ISPRAT
Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie e.V.

Datenhoheit in der Cloud

Studie

Pino Bosesky, Peter H. Deussen, Anne Quandt, Sönke E. Schulz, Linda Strick

Fraunhofer FOKUS

Datenhoheit in der Cloud

Studie

Pino Bosesky, Peter H. Deussen,
Anne Quandt, Sönke E. Schulz,
Linda Strick

Zusammenfassung

Die umfassende Digitalisierung von Daten, die alle Lebensbereiche des Bürgers betreffen, betrifft insbesondere auch die Interaktion von Bürgern, Firmen und Verwaltungen. Aktuell diskutierte Ansätze des Datentransfers zwischen diesen Parteien laufen meist auf eine zentrale Speicherung von Daten durch die Behörde hinaus. Die grundsätzliche Fragestellung, wie die Hoheit des Bürgers über seine Daten sichergestellt werden kann, ist bisher nicht ausreichend beantwortet.

Denn informationelle Selbstbestimmung erfordert, dass die rechtlich bedenkliche Speicherung von Daten auf den bloßen Verdacht der späteren Nutzung für behördliche Zwecke durch andere, datenschutzrechtlich konforme Mechanismen ersetzt wird. Ein Paradigmenwechsel zur Datenfreigabe durch den Bürger ist erforderlich, der durch konkrete, für den Bürger verfügbare technische Konzepte sichergestellt werden muss.

Die Nutzung öffentlicher Cloud-Dienste wird angesichts vieler Unsicherheiten nur zögerlich umgesetzt. Cloud Computing offeriert aber auch das Potenzial, Bürgerdaten unter der Kontrolle des Bürgers zu speichern und kann somit als technologische Umsetzung des Prinzips »Datenhoheit« verstanden werden.

Die vorliegende Studie befasst sich mit den rechtlichen Rahmenbedingungen sowie technischen Lösungskonzepten und untersucht beispielhaft anhand vorhandener Projekte die rechtlichen und technisch-organisatorischen Aspekte, die die individuelle Datenhoheit betreffen, und deren Auswirkung auf die Speicherung der personenbezogenen Daten und Informationen in einer öffentlichen Cloud.

Inhaltsverzeichnis

1 Einleitung

Cloud-Technologien halten zunehmend Einzug in die alltägliche Arbeits- und Lebenswelt des Einzelnen. Die Speicherung unter Nutzung von Virtualisierungstechniken entbindet einerseits von dem Erfordernis, individuelle Infrastrukturen vorzuhalten und eigene Datenschutz- und Datensicherungsmaßnahmen zu ergreifen. Andererseits kann der Datenaustausch »über die Cloud« in Form von Freigabe- und Abruffunktionen die bestehenden Kommunikationsprozesse mit Behörden und Unternehmen nachhaltig erleichtern. Gerade der Privatnutzer wird diese Möglichkeiten jedoch nur nutzen, wenn er sicher sein kann, »Herr seiner Daten zu bleiben«. Die **individuelle Datenhoheit** ist also ein Kernelement, welches es technisch-organisatorisch als auch rechtlich zu erfassen und zu sichern gilt.

Elektronische Safes – in der Regel derzeit noch als Online-Festplatte oder Webspace betitelt und mit begrenzten Funktionalitäten ausgestattet – sind keine völlig neue Entwicklung. Sie werden auch insbesondere von Unternehmen im Zuge der Verbreitung der Cloud-Technologien in zunehmendem Umfang genutzt. Ein wirklicher **Zusatznutzen** ist mit derartigen Systemen aber erst verbunden, wenn es einerseits ermöglicht wird, dass anderen Nutzern (bspw. Banken, Versicherungen oder staatlichen Behörden) gezielt **Zugriff auf einzelne Dokumente** bzw. perspektivisch strukturierte Daten erteilt werden kann. Andererseits muss ein elektronischer Safe technisch-organisatorisch die Vertraulichkeit der Daten gewährleisten (bspw. durch den Einsatz von Verschlüsselungstechnologien sowohl auf Client- als auch auf Providerseite oder die Einbindung neutraler vertrauensvoller Dritter im Sinne einer »Trusted Third Party«).

Eine in der Cloud realisierte elektronische Datenablage entbindet den Einzelnen von der Vorhaltung eigener Infrastrukturen. Die einmalige Registrierung reicht aus, um die gewünschten Kapazitäten im Bedarfsfall zu buchen und auf diese binnen kurzer Zeit von einer beliebigen »Basisstation«[1] aus zuzugreifen.[2] Bereitgestellte Software nutzt der Anwender sodann einfach über seinen Internetbrowser, wodurch bspw. auch die Möglichkeit eröffnet ist, Dokumente mit einem über die ganze Welt verstreuten Nutzerkreis kollaborativ zu bearbeiten.[3]

---

1 Auf Seiten des Nutzers wird perspektivisch nicht einmal ein PC im klassischen Verständnis erforderlich sein; es bedarf lediglich eines breitbandigen Zugangs zum Internet, Zwischenspeichermedien und Anzeige- sowie Bedienvorrichtungen.

2 Pohle/Ammann, CR 2009, 273 (273).

3 Pohle/Ammann, CR 2009, 273 (273).

Der Umstand, dass die Daten von jedem Ort, zu jeder Zeit und von jeder Person (bzw. Organisationseinheit) erreicht werden können, bietet eine Option für die **grundlegende Veränderung von Kommunikationsprozessen,** die bisher – auch im elektronischen Zeitalter – noch auf dem Prinzip »Senden – Empfangen« basieren. Die Cloud ermöglicht demgegenüber Zugriffe Dritter auf die unverändert am gleichen physischen Speicherort liegenden Dateien. Der Dritte kann sich die Daten herunterladen, in Betracht kommt es aber auch, dass nicht einmal eine Kopie erstellt wird, sondern sich der Zugriff im lesenden Zugriff, gleichsam der Vorlage eines Dokumentes, erschöpft. Derartige Kommunikationsanlässe bestehen sowohl im Kontakt mit Behörden als auch mit privaten Unternehmen. Das Bedürfnis, so zu kommunizieren, wird zunehmen, je mehr wichtige Dokumente – Zeugnisse, Bescheide, Rechnungen u. v. m. – perspektivisch ausschließlich elektronisch oder als strukturierter XML-Datensatz[4] vorliegen. Diese ließen sich über ein intelligentes digitales Rechtemanagement[5] gezielt für einzelne Verwaltungs- oder Geschäftsprozesse freigeben.

Auch zahlreiche aktuelle Projekte zeigen das Bedürfnis, die Austauschprozesse zwischen Bürgern bzw. Unternehmen und staatlichen Stellen auf eine andere Grundlage zu stellen:

- Der sog. **Prozessdatenbeschleuniger** (kurz: P23R[6]) stellt ein Infrastrukturkonzept dar, auf dessen Grundlage Unternehmen ihre gesetzlichen Informations- und Meldepflichten in einer abgesicherten Umgebung effizient erfüllen können. Lösungen auf Basis des P23R-Prinzips generieren die erforderlichen Meldungen und stellen sie den zuständigen Behörden ordnungsgemäß zu. Dabei liegen die Daten **beim Unternehmen selbst** bzw. bei einem von diesem beauftragten Dritten; sie werden nicht »auf Vorrat« an staatliche Stellen übermittelt.
- **§ 8 DeMailG**[7] normiert die Option für De-Mail-Anbieter, auch eine sichere Dokumentenablage anzubieten. Eine Freigabefunktion ist nicht angelegt, aber durchaus perspektivisch denkbar und – soweit ersichtlich – auch nicht vom gesetzlichen Rahmen ausgeschlossen. Gerade diese Variante, die Speicherung von Daten **bei einem privaten vertrauenswürdigen Diensteanbieter,** dürfte für Privatpersonen besondere Attraktivität besitzen, zumal derartige Dienste zunehmend auch Einzug in den Alltag halten (iCloud, TelekomCloud usw.).

---

4 XML steht für »eXtensible Markup Language« und ist sowohl ein Datenformat als auch eine Metasprache zur Beschreibung der formalen Eigenschaften eines Textes. XML kann Metadaten wie bspw. Versionsinformationen oder selbstdefinierte Indexwerte beinhalten und eignet sich daher zur Kommunikation zwischen verschiedenen Anwendungen.

5 Digitales Rechtemanagement (DRM) ist ein Sammelbegriff für alle technischen Maßnahmen zur digitalen Kontrolle von Urheber- bzw. Verwertungsrechten an digitalen Inhalten aller Art. Grundprinzip ist die Markierung und/oder Verschlüsselung mit der Konsequenz der Einschränkung von Nutzung und Weitergabe. Die Markierung erfolgt durch sog. digitale Wasserzeichen, die sichtbar oder unsichtbar sein können. Die Verschlüsselung geht mit einer Chiffrierung einher, die nur mit einem passenden Schlüssel überwunden werden kann. Entsprechende Schlüssel können soft- oder hardwarebasiert sein. Systeme für den digitalen Rechteschutz (DRM-Systeme) verfügen im Allgemeinen über vier grundlegende Funktionsbereiche: Zugangssteuerung, Nutzungssteuerung, Abrechnung sowie Verfolgung von Rechtsverletzungen; vgl. Siepermann, Stichwort: Digital Rights Management, in: Gabler Verlag (Hrsg.), Gabler Wirtschaftslexikon, abrufbar unter www.wirtschaftslexikon.gabler.de/.

6 Weitere Informationen auf www.p23r.de/; zu den wissenschaftlichen Grundlagen Krcmar, in: Schliesky/Schulz (Hrsg.), Die Erneuerung des arbeitenden Staates, 2012, S. 31 ff.; Schilling u. a., in: Brüggemeier/Lenk (Hrsg.), Bürokratieabbau im Verwaltungsvollzug, 2011, S. 179 ff.

7 BGBl I, S. 666; dazu Rose, K&R 2011, 439 ff.; Roßnagel, NJW 2011, 1473 ff.; Spindler, CR 2011, 309 ff.

- ELENA[8] bzw. das Nachfolgeprojekt **»OMS«**[9] setzen hingegen auf eine **zentrale Datenspeicherung** bei derjenigen Stelle (hier: dem Staat), die anlassbezogen auf bestimmte Informationen zugreifen muss. Auch diese Option sollte nicht vernachlässigt werden, da zwar einerseits eine Datenhaltung »auf Vorrat« – mit den damit verbundenen rechtlichen Bedenken[10] – erfolgt, andererseits die betroffenen Privaten aber von der Vorhaltung eigener Strukturen (wie bei P23R) entbunden werden. Die Mehrfachnutzung beim Staat vorhandener Daten kann gerade für Privatpersonen eine Erleichterung darstellen[11] und stellt nicht zwangsläufig eine größere Gefährdung für die Datenhoheit dar als die vorgenannten Varianten, wenn – wie bspw. in § 5 Abs. 2 des Entwurfes eines E-Government-Gesetzes des Bundes vorgesehen[12] – explizit das Einverständnis zur Weitergabe abgefragt wird.
- Die **elektronische Gesundheitskarte** (eGK) soll ein vernetztes Datenmanagement im Gesundheitswesen ermöglichen. Zudem ist sie eingebettet in die Entwicklung einer Kommunikationsinfrastruktur, die gesicherte und vertrauliche Kommunikationsmöglichkeiten schafft.[13] In das Kartenlesegerät werden die elektronische Gesundheitskarte und der elektronische Heilberufsausweis (HBA) eingelesen und der »Konnektor« verbindet die Praxis online mit den Servern der Telematik-Infrastruktur, auf denen die Patientendaten liegen.[14] Zusätzlich muss vom Patienten eine PIN-Nummer eingegeben werden. Kerngedanke ist – wie bei OMS –, dass die Daten zwar nicht auf Vorrat bei all denjenigen Stellen liegen, die diese ggf. anlassbezogen benötigen (hier: den Ärzten), diesen aber auf einfache und effektive Weise unter Mitwirkung des Betroffenen (PIN-Eingabe) Zugriff auf einen zentralen Datenbestand gewährt werden kann.

Deutlich wird, dass den genannten Projekten im Wesentlichen **drei unterschiedliche Grundmodelle** zugrunde liegen: die unmittelbare Vorhaltung der ggf. erforderlichen Daten bei staatlichen Stellen (OMS und eGK), beim Bürger/Unternehmen selbst (P23R) oder bei einer vertrauenswürdigen dritten Instanz (De-Safe oder andere sichere Cloud-Angebote mit Freigabefunktion). Alle verfolgen jeweils die gleiche Zielsetzung, nämlich den Datenaustausch zwischen Bürger/Unternehmen und staatlichen Stellen zu erleichtern, sodass die Varianten zumindest partiell als **austauschbare Äquivalente** zu betrachten sind. Diesen Umstand muss eine Analyse, was Datenhoheit des Einzelnen in einer veränderten Kommunikationsumgebung bedeutet, berücksichtigen.

---

8 ELENA steht für »Elektronisches Entgeltnachweis-Verfahren«.

9 OMS steht für »Optimiertes Meldeverfahren in der sozialen Sicherung«.

10 Zur Vorratsdatenspeicherung statt Vieler BVerfGE 125, 260 ff.; zu den diesbezüglichen Bedenken gegenüber ELENA und vergleichbaren Projekten Hilderink/Paatz, AuA 2010, 48 ff.; das erwähnte Spannungsfeld bringt Wedde, ArbuR 2010, 94 ff., zutreffend zum Ausdruck: »ELENA – Meilenstein auf dem Weg zum Bürokratieabbau oder Stolperstein für das Persönlichkeitsrecht?«.

11 Die Nutzung bereits beim Staat (unabhängig davon, bei welcher Ebene) vorhandener Daten ist nämlich als »milderes Mittel« zu charakterisieren, auf das vorrangig zurückgegriffen werden muss; so zutreffend Schliesky, in: Knack/Henneke (Hrsg.), VwVfG Kommentar, 9. Aufl. 2010, § 3a Rn. 18.

12 Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) sowie zur Änderung weiterer Vorschriften, BT-Drs. 17/11473 v. 14. 11. 2012; weitere Informationen abrufbar unter www.bmi.bund.de/; dazu Müller-Terpitz/Rauchhaus, MMR 2013, 10 ff.

13 Wirtz/Ullrich/Mory, e-Health – Akzeptanz der elektronischen Gesundheitskarte, 2008, S. 16; Dietzel, in: Jähn/Nagel (Hrsg.), e-Health, 2004, S. 2 (2 f.).

14 Lücke/Köhler, Dtsch Med Wochenschrift 2007, 448 (449).

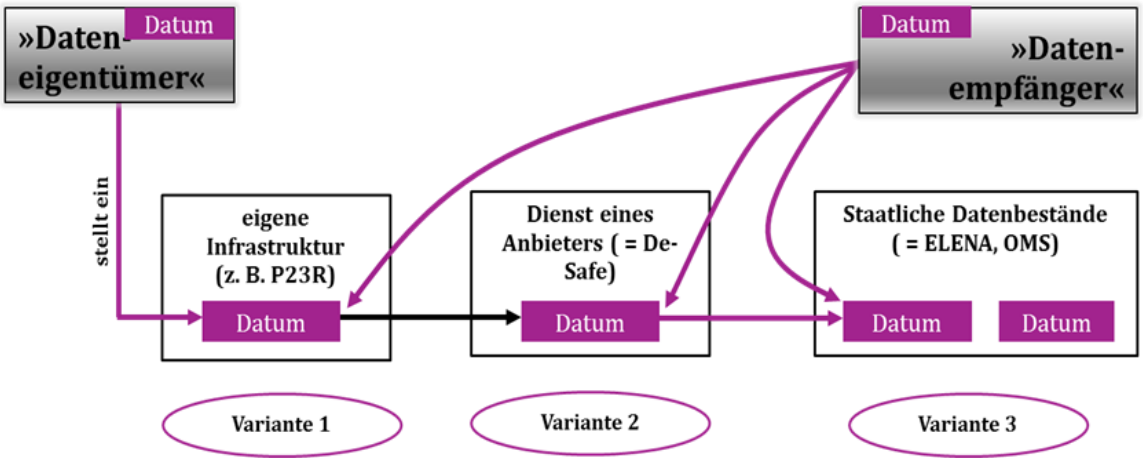

ABBILDUNG 1: DREI UNTERSCHIEDLICHE GRUNDMODELLE

2 Begriffsbestimmungen

Will man sich den rechtlichen und technisch-organisatorischen Anforderungen von Konzepten nähern, die die Datenhoheit des Einzelnen in der Cloud zu sichern suchen, muss zunächst eine Begriffsklärung erfolgen. Kernbegriff, der nicht ohne Berücksichtigung seiner rechtlichen Hintergründe definiert werden kann, ist insofern die **»Datenhoheit«** (2.1).

Demgegenüber ist die **»Cloud«** eher außerrechtlich aufgrund tatsächlicher Angebote zu konkretisieren, wobei – dies zeigen bereits die genannten Beispiele (1) – ein weites Verständnis zugrunde gelegt werden soll (2.2).

2.1 Datenhoheit

Der Begriff der Datenhoheit[15] wird zwar häufig gebraucht,[16] eine zufriedenstellende Definition ist jedoch – soweit ersichtlich – bisher ebenso wenig erfolgt wie eine Benennung einzelner Bestandteile. Im Folgenden soll daher der Versuch unternommen werden, den Begriff der (individuellen) Datenhoheit zu bestimmen, um so die erforderlichen Grundbedingungen und die Anforderungen an Cloud-Services zu definieren, damit der Privatnutzer bei deren Verwendung »Herr seiner Daten« bleibt.

2.1.1 Erste Ansätze einer Begriffsbestimmung

Obwohl eine eingehende Untersuchung des Begriffs »Datenhoheit« bislang noch nicht vorgenommen worden ist, gibt es in Literatur, Rechtsprechung und Normen durchaus Ansätze, anhand derer man sich einer Klärung des Begriffs nähern könnte.

---

15 Mitunter ist auch von der sog. Datenherrschaft die Rede; vgl. Heckmann, in: Hill/Schliesky (Hrsg.), Innovationen im und durch Recht, 2010, S. 97 (110); ders., NJW 2012, 2631 (2633). Das dürfte jedoch in der Sache keinen Unterschied machen.

16 Vgl. nur Luch, MMR 2011, 75 (76); Klostermeier, Ein Prozessdatenbeschleuniger soll helfen – Bitkom rügt Unternehmen, abrufbar unter www.cio.de/public-ict/2305883/index2.html/; v. Liere, Könige der Datenhoheit, abrufbar unter www.spiegel.de/spiegel/unispiegel/d-75662512.html/; Friedmann, Gartner definiert Rechte und Pflichten – Spielregeln in der Cloud, abrufbar unter www.cio.de/dynamicit/bestpractice/2243853/.

Explizit verwendet wird der Begriff der Datenhoheit in der Überschrift von Art. 13 des Beschlusses 2009/917/JI des Rates vom 30. 11. 2009 über den Einsatz der Informationstechnologie im Zollbereich. Danach ist nur der Daten eingebende Mitgliedstaat befugt, die jeweils von ihm in das Zollinformationssystem eingegebenen Daten zu ändern, zu ergänzen, zu berichtigen oder zu löschen. Daraus ließe sich schließen, dass stets demjenigen die Datenhoheit zukäme, der die beschriebene Befugnis zur Änderung, Ergänzung, Berichtigung oder Löschung inne hat. Das wäre im Rahmen von Art. 13 Abs. 1 des Beschlusses der jeweilige Mitgliedstaat. Gegen ein solches Verständnis der Datenhoheit spricht jedoch, dass die Daten von Bürgern in der Regel personenbezogen sind. Dann ist aber zugleich das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG) betroffen. Dieses würde jedoch ausgehöhlt, wenn ein Mitgliedstaat der Europäischen Union allein aufgrund der Eingabe von Daten des Bürgers in ein Informationssystem die Hoheit über sie erlangen könnte. Der Bürger muss die vollständige Herrschaft über die Zugriffsberechtigung und Verwendung der Daten behalten, da nur dann von einer »Hoheit« im Sinne einer vollständigen Herrschaft die Rede sein kann. Würde man die Datenhoheit in dem soeben beschriebenen Sinne verstehen, könnte der Bürger seine Datenhoheit durch eine **rein tatsächliche Handlung** – nämlich die Eingabe in das Zollinformationssystem – zumindest teilweise verlieren und zwar gegen oder ohne seinen Willen. Zudem hingen der Erwerb und der Verlust der Datenhoheit von der als zufällig erscheinenden Eingabe in das Zollinformationssystem ab.

Ein anderes Verständnis des Begriffs »Datenhoheit« geht dahin, diese dann anzunehmen, »wenn das jeweils genutzte informationstechnische System entweder das eigene ist oder ein fremdes, bei dem der Nutzer von einem **alleinigen Zugriffsrecht** unter Ausschluss nicht autorisierter Dritter ausgehen darf«.[17] Entscheidend sei demnach die berechtigte Vertraulichkeitserwartung des jeweiligen Nutzers, die aus der Beherrschbarkeit des jeweiligen Systems folgt. Es gilt jedoch zu beachten, dass sich der aufgezeigte Ansatz in erster Linie auf informationstechnische Systeme bezieht. In diesem Zusammenhang ist die berechtigte Vertraulichkeitserwartung durchaus das richtige Kriterium zur Bestimmung der Datenhoheit. Was aber die im System enthaltenen Daten des Bürgers anbelangt, wird für eine vollständige Herrschaft (im Sinne einer Datenhoheit) mehr zu verlangen sein als eine bloße Vertraulichkeitserwartung. Vielmehr geht es neben dem Ausschluss unberechtigter Zugriffe auch um Datensicherheit und Datenschutz.

Des Weiteren wird zur Klärung des Begriffs »Datenhoheit« vorgeschlagen, diesen als Ausschluss des Missbrauchs von Daten zu verstehen. Datenhoheit werde durch die Verhinderung des Missbrauchs von Daten erreicht.[18] Das ist zwar grundsätzlich richtig, aber doch so vage, allgemein und unpräzise, dass darin keine ernsthafte Bestimmung des Begriffs »Datenhoheit« gesehen werden kann. Offen bleibt vor allem, wann ein Datenmissbrauch in diesem Sinne vorliegen soll. Datenhoheit könne daher insbesondere durch **»privacy by trust«**, also vertrauensbildende Maßnahmen hinsichtlich der technisch-organisatorischen Ausgestaltung des jeweiligen Systems, hergestellt werden.[19] Bloßes Vertrauen in ein System führt jedoch nicht zu einer faktischen Hoheit über die Daten; vielmehr sind technisch-organisatorische Maßnahmen bzw. die Verpflichtung, solche zu ergreifen, weniger begrifflich prägend als vielmehr Rechtsfolge einer anderweitig zu definierenden Datenhoheit.

---

17 So Luch, MMR 2011, 75 (76); BVerfGE 120, 274 (315), anstelle von »Datenhoheit« den Begriff »Verfügungsgewalt« verwendend.

18 Heckmann, NJW 2012, 2631 (2633).

19 Heckmann, NJW 2012, 2631 (2634).

2.1.2 Eigener Ansatz zur Begriffsbestimmung

Einen ersten Hinweis auf die Bedeutung des Wortes »Datenhoheit« erhält man, wenn man dieses in seine beiden Bestandteile »Daten« und »Hoheit« trennt und sich deren Bedeutung etymologisch nähert. Demnach sind **Daten** dem ursprünglichen lateinischen Wortsinn nach beliebige Angaben.[20] Heute werden Daten allgemein als zum Zwecke der Verarbeitung zusammengefasste Zeichen verstanden, die aufgrund bekannter oder unterstellter Abmachungen Informationen (d. h. Angaben über Sachverhalte und Vorgänge) darstellen.[21] Ebenso wird der Datenbegriff in der strafrechtlichen Literatur zu § 202a Abs. 2 StGB definiert.[22] Das Wort »Hoheit« beschreibt unter anderem eine unabhängige Gewalt, mithin eine Herrschaft.[23] Damit ist bereits klar, dass mit Datenhoheit eine irgendwie geartete Gewalt über Informationen gemeint ist. Wie diese konkret ausgestaltet sein muss, damit von einer Datenhoheit gesprochen werden kann, wird im Folgenden näher untersucht.

2.1.2.1 Datenverfügbarkeit

Um von einer wirklich unabhängigen Gewalt über Daten sprechen zu können, ist es zunächst unerlässlich, dass der jeweilige Datenbetroffene jederzeit auf seine Daten zugreifen kann. Ohne diese ständige Verfügbarkeit könnte der Datenbetroffene nicht so mit ihnen verfahren, wie er es wünscht. Dann wäre der Umgang mit den Daten jedoch fremdbestimmt. Von einer unabhängigen Gewalt oder Herrschaft über die personenbezogenen Daten könnte dann nicht mehr die Rede sein.

> ***Schlussfolgerungen für die Ausgestaltung von Cloud-Diensten***
>
> Bezogen auf Cloud-Dienste bedeutet dies, dass der Datenbetroffene die Möglichkeit haben muss, ständig auf die Daten zuzugreifen, bspw. unabhängig davon, wer das System betreibt, wo dieses gelegen ist oder wer zur selben Zeit auch noch auf die Informationen zugreifen möchte. Eine hohe – über Service Level Agreements (SLAs) abgesicherte – Verfügbarkeitszusage eines Drittbetreibers ist ein denkbares Realisierungsmittel und auch bei staatlichen Stellen vorgehaltene Datenbestände müssen diesen Anforderungen genügen, auch wenn hier zivilrechtliche Sanktionsmechanismen nicht greifen.

2.1.2.2 Umfassende Verfügungsbefugnis

Gemäß Art. 17 des Entwurfs der Europäischen Kommission für eine Europäische Datenschutz-Grundverordnung vom 25. 01. 2012[24] kann eine Person eine andere Person oder Institution, die ihre Daten inne hat, verbindlich dazu veranlassen, alle sie betreffenden Daten zu löschen

---

20 Ronellenfitsch, in: Wolff/Brink (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht (Ed. 1, 01. 08. 2012), Einleitung zum BDSG Rn. 1.

21 Wohltmann/Lackes/Siepermann, Stichwort: Daten, in: Gabler Verlag (Hrsg.), Gabler Wirtschaftslexikon, abrufbar unter www.wirtschaftslexikon.gabler.de/.

22 Vgl. nur Kargl, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Strafgesetzbuch, 3. Aufl. 2010, § 202a Rn. 4.

23 Duden, Stichwort: Hoheit, in: Das Bedeutungswörterbuch, 2. Aufl. 1985.

24 KOM(2012) 11 endgültig; dazu statt Vieler Hornung, ZD 2012, 99 ff.; v. Lewinski, DuD 2012, 564 ff.; Eckhardt, CR 2012, 95 ff.

und deren weitere Verbreitung zu verhindern.[25] Dieses **»Recht auf Vergessenwerden«** wird aus einer umfassenden Verfügungsbefugnis einer Person über ihre Daten abgleitet.[26] Ohne eine umfassende Verfügungsbefugnis, die es dem Datenbetroffenen erlaubt, Dritte im Umgang mit den sie betreffenden Daten zu unterweisen, wird man kaum von einer »Hoheit« im Sinne einer unabhängigen Gewalt über personenbezogene Daten sprechen können. Insofern ist die umfassende und uneingeschränkte Verfügungsbefugnis über diese ebenfalls ein Bestandteil der Datenhoheit.

> ***Schlussfolgerungen für die Ausgestaltung von Cloud-Diensten***
>
> Bezogen auf Anwendungen in der Cloud bedeutet dies, dass alle datenrelevanten Handlungen – insofern kann eine Anlehnung an die Begriffsbestimmungen in § 3 Abs. 4 BDSG erfolgen –, also das Speichern, Verändern, Übermitteln, Sperren und Löschen, jeweils vom Datenbetroffenen legitimiert werden müssen. Dies gilt für Handlungen des Providers, für die der jeweilige Vertrag auch die datenschutzrechtliche Einwilligung zum Speichern darstellt, ebenso wie für Freigabefunktionen, bei denen bspw. sichergestellt werden muss, dass tatsächlich nur Berechtigte Zugriff erhalten.

2.1.2.3 Recht auf informationelle Selbstbestimmung

Aus den vorstehenden Erörterungen wird ersichtlich, dass man bei der Bestimmung des Begriffs der Datenhoheit nicht umhin kommt, auch das Recht auf informationelle Selbstbestimmung als Ausgangspunkt für die Definition und Begriffsbestimmung zu wählen. Dies liegt nicht zuletzt daran, dass die Daten, die der Bürger in Cloud-Anwendungen transferiert, in aller Regel einen Personenbezug aufweisen.

Das Recht auf informationelle Selbstbestimmung schützt den Einzelnen vor einer unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten.[27] Insofern gewährleistet es die Befugnis des jeweiligen Grundrechtsträgers, selbst über die Veröffentlichung und Verwendung seiner personenbezogenen Daten zu bestimmen.[28] Das Recht auf informationelle Selbstbestimmung umfasst folglich »die aus dem Gedanken der Selbstbestimmung folgende Befugnis des einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden«.[29] Beim Recht auf informationelle Selbstbestimmung handelt es sich somit um ein Selbstbestimmungsrecht über personenbezogene Daten.[30] Ein Eingriff durch einen Akt der Datenerhebung scheidet jedoch dann aus, wenn die betreffende Information aus allgemein zugänglichen Quellen stammt.[31] Im Kern geht es bei der informationellen Selbstbestimmung somit um Datenvertraulichkeit und Datenschutz. Diese schützen die Daten des Bürgers sowohl im gespeicherten Zustand als auch während der Übertragung. Der Bürger muss die

---

25 Gstrein, ZD 2012, 424 (425).

26 Gstrein, ZD 2012, 424 (424).

27 Starck, in: v. Mangoldt/Klein/Starck, GG, Kommentar, Bd. 1, 6. Aufl. 2010, Art. 2 Rn. 114; Murswiek, in: Sachs (Hrsg.), Grundgesetz, Kommentar, 4. Aufl. 2007, Art. 2 Rn. 72.

28 Murswiek (Fn. 27), Art. 2 Rn. 72.

29 BVerfG, NJW 1984, 419 (421).

30 Di Fabio, in: Maunz/Dürig, Grundgesetz-Kommentar, Loseblatt-Sammlung (65. Erg.-Lieferung, 2012), Art. 2 Rn. 175.

31 Di Fabio (Fn. 30), Art. 2 Rn. 176.

Möglichkeit haben, jeden Zugriff auf seine Daten abzuwehren bzw. diesen zu legitimieren und Berechtigte festzulegen.

Hieraus folgt, dass es der Bürger als Inhaber des Rechts auf informationelle Selbstbestimmung und damit als Träger der Datenhoheit allein in der Hand haben muss, welche seiner personenbezogenen Daten preisgegeben werden und welche nicht. Zugriffe auf die Daten und die Verwendung derselben müssen stets durch ihn legitimiert werden (rechtlich). Unberechtigte Zugriffe müssen wirksam verhindert werden (technisch-organisatorisch). Im Kern geht es beim Recht auf informationelle Selbstbestimmung also um die **vollständige Entscheidungsfreiheit** im Hinblick auf die persönlichen Daten der Bürger.

> ***Schlussfolgerungen für die Ausgestaltung von Cloud-Diensten***
>
> Bezogen auf Cloud-Anwendungen folgt daraus zunächst eine Wahlfreiheit, ob der Bürger seine personenbezogenen Daten überhaupt in eine Cloud-Computing-Anwendung übermittelt. Falls er sich dafür entscheidet, so bezieht sich die Wahlfreiheit in einem zweiten Schritt auch darauf, welches der drei Grundmodelle (eigene IT-Infrastruktur, sichere Cloud-Dienste Dritter oder die Speicherung beim Datenempfänger) er verwendet.
>
> Darüber hinaus besitzt der Bürger die Freiheit, den Zugriff auf die Daten zu regeln. Bei Cloud-Anwendungen ohne eine spezifische Datenfreigabefunktion liegt auf der Hand, dass sichergestellt sein muss, dass Dritte nicht auf die in der Cloud gelagerten Daten zugreifen können. Im Zusammenhang mit Cloud-Anwendungen mit einer spezifischen Datenfreigabefunktion muss bei allen drei Modellen der Zugriff auf die Daten grundsätzlich ausgeschlossen sein. Der Inhaber des Rechts auf informationelle Selbstbestimmung kann jedoch den Zugriff Dritter auf die Daten legitimieren, sodass Dritte als Berechtigte auf die Daten zugreifen können. Die aus dem Recht auf informationelle Selbstbestimmung folgende Entscheidungsfreiheit wirkt sich hier so aus, dass der Inhaber dieses Rechts allein festlegen darf, wer in welchem Umfang auf welche Daten zugreifen darf.
>
> Zur rechtlichen Erfassung der denkbaren Konstellationen erscheint eine **Differenzierung zwischen staatlichen Zugriffen, Zugriffen des Providers und Drittzugriffen** sachgerecht. Sofern der Anbieter eines Cloud-Dienstes oder ein Dritter – etwa im Rahmen eines Vertragsverhältnisses – vom Safe-Nutzer die Einwilligung zu einer Erhebung, Verarbeitung oder Nutzung der Daten einfordert, sind die einfachgesetzlichen Vorgaben des § 4a BDSG zu beachten, insbesondere die Freiwilligkeit und die Schriftform der Einwilligung.

