übertragenen Daten erst gar keinen Personenbezug zu Dritten, sind der datenschutzrechtliche Anwendungsbereich und damit der Anwendungsbereich dieser Pflichten erst gar nicht eröffnet.

Der Cloud-Anbieter kann den Cloud-Nutzer unterstützen, keine personenbezogenen Daten in die Cloud zu übertragen, indem er auf Anonymisierungs- und Pseudonymisierungsmöglichkeiten vor der Cloud-Nutzung hinweist (zur Möglichkeit der Verschlüsselung beispielsweise Kroschwald 2014b, S. 75 ff.).

Anforderungsmuster: Inhaltsdaten enthalten keine personenbezogenen Daten	
Ziel:	Es findet in der Cloud keine Speicherung und Verarbeitung personenbezogener Daten statt.
Standardisierte Anforderung:	Die Cloud-Applikation soll den Cloud-Nutzer darauf hinweisen, dass in der Cloud keine personenbezogenen Inhaltsdaten betroffener Dritter ohne deren Einverständnis verarbeitet werden sollten oder anonymisiert die Daten eigenständig.
Hinweis:	/
Perspektive:	Nutzer und Rechtsverträglichkeit
Datenart:	Inhaltsdaten

4.2.2.2 Cloud-Applikation erlaubt nur unlesbare Daten

Durch die kryptographische Verschlüsselung von Daten kann die darin gebundene Information nur noch von Personen zur Kenntnis genommen werden, die einen Schlüssel hierzu besitzen. Durch die Datenverschlüsselung wird folglich auch der Missbrauch, die Zweck- und Kontextänderung der Daten sowie die Erstellung von Persönlichkeitsprofilen oder die geheimdienstliche Auswertung verhindert.

Die Datenverschlüsselung ist nicht nur als technisch-organisatorische Maßnahme in der Anlage zu § 9 BDSG vorgesehen, sie kann auch eine sonst unzulässige Datenübermittlung in eine Cloud ermöglichen. Hierzu genügt es allerdings nicht, dass die Daten nur verschlüsselt übertragen werden und vom Cloud-Anbieter entschlüsselt werden. Vielmehr muss der Cloud-Nutzer selbst die Daten verschlüsseln und den Schlüssel vertraulich gegenüber dem Cloud-Anbieter verwahren. Nur so wird verhindert, dass die Daten durch den Cloud-Anbieter oder Dritte unbefugt ausgelesen werden (Kroschwald 2014b, S. 75 ff.).

Sollen Daten in der Cloud verarbeitet werden, wozu sie unverschlüsselt vorliegen müssen, können sie alternativ auch „versiegelt“ werden. Hierbei verhindert eine Art digitale Käseglocke, dass der Anbieter oder ein Dritter die unverschlüsselten Daten einsehen kann. Indem nur der Cloud-Nutzer Kenntnis vom Inhalt der Daten hat, kann im Verhältnis zum Cloud-Anbieter auch nur er einen Bezug zu einer dritten Person herstellen. Der Cloud-Anbieter kann den Cloud-Nutzer bei der verschlüsselten Cloud-Nutzung unterstützen, indem er über Möglichkeiten informiert, Verschlüsselungsmechanismen empfiehlt, generell nur verschlüsselte Daten annimmt oder mit einer Versiegelungstechnik arbeitet (Kroschwald 2013b, S. 300 ff.).

Anforderungsmuster: Cloud-Applikation erlaubt nur unlesbare Inhaltsdaten	
Ziel:	Schutz der Inhaltsdaten vor Zugriffen von unbefugten Dritten. Nur der Cloud-Nutzer selbst kann einen Bezug zwischen Inhaltsdaten und Personen herstellen.
Standardisierte Anforderung:	Die Applikation soll sicherstellen, dass nur der Benutzer die Inhaltsdaten lesen kann.
Hinweis:	Die Cloud-Applikation stellt die Verschlüsselung der Inhaltsdaten sicher und weist unverschlüsselte Inhaltsdaten zurück. Als unbefugte Dritte gelten auch die Mitarbeiter des Cloud-Anbieters.
Perspektive:	Nutzer und Rechtsverträglichkeit
Datenart:	Inhaltsdaten

4.2.2.3 Datenverarbeitung in Rechtsräumen mit hohem Datenschutzniveau oder im gleichen Rechtsraum

An eine Datenübermittlung in ein Land, das nicht der EU oder dem EWR angehört, sind hohe und für das Cloud Computing praktisch unerfüllbare Anforderungen geknüpft. Auch eine Auftragsdatenverarbeitung ist in einem sogenannten „Drittland“ nicht ohne eine weitere spezielle Erlaubnis oder Einwilligung zulässig (hierzu Maier 2014, S. 58 ff.).

