RESEARCH

Stephan Sädtler

Rechtskonformes Identitätsmanagement im Cloud Computing

Anforderungen an den Einsatz elektronischer Ausweise

Springer

Rechtskonformes Identitätsmanagement im Cloud Computing

Stephan Sädtler

Rechtskonformes Identitätsmanagement im Cloud Computing

Anforderungen an den Einsatz elektronischer Ausweise

Springer

Stephan Sädtler
Passau, Deutschland

Dissertation an der Universität Passau, Juristische Fakultät, 2016

Disputation am 4.5.2016

Die Dissertation entstand im Rahmen des vom Bundeswirtschaftsministerium für Wirtschaft und Energie geförderten Forschungsprojektes „SkIDentity - Vertrauenswürdige Identitäten für die Cloud“ des Technologieprogramms „Trusted Cloud“.

ISBN 978-3-658-14806-5 ISBN 978-3-658-14807-2 (eBook)
DOI 10.1007/978-3-658-14807-2

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

Springer

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH

Meinen Eltern Doris und Wolfgang

Vorwort

Die vorliegende Arbeit entstand während meiner Beschäftigung als Wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Informationstechnologierecht und Rechtsinformatik der Universität Passau von Prof. Dr. Gerrit Hornung, LL.M., und speziell im Rahmen der Mitwirkung in dem BMWi-geförderten Forschungsprojekt „SkIDentity – Vertrauenswürdige Identitäten für die Cloud“ des Technologieprogramms Trusted Cloud. Die Arbeit wurde im Wintersemester 2015/2016 an der Juristischen Fakultät der Universität Passau als Dissertation angenommen. Die Disputation fand am 4.5.2016 statt.

Besonderer Dank gebührt vor allem meinem Doktorvater, Herrn Prof. Dr. Gerrit Hornung, für seine exzellente Betreuung sowohl in fachlicher als auch menschlicher Hinsicht. Ohne seine kontinuierliche Begleitung, seinen durchgehend angenehmen, aber höchst effizienten Führungsstil und nicht zuletzt seine Vorarbeiten auf dem Forschungsgebiet wäre die Arbeit in dieser Form nicht möglich gewesen. Diese überaus gute Zusammenarbeit hat sich auch in einer Reihe weiterer – teilweise gemeinsamer – Publikationen manifestiert.

Bei Herrn Prof. Dr. Dirk Heckmann bedanke ich mich herzlich für die Zweitbegutachtung.

Danken möchte ich auch meinen Kolleginnen und Kollegen des Lehrstuhls für ihre fortlaufende Unterstützung. Hervorzuheben ist insbesondere der fachliche und technische Input von Kai Hofmann und das erste Korrekturlesen der Arbeit von Stephan Schindler.

Ebenso bedanke ich mich bei allen Projektpartnern des Forschungsprojektes SkIDentity (https://www.skidentity.com/en/home) für die intensive und produktive Zusammenarbeit über drei Jahre hinweg. Die mehrfache Auszeichnung der Projektergebnisse unter anderem durch „Trusted Cloud 2011“ und „Deutschland – Land der Ideen 2015“ lassen darauf schließen, dass diese Ergebnisse dazu beitragen können, das interdisziplinäre Problem eines technisch sicheren, rechtskonformen und wirtschaftlich sinnvollen Identitätsmanagements im Internet einer Lösung zuzuführen.

Mein persönlicher Dank gilt schließlich meiner Familie und meiner Partnerin Kerstin, die mich auch bei den grafischen Darstellungen unterstützt hat.

Passau, im Mai 2016 Stephan Sädtler

Inhaltsverzeichnis

Abkürzungsverzeichnis

a. A.	andere Ansicht
ABl.	Amtsblatt
Abs.	Absatz
a. E.	am Ende
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a. F.	alte Fassung
AG	Amtsgericht
AktG	Aktiengesetz
AO	Abgabenordnung
API	Application Programming Interface
Art.	Artikel
B2B	Business-to-Business
B2C	Business-to-Customer
BAG	Bundesarbeitsgericht
BayGO	Bayerische Gemeindeordnung
BayVGH	Bayerischer Verfassungsgerichtshof
BayVwVfG	Bayerisches Verwaltungsverfahrensgesetz
BB	Betriebs-Berater (Zeitschrift)
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidung des Bundesgerichtshofes in Zivilsachen
BMWi	Bundesministerium für Wirtschaft und Energie
BremLDS	Bremisches Datenschutzgesetz
BR-Drs.	Bundesrat-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsgesetz
CR	Computer und Recht (Zeitschrift)
CRM	Customer-Relationship-Management
dass.	dasselbe
De-Mail-G	Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften
ders.	derselbe
dies.	dieselbe