2.1.2.4 Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Die Datenhoheit erschöpft sich jedoch nicht in der umfassenden Verfügbarkeit, der Verfügungsbefugnis und der Datenvertraulichkeit, sondern geht noch darüber hinaus. Auch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme leistet seinen Beitrag zur Datenhoheit.[32] Es ist gleichsam die Voraussetzung des Schutzes der in einem informationstechnischen System gelagerten Daten. Sofern eine Infiltration des Systems ohne gleichzeitige Kenntnisnahme der darin gelagerten Daten stattfindet, ist

[32] Vgl. dazu Luch, MMR 2011, 75 ff.

die Vertraulichkeit des Systems betroffen. Unter der »Integrität« eines informationstechnischen Systems ist die **Unversehrtheit** desselben vor Ausspähung, Überwachung und Manipulation durch Dritte zu verstehen.[33] Der Integritätsschutz ist folglich so zu verstehen, dass **keine Möglichkeit der Veränderung** besteht.[34] Erst wenn auch dies sichergestellt ist, sind die in einem informationstechnischen System – etwa einer Cloud – gelagerten Daten in einem umfassenden Sinne geschützt.

> ***Schlussfolgerungen für die Ausgestaltung von Cloud-Diensten***
>
> Für Cloud-Anbieter bedeutet dies, dass sie ihren Nutzern diese Integrität zusichern müssen – auch wenn keine unmittelbare Verpflichtung dazu besteht, sondern die Grundrechte im Verhältnis zwischen Privaten nur über eine mittelbare Drittwirkung zur Geltung kommen. So kann die Rechtsordnung bspw. Vertragsbestimmungen, die den Anbieter aus der Verantwortung für die Integrität entlassen, obwohl der Nutzer (mangels Zugriffsmöglichkeit auf die IT-Systeme) keinerlei Möglichkeiten des Eigenschutzes hat, rechtliche Wirkungen versagen. Insofern ist ggf. eine staatliche Schutzpflicht zu aktivieren.

Fraglich ist in diesem Kontext jedoch, wie die **Abgrenzung** zwischen dem Recht auf informationelle Selbstbestimmung und dem ebenfalls aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG) abgeleiteten Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vorzunehmen ist. Auch Letzteres schützt nämlich die Datenvertraulichkeit in dem Sinne, dass kein Zugriff Unbefugter auf die in einem System verfügbaren Daten stattfinden darf.[35] Das richtige Abgrenzungskriterium ist im Vorliegen einer Infiltration des jeweiligen Systems zu sehen.[36] Liegt eine bloße Infiltration des Zielsystems vor, so ist allein das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme betroffen.[37] Sobald aber personenbezogene Daten vom PC, aus einem elektronischen Daten- und Dokumentensafe oder einer Cloud von Dritten auch zur Kenntnis genommen werden, ist das Recht auf informationelle Selbstbestimmung zusätzlich tangiert.[38]

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfüllt daher einen vergleichbaren **»Infrastruktur- und Systemschutz«** wie Art. 10 GG (und bspw. auch Art. 13 GG). Auch hier findet im Interesse der auf diesen Systemen befindlichen (personenbezogenen) Daten eine Vorverlagerung der Schutzwirkungen der Grundrechte auf die Infrastruktur selbst statt. Nach dem BVerfG wird der Schutzbereich des IT-Grundrechts mit dem Interesse des Nutzers umschrieben, dass die von einem (vom Schutzbereich erfassten) informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff sei zudem anzunehmen, wenn die Integrität des Systems angetastet wird, indem so auf das System zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann sei die entscheidende Hürde für eine Ausspähung, Überwachung und Manipulation des Systems genommen. Aus dieser Herleitung lässt sich dann auch das Verhältnis der Grundrechte zueinander erklären. Das **Verhältnis zwischen Systemschutz und dem Schutz der Inhalte**

---

33 BVerfGE 120, 274 (314).

34 Hoffmann, Die Gewährleistung der Vertraulichkeit und Integrität elektronischer Daten- und Dokumentensafes, 2012, S. 87.

35 Hoffmann (Fn. 34), S. 86.

36 Hoffmann (Fn. 34), S. 80, 93.

37 Vgl. Pieroth/Schlink, Grundrechte, Staatsrecht II, 26. Aufl. 2010, Rn. 400.

38 Hoffmann (Fn. 34), S. 101.

durch das Recht auf informationelle Selbstbestimmung gestaltet sich ebenso wie bei Art. 13 Abs. 1 und Art. 10 Abs. 1 GG. Kommt es tatsächlich zu einem Zugriff auf personenbezogene Daten, sind beide Grundrechte parallel anwendbar (Idealkonkurrenz), da unterschiedliche Schutzgüter (Infrastruktur und Daten) betroffen sind und es zwangsläufig einer Beeinträchtigung der Integrität des Systems bedarf, um auf die personenbezogenen Daten zugreifen zu können. Umgekehrt hat aber nicht jede Integritätsbeeinträchtigung zugleich auch die Erhebung personenbezogener Daten zum Gegenstand.

	Daten/Inhalte	Infrastruktur
Räumliche Infrastruktur	**Art. 2 Abs. 1 GG** (ggf. beim Menschenwürdegehalt i. V. m. Art. 1 Abs. 1 GG)	**Art. 13 Abs. 1 GG** Begrenzung des Systemschutzes auf Wohnräume
Telekommunikationsinfrastruktur	**Art. 2 Abs. 1 GG** (ggf. beim Menschenwürdegehalt i. V. m. Art. 1 Abs. 1 GG)	**Art. 10 Abs. 1 GG** Begrenzung des Systemschutzes auf die Kommunikation zwischen zwei Personen
Computerinfrastruktur	**Art. 2 Abs. 1 GG** (ggf. beim Menschenwürdegehalt i. V. m. Art. 1 Abs. 1 GG)	**Art. 2 Abs. 1 GG (Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)** Begrenzung des Systemschutzes auf komplexe Systeme, die auch personenbezogene Daten enthalten

TABELLE 1: ABGRENZUNG VON SYSTEM- UND DATENSCHUTZ (COMPUTERINFRASTRUKTUR)

Für die Definition des Begriffs der Datenhoheit ergibt sich daraus, dass es sich um zwei eigenständige Merkmale handelt, zumal die Datenhoheit bei einem nicht-integeren System von vornherein ausgeschlossen erscheint, selbst wenn es nicht zu einem Zugriff auf personenbezogene Daten gekommen ist.

2.1.3 Fazit: Definition und dogmatische Einordnung der Datenhoheit

Somit lässt sich der Begriff der »Datenhoheit« nunmehr samt seiner einzelnen Ausprägungen prägnant beschreiben. Datenhoheit liegt vor, wenn die personenbezogenen Daten des jeweils Datenbetroffenen für diesen als Träger der Datenhoheit

- jederzeit **verfügbar** sind,
- er bezüglich der Daten **verfügungsbefugt** ist,
- die Daten im jeweils genutzten System **vertraulich** behandelt werden und
- das genutzte System **integer** ist.

Die vorgeschlagene Begriffsbestimmung zeigt, dass es sich bei der Datenhoheit dogmatisch gesehen nicht um ein eigenständiges Recht, einen eigenständigen Anspruch oder Ähnliches handelt. Vielmehr ist »Datenhoheit« ein **Sammelbegriff**, der neben dem tatsächlichen Element der Verfügbarkeit die rechtlichen Elemente der Verfügungsbefugnis, Vertraulichkeit und Integrität enthält.

2.2 … in der Cloud

Für die nachfolgende Analyse besitzt neben der Datenhoheit also auch eine Cloud-Definition besondere Relevanz. Es existieren unterschiedliche Definitionsansätze, vor allem aber auch Ausgestaltungsvarianten. Da im Mittelpunkt der nachfolgenden Analyse nicht isolierte Cloud-Konzepte stehen, die von einem Nutzer – sei es einem Unternehmen, von Privatpersonen oder Behörden des öffentlichen Sektors – zur Auslagerung ihrer Daten genutzt werden, sondern vielmehr darauf basierende Kommunikationsprozesse, muss ein **weites Verständnis** gewählt werden, welches auch Daten- und Dokumentensafes einbezieht, die zwar für den Austausch mit anderen konzipiert wurden, aber nicht vollständig dem Cloud-Paradigma entsprechen. Maßgeblich sind also Konzepte, bei denen eine Person – der Träger der Datenhoheit – »seine« Daten außerhalb des eigenen Clients speichert und Dritten darauf einen Zugriff gestattet.

2.2.1 Cloud Computing

Unter Cloud Computing versteht man die gemeinsame Nutzung von Hard- und Softwaresowie Rechenkapazitäten, die nicht mehr lokalisierbar, sondern weltweit auf verschiedenen Servern nachfrage- und einzelfallabhängig zur Verfügung gestellt werden, durch verschiedene Organisationseinheiten und Individuen.[39] Cloud Computing baut dabei auf dem Konzept der **Virtualisierung** auf,[40] bei dem spezielle systemnahe Software genutzt wird, um Hardware (als virtuelle Maschine) und deren Systemsoftware (das Gastbetriebssystem) nachzubilden.

Das Modell der Virtualisierung sieht vor, dass, wenn ein Kunde Speicher-, Rechen- oder Softwarekapazitäten benötigt, ihm diese von unterschiedlichen Servern zur Verfügung gestellt wird. Ist der zunächst genutzte Server ausgelastet, wird automatisch ein anderer Server weltweit genutzt. Reichen die Ressourcen eines Anbieters nicht aus, kann er weitere Kapazitäten bei den jeweiligen Anbietern buchen und in seine Cloud integrieren. Der Kunde merkt hiervon nichts und misst ggf. lediglich die Performance am entsprechenden Service Level Agreement. Die genutzte Cloud lässt sich durch den Anbieter dem Bedarf des Anwenders entsprechend anpassen, also vergrößern oder verkleinern, fortentwickeln bzw. um spezifische Elemente ergänzen. Typisch und allen konkreten Ausgestaltungen gemein – quasi systemimmanent – ist jedoch der Umstand, dass die Nutzerdaten auf Servern verarbeitet und gespeichert werden, die weltweit verteilt sein können.[41] In der Regel weiß der Nutzer nicht, an welche geografischen Orte seine Daten übermittelt werden und wo sie physische Speicherung erfahren.

---

39 Weiss, netWorker 11 (2007), 16 ff.; Krcmar, Informationsmanagement, 5. Aufl. 2010, S. 692 ff.

40 Baun/Kunze/Ludwig, Informatik Spektrum 32 (2009), 197 ff.

41 Pohle/Ammann, CR 2009, 273 (274).

2.2.2 Daten- und Dokumentensafes mit Kommunikationsfunktion

Das Anbieten – auch Cloud-basierter – Dokumentensafes stellt keine neue Erscheinung dar, sondern wird bereits von Unternehmen, vereinzelt auch Privatpersonen, genutzt.[42] Als Dokumenten- bzw. Datensafe[43] lässt sich ein Dienst bezeichnen, der die langfristige Ablage und Verwaltung von elektronischen Dokumenten erlaubt. Er entspricht damit der Bereitstellung von Webspace auf Servern (Online-Festplatten), der internetbasiert zu erreichen ist, und kann als Teilelement des technikgestützten Identitätsmanagements verstanden werden.[44] Ein wirklicher Zusatznutzen ist mit einem Dokumentensafe erst verbunden, wenn anderen Nutzern gezielt Zugriff auf einzelne Dokumente erteilt werden kann und technisch-organisatorische Maßnahmen die Vertraulichkeit der Daten gewährleisten.

Dokumente, die im Dokumentensafe gespeichert werden, können alle elektronischen Informationen unabhängig von einem bestimmten Dateiformat sein,[45] wobei es diesbezüglich ggf. einer **Standardisierung**, vor allem zum Austausch von Dokumenten mit staatlichen Stellen aber auch zur Sicherung der **Interoperabilität** unterschiedlicher Safebetreiber, bedarf. Insbesondere werden zukünftig Bescheide,[46] Verträge o. Ä., die über einen sicheren Postfach- und Versanddienst beim Nutzer eingegangen sind, im Dokumentensafe abgelegt und bei Bedarf freigegeben oder erneut versendet werden.

Die Nutzung **unterschiedlicher Authentisierungsniveaus** ermöglicht auch innerhalb eines Cloud-basierten Dokumentensafes eine Abstufung ausgehend von den Sicherheitsinteressen des Nutzers. So kann der Zugriff auf sehr sensible Dokumente (DNA-Analyse o. Ä.) durch das Erfordernis einer Smartcard, weitergehend eines biometrischen Merkmals, erschwert werden, mit der Folge, dass die Kompromittierung des Passworts – welches bspw. den Zugriff auf Urlaubsbilder o. Ä. absichert – unschädlich ist.

Ein in die technische Lösung zu integrierendes **digitales Rechtemanagement** muss unterschiedliche Zugriffs-, Lese- und Schreibrechte abbilden können. Für bestimmte Geschäftsprozesse oder Verwaltungsverfahren ist es nämlich ausreichend, dass der Gegenseite das betreffende Dokument lediglich zur Kenntnis gegeben, jedoch nicht ausgehändigt wird.[47]

---

42 Exemplarisch sei auf folgende Angebote hingewiesen: www.xdrive.com/, www.teamdrive.de/, www.box.net/, www.mydrive.ch/de/, www.skydrive.live.com/.

43 Perspektivisch erscheint es denkbar, dass nicht mehr nur ein »Eins-zu-eins-Abbild« des herkömmlichen Dokuments (bspw. durch einen Scan-Vorgang) im Safe abgelegt wird, sondern aus den Dokumenten auch strukturierte Daten, bspw. im XML-Format, generiert und für andere (behördliche) Prozesse zur Verfügung gestellt werden. Ein solches Vorgehen findet sich bspw. bei der Realisierung der »elektronischen Grundschuld« nach dem »Gesetz zur Einführung des elektronischen Rechtsverkehrs und der elektronischen Akte im Grundbuchverfahren« (BT-Drs. 16/12319); dazu Gassen/Mödl, ZRP 2009, 77 (78).

44 Umfassend Schliesky (Hrsg.), Technikgestütztes Identitätsmanagement, 2010.

45 Aus technischer Sicht erscheint es daher passender, von einem »Datensafe« zu sprechen. Problematisch an Safesystemen, die Vertraulichkeit auch gegenüber dem Anbieter garantieren (vgl. dazu 5.3.3.2), erscheint, dass eine »automatische« Konvertierung zur Erhaltung der langfristigen Lesbarkeit ausgeschlossen ist. Denkbar wären allenfalls allgemeine Hinweise an die Nutzer, die Lesbarkeit der verwendeten Dateiformate in regelmäßigen Abständen zu überprüfen. Derzeit wird vor allem das PDF/A-Format zur Langzeitarchivierung eingesetzt. Optimalerweise werden Daten jedoch im XML-Format abgelegt, da so eine Wiederherstellung auch in vielen Jahren noch möglich ist.

46 Auch hier wäre zukünftig der Einsatz der XML-Technologie wünschenswert, im Gegensatz zur heutigen Digitalisierung analoger Dokumente (bspw. Zeugnisse, Geburtsurkunden o. Ä.) hat das XML-Format den Vorteil, eine direkte Einbindung der Daten in die Software-Systeme anderer Behörden oder privater Unternehmen zu ermöglichen.

47 Durch den Einsatz spezieller »Viewer« ließe sich die (unzulässige) Speicherung technisch ausschließen. Bis zu einem flächendeckenden Einsatz derartig sicherer Hard- und Software-Komponenten, erscheint aber auch

Der technische Ausschluss des Kopierens von Dateien aus dem Dokumentensafe könnte bspw. diesem herkömmlichen Verfahren entsprechen. Erforderlich sind zudem Protokollfunktionen, die ebenso wie beim Postfach- und Versanddienst rechtssicheren Nachweis über Zugriffe o. Ä. erbringen.

Insoweit würde eine gesetzliche Festlegung von datenschutzrechtlichen Vorgaben zur Datensicherheit bzw. die Regelung von Zugriffsrechten lediglich zusätzliche Rechtssicherheit bewirken und ggf. das Rechtsregime des BDSG verschärfen, zumindest aber durch eine präventive staatliche Prüfung aktivieren. Interessant – und in der Tat regelungsbedürftig – wären in diesem Bereich vor allem **zusätzliche Funktionen bezogen auf die im Safe enthaltenen Dokumente.** Insoweit können ggf. Parallelen zu den herkömmlichen Notaren gezogen werden. So bietet ein niederländisches Unternehmen derartige Funktionen – in Übereinstimmung mit dem niederländischen Recht, das einen Notar im Vorstand des Unternehmens verlangt – in Kooperation mit herkömmlichen Notar-Strukturen an.[48] In gewisser Weise staatlich initiiert wurde die Nutzung von Dokumentensafes auch in Dänemark, zumal dort die Zustellung der Lohnabrechnungen für die Beschäftigten im öffentlichen Dienst durch ein derartiges System vorgenommen wurde.[49] Schließlich sind auch Verfahren zur elektronischen Langzeitarchivierung in die Überlegungen zu Cloud-basierten Daten- und Dokumentensafes einzustellen. Eine derartige Infrastruktur wurde (für den Teilbereich notarieller Dokumente) in Österreich mit dem Project CyberDOC realisiert.[50]

Problematisch an der derzeitigen gesetzlichen Ausgestaltung in Deutschland ist, dass in § 8 DeMailG zwar ein Dokumentensafe angelegt und explizit als »De-Mail-Dienst« bezeichnet wird, verbindliche Vorgaben zum Umgang mit Daten in einem solchen System aber fehlen. Hier erscheinen dem Postfach- und Versanddienst i. S. d. § 5 DeMailG vergleichbare Vorgaben erforderlich. In diesem Kontext müsste – gerade auch um die Datenhoheit nachhaltig abzusichern – über eine Erweiterung der Dokumentensafe-Funktionalitäten über einen bloß virtuellen Tresor hinaus nachgedacht werden. Ergänzend könnte man den Dokumentensafe-Betreibern oder diesen in Zusammenarbeit mit Notaren notarielle Funktionen, also bspw. die Beurkundung digitaler Dokumente, übertragen.[51] Zumindest in einer Übergangszeit bis zur flächendeckenden Verbreitung von elektronischen Dokumenten (Verwaltungsakten, Zeugnissen, Verträgen etc.), die bereits im Zeitpunkt ihrer Erstellung bspw. durch eine elektronische Signatur vor nachträglichen unbefugten Änderungen gesichert und somit auch im digitalen Geschäftsverkehr als authentisch anzusehen sind, müssen zudem Optionen

---

eine gesetzliche Regelung, die ein Speichern der Dokumente (bspw. aus den temporären Internetdateien heraus) verbietet, ausreichend.

48 www.diginotar.nl/.

49 www.e-boks.dk/.

50 Dort besteht seit dem 01. 01. 2000 die Möglichkeit, notarielle Urkunden in CyberDOC zu speichern. Das gesamte österreichische Notariat, bestehend aus ca. 450 Notaren, verfügt über eine einheitliche technische Infrastruktur aus Hard- und Software mit identischen Kommunikationsschnittstellen. Die Urkunden werden im TIFF-Format und mit Suchbegriffen versehen auf einem speziell gesicherten Server gespeichert. Die Datensicherheit wird dabei über eine verschlüsselte Übersendung sowie durch regelmäßige Daten-Backups gewährleistet. Außerdem werden die Sicherungsmaßnahmen und Speichermedien halbjährig durch einen zertifizierten Sicherheitsingenieur geprüft; s. dazu etwa Benesch/Weichselbaumer, MittBayNot 2000, 395 (396 ff.); Weichselbaumer, MittBayNot 2001, 452 (454); Bittner, BWNotZ 2001, 97 (105).

51 Vgl. dazu Fraunhofer Institut für Offene Kommunikationssysteme, White Paper »Elektronische Safes für Daten und Dokumente«, abrufbar unter: www.fokus.fraunhofer.de/; vgl. allgemein zur Beurkundung digitaler Dokumente Wahlmann, in: Scherf/Schmieszek/Viefhues (Hrsg), Elektronischer Rechtsverkehr, Kommentar und Handbuch, 2006, S. 166 ff.; Rapp, Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen, 2002, S. 185 ff.

bereitgestellt werden, »klassische« Dokumente dergestalt in einen elektronischen Safe zu überführen, dass sie das gleiche Vertrauen für sich in Anspruch nehmen wie das »Papierdokument«. Auch hier gibt es ggf. Möglichkeiten, die herkömmlichen Notarstrukturen in die erforderlichen Transformationsprozesse[52] einzubinden. Ohne Präjudiz für eine Ansiedlung bzw. Zuweisung derartiger Zusatzfunktionalitäten an den Notarberuf sollen diese Dienste als **»Datennotardienste«**[53] bezeichnet werden, die das Angebot der (ggf. akkreditierten) Safe-Provider ergänzen.

2.2.3 Fazit: Freigabe- und Zugriffsfunktionen als Mehrwert von Datenbeständen in der Cloud

Im Mittelpunkt der Analyse rechtlicher und technisch-organisatorischer Anforderungen zur Sicherstellung von Datenhoheit im Cloud-Umfeld sollen also alle Konzepte stehen, bei denen eine Person – der Träger der Datenhoheit – »seine« Daten außerhalb des eigenen Clients speichert und Dritten darauf einen Zugriff gestattet. Diese basieren in der Regel auf dem Cloud-Paradigma, da erst die Raum- und Zeitunabhängigkeit dieser Dienste neuartige Kommunikationsprozesse ermöglicht. Auch die genannten Beispiele und Grundmodelle passen in dieses Begriffsverständnis:

- Beim **P23R** werden die relevanten Datensätze eines Unternehmens regelbasiert – in der Regel von einem Intermediär – aufbereitet und in bestimmten Zyklen von den zuständigen Stellen abgerufen.
- Dokumentensafes nach **§ 8 DeMailG** haben zwar keinen unmittelbaren Kommunikationsbezug, basieren aber ebenfalls auf dem Grundgedanken der ausgelagerten und geteilten Infrastrukturen.
- Und schließlich werden die Daten beim Projekt **»OMS«** und der **elektronischen Gesundheitskarte** gerade nicht bei einer Vielzahl von Stellen gehalten, sondern Kernelement ist ein digitales Rechtemanagement, welches gezielte Zugriffe, zudem in der Regel gekoppelt mit einer technischen Sicherung, die eine Mitwirkung des Betroffenen sicherstellt, ermöglicht.

---

52 Vgl. dazu Roßnagel/Fischer-Dieskau/Wilke, CR 2005, 903 ff.

53 Als solche kommen zunächst die Beglaubigung elektronischer Dokumente (im Safe), die Digitalisierung und Beglaubigung »analoger« Dokumente, die Einschaltung als »Trusted Third Party« (bspw. beim Schlüsselverlust durch den Safe-Owner) und eine Beratungsfunktion (bspw. zur Auswahl verschiedener Anbieter von Speicherplatz) in Betracht.

3 Grundlagen und Ausgangssituation

Um Konzepte zur Sicherung der individuellen Datenhoheit in Cloud-Systemen zu entwickeln, bedarf es neben einer Betrachtung exemplarischer Projektansätze (4) einer Analyse der infrastrukturellen (3.1) und rechtlichen Grundlagen (3.2). Um die erforderliche Akzeptanz zu erzielen, Synergien zu heben und die Kosten gering zu halten, sollten sich diese Konzepte nämlich in den bestehenden Rahmen einfügen und nicht – wie bspw. zum Teil bei OMS und der eGK – »das Rad neu erfinden«.

3.1 Infrastrukturelle Grundlagen

3.1.1 Cloud Computing

Cloud Computing wird ein großes Potenzial vorausgesagt. Laut einer aktuellen Studie von IDC[54] könnte die Akzeptanz von Cloud Computing in Europa einen Beitrag von bis zu 88 Milliarden Euro zum BIP generieren, geschähe dies noch mit politischer Unterstützung könnten es sogar 250 Milliarden Euro sein. Um dieses Potenzial zu nutzen, müssen die Bedingungen auf den europäischen Markt angepasst werden. Hierbei geht es im Besonderen um die Einhaltung der gesetzlichen Rahmenbedingungen und die Möglichkeit, den Cloud-Anbieter zu wechseln. Die Europäische Kommission hat in einer Mitteilung an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen auf die Herausforderung eines europaweiten, cloud-freundlichen Marktes hingewiesen, der das Potenzial zu Produktivitätswachstum und erhöhter Wettbewerbsfähigkeit hat, aber auch um Europa als einen wichtigen »global player« zu platzieren.[55] Unsicherheit des Rechtsrahmens, unklare Vertragssituationen und ein Dschungel an Standards verhindern die Akzeptanz von Cloud Computing.

- Unsicherheit des Rechtsrahmens

  Gerade die Unsicherheit hinsichtlich des anzuwendenden Rechtsrahmens zählt zu den ranghöchsten Hindernissen für die Nutzung von Cloud Computing. Unklar ist, welche Gesetze anzuwenden sind, was gerade im europäischen Raum besonders problematisch ist durch die nationalen Implementierungen, bspw. des Datenschutzgesetzes. Digitale Inhalte und Lokation der Daten stehen in engem Zusammenhang mit der Komplexität der Administration der angebotenen Dienste und

---

[54] Vgl. Quantitative Estimates of the Demand for Cloud Computing in Europe and the likely Barriers to Uptake, 2012, abrufbar unter www.ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitytive.pdf/.

[55] Vgl. Unleashing the potential of Cloud Computing, 2012, abrufbar unter www.ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_pdf/.

den entsprechenden Nutzungsmustern, die ggf. mehrere rechtliche Zuständigkeiten berühren und so besondere Sorgfalt des Cloud-Anbieters bezüglich Datenschutz und Verbraucherschutz erfordern.

- Unklare Vertragssituationen

  Abhängig von der Art der Bereitstellung durch den Cloud-Anbieter (Abbildung 2) sind die Verträge für die Dienstleistung in einer privaten Cloud spezifischer als in einer Public Cloud. Dort sind in der Regel nur allgemeine Dienstleistungsvereinbarungen (SLAs) anzufinden. Die Sorge um den Zugriff auf und die Portabilität der Daten bei einem Wechsel stehen in engem Zusammenhang mit dem »Eigentumsrecht« an den Daten und einem Kontrollwechsel. Unklar ist, wie die Haftung bei Datenverlust oder Dienstausfall behandelt wird, wem die Daten »gehören«, die in der Cloud erzeugt werden, und wie Streitigkeiten gelöst werden.

- »Standarddschungel«

  Verwirrung herrscht zudem aufgrund der Vielfalt an Standards und darüber, welche Standards ein adäquates Niveau für Interoperabilität bieten und welche Sicherheitsmechanismen zum Schutz personenbezogener Daten vorhanden sind.

Um den Problemen zu begegnen, hat die Kommission 2012 eine Cloud-Strategie entwickelt und will diese in Förderprogrammen umsetzen. Die zentralen Ziele der Strategie sind:

- Nutzern Gewissheit zu verschaffen, dass ihre Daten zwischen Clouds übertragen werden können oder aber auch ganz entfernt werden können,
- vertrauensbildende Maßnahmen für eine EU-weite Zertifizierung vertrauenswürdiger Cloud-Anbieter zu unterstützen,
- Musterverträge für Cloud-Computing, die rechtliche Verpflichtungen klar darstellen, zu entwickeln und
- eine europäische Cloud-Partnerschaft zwischen dem öffentlichen Sektor und der Industrie zu etablieren, um Bedarf zu ermitteln und zu gewährleisten, dass der europäische IT-Sektor diesen decken kann. Ziel ist die Stärkung europäischer Unternehmen im Wettbewerb.[56]

In Deutschland hat das Bundesministerium für Wirtschaft und Technologie 2010 einen »Trusted Cloud«-Wettbewerb initiiert und mit den Gewinnern des Wettbewerbs 2011 das Technologieprogramm mit einem Fördervolumen von rund 50 Millionen Euro und einem Gesamtvolumen von 100 Millionen Euro gestartet. 14 Projekte mit 38 Unternehmen, 26 wissenschaftliche Einrichtungen und fünf weitere Institutionen wurden gefördert, um Cloud Computing mit konkreten Referenzimplementierungen zu zeigen. Es ist zu erwarten, dass einige der oben genannten Hürden im Bereich der rechtlichen Rahmenbedingungen und der besseren Identifizierung notwendiger Standards durch Pilotierung der Projekte aufgelöst werden.

Der Blick auf die Aktivitäten der Europäischen Kommission zeigt deutlich, dass die EU eine wichtige Rolle bezüglich einer vertrauenswürdigen Nutzung des Cloud-Computings spielt, an der sich nationale Staaten beteiligen. Vertrauensbildende Schritte wurden mit dem Vor-

[56] www.ec.europa.eu/news/science/120927_de.htm/.

schlag einer harmonisierten Datenschutzverordnung eingeleitet, die zwar noch auf nationaler Ebene kommentiert und diskutiert wird, aber dafür Sorge trägt, dass u. A. für die Behandlung personenbezogener Daten in der IT eine europaweit einheitliche Regelung getroffen wird.

Ein kurzer Überblick über die Hoheit über die Daten bzw. deren Kontrolle wird in Abbildung 2 gegeben. Die vollständige Kontrolle über die Daten ist nur in einer privaten Cloud gegeben, was dann auch vertraglich über hochspezialisierte SLAs festgelegt wird. Die Daten, die bei einem Cloud-Anbieter liegen, im Fall eines Hostings, sind nur bedingt unter eigener Kontrolle, da u. U. der Cloud-Anbieter die Daten im Fall eines Schadens (bspw. Denial of Service) verlieren kann. Dieser Fall kann zwar auch vertraglich im Rahmen von Haftungsklauseln geregelt werden, sodass der Cloud-Anbieter entsprechende Sicherheitsmechanismen implementieren muss, was wiederum ein Spezialfall ist und entsprechend finanziell abgegolten werden muss. In einer Public Cloud kann man zwar Sicherheitspakete dazu kaufen, aber die Nutzungsbedingungen werden durch den Cloud-Anbieter festgelegt und die Haftung für den Datenverlust in der Regel ausgeschlossen. Ansonsten könnten diese Angebote nicht zu einem relativ günstigen Preis angeboten werden.

Um Daten in der Cloud abzulegen, empfiehlt es sich, eine Risikoabschätzung vorzunehmen und die eigenen Sicherheitsbedürfnisse auf die SLAs des Cloud-Anbieters abzubilden. Dabei ist darauf zu achten, was für ein Sicherheitsmanagement der Cloud-Anbieter vorhält. Hier kann es von Vorteil sein, dass ein Anbieter zertifiziert[57] ist. Hinsichtlich der Details für ein entsprechendes Risikomanagement und entsprechende Maßnahmen sei auf die ISPRAT-Studie »Cloud Computing für die öffentliche Verwaltung«[58] verwiesen.