Zwar ist eine Auftragsdatenverarbeitung außerhalb des EWR möglich. Bei besonders sensiblen Daten ist es aber aus datenschutzrechtlicher Sicht besonders förderlich, wenn die Daten im deutschen Rechtsraum verbleiben. Unabhängig davon, ob Daten aufgrund des Cloud Computing die EU oder den EWR verlassen, wirkt es grundsätzlich auf eine rechtsverträgliche Cloud-Nutzung hin, wenn die Daten ausschließlich in Rechtsräumen mit hohem Datenschutzniveau gespeichert, verarbeitet und übertragen werden. Aufgrund der weitgehenden Vereinheitlichung des Datenschutzrechts durch die EU Datenschutzrichtlinie ist ein solch hohes Datenschutzniveau zumindest innerhalb der EU und des EWR anzunehmen. Eine rechtsverträgliche Cloud-Nutzung wirkt folglich auf eine lokale, zumindest aber rein nationale oder europäische Cloud hin.

Anforderungsmuster: Datenverarbeitung in Rechtsräumen mit hohem Datenschutzniveau oder im gleichen Rechtsraum	
Ziel:	Sicherstellung des höchsten Datenschutzniveaus für die eigenen personenbezogenen Bestands- und Nutzungsdaten. Maximierung des Datenschutzes für die eigenen Daten.
Standardisierte Anforderung :	Die Verwaltung der Bestands- und Nutzungsdaten des Cloud-Nutzers wie auch die Speicherung und Verarbeitung von Inhaltsdaten durch den Cloud-Anbieter soll nur in Rechtsräumen mit hohem Datenschutzniveau erfolgen.
Hinweis:	Je nach Risikopotential aufsteigende Begrenzung des Cloud Computing auf eine Region, ein Land oder einen Kontinent.
Perspektive:	Nutzer und Rechtsverträglichkeit
Datenart:	Inhaltsdaten

4.2.2.4 Konfigurierbarkeit des Angebotes

Als verantwortliche Stelle im Rahmen einer Auftragsdatenverarbeitung ist der Cloud-Nutzer verpflichtet, Weisungen zu erteilen sowie Rechte der Betroffenen sicherzustellen und zu erfüllen. Hierzu muss er den Zweck und die wesentlichen Mittel der Verarbeitung bestimmen können (Kroschwald 2013a, S. 388 ff.). Auch für den Betroffenen liegt der Kern der informationellen Selbstbestimmung darin, die Kontrolle über den Umgang mit seinen Daten zu behalten.

Um einer solchen Verantwortung und Kontrolle im standardisierten Massengeschäft Cloud Computing gerecht werden zu können, muss der Cloud-Nutzer auf ebenso standardisierte und modularisierte Entscheidungsfunktionalitäten treffen (Bedner 2013). Diese können zur autonomen Entscheidung beitragen, zugleich aber eine – praktisch undenkbare – individuelle Anforderung jedes einzelnen Cloud-Nutzers verhindern. Geeignet sind etwa Entscheidungen des Nutzers über Auswahloptionen oder opt-in / opt-out -Modelle. Auch automatisierte Informations- und Steuerungstools ermöglichen der verantwortlichen Stelle oder dem selbstbestimmten Betroffenen eine rechtsverträgliche Cloud-Nutzung.

Anforderungsmuster: Konfigurierbarkeit des Angebotes	
Ziel:	Der Cloud-Nutzer kann durch Funktionen leicht über die Verarbeitung der von ihm bereitgestellten Daten bestimmen und verfügen.
Standardisierte Anforderung:	Die Cloud-Applikation soll die Aktivierung einzelner Funktionalitäten durch die Cloud-Nutzer ermöglichen.
Hinweis:	Die Cloud-Applikation muss so gestaltet sein, dass die Funktionalitäten weitestgehend modular nutzbar sind. Dabei unterstützt eine explizite Aktivierung (Opt-in) die Selbstbestimmung am besten.
Perspektive:	Nutzer und Rechtsverträglichkeit
Datenart:	Bestandsdaten, Nutzungsdaten und Inhaltsdaten