DIN	Deutsches Institut für Normung e. V.
DKK	dienste- und kartenspezifisches Kennzeichen
DÖV	Die öffentliche Verwaltung (Zeitschrift)
DSG SH	Datenschutzgesetz Schleswig-Holstein
DS-GVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/45/EG (Datenschutz-Grundverordnung)
DS-GVO-E/K	Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)
DS-GVO-E/P	Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung)
DSRL	Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EC-Karte	Eurocheque-Karte
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaften
eGK	elektronische Gesundheitskarte
EGMR	Europäischer Gerichtshof für Menschenrechte
eID	electronic Identification
eIDAS-VO	Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
eIDAS-VO-E	Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
EMRK	Konvention zum Schutz der Menschenrechte und Grundfreiheiten
EN	Europäische Norm
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
FISA	Foreign Intelligence Surveillance Act
Fn.	Fußnote
GCHQ	Government Communications Headquarters
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung

GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GVBl.	Bayerisches Gesetz- und Verordnungsblatt
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz)
HBCI	Homebanking Computer Interface
Hrsg.	Herausgeber
IaaS	Software as a Service
ID	Identity
IDM	Identitätsmanagement
IdP	Identity Provider
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
i. S. V.	im Sinne von
IT	Informationstechnologie
i. V. m.	in Verbindung mit
KG	Kammergericht
KMU	kleine und mittelständische Unternehmen
KOM	Europäische Kommission, Dokumente
K&R	Kommunikation und Recht (Zeitschrift)
LG	Landgericht
lit.	litera
LRA	Landratsamt
MedR	Medizinrecht (Zeitschrift)
MMR	Multimedia und Recht (Zeitschrift)
m. w. N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJW-RR	Neue Juristische Wochenzeitschrift, Rechtsprechung Report (Zeitschrift)
nPA	neuer Personalausweis
NSA	National Security Agency
NStZ	Neue Zeitschrift für Strafrecht (Zeitschrift)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
NZS	Neue Zeitschrift für Sozialrecht (Zeitschrift)
OLG	Oberlandesgericht
o. V.	ohne Verfasser
OVG	Oberverwaltungsgericht
PaaS	Platform as a Service
PACE	Password Authenticated Connection Establishment
PAuswG	Personalausweisgesetz

PAuswV	Personalausweisverordnung
PIN	Personal Identification Number
PinG	Privacy in Germany (Zeitschrift)
PKI	Public Key Infrastructure
PR-ITR	Der juris PraxisReport IT-Recht
RDV	Recht der Datenverarbeitung
Rn.	Randnummer
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SMS	Short Message Service
SSL	Secure Sockets Layer
SSLA	Security Service Level Agreement
StaaS	Storage as a Service
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TAN	Transaktionsnummer
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
TR	Technische Richtlinie
USA	United States of America
USC	United States Code
VfB	Vergabestelle für Berechtigungszertifikat beim Bundesverwaltungsamt
VG	Verwaltungsgericht
VPN	Virtual Private Network
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
XaaS	X as a Service
XML	Extensible Markup Language
ZD	Zeitschrift für Datenschutz (Zeitschrift)
ZD-Aktuell	Newsdienst Zeitschrift für Datenschutz aktuell (Zeitschrift)
ZPO	Zivilprozessordnung
ZUM	Zeitschrift für Urheber- und Medienrecht (Zeitschrift)

Abbildungsverzeichnis

1 Sicherheit im Cloud Computing (Einleitung)

In der Cloud sind „Daten immer und überall verfügbar“[1]. So oder so ähnlich bewerben viele Cloud-Anbieter ihre Dienste. Kaum ein Trend der IT-Branche hat in den letzten Jahren sowohl in technischer als auch in rechtlicher Hinsicht so viel Aufmerksamkeit erregt wie das Cloud Computing. Zu verstehen ist darunter ein Konzept, „das es erlaubt[,] bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können“[2]. Das Cloud Computing bedient sich dabei unterschiedlicher Techniken und hat sich zu einem Paradebeispiel für die „digitale Revolution“ entwickelt.

Der Erfolg des Cloud Computings beruht in erster Linie auf dem enormen wirtschaftlichen Potenzial von Cloud-Anwendungen in nahezu allen Geschäfts- und Lebensbereichen. Kaum ein anderes technisches Konzept profitiert von immer größeren Speichermöglichkeiten bei immer schnelleren Übertragungsraten und wird somit derart von dem rasanten technologischen Fortschritt beflügelt.

Das Potenzial des Cloud Computings belegen folgende Zahlen: 2014 haben 44 % der deutschen Unternehmen Cloud-Anwendungen genutzt, während weitere 24 % den Einsatz planen oder erwägen.[3] Für das Jahr 2015 wurde dem Cloud Computing ein Marktvolumen von 9,23 Milliarden Euro allein in Deutschland vorausgesagt.[4]

Gedämpft wurde die Nachfrage allerdings vor allem durch den sogenannten NSA-Skandal im Sommer 2013, als der Whistleblower Edward Snowden, ein ehemaliger Mitarbeiter des US-amerikanischen Geheimdienstes National Security Agency (NSA), damit begonnen hatte, Dokumente über außer Kontrolle geratene Geheimdienste veröffentlichen zu lassen.[5] Betroffen von den geheimdienstlichen Aktivitäten ist danach vor allem der Internetverkehr mit Bezug zu den USA, wo ein Großteil der Anbieter auf dem Cloud-Markt angesiedelt ist bzw. seine IT-Infrastruktur unterhält. Die Themen Datenschutz und Datensicherheit werden seitdem auch in einer breiten Öffentlichkeit disku-

---

1 http://www.telekom.com/konzern/10920; alle URLs wurden letztmalig am 1.4.2016 abgerufen.
2 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html.
3 *KPMG/Bitkom Research GmbH* 2015, 5.
4 http://www.presseportal.de/pm/23295/2781159.
5 http://www.heise.de/-2101229.html.