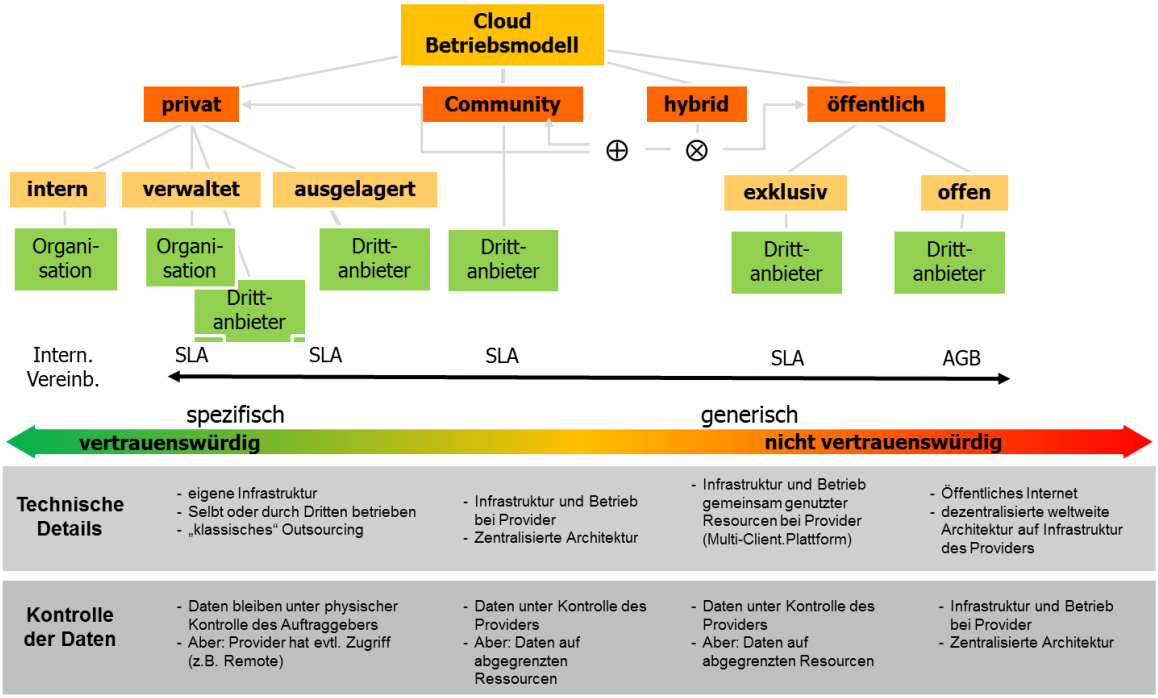

ABBILDUNG 2: BETRIEBSMODELLE CLOUD-COMPUTING UND SICHERHEITSLEVEL

57 ISO 27001 Zertifizierung auf Basis des IT Grundschutzes des BSI.

58 Deussen/Strick/Peters, ISPRAT-Studie »Cloud Computing für die öffentliche Verwaltung«, 2010; abrufbar unter www.fokus.fraunhofer.de/de/elan/projekte/national/cloud_computing_e-gov/index.html.

3.1.2 Digitale Identitäten

Bei weiterhin steigender und zunehmend mobiler Nutzung von Informations- und Kommunikationstechnologien[59] gewinnen Fragen der sicheren Identität und des Schutzes persönlicher Daten zunehmend an Bedeutung. Obwohl Vertrauen und Sicherheit die wichtigsten Voraussetzungen für Online-Transaktionen sind, wurden bei insgesamt erheblichen Sicherheitsbedenken auf Seiten der privaten Anwender Fragen des Schutzes persönlicher Daten nur von wenigen als zentral benannt.[60] Angesichts der gleichzeitig zu beobachtenden Professionalisierung des Diebstals persönlicher Daten[61] zeigt sich besonderer Handlungsbedarf in diesem Feld. Dabei konnte bereits bei einer Befragung im Jahr 2010 eine grundlegende Akzeptanz des neuen Personalausweises als zentrales Instrument des sicheren Identitätsmanagements festgestellt werden.[62]

Digitale Identitäten sind eine Grundvoraussetzung für sichere Transaktionen im Internet. Abhängig von der Lebenslage haben Personen verschiedene Identitäten. Identitäten können durch den Namen einer Person, die Adresse, wie sie im Personalausweis steht, die Bankverbindung, die private oder berufliche E-Mail-Adresse, ein Pseudonym im Chat oder, falls möglich, anonym beim Surfen im Internet repräsentiert werden. Damit stehen digitale Identitäten immer in einem Kontext, in dem sie benutzt werden, und fassen die für diesen Kontext benötigten Attribute zusammen. Darüber hinaus können Nutzer durchaus mehrere digitale Identitäten besitzen. Die Verwaltung und kontextspezifische Auswahl von Identitäten sowie deren Schutz ist ein komplexer Prozess und erfordert ein Verwalten des gesamten Lebenszyklus‘ digitaler Identitäten. Technische Unterstützung dazu bieten Identitätsmanagementsysteme.

Digitale Identitäten beschränken sich aber nicht nur auf Personen, sondern können auch auf Produkte, Materialien, Technologien und geistiges Eigentum (Schutz des Urheberrechts) bezogen sein[63]. Damit werden nicht nur wirtschaftliche und technische, sondern in besonderer Weise auch gesellschaftliche Fragen tangiert. So stellen sich neben den Bedrohungen für die IT-Sicherheit[64] zunehmend auch Gefährdungen hinsichtlich der Integrität von Netzen dar.

Um personenbezogene Daten konsistent, sicher und vollständig bereitzustellen und ständig verfügbar zu haben, gewinnt ein Identitätsmanagement an Bedeutung[65]. So zeigt eine Studie über US-amerikanische und europäische Cloud-Provider und -Anwender, dass sicheres Zugangs- und Identitätsmanagement als eine wesentliche Sicherheitsherausforderung angesehen wird.[66]

---

59 Vgl. Bitkom (Hrsg.), Netzgesellschaft, Eine repräsentative Untersuchung zur Mediennutzung und dem Informationsverhalten der Gesellschaft in Deutschland, 2011.

60 Vgl. Bitkom, Studie »Internet-Sicherheit«, Verbrauchermeinungen zur Datensicherheit im Web, 26.08.2011, abrufbar unter www.bitkom.org/files/documents/bitkom_internet_sicherheit_extranet.pdf/.

61 Vgl. Bundesamt für Sicherheit in der Informationstechnologie (Hrsg.), Die Lage der IT-Sicherheit in Deutschland 2011, S. 21-23.

62 Vgl. Bitkom, Studie »Neuer Personalausweis«, Aktuelle Akzeptanz in der Bevölkerung, 26.08.2011, abrufbar unter www.bitkom.org/files/documents/bitkom_epa_extranet.pdf/.

63 Vgl. Bundesministerium für Bildung und Forschung (Hrsg.), Forschung für die zivile Sicherheit, Kooperation in der zivilen Sicherheitsforschung zwischen Deutschland und Israel, 2010, S. 7.

64 Vgl. Microsoft (Hrsg.), Microsoft Security Intelligence Report, Volume 7.

65 Vgl. Essoh/Doubrava/Münch, Sicherheitsempfehlungen für Cloud Computing Anbieter (Mindestanforderungen in der Informationssicherheit), Eckpunktepapier, 2011, S. 38-40.

66 Deussen/Strick/Peters (Fn. 58), S. 117.

3.1.3 Elektronische Dokumentenspeicher

Aktuell werden von verschiedensten Herstellern Möglichkeiten zur Speicherung von Daten und Dokumenten angeboten. Ein detaillierter Überblick über elektronische Speichermöglichkeiten ist in der ISPRAT-Studie »Der elektronische Safe als vertrauenswürdiger Cloud Service«[67] zu finden. Darin wurden insbesondere Verfahren für die sichere Aufbewahrung von Daten- und Dokumenten in der Cloud untersucht. Als besonders sicher gilt das Aufteilen von Daten- und Dokumenten in Teilstücke und die entsprechende Verschlüsselung dieser Teilstücke, die dann an beliebigen Speicherorten in der Cloud abgelegt werden können. Dieser »elektronische Safe« als Cloud-Dienst sichert sowohl die Vertraulichkeit der Daten als auch deren Integrität. Niemand kann mit den Teilstücken etwas anfangen, insbesondere, da die Verschlüsselung auf dem eigenen Endgerät erfolgt und der Schlüssel nicht beim Safe-Anbieter gehalten wird. Nur für Freigabezwecke wird der Schlüssel übermittelt. Aus Gründen der persönlichen Identifikation kann dazu der neue Personalausweis genutzt werden.

Andere Angebote, die **Speicherplatz** im Netz zusammen **mit Verschlüsselungsfunktionen** anbieten, findet man auch. Der Schutz der dort gespeicherten Daten ist durch Passwort und/oder Chipkarten gegeben, jedoch kann durch einen technischen Defekt der angemietete Speicherplatz defekt werden und zum Verlust der Daten führen. Anders als beim elektronischen Safe als Cloud-Dienst ist der »Eigentümer« der Daten selbst für die Verfügbarkeit verantwortlich.

Eine komfortablere Lösung bieten **Online-Festplatten**, beispielsweise Dropbox, bei der der Anbieter für die Datensicherung sorgt. Diese erfolgt zwar verschlüsselt bei beliebigen Storage-Anbietern, ist aber mit entsprechender Client-Software leicht von beliebigen anderen Endgeräten zugreifbar. Bei dieser Art der Speicherung gibt es seitens des Anbieters keine konkrete Aussage, wo sich der Speicherplatz befindet. Auch gibt es keine Werkzeuge für ein nachvollziehbares Protokoll über Zugriffe auf die Daten. Allerdings ist bei geringem Datenvolumen die Nutzung kostenlos.

Die **Dokumentenablage** bei **De-Mail** ist eine vom De-Mail-Anbieter angebotene (optionale) Komponente, die dem Benutzer eine persönliche Ablage für Dokumente zuordnet. Der Zugriff auf die Daten erfolgt über die Anmeldung und bietet verschiedene Authentifizierungsmechanismen an, die Sichtbarkeit und Zugriff auf die eigenen Dokumente regelt. Eine Erweiterung bezüglich Freigabefunktionen für Dritte und den dazu erforderlichen sicheren Transport der Dokumente zwischen den De-Mail-Nutzern ist ebenso wie die Langzeitarchivierung geplant.

3.1.4 Infrastrukturen sicherer Kommunikation

De-Mail-Dienste unterstützen einen sicheren, vertraulichen und nachweisbaren E-Mail-Geschäftsverkehr zwischen Bürger, Verwaltung und Unternehmen über das Internet. Mit De-Mail ist eine personengebundene, identitätsbezogene E-Mail-Adresse verbunden. Die rechtlichen Grundlagen wurden im De-Mail-Gesetz[68] festgelegt und durch technische Richtlinien[69] definiert. De-Mail-Dienste umfassen den Postfach- und Versanddienst für sichere elektronische Post, einen optionalen Identitätsbestätigungsdienst sowie einen optionalen

---

67 Vgl. Klieme u. a., ISPRAT-Studie »Der elektronische Safe als vertrauenswürdiger Cloud Service«, 2011, abrufbar unter www.isprat.net/fileadmin/downloads/pdfs/ISPRAT-Studie_Cloud-Safe_V1_20120121.pdf.

68 BGBl I, S. 666; dazu Rose, K&R 2011, 439 ff.; Roßnagel, NJW 2011, 1473 ff.; Spindler, CR 2011, 309 ff.; zum Entwurf Roßnagel, CR 2011, 23 ff.

69 Vgl. Technische Richtlinien TR-0120 [TR-DM].

De-Safe für die sichere Dokumentenablage. Mit dem Identitätsbestätigungsdienst wird auf Anforderung des Nutzers eine Identitätsbestätigung erstellt, die an die De-Mail-Adresse des Empfängers geschickt wird. Durch eine qualifizierte Signatur wird zudem die Korrektheit der übermittelten Daten bestätigt.

Grundsätzlich ist die Kommunikation zwischen Nutzern und Anbietern eines De-Mail-Dienstes gesichert (über SSL – Secure Sockets Layer bzw. TSL – Transport Layer Security) und bietet eine zusätzliche Funktion für eine Ende-zu-Ende Verschlüsselung mittels qualifizierter Signatur an.

Das De-Mail-Gesetz sieht vor, dass die De-Mail-Anbieter im Rahmen einer Akkreditierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Umsetzung technischer und organisatorischer Maßnahmen nachweisen müssen, um so bspw. den internen oder externen Zugriff auf Daten durch Unberechtigte zu verhindern.

Der **E-Postbrief** der Deutschen Post AG[70] bietet ähnliche Funktionen wie der De-Mail-Dienst und soll eine verbindliche, verlässliche und vertrauliche E-Mail-Kommunikation zwischen zwei Parteien (Privatkunden und Geschäftskunden) ermöglichen. Dem Nutzer wird ein elektronischer Briefkasten (Postfach) zum Empfangen und Versenden von E-Postbriefen, E-Mails und Faxen zur Verfügung gestellt. Der verfügbare Speicherplatz ist auf 100 MB begrenzt.

Der Versand aller E-Postbriefe erfolgt nur zwischen E-Postbrief-Adressen der registrierten und identifizierten Nutzer und ist daher ein geschlossenes Kommunikationssystem, ebenso wie De-Mail. E-Postbriefe können auch als klassische Briefe auf dem Postweg zugestellt werden. Der Absender kann zwischen verschiedenen Zusatzleistungen wählen: Einschreiben Einwurf, Einschreiben mit Empfangsbestätigung, mit Absender-Ident-Nachweis, persönlich verschlüsselt und/oder persönlich signiert. Die eingesetzten Signaturverfahren erfüllen nicht die Voraussetzungen einer qualifizierten elektronischen Signatur nach dem Signaturgesetz (SigG), sodass gesetzlich vorgesehene Formerfordernisse in der rein elektronischen Variante nicht erfüllt werden[71]. Die Post hat angekündigt, dass sie eine Akkreditierung als De-Mail-Dienstanbieter beantragen wird.

Die Identifizierung des Kunden erfolgt mit dem PostIdent-Verfahren. Die Authentifizierung am E-Postbrief-Portal kann in verschiedenen Sicherheitsniveaus erfolgten: »normal« mit E-Postbrief-Adresse und Passwort und »hoch« mit Handy-TAN. E-Postbriefe werden verschlüsselt verschickt (Portalverschlüsselung). Die Verbindungsstrecke vom Anwender zum E-Postbrief-System wird durch TLS (Transport Layer Security) gesichert. Auch die Ablage im Postfach erfolgt verschlüsselt.

---

70 Deutsche Post AG, Leistungsbeschreibung E-Postbrief, Stand 05/2011, abrufbar unter www.service.epost.de/downloads/7/leistungsbeschreibung_e-postbrief.pdf/.

71 Ausführlich Hoffmann u. a., Der E-POSTBRIEF in der öffentlichen Verwaltung – Chancen, Einsatzoptionen, rechtliche Handlungsspielräume, 2011.

3.2 Rechtliche Grundlagen

Um Konzepte im Cloud-Umfeld entwerfen zu können, die sowohl technisch-organisatorisch als auch rechtlich die Datenhoheit der Betroffenen sichern, bedarf es einer Analyse, in welchem Rechtsrahmen sich derartige Dienste bewegen. Dabei wird einerseits zwischen verfassungs- und einfachgesetzlichen Grundlagen zu differenzieren sein, andererseits soll zunächst die deutsche bzw. europäische Rechtslage zugrunde gelegt werden – wohl wissend, dass zahlreiche (Cloud-)Angebote außerhalb dieses Rechtsraums realisiert werden. Ein Umstand, den das geltende Recht aber mit den Vorgaben an eine (zulässige) Auftragsdatenverarbeitung aufnimmt. Im Folgenden werden daher die Rechtsgrundlagen der Datenhoheit (3.2.1), des Cloud Computings (3.2.2), von Dokumentensafes (3.2.3) sowie insbesondere von Diensten beleuchtet, die im Rahmen des Zugangs- und Identitätsmanagements eine besondere Rolle spielen können (3.2.4).

3.2.1 Datenhoheit

Die verfassungsrechtlichen Grundlagen der Datenhoheit sind – wie bereits dargestellt (2.1) – im Recht auf informationelle Selbstbestimmung und im Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme zu erblicken. Vor allem aber das Recht auf informationelle Selbstbestimmung entfaltet für den Bürger eine essenzielle Schutzwirkung in Bezug auf seine personenbezogenen Daten. Diese Schutzwirkung wird durch das BDSG bzw. die Datenschutzgesetze der Länder einfachgesetzlich konkretisiert. Je nachdem, wer dem Bürger im Rahmen einer Cloud-Anwendung gegenübertritt – der Staat oder ein Unternehmen – entfaltet das Recht auf informationelle Selbstbestimmung unterschiedliche Schutzrichtungen. Diese fallen ggf. auch zusammen, wenn der Bürger mit mehreren Akteuren interagiert. Auf diese Weise entstehen unterschiedliche »Mehrpersonenverhältnisse«.

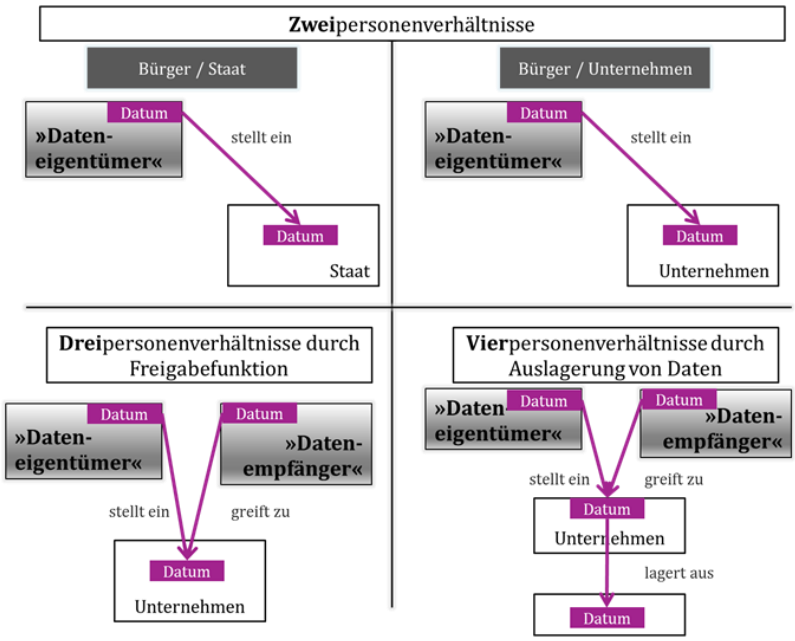

ABBILDUNG 3: MEHRPERSONENVERHÄLTNISSE IM KONTEXT VON CLOUD-ANGEBOTEN

3.2.1.1 »Zweipersonenverhältnis« Bürger – Staat: Unmittelbare Schutzwirkung des Rechts auf informationelle Selbstbestimmung

Hinter dem »Zweipersonenverhältnis« Bürger – Staat verbirgt sich die Konstellation, dass der Bürger Daten in einen vom Staat betriebenen (Cloud-)Service einstellt. In diesem Bürger-Staat-Verhältnis entfaltet das Recht auf informationelle Selbstbestimmung die klassische Schutzfunktion der Grundrechte als Abwehrrecht des Bürgers gegenüber dem Staat.[72] Demzufolge kann der Bürger vom Staat als Grundrechtsverpflichtetem verlangen, bevorstehende Eingriffe zu unterlassen und geschehene Eingriffe zu beseitigen.[73] Ein Eingriff in das Recht auf informationelle Selbstbestimmung ist verfassungsrechtlich nur zugelassen, wenn dieser auf einer verfassungsmäßigen Rechtsgrundlage beruht (**Vorbehalt des Gesetzes**).[74] Dabei ist stets das datenschutzrechtliche Grundprinzip zu beachten, dass personenbezogene Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie rechtmäßigerweise erhoben wurden (**Zweckbindungsgrundsatz**).[75]

In diese Kategorie sind also die Projekte »OMS« und die elektronische Gesundheitskarte einzuordnen. Neben der gesetzlichen, zweckgebundenen Ermächtigung zum Zugriff auf existierende Datenbestände (durch weitere als die speichernde Stelle) erscheint es auch möglich, weiteren Akteuren durch eine Einwilligungserklärung diesen Zugriff zu gestatten – bspw. weil aus Sicht des Betroffenen damit eine Verfahrenserleichterung einhergeht und er seine Daten nicht erneut angeben muss. Auch zur Erhöhung des Sicherheitsniveaus kann eine explizite Freigabe – so bei OMS und eGK – vorgesehen werden, wobei technisch unterschiedliche Ansätze (z. B. PIN-Eingabe) realisiert werden können. Den Gedanken der Mehrfachnutzung der beim Staat bereits vorhandenen Daten greift bspw. auch der Entwurf eines E-Government-Gesetzes des Bundes auf. § 5 des Entwurfs normiert, dass »die zuständige Behörde erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, mit der Einwilligung des Verfahrensbeteiligten direkt bei der ausstellenden öffentlichen Stelle elektronisch einholen« kann.

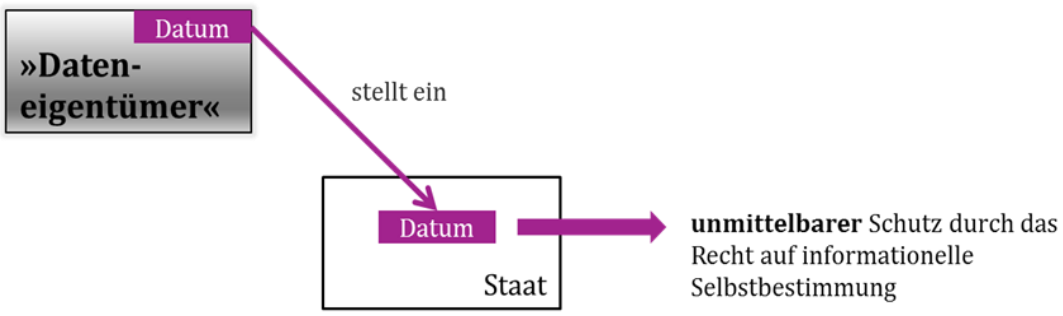

Abbildung 4: Unmittelbare Schutzwirkung des Rechts auf informationelle Selbstbestimmung gegenüber dem Staat

---

72 Vgl. Pieroth/Schlink (Fn. 37), Rn. 76.
73 Pieroth/Schlink (Fn. 37), Rn. 76.
74 Herzog/Greszik, in: Maunz/Dürig (Fn. 30), Art. 20 Rn. 75.
75 Wolff, in: ders./Brink (Fn. 20), Syst. A., B. Rn. 11.

3.2.1.2 »Zweipersonenverhältnis« Bürger – Unternehmen: Mittelbare Schutzwirkung des Rechts auf informationelle Selbstbestimmung

Im »Zweipersonenverhältnis« Bürger – Unternehmen hingegen wirkt sich der grundrechtliche Schutz durch das Recht auf informationelle Selbstbestimmung anders aus als im Staat-Bürger-Verhältnis. Unternehmen, mithin Private, sind nämlich nicht unmittelbar grundrechtsverpflichtet. Unternehmen dürfen – auch ohne gesetzliche Grundlage – innerhalb der Grenzen des BDSG personenbezogene Daten von Bürgern sammeln, verarbeiten und weitergeben, weil diese Tätigkeiten insoweit ihrerseits grundrechtlich geschützt sind (Art. 2 Abs. 1, Art. 5 Abs. 1 Satz 1 und 2, Art. 5 Abs. 3 und Art. 12 Abs. 1 GG).[76]

Hier wird deutlich, dass die Ausgangssituation für Staat und Unternehmen vollkommen unterschiedlich ist. Private dürfen grundsätzlich auch mit fremden Daten umgehen, weil sich dies im Rahmen ihres grundrechtlich geschützten Handlungsspielraums bewegt. Insoweit stellen Regelungen zum Umgang mit fremden Daten eine **Grundrechtseinschränkung** dar, die rechtfertigungsbedürftig ist. Der Staat hingegen darf grundsätzlich keine Daten von Bürgern sammeln, verarbeiten und weitergeben, soweit keine hinreichende **Ermächtigungsgrundlage** vorliegt. Interessanterweise enthält das BDSG bzw. enthalten die Landesdatenschutzgesetze nicht nur eben diese Ermächtigung, sondern zugleich eine Einschränkung im Umgang mit fremden Daten für Private. Die Datenschutzgesetze unterwerfen den Umgang mit fremden Daten durch den Staat und durch Unternehmen letztlich denselben Voraussetzungen, sodass insoweit ein Gleichlauf hergestellt wird, obwohl sich die rechtlichen Ausgangssituationen diametral gegenüberstehen. Für nicht-öffentliche Stellen nach dem BDSG errichtet dieses einfachgesetzlich ebenfalls einen datenschutzrechtlichen »Vorbehalt des Gesetzes«[77], der eigentlich nur im Bürger-Staat-Verhältnis zur Anwendung kommt.

Unter Privaten entfalten Grundrechte nur eine **mittelbare Drittwirkung**. Darunter ist die Ausstrahlungswirkung der Grundrechte als objektive Ordnung in das Privatrecht durch deren Beachtlichkeit bei der Auslegung von Rechtsnormen zu verstehen.[78]

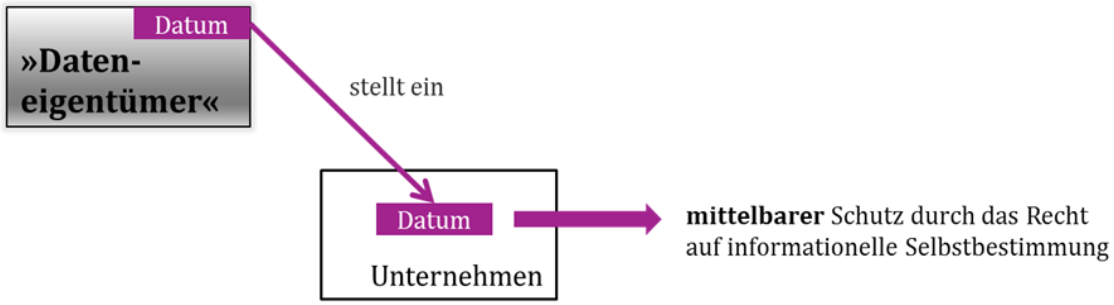

ABBILDUNG 5: MITTELBARE SCHUTZWIRKUNG DES RECHTS AUF INFORMATIONELLE SELBSTBESTIMMUNG GEGENÜBER UNTERNEHMEN

---

76 Starck (Fn. 27), Art. 2 Rn. 177.

77 Zum »Verbotsprinzip« jüngst Karg, DuD 2013, 75 ff.

78 Kischel, in: Epping/Hillgruber (Hrsg.), Beck'scher Online-Kommentar GG (Ed. 15, 01. 07. 2012), Art. 3 Rn. 85.

Dem Staat obliegt die Pflicht, vor Gefahren zu schützen: »Wo die technische Entwicklung, von wem auch immer initiiert und befördert, mit neuen Produkten und Prozessen auch neue Gefahren schafft, die ebenso außer Kontrolle geraten können wie die Entwicklung selbst, muss der Staat den technischen Fortschritt kontrollierend und die betroffenen Grundrechte schützend begleiten«[79]. Da der technische Fortschritt jedoch unerlässlich und grundsätzlich nützlich ist, ist der Staat nicht dazu verpflichtet, alle mit dem technischen Fortschritt verbundenen Risiken restlos zu unterbinden bzw. zu beseitigen.[80] Bezogen auf von privaten Unternehmen betriebene Cloud-Services bedeutet dies, dass der Staat die **Rahmenbedingungen** dafür schaffen muss, dass das Recht des Bürgers auf informationelle Selbstbestimmung und das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme geschützt werden, indem er die Anbieter von Cloud-Services dazu verpflichtet, entsprechende Vorkehrungen zu treffen, und deren Einhaltung überwachen muss.

In diese Kategorie sind sowohl De-Safe-Dienste nach § 8 DeMailG als auch zum Teil P23R-Lösungen einzustufen. Diese werden in der Regel nämlich nicht von den Unternehmen selbst, sondern von Intermediären betrieben. Insofern kann derjenige, der »seine« Daten auslagert, sich zwar nicht unmittelbar auf das Recht auf informationelle Selbstbestimmung berufen und bspw. eine Speicherung, Weitergabe usw. verhindern, sondern lediglich auf die einfachgesetzlichen Vorgaben des BDSG und vor allem die Regelungen des jeweiligen Vertragsverhältnisses, zumal der zulässige Umfang der Datenverarbeitung insbesondere von der erteilten Einwilligung abhängt.

3.2.1.3 Entstehen von »Dreipersonenverhältnissen« Bürger – Unternehmen – Staat durch Freigabefunktionen

Neben diesen beiden »Zweipersonenverhältnissen« können aber im Zusammenhang mit Cloud-Diensten auch »Dreipersonenverhältnisse« entstehen.

Denkbar sind folgende Varianten:

1. Die Nutzung eines Drittanbieters zur Ablage und Verwaltung der eigenen Datenbestände (bspw. De-Safe) und nachfolgend die **Freigabe** einzelner Daten und Dokumente an einen privaten, behördlichen oder unternehmerischen Empfänger

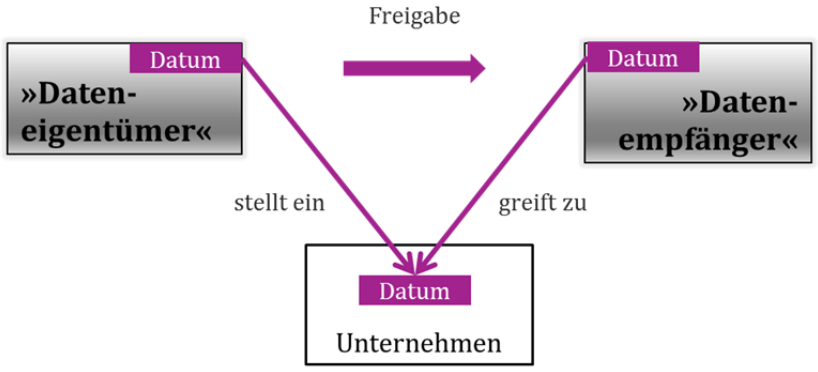

ABBILDUNG 6: »DREIPERSONENVERHÄLTNIS« AUFGRUND VON FREIGABEN

[79] Pieroth/Schlink (Fn. 37), Rn. 110.

[80] BVerfGE 56, 54 (80 ff.).

2. Die **Freigabe von »drittbezogenen Daten«** durch ein Unternehmen oder eine Behörde an eine weitere (juristische) Person, bspw. indem die in P23R enthaltenen Datensätze auch personenbezogene Daten der Arbeitnehmer des meldepflichtigen Unternehmens enthalten

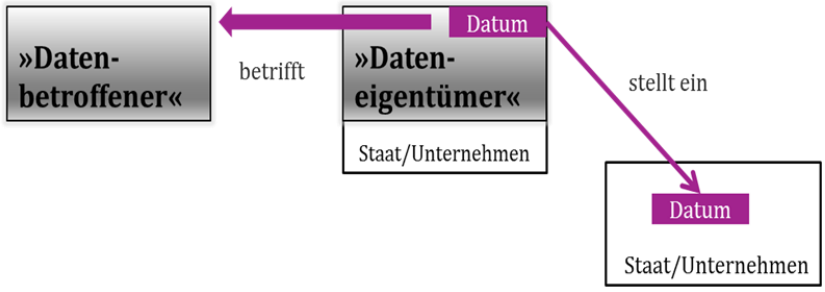

ABBILDUNG 7: »DREIPERSONENVERHÄLTNIS« DURCH DIE FREIGABE DRITTBEZOGENER DATENSÄTZE

3. Schließlich **alle anderen Arten von Drittzugriffen** auf Datensätze, die beim Staat oder einem Unternehmen gespeichert sind, bspw. seitens des Staates aus Gründen der Gefahrenabwehr oder zur Strafverfolgung

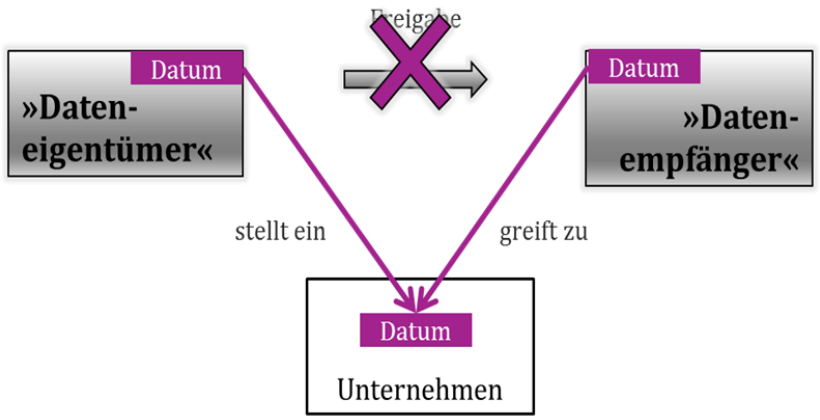

ABBILDUNG 8: NICHT-LEGITIMIERTE DRITTZUGRIFFE

Die erste Variante liegt vor, wenn der Cloud-Service eine Freigabefunktion besitzt und der Bürger davon Gebrauch macht. Wird die Cloud vom **Staat** betrieben und gibt der Bürger die darin gespeicherten Daten einem Unternehmen oder einer anderen staatlichen Stelle frei, so stellt sich die Situation ebenso dar wie soeben (3.2.1.1) geschildert, weil der Staat hier als unmittelbar Grundrechtsverpflichteter dafür zu sorgen hat, dass die Rechte auf informationelle Selbstbestimmung und auf Integrität und Vertraulichkeit informationstechnischer Systeme gewahrt werden. Insbesondere folgt daraus die Pflicht des Staates, sich an Anweisungen bezogen auf die Freigabe zu halten. Dieser Grundgedanke zeigt sich auch an § 5 des Entwurfes eines E-Government-Gesetzes des Bundes, zumal der Zugriff auf an anderer – staatlicher – Stelle gespeicherten Daten nur beim Vorliegen einer Einwilligung und selbstverständlich nur in deren Rahmen zulässig ist. Wird die Cloud von einem **Unternehmen** betrieben und

findet eine Freigabe für ein anderes Unternehmen oder eine staatliche Einrichtung statt, gilt Entsprechendes, allerdings nur aufgrund der einfachgesetzlichen Vorgaben des BDSG und einer mittelbaren Grundrechtswirkung. Das die Cloud betreibende Unternehmen muss sich schon aufgrund der vertraglichen Abrede mit dem Bürger an die Modalitäten der Freigabe halten. Dem Staat obliegt für den Schutz der Rechte des Bürgers eine Schutzpflicht.