4.2.2.5 Protokollieren von Vorgängen durch den Cloud-Anbieter

Nach § 11 Abs. 2 Satz 4 BDSG ist der Cloud-Nutzer als Auftraggeber verpflichtet, den Cloud-Anbieter zu kontrollieren und das Ergebnis zu dokumentieren. Um dieser Aufgabe gerecht zu werden, bedarf es der Mithilfe des Cloud-Anbieters. Der Cloud-Nutzer ist deshalb schon nach § 11 Abs. 2 Satz 2 Nr. 5 und 7 BDSG verpflichtet, dem Cloud-Anbieter vertraglich aufzugeben, selbst Kontrollen bei sich durchzuführen, sowie bei den Kontrollen des Auftraggebers mitzuwirken (Zu den Pflichten des Auftraggebers Petri, in: Simitis 2014 § 11 BDSG Rn. 85 ff.). Eine solche Mitwirkung des Cloud-Anbieters könnte sich möglicherweise darauf beschränken, dem Cloud-Nutzer Zutritt zu verschaffen sowie technische Protokolle vorzulegen, die der Cloud-Nutzer dann eigenständig aus- und bewerten müsste. Allerdings wäre das in einem Massengeschäft wie dem Cloud Computing mit vielen, regelmäßig wechselnden und technisch unterschiedlich versierten Cloud-Nutzern unrealistisch und würde sogar die technischen und organisatorischen Datenschutzziele beim Cloud-Anbieter konterkarieren.

Der Cloud-Anbieter kann jedoch eine rechtsverträgliche Cloud-Nutzung fördern, indem er anschaulich und zielgruppenorientiert Informationen zusammenstellt und diese über entsprechende Plattformen (zum Beispiel eine online-Kundenplattform) immer aktuell abrufbar macht. Indem die Informationen dort – je nach Bedarf – dauerhaft zur Verfügung stehen und nachvollziehbar sind, könnte der Cloud-Nutzer auch bei der Erfüllung seiner eigenen Dokumentations- und Protokollierungspflichten unterstützt werden. Zu der hier genannten Transparenzanforderung gehört auch die Möglichkeit des Cloud-Nutzers stets den aktuellen Funktionsstatus erkennen zu können. Ein rechtsverträgliches Cloud-Angebot sollte dem Cloud-Nutzer folglich während der Nutzung – beispielsweise über die Nutzungsoberfläche – die wesentlichen Funktionsmerkmale und Einstellungen anzeigen.

Anforderungsmuster: Protokollieren von Vorgängen durch den Cloud-Anbieter	
Ziel:	Die Cloud-Nutzer können nachvollziehen, welche Vorgänge in der Cloud-Anwendung abgelaufen sind und welchen Funktionsstatus die Anwendung hat.
Standardisierte Anforderung:	Die Cloud-Anwendung soll die Cloud-Nutzer automatisiert über durchgeführte Vorgänge und den aktuellen Funktionsstatus der Cloud-Anwendung informieren.
Hinweis:	Vorgänge und Funktionen sollten so dokumentiert werden, dass der Cloud-Nutzer sie auch im Nachhinein noch nachvollziehen kann.
Perspektive:	Nutzer und Rechtsverträglichkeit
Datenart:	Bestandsdaten, Nutzungsdaten und Inhaltsdaten

4.2.2.6 Datenumgang im Falle von Vormundschaft und Todesfall

Für den Fall, dass der Cloud-Nutzer seine Rechte und Pflichten nicht mehr selbst ausüben kann, müssen andere Personen, wie Erben, Angehörige oder gesetzliche Vertreter, die Möglichkeit haben, auf Daten der Betroffenen – seien es die der Cloud-Nutzer oder die der betroffenen Dritten – zuzugreifen. Nur so können sie der ihnen mit der Verhinderung des Nutzers zufallenden Pflicht der rechtlichen Verantwortung oder ihrem eigenen Recht auf informationelle Selbstbestimmung gerecht werden.

Anforderungsmuster: Datenumgang im Falle von Vormundschaft und Todesfall	
Ziel:	Regelung des Datenumgangs im Todesfall oder Vormundschaft.
Standardisierte Anforderung:	Der Cloud-Anbieter soll dem Cloud-Nutzer Optionen für den Datenumgang im Todesfall oder bei Vormundschaft zur Verfügung stellen.
Hinweis:	Zugangswege sollten geöffnet werden. Zur Autorisierung könnte beispielsweise der Erbschein oder ein Berechtigungsnachweis (vgl. auch Regelungen bei Google und Facebook) eingefordert werden. Alternativ könnte der Anbieter den Nutzer auffordern, bereits zu Beginn der Nutzung den Umgang mit den Daten im Todesfall oder nach Ablauf einer vorab festgesetzten inaktiven Zeit des Nutzer-Accounts, selbst zu regeln.
Perspektive:	Nutzer und Rechtsverträglichkeit
Datenart:	Bestandsdaten, Nutzungsdaten und Inhaltsdaten

4.2.2.7 Auskunftspflicht des Cloud-Anbieters gegenüber staatlichen Behörden

Aufgrund öffentlich-rechtlicher Vorschriften kann der Cloud-Anbieter verpflichtet werden, Daten an inländische wie auch ausländische Behörden oder Geheimdienste herauszugeben oder Zugang zu den Daten zu gewähren (Wicker 2013b). Insbesondere wo nationales Datenschutzrecht mit entsprechendem Herausgabeverlangen aus Staaten mit schwächeren Datenschutzbestimmungen kollidiert, befindet sich der Cloud-Anbieter in einem Dilemma.