S. Sädtler, *Rechtskonformes Identitätsmanagement im Cloud Computing*,
DOI 10.1007/978-3-658-14807-2_1

tiert. Sie wurden zu einem maßgeblichen Bestandteil der von der Bundesregierung vorgestellten „Digitalen Agenda“[6]. Sie galten zum anderen allerdings schon zuvor als häufigste Hemmnisse des Cloud Computings.[7] Laut einer Studie von Microsoft aus dem Jahr 2012 entscheiden vor allem Datenschutz und Compliance über die Wahl des Cloud-Anbieters.[8] Aus diesem Blickwinkel erhält das Werbeversprechen hinsichtlich der Datenverfügbarkeit in der Cloud einen anderen Kontext, als von den Werbenden beabsichtigt.

Obwohl das Cloud Computing in rechtlicher Hinsicht als Querschnittsmaterie sämtliche Bereiche des IT-Rechts tangiert und sich regelrecht zur Spielwiese für Juristen entwickelt hat, nehmen Datenschutz und Datensicherheit eine herausragende Rolle ein. Die Datensicherheit ist dabei einerseits als Teil des Datenschutzrechts zu verstehen, das als einfachgesetzliche Ausgestaltung des allgemeinen Persönlichkeitsrechts auf personenbezogene Daten beschränkt ist. Andererseits geht die Datensicherheit darüber hinaus: Gemäß der Begriffsdefinition des § 2 Abs. 2 BSIG ist Schutzgegenstand der Sicherheit in der Informationstechnik die Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen. Die Datensicherheit fungiert daher als Schnittstelle zwischen Recht und Technik.[9]

Nach der Definition des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) ist die Verfügbarkeit von Informationen demnach ein fester Bestandteil der Datensicherheit. Durch Cloud-Anwendungen wird ein hohes Maß an Datenverfügbarkeit erreicht. Die Schutzziele der Vertraulichkeit und Unversehrtheit verhalten sich im Cloud Computing allerdings hierzu meist konträr. Daten, auf die von überall und über beliebige Endgeräte zugegriffen werden kann, bedürfen einer zentralen Speicherung und Verwaltung. Die Kostenvorteile des Cloud Computings ergeben sich gerade dadurch, dass dies nicht beim Nutzer selbst geschieht, sondern bei einem Dritten, dem Cloud-Anbieter. Die Vorteile liegen aus dessen Sicht aber auch gerade in einer Kapazitätenauslastung, die zum einen durch eine flexible Verteilung von Daten und zum anderen durch den Zugriff vieler Nutzer erreicht wird.

Aufgrund der technischen Möglichkeiten und der potenziellen Einsatzvielfalt ist mittlerweile praktisch jede in Datenform gespeicherte Information cloudfähig. So vielfältig

---

6 http://www.heise.de/-2296280.html; http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.

7 S. *BITKOM* 2013, 22.

8 DuD 2012, 781 f.

9 Im Datenschutzrecht ist sie insbesondere im Rahmen der technischen und organisatorischen Maßnahmen aus § 9 BDSG angesiedelt. Auf diese und ähnliche Vorschriften ist ein besonderes Augenmerk zu richten. S. dazu unter 3.1.3.2.1.

die Einsatzmöglichkeiten von Cloud-Anwendungen gestaltet werden können, so unterschiedlich und vielseitig können die anfallenden Daten und deren Gebrauch sein. Je nach Datenart – z. B. Daten mit oder ohne Personenbezug – bestehen allerdings unterschiedliche Schutzpflichten für Cloud-Inhalte, sofern deren Verarbeitung in einer Cloud nicht gänzlich untersagt ist. Cloud-Daten sind dem potenziellen Zugriff vieler Akteure[10] ausgesetzt, da sich das Cloud Computing gerade sowohl durch eine Ressourcen-Verteilung auf Anbieterseite als auch durch eine Ressourcen-Teilung auf Nutzerseite auszeichnet.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt als wesentliches Element einer sicheren Infrastruktur ein zuverlässiges Identitäts- und Rechtemanagement auf, mit dem gewährleistet werden soll, dass nur autorisierte Personen innerhalb ihrer Befugnisse auf die jeweiligen Cloud-Ressourcen zugreifen können.[11] Teil eines solchen Identitäts- und Rechtemanagements ist dabei die Identifikation und Authentisierung der jeweiligen Personen. Für sensible Bereiche wird im Cloud Computing explizit entsprechend dem Online-Banking eine starke Zwei-Faktor-Authentisierung mittels Chipkarten, USB-Sticks oder von Hardwaregeräten generierten Einmalpasswörtern empfohlen.[12]