Daraus erklärt sich auch, dass in der zweiten Variante zunächst einmal zu klären ist, ob die Weitergabe (Freigabe) an einen Dritten von der ursprünglichen Einwilligung abgedeckt ist. Liegt eine solche vor, ist diese als Legitimation ausreichend. Ansonsten bedarf es einer gesetzlichen Ermächtigung zur Verarbeitung drittbezogener Datensätze (Vorbehalt des Gesetzes), die gerade im Bereich der Arbeitgebermeldungen, welche auch Arbeitnehmerdaten beinhalten, sowohl die Speicherung (die schon für eigene Zwecke des Arbeitgebers, bspw. Lohnabrechnung etc., erforderlich ist) als auch die Weitergabe an bestimmte staatliche Stellen abdecken wird.

Schließlich entstehen »Dreipersonenverhältnisse« auch, wenn ein **externer Datenzugriff** stattfindet, ohne dass eine Freigabe durch den Bürger vorliegt. In erster Linie ist hier an staatliche Zugriffe auf die Daten – etwa im Rahmen eines Ermittlungsverfahrens – zu denken. Dieser Zugriff auf die Daten durch den Staat bedarf zwingend einer **Rechtsgrundlage** und die Daten dürfen ausschließlich dem Zweck der Rechtsgrundlage entsprechend verwendet werden. Datenzugriffe durch Unternehmen und sonstige Private müssen ausgeschlossen bleiben. Dafür trifft den Staat eine grundrechtliche Schutzpflicht.

3.2.1.4 »Vierpersonenverhältnisse« – Schutzfunktion der Auftragsdatenverarbeitung

Anders als in den beschriebenen Konstellationen stellt sich die Situation dar, wenn nicht der originär Verfügungsberechtigte Daten in eine Cloud einstellt – die in eigener Entscheidung auch eine »unsichere« sein kann – und anderen Akteuren freigibt, sondern wenn ein Dritter (bspw. auch der Anbieter von Online-Festplatten) mit diesen personenbezogenen Daten umgeht. Fraglich ist, was hier unter Datenhoheit zu verstehen ist. Liegt die Datenhoheit weiterhin beim Betroffenen, gibt es eine geteilte Datenhoheit oder wird diese letztlich nur durch die datenhaltende Stelle ausgeübt? Anwendungsfälle sind vielfach denkbar: So erscheint die Auslagerung von Datenbeständen, einschließlich personenbezogener Daten, gerade durch kleinere Unternehmen, Gewerbetreibende oder Freiberufler, wie z. B. Versicherungsmakler, Steuerberater und Rechtsanwälte, angesichts der Einsparpotenziale eine zielführende Alternative zur eigenen IT-Infrastruktur.

Dem Umstand, dass dem letztlich Betroffenen »seine« Datenhoheit (bzw. die Verfügungsbefugnis) zum Teil genommen wird, er sich gegenüber dem Anbieter auch nur auf einen mittelbaren Schutz berufen kann, wird ebenfalls durch staatliche Maßnahmen Rechnung getragen, mit denen dieser der Schutz- und objektiven Gewährleistungsfunktion der Grundrechte nachkommt. Grundsätzlich ist dem Dritten, der mit »fremden« personenbezogenen Daten umgeht, die Weitergabe dieser Daten untersagt. In Betracht kommen lediglich eine Einwilligung, das Vorliegen der Voraussetzungen einer Auftragsdatenverarbeitung oder einer zulässigen Datenübermittlung.

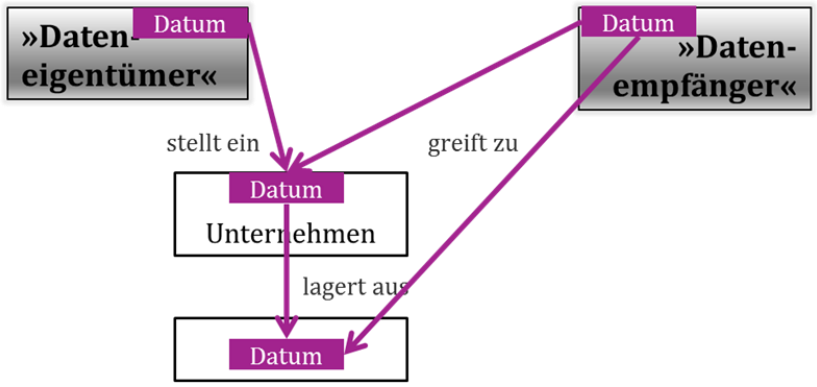

ABBILDUNG 9: »VIERPERSONENVERHÄLTNISSE«

3.2.2 Cloud Computing

Die datenschutzrechtliche Beurteilung des Einsatzes des Cloud Computing bestimmt sich für all diejenigen **öffentlichen und nicht-öffentlichen Stellen**, die vom Anwendungsbereich des BDSG oder eines LDSG erfasst werden,[81] nach diesem Regime. Der Umgang mit personenbezogenen Daten ist trotz unterschiedlicher Ausgangssituation (dazu 3.2.1.2) bei beiden Gruppen ähnlich zu beurteilen.[82] Lediglich fachspezifisch können für einzelne Behörden spezielle Datenschutzvorgaben (bspw. nach dem SGB) hinzu treten. Da das Modell der Virtualisierung vorsieht, dass, wenn ein Kunde Speicherkapazitäten benötigt, ihm diese von unterschiedlichen Servern zur Verfügung gestellt werden, ist es für das Cloud Computing charakteristisch – quasi systemimmanent –, dass die Nutzerdaten auf Servern verarbeitet und gespeichert werden, die weltweit verteilt sein können.[83] Ist der zunächst genutzte Server ausgelastet, wird automatisch ein anderer Server, in der Regel unabhängig vom Standort, zugeschaltet.

Kommt es bei der Nutzung Cloud-basierter Dienste zur Verarbeitung personenbezogener Daten, ist im Verhältnis des nutzenden Unternehmens bzw. der öffentlichen Verwaltung zum Anbieter von einer **Auftragsdatenverarbeitung** i. S. d. § 11 BDSG auszugehen. Der Auftraggeber bleibt datenschutzrechtlich verantwortlich; er ist gem. § 11 Abs. 2 Satz 1 und 4 BDSG zur sorgfältigen Auswahl und Überwachung des Anbieters verpflichtet. Entsprechende Aufträge sind schriftlich zu erteilen, wobei Verarbeitungsprozesse, technische und organisatorische Maßnahmen sowie etwaige Unterauftragsverhältnisse detailliert festzulegen sind.[84]

---

81 Die Entscheidung einer Privatperson, ihre Daten in Angeboten eines Dritten zu lagern, ist hingegen keinen rechtlichen Restriktionen unterworfen. Ob er eine »sichere« oder »unsichere« Lösung wählt, bleibt eine privatautonome Entscheidung; sie kann gerade ausgehend von unterschiedlichen Sicherheitsanforderungen auch variieren.

82 Zum Einsatz durch private Unternehmen Spies, MMR 5/2009, XI ff.; Pohle/Ammann, CR 2009, 273 (276 f.); Niemann/Paul, K&R 2009, 444 (448 ff).

83 Pohle/Ammann, CR 2009, 273 (274).

84 Simitis/Walz, BDSG, 6. Aufl. 2006, § 11 Rn. 50 ff.; s. auch Pohle/Ammann, CR 2009, 273 (276).

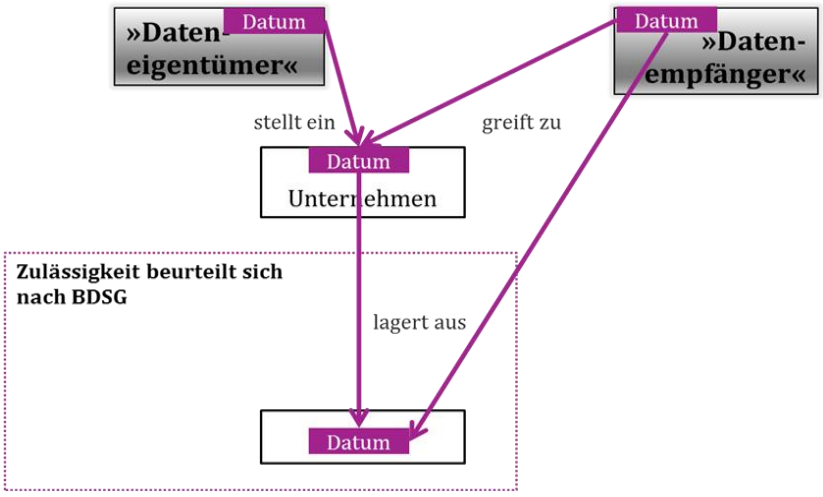

ABBILDUNG 10: SCHUTZFUNKTION DER AUFTRAGSDATENVERARBEITUNG

Gerade durch die exzessive Nutzung derartiger Unterauftragsverhältnisse treten Gefahren für den Schutz der personenbezogenen Daten auf – sie ist aber für eine öffentliche Cloud idealtypisch und prägend, zumal ein Cloud-Anbieter in der Regel zumindest in Zeiten einer Höchstauslastung zum Zukauf externer Server-, Rechen- und Softwarekapazitäten gezwungen ist. Hinzu kommt, dass personenbezogene Daten nicht ohne Weiteres in Drittstaaten außerhalb der Europäischen Union übermittelt werden dürfen. Eine solche Übermittlung ohne Einschränkungen in Staaten außerhalb der Europäischen Union bzw. des Geltungsbereichs der Richtlinie 95/46/EG ist nur gem. § 4b Abs. 2 und 3 BDSG statthaft, wenn in den einbezogenen Drittstaaten ein angemessenes Datenschutzniveau sichergestellt ist. Scheidet eine Auftragsdatenverarbeitung also in der Regel aus, käme eine Datenübermittlung in Betracht, die jedoch ebenfalls nur beim Vorliegen einer konkreten Einwilligung oder unter den strengen Voraussetzungen der §§ 28 ff. BDSG zulässig ist.[85] Das Kostensparinteresse wird keine Rechtfertigung für eine Weitergabe und Auslagerung der Daten Dritter geben können; Gleiches gilt für die Vereinfachung von Geschäftsprozessen aufgrund der dann möglichen Freigabe an weitere Datenempfänger.

3.2.3 Elektronische Daten- und Dokumentenspeicher

Bei der Auslagerung von möglicherweise sensiblen personenbezogenen Daten und Dokumenten auf externe Provider stellt sich insbesondere dem Nutzer die Frage, ob und unter welchen Voraussetzungen die Daten anderweitigen – als den selbst legitimierten – Zugriffen zugänglich sind. So könnten sowohl die über den Safe geführte Kommunikation (3.2.3.1) als auch die im Safe gespeicherten Inhalte (3.2.3.2) durch die Strafverfolgungs- oder andere Sicherheitsbehörden beim Provider sichergestellt bzw. beschlagnahmt werden. Dabei unterliegen die Daten jedoch einem umfassenden verfassungs- und einfachgesetzlichen Schutz.

[85] Niemann/Paul, K&R 2009, 444 (449).

3.2.3.1 Verfassungsrechtlicher Schutz der Safe-Kommunikation

Ebenso wie die verkörperte Papierpost vom Brief- und Postgeheimnis aus Art. 10 GG geschützt ist, unterliegen elektronische Nachrichten, wie sie im Rahmen der Kommunikation über Dokumentensafes möglich sind, dem Schutz des **Fernmeldegeheimnisses**. Dieses ebenfalls in Art. 10 GG enthaltene Grundrecht schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe der Telekommunikationstechnologien.[86] Ziel ist, die Beteiligten dabei möglichst so zu stellen, wie sie bei einer Kommunikation unter Anwesenden stünden.[87]

Aufgrund der Entwicklungsoffenheit des Grundrechts ist dabei nicht nur die Kommunikation mittels traditioneller Medien erfasst, sondern jede Kommunikation mittels der verfügbaren Telekommunikationstechnologien.[88] Für den Schutz ist es irrelevant, wie die Telekommunikation technisch vermittelt und in welcher Form die Inhalte übertragen werden.[89] Der Schutz des Fernmeldegeheimnisses erstreckt sich auf unterschiedliche Übertragungsformen, unabhängig davon, welche Übermittlungsart oder Ausdrucksform genutzt wird.[90] Erfasst werden daher nicht nur die für den öffentlichen Verkehr bestimmten Fernmeldeanlagen, sondern alle technisch verfügbaren Mittel der unkörperlichen Kommunikation. Darunter fallen u. a. Kabel, Telefon, Telegramm, Funkverkehr, Teletext, Telefax[91], Bildschirmtext oder E-Mail.[92] Als Ausdrucksform kommen neben Sprache oder Text auch Bilder, Töne, Zeichen oder sonstige Daten in Betracht.[93] Damit unterliegt auch die Cloud-basierte Kommunikation, also bspw. die Versendung oder Freigabe von Dokumenten, dem verfassungsgewährleisteten Schutz des Art. 10 GG. Geschützt sind die näheren **Umstände des Kommunikationsvorgangs**, oft als Verkehrs- oder Verbindungsdaten bezeichnet.[94] Dazu zählt, ob, wann und wie oft zwischen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder dieser versucht wurde.[95] Insofern ist die Kommunikation zum Cloud-Anbieter ebenfalls erfasst.

3.2.3.2 Verfassungsrechtlicher Schutz der im Safe gespeicherten Inhalte

Schwieriger ist die Frage zu beantworten, ob der verfassungsrechtliche Schutz auch für die in der Cloud abgelegten Daten gilt. Denn von Art. 10 GG ist stets nur die **»laufende Kommunikation«** geschützt, sodass bezweifelt werden kann, ob dieses Erfordernis auch (noch) für dauerhaft gespeicherte Daten angenommen werden kann.

Diesbezüglich kann eine Parallele zu E-Mails gezogen werden, die auf dem Mailserver eines Providers zwischen- bzw. endgespeichert sind. Während lange Zeit umstritten war, welchem

---

86 Ipsen, Grundrechte, 13. Aufl. 2010, Rn. 306; Jarass, in: ders./Pieroth (Hrsg.), GG, 11. Aufl. 2011, Art. 10 Rn. 5; Pagenkopf, in: Sachs (Hrsg.), GG, 5. Aufl. 2009, Art. 10 Rn. 15; Pieroth/Schlink (Fn. 37), Rn. 837.

87 BVerfGE 115, 166 (182).

88 BVerfGE 46, 120 (144); 115, 166 (182).

89 BVerfGE 106, 28 (36); 115, 166 (182).

90 Durner, in: Maunz/Dürig (Fn. 30), Art. 10 Rn. 82.

91 Zweifel zur Einordnung noch bei Schmittmann, RDV 1995, 234 (237).

92 BVerfGE 113, 348 (383).

93 Durner (Fn. 30), Art. 10 Rn. 82.

94 Baldus, in: Epping/Hillgruber (Fn. 78), Art. 10 Rn. 8.

95 BVerfG, NJW 2006, 976.

Grundrechtsschutz solche E-Mails unterliegen,[96] hat das BVerfG im Jahr 2009 entschieden, dass auch die Sicherstellung und Beschlagnahme solcher E-Mails am Grundrecht auf Gewährleistung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG zu messen ist.[97] Da sich die auf dem Server eines Anbieters gespeicherten E-Mails nicht im Herrschaftsbereich des Kommunikationsteilnehmers, sondern des Providers befinden, leidet der Kommunikationsteilnehmer an einem Mangel der Beherrschbarkeit. Auch wenn ein Zugriff durch technische Maßnahmen erschwert werden kann, schließt dies nicht aus, dass Strafverfolgungsbehörden evtl. in der Lage sind, auf die gespeicherten Inhalte zuzugreifen.[98]

Diese Argumentation lässt sich – grundsätzlich – auch auf die im Safe gelagerten Daten übertragen. Das BVerfG hat klargestellt, dass es für Art. 10 Abs. 1 GG irrelevant ist, ob es sich bei den beschlagnahmten Daten um **zwischen- oder um endgespeicherte, gelesene oder ungelesene Nachrichten** handelt. Ausreichend ist, dass es sich um elektronische Nachrichten handelt, sie also einen **Bezug zum Kommunikationsvorgang** aufweisen. Ein mit der Nutzung eines elektronischen Safes verbundener Vorteil ist die Freigabemöglichkeit von Dokumenten, mit der ausgewählten Dritten die Möglichkeit des Zugriffs eröffnet wird. Der Verzicht auf einen dynamischen Kommunikationsvorgang seitens des BVerfG in dem Sinne, dass nicht nur ungelesene E-Mails vom Schutzbereich des Art. 10 GG erfasst sind, führt dazu, dass auch die dauerhaft im Safe gespeicherten Daten dem Schutzbereich des Art. 10 Abs. 1 GG unterliegen sollen. Bereits mit dem potenziellen Kommunikationsbezug ließe sich die Zuordnung aller im Safe vorgehaltenen Daten zu Art. 10 GG begründen.[99] Eine Differenzierung zwischen den freigegebenen und nicht freigegebenen Daten sei schon deshalb ausgeschlossen, da sich nicht gewährleisten ließe, wer die Trennung der Daten vornehmen soll. Sollte dies dem Provider technisch möglich sein oder ließe er einen staatlichen Zugriff zu, so würde er damit jedenfalls auch den Zugriff zu den auf Dauer abgelegten Daten ohne Kommunikationsbezug eröffnen. Soweit jedoch keine Freigabemöglichkeit besteht, fehlt es am nötigen Kommunikationsbezug der im elektronischen Safe gelagerten Daten. Da insoweit **keine »Nachrichtenähnlichkeit«** vorliegt, wäre der Schutzbereich von Art. 10 GG nicht eröffnet. Vielmehr müsste der grundrechtliche Schutz der (personenbezogenen) Daten hier nach dieser Ansicht lediglich aus dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG) resultieren.

Problematisch an dieser Differenzierung ist jedoch, dass es vom **Zufall** abhängt, durch welches Grundrecht die in einer Cloud gelagerten Daten geschützt werden; zufällig deshalb, weil die Möglichkeit einer Freigabe in einem Moment vorhanden sein kann und in einem anderen nicht mehr. So könnte etwa der reine Speicherplatz kostenlos sein, während die Freigabemöglichkeit eine kostenpflichtige Zusatzoption darstellt. Endet der der Zusatzoption zugrundeliegende Vertrag, so besteht die Freigabemöglichkeit nicht mehr. Ebenso könnte sie durch die erneute Buchung der Freigabeoption kurz darauf wieder bestehen. Es erscheint unbefriedigend, dass hier aufgrund der als zufällig erscheinenden Freigabemöglichkeit jeweils unterschiedliche Schutzbereiche eröffnet sein sollen, zumal es immer um ein

---

96 Vgl. etwa Palm/Roy, NJW 1996, 1791 ff.; Schlegel, HRRS 2007, 44 ff.

97 BVerfGE 124, 43 ff.; dazu Albrecht, jurisPR-ITR 25/2009, Anm. 4; Brodowski, JR 2009, 402 ff.; Brunst, CR 2009, 591 ff.; Härting, CR 2009, 581 ff.; Keller, Kriminalistik 2009, 491 ff.; Klein, NJW 2009, 2996 ff.; Krüger, MMR 2009, 680 ff.; Störing, CR 2009, 475 ff.; Szebrowski, K&R 2009, 563 ff.; Durner, JA 2010, 238 ff.; Gurlit, NJW 2010, 1035 (1036 f.).

98 BVerfGE 124, 43 (54).

99 Wie hier Bäcker, in: Rensen/Brink (Hrsg.), Leitlinien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 99 (109, 117); ders., in: Lepper (Hrsg.), Privatsphäre mit System – Datenschutz in einer vernetzten Welt, 2010, S. 4 (16 ff.).

und dasselbe Schutzgut, nämlich die personenbezogenen Daten des Bürgers, geht. Überdies scheint nicht eindeutig zu klären zu sein, wann genau eine Freigabeoption vorliegt und wann nicht bzw. in welchen Fällen die notwendige Nachrichtenähnlichkeit vorliegt, um einen Kommunikationsbezug anzunehmen. Muss die Freigabe für Dritte etwa durch das genutzte System vorgesehen sein oder genügt die rein faktische Möglichkeit der Freigabe? Nähme man Letzteres an, so müsste man wohl davon ausgehen, dass hinsichtlich elektronischer Safes und Clouds stets ein möglicher Kommunikationsbezug bestünde, weil die darin gespeicherten Daten stets durch eine Weitergabe der Zugangsdaten durch den Nutzer des Angebots an einen Dritten anderen Personen zugänglich gemacht werden können. Nähme man Ersteres an, so ergäbe sich ein mit der herrschenden Dogmatik wohl nicht zu lösendes Abgrenzungsproblem zwischen den Schutzbereichen von Art. 10 GG und Art. 2 Abs. 1 GG. Weitere Abgrenzungsschwierigkeiten sind aufgrund des fortschreitenden technischen Fortschritts und der damit einhergehenden Erweiterung der Möglichkeiten der Safe- und Cloud-Nutzer, mit ihren Daten umzugehen, zu erwarten. Daher müssen entwicklungsoffene Abgrenzungskriterien gefunden werden.

Eine Lösung der Abgrenzungsproblematik könnte dadurch herbeigeführt werden, dass das Schutzgut der personenbezogenen Daten in den Fokus gerückt wird. Ausgehend von der großen Bedeutung personenbezogener Daten für den Einzelnen erscheint es interessengerecht, das Recht auf informationelle Selbstbestimmung im Hinblick auf die personenbezogenen Daten als Lex specialis anzusehen. Der **Inhaltsschutz** könnte somit durchweg durch **Art. 2 Abs. 1 GG** gewährleistet werden, ohne dass es zu Abgrenzungsschwierigkeiten kommt. Der Schutz der genutzten Infrastruktur wäre dann, je nachdem, welches System genutzt wird, durch Art. 10 GG (bei Kommunikationssystemen) oder Art. 2 Abs. 1 GG in seiner Ausprägung als Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (bei statischen Systemen) gewährleistet.[100]

	Daten/Inhalte	Infrastruktur
Räumliche Infrastruktur	**Art. 2 Abs. 1 GG** (ggf. beim Menschenwürdegehalt i. V. m. Art. 1 Abs. 1 GG)	**Art. 13 Abs. 1 GG** Begrenzung des Systemschutzes auf Wohnräume
Telekommunikationsinfrastruktur	**Art. 2 Abs. 1 GG** (ggf. beim Menschenwürdegehalt i. V. m. Art. 1 Abs. 1 GG)	**Art. 10 Abs. 1 GG** Begrenzung des Systemschutzes auf die Kommunikation zwischen zwei Personen
Computerinfrastruktur	**Art. 2 Abs. 1 GG** (ggf. beim Menschenwürdegehalt i. V. m. Art. 1 Abs. 1 GG)	**Art. 2 Abs. 1 GG (Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)** Begrenzung des Systemschutzes auf komplexe Systeme, die auch personenbezogene Daten enthalten

TABELLE 2: ABGRENZUNG VON SYSTEM- UND DATENSCHUTZ (TELEKOMMUNIKATIONSINFRASTRUKTUR)

[100] So auch Bosesky/Hoffmann/Schulz, DuD 2013, 95 ff.

3.2.3.3 Einfachgesetzlicher Schutz

Der verfassungsrechtlichen Differenzierung folgend existieren auch im einfachen Gesetzesrecht verschiedene Rechtsregime, die einerseits die grundgesetzlichen Verbürgungen zum Teil wiedergeben und konkretisieren, andererseits aber auch bereichsspezifischen Datenschutz sicherstellen wollen.

Für den Bereich der **Telekommunikationsdienstleistungen** existiert in den §§ 88 ff. des Telekommunikationsgesetzes (TKG) eine einfachgesetzliche Ausformung des Fernmeldegeheimnisses, zumal der Regelungsgegenstand des TKG (Telekommunikation) dem Schutzbereich des Fernmeldegeheimnisses (unkörperliche Kommunikation) entspricht. Dies bedeutet umgekehrt allerdings nicht, dass nicht auch Schutzgüter des Art. 10 Abs. 1 GG, speziell des Fernmeldegeheimnisses, existieren, die nicht vom TKG erfasst werden. Regelungen zum Umgang mit den im Zusammenhang mit der Telekommunikation typischerweise erhobenen und verarbeiteten personenbezogenen Daten – Bestands-, Verkehrs- und Inhaltsdaten – finden sich in den §§ 91 ff. TKG, die als bereichsspezifischer Datenschutz in ihrem Regelungsbereich Vorrang genießen. Ergänzend tritt für bestimmte Dienstleistungen, die auf Grundlage der vom TKG erfassten Telekommunikation erbracht werden, den sog. **Telemediendiensten**, das Telemediengesetz (TMG) hinzu, welches in den §§ 11 ff. ebenfalls bereichsspezifischen Datenschutz sicherstellen soll.

Nur soweit die genannten Gesetze keine Regelungen enthalten bzw. hinsichtlich der datenschutzrechtlichen Vorgaben als nicht abschließend anzusehen sind, besitzen auch das BDSG bzw. die landesrechtlichen Entsprechungen Relevanz für die datenschutzrechtliche Bewertung elektronischer Dokumentensafes und von Cloud-Angeboten. Da Anbieter elektronischer Safes auch die Funktion anbieten, Daten ausgewählten Dritten freizugeben, bzw. Dritte Dokumente in den Safe einstellen können, bestehen aus rechtlicher Perspektive Parallelen zu den E-Mail-Diensten. Je nachdem, wie diese Funktion technisch realisiert wird, handelt es sich bei diesem Dienst um einen Telekommunikationsdienst i. S. d. § 3 Nr. 24 TKG oder einen elektronischen Informations- und Kommunikationsdienst nach § 1 Abs. 1 TMG.

Die erforderliche funktionelle Abgrenzung der Anwendungsbereiche der verschiedenen datenschutzrechtlichen Regelungen erfolgt dabei anhand des sog. Schichtenmodells.[101] Davon ausgehend wird danach differenziert, ob es um die Übertragung von Inhalten oder das Angebot und die Verantwortung für die Inhalte geht. Das TKG regelt die Technik und Marktregulierung von Diensten, welche die Übertragung von Nachrichten ohne Rücksicht auf deren Inhalt zum Gegenstand haben, während das TMG diese Inhalte regelt.[102] Bei gemischten Angeboten ist ein »Aufschnüren« des Leistungspakets mit anschließender Einordnung der einzelnen Leistungsmerkmale geboten.[103]

Strittig ist dies neben den E-Mail-Diensten auch bei der »reinen« **Zugangsgewährung zum Internet** (»Internet-Access«), bei der der Provider nur für eine Datenübertragung fremder Inhalte aus dem Internet zum Kunden (und umgekehrt) sorgt.[104] Wichtig ist es

---

[101] Eckhardt, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2008, § 91 TKG Rn. 5; das sog. »Schichtenmodell« wird auch durch die Datenschutzaufsichtsbehörden des Bundes und der Länder zugrunde gelegt; s. Gola/Klug, Grundzüge des Datenschutzrechts, 2003, S. 59 f., 189; Schaar, MMR 2001, 644 (645).

[102] Eckhardt (Fn. 101), § 91 TKG Rn. 5.

[103] LG Darmstadt, K&R 2006, 290 ff.; Schmitz, MMR 2003, 215; Eckhardt, K&R 2006, 293 (294); Schuster, in: Geppert u. a. (Hrsg.), Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 3 Rn. 49; Cebulla, DuD 2010, 308 (308).

[104] Schmitz, in: Spindler/Schuster (Fn. 82), § 1 TMG Rn. 17.

dabei, Begrifflichkeiten und Dienste klar nach ihren Funktionen zu beschreiben und zu unterscheiden.[105] »Reine« Internet-Accessdienste, bei denen keinerlei Inhalt vom Anbieter ausgesucht oder aufbereitet wird, die also nur die Erreichbarkeit eines Peeringpunktes mit dem Internet hergestellten und Navigation und Auswahl der im Internet verfügbaren Inhalte und Dienste alleine dem Nutzer überlassen,[106] sind als Telekommunikationsdienste einzuordnen, da funktional betrachtet keinerlei Inhalte vom Access-Provider aufbereitet oder geändert werden.[107] Von diesem reinen Internet-Access sind Zugangsdienste zu unterscheiden, bei denen der Anbieter selbst auch Inhalte anbietet oder zumindest aufbereitet oder aussucht. Dies ist insbesondere bei den Internetzugangsdiensten der Fall, welche eigene Portalseiten anbieten. Diese Dienste nehmen folglich sowohl die Funktion der Zugangsgewährung zum Internet als auch der Bereitstellung von Inhalten wahr[108] und sind damit – je nach betroffenem Teil des Angebots – auch als Telemediendienste zu bewerten.

Die gleiche Differenzierung ist bei **E-Mail-Diensten** zu treffen. »Reine« E-Mail-Dienste bieten nur die Übertragung von Nachrichten an, die der Nutzer selbst auf seinem Rechner verfasst und dann dem Anbieter zur Übertragung übergibt. Dieser Dienst unterscheidet sich technologieneutral und funktional betrachtet nicht von der klassischen Datenübertragung von Sprache oder der Versendung eines Telefaxes.[109] Der Dienst kann deshalb als Telekommunikationsdienst eingeordnet werden. Hiervon zu unterscheiden sind die Online-E-Mail-Dienste, die neben der Übertragungs- und Übermittlungsfunktion einen im Internet erreichbaren Dienst anbieten, der das Schreiben, Lesen und Verwalten von E-Mails mittels der vom Anbieter online zur Verfügung gestellten (Software-)Systeme ermöglicht.[110] Der Rechner des Nutzers dient insofern nur als Eingabe- und Ausgabegerät, die eigentliche Datenverarbeitung findet mittels der Online-Plattform des Anbieters statt;[111] insofern ist die Rechtslage derjenigen beim »Software as a Service (SaaS)« vergleichbar. »Online-E-Mail-Dienste« sind daher hinsichtlich des Teilaspekts, bei dem zusätzlich Inhalte aufbereitet[112] oder Applikationen zur Verfügung gestellt werden, als Telemediendienste einzuordnen.