Ist der Cloud-Anbieter beispielsweise aufgrund gesellschaftsrechtlicher Verstrickungen in die USA zur Herausgabe von Daten an US-amerikanische Geheimdienste verpflichtet, könnte dies eine unzulässige und unter Umständen vom Cloud-Nutzer zu verantwortende Datenübermittlung in die USA zur Folge haben. Im Rahmen seiner Auswahl und Kontrolle als Auftraggeber muss der Cloud-Nutzer folglich sicherstellen, dass keine solchen Auskunftspflichten, die dem deutschen Datenschutzrecht widersprechen, beim Cloud-Anbieter bestehen könnten. Der Cloud-Anbieter sollte den Cloud-Nutzer hierbei unterstützen, indem er bereits vor Buchung des Dienstes eine vollständige Transparenz über Abhängigkeiten gegenüber und mögliche Herausgabeverlangen von anderen Staaten herstellt.

Anforderungsmuster: Auskunftspflicht des Cloud-Anbieters gegenüber staatlichen Behörden	
Ziel:	Schaffung von Transparenz ggü. dem Cloud-Nutzer über die Zusammenarbeit mit staatlichen Behörden.
Standardisierte Anforderung:	Der Cloud-Anbieter soll den Cloud-Nutzer darüber informieren, dass dieser einer Auskunftspflicht ggü. staatlichen Behörden unterliegt.
Hinweis:	Der Cloud-Anbieter sollte den Cloud-Nutzer genau darüber informieren, wann eine staatliche Behörde Auskunft hinsichtlich der Cloud-Nutzer Daten erhält (z. B. nur mit Gerichtsbeschluss) und in welcher in Form die Daten (verschlüsselt oder unverschlüsselt) übermittelt werden.
Perspektive:	Nutzer und Rechtsverträglichkeit
Datenart:	Bestandsdaten, Nutzungsdaten und Inhaltsdaten

5 Fazit

5.1 Zusammenfassung

Die zurückhaltende Nutzung von Cloud Computing-Diensten wird oft auf einen Mangel an Vertrauen in die Anbieter und die Technik an sich zurückgeführt. Die Vertrauenswürdigkeit von Informationssystemen und IT-Anbietern hängt unter anderem davon ab, inwiefern Systeme dem geltenden Recht entsprechen oder den Nutzer bei der Einhaltung rechtlicher Vorgaben unterstützen. Deshalb war das Ziel des Beitrages, Anbieter von Cloud Computing-Diensten zu unterstützen, die Dienste rechtmäßig sowie rechtsverträglich zu gestalten. Dazu wurden in Zusammenarbeit von juristischen Experten und Anforderungsanalysten 24 Anfor-

derungsmuster zur rechtmäßigen und rechtsverträglichen Gestaltung von Cloud Computing-Diensten entwickelt und erläutert.

Während der Entwicklung dieser Anforderungsmuster wurde zwischen verschiedenen Perspektiven unterschieden. Dieser Beitrag fokussiert ausschließlich die Cloud-Anbieter und wie deren Cloud Computing-Dienste gestaltet sein müssen, dass das Angebot rechtmäßig und darüber hinaus rechtsverträglich ist. Insgesamt wurden neun Anforderungsmuster entwickelt, die die Rechtmäßigkeit des Anbietens von Cloud Computing-Diensten adressieren. Um die Nutzungsbereitschaft zu erhöhen, reicht eine Erfüllung dieser Anforderungsmuster allerdings nicht aus, sondern der Anbieter sollte zudem sicherstellen, dass die Rechtsunsicherheit auf Seiten der Nutzer minimiert wird, in dem dieser seinen Cloud Computing-Dienst auch rechtsverträglich gestaltet. Damit unterstützt der Cloud-Anbieter, obwohl dieser rechtlich nicht dazu verpflichtet wäre, die Cloud-Nutzer bei der Erfüllung ihrer rechtlichen Pflichten, indem der Cloud-Dienst so gestaltet ist, dass auch das Nutzen rechtmäßig als auch rechtsverträglich möglich ist. Zur Förderung der rechtmäßigen Nutzung wurden insgesamt acht sowie zur Förderung der rechtsverträglichen Nutzung sieben Anforderungsmuster entwickelt und erläutert.