Die derzeitige Praxis ist von diesen Vorgaben allerdings noch weit entfernt. Am häufigsten werden Zugänge zu Online-Ressourcen noch durch Nutzername und Passwort geschützt,[13] was im Allgemeinen als sehr unsicher gilt. Meldungen über Identitätsdiebstähle immer größeren Ausmaßes häufen sich. So erbeuteten Hacker Anfang des Jahres 2014 Zugangsdaten von 16 Millionen E-Mail-Accounts.[14] Mitte 2014 wurde die Entwendung von 1,2 Milliarden Datensätzen, die aus Nutzernamen und Passwörtern bestehen, bekannt.[15]

Dies wirft einerseits die Frage auf, inwieweit Anbieter verpflichtet sind bzw. verpflichtet werden können, ein bestimmtes und als sicher geltendes Verfahren einzusetzen. Dies hängt im Einzelnen von der Qualität und der potenziellen Nutzung der Daten ab und ist Gegenstand der folgenden Untersuchungen.

---

10 Zum Zugriff durch potenziell viele Nutzer *BITKOM* 2009, 30.

11 *BSI* 2012a, 43; *dass.* 2016, 57 f.

12 S. zu diesem Absatz *BSI* 2012a, 43; s. auch *dass.* 2016, 58; zur Erforderlichkeit der sicheren Gestaltung von Identifizierung und Authentisierung auch *Bedner* 2013, 343 ff.; zu den technischen Hintergründen bzgl. Identitätsdiebstahl und -missbrauch s. *Borges et al.* 2011, 17 ff.

13 *Hühnlein/Schmölz* 2012, 44; vgl. *Schröder/Morgner,* DuD 2013, 530; *Bichsel et al.* 2015, 12; auf den B2C-Bereich beschränkt *Kubach/Roßnagel* 2014, 38 (Abbildung 10).

14 S. http://www.handelsblatt.com/9362082.html.

15 S. http://www.heise.de/-2285655.html.

Andererseits unterliegt der Umgang mit Identitätsdaten, die einer Authentisierung und einem Rechtemanagement zugrunde liegen, selbst rechtlichen Anforderungen und ist schutzbedürftig.[16] Da Identitätsdaten den Zugang zu sensiblen Daten vermitteln können, sind sie selbst als sensibel einzustufen. Obwohl sie selbst auch Cloud-Inhalte darstellen können, sind sie funktionell von den durch sie geschützten Daten abzugrenzen und bilden den Fokus dieser Arbeit. Es soll untersucht werden, ob sie möglicherweise anders behandelt werden können als herkömmliche Cloud-Inhaltsdaten. Hierbei wird auf bestehende Referenzszenarien zurückgegriffen. Allein der Begriff des Cloud Computings ist nämlich für sich gesehen einer rechtlichen Analyse nicht zugänglich. Vielmehr müssen dafür die einzelnen technischen Gegebenheiten, die sich im Rahmen des Cloud Computings erheblich unterscheiden können, genau beleuchtet werden. Als konkretes Referenzszenario für die Untersuchungen wird daher die Architektur des Forschungsprojekts *SkIDentity – Vertrauenswürdige Identitäten für die Cloud* aus dem durch das Bundesministerium für Wirtschaft und Energie (BMWi) geförderten Technologie-Programm *Trusted Cloud*[17] herangezogen (Referenzarchitektur). Dieses Projekt hat es sich zum Ziel gesetzt, eine Brücke zwischen sicheren elektronischen Ausweisen einerseits und unterschiedlichen Cloud-Anwendungen andererseits zu schlagen. Im Vordergrund steht dabei die Integration von als sicher geltenden Chipkarten wie dem neuen Personalausweis (nPA) oder der elektronischen Gesundheitskarte (eGK). Da der Einsatz des nPAs allerdings an die gesetzlichen Vorgaben des Personalausweisrechts und der Einsatz der eGK an das Sozialrecht gebunden ist und auch der allgemeine datenschutzrechtliche Rahmen konkrete Anforderungen an den Umgang mit Identitätsdaten enthält, müssen die einschlägigen Rechtsvorschriften identifiziert und bei einer rechtskonformen Technikgestaltung beachtet werden.

Die Wahl des Identifikationsmittels und der rechtliche Rahmen der Verarbeitung von Identitätsdaten können von der jeweiligen Cloud-Art abhängig sein. Aufseiten der Cloud-Anbieter können unterschiedliche Modelle angesiedelt sein.[18] Es kann zunächst zwischen Cloud-Anwendungen unterschieden werden, die sich direkt an Verbraucher richten, und solchen, die Unternehmen eine Plattform bieten, innerhalb derer sie beispielsweise Daten Dritter verarbeiten (lassen). Auch existieren inzwischen Bestrebungen der öffentlichen Hand, die Vorteile des Cloud Computings zu nutzen, was eine Unterscheidung zwischen privaten und öffentlich-rechtlichen Anwendern notwendig macht.