Für die Cloud-basierte Kommunikation, also die Freigabe und das Einstellen von Daten in einen Safe, hat also auf der Grundlage einer funktionalen Betrachtung die Unterscheidung zwischen der Übertragung einer Nachricht (**Transportebene**) und damit TKG sowie deren inhaltlicher Aufbereitung bzw. Bereitstellung zum Abruf (**Anwendungsebene**) und damit TMG zu erfolgen[113]. Ist der Zugriff zur Cloud lediglich über ein clientbasiertes Verfahren möglich, handelt es sich um eine reine Übertragung von (fremden) Inhalten und damit um einen Telekommunikationsdienst i. S. d. § 3 Nr. 24 TKG. Wird dagegen der Zugriff auch über ein webbasiertes Verfahren ermöglicht, bietet der Anbieter durch das Zurverfügungstellen der Onlineplattform zugleich Inhalte an, wodurch dieses Angebot als Telemediendienst i. S. d. § 1 Abs. 1 TMG einzuordnen ist.

---

105 Schmitz (Fn. 104), § 1 TMG Rn. 17.
106 Schmitz (Fn. 104), § 1 TMG Rn. 17.
107 BGH, CR 2004, 355 ff.; OVG Münster, K&R 2003, 305.
108 Schmitz (Fn. 104), § 1 TMG Rn. 17.
109 Schmitz (Fn. 104), § 1 TMG Rn. 18.
110 Schmitz (Fn. 104), § 1 TMG Rn. 18.
111 Schmitz (Fn. 104), § 1 TMG Rn. 18.
112 Schmitz (Fn. 104), § 1 TMG Rn. 18.
113 Eckhardt (Fn. 101), § 91 TKG Rn. 5.

3.2.4 Elektronische Identitäten

Da für Zugriffserlaubnisse und Freigaben das Identitätsmanagement eine herausragende Rolle spielt, zumal so sichergestellt werden kann, dass nur Berechtigte zugreifen, müssen auch die Rechtsgrundlagen »elektronischer Identitäten« beleuchtet werden. Technikgestütztes Identitätsmanagement soll verstanden werden als die durch einen rechtlichen Rahmen reglementierte,[114] in der Regel webbasierte,[115] seitens eines Serviceproviders angebotene Möglichkeit, persönliche Daten, Dokumente, partielle Identitäten und Pseudonyme elektronisch zu speichern, zu verwalten und mittels unterschiedlicher Schreib-, Lese- und Zugriffsrechte anderen zu offenbaren.[116]

Hierzu zählen neben dem elektronischen Personalausweis (3.2.4.1), also hardwarebasierten Systemen (s. auch 3.2.4.2), auch Identitätsbestätigungsdienste (3.2.4.3), die, soweit ersichtlich, bisher nur in einem zu vernachlässigenden Umfang als eigenes Geschäftsmodell angeboten werden – obwohl sie, allerdings nur unter Inkaufnahme eines Medienbruchs, auch schon ohne den neuen Personalausweis zu realisieren gewesen wären. Durch die Nutzung des Postident-Verfahrens[117] – welches im Übrigen auch nicht gesetzlich erfasst ist –, bei dem die Identität durch die Vorlage des (klassischen) Personalausweises durch einen Angestellten der Deutschen Post AG überprüft und dem Anbieter von Dienstleistungen bestätigt wird, wäre es möglich, (auch im Internet) als Identitätstreuhänder in Erscheinung zu treten. Hinzu kommt die Entwicklung, dass zunehmend Kommunikationskanäle, die eigentlich der Nachrichtenübermittlung dienen, ebenfalls als Identifizierungsmittel eingesetzt werden (3.2.4.4).[118]

3.2.4.1 Elektronischer Identitätsnachweis

Das Thema »Identitätsmanagement« ist zwar nicht unmittelbar mit der Einführung des neuen Personalausweises verknüpft – offenbar bestehen allerdings Parallelitäten. Das »Gesetz über Personalausweise und den elektronischen Identitätsnachweis«[119] transformiert das herkömmliche – überwiegend auf hoheitliche Zwecke ausgerichtete – Ausweisdokument in die Welt des E-Government und des E-Commerce. Im hier zu bewertenden Kontext von untergeordneter Bedeutung ist die Erweiterung der hoheitlichen Ausweisfunktion durch das Recht, mittels hoheitlicher Berechtigungszertifikate i. S. d. § 2 Abs. 4 Satz 3 PAuswG[120] und unter Einsatz der RFID-Technologie unter den Voraussetzungen des § 17 PAuswG auch auf das elektronische Speicher- und Verarbeitungsmedium[121], das ausschließlich zu diesem

---

114 Wobei damit noch keine Aussage getroffen werden soll, in welchem Umfang ggf. eine spezielle Regulierung erforderlich ist. Auch die Geltung des »allgemeinen« Rechtsrahmens, bspw. durch das BDSG und TMG, soll als eine solche »Reglementierung« gelten.

115 Erfasst werden daher auch andere elektronische Fernkontakte ohne Einsatz einer Browser- bzw. Html-Technologie; bspw. im Rahmen von Bankingsoftware, bei der ein Direktkontakt zwischen Client und Server stattfindet.

116 Schulz, in: Schliesky (Fn. 44), S. 51 (52 ff.).

117 S. dazu Möller, NJW 2005, 1605 ff.

118 Zu diesem Aspekt auch Schulz, DVP 2011, 222 ff.

119 Personalausweisgesetz v. 18. 06. 2009 (BGBl I S. 1346), zuletzt geändert durch Art. 4 d. G. v. 22. 12. 2011 (BGBl I S. 2959).

120 Vgl. Schulz, in: Schliesky (Hrsg.), Gesetz über Personalausweise und den elektronischen Identitätsnachweis – Kommentar, 2009, § 2 Rn. 22.

121 Schulz (Fn. 120), § 17 Rn. 4 ff.

Zweck[122] biometrische Daten beinhaltet, zuzugreifen – anstatt wie bisher auf eine reine Sichtkontrolle angewiesen zu sein.

Neu und für den Einsatz im E-Commerce, im E-Government und damit auch im Kontext von Cloud-Anwendungen, die auf der Freigabe von Daten und Dokumenten basieren, von besonderem Interesse ist vor allem die eID-Funktion. Der elektronische Identitätsnachweis gem. § 18 PAuswG[123] ermöglicht dem Nutzer, einen Teil der auf dem Personalausweis gespeicherten Identitätsattribute an Diensteanbieter zu übermitteln. Diese werden wiederum von einer Vergabestelle mit Berechtigungszertifikaten ausgestattet, die dazu führen, dass eine gegenseitige Authentisierung erfolgt.[124] Bei der Zuteilung der Zertifikate wird präventiv insbesondere geprüft, welche Daten der Diensteanbieter für seinen Geschäftszweck benötigt.[125] Lediglich auf diese Daten kann er technisch zugreifen – und dies auch nur, wenn der Ausweisinhaber die Übermittlung der Daten im konkreten Fall durch die Eingabe einer Geheimnummer (PIN) freischaltet.[126]

Diese Funktionalität des Personalausweises ist geeignet, die Rolle des **notwendigen elektronischen Identifikators** für Dokumentensafes zu übernehmen. Dies gilt einerseits für das Erfordernis einer sicheren Erstregistrierung, um einen Datensafe einer realen Identität zuzuordnen, sowie andererseits im Kontext der Legitimation von Zugriffen Dritter. Der Cloud- bzw. Safeanbieter müsste sich ein entsprechendes Berechtigungszertifikat (bspw. hinsichtlich Vorname, Name, Geburtsdatum und Adresse) erteilen lassen, um personenbezogene Freigaben des Nutzers – dem Träger der Datenhoheit – rechtssicher ausführen und Gewähr dafür bieten zu können, dass tatsächlich nur an Berechtigte freigegeben wird.

Hinzu kommt, dass die eID-Funktion auch für die Nutzung gesetzgeberisch und infrastrukturell vom Staat begleiteter (bspw. De-Mail) oder rein privater Identitätsmanagement-Systeme (bspw. E-Postident) als eindeutiger Identifikator dienen und diese damit überhaupt erst (medienbruchfrei[127]) ermöglichen kann.

3.2.4.2 E-Card-Strategie

Neben dem elektronischen Personalausweis verfolgt die Bundesregierung im Rahmen der sog. »E-Card-Strategie« das Ziel, in weiteren Bereichen Verfahrensabläufe durch den Einsatz elektronischer Smartcards zu beschleunigen. Damit stünden weitere sichere hardwarebasierte Identifikatoren zur Verfügung. Während die Reise- und Ausweisdokumente – Reisepass, Personalausweis, aber auch **Aufenthaltstitel** – bereits in elektronischer Form, zum Teil auch unter Ausstattung mit Zusatzfunktionalitäten für den Einsatz im Privaten realisiert

---

122 Zu Zugriffsmöglichkeiten Privater Luch, in: Schliesky (Fn. 120), § 20 Rn. 9; Schulz, ebd., § 5 Rn. 15; ders., CR 2009, 267 (269); s. auch Süßmuth/Koch, Pass- und Personalausweisrecht, 4. Aufl. 2006, § 4 PAuswG Rn. 9; Wollweber, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 8.5 Rn. 32; unklar zur alten Rechtslage Reichl/Roßnagel/Müller (Hrsg.), Digitaler Personalausweis, 2005, S. 127, 150 f., 225; Hornung, Digitale Identität, 2005, S. 204 f.

123 Ausführlich Luch (Fn. 122), § 18 Rn. 5 ff.

124 Dazu Luch (Fn. 122), § 18 Rn. 24 ff.; s. auch Roßnagel/Hornung/Schnabel, DuD 2008, 168 (170): »Identität seines Interaktionspartners sicher zu validieren«; Hansen, DuD 2006, 543 (546): »beiderseitige Authentisierung«; vgl. auch Schulz, CR 2009, 267 (269).

125 Vgl. Schulz (Fn. 120), § 21 Rn. 23 ff.

126 Luch (Fn. 122) § 18 Rn. 24 ff.

127 Vgl. zur Option, eine digitale Signatur unter Nutzung des elektronischen Identitätsnachweises medienbruchfrei am heimischen PC zu erhalten Schulz (Fn. 120), § 22 Rn. 9.

werden, befindet sich die elektronische Gesundheitskarte noch in der Testphase. Gleiches gilt für die im Kontext von ELENA angedachte sog. JobCard[128].

So soll die **eGK** ein vernetztes Datenmanagement im Gesundheitswesen ermöglichen. Sie ist eingebettet in eine Infrastruktur, die gesicherte und vertrauliche Kommunikationsmöglichkeiten schafft.[129] In das Kartenlesegerät werden die elektronische Gesundheitskarte und der elektronische Heilberufsausweis (HBA) eingelesen und der »Konnektor« verbindet die Praxis mit den Servern der Telematik-Infrastruktur, auf denen die Patientendaten liegen.[130] Im Prinzip handelt es sich lediglich um ein »Freigabeinstrument« – den **Schlüssel** – zu existierenden Datenbeständen.

Gleiches gilt im Kontext von ELENA bzw. **OMS**. Beabsichtigt ist, dass, nachdem der Arbeitnehmer eine Chipkarte mit integriertem Zertifikat zur Erstellung qualifizierter elektronischer Signaturen von einem Zertifizierungsdienstanbieter (i. S. d. § 2 Nr. 8 SigG) erhalten hat, er diese bei der sog. Registratur Fachverfahren, einer zentralen öffentlich-rechtlichen Stelle, als JobCard registrieren lässt (vgl. § 100 SGB IV). Hierzu erfolgt eine Verknüpfung von Identifikationsnummer des Zertifikats der Chipkarte mit der Rentenversicherungsnummer des Arbeitnehmers. Unabhängig davon meldet der Arbeitgeber regelmäßig bestimmte Daten seines Arbeitnehmers an die zentrale Speicherstelle (vgl. § 97 SGB IV). Will ein Arbeitnehmer, der im Besitz einer JobCard ist, Leistungen, die vom neuen Verfahren erfasst werden, beziehen, ist lediglich eine Vorlage der Karte erforderlich: Mit der so erteilten Einwilligung zum Datenabruf und der die staatliche Stelle legitimierenden Signaturkarte wird der Abruf der Daten aus der zentralen Speicherstelle und so die Berechnung der Leistungen ermöglicht. Insofern übernimmt die JobCard, die in jede beliebige Karte integriert werden kann, ebenfalls nur eine **»Schlüsselfunktion«**.

Bedenkt man, dass es der elektronische Personalausweis aufgrund seiner Funktion ermöglicht, Zugriffe auf Datenbestände eindeutig an einen bestimmten Personenkreis zu binden, erscheinen diese Bestrebungen jedoch eher kontraproduktiv, zumal die Etablierung weiterer Kartensysteme eigentlich entbehrlich ist. Unnötigerweise kommt es in den Projekten »eGK« und »OMS« zu einer Verknüpfung des Aufbaus von bestimmten (zentralen) Datenbeständen mit den Modalitäten des rechtssicheren und eindeutig identifizierbaren Zugriffs auf diese Datenbestände. Eine separate Behandlung dieser Fragestellungen bei Fokussierung auf den **elektronischen Identitätsnachweis als zentrale Identitätsinfrastruktur** wäre insofern zielführender gewesen.

---

[128] Vgl. dazu Schöttle, in: Scherf/Schmieszek/Viefhues (Hrsg.), Elektronischer Rechtsverkehr, Kommentar und Handbuch, 2006, S. 176 ff.; Hornung (Fn. 103), S. 46 f., 241 ff.; s. auch Schaefer, ZRP 2006, 93 ff.; Ernestus, DuD 2004, 404 ff.; Hornung/Roßnagel, K&R 2004, 263 ff.

[129] Wirtz/Ullrich/Mory (Fn. 13), S. 16; Dietzel (Fn. 13), S. 2 (2 f.).

[130] Lücke/Köhler, Dtsch Med Wochenschrift 2007, 448 (449).

3.2.4.3 Identitätsbestätigungsdienste (vor allem § 6 DeMailG)

Als Identifizierungsdienste (= Verwaltung von partiellen Identitäten und Pseudonymen = **Identitätsmanagement**[131]) werden Funktionalitäten beschrieben, die es dem Nutzer ermöglichen, seine verschiedenen virtuellen Teilidentitäten (= Teilmengen der Identitätsattribute[132]) zu verwalten. Gesetzlich wird ein solcher Dienst – allerdings nur für De-Mail-akkreditierte Anbieter – von § 6 DeMailG aufgegriffen. Neben den nach § 6 DeMailG akkreditierten Anbietern etablieren sich derzeit auch weitere Angebote am Markt, die eine vergleichbare Funktion und das gleiche Sicherheitsniveau bieten, so bspw. der Dienst »E-Postident« der Deutschen Post AG, der enge Bezüge sowohl zum neuen Produkt »E-Postbrief«[133] als auch zum überkommenen Identifizierungsdienst »Postident«[134] aufweist.

Diese Dienste können auch als Authentisierungsdienste bezeichnet werden. Der Nutzer kann sich gegenüber anderen Fachverfahren und Diensten anderer Anbieter (Service Provider) authentisieren und diesen **überprüfte Identitätsattribute** zur Verfügung stellen. Zu diesem Zweck kann der Nutzer alle auf einem sicheren Weg – Postident oder elektronischer Identitätsnachweis – an den Diensteanbieter übermittelten Identitätsattribute beliebig zusammenstellen und je nach Anforderung des Service Providers individuell übermitteln. Dieses Vorgehen lässt einerseits die Notwendigkeit der Pflege zahlreicher Nutzer- und Kundenprofile entfallen, andererseits wird so der datensparsame Umgang mit sensiblen personenbezogenen Daten ermöglicht.

Derartige Dienste sind im Kontext von Daten- und Dokumentensafes also ebenfalls geeignet, sowohl den Safenutzer seitens des Safe-Anbieters sicher zu identifizieren als auch nachfolgend die Freigaben auf Berechtigte zu begrenzen. Identifizierungsdienste entsprechen daher von ihrer Funktion letztlich dem Einsatz des elektronischen Identitätsnachweises des neuen Personalausweises[135], stehen zu diesem jedoch auch in einem datenschutzrechtlichen Spannungsverhältnis.[136] Der Identitätsbestätigungsdienst nach § 6 DeMailG ist nämlich geeignet, die präventive Prüfung des Geschäftszwecks nach § 21 PAuswG durch die Vergabestelle für Berechtigungszertifikate leerlaufen zu lassen. Da auch die De-Mail-Anbieter als Diensteanbieter i. S. d. PAuswG in Erscheinung treten, werden sie sich Berechtigungszertifikate ausstellen lassen, die voraussichtlich *alle* anzufragenden Datenkategorien abdecken werden. Dies ist zum einen dem Umstand geschuldet, dass der De-Mail-Diensteanbieter zwingend auf eine sichere Erstregistrierung angewiesen ist – diese sogar gesetzlich verlangt wird. Zum anderen verlangt der Geschäftszweck »Anbieten des Identitätsbestätigungsdienstes nach § 6 DeMailG« die Übermittlung aller sicher verifizierbaren Daten. Sollte sich der Einsatz der De-Mail und des Identitätsbestätigungsdienstes nach § 6 DeMailG verbreiten,

---

131 Sorge/Westhoff, DuD 2008, 337 (337); zum Begriff Identitätsmanagement auch Hansen u. a., DuD 2003, 551 (551 ff.).

132 Sorge/Westhoff, DuD 2008, 337 (337).

133 Hoffmann u. a., Der E-POSTBRIEF in der öffentlichen Verwaltung – Chancen, Einsatzoptionen, rechtliche Handlungsspielräume, 2011; Hoffmann u. a., Der E-POSTBRIEF in der öffentlichen Verwaltung – Einsatzoptionen im Sozial- und Steuerverfahren sowie für Berufsgeheimnisträger, 2011; Brackmann u. a., Der E-POSTBRIEF in der Kommunalverwaltung – Einsatzoptionen für kommunale Fachverfahren, 2012; zu Einzelfragen Schulz/Tischer, NZS 2012, 254 ff.; Schulz, MMR 2011, 748 f.; ders., DuD 2011, 263 ff.; Luch/Tischer, DÖV 2011, 598 ff.; Hoffmann/Tallich/Warnecke, MMR 2011, 775 ff.

134 S. dazu Möller, NJW 2005, 1605 ff.

135 So auch Stach, DuD 2008, 184 (186): »Dieser Dienst [Identifizierungsdienst] kann insbesondere dann eingesetzt werden, wenn eine Person (noch) keinen elektronischen Personalausweis besitzt«.

136 Vgl. dazu Schulz (Fn. 120), § 21 Rn. 9 f.; s. auch ders., CR 2009, 267 (270).

besteht also die Gefahr, dass Anbieter anderer Dienste nicht auf ein Zertifikat nach § 21 PAuswG zurückgreifen, um selbst den elektronischen Identitätsnachweis durchzuführen. Stattdessen werden sie von ihren Kunden ein Vorgehen nach dem Identitätsbestätigungsdienst verlangen. Dabei sind sie zwar durch das BDSG und TMG auch auf die erforderlichen Daten beschränkt – allerdings wird dies dann nicht mehr präventiv staatlich geprüft.

3.2.4.4 Weitere Infrastrukturen rechtssicherer Kommunikation

Neben diese explizit vom Gesetzgeber als sichere Identitäten ausgestalteten Infrastrukturen (De-Ident und eID-Funktion) treten jedoch eine Vielzahl von anderen Angeboten, die ebenfalls eine rechtssichere Identifikation ermöglichen können. Dies gilt zunächst für das Postident-Verfahren, welches aber für die Identifizierung im Rahmen von Safe- und Cloud-Freigaben weniger geeignet erscheint. Insofern käme ein Rückgriff auf den Dienst **E-Postident** in Betracht, der auf dem herkömmlichen Dienst aufbaut und wie dieser nicht gesetzlich geregelt ist. Dennoch kann er von den Nutzern im Rahmen von Cloud-basierten Kommunikationsprozessen als hinreichend sicher eingestuft werden und zum Einsatz kommen.

Daneben ist es denkbar, dass auch **sichere Formen der Nachrichtenübermittlung** eingesetzt werden, um Freigaben tatsächlich nur den Berechtigten zukommen zu lassen. Werden Freigabe-Links bspw. auf solche E-Mail-Adressen gesendet, bei denen eine sichere Erstregistrierung (durch Postident oder den elektronischen Identitätsnachweis) stattgefunden hat, dürfte dies den Anforderungen an eine Identifizierbarkeit des Zugreifenden in den meisten Fallkonstellationen genügen. Hintergrund ist ein typisiertes »Vertrauen« in den dritten Akteur,[137] der durch die Übermittlung der Nachricht nicht nur als E-Mail- bzw. Nachrichtenprovider, sondern quasi zusätzlich als Identitätsprovider auftritt.[138] Dieses Vertrauen kann durch Zertifizierungs- oder Akkreditierungsverfahren sichergestellt werden. Ob und inwieweit dieses Vorgehen einer weitergehenden gesetzlichen Abbildung bedarf, kann nicht abschließend bewertet werden. Will man damit aber auch gesetzliche Identifizierungserfordernisse ersetzen, ist eine solche wohl unumgänglich. Letztlich stellt sich dieses Vorgehen zum Teil auch als »Identitätsbestätigungsdienst« nach § 6 DeMailG dar, der ursprünglich allerdings als die bloße Übermittlung von Identitätsattributen gedacht war. Zumal aber in der Regel auch Mitteilungen übermittelt werden sollen, kann die »Zusammenfassung« von Postfach- und Versanddienst (§ 5 DeMailG) und Identitätsbestätigungsdienst (§ 6 DeMailG) zu keiner anderen rechtlichen Bewertung führen.

---

[137] Zur Rolle des Rechts zur Erhöhung von »Vertrauen« Barthel/Braczyk/Fuchs, in: Kubicek (Hrsg.), Multimedia@Verwaltung, 1999, S. 119; wobei teilweise vertreten wird, dass das Recht alleine nicht in der Lage ist, ausreichend Vertrauen in der virtuellen Welt zu schaffen, vgl. Boehme-Neßler, MMR 2009, 439 ff.; speziell zum Technikmisstrauen Heckmann, DuD 2009, 656 ff.; zur Vertrauenserhöhung durch »Drittbekräftigungen« Hoffmann/v. Kaenel, in: Schliesky (Fn. 44), S. 79 ff.

[138] Zum Begriff des Identitätsproviders Schulz, in: Schliesky (Fn. 44), S. 51 (67 ff.).

4 Praxisbeispiele

Erfahrungen mit aktuellen Projekten, die ebenfalls einen Bezug zu personenbezogenen Daten aufweisen, verteilte Datenbestände nutzen und Freigabefunktionen für andere Akteure – noch dazu aufbauend auf dem Konzept der Virtualisierung – abbilden sollen, können weitergehende Anhaltspunkte für Konzepte zur Sicherung der individuellen Datenhoheit im Cloud-Umfeld geben. Im Sinne von »lessons learned« werden daher die eingangs bereits genannten Projekte »De-Mail«, »OMS«, »eGK« und »P23R« betrachtet.

4.1 Das elektronische Entgeltnachweis-Verfahren (ELENA)

4.1.1 Zielsetzung und Funktionsweise

Die Übermittlung von Informationen zum Einkommen als Voraussetzung für die Leistungsberechnung an die zuständigen Behörden geschieht zurzeit in Papierform. Mit dem elektronischen Entgeltnachweis-Verfahren (ELENA-Verfahren) wurden die technischen und organisatorischen Grundlagen geschaffen, um die beim Arbeitgeber vorliegenden Entgeltdaten der Arbeitnehmer elektronisch zu der jeweils berechtigten Behörde zu übermitteln und eine elektronische Verarbeitung zu vereinfachen. Neben einer Verbesserung der Datenauthentizität bei den abrufenden Stellen und einem verbesserten Schutz vor Datenmissbrauch wurde die Einführung des Verfahrens insbesondere auch durch Einsparungspotenziale motiviert. Man hoffte, dass bereits im ersten Nutzungsjahr 2012 eine Einsparung von 85,6 Millionen Euro erreicht werden könne. Langfristig wurde eine Einsparung von 500 Millionen Euro pro Jahr geschätzt.[139]

Das Verfahren beruhte auf der Speicherung von Arbeitnehmerdaten in einer zentralen Stelle, von der aus diese Daten für die Agenturen für Arbeit und weitere Stellen verfügbar gemacht werden sollten. Die Autorisierung von Abfragen der jeweiligen Leistungsträger durch den Antragsteller sollte mit Hilfe beliebiger Signaturkarten (EC-/Maestro-Card, elektronische Gesundheitskarte, neuer Personalausweis etc.) erfolgen.

ELENA sollte zunächst auf die folgenden Vorgänge angewendet werden:[140]

- Arbeitsbescheinigungen nach § 312 SGB III
- Nebeneinkommensbescheinigungen nach § 313 SGB III
- Auskunft über die Beschäftigung nach § 315 Abs. 3 SGB III

---

[139] Vgl. Warga, DuD 2010, 216 ff.

[140] Ebd.

- Auskunft über den Arbeitsverdienst zum Wohngeldantrag nach § 23 Abs. 2 WoGG
- Einkommensnachweis nach § 2 Abs. 7 Satz 4 und § 9 BEEG.

Das Verfahren involvierte die folgenden Rollen:[141]

- Der **Teilnehmer** (d. h. eine leistungsberechtigte Person) erteilt einer **abrufenden Stelle** (z. B. einer Agentur für Arbeit) die Berechtigung, im Zuge eines Antrags auf relevante Entgeltbescheinigungen zuzugreifen.
- Der **Arbeitgeber** erstellt Datensätze entsprechend der oben genannten Vorgänge. Diese Datensätze werden verschlüsselt an die **zentrale Speicherstelle** (ZSS) übermittelt.
- Die abrufende Stelle ruft im Zuge eines Antrags des Teilnehmers die dafür relevanten Entgeltbescheinigungen von der ZSS ab.
- Die zentrale Speicherstelle speichert die Datensätze, die ihr vom Arbeitgeber übermittelt werden. Eine Entschlüsselung der Daten findet dabei nicht statt. Als Ordnungskriterium wird die (bzw. eine) Zertifikatsidentifikationsnummer des Teilnehmers verwendet, die sich auf das auf der Signaturkarte gespeicherte Zertifikat bezieht.
- Die **Registratur Fachverfahren** (RFV) stellt die Verbindung zwischen der Rentenversicherungsnummer des Teilnehmers und der Zertifikatsidentifikationsnummer des Teilnehmers her. Diese Indirektion (anstelle der Speicherung von Arbeitnehmerdaten unter der Rentenversicherungsnummer als Hauptschlüssel in der ZSS) ist notwendig, um die Erstellung von Persönlichkeitsprofilen zu vermeiden.[142]
- Ein Zertifizierungsdienstanbieter (**Trustcenter**) erstellt Schlüssel und Zertifikate für die Teilnehmer bzw. ebenso für die **Mitarbeiter** der abrufenden Stelle und erstellt die erforderlichen Signaturkarten. Als Trustcenter waren dabei die durch die Bundesnetzagentur gemäß § 15 Abs. 1 SiG akkreditierten Institutionen vorgesehen.
- Eine Anmeldung des Teilnehmers zum ELENA-Verfahren kann entweder direkt bei der RFV oder einer autorisierten **Anmeldestelle** (z. B. einer Arbeitsagentur) erfolgen.

---

[141] Vgl. Arbeitskreis Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, DuD 2005, 29 ff.

[142] Die Erschließung eines Datenverbundes durch ein einheitliches Ordnungsmerkmal (bspw. die die Rentenversicherungsnummer) ist verfassungsrechtlichen Bedenken ausgesetzt; vgl. Roßnagel/Hornung/Schnabel, DuD 2008, 168 (171); ausführlich Hornung, Die Digitale Identität, 2005, S. 159 ff.

Der grundlegende Ablauf des Verfahrens war wie folgt definiert (Abbildung 11):

1. Der Teilnehmer beantragt bei einem Trustcenter eine geeignete Signaturkarte.[143]
2. Der Teilnehmer meldet sich für die Teilnahme am ELENA-Verfahren entweder direkt bei der RFV oder bei einer Anmeldestelle an. Dabei erfolgt die Verknüpfung des Zertifikats (d. h. seiner Identifikationsnummer) der angemeldeten Signaturkarte mit der Rentenversicherungsnummer des Teilnehmers.
3. Der Arbeitgeber übermittelt monatlich Daten über seine Arbeitnehmer an die zentrale Speicherstelle (ZSS). Dabei sind die zu übermittelnden Daten in sogenannten multifunktionalen Verdienstdatensätzen (MFDS) zusammengefasst[144] und werden verschlüsselt gesendet. Zur Speicherung beim ZSS werden die Datensätze jedoch zunächst entschlüsselt und mit einem datensatzspezifischen Schlüssel zur Speicherung wieder verschlüsselt.
4. Ein Teilnehmer, der arbeitslos wird bzw. Wohn- oder Elterngeld beantragen will, kann bei der Agentur für Arbeit, der Wohn- oder der Elterngeldstelle seine Signaturkarte nutzen, damit die entsprechende Stelle als abrufende Stelle die Arbeitnehmerdaten bei der ZSS anfordern kann, die für die Beantragung der Sozialleistung benötigt werden. Die Chipkarte des Teilnehmers und die Chipkarte des Mitarbeiters der abrufenden Stelle dienen dabei der Legitimation der Beteiligten.
5. Bei der ZSS werden alle Informationen überprüft und die angeforderten Arbeitnehmerdaten werden an die abrufende Stelle übermittelt. Dort werden dann die entsprechenden Sozialleistungen anhand der übermittelten Daten berechnet.

---

143 D. h. eine Karte mit qualifizierter elektronischer Signatur, die den Spezifikationen des vom Bundesamt für Sicherheit in der Informationstechnik definierten eCard-API-Frameworks entspricht; vgl. TR-03112.

144 Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V., »ELENA – Elektronischer Entgeltnachweis; Verfahrensbeschreibung Anlage 6: MVDS Fachlicher Inhalt (Version 1.5)«, abrufbar unter www.das-elena-verfahren.de/archiv/elena-fuer-arbeitgeber/verfahrensbeschreibung/verfahrensbeschreibung-anlage-6-3/at_download/file/. Das ELENA-Verfahren wurde unter anderem wegen der Möglichkeit, in den MFDS beliebige Informationen übermitteln zu können, kritisiert. Dies betrifft in der letzten Version 1.5 des Dokuments die Datumsangaben ohne festes Format (z. B.»1. Montag im Monat«, »einmal in der Woche«) zur Bestimmung des Zeitpunkts von Ausgabe/Abgabe bei Heimarbeit. Ein in früheren Versionen vorgesehenes Freitextfeld zur »Schilderung vertragswidrigen Verhaltens/Entlassungsanlass« ist in der Version 1.5 nicht mehr vorhanden. Auch Informationen zu Streiks und Aussperrungen werden nun zusammen mit »unentschuldigtem Fehlen«, »Wochenende oder Feiertage ohne Entgelt« und »Pflege eines kranken Kindes ohne Kranken- oder Verletztengeldbezug« summarisch als »sonstige unbezahlte Fehlzeit« übermittelt. Zusammenfassend lässt sich also feststellen, dass das Problem der Übermittlung von Freitexten durch die Definition eines flexibleren Datumformats hätte gelöst werden können.