Damit kann dieser Beitrag das rechtmäßige Anbieten als auch das rechtmäßige und rechtsverträgliche Nutzen von Cloud Computing-Diensten fördern. Durch die interdisziplinäre Zusammenarbeit zwischen Wirtschaftsinformatikern und Rechtswissenschaftlern schließt dieser Beitrag zudem die Lücke zwischen einer technisch analytischen Herangehensweise und juristischem Fachwissen.

5.2 Einschränkungen

Die in diesem Beitrag entwickelten Anforderungsmuster basieren auf Grundlage des deutschen Rechts. Die Gültigkeit der Anforderungsmuster ist folglich auf den Anwendungsbereich des deutschen, gegebenenfalls des europäischen, Rechts begrenzt.

Darüber hinaus erheben die hier erarbeiteten Anforderungsmuster keinen Anspruch auf Vollständigkeit. Dementsprechend kann keine Gewährleistung gegebenen werden, dass eine vollständige Erfüllung der Anforderungen tatsächlich zu einem rechtmäßigen Anbieten oder Nutzen des Cloud Computing-Dienstes führen wird. Hierzu ist stets eine juristische Einzelfallbetrachtung erforderlich. Die Anforderungsmuster sollen lediglich erste Hinweise geben, wie ein Cloud Computing-Dienst gestaltet sein sollte, damit dessen Rechtmäßigkeit und Rechtsverträglichkeit gefördert werden kann. Eine weitere Einschränkung des Beitrages ist, dass die entwickelten Anforderungsmuster bisher nicht hinsichtlich deren Anwendbarkeit und deren Wirkung evaluiert wurden.

5.3 Ausblick

Die in diesem Beitrag konzeptionell und interdisziplinär entwickelten Anforderungsmuster zur Förderung der Rechtmäßigkeit und Rechtsverträglichkeit von Cloud Computing-Diensten sollten in weiteren Schritten im Rahmen der Systementwicklung angewendet und so hinsichtlich deren Anwendbarkeit und Umsetzbarkeit evaluiert werden.

Da die bisherige Forschung gezeigt hat, dass eine rechtmäßige und rechtsverträglichere Gestaltung von Informationssystemen sowohl das Vertrauen als auch die Akzeptanz fördern, gilt es daher in einem weiteren Schritt zu evaluieren, ob dies auch für den Kontext Cloud Computing zutrifft. Dazu müsste überprüft werden, ob ein Cloud Computing-Dienst, der unter Anwendung der Anforderungsmuster zur Förderung der Rechtmäßigkeit und Rechtsverträglichkeit entwickelt wurde, auf die Endkonsumenten vertrauenswürdiger wirkt als ein vergleichbarer Cloud Computing-Dienst, der diesen Anforderungen nicht gerecht wird.

6 Literaturverzeichnis

Ackermann, T.; Miede, A.; Buxmann, P.; Steinmetz, R. (2011): Taxonomy of Technological IT Outsourcing Risks: Support for Risk Identification and Quantification. Paper presented at the European Conference on Information Systems (ECIS). Paper 240, Helsinki, Finland.

Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; Zaharia, M. (2010): A View of Cloud Computing. In: Communications of the ACM, Vol. 53 (2010) No. 4, pp. 50-58.

Bedner, M. (2013): Cloud Computing – Technik, Sicherheit und rechtliche Gestaltung, Kassel 2013.

BITKOM (2010): IT- und Telekommunikations-Trends 2010. http://www.bitkom.org/files/documents/BITKOM-Presseinfo_IT-Trends_2010_-_13_01_2010.pdf, zugegriffen am 19.03.2014.

BITKOM (2011): Cloud Computing ist erneut IT-Trend des Jahres. http://www.bitkom.org/files/documents/BITKOM-Presseinfo_IT-Trends_2011_-_18_01_2011.pdf, zugegriffen am 19.03.2014.

BITKOM (2012): Die Hightech-Trends des Jahres 2012 http://www.bitkom.org/files/documents/BITKOM-Presseinfo_IT-Trends_des_Jahres_18_01_2012.pdf, zugegriffen am 19.03.2014.

BITKOM (2013): Die wichtigsten Hightech-Themen 2013 http://www.bitkom.org/files/documents/BITKOM_Presseinfo_Hightech-Trends_16_01_2013.pdf, zugegriffen am 19.03.2014.