---

16 *Sädtler* 2013a, 259 ff.

17 http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/trusted-cloud-cloud-computing,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf; *Kubach/Hühnlein* 2014. Die Universität Passau behandelte unter Mitwirkung des Autors die rechtlichen Aspekte des Projekts.

18 S. zu diesem Abschnitt u. 2.1.

Hierdurch entsteht eine Struktur unterschiedlicher Akteure, deren Rechtsverhältnisse und Verantwortlichkeiten anhand der relevanten Rechtsmaterien zu untersuchen sind. Im Vordergrund steht dabei das Datenschutzrecht, das sowohl an private als auch an öffentliche Stellen adressiert ist. Einen wesentlichen Bestandteil bilden auch die Normen des Personalausweisrechts. Soll die elektronische Gesundheitskarte zum Einsatz kommen, sind darüber hinaus die entsprechenden Normen des Sozialrechts zu beachten. Von den genannten Regelungsgebieten, die allesamt Zulässigkeitsvoraussetzungen enthalten, sind solche zu unterscheiden, die die rechtliche Wirkung eines Verfahrens beinhalten. Hierzu gehört vor allem das Beweisrecht. Die sich aus diesen Themengebieten ergebenden Rechtsfragen sind Gegenstand der vorliegenden Untersuchung.

Dabei ist das zugrunde liegende Modell für das Identitätsmanagement kein zwingendes, was dementsprechend auch für die aufgeworfenen Rechtsfragen gilt. Allerdings verspricht es, Datensicherheit auf der einen Seite bei Interoperabilität und Nutzerfreundlichkeit auf der anderen Seite in Einklang zu bringen.[19] Der Anspruch an die vorliegende Arbeit besteht darin, nach einer Analyse der rechtlichen Vorgaben an der Schnittstelle zwischen Recht und Technik konkrete Gestaltungsvorschläge zu formulieren.

Im Einzelnen gliedert sich die Arbeit wie folgt: Zunächst werden die technischen Grundlagen des Cloud Computings, des Identitätsmanagements sowie des Einsatzes elektronischer Ausweise im Cloud-Umfeld erläutert (Kapitel 2). In einem weiteren Kapitel werden die rechtlichen Grundlagen in Bezug auf das Identitätsmanagement im Cloud-Kontext erläutert, und im Anschluss daran wird auf die Besonderheiten des Einsatzes von elektronischen Ausweisen, allen voran des nPAs, eingegangen (Kapitel 3). Schließlich werden die einzelnen Rechtsverhältnisse anhand der gefundenen Ergebnisse untersucht (Kapitel 4), um zusammenfassend konkrete Anforderungen an eine rechtskonforme Technikgestaltung zu formulieren (Kapitel 5). Dabei wird auch an geeigneten Stellen auf etwaige Änderungen durch die europäische Datenschutzreform, insbesondere vor dem Hintergrund des rasanten technologischen Fortschritts, eingegangen.

[19] *Kubach et al.* 2014b, 4.

2 Technische Grundlagen

2.1 Cloud Computing

2.1.1 Definition

Angelehnt an die in der Einleitung vorgestellte Definition des Cloud Computings sind folgende Merkmale hervorzuheben:[20] Cloud-Dienste werden zentral von einem Cloud-Diensteanbieter über ein öffentliches Netz, im Regelfall das Internet, angeboten. Sie sind skalierbar und können bedarfsgerecht abgerufen werden. Cloud-Dienste basieren auf abstrakten Infrastrukturen und Virtualisierung. Dies bedeutet, dass „Softwaredienste und Anwendung von der Hardware getrennt" werden, um eine optimale Serverauslastung zu erreichen.[21] Die Ressourcen befinden sich in sogenannten Ressourcen-Pools, auf die eine Vielzahl von Personen – abhängig von ihrer Autorisierung – zugreifen kann.

Da die Dienste in der Regel über ein Web-Portal erreichbar sind, kann die Nutzung unabhängig vom Ort und der Art des Endgeräts des jeweiligen Nutzers gestaltet werden. Auch wenn dies zunächst an das IT-Outsourcing erinnert,[22] bestehen doch wesentliche Unterschiede, die anhand der folgenden Erscheinungsformen dargestellt werden. Diese können nach Cloud-Modellen, nach verschiedenen Leistungs-Modellen und sowohl nach unterschiedlichen Strukturen als auch nach Personenkreisen auf Kunden- und Anbieterseite unterteilt werden.