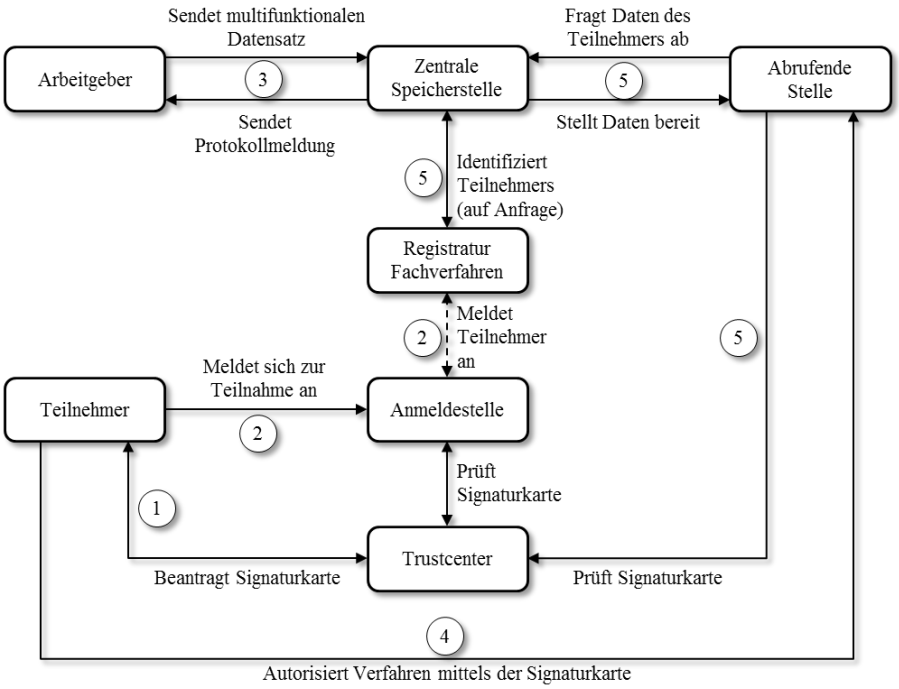

ABBILDUNG 11: ELENA-VERFAHRENSABLAUF (EIGENE DARSTELLUNG)

Die ELENA-Verfahrensbeschreibung[145] definiert eine Reihe von technischen und organisatorischen Maßnahmen zur Datensicherheit. Von besonderem Interesse für die Zwecke dieser Studie ist hier die Frage nach der geeigneten Verschlüsselung der Teilnehmerdaten. Die Übermittlung der Arbeitnehmerdaten durch den Arbeitgeber an die ZSS erfolgt unter Verwendung des DEÜV-Verfahrens[146], d. h. der Datentransport erfolgt verschlüsselt. Nach dem »Entfernen« der Transport-Verschlüsselung in der ZSS sowie der Durchführung von logischen und fachlichen Prüfungen werden die Daten mit einem hybriden Verschlüsselungsverfahren unter Verwendung eines dynamischen Sitzungsschlüssels verschlüsselt, der wiederum mit einem festen Datenbank-Hauptschlüssel verschlüsselt wird und im zentralen Datenbanksystem gespeichert wird. Dieser Hauptschlüssel wird dabei vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verwaltet. Zur Übermittlung der Daten von der ZSS an die abrufende Stelle werden die Arbeitnehmerdaten wiederum entschlüsselt und für den Transport neu verschlüsselt.[147]

Daneben wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) durch den Bundesverband Mediation in Wirtschaft und Arbeitswelt (BMWA) und den Bundesbeauftragten für Datenschutz (BfD) beauftragt, die technischen und organisatorischen Voraussetzungen für eine Ende-zu-Ende-Verschlüsselung der Teilnehmerdaten zu prüfen. Dieses Modell beruht auf einem asymmetrischen Verschlüsselungsverfahren. Dabei wird der öffentliche Schlüssel zur Verschlüsselung der Daten bereits durch den Arbeitgeber verwendet.

---

145 Zentrale Speicherstelle/Registratur Fachverfahren, ELENA Verfahrensbeschreibung, Version 1.0, abrufbar unter www.das-elena-verfahren.de/archiv/elena-fuer-arbeitgeber/verfahrensbeschreibung/elena-verfahrensbeschreibung/at_download/file/.

146 Die Datenerfassungs- und Datenübermittlungsverordnung (DEÜV) regelt, nach welchen Maßgaben die sozialversicherungsrelevanten Daten der Beschäftigten in Unternehmen erfasst und an die Sozialversicherungsträger übermittelt werden.

147 Vgl. Zentrale Speicherstelle/Registratur Fachverfahren (Fn. 145), S. 23 f.

Eine Entschlüsselung in der ZSS findet nicht statt. Erst, wenn ein spezifischer Datensatz bei der abrufenden Stelle aufgrund eines Antrags eines Teilnehmers eintrifft, wird er mit Hilfe des privaten Schlüssels, der auf der Signaturkarte des Teilnehmers gespeichert ist, entschlüsselt.[148]

Das Gutachten kommt zu dem Schluss, »*dass das JobCard-Verfahren mit einer Ende-zu-Ende-Verschlüsselung technisch möglich erscheint. Doch würde es hohe Anforderungen an die Technik bereits bei typischen Geschäftsabläufen stellen. Schwierigkeiten würden sich bei der Behandlung von Problemfällen ergeben, etwa wenn Dritte, deren Daten für die Berechnung der Sozialleistungen relevant sind, nicht kooperieren, wenn Daten etwa durch Konkurs oder durch unsachgemäße Handhabung des Arbeitgebers, verloren gingen, wenn eine unsachgemäße Umschlüsselung erfolgt oder wenn der Betroffene seine Chipkarte mit dem privaten Schlüssel verliert.*«[149]

4.1.2 Geschichte

Das elektronische Entgeltnachweis-Verfahren nahm seinen Anfang im Jahr 2002 mit einem Vorschlag der sog. Kommission »Moderne Dienstleistungen am Arbeitsmarkt«, dessen Umsetzung die Einführung einer elektronischen Signaturkarte beinhaltete, die einen elektronischen Zugriff der Bundesagenturen für Arbeit auf Daten zum Zweck der Ermittlung von Ansprüchen auf Sozialleistungen erlauben sollte.[150] Diese sog. JobCard sollte als Authentisierung- und Autorisierungsmittel für solche Zugriffe durch den Arbeitnehmer dienen. Arbeitnehmerdaten sollten durch eine zentrale Speicherstelle erfasst werden. Eine Archivierung dieser Daten durch die Arbeitgeber sollte entfallen. Medienbrüche bei der Weitergabe und Verarbeitung der Daten sollten vermieden werden.

Die Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung (ITSG) legte ein erstes Konzept zu ELENA am 31. Juli 2003 vor.[151] Eine Erprobung erfolgte in einem mehrstufigen Pilotprojekt in den Jahren 2002 bis 2005, das durch die Spitzenverbände der gesetzlichen Krankenkassen und deren IT-Dienstleister, der ITSG im Auftrag des Bundesministerium für Wirtschaft und Arbeit durchgeführt wurde. Beteiligt waren unter anderem die Deutsche Angestellten-Krankenkasse (Hamburg), die Deutsche Lufthansa AG (Hamburg), die ITSG, das Personal- und Organisationsamt der Stadt Frankfurt am Main und die Volkswagen AG (Wolfsburg) als meldende Stellen und verschiedene Arbeitsagenturen (Darmstadt, Potsdam, Bamberg, Essen), verschiedene Städte, Bezirke und Landkreise (Münster, Emsland, Miltenberg, Würzburg, Dortmund, Frankfurt am Main, Rodgau, Würzburg) sowie der Verband der Rentenversicherungsträger als abrufende Stellen.[152]

---

148 Arbeitskreis Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, DuD 2005, 29 ff.

149 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, ULD-Stellungnahme zum Entwurf eines Gesetzes über die Einführung des Verfahrens des elektronischen Einkommensnachweises (ELENA-GE), 20.02.2007, abrufbar unter www.datenschutzzentrum.de/elena/070302-stellungnahme.htm/.

150 Bundesministerium für Arbeit und Soziales, Sachstandsbericht des Staatssekretärsausschusses zur Umsetzung der Vorschläge der Kommission »Moderne Dienstleistungen am Arbeitsmarkt«, 03.09.2002, abrufbar unter www.ak-sozialpolitik.de/doku/02_politik/hartz_kommission/umsetzung/2002_09_04_sachstand.pdf/.

151 Vgl. Warga, DuD 2010, 216 ff.

152 Bundesministerium für Wirtschaft und Technologie, Das ELENA-Verfahren, 2008, abrufbar unter: www.einblick-archiv.dgb.de/hintergrund/2008/13/bmwi_info.pdf/.

Im Jahre 2003 wurden erstmals datenschutzrechtliche Bedenken gegenüber der JobCard bzw. dem ELENA-Verfahren laut. In seinem 19. Rechenschaftsbericht schrieb der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit:

> »*Es entsteht eine Datenspeicherung auf Vorrat, deren Vereinbarkeit mit den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten verfassungsrechtlichen Grundsätzen noch geprüft werden muss. So sind nach § 312 SGB III die Arbeitgeber verpflichtet, bei Beendigung des Arbeitsverhältnisses alle Tatsachen zu bescheinigen, die für die Entscheidung über den Anspruch auf Arbeitslosengeld, Arbeitslosenhilfe, Unterhaltsgeld oder Übergangsgeld erheblich sein können (Arbeitsbescheinigung). Diese Arbeitsbescheinigung wird daher bei jeder Beendigung eines Arbeitsverhältnisses ausgestellt. Aber nur ein geringer Teil der ehemaligen Arbeitnehmer muss bei einem entsprechenden Antrag die Arbeitsbescheinigung beim Arbeitsamt tatsächlich vorlegen. Ein großer Teil der in den Datenpool einfließenden Daten wird daher nie benötigt werden.*
>
> *Der Bericht der Hartz-Kommission sieht in diesem Zusammenhang die Einführung einer einheitlichen Versicherungsnummer aller Sozialversicherungsträger als sinnvoll an. Im Zusammenhang mit der Schaffung der digitalen Signaturkarte für Arbeitgeberbescheinigungen ist eine solche Nummer als Ordnungsnummer erforderlich, um Daten einem bestimmten Arbeitnehmer eindeutig zuweisen zu können. Dabei ist zu beachten, dass die Restriktionen bei der Nutzung der Sozialversicherungsnummer (§§ 18f und g SGB IV) [...] vom Gesetzgeber aus gutem Grund geschaffen wurden. Insbesondere für die Sozialversicherungsnummer hat der Gesetzgeber ausdrücklich angeordnet, dass diese nicht als Ordnungsmerkmal dienen soll (§ 18f Abs. 5 SGB IV).*«[153]

Ähnlich äußerten sich die Datenschutzbeauftragten des Bundes und der Länder im November 2008 anlässlich der Verabschiedung des Gesetzentwurfs über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) am 25. Juni 2008 durch den Bundestag:[154]

> *»Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.«*[155]

Auch die Absicherung der Verfügungsbefugnis über die zentral gespeicherten Einkommensdaten durch die betroffenen Personen wurde schnell in Frage gestellt. Eine Ende-zu-Ende-Verschlüsselung dieser Daten, die sichergestellt hätte, dass die technischen Mittel zur Entschlüsselung dieser Daten ausschließlich dem Teilnehmer an dem Verfahren zur Verfügung

---

153 Tatigkeitsbericht 2001 und 2002 des Bundesbeauftragten fur den Datenschutz (19. Tätigkeitsbericht), 2003, abrufbar unter www.bfdi.bund.de/cae/servlet/contentblob/409322/publicationFile/25222/19TB_2001_02.pdf/.

154 BT-Drs. 16/10492.

155 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn: Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren, abrufbar unter www.bfdi.bund.de/cae/servlet/contentblob/416448/publicationFile/25156/76DSK_Elena.pdf/.

gestanden hätten, wurde mit einem Verweis auf das Gutachten des BSI von 2005 (4.1.1) auch durch die Bundes- und Landesdatenschutzbeauftragten ad acta gelegt.[156]

Die Datenschutzbeauftragten gingen über die grundsätzliche Fragestellung nach der Verhältnismäßigkeit und Erforderlichkeit der Datenspeicherung im Rahmen des ELENA-Verfahrens hinaus. In der Entschließung der 76. Konferenz der Datenschutzbeauftragten[157] wird eine Reihe von konkreten technischen und organisatorischen Verbesserungsmaßnahmen vorgeschlagen:

1. Die Einrichtung eines Verwaltungsausschusses der ZSS zur Wahrung des Datenschutzes und der technischen Sicherheit. Ein für die ZSS eingesetzter Datenschutzbeauftragter, der dem Verwaltungsausschuss regelmäßig Bericht zu erstat-erstatten hat.
2. Die Schlüssel zur Ver- und Entschlüsselung der bei der ZSS gespeicherten Daten dürfen nicht in der Verfügungsgewalt der ZSS liegen. Stattdessen soll eine unabhängige Treuhänderstelle für die kryptografischen Komponenten verantwortlich sein.
3. Verfahren sind zu etablieren, die die technische Verfügungsmöglichkeit über individuelle Daten durch die Betroffenen ermöglichen.
4. Abrufende Stellen haben starke Authentisierungsverfahren einzusetzen, die dem Stand der Technik entsprechen.
5. Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.[158]

Das ELENA-Verfahrensgesetz wurde am 28. März 2009 vom Bundestag verabschiedet.[159] Dieses Gesetz bezog sich zunächst auf die eingangs beschriebenen Vorgänge, allerdings heißt es in der Begründung des Gesetzentwurfs:

> *»Der Einstieg in das ELENA-Verfahren soll im ersten Schritt durch die gesetzliche Umsetzung der Bescheinigungen zur Leistungsberechnung für das Arbeitslosen-, das Wohn-, und Elterngeld erfolgen und Schritt für Schritt auf weitere Bescheinigungen ausgebaut werden. Dazu prüft das Bundesministerium für Wirtschaft und Technologie, ab dem 1.1.2015 alle weiteren Auskünfte, Bescheinigungen und Nachweise nach dem Sozialgesetzbuch und seiner besonderen Teile nach § 68 SGB I in das Verfahren mit einzubeziehen«.*

Mitte 2010 stand das ELENA-Projekt zunehmend im Fokus der öffentlichen Kritik. Neben Zweifeln an dem Einsparungspotenzial des Verfahrens (das in einem Gutachten des Normenkontrollrats aus dem Jahre 2007[160] noch einmal bekräftigt wurde), stand auch die

---

156 Beschluss der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSB-Konferenz) vom 27./28.10.2005 in Lübeck zu einer Vorlage der Arbeitsgemeinschaft (AG) JobCard der DSB-Konferenz (heute ELENA-Vefahren), abrufbar unter www.datenschutzzentrum.de/elena/dsbk70-jobcard.pdf/.

157 Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn (Fn. 155).

158 Vgl. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren, abrufbar unter www.sachsen-anhalt.de/index.php?id=20565/.

159 BGBl I 2009 S. 635.

160 Nationaler Normenkontrollrat, Gutachterliche Stellungnahme zum heutigen papiergebundenen Verfahren und den künftigen Kosten des ELENA-Verfahrens, 10.12.2007, abrufbar unter

Verfassungskonformität des ELENA-Verfahrens in Frage.[161] Die aktuelle Kritik am ELENA-Verfahren und dem ELENA-Verfahrensgesetz orientierte sich an einem Urteil des Bundesverfassungsgericht zur Vorratsdatenspeicherung vom 2. März 2010.[162] Hier wird festgestellt, dass die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten einen »*besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt*« darstellt. Am 31. März 2010 wurde eine Verfassungsbeschwerde gegen ELENA eingereicht.[163]

Am 11. November 2011 beschloss der Bundesrat die Einstellung des ELENA-Verfahrens.[164] In der Begründung heißt es:

> »*[…] das* ***Bundesverfassungsgericht*** *hat 2010 in seinem Urteil zur Vorratsdatenspeicherung klargemacht, dass die Daten dezentral gespeichert und vor unberechtigtem Zugriff geschützt werden müssen. Im Prinzip lief* ***ELENA*** *auf nichts anderes hinaus als auf eine* ***neue Variante der Vorratsdatenspeicherung. Datenschutz*** *ist ein* ***zentrales Bürgerrecht.*** *Hier kann es keine Abstriche geben. Die Datenbank erfasste nicht nur, wieviel die Arbeitnehmer verdienten oder wie lange sie arbeiteten, sondern enthielt auch Angaben zu Krankheitstagen oder dem Verhalten am Arbeitsplatz. Bei vielen dieser Daten war unklar, wann und ob sie überhaupt benötigt werden.*
>
> *Das gravierendste Problem war, dass die Sicherheit des Verfahrens nicht gewährleistet war, weil sich die elektronische Signatur bisher in Deutschland nicht flächendeckend durchsetzen konnte. Der fortbestehenden* ***Sicherheitsbedenken*** *wegen hatten das FDP geführte Bundeswirtschaftsministerium, aber auch das unionsgeführte Arbeitsministerium bereits im Juli 2011 angekündigt, das ELENA-Verfahren einzustellen.«*[165] (Hervorhebungen im Original)

Auf eine kleine Anfrage mehrerer Abgeordneter vom 3. September 2011 bezüglich der Kosten der Einstellung des ELENA-Verfahrens konnte die Bundesregierung nicht antworten. Die Verfasser der Anfrage rechnen vor:

> »*Tatsächlich seien durch das Projekt seit 2008 nach Angaben des BdSt allein dem Staat Kosten von mindestens 33 Mio. Euro entstanden. Dazu kämen noch die Kosten der Startfinanzierung in Höhe von 55 Mio. Euro (vgl. hierzu WELT Online vom 19. Juli*

---

www.normenkontrollrat.bund.de/Webs/NKR/Content/DE/Publikationen/2007-12-07-gutachten-des-nkr-zum-elena-verfahren.pdf;jsessionid=7783F02636CB306C30E13ABE2002935D.s3t1?__blob=publicationFile/.

161 Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, 29.12.2009: »Die Einrichtung einer solchen Datei wirft schwerwiegende datenschutzrechtliche Fragen auf: Ist sie überhaupt angemessen? Können die Missbrauchsrisiken beherrscht werden? Wie kann verhindert werden, dass die umfangreichen Datenbestände, wenn sie erst einmal gespeichert sind, für andere Zwecke verwendet werden?« abrufbar unter www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2009/PM_35_DatenschutzBei-Elenaverfahren.html/. Vgl. auch »Zentrale Speicherstelle Elena: verdi erwägt Klagen gegen die Datensammelwut der Regierung«, abrufbar unter fidi.nrw.verdi.de/stichwort/datenschutz/, sowie »Ex-Innenminister Baum fordert das Ende von Elena«, Spiegel Online, 10.04.2010, abrufbar unter www.spiegel.de/spiegel/vorab/0,1518,688270,00.html/.

162 BVerfGE 125, 260 ff.

163 Verfassungsbeschwerde ELENA, 1 BvR 902/10, www.starostik.de/media/Verfassungsbeschwerde-ELENA-Verfahrensgesetz.pdf/.

164 BR-Drs. 608/11.

165 Plenarprotokoll der 889. Sitzung des Deutschen Bundesrates, 04.11.2011, S. 515.

2011). […] Nach Angaben der Bundesvereinigung der Deutschen Arbeitgeberverbände hätten die Unternehmen mehrere 100 Mio. Euro für ELENA ausgegeben.«[166]

4.1.3 Kritik und Gründe des Scheiterns

Die Kritik am ELENA-Verfahren beinhaltet die folgenden Elemente:

- Der Umfang der durch die meldenden Stellen übermittelten Daten geht weit über die Erfordernisse der Bearbeitung konkreter Anträge hinaus. Darüber hinaus existieren in den Datenübermittlungsformaten Freitextfelder, die die Übermittlung weitergehender Informationen (z. B. Gründe für Fehlzeiten, Teilnahme an Streiks) erlauben.
- Es bestehen Mängel in der Übertragungsverschlüsselung. So gibt es z. B. keine Ende-zu-Ende-Verschlüsselung, sondern stattdessen Verfahren mit der Zwischenstelle RFV. Die Teilnehmer selbst erhalten keine Schlüssel.
- Die Ersparnis für Unternehmen bezieht sich vor allem auf große und mittelständische Unternehmen, da diese meist über ein Personalwesen verfügen. Für Klein- und Kleinstunternehmen wird eine Kostenzunahme durch den zusätzlichen Mehraufwand erwartet.

4.1.4 Schlussfolgerungen für IT-Projekte mit Datenbezug

Im Sinne der Datensparsamkeit ist darauf zu achten, dass der Umfang der personenbezogenen Daten so gering wie möglich gehalten wird. Es dürfen nur die für einen konkreten Zweck erforderlichen Daten erhoben und verarbeitet werden.

Es ist darauf zu achten, dass die im Rahmen eines Verfahrens erhobenen Daten einer strikten Zweckbindung unterliegen. Daten dürfen nur anlassbezogen erhoben und verarbeitet werden.

Technische und organisatorische Maßnahmen sind zu treffen, die sowohl eine eindeutige Identifizierung aller am Verfahren Beteiligten ermöglichen als auch eine Protokollierung der Aktivitäten bereitstellt. Verschlüsselung ist eine Mindestvoraussetzung um die Sicherheit der Daten zu gewährleisten.

[166] BT-Drs. 17/6747.

4.2 Die elektronische Gesundheitskarte (eGK)

Durch die eGK wird die 1995 eingeführte Krankenversichertenkarte[167], die ihrerseits den Krankenschein ersetzte, abgelöst und zu einem Datenspeicher und Zugangsschlüssel für medizinische Daten erweitert.[168] Um eine Vernetzung zu erreichen, ist gleichzeitig die Ausstattung der beteiligten Akteure mit entsprechender Soft- und Hardware und damit die Errichtung einer neuen »interoperablen und kompatiblen Informations-, Kommunikations- und Sicherheitsinfrastruktur«[169] notwendig. Daher wird es neben der eGK für den sicheren Zugriff auf die eGK-Daten den Heilberufsausweis (HBA) geben. Einerseits verfolgt die eGK das Ziel, das Gesundheitswesen zu modernisieren und ein vernetztes Datenmanagement zu ermöglichen; andererseits ist sie eingebettet in die Entwicklung einer Infrastruktur, die gesicherte und vertrauliche Kommunikationsmöglichkeiten schafft.[170] Die eGK bildet den zentralen »Knoten« im Netz der IT-Systeme zur Verarbeitung von Gesundheitsdaten.[171]

4.2.1 Zielsetzung und Funktionsweise

Das Ziel dieses Projektes ist in § 291a Abs. 1 SGB V aufgenommen. Danach soll die Einführung der eGK der Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz der Behandlung dienen. Ziel ist also die Verbesserung der Behandlungsabläufe über eine **schnellere und sicherere administrative sowie medizinische Kommunikation** zwischen allen Beteiligten.[172] Durch das Zusammenspiel von besserer Kommunikation und gesteigerter Transparenz soll erreicht werden, dass die Qualität der medizinischen Versorgung verbessert wird. Ein weiterer Vorteil erhöhter Transparenz ist die Verhinderung von unerwünschten Wechselwirkungen von Arzneimitteln.[173] Gleichzeitig eröffnet sie aber ein großes Rationalisierungspotenzial. Zwischen 20 und 40 % der Leistungen im Gesundheitswesen entfallen auf Datenerfassung und Kommunikation.[174] Folglich liegt ein weiterer Effekt bei der Einführung der eGK in einer Kostenersparnis.[175]

Die eGK bietet als Smartcard zahlreiche Anwendungen. Der Pflichtteil der Karte soll gem. § 291 Abs. 2 i. V. m. Abs. 2a, § 291a Abs. 1, Abs. 2 Nr. 1 und 2 SGB V die Versichertenstammdaten enthalten. Dies umfasst den Namen, das Geburtsdatum, das Geschlecht, die Adresse sowie Angaben zur Krankenversicherung. Darüber hinaus zählt zu den Pflichtanwendungen gem. § 291a Abs. 2 Nr. 1 SGB V auch das elektronische Rezept. Eine weitere Neuerung ist, dass die eGK mit einem Lichtbild des Versicherten auszustatten ist. Der freiwillige Teil gem. § 291 Abs. 2a Sätze 1, 2 SGB V i. V. m. § 291 a Abs. 2, 3 SGB V muss geeignet sein, folgende Anwendungen der Datenerhebung, -verarbeitung und -nutzung zu unterstützen: Medizini-

---

167 § 291 Abs. 1 SGB V, geändert durch Gesetz v. 21. 12. 1992 (BGBl I, S. 2266).

168 Speth/Koutses, MedR 2005, 493 ff.

169 Lücke/Köhler, Dtsch Med Wochenschrift 2007, 448 (449); Meister, in: Deutsche Krankenhausgesellschaft (Hrsg.), Das Krankenhaus, 2005, S. 741 ff.; Pitschas, NZS 2009, 177 (179).

170 Wirtz/Ullrich/Mory (Fn. 13), S. 16; Dietzel (Fn. 13), S. 2 (2 f.).

171 Pitschas, NZS 2009, 177 (179).

172 Pitschas, NZS 2009, 177 (179).

173 So sterben nach konservativen Schätzungen jährlich über 10. 000 Menschen durch unerwünschte Arzneimittelereignisse. Siehe hierzu: Bales, Bundesgesundheitsbl 2005, 727 (728).

174 Paland/Riepe, Bundesgesundheitsbl 2005, 623.

175 Braun, in: Eberspächer/Picot/Braun (Hrsg.), eHealth: Innovations- und Wachstumsmotor für Europa, 2006, S. 61 (72 f.); zum Rationalisierungspotenzial: Paland/Riepe, Bundesgesundheitsbl 2005, 623; Bales, Bundesgesundheitsbl 2005, 727 (727).

sche Notfalldaten, elektronischer Arztbrief, Arzneimitteldokumentation, elektronische Patientenakte, freiwillige Daten von oder durch den Versicherten, in Anspruch genommene Leistungen und deren vorläufige Kosten (§ 305 Abs. 2 SGB V). Der freiwillige Teil der eGK kann im Unterschied zu dem Pflichtteil der Karte gem. § 291a Abs. 3 Sätze 4, 5 SGB V nur mit **Einwilligung des Betroffenen** aktiviert werden, wobei diese nach § 291a Abs. 3 Satz 5 Hs. 2 SGB V jederzeit auf einzelne Anwendungen beschränkt oder aber auch vollständig widerrufen werden kann.

4.2.2 Geschichte

Aufgrund des Beschlusses der Bundesregierung vom 01. 12. 1999 wurde am 17. 10. 2003 die erste Fassung des Gesetzes zur Einführung der eGK verabschiedet, das am 01. 01. 2004 in Kraft getreten ist.[176] In der Folgezeit wurde nach langwierigen Verhandlungen von den Spitzenverbänden im Gesundheitswesen die gematik mbH gegründet,[177] die nicht nur für die Einführung der Gesundheitskarte, sondern auch darüber hinaus für den langfristigen Betrieb verantwortlich sein sollte. Laut Gesetz sollte die Ausgabe der eGK im Januar 2006 beginnen. Allerdings bestanden erhebliche technische Schwierigkeiten, sodass dieser Zeitpunkt auf unbestimmte Zeit verschoben wurde und stattdessen Labortests vorbereitet und durchgeführt wurden. Nach neuerlicher Verschiebung des Starttermins wird die eGK nunmehr seit dem 29. 09. 2011 durch die Krankenkassen an die Versicherten ausgegeben.

4.2.3 Kritische Faktoren[178]

Bei der Einführung der eGK erwies sich der fehlende Überblick über den Umfang des Projekts als Kernproblem. Die lange Zeit unvollständige Rahmenarchitektur war u. a. Ursache dafür, dass keine weiteren Lösungen und Komponenten entwickelt werden konnten.[179] Die Defizite im Bereich der Projektplanung zeigten sich am deutlichsten im Rahmen der zeitlichen Planung.[180] So war für eine Vielzahl von Beteiligten aufgrund der schleppenden Fertigstellung der Rahmenarchitektur klar, dass das Projekt nicht – wie vom Bundesministerium für Gesundheit zunächst geplant – bis zum 01. 06. 2006 fertiggestellt werden könne.[181] Des Weiteren wurde die notwendige Organisation und Koordination der zahlreichen Beteiligten unterschätzt.[182] Dies wirkte sich bei diesem Projekt aufgrund der zahlreichen Beteiligten, die ihrerseits in erster Linie die eigenen Interessen vertreten (haben),[183] in besonderer Weise aus. Zum anderen wurde auch die in § 291 SGB V verankerte Möglichkeit der Ersatzvornahme durch das Bundesministerium für Gesundheit bei Fristüberschreitung deutlich überschätzt.[184]

Im Kontext von **IT-Konzepten mit Daten- und Cloudbezug** von besonderer Relevanz sind die Erkenntnisse aus dem eGK-Projekt zur **Akzeptanz** eines Lösungsansatzes durch die Beteiligten – konkret: die Träger der Datenhoheit, noch dazu in einem besonders sensiblen Be-

---

176 BGBl I 2003, S. 2190 ff.

177 Speth/Koutses, MedR 2005, 493 (494).

178 Ausführlich Classen, in: Schliesky (Hrsg.), Staatliches Innovationsmanagement, 2010, S. 369 ff.

179 Riebling, Medical Tribune 2006, 55.

180 Hierzu ebenfalls Riebling, Medical Tribune 2006, 55.

181 So äußerten sich beteiligte IT-Fachleute ebenso kritisch wie Krankenkassen und Ärzte; vgl. Riebling, Medical Tribune 2006, 55; Krüger-Brandt, DÄ 2004, A 889.

182 Zum Koordinationsumfang vgl. Paland/Riepe, Bundesgesundheitsbl 2005, 623 (626).

183 Riebling, Medical Tribune 2006, 55.

184 Riebling, Medical Tribune 2006, 55.

reich. Die aufgetretenen technischen Umsetzungsschwierigkeiten dürften zu einem **eingeschränkten Vertrauen** der Betroffenen in das System geführt haben. So bereitete es den Ärzten erhebliche Schwierigkeiten, die eGK in den täglichen Arbeitsablauf einzugliedern. Bspw. kam es in den Praxistests beim Ausstellen elektronischer Rezepte vielfach zu Schwierigkeiten.[185] Als ebenfalls in der Praxis schwer handhabbar hat sich der Umgang mit der PIN herausgestellt.[186] Daneben bringt die praktische Umsetzung für die beteiligten Akteure (hier am Beispiel der niedergelassenen Ärzte)[187] tief greifende Veränderungen mit sich. So muss künftig jede Arztpraxis mit einem internetfähigen EDV-System ausgestattet, ein schneller Internetzugang (DSL oder ISDN) verfügbar und alle Arbeitsrechner durch ein Netzwerk miteinander verbunden sein.[188] Dafür müssen alle Arbeitsrechner mindestens mit Windows 2000 oder Linux ausgestattet sein. Ältere Betriebssysteme, die z. Zt. noch in ca. 45 % der Praxen vorhanden sind,[189] müssen ausgetauscht werden.[190]

4.2.4 Schlussfolgerungen für IT-Projekte (Konzepte) mit Datenbezug

Positiv ist die Tatsache zu bewerten, dass dem **Patientengeheimnis** als Ausprägung des Rechts auf informationelle Selbstbestimmung dadurch gerecht geworden ist, dass es der Patient in der Hand hat, mit seinem Schlüssel die über die eGK zugänglichen Daten des freiwilligen Teils freizuschalten.[191] Ebenso erscheint es zielführend, Datenbestände, auf die eine Vielzahl von Akteuren zugreifen muss und bei denen gerade dieser raum- und zeitunabhängige Zugriff erhebliche (hier nicht nur Kosten-)Vorteile hat, zentral auszugestalten, dem Betroffenen aber den »Schlüssel« zu belassen. Das auch dem Cloud Computing zugrundeliegende Konzept der Virtualisierung (von Speicherkapazitäten) wurde hier sinnvoll eingesetzt.

Allerdings zeigen sich auch hier Defizite in der konkreten Umsetzung. Einerseits erscheint es wenig nutzerfreundlich, die Eingabe einer sechsstelligen PIN zu fordern, ohne dass abschließend gesagt werden kann, wie ein **sachgerechter Ausgleich zwischen Usability und hinreichendem Schutzniveau** hätte aussehen können. Andererseits ist die Einführung einer eigenen »Karte« nicht zielführend, da mit dem elektronischen Personalausweis eine entsprechende Infrastruktur bereit steht, die offensichtlich auch für andere Anwendungen offen ist. Unnötigerweise kam es im Projekt »eGK« zu einer Verknüpfung des Aufbaus von Datenbeständen mit den Modalitäten des rechtssicheren und eindeutig identifizierbaren Zugriffs auf diese Datenbestände. Eine separate Behandlung dieser Fragestellungen bei Fokussierung auf den elektronischen Identitätsnachweis als zentrale Identitätsinfrastruktur wäre insofern zielführender gewesen. Der Rückgriff auf eine Karte in verschiedenen Zusammenhängen könnte auch den aufgetretenen Problemen mit der PIN entgegenwirken: muss man sich nur eine merken, kann diese ggf. auch sechsstellig sein.

---

185 Rabbata, DÄ 2009, A 490.

186 Krüger-Brandt, DÄ 2006, A 1453; ders., DÄ 2009, A 2454 (A 2455).

187 Zu den Anforderungen an die Krankenhäuser siehe Häber, in: Hegering (Hrsg.), Informatik 2008, Beherrschbare Systeme – dank Informatik, Bd. 1, 2008, S. 53 ff.

188 Lücke/Köhler, Dtsch Med Wochenschrift 2007, 448 (449).

189 Booz Allen Hamilton GmbH, Endbericht zur Kosten-Nutzen-Analyse der Einrichtung einer Telematik-Infrastruktur im deutschen Gesundheitswesen vom 31. 07. 2007, S. 55.