BITKOM (2014): Nutzung von Cloud Computing in Unternehmen wächst. http://www.bitkom.org/files/documents/Presseinfo_BITKOM_und_KPMG_zum_Cloud-Monitor_30_01_2014.pdf, zugegriffen am 19.03.2014.

Bittner, E.A.C.; Leimeister, J.M. (2013): Why Shared Understanding Matters – Engineering a Collaboration Process for Shared Understanding to Improve Collaboration Effectiveness in Heterogeneous Team. Paper presented at the 46th Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii.

Bittner, E.A.C.; Leimeister, J.M. (2014): Creating Shared Understanding in Heterogeneous Work Groups – Why It Matters and How to Achieve It. In: Journal of Management Information Systems (JMIS), Vol. 31 (2014) No. 1.

Böhm, M.; Leimeister, S.; Riedel, C.; Krcmar, H. (2009): Cloud Computing: Outsourcing 2.0 oder ein neues Geschäftsmodell zur Bereitstellung von IT-Ressourcen? In: Information Management und Consulting, Ausgabe 24 (2009) Nr. 2, S. 6-14.

Boos, C.; Kroschwald, S.; Wicker, M. (2013): Datenschutz bei Cloud Computing zwischen TKG, TMG und BDSG – Datenkategorien bei der Nutzung von Cloud-Diensten. In: Zeitschrift für Datenschutz (ZD), Ausgabe 3 (2013) Nr. 5, S. 205-210.

Durán Toro, A.; Bernárdez Jiménez, B.; Ruiz Cortés, A.; Toro Bonilla, M. (1999): A Requirements Elicitation Approach Based in Templates and Patterns. Paper presented at the Workshop em Engenharia de Requisitos, Buenos Aires, .

Featherman, M.S.; Pavlou, P.A. (2003): Predicting E-Services Adoption: A Perceived Risk Facets Perspective. In: International Journal of Human-Computer Studies, Vol. 59 (2003) No. 4, pp. 451-474.

Gebauer, L.; Söllner, M.; Leimeister, J.M. (2012): Hemmnisse bei der Nutzung von Cloud Computing im B2B-Bereich und die Zuordnung dieser zu den verschiedenen Vertrauensbeziehungen. Paper presented at the Conference and Exhibition for Connected Life (ConLife), Cologne, Germany.

Gefen, D.; Karahanna, E.; Straub, D.W. (2003): Trust and TAM in Online Shopping: An Integrated Model. In: MIS Quarterly, Vol. 27 (2003) No. 1, pp. 51-90.

Glover, S.; Benbasat, I. (2010): A Comprehensive Model of Perceived Risk of E-Commerce Transactions. In: International Journal of Electronic Commerce, Vol. 15 (2010) No. 2, pp. 47-78.

Golkowsky, C.; Vehlow, M. (2011): Cloud Computing im Mittelstand: Erfahrungen, Nutzen und Herausforderungen. AG, P. In: http://www.pwc.de/de_DE/de/mittelstand/assets/Cloud_Computing_Mittelstand.pdf, zugegriffen am 27.10.2014.

Hammer, V.; Pordesch, U.; Roßnagel, A. (1993): Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, Heidelberg 1993.

Hoffmann, A. (2014): Anforderungsmuster zur Spezifikation soziotechnischer Systeme – Standardisierte Anforderungen der Vertrauenswürdigkeit und Rechtsverträglichkeit (Dissertation), (Ausgabe 3), Kassel University Press, Kassel 2014.

Hoffmann, A.; Bittner, E.A.C.; Leimeister, J.M. (2013): The Emergence of Mutual and Shared Understanding in the System Development Process. In: Requirements Engineering: Foundation for Software Quality, Lecture Notes in Computer Science. Eds.: Doerr, J.; Opdahl, A.L. Springer Verlag, Essen, Germany 2013, pp. 174-189.

IDC (2011): Cloud Computing in Deutschland. http://www.idc.de/press/presse_mc_cloud2011.jsp, zugegriffen am 23.02.2012.

IEEE (1990): Standard Glossary of Software Engineering Terminology, IEEE Std 610.12-1990. IEEE Computer Society Press 1990.

Jandt, S. (2008): Vertrauen im Mobile Commerce – Vorschläge für die rechtsverträgliche Gestaltung von Location Based Services, Nomos, Baden-Baden 2008.

Kiyavitskaya, N.; Krausova, A.; Zannone, N. (2008): Why Eliciting and Managing Legal Requirements Is Hard. Paper presented at the Requirements Engineering and Law (RELAW), Barcelona, Spain.