2.1.2 Cloud-Modelle

Hinsichtlich der verschiedenen Cloud-Modelle haben sich folgende Unterscheidungen herausgebildet: Cloud-Betreiber-Modelle werden in „Public Clouds", „Private Clouds", „Hybrid Clouds" und „Community Clouds" unterteilt. Dabei unterscheiden sich diese weniger hinsichtlich der technischen Umsetzung als vielmehr in ihrer Organisation: Eine Public Cloud steht abstrakt einem nicht begrenzten Personenkreis zur Verfügung. „Sie [die Public Cloud] kann von beliebigen Personen, Nutzern und Unternehmern genutzt werden und ist nicht mehr auf interne Anwendungen einer einzelnen Institution, eines

[20] Zum Folgenden *Rhoton/Haukioja* 2013, Chapter 1, 4 ff.; s. zum Ganzen auch *Heckmann* 2014, Kapitel 9, Rn. 599 ff.
[21] S. http://www.global.de/virtualisierung-als-basis-des-cloud-computing/.
[22] Vgl. *Weichert,* DuD 2010, 679.

S. Sädtler, *Rechtskonformes Identitätsmanagement im Cloud Computing*,
DOI 10.1007/978-3-658-14807-2_2

Departements oder eines Unternehmens beschränkt."[23] Charakteristisch für eine Private Cloud ist dagegen, dass sie von Anwendern und Nutzern einer geschlossenen Institution genutzt wird. Dies ist etwa bei unternehmens-, konzern-, behörden- oder universitätsinternen Clouds der Fall. Auch in rechtlicher Hinsicht stehen Private Clouds unter der Verantwortung einer einzigen Stelle.[24] Oftmals zeichnen sie sich dadurch aus, dass sich die zugrunde liegende Infrastruktur ebenfalls an einem Ort bzw. an wenigen Orten befindet. Die „Community Cloud" stellt eine Variante der Private Cloud dar. Mit ihr schließen sich unterschiedliche Institutionen zusammen.[25] Zwar ist hier der Nutzerkreis nicht mehr auf eine Stelle beschränkt, dennoch handelt es sich um einen stark begrenzten Kreis, der darüber hinaus einen gemeinsamen Zweck verfolgt. Die Mischform aus einer Private Cloud, einer Public Cloud und einer traditionellen IT-Umgebung wird als Hybrid Cloud bezeichnet.[26] Diese kann erforderlich werden, wenn die jeweils einzelnen Erscheinungsformen spezielle Kunden-Anforderungen nur unzureichend umsetzen.[27]

2.1.3 Cloud-Leistungen

Hinsichtlich der verschiedenen Service-Modelle wird grob zwischen Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS) unterschieden. IaaS bezeichnet die Bereitstellung von IT-Ressourcen in Form einer Basisinfrastruktur. Dies beinhaltet eine „wenig veredelte Rechen- und Speicherleistung auf virtualisierten Servern sowie Netzwerkinfrastruktur-Funktionalität mit hohem Standardisierungsgrad und intelligentem System-Management als Service".[28] Infrastrukturkomponenten bestehen vornehmlich aus Servern, Rechenleistung, Netzkapazität, Datenspeichern und Backup-Systemen.[29]

Im Rahmen von PaaS werden Entwicklungs-Plattformen für System-Architekten und Anwendungsentwickler bereitgestellt.[30] Hierbei handelt es sich um eine vordefinierte „Kombination von Betriebssystem, Hardware und Anwendung", die vom Nutzer über einen administrativen Zugriff verwaltet wird.[31]

---

23 *Metzger/Reitz/Villar* 2011, 19; s. dazu auch *Reuter/Brix* 2012, 22.
24 *Weichert,* DuD 2010, 679, mit Verweis auf *Feilner,* Linux-Magazin 2010, Heft 5, 44.
25 *Reuter/Brix* 2012, 25.
26 *BITKOM* 2009, 30 f.
27 Vgl. http://www.microsoft.com/de-de/cloud/glossar/hybrid_cloud.aspx.
28 *BITKOM* 2010, 16.
29 S. dazu *Reuter/Brix* 2012, 21.
30 *BITKOM* 2010, 16.
31 *Reuter/Brix* 2012, 21.

SaaS schließlich beinhaltet die Bereitstellung von Software über eine Cloud-Anwendung. Dies bedeutet, dass das jeweilige Programm nur auf dem Rechner des Cloud-Diensteanbieters abläuft und bei dem Cloud-Nutzer nur angezeigt wird. Die Software kann dabei gleichzeitig von einer Vielzahl von Nutzern verwendet werden, ohne dass diese eine Programmkopie benötigen. Eine Vervielfältigung findet nicht statt. Hierunter wird die Mandantenfähigkeit der Anwendung verstanden.[32] Grundsätzlich ist dies bei jeder Art von Software vorstellbar. SaaS kann an weitere Leistungen gekoppelt sein. Werden mit dem Programm z. B. Daten verarbeitet, können diese in der Regel auch in der Anwendung – d. h. auf den Ressourcen des Anbieters – gespeichert werden. Dies beinhaltet zusätzlich die Leistung Storage as a Service (StaaS).

Mit der Bezeichnung X as a Service (XaaS) kommt schließlich zum Ausdruck, dass auch außerhalb der benannten Kategorien Cloud-Leistungen erbracht werden können.