190 Lücke/Köhler, Dtsch Med Wochenschrift 2007, 448 (449).

191 Pitschas, NZS 2009, 177 (177); Menzel, DuD 2006, 148 (152); Weichert, DuD 2004, 391 (399 ff., 403).

4.3 Prozessdatenbeschleuniger (P23R)

4.3.1 Zielsetzung und Funktionsweise

Aufgrund nationaler Gesetze und Verordnungen müssen Unternehmen für verschiedenste Zwecke Daten an die Verwaltung übermitteln. So bestehen über 10.000 Informations- und Meldepflichten für Unternehmen, was zu jährlichen Bürokratiekosten von über 47 Milliarden Euro auf Seiten der Wirtschaft führt.[192] Aktuell werden diese Verpflichtungen selbst innerhalb einer Berichtsdomäne, wie z. B. der Umweltberichterstattung oder den Meldungen mit Arbeitgeberbezug, meist isoliert voneinander betrachtet und bearbeitet. Die Folgen sind Mehrfachaufwände und ein erhöhtes Fehlerrisiko. So werden Datenfelder in unterschiedlichen Fachverfahren mehrfach erfasst und verarbeitet, was neben einem erhöhten Aufwand auch mit einem Verlust der Datenqualität einhergeht.

Zudem müssen die Informationssysteme, die von Unternehmen zur Abwicklung eingesetzt werden, aufgrund gesetzlicher Änderungen fortlaufend aktualisiert und angepasst werden – zum Teil unter erheblichem Kosten- und Ressourcenaufwand. Dies hat zur Folge, dass für zahlreiche Berichtsdomänen keine geeigneten Informationssysteme zur Verfügung stehen und dadurch Informationspflichten manuell erfüllt werden müssen.

4.3.1.1 Prinzipien

Ausgehend von diesen Umständen adressiert das Projekt P23R[193] zwei zentrale Ansatzpunkte, die Bündelung von Prozessketten einerseits und die Anwendung von Benachrichtigungsregelwerken andererseits zur Verbesserung der Qualität, Effizienz und Effektivität von Prozessen zur Interaktion zwischen Wirtschaft und Verwaltung. Prozessketten zwischen Wirtschaft und Verwaltung dienen zur Erfüllung gesetzlich vorgeschriebener Informationspflichten. Beispiele hierfür sind in den Machbarkeitsstudien zum P23R-Projekt zu finden.[194]

Zunächst werden Prozessketten zwischen Wirtschaft und Verwaltung nach inhaltlichen und prozessualen Gesichtspunkten systematisch miteinander zu sogenannten **Prozessketten-bündeln** vernetzt. Durch eine einheitliche Datenaufbereitung für Informationspflichten können einerseits Synergieeffekte erzielt und andererseits die Datenqualität erhöht werden. Dabei werden Prozessketten gebündelt, die gleiche oder ähnliche Inhalte zum Gegenstand haben, mit der Zielsetzung für derartige Prozessketten eine gemeinsame Informationsbasis zu nutzen. Berichts- oder Meldedaten müssen auf diese Weise nicht mehr redundant ermittelt, gepflegt und archiviert werden. Berichts- und Meldepflichten an unterschiedliche Adressaten auf Verwaltungsseite können effizient und mit hoher Informationsqualität abgewickelt werden.

---

[192] Bundesregierung, Zahlen und Fakten zum Bürokratieabbau, 2012, abrufbar unter www.bundesregierung.de/Content/DE/StatischeSeiten/Breg/Buerokratieabbau/zahlen-und-fakten-zum-buerokratieabbau.html/.

[193] Das Material zum Prozessdatenbeschleuniger in diesem Abschnitt beruht weitgehend auf der Darstellung in Baum u. a., Pilotierung und Realisierung des Prinzips Prozess-Daten-Beschleuniger | P23R für den Datenaustausch zwischen Wirtschaft und Verwaltung, Whitepaper zum P23R-Prinzip, zur Veröffentlichung vorgesehen.

[194] In den Machbarkeitsstudien (Fn. 205 bis 207) werden Prozessketten zu den Themenfeldern Umwelt, Finanzdienstleistungen bzw. der Informations- und Meldepflichten für Arbeitgeber beschrieben.

Weiterhin werden gesetzliche Regelungen in Form von formal beschriebenen **Benachrichtigungsregelwerken** bereitgestellt, wodurch sowohl der Aufwand für den Transfer an sich als auch für die Sicherstellung der Rechtskonformität reduziert wird. Hierdurch erhalten Informationssysteme, die nach dem P23R-Prinzip (im Folgenden als P23R-Lösungen bezeichnet) arbeiten, Zugang zu Benachrichtigungsregelwerken verschiedener Gesetzesdomänen, die in Benachrichtigungsregelpaketen organisiert werden, sowie deren Aktualisierungen. Das P23R-Prinzip beschreibt hierzu sowohl methodische Elemente zur Analyse und Gestaltung von Prozessketten als auch eine technische Infrastruktur (Rahmenarchitektur) zur Implementierung entsprechender Lösungen. Zudem vereinfacht seine Anwendung die Kommunikation zwischen Unternehmen und öffentlichen Stellen, ohne in die Datenautonomie der Unternehmen einzugreifen oder zentrale Datenbestände aufzubauen. Auf Verwaltungsseite ergibt sich bei einer breiten Anwendung des P23R-Prinzips darüber hinaus der Vorteil, dass Berichts- und Meldedaten in höherer Qualität medienbruchfrei und nachvollziehbar entsprechend der aktuellen Gesetzgebung abgerufen werden können.

4.3.1.2 Anwendungsszenarien

Ein typischer Verfahrensablauf, der durch eine P23R-Lösung organisiert werden kann, ist die Erstellung eines Berichts (Abbildung 12). Auf Anfrage oder zu vorab festgelegten bzw. vorgegebenen Terminen kann die P23R-Lösung das Erstellen einer Meldung bzw. eines Berichts (z. B. die Jahresmeldung zur Sozialversicherung) auslösen. Dazu wird die P23R-Lösung durch eine interne Nachricht angesteuert, die die Generierung einer Benachrichtigung auslöst. Ein oder mehrere Benachrichtigungsregelwerke steuern dabei die Erzeugung von Benachrichtigungen aus den Daten des Unternehmens. Regelwerke für die verschiedenen Berichtsdomänen werden, in Form von Benachrichtigungsregelpaketen, durch eine Leitstelle bereitgestellt. Eine Benachrichtigung kann nun von einem zuständigen Mitarbeiter des Unternehmens freigegeben und bei Bedarf auch angepasst werden, um daraufhin an die Verwaltung gesendet zu werden, wo sie überprüft und eine Eingangsbestätigung erstellt wird. Die Eingangsbestätigung wird als externe Nachricht an die P23R-Lösung des Unternehmens zurückgespielt und kann daraufhin an den zuständigen Mitarbeiter bzw. die Unternehmenssoftware weitergeleitet werden. Hat die Verwaltung im Zuge der Verarbeitung der Meldung bzw. des Berichts Nachfragen, kann sie diese sowohl persönlich stellen oder auch – als externe Nachricht – an die P23R-Lösung des Unternehmens schicken, um bspw. eine korrigierte Version anzufordern. Ein Mitarbeiter korrigiert im Normalfall die beanstandeten Daten und initiiert anschließend manuell die Abgabe einer neuen bzw. korrigierten Meldung (bzw. eines neuen Berichts).

Eine konkrete Anwendung dieses Anwendungsszenarios ist die Jahresmeldung zur Sozialversicherung.[195] Unternehmen, die sozialversicherungspflichtige Arbeitnehmer beschäftigen, müssen am Jahresanfang die Jahresmeldung zur Sozialversicherung für das vergangene Jahr an die Sozialversicherungsträger (d. h. die Annahmestellen der Krankenkassen) übermitteln.[196] Seit dem 1.1.2006 besteht für die Arbeitgeber die gesetzliche Pflicht, die Sozialversicherungsmeldungen an die gesetzlichen Krankenversicherungen nur noch elektronisch zu übermitteln. Die Kopfstellen der gesetzlichen Krankenversicherung leiten die Daten (Sozial-

---

[195] Brockmann/Hauke, Festlegung von Prozessketten aus dem Bereich der Arbeitgebermeldepflichten für die weitere Pilotierung, Bericht D 3.1.3 des Projekts Pilotierung und Realisierung eines Prozess-Daten-Beschleunigers (P23R) für den Datenaustausch zwischen Wirtschaft und Verwaltung, 2011.

[196] Die Meldepflicht wird durch die Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung (Datenerfassungs- und -übermittlungsverordnung – DEÜV) geregelt. Grundlagen der Vorschriften dieser Verordnung bilden das Vierte, Fünfte und Sechste Buch des Sozialgesetzbuchs sowie das Zweite Gesetz über die Krankenversicherung der Landwirte (KVLG).

versicherungsmeldungen der Unternehmen und Beitragsnachweise der Beschäftigten) unmittelbar an die zuständigen Träger der Krankenversicherung weiter. Die Meldung wird durch den in Tabelle 3 dargestellten Steckbrief beschreiben.

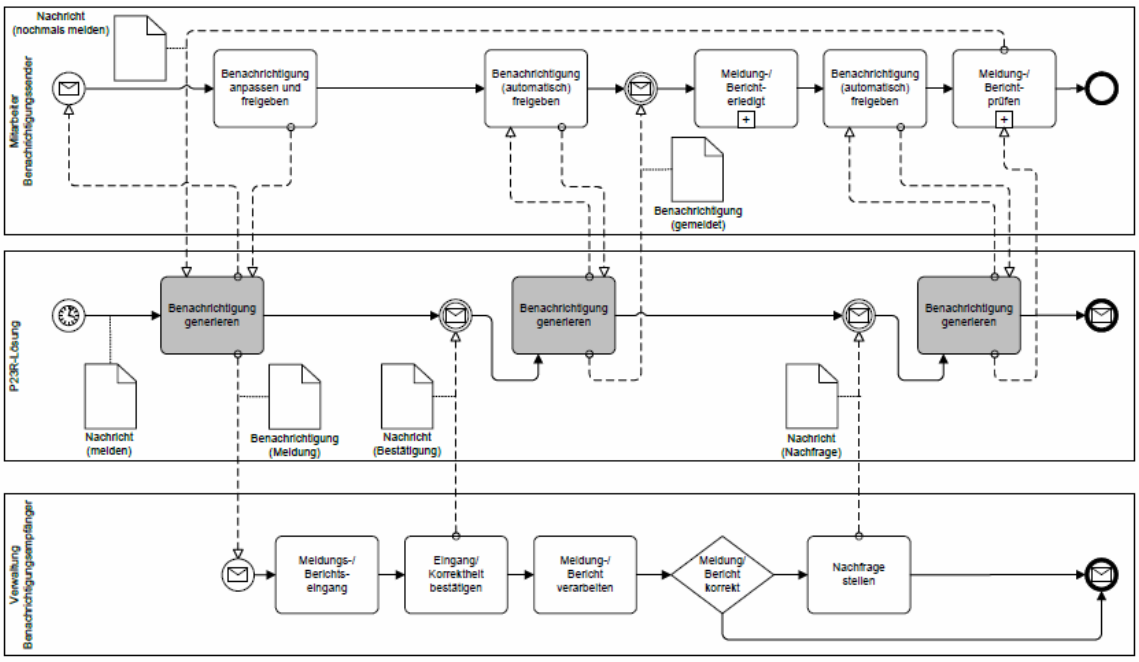

Abbildung 12: P23R Anwendungsszenario »Bericht«[197]

[197] Baum u. a. (Fn. 193).

Allgemeine Beschreibung	**Titel der Informationspflicht**	DEÜV-Jahresmeldung zur Sozialversicherung
	Kontakttyp	Meldung
	Zweck des Verfahrens	Dateninput für das Versichertenverzeichnis der Krankenkasse, für das Versichertenkonto der Rentenversicherungsträger sowie für die Bundesagentur für Arbeit zur Analyse von arbeitsmarktsteuernden Aufgaben.
Inhaltliche Klassifikation	**Thematischer Bereich**	Sozialversicherung
	Typische Informationselemente	Zeitraum der Beschäftigung im Vorjahr, Höhe des beitragspflichtigen Entgelts
	Inhaltstypen	Versicherungsnummer (soweit bekannt), Familien- und Vornamen, Geburtsdatum, Staatsangehörigkeit, Angaben über die Tätigkeit nach dem Schlüsselverzeichnis der Bundesagentur für Arbeit, Betriebsnummer des Beschäftigungsbetriebes, die Beitragsgruppen, zuständige Einzugsstelle, Arbeitgeber
	Beteiligte Akteure – Wirtschaft	Unternehmen mit sozialversicherungspflichtigen Beschäftigten
	Adressat auf Behördenseite	Annahmestellen der Krankenkassen
Technische Beschreibung	**Informationssystem auf Unternehmensseite**	Unterschiedliche, das Schnittstellenverfahren unterstützende Systeme (z.B. maschinell geführte Lohn- und Gehaltsabrechnungsprogramme) oder das durch die Verwaltung bereitgestellte sv.net/classic oder sv.net/online.
	Informationssystem auf Behördenseite	Unbekannt
	Informationssystem/Schnittstelle zur Datenübermittlung	Elektronische Übermittlung gemäß den Vorschriften in § 17 DEÜV, entweder per Datenträger oder mittels DFÜ[198]
	Transportprotokoll	E-Mail, HTTPS 1.1, FTP und andere[199]
	Datenformat	KKS (Dateiformat) oder eXTra (XML)
Gesetzliche Grundlagen	**Gesetzliche Einordnung**	Datenerfassungs- und -übermittlungsverordnung (DEÜV): § 5–15 DEÜV
Prozesskosten	**Bürokratiekosten nach SKM[200]**	Kosten berücksichtigt in Meldepflicht »Information des Beschäftigten über Sozialversicherungsmeldungen« (§ 28a Abs. 5 SGB IV): 29.600.000 Euro
	Zahl der betroffenen Unternehmen	Keine Angaben ermittelbar

TABELLE 3. STECKBRIEF JAHRESMELDUNG ZUR SOZIALVERSICHERUNG[201]

198 GKV Spitzenverband, Elektronischer Datenaustausch, 2010, abrufbar unter www.gkv-datenaustausch.de/.

199 ITSG, Richtlinien für den Datenaustausch im Gesundheits- und Sozialwesen, 2010, abrufbar unter www.gkv-ag.de/upload/TAGKV_2008_V4_09_12_3124.pdf/.

200 Statistisches Bundesamt. (2010). SKM-Datenbank der Bundesregierung: Datenbank aller Informationspflichten (WebSKM) [Online]. Verfügbar: https://www-skm.destatis.de/webskm/online.

4.3.1.3 Architektur

Eine P23R-Lösung kann im jeweiligen Unternehmenskontext spezifisch implementiert und flexibel in bestehende Prozesse (und Prozessverarbeitungssysteme) von Unternehmen und Verwaltung integriert werden. Die zentrale Komponente, der Prozessdatenbeschleuniger (P23R), speichert hierzu nicht nur eine temporäre, zweckgebundene Kopie eines Teils der Unternehmensdaten, um zügig neue Benachrichtigungen erstellen zu können, sondern archiviert auch alle erzeugten Benachrichtigungen sowie die Protokolle über alle Transaktionen (Abbildung 13). Auf der einen Seite wird die P23R-Lösung durch die IT-Unternehmenssysteme (Fachsystem bzw. P23R-Client) gesteuert. Die benötigten Daten werden entweder direkt oder aus einer Transfer-Datenbank (z. B. aus Sicherheitsgründen) geladen und bei Bedarf auch zwischengespeichert. Auf Seiten der Benachrichtigungsempfänger kommuniziert die P23R-Lösung mit den IT-Fachverfahren der Verwaltungen. Fertige Benachrichtigungen empfängt der Benachrichtigungsempfänger normalerweise über die vorgegebenen Schnittstellen des jeweiligen IT-Fachverfahrens.

Die föderative Verteilung von Zuständigkeiten auf verschiedenen Ebenen sowohl bei der Rechtsetzung als auch bei der Aufgabenerledigung macht es erforderlich, Unterstützungsaufgaben entsprechend der jeweiligen politischen und rechtlichen Verantwortung aufzuteilen. Dennoch erfordert die Funktionsfähigkeit von P23R-Lösungen die Bereitstellung einiger zentraler Funktionen, allen voran die Bereitstellung von Benachrichtigungsregelwerken. Weitere Aufgaben der Leitstelle sind die fachliche Beratung der Vorschriftengeber in der Entstehungsphase einer gesetzlichen Vorschrift, die Erarbeitung von Vorschlägen zur Optimierung der Gesamtheit der unterstützten Prozesse sowie die Betreuung von Gremien, die die Interessen verschiedener Beteiligter[202] einbringen.

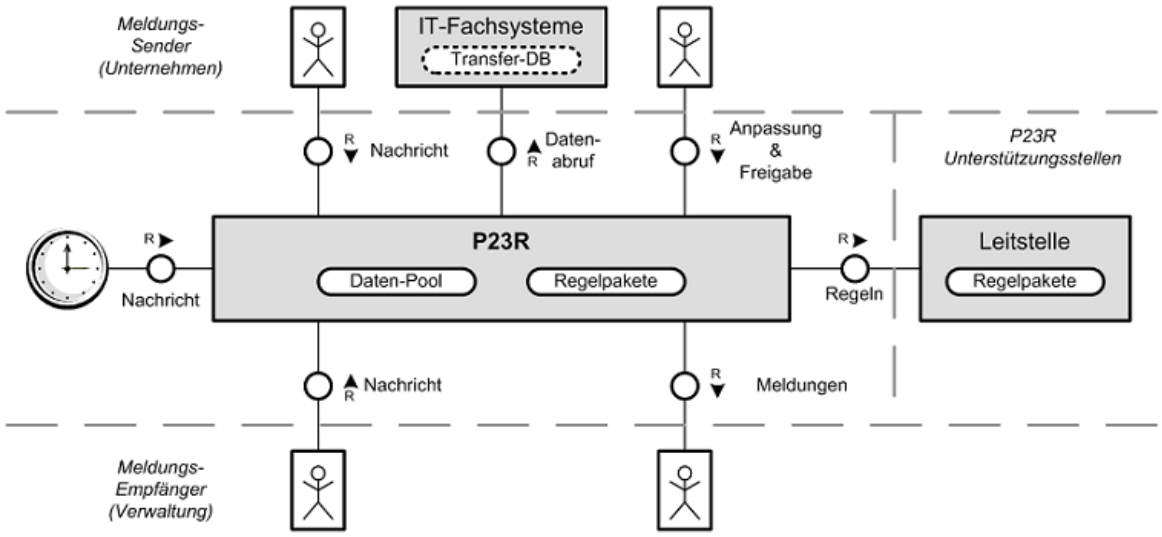

ABBILDUNG 13: P23R-GROBARCHITEKTUR[203]

[201] Brockmann/Hauke, Beschreibung der ausgewählten Prozessketten in Form von Prozess-Steckbriefen, Bericht D 3.1.3 des Projekts Pilotierung und Realisierung eines Prozess-Daten-Beschleunigers (PDB) für den Datenaustausch zwischen Wirtschaft und Verwaltung, 2010.

[202] Hiermit sind im Wesentlichen die betroffenen Unternehmen sowie die Anbieter von IT-Fachsystemen der Unternehmen, die Quelldaten bereitstellen, die Anbieter von P23R-Lösungen und P23R-Provider sowie die Vorschriftengeber und die Empfängerbehörden gemeint.

[203] Baum u. a. (Fn. 193).

4.3.2 Geschichte

Das im Jahre 2006 als Teil des Regierungsprogramms »Zukunftsorientierte Verwaltung durch Innovationen« ins Leben gerufene Programm E-Government 2.0 des Bundes adressierte die »qualitative Optimierung des E-Government-Angebots durch möglichst durchgängige elektronische Transaktionsdienstleistungen sowie ein konsequent service- und nutzerorientiertes Angebot.«[204] Im Rahmen des Programms wurden im Jahre 2008 verschiedene Forschungsaufträge vergeben. Hierbei stand die Entwicklung einer Systematik zur Abwicklung von Datenflüssen und Vorgangsbearbeitungen zwischen Verwaltungen und Unternehmen im Vordergrund. Weiterhin wurden Datenschutz- und Datensicherheitsaspekte untersucht. Die Forschungsergebnisse wurden anhand dreier Machbarkeitsstudien dokumentiert:

1. Entwicklung eines übergreifenden Ansatzes einer Prozesskette zu den Informationspflichten im Bereich »Umwelt«. Federführung: Technische Universität München, Lehrstuhl für Wirtschaftsinformatik.[205]
2. Entwicklung eines übergreifenden Ansatzes einer Prozesskette zu den Informationspflichten im Bereich »Finanzdienstleistungen«. Federführung: Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, Stuttgart.[206]
3. Entwicklung eines übergreifenden Ansatzes einer Prozesskette zu den Informationspflichten im Bereich »Informations- und Meldepflichten der Arbeitgeber«. Federführung Fraunhofer-Institut für Experimentelles Softwareengineering IESE, Kaiserslautern.[207]

Basierend auf den in einem anschließenden Transferprojekt konsolidierten Ergebnissen dieser Studien wurde das P23R-Projekt im Maßnahmenbereich »Zukunftsfähigkeit mit Innovationen« des IT-Investitionsprogramms[208] der Bundesregierung ausgeschrieben.

Im Projekt »Pilotierung und Realisierung des Prinzips Prozess-Daten-Beschleuniger | P23R für den Datenaustausch zwischen Wirtschaft und Verwaltung«[209] wurde die Entwicklung von Methoden und offenen Standards für eine vernetzte und übergreifende Architektur für den vereinfachten Datenaustausch zwischen Wirtschaft und Verwaltung dargestellt. Von Juni 2010 bis November 2011 wurden die Ergebnisse dieses Projekts von einem Konsortium

---

204 Bundesministerium des Innern, Abschlussbericht E-Government 2.0, Berlin, 2010, abrufbar unter www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/Abschlussbericht_E-Gov2_0.pdf?__blob=publicationFile/.

205 Bundesministerium des Innern, Machbarkeitsstudie Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung: Umwelt, 2009, abrufbar unter www.cio.bund.de/SharedDocs/Publikationen/DE/E-Government/090515_machbarkeitsstudie_umwelt_download.pdf?__blob=publicationFile/.

206 Bundesministerium des Innern, Machbarkeitsstudie Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung: Finanzdienstleistungen, 2009, abrufbar unter www.cio.bund.de/SharedDocs/Publikationen/DE/E-Government/090512_machbarkeitsstudie_finanzdienstleistungen_download.pdf?__blob=publicationFile/.

207 Bundesministerium des Innern, Machbarkeitsstudie Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung: Arbeitgebermeldungen, 2009, abrufbar unter www.cio.bund.de/SharedDocs/Publikationen/DE/E-Government/090213_machbarkeitsstudie_arbeitgebermeldungen_download.pdf?__blob=publicationFile/.

208 www.cio.bund.de/DE/Strategische-Themen/IT-Investitionsprogramm/it_investitionsprogramm_node.html/.

209 www.cio.bund.de/DE/Strategische-Themen/IT-Investitionsprogramm/it_investitionsprogramm_node.html/.

bestehend aus 13 Organisationen aus Wirtschaft und Wissenschaft sowie der Metropolregion Rhein-Neckar exemplarisch umgesetzt.

Als Testgebiet für die Funktionsfähigkeit und Interoperabilität des P23R-Prinzips wurde die Metropolregion Rhein-Neckar ausgewählt. Zu den Pilotpartnern zählen meldepflichtige Unternehmen und Dienstleister und auf der Empfängerseite der Meldungen sechs Berufsgenossenschaften, drei statistische Landesämter sowie das Umweltbundesamt und weitere Umweltüberwachungsbehörden in Hessen und Rheinland-Pfalz.

4.3.3 Schlussfolgerungen für IT-Projekte mit Datenbezug

Als positiv zu bewerten ist, dass die Sicherheitsanforderungen von vorneherein beachtet wurden und auch ein umfassendes Sicherheitskonzept erstellt wurde. Ergebnisse über die Pilotierung des P23R-Projekts stehen im Internet zur Verfügung.[210] Software-Hersteller können sich darüber hinaus mit anderen Anbietern austauschen oder über Weiterentwicklungen diskutieren.[211]

Dienstleister, die P23R anbieten, können dies auch in Form eines Software-as-a-Service Angebots tun, müssen jedoch ein entsprechendes Sicherheitskonzept nachweisen. Eine Anforderung besteht bezüglich Mandantenfähigkeit, um Daten und Prozesse vor anderen Mandanten zu schützen.

Um Intermediären, bspw. Steuerberatern oder Buchhaltern, die im Auftrag einer Firma handeln, Zugriff auf die Daten zu gestatten, muss es sichere rollen- und rechtebasierte Zugriffsfunktionen geben. Dieser Zugriffschutz gilt nicht nur für Externe, sondern auch intern muss ein entsprechender Zugriffsschutz festgelegt sein.

4.4 De-Mail, insbesondere Dokumentensafes nach § 8 DeMailG

Schließlich sind zur Ermittlung der Anforderungen an IT-Systeme, die der Kommunikation auch mit staatlichen Stellen dienen sollen und auf dem Gedanken der Freigabe von Dokumenten basieren, die De-Mail und das zugrundeliegende Gesetz zu betrachten. Zunächst zeigt die Fokussierung auf den Postfach- und Versanddienst nach § 5 DeMailG als Kernfunktionalität ein Verständnis von Kommunikationsprozessen, welches auf dem Prinzip »Senden – Empfangen« basiert, während bspw. alle genannten Projekte schon einen Schritt weiter gehen und das »Freigabe-Paradigma« zu realisieren suchen. Das Cloud- und Safe-Prinzip ist zwar in § 8 DeMailG angelegt, allerdings nur rudimentär und ohne explizit Freigaben zu thematisieren.

4.4.1 Geschichte

Das Projekt »Bürgerportale« war zunächst Teil der High-Tech-Strategie und des E-Government-Programms 2.0[212] der Bundesregierung. Es wurde federführend vom Bundesministerium des Innern (BMI) in Zusammenarbeit mit weiteren Institutionen und Organisationen durchgeführt. Die Erarbeitung der konzeptionellen Grundlagen war schon im Jahre 2007 im

---

[210] www.p23r.de/.

[211] Deployment-board@p23r.de.

[212] Dazu auch Biernert, GewArch 2008, 417 ff.; Otten, VW 2007, 1440.

Wesentlichen abgeschlossen, wobei lediglich das Grobkonzept sowie ein Gesetzesentwurf der Öffentlichkeit zugänglich gemacht wurden,[213] der aufgrund der Diskontinuität jedoch in der vergangenen Legislaturperiode nicht verabschiedet werden konnte. Unter verändertem Titel wurde das De-Mail-Gesetz schließlich als Art. 1 des Gesetzes vom 28. 04. 2011[214] vom Bundestag beschlossen. Es ist gem. Art. 6 dieses Gesetzes am 03. 05. 2011 in Kraft getreten.[215]

Im Gesetzgebungsverfahren wurden auch **(Daten-)Sicherheitsaspekte** kontrovers diskutiert. Explizit wurde eine Ende-zu-Ende-Verschlüsselung als Standard gefordert; eine Forderung, die sich jedoch nicht durchsetzen konnte.[216] Dienste, die die De-Mail-Sicherheitsstandards erfüllen, eignen sich daher bspw. auch für einen Einsatz im Sozialverfahren – die Akkreditierung verdeutlicht dies lediglich nach außen erkennbar, zwingende Voraussetzung für die Einsetzbarkeit ist sie hingegen nicht.[217] Das eingesetzte Verfahren ist hinreichend im Rahmen des § 78a SGB X in Verbindung mit der entsprechenden Anlage zu bewerten; es dürfte darüber hinaus auch die explizite Anordnung von **Verschlüsselungsverfahren nach dem »Stand der Technik«** gem. der Anlage zu § 9 BDSG und nach § 87a Abs. 1 AO erfüllen. Diese ist in Form einer **Transport- und providerseitigen Nachrichtenverschlüsselung** gewährleistet und der Gesetzgeber hat diese – insofern für alle Verwaltungsbereiche verbindlich, soweit nicht explizit für besonders sensible Daten Ende-zu-Ende-Verschlüsselungen begründet werden können – als ausreichend erachtet.

4.4.2 Zielsetzung und Funktionsweise

In § 1 Abs. 1 DeMailG werden die De-Mail-Dienste als »Dienste auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen«, beschrieben. Die Anbieter sind verpflichtet, eine sichere Anmeldung (bezogen auf die Erstregistrierung und die späteren Anmelde- und Versandprozesse), einen Postfach- und Versanddienst für sichere elektronische Post sowie einen Verzeichnisdienst verpflichtend anzubieten, zusätzlich können auch Identitätsbestätigungs- und Dokumentenablagedienste ermöglicht werden.

Mit Blick auf Dokumentensafes ist vor allem die Regelung des § 8 DeMailG von besonderer Bedeutung, für die Absicherung der Datenhoheit in Cloud-Systemen – wie bereits gezeigt (3.2.4.3) – der Identitätsbestätigungsdienst nach § 6 DeMailG und ganz allgemein der Umstand, dass der Postfach- und Versanddienst eine identifizierbare elektronische Nachrichtenübermittlung etabliert (3.2.4.4).

Reine »Online-Festplatten« unterliegen bisher keinem speziellen Rechts- und Datenschutzregime, vielmehr kommen die allgemeinen Vorgaben aus TKG, TMG und BDSG zur Anwen-

---

213 Vgl. BR-Drs. 174/09; BT-Drs. 16/12598; zum Referentenentwurf Stach, DuD 2008, 1 ff.; Probst, DSB 2/2009, 16 ff.; Stach/Wappenschmidt, eGov Präsenz 2/2009, 78 ff.; Warnecke, MMR 2010, 227 ff.; s. auch Werner/Wegner, CR 2009, 310 ff.; Schallbruch, it 2009, 125 ff.; Steppling, NJW-Editorial 18/2009; Roßnagel u. a., DuD 2009, 728 ff.; kritisch Lapp, DuD 2009, 651 ff.; Fox, DuD 2009, 387; zur Authentizität elektronischer Kommunikation vor Einführung der »De-Mail« Kast, CR 2008, 267 ff.; vgl. auch Schulz, DuD 2009, 601 ff.

214 BGBl I, S. 666; dazu Rose, K&R 2011, 439 ff.; Roßnagel, NJW 2011, 1473 ff.; Spindler, CR 2011, 309 ff.; zum Entwurf Roßnagel, CR 2011, 23 ff.

215 Die weiteren Artikel enthalten Änderungen der ZPO, des VwZG sowie eine Evaluationsklausel.

216 Vgl. zu der zu diesem Aspekt geführten Diskussion im Rahmen des Gesetzgebungsverfahrens zum De-Mail-Gesetz die Pressemitteilung des Deutschen Bundestages vom 17. 12. 2010 unter dem Titel »Bundesrat fordert Ende-zu-Ende-Verschlüsselung bei De-Mail«; abrufbar unter www.bundestag.de/; dazu auch Roßnagel, CR 2011, 23 (27); Lechtenbörger, DuD 2011, 268 f.

217 Ausführlich Schulz/Tischer, NZS 2012, 254 ff.

dung. § 8 DeMailG schafft insoweit (begrenzte) Abhilfe, zumal einige spezielle Funktionen und Sicherheitsanforderungen an den Safe (und den Safe Provider) gestellt werden.