Kroschwald, S. (2013a): Kollektive Verantwortung für den Datenschutz in der Cloud. In: Zeitschrift für Datenschutz (ZD), Ausgabe 3 (2013a) Nr. 8, S. 388 ff.

Kroschwald, S. (2013b): Verschlüsseltes Cloud Computing – Anwendung des Daten- und Geheimnisschutzrechts auf „betreibersichere“ Clouds am Beispiel der „Sealed Cloud“. In: Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter. Hrsg.: Taeger, J. Tagungsband DSRI Herbstakademie 2013, Oldenburg 2013b, S. 289-308.

Kroschwald, S. (2014a): Schutz von Persönlichkeitsrechten in der „versiegelten“ Cloud – Anwendung und Rechtsfolgen des Datenschutz- und Berufsgeheimnisrechts auf „betreibersicheres“ Cloud Computing in der „Sealed Cloud“. In: Wie macht man Cloud sicher? Sealed Processing – Schutz der Inhalte und Metadaten. Hrsg.: Uniscon. Tagungsband zum Symposium am 24. September 2014, München 2014a, S. 18-28.

Kroschwald, S. (2014b): Verschlüsseltes Cloud Computing – Auswirkung der Kryptografie auf den Personenbezug in der Cloud. In: Zeitschrift für Datenschutz (ZD), Ausgabe 4 (2014b) Nr. 2, S. 75 ff.

Kroschwald, S.; Wicker, M. (2012a): Kanzleien und Praxen in der Cloud – Strafbarkeit nach § 203 StGB. In: Computer und Recht (CR), Ausgabe 11 (2012a), S. 758-764.

Kroschwald, S.; Wicker, M. (2012b): Zulässigkeit von Cloud Computing für Berufsgeheimnisträger: Strafbarkeit von Anwälten und Ärzten durch die Cloud? In: IT und Internet – mit Recht gestalten. Hrsg.: Taeger, J. Tagungsband DSRI Herbstakademie 2012, Oldenburg 2012b, S. 733-758.

Kroschwald, S.; Wicker, M. (2014): Einwilligung des Betroffenen in den Umgang mit seinen Daten als Lösung für das Cloud Computing, Datenschutzberater (DSB). In: Newsletter zum 15. Euroforum Datenschutzkongress 2014, (2014), S. 12-13.

Leimeister, J.M. (2012): Dienstleistungsengineering und -management, Springer Verlag, Berlin, Heidelberg 2012.

Leimeister, J.M. (2014): Collaboration Engineering: IT-gestützte Zusammenarbeitsprozesse systematisch entwickeln und durchführen, Springer Gabler Verlag 2014.

Luo, X.; Li, H.; Zhang, J.; Shim, J.P. (2010): Examining Multi-Dimensional Trust and Multi-Faceted Risk in Initial Acceptance of Emerging Technologies: An Empirical Study of Mobile Banking Services. In: Decision Support Systems, Vol. 49 (2010) No. 2, pp. 222-234.

Maier, N. (2014): Die Datenweitergabe im Rahmen des Cloud Computing unter besonderer Betrachtung von Unterauftragsverhältnissen, Kassel 2014.

Marston, S.; Li, Z.; Bandyopadhyay, S.; Zhang, J.; Ghalsasi, A. (2011): Cloud Computing – The Business Perspective. In: Decision Support Systems, Vol. 51 (2011) No. 1, pp. 176-189.

Mayer, R.C.; Davis, J.H.; Schoorman, F.D. (1995): An Integrative Model of Organizational Trust. In: The Academy of Management Review, Vol. 20 (1995) No. 3, pp. 709-734.

Otto, P.N.; Anton, A.I. (2007): Addressing Legal Requirements in Requirements Engineering. Paper presented at the 15th IEEE International Requirements Engineering Conference, New Delhi, India.

Pohl, K. (2007): Requirements Engineering: Grundlagen, Prinzipien, Techniken, Dpunkt-Verlag 2007.

Repschlaeger, J.; Zarnekow, R.; Wind, S.; Turowski, K. (2012): Cloud Requirement Framework: Requirements and Evaluation Criteria to Adopt Cloud Solutions. *20th European Conference on Information Systems (ECIS). Paper 42*. Barcelona, Spain.

Roßnagel, A. (1997): Rechtliche Regelungen als Voraussetzung für Technikgestaltung. In: Mehrseitige Sicherheit in der Kommunikationstechnik, Band 1 - Verfahren - Komponenten - Integration. Hrsg.: Müller, H.; Pfitzmann, A., Bonn 1997, S. 361.