2.1.4 Cloud-Strukturen

Cloud-Strukturen können danach unterteilt werden, wie viele Akteure involviert sind bzw. in welchem Verhältnis sie zueinander stehen. Variationen gibt es sowohl auf Anbieter- als auch auf Nutzerseite. In rechtlicher Hinsicht ist dies insbesondere für die Abgrenzung von Verantwortlichkeiten notwendig.

2.1.4.1 Basisstruktur

Der Basisstruktur von Cloud-Modellen liegt ein Zwei-Personen-Verhältnis zugrunde. Der Cloud-Diensteanbieter stellt einem Cloud-Kunden eine Applikation zur Verfügung, die dieser unmittelbar nutzt. Als Cloud-Kunde wird grundsätzlich derjenige bezeichnet, der die Nutzung des Cloud-Dienstes veranlasst, also regelmäßig in einem Vertragsverhältnis zu dem Cloud-Diensteanbieter steht. Im Zwei-Personen-Verhältnis ist auch der Cloud-Nutzer, derjenige, der die Cloud-Anwendung tatsächlich in Anspruch nimmt. Als Beispiel kann hier ein einfaches E-Mail-Programm genannt werden. Aber auch Anwendungen wie die iCloud[33] der Firma Apple erlauben es dem Kunden, unmittelbar Daten in dem Portal des Anbieters abzulegen und zu nutzen. Trotz des Zwei-Personen-Verhältnisses wird ein Cloud-Angebot von einer Vielzahl von Nutzern genutzt, die zwar in einer direkten Leistungsbeziehung mit dem Cloud-Diensteanbieter stehen, die sich aber des-

[32] *AG Rechtsrahmen des Cloud Computing* 2012a, 5 f.
[33] https://www.icloud.com/.

sen Ressourcen in physischer Hinsicht teilen, ohne notwendigerweise in einer Beziehung zueinander zu stehen.

2.1.4.2 Besonderheiten auf Cloud-Kunden-Seite/Cloud-Nutzer-Seite

Auf Kundenseite können mehrere Akteure involviert sein. So kann ein Cloud-Kunde Cloud-Ressourcen beim Cloud-Diensteanbieter abrufen, um diese Dritten zur Verfügung zu stellen bzw. diese mit Dritten zu teilen. Der Cloud-Kunde fungiert dann nicht mehr als alleiniger Nutzer, sondern als Administrator für weitere Nutzer. Ein Rechtsverhältnis zwischen dem weiteren Nutzer und dem Cloud-Diensteanbieter muss dabei nicht begründet werden. Vielmehr besteht auch in diesen Fällen ein vertragliches Verhältnis bezüglich der Cloud-Leistung zwischen dem Cloud-Kunden und dem Cloud-Diensteanbieter. Davon zu trennen ist das Verhältnis, in dem der Cloud-Kunde und die weiteren Nutzer zueinander stehen, das beispielsweise aus einer Kundenbeziehung, in einem Arbeits- oder Mitgliedsverhältnis oder in einem Verhältnis zwischen dem Bürger und einer öffentlichen Stelle bestehen kann.

Sowohl in Zwei- als auch in Mehr-Personen-Verhältnissen kann die Art der Nutzer variieren. Hierbei kann zunächst zwischen „B2C“[34], also dem Verkehr zwischen Unternehmer und Verbraucher, und „B2B“[35], dem Verkehr unter Unternehmern, unterschieden werden. Dabei gibt es Cloud-Angebote mit einem genauen Zuschnitt auf eine der beiden Gruppen und solche, die sich an beide richten. Schließlich kann die Cloud auch zur Abbildung eines Verhältnisses zwischen Bürgern und der öffentlichen Hand eingesetzt werden, soweit Letztere Cloud-Leistungen als Cloud-Kunde bezieht.

2.1.4.3 Besonderheiten aufseiten des Cloud-Diensteanbieters

Die Cloud-Anwendungen werden in Rechenzentren der Cloud-Diensteanbieter selbst oder von etwaigen Unterauftragnehmern, deren sich Cloud-Diensteanbieter zur Erbringung ihrer Leistungen bedienen, gehostet. Die jeweiligen Leistungen sind abhängig vom jeweiligen Cloud-Modell. Typisch für eine Cloud ist allerdings, dass sie auf unterschiedlichen Servern aufsetzt. In diesem Zusammenhang wird von „nicht eindeutig zugeordneten IT-Ressourcen“[36] gesprochen. In der so geschaffenen Infrastruktur können Daten jederzeit verschoben werden. Die Anwendungsoberfläche ist virtualisiert, d. h. von der da-

[34] Business-to-Customer.
[35] Business-to-Business.
[36] *BITKOM* 2010, 16.

runter liegenden physischen Ebene getrennt, sodass beim Nutzer ein virtueller, abgetrennter Raum entsteht.[37]

Auch wenn sich der Cloud-Diensteanbieter zur Erfüllung seiner Vertragspflichten häufig Unterauftragnehmern bedient, treten diese aber (zumindest rechtlich) regelmäßig nicht direkt gegenüber dem Cloud-Kunden auf. Dieser kann entweder die Cloud unmittelbar nutzen und/oder sie Dritten zur Verfügung stellen, beispielsweise für Mitarbeiter oder Kunden in einem Unternehmen oder für Mitglieder einer sonstigen Organisation (Community Cloud).