Er lautet:

> *»Der akkreditierte Diensteanbieter kann dem Nutzer eine Dokumentenablage zur sicheren Ablage von Dokumenten anbieten. Bietet er die Dokumentenablage an, so hat er dafür Sorge zu tragen, dass die Dokumente sicher abgelegt werden; Vertraulichkeit, Integrität und ständige Verfügbarkeit der abgelegten Dokumente sind zu gewährleisten. Der akkreditierte Diensteanbieter ist verpflichtet, alle Dokumente verschlüsselt abzulegen. Der Nutzer kann für jede einzelne Datei eine für den Zugriff erforderliche sichere Anmeldung nach § 4 festlegen. Auf Verlangen des Nutzers hat der akkreditierte Diensteanbieter ein Protokoll über die Einstellung und Herausnahme von Dokumenten bereitzustellen, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz gesichert ist.«*

Bisher ist allerdings nicht erkennbar, dass im Rahmen des Akkreditierungsverfahrens auch **safespezifische Aspekte** explizit geprüft werden,[218] da sich das Prüfprogramm überwiegend auf den »Postfach- und Versanddienst« des § 5 DeMailG bezieht und das Verhältnis beider Angebote zueinander nicht abschließend geklärt ist. Fraglich ist bspw., ob die Akkreditierung für »isolierte« Cloud- und Safe-Anbieter überhaupt in Betracht zu ziehen ist, zumal immer auch die »De-Mail-Grundfunktionalität« des Postfach- und Versanddienstes zur Verfügung gestellt werden muss.[219] Auch wird der Unterschied zwischen elektronischen Safes, die eine erhöhte Sicherheit bieten, bspw. weil die nachfolgend formulierten Vorgaben zur Sicherstellung der Datenhoheit vollständig erfüllt werden, und solchen, die eher als Online-Festplatte anzusehen sind, gleichwohl die Vorgaben des § 8 DeMailG erfüllen, nach außen nicht sichtbar. Beide könnten sich in zulässiger Weise als »De-Mail akkreditiert« betiteln.

4.4.3 Schlussfolgerungen für IT-Projekte mit Datenbezug

Für IT-Projekte mit Datenbezug lassen sich aus dem De-Mail-Gesetz und vor allem auch der Debatte im Vorfeld folgende Aspekte festhalten:

- Angesichts der Komplexität sicherer Infrastrukturen ist es für einen Großteil der Nutzer nicht möglich, selbst die entsprechenden Vorkehrungen zu unterhalten. Insofern wird zukünftig gerade im Cloud- und Datensafe-Umfeld **vertrauenswürdigen Dritten**, derer sich die Nutzer bedienen, eine herausragende Rolle bei der Absicherung der individuellen Datenhoheit zukommen.
- Diese Entwicklung kann der Staat begleiten, indem er **Akkreditierungs- und Zertifizierungsverfahren** etabliert, die als »Vertrauensanker« und zur Steigerung der Akzeptanz dienen. Denkbar ist auch eine rechtliche Förderung

---

[218] Einen Anhaltspunkt bietet § 18 Abs. 1 Nr. 3 DeMailG, nach dem im Akkreditierungsverfahren die »technischen und organisatorischen Anforderungen an die Pflichten nach den §§ 3 bis 13« geprüft werden und insofern die Regelung des § 8 DeMailG zur »sicheren Dokumentenablage« einbezogen ist.

[219] Dies ergibt sich aus § 1 Abs. 2 DeMailG, der den Postfach- und Versanddienst pflichtig, alle anderen Dienste optional und quasi »akzessorisch« ausgestaltet: »Ein De-Mail-Dienst muss eine sichere Anmeldung, die Nutzung eines Postfach- und Versanddienstes für sichere elektronische Post sowie die Nutzung eines Verzeichnisdienstes und kann zusätzlich auch Identitätsbestätigungs- und Dokumentenablagedienste ermöglichen.«

»sicherer« Dienste, bspw., indem staatliche Kommunikationsprozesse auf akkreditierte Angebote beschränkt bleiben.[220]

- Zudem lässt sich festhalten, dass bei derartigen Diensten immer ein **Ausgleich zwischen Usability und Sicherheitsaspekten** gefunden werden muss, was im Kontext der De-Mail dazu geführt hat, auf eine Ende-zu-Ende-Verschlüsselung zu verzichten. Die Kombination aus Transport- und providerseitiger Nachrichtenverschlüsselung dürfte auch für Cloud-Lösungen (soweit nicht aufgrund der Verlagerung von Datenbeständen in andere als EU-Staaten eine Aufhebung des Personenbezugs notwendig wird) in der Regel ausreichend sein.

4.5 Analyse und Definition grundlegender Anforderungen für IT-Projekte mit Datenbezug

Anforderungen seitens eines Kunden – seien es Firmen, Verwaltungen oder Verbraucher – beziehen sich hautsächlich auf die Einhaltung eines angemessenen Datenschutzniveaus, beim Wechsel zwischen Anbietern die Daten wiederzubekommen, jederzeit auf die Daten zugreifen und vor allen Dingen dem Anbieter vertrauen zu können. Vertrauen bezieht sich in diesem Fall auf die Konformität der Datenverarbeitung mit den gesetzlichen Vorschriften, die nachweisbar dem Kunden zur Verfügung gestellt werden, damit dieser seiner Kontrollpflicht nachkommen kann.

So haben Kunden, seien es Firmen oder Verwaltung, die Verpflichtung zur Kontrolle beim Cloud-Anbieter. Sie sind verantwortlich, zu überprüfen, ob dieser den gesetzlichen Bedingungen im Umgang mit personenbezogenen Daten nachkommt. Dabei müssen die Kunden selbst darauf achten, dass die zum Zweck der Datenverarbeitung gespeicherten personenbezogenen Daten dem Grundsatz der Datensparsamkeit unterliegen, fristgerecht gelöscht und vom Cloud-Anbieter nicht eingesehen werden können.

Anforderungen an Cloud-Anbieter beziehen sich in diesem Zusammenhang auf den Zugriffsschutz vor Fremden, Möglichkeit der Einsichtnahme in Protokolle, die die fristgerechte Löschung von Daten erfordern, Einsichtnahme in die Protokollierung der Zugriffe auf personenbezogenen Daten, um sicherzustellen, dass kein Missbrauch stattgefunden hat und eine Aussage darüber, an welchen Orten die Daten verarbeitet und gespeichert werden, falls ein der Cloud-Anbieter aus Gründen der Verfügbarkeit selbst weitere Anbieter unterbeauftragt.

Dem Endnutzer/Verbraucher muss das Recht auf Löschung oder Berichtigung seiner Daten gewährt werden. Dazu muss der Cloud-Anbieter entsprechende Werkzeuge bereitstellen, die einerseits dem Kunden ermöglichen, eine entsprechende Anfrage zu stellen, darüber hinaus aber auch eine Funktion für die Berichtigung falscher Daten ermöglicht. Cloud-Anbieter die nachweislich »Privacy-by-Design«-Prinzipien verfolgen sind von Vorteil.

Dritten wird die Einsichtnahme personenbezogener Daten erschwert, wenn die Daten seitens der Kunden auf eigenen Endgeräten verschlüsselt und erst dann in der Cloud abgelegt

[220] Dies zeigt sich am Beispiel des Entwurfs eines E-Government-Gesetzes des Bundes, der die Schriftformäquivalenz elektronischer Dokumente auf De-Mails beschränken will (§ 3a VwVfG-E). Andere Dienste, die zwar die gleichen Sicherheitsanforderungen verwirklichen, aber aus bestimmten Gründen auf eine Akkreditierung verzichten, sind insofern ausgeschlossen.

werden. Allerdings ist dies nur für die Speicherung von Daten möglich; zum Zweck der Datenverarbeitung beim Cloud-Anbieter müssen die Daten entschlüsselt werden, was bedeutet, dass der Schlüssel beim Cloud-Anbieter aufbewahrt wird.

Eine grundlegende Anforderung ist, dass der Cloud-Anbieter ein Datenschutz- und Sicherheitsmanagement unterstützt. Nur so können die Schutzziele[221] Vertraulichkeit, Verfügbarkeit und Informationssicherheit gewährleistet werden.

[221] Bundesamt für Sicherheit in der Informationstechnik, Leitfaden Informationssicherheit, IT-Grundschutz kompakt, 2012, abrufbar unter www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile/.

5 Konzepte für Datenhoheit in der Cloud

Die Grundidee des Cloud Computings weist erhebliche Parallelen zu anderen Infrastrukturen der Grundversorgung auf, die zentral und gerade nicht auf Nutzerseite vorgehalten werden. »Ebenso wenig wie Unternehmer und Privatleute zur Deckung ihres Energiebedarfs zum Betrieb eigener Stromgeneratoren gezwungen sind, soll der Anwender auch keine eigene IT-Infrastruktur mehr bereithalten müssen, sondern Speicher, Rechenkapazitäten und Softwareanwendungen aus der Steckdose beziehen«.[222] Insofern liegt es nahe, ebenfalls von einer infrastrukturellen Verantwortung des Staates auszugehen, die sich zunehmend auch auf die verschiedenen Elemente eines technikgestützten Identitätsmanagements bezieht.

Ausgehend von der Definition einer individuellen Datenhoheit (2.1), die es zu sichern gilt, der Beschreibung der rechtlichen und technisch-infrastrukturellen Grundlagen (3) sowie einer Anforderungsanalyse aufgrund von Referenzprojekten mit Daten- und Safebezug im Sinne von »Lessons learned« (4) sollen nachfolgend rechtliche und technisch-organisatorische Konzepte vorgestellt werden, die einerseits eine **größtmögliche Absicherung der Datenhoheit** bewirken, andererseits aber die mit den Cloud-Technologien verbundenen Chancen nutzen. Ausgehend vom oben genannten Verständnis der Datenhoheit gilt es, die Elemente »Verfügbarkeit«, »Verfügungsbefugnis«, »Vertraulichkeit« und »Integrität« abzusichern (5.3). Vorgelagert stellt sich aber die Frage, ob dem Einzelnen überhaupt ein rechtliches und faktisches Wahlrecht zwischen sicheren und unsicheren Varianten bzw. zwischen eigener Infrastruktur, staatlicher Datenhaltung und vertrauenswürdigen Dritten eingeräumt ist, oder der Staat dies zunächst quasi in einem ersten Schritt abzusichern hat (5.1 und 5.2).

[222] Pohle/Ammann, CR 2009, 273 (273).

5.1 Wahlfreiheit des Bürgers zwischen den denkbaren Modellen

Nach dem zuvor Gesagten bezieht sich die Gewährleistungsverantwortung des Staates auch darauf, die Datenhoheit des Einzelnen im beschriebenen Sinne – vor allem gegenüber anderen Privatrechtssubjekten – effektiv abzusichern. Dies bedeutet zunächst, dass eine Wahlfreiheit zwischen den unterschiedlichen Varianten (Datenhaltung in einer eigenen Infrastruktur, bei vertrauenswürdigen Dritten oder bei staatlichen Stellen) bestehen muss, die sich gerade durch den Grad an eigener Beherrschung der Daten unterscheiden.

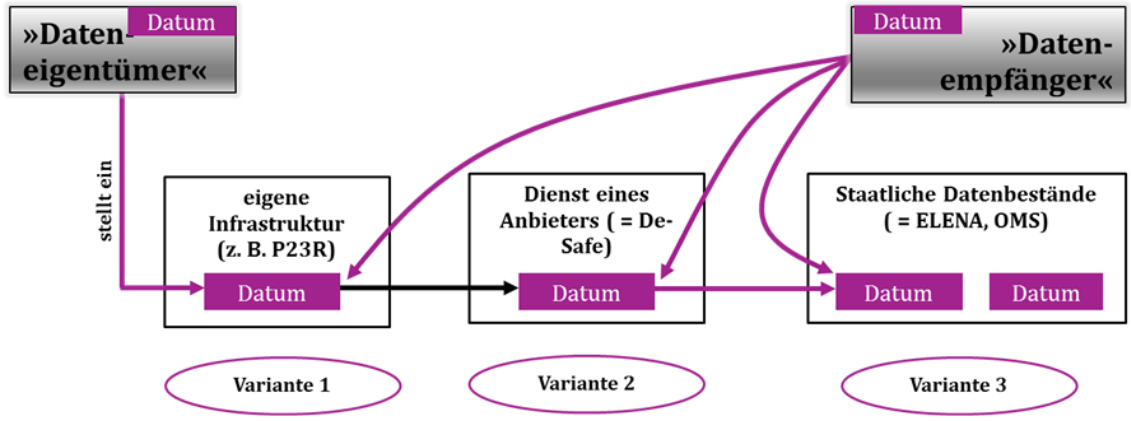

ABBILDUNG 14: DREI UNTERSCHIEDLICHE GRUNDMODELLE

Grundvoraussetzung ist einerseits die **faktische Existenz** der verschiedenen Grundmodelle, die nicht unmittelbar vom Staat gesichert werden kann (sollte). Staatliche Aktivitäten können aber auf eine Förderung sicherer Dienste gerichtet sein, sei es durch die Finanzierung von Forschungsvorhaben (wie im Kontext P23R) oder auch durch Subventionierungen.

Auf regulativer **rechtlicher Ebene** sollten zukünftig alle drei Modelle – soweit sie ein vergleichbares Sicherheitsniveau aufweisen – als gleichwertig anerkannt werden. Dies bedeutet, dass, wenn eine bestimmte Meldepflicht oder Ähnliches gegenüber staatlichen Stellen besteht, der Bürger bspw. nicht auf eine Übermittlung des Datensatzes verwiesen werden kann, wenn er dem P23R-Prinzip entsprechende Infrastrukturen besitzt. In diesem Fall hat die Behörde die erforderlichen Daten ihrerseits abzurufen. Gleiches gilt insofern auch für Daten, die in Datensafes bei einem privaten Dritten vorgehalten werden. Nach heutigem Stand ist die elektronische Kommunikation »über Safes« zwar unter § 3a VwVfG zu subsumieren,[223] dennoch ist nicht ersichtlich, dass solche Kommunikationsformen schon als gleichwertig betrachtet werden. Diesbezüglich besteht – bspw. was die Zugangseröffnung angeht – weiterer Konkretisierungsbedarf, um eine rechtliche Gleichwertigkeit der drei Grundmodelle und damit das Wahlrecht des Betroffenen effektiv abzusichern. Akkreditierungen können zwar eine vertrauensverstärkende Wirkung haben, die Verknüpfung mit rechtlichen Privilegien (bspw. die Begrenzung der Schriftformäquivalenz auf De-Mail-

[223] Vgl. Albrecht/Heckmann, in: Bauer u. a. (Hrsg.), VwVfG, 2011, § 3a Rn. 53.

akkreditierte Anbieter)[224] müssen aber – schon aus wettbewerbsrechtlichen Gründen – sorgfältig abgewogen werden.

5.2 ...und Absicherung des »Grundmodells 2« (Existenz vertrauenswürdiger Diensteanbieter) durch den Staat

Eine bestehende Wahlfreiheit in diesem Sinne kann aber nur real werden, wenn tatsächlich entsprechende Angebote am Markt bestehen, was vor allem für elektronische Datenablagen bei Dritten bedeutet, dass diese auch hinreichend vertraulich sein und den steigenden Anforderungen an Datenschutz, Datensicherheit und Datenverfügbarkeit gerecht werden müssen. Online-Festplatten unterliegen bisher keinem speziellen Rechts- und Datenschutzregime – eine präventive Prüfung findet nicht statt, der Nutzer muss auf die Einhaltung dieser Standards durch den Anbieter vertrauen.[225]

§ 8 DeMailG schafft insoweit begrenzte Abhilfe, zumal einige spezielle Funktionen und Sicherheitsanforderungen an die Dateiablage (und deren Betreiber) gestellt werden. Der akkreditierte Diensteanbieter hat dafür Sorge zu tragen, dass die Dokumente sicher abgelegt werden, d. h., dass **Vertraulichkeit, Integrität und ständige Verfügbarkeit** der abgelegten Dokumente gewährleistet sind. Er ist zudem verpflichtet, die Dokumente verschlüsselt abzulegen und es dem Nutzer zu ermöglichen, für jede einzelne Datei eine für den Zugriff erforderliche sichere Anmeldung nach § 4 DeMailG festzulegen. Auf Verlangen des Nutzers hat der akkreditierte Diensteanbieter ein Protokoll über die Einstellung und Herausnahme von Dokumenten bereitzustellen, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz gesichert ist.

Zwar lassen sich Cloud-Dienste aufgrund technischer Möglichkeiten so fortentwickeln, dass von einem neuen Niveau bezüglich Datensicherheit und Datenschutz ausgegangen werden kann. Allerdings kommt trotz der verbesserten technischen Sicherheit der Ausgestaltung der organisatorischen und rechtlichen Rahmenbedingungen auch in Zukunft eine gewisse Bedeutung zu, da kein technisches System vollständige Sicherheit gewährleisten kann. Für den Nutzer wird auch weiterhin technisch kaum nachvollziehbar sein, ob der ausgewählte Anbieter die ihm anvertrauten Daten tatsächlich sicher und vertraulich behandelt. Weil der Nutzer informationstechnische Systeme immer weniger beherrscht und die technischen Arbeitsabläufe nicht »durchschaut«, muss er auf die Integrität, also das Fehlen einer Infiltration und Manipulation vertrauen. Das IT-Grundrecht ist daher eine gefährdungsspezifische Ausprägung des allgemeinen Persönlichkeitsrechts, die rechtliche Antwort auf diese fehlende Beherrschbarkeit und Anknüpfungspunkt staatlicher Schutzpflichten. Gerade gesetzliche Grundlagen können daher zur Bildung des notwendigen Vertrauens und so zur Akzeptanzsteigerung beitragen: Zum einen kann dem Nutzer die Auswahl eines geeigneten und vertrauenswürdigen Anbieters erleichtert werden, indem der Staat seiner Infrastrukturverantwortung durch das Aufstellen von Rahmenbedingungen nachkommt, die ein vertrauenswürdiger Anbieter erfüllen muss. Von diesem Verständnis zeugt auch § 8 DeMailG. Das Instrument der Zertifizierung basiert auf der Idee, dass derjenige Anbieter einen Marktvorteil erhalten soll, der vordefinierte rechtliche Standards einhält und dieses

---

224 S. bereits Fn. 220.

225 Zum Vertrauen im Kontext der Internetnutzung Boehme-Neßler, MMR 2009, 439 ff.; speziell zum Technikmisstrauen Heckmann, DuD 2009, 656 ff.

seinen Kunden gegenüber durch ein Zertifikat nachweisen kann.[226] Zum anderen kann ein gesetzlicher Rahmen, der unerwünschte Risiken abfedert (z. B. Fragen der Haftung im Falle des Datenverlustes, Zulässigkeit von Vertragsklauseln, allgemeine Rechtsschutzmöglichkeiten), dem Einzelnen ein subjektives Sicherheitsgefühl vermitteln. Da aber ein blinder Glaube an die Schutzpotenziale des Rechts genausowenig wie an die der Technik zum Ziel führt, bedarf es eines sinnvollen Zusammenspiels beider Komponenten.[227]

Gleichzeitig muss ein gesetzlicher Rahmen den Anbietern aber auch hinreichende Flexibilität für attraktive Geschäftsmodelle bieten. So können einige Funktionalitäten und Anforderungen verpflichtend, bspw. im Rahmen einer Regulationsrechtsetzung bzw. eines Zertifizierungsverfahrens zu erbringen sein, andere freiwillig als Ergänzung zu diesem Mindeststandard ausgehend von der Nachfrage der Nutzer hinzutreten. Notwendig wäre daher ein (eigenständiger) gesetzlicher Rahmen, gegebenenfalls in Verbindung mit einer Rechtsverordnung, welcher verbindliche Anforderungen an Cloudanbieter aufstellt. Denkbar wäre alternativ eine Fortentwicklung der safespezifischen Bestandteile des De-Mail-Gesetzes, zumal derzeit wohl auch zahlreiche »Online-Festplatten« unter § 8 DeMailG fallen und das konkrete safespezifische Prüfprogramm im Rahmen des Akkreditierungsprozesses nicht erkennbar ist.

Legt man dieses Modell zugrunde, würde sich der Markt für Cloud-Anbieter differenzieren – nach Durchführung eines (freiwilligen) Zertifizierungsverfahrens wäre man nicht nur zum Führen einer bestimmten Bezeichnung berechtigt, denkbar erscheint, es gerade auch bestimmte Funktionalitäten (bspw. den rechtssicheren Austausch mit Behörden, die Gleichstellung elektronischer Safe-Kommunikation mit der Brief- oder De-Mail-Kommunikation) ausschließlich auf Anbieter, die einen »sicheren Safe« anbieten, zu begrenzen. Allerdings ist in diesem Zusammenhang auf die Technologie- und Zukunftsoffenheit derartiger Regelungen und die konkrete Ausgestaltung zu achten. Diesen Anforderungen wird bspw. die beabsichtigte Änderung des § 3a VwVfG in Form der Gleichstellung der De-Mail mit der Schriftform nicht gerecht, da andere – gleichwertig »sichere« – Kommunikationsformen (wie z. B. der E-Postbrief der Deutschen Post AG) zur Verfügung stehen, denen zwar eine Akkreditierung möglich ist, aber mit einer unverhältnismäßigen Beeinträchtigung ihres Geschäftsmodells verbunden wäre.[228] Daneben bestünde weiterhin ein Markt »freier« Anbieter, die bspw. die schon heute denkbaren und vorhandenen Services einer Online-Festplatte anbieten könnten. Der Nutzer ist dann in die Lage versetzt, ausgehend von seinen persönlichen Anforderungen eine Entscheidung zu treffen.

---

[226] Weichert, in: Klumpp u. a. (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, 2008, S. 325 ff.; zu Zertifizierungen von Software und Systemen Quiring-Kock, DuD 2010, 178 (179); zum sog. Datenschutzaudit Bizer, in: Simitis (Hrsg.), BDSG, § 9a Rn. 2 ff; Albers, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. II, § 22 Rn. 164.

[227] Hornung, MMR 2004, 3 (7); vgl. dazu auch Gusy, DuD 2009, 33 (35); speziell zum Datenschutzrecht Albers (Fn. 226), Rn. 34 ff.

[228] Da bestimmte Funktionalitäten, die gerade den Mehrwert des Angebots der Deutschen Post AG darstellen (der Hybridbrief), strikt von den De-Mail-Diensten zu trennen sind; eine kaum praktikable Lösung.

5.3 Absicherung der Bestandteile individueller Datenhoheit

Neben der Wahlfreiheit müssen auch die einzelnen Bestandteile der individuellen Datenhoheit abgesichert werden. Einerseits ist es aus (IT-)infrastrukturellen Gründen erwünscht, dass vermehrt Cloud-Angebote genutzt werden. Der Staat steht hier in der Verantwortung, die nötigen Voraussetzungen für diese IT-Infrastruktur zu schaffen. Andererseits darf sich der Staat nicht damit begnügen, Cloud-Konzepte zu ermöglichen, da sonst die Gefahr bestünde, dass die Nutzer dieser Cloud-Angebote Einbußen an ihren aus Art. 2 Abs. 1 GG folgenden Rechten erleiden. Daraus folgt, dass der Staat auch dafür Sorge zu tragen hat, dass die Datenhoheit der Bürger bei der Inanspruchnahme von Cloud-Services – unabhängig in welchem Modell realisiert – gewahrt bleibt. Dabei muss das zwischen der Ermöglichung von Cloud-Konzepten und der Absicherung der Datenhoheit in der Cloud bestehende Spannungsfeld aufgelöst werden. Es gilt, sowohl für den Anbieter von Cloud-Services attraktive Geschäftsmodelle zu ermöglichen als auch für den Nutzer dieser Angebote reizvolle Rahmenbedingungen zu schaffen, damit er den angebotenen Cloud-Infrastrukturen guten Gewissens seine Daten anvertrauen kann.

5.3.1 Verfügbarkeit

Der Träger der Datenhoheit muss jederzeit und von jedem Ort aus auf seine in der Cloud gespeicherten Daten zugreifen können. Dies müssen die Anbieter von Cloud-Services gewährleisten. Die Verfügbarkeit wiederum ist Bestandteil des Vertrags zwischen Cloud-Anbieter und Kunden, wobei der Cloud-Anbieter dafür Sorge tragen muss, dass technische Maßnahmen wie Redundanzen und Schutz vor Sabotageversuchen entsprechend abgebildet werden. Eine weitere wesentliche Voraussetzung für die Verfügbarkeit ist die Netzverfügbarkeit, damit der Kunde überhaupt auf die Cloud zugreifen kann.

5.3.1.1 Rechtliche Aspekte

Insofern stellt sich zunächst die Frage, durch welche rechtlichen Instrumentarien die Verfügbarkeit der Daten als Teil der Datenhoheit gewährleistet werden kann.

Fallkonstellationen

Schwierigkeiten im Bereich der Datenverfügbarkeit ergeben sich aus den verschiedensten Gründen. So kann es etwa sein, dass der Vertrag zwischen Cloud-Nutzer und Cloud-Anbieter schlicht »ausläuft« (Befristung) oder von einer Seite außerplanmäßig beendet wird (**ordentliche oder außerordentliche Kündigung** – etwa aufgrund eines Zahlungsverzugs des Cloud-Nutzers –, Anfechtung). Daneben könnte es vorkommen, dass der Cloud-Anbieter insolvent wird und eine Fortführung des Unternehmens und infolgedessen des Cloud-Services nicht in Betracht kommt. In den genannten Beispielen wird das Nutzungsverhältnis bezüglich der Cloud jeweils beendet.

Darüber hinaus ist denkbar, dass sich der Anbieter von Cloud-Diensten in seinen **Service Level Agreements** (SLA) bestimmte Zugriffsrechte auf die Daten vorbehält und während des Zugriffs durch den Anbieter ein Zugriff durch den Nutzer und Datenhoheitsträger ausgeschlossen ist. Außerdem ist es üblich, nur eine bestimmte **Verfügbarkeitsquote** zu ga-

rantieren.[229] Ebenso vorstellbar ist eine anbieterseitige Sperrung des Zugangs für den Cloud-Verwender, etwa bei Zahlungsverzug oder anderen Pflichtverletzungen. In diesen Fällen wird das Nutzungsverhältnis nicht beendet, sondern die Zugriffsmöglichkeit des Nutzers auf seine Daten lediglich beschränkt.

Tatsächliche Handhabung

In den Fällen, in denen das Nutzungsverhältnis **beendet** wird, stellt sich jeweils die Frage, was mit den Daten geschehen soll. Die Schwierigkeit in den Fällen des beendeten Nutzungsverhältnisses ist, dass der Cloud-Anbieter grundsätzlich nicht (mehr) verpflichtet ist, Leistungen zu erbringen. Es stellt sich daher die Frage, *ob* auch in diesen Fallgruppen die Datenhoheit gewährleistet werden muss und, wenn ja, *wie* dann die Verfügbarkeit der Daten sicherzustellen ist und vor allem, *wer* sie sicherstellen muss (der Anbieter oder der Nutzer selbst). Dabei ist stets zu bedenken, dass aus schuldrechtlicher Sicht grundsätzlich keine Pflicht des Anbieters mehr besteht, die Daten des Betroffenen weiterhin in der Cloud zu speichern, wenn der Vertrag über die Nutzung der Cloud-Dienste nicht mehr existent ist.

Aus diesem Grund schweigen die Nutzungsbedingungen von Cloud-Angeboten in der Regel auf die Frage, was nach Beendigung des Nutzungsverhältnisses mit den Daten geschieht. Exemplarisch sei hier auf die Nutzungsbedingungen der »Amazon Cloud Drive« verwiesen.[230] Diese enthalten unter Nr. 5.1 für den Fall der anbieterseitigen Kündigung des Nutzungsverhältnisses lediglich den Hinweis, dass der jeweilige Nutzer »möglicherweise« nicht mehr auf seine Daten zugreifen kann. Eine Präzisierung dieser schwammig formulierten Klausel fehlt in den Nutzungsbedingungen. Da der Cloud-Anbieter kein Interesse daran hat, seine Kapazitäten ohne Gegenleistung weiter zur Verfügung zu stellen, dürfte ein Löschen der Daten die wahrscheinlichste Folge der Beendigung des Nutzungsverhältnisses sein. Für die sonstigen Fälle der Vertragsbeendigung fehlt jegliche Regelung in den Nutzungsbedingungen. Ein Verlust der Daten ist auch hier wahrscheinlich.

Lösungsmöglichkeiten

Es wäre jedoch mit dem Grundrecht des Datenhoheitsträgers aus Art. 2 Abs. 1 GG unvereinbar, wenn seine Daten allein aufgrund des beendeten Nutzungsverhältnisses unwiederbringlich verlorengingen. Es muss daher eine für Cloud-Anbieter und Cloud-Nutzer gleichermaßen angemessene Lösung für den Erhalt der Datenhoheit gefunden werden.

In Betracht kommt zunächst ein anbieterseitiges Löschen der Daten. Das ist aus Sicht des Trägers der Datenhoheit ein denkbar unbilliges Ergebnis, weil seine Daten dann verloren gehen und er unweigerlich seine Datenhoheit verliert. Des Weiteren könnte der Cloud-Anbieter den Zugriff auf die in der Cloud gelagerten Daten sperren bzw. den Zugang des Nutzers sperren. Auch dies widerstrebt der Datenhoheit, da die jederzeitige Verfügbarkeit der Daten beeinträchtigt wird. Wird die Sperre dauerhaft ausgeführt, so wirkt sie im Ergebnis ebenso intensiv wie eine Löschung. Außerdem könnte der Cloud-Anbieter einen **Transfer der Daten** in eine andere Cloud vornehmen. Das hätte für ihn den Vorteil, dass Kapazitäten in seiner Cloud frei würden. Für den Cloud-Nutzer hätte diese Vorgehensweise den Vorteil, dass er weiterhin auf seine Daten zugreifen könnte, wenn der ursprüngliche

---

[229] Vgl. Nr. 9 der AGB von Web.de Freemail, abrufbar unter www.agb.web.de/WEB.DE/AGB/20120801/#7/ sowie den Punkt »Gewährleistung und Haftungsausschluss« der Nutzungsbedingungen von Google Mail, abrufbar unter www.google.de/intl/de/policies/terms/regional.html/.

[230] www.amazon.de/gp/feature.html/ref=sa_menu_acd_lrn1?ie=UTF8&docId=1000655923/.

Anbieter ihm die Zugangsdaten mitteilt. Dieses Vorgehen wirft jedoch sowohl die Frage nach der Kostentragung als auch nach dem organisatorischen Aufwand auf. Schließlich könnte der Anbieter dem Nutzer eine **Frist** einräumen, innerhalb derer der Nutzer seine Daten aus der Cloud herunterladen und anderweitig speichern kann. Auf diese Weise hätte es der Cloud-Nutzer selbst in der Hand, seine Datenhoheit zu sichern. Aufwand und Kosten dürften zu vernachlässigen sein. Dadurch erscheint diese Lösung auch für den Cloud-Anbieter vorzugswürdig, auch wenn damit die schwierigen technischen Aspekte der Standardisierung und Interoperabilität verbunden sind. Problematisch ist aber, dass diese Lösung für den Anbieter unter Umständen eine überobligatorische Pflicht beinhaltet. Eine solche Verpflichtung wird er sich im Zweifel nicht selbst durch seine SLA auferlegen.

AGB-rechtliche Abbildung?

Fraglich ist, wie diese Erwägungen rechtsdogmatisch Eingang in das zwischen Cloud-Anbieter und Cloud-Nutzer bestehende Nutzungsverhältnis finden können. Denkbar wäre zunächst, eine Klauselkontrolle der SLA anhand der §§ 305 ff. BGB vorzunehmen. Das setzt gem. § 305 Abs. 1 Satz 1 BGB voraus, dass die SLAs vorformulierte Vertragsbedingungen sind. Dies ist im **Bürger-Unternehmer-Verhältnis** anzunehmen.

Weniger eindeutig ist die Frage im **Bürger-Staat-Verhältnis** zu beantworten. Wenn der Staat in hoheitlicher Form handelt, ist nicht davon auszugehen, dass er mit dem Bürger ein Vertragsverhältnis eingeht. Demnach scheiden Vertragsbedingungen in dem genannten Sinne aus, sodass die §§ 305 ff. BGB insoweit unanwendbar sind.

Zudem ist zu berücksichtigen, dass das Recht der allgemeinen Geschäftsbedingungen infolge einer Inhaltskontrolle als Rechtsfolge nur die Unwirksamkeit bzw. Nichteinbeziehung einer Klausel in das Vertragsverhältnis vorsieht (vgl. § 305c Abs. 1, § 306 Abs. 1, § 307 Abs. 1 Satz 1, § 308 Hs. 1, § 309 Hs. 2 BGB). Der anbieterseitige Datentransfer in die Cloud eines Drittanbieters und die Ermöglichung der Datensicherung durch den Datenbetroffenen verlangen dem Cloud-Anbieter aber eine überobligatorische Leistung ab. Da dies weder mit der