Roßnagel, A. (2008): Rechtswissenschaftliche Gestaltung der Informationstechnik. In: Wissen, Vernetzung, Virtualisierung - liber amicorum zum 65. Geburtstag von Univ.-Prof. Dr. Udo Winand. Hrsg.: Kortzfleisch, F.O.; Bohl, O. Lohmar 2008, S. 381.

Simitis, S. (2014): Bundesdatenschutzgesetz, München 2014.

Söllner, M.; Hoffmann, A.; Hoffmann, H.; Leimeister, J.M. (2012a): Vertrauensunterstützung für sozio-technische ubiquitäre Systeme. In: Zeitschrift für Betriebswirtschaft, Ausgabe 82 (2012a) Nr. 4, S. 109-140.

Söllner, M.; Hoffmann, A.; Hoffmann, H.; Wacker, A.; Leimeister, J.M. (2012b): Understanding the Formation of Trust in IT Artifacts. Paper presented at the 33rd International Conference on Information Systems (ICIS), Orlando Florida, USA.

Söllner, M.; Leimeister, J.M. (2012): Opening up the Black Box: The Importance of Different Kinds of Trust in Recommender System Usage. *72nd Academy of Management Annual Meeting*. Boston, Mass., USA.

Söllner, M.; Pavlou, P.A.; Leimeister, J.M. (2013): Understanding Trust in IT Artifacts – A new Conceptual Approach. *Academy of Management Annual Meeting*. Orlando, Florida, USA.

Trusted Cloud AG Rechtstrahmen des Cloud Computing (2012): Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, Berlin 2012.

Wicker, M. (2013a): Durchsuchung in der Cloud – Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden. In: MultiMedia und Recht (MMR), (2013a), S. 765-769.

Wicker, M. (2013b): Ermittlungsmöglichkeiten in der Cloud – Vereitelt das Speichern in der Cloud die Zuständigkeit deutscher Ermittlungsbehörden? In: Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter. Hrsg.: Taeger, J. Tagungsband der Herbstakademie, Band 2, Edewecht 2013 2013b, S. 981-1000.

Wicker, M. (2014): Die Neuregelung des § 100j StPO auch beim Cloud Computing? – Zugriff auf Zugangsdaten zur Cloud nach der neuen Bestandsdatenauskunft? In: MultiMedia und Recht (MMR), (2014), S. 298-302.

Danksagung

Wir danken allen Workshop-Teilnehmerinnen und Teilnehmern für ihr Engagement und die erfolgreiche Zusammenarbeit. Das diesem Beitrag zugrundeliegende Vorhaben wurde im Rahmen des Projekts Value4Cloud (Förderkennzeichen: 01MD11044) erarbeitet und mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen des Technologieprogramms Trusted Cloud gefördert. Weiterführende Informationen zum Projekt finden Sie unter: www.value4cloud.de.

Autorenhinweise

Lysann Gebauer, Dipl.-Psych., ist wissenschaftliche Mitarbeiterin am Fachgebiet Wirtschaftsinformatik von Prof. Dr. Jan Marco Leimeister und am dortigen wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel tätig. Im Rahmen des Projektes Value4Cloud beschäftigt sich die Autorin überwiegend mit dem Themenschwerpunkt wie Vertrauen in Cloud Computing entsteht, beeinflusst wird und gefördert werden kann. Zudem beschäftigt sich die Autorin intensiv mit der Erforschung der kontinuierlichen Nutzung von Informationssystemen.

Steffen Kroschwald, LL.M., ist wissenschaftlicher Mitarbeiter in der Projektgruppe für verfassungsverträgliche Technikgestaltung von Prof. Dr. Alexander Roßnagel am wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel. Im Rahmen des Projektes Value4Cloud und seiner Dissertation mit dem Titel „Informationelle Selbstbestimmung in der Cloud“ beschäftigt sich der Autor mit Fragen des Daten- und Geheimnisschutzrechts beim Cloud Computing sowie der rechtsverträglichen Gestaltung von Cloud-Diensten.

Magda Wicker, Ass. Jur., ist wissenschaftliche Mitarbeiterin in der Projektgruppe für verfassungsverträgliche Technikgestaltung von Prof. Dr. Alexander Roßnagel am wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel. Im Rahmen des Projektes Value4Cloud und ihrer Dissertation mit dem Titel „Cloud Computing und Staat“ beschäftigt sich die Autorin mit Strafbarkeitsrisiken und strafprozessualen Zugriffen beim Cloud Computing sowie darauf aufbauend mit Möglichkeiten zur Vermeidung einer Strafbarkeit und der Schaffung von Rechtsicherheit bei Eingriffen durch Strafverfolgungsbehörden.