Vor allem auch im Zusammenhang mit Unterauftragnehmern muss beachtet werden, dass viele Cloud-Anwendungen aus den USA stammen, wo die Cloud-Anbieter und/oder deren Unterauftragnehmer ihre Rechenzentren betreiben. Zwar steigt die Anzahl der Rechenzentren in Europa,[38] allerdings ist es für Außenstehende häufig nicht erkennbar, ob amerikanische Unternehmen die Daten aus Europa auch tatsächlich in Europa verarbeiten. Um eine optimale Ressourcen-Auslastung zu erzielen, bietet sich eher ein flexibler Datentransfer zwischen den einzelnen Servern an.

Schließlich können unterschiedliche Service-Modelle eine unterschiedliche Verteilung der tatsächlichen Verantwortlichkeiten bedingen. So wird die „inhaltliche Gestaltung der Datenverarbeitung einerseits, die technische Steuerung andererseits, durch unterschiedliche Personen erbracht“[39]. In rechtlicher Hinsicht erfordert dieser Punkt ebenfalls besondere Beachtung, da er maßgeblich für die Ausgestaltung der Rechte und Pflichten der unterschiedlichen Akteure im Cloud Computing ist.

2.1.5 Ausgewählte Beispiele

Nach der Unterteilung von abstrakten Cloud-Modellen und Cloud-Strukturen sollen im Folgenden einige ausgewählte Beispiele der Veranschaulichung dienen. Dabei können die Modelle einmal von Anbieter- und einmal von Anwenderseite her betrachtet werden.

---

37 Vgl. *BIKOM* 2010, 16; *Hennrich* 2015, 63.
38 Dazu *Niemann/Hennrich,* CR 2010, 686, 687.
39 *AG Rechtsrahmen des Cloud Computing* 2012b, 5.

2.1.5.1 Cloud-Diensteanbieter

2.1.5.1.1 Amazon Cloud Drive, iCloud, Facebook[40]

Anwendungen wie Amazon Cloud Drive und iCloud haben zunächst gemeinsam, dass sie sich überwiegend an Verbraucher wenden. Diese mieten Speicherplatz beim Cloud-Diensteanbieter auf dessen Ressourcen bzw. denen des Unterauftragnehmers an und können dort Informationen in Datenform speichern und jederzeit abrufen. Dabei handelt es sich meistens um private Fotos, Videos, E-Mails etc. Die Dienste sind vornehmlich als Storage as a Service zu qualifizieren. Die Systeme beruhen auf einer Public Cloud, da der potenzielle Nutzerkreis nicht begrenzt ist.

Eine Besonderheit stellt das soziale Netzwerk Facebook dar, das im weiten Sinn ebenfalls als Cloud-Anwendung bezeichnet werden kann. Auch diese Plattform richtete sich primär an Verbraucher und ermöglicht es, Informationen über eine zentrale Plattform zu teilen. Ziel ist es zunächst, möglichst viele Nutzer zu vernetzen.

2.1.5.1.2 Salesforce[41]

Salesforce stellt seinen Kunden eine Plattform zur Verfügung, die es erlaubt, ein System mit weiteren Nutzern aufzusetzen. Dies soll unter anderem die unternehmensinterne Kommunikation verbessern. Die „Sales-Cloud“ ist dabei insbesondere auf das „Customer-Relationship-Management“ (CRM), das Kundenbeziehungsmanagement, zugeschnitten. CRM-Systeme haben das Ziel, Kundenverhalten möglichst umfangreich zu erfassen und zu analysieren. Die Mitarbeiter eines Unternehmens bzw. eines Konzerns erhalten einen Account auf der Plattform mit vielseitigen Funktionen, der es erlaubt, Kundendaten zu speichern und zu verwalten sowie mit Kunden und Mitarbeitern über Service- und Support-Tools zu kommunizieren. Ein wichtiger Bestandteil ist die integrierte E-Mail-Funktion. Dementsprechend werden dort große Datenmengen verwaltet, diese dürfen nur dem Zugriff von Berechtigten unterliegen. Die Dienste werden Software as a Service und Platform as a Service zugeordnet.[42] Wenn die Cloud-Anwendung nur von einem bestimmten Personenkreis genutzt werden kann, ist sie zusätzlich als Community Cloud zu qualifizieren.

---

[40] S. https://www.amazon.de/clouddrive/; http://www.apple.com/de/icloud/; https://www.facebook.com/.

[41] S. http://www.salesforce.com/de/#more.

[42] http://de.wikipedia.org/wiki/Salesforce.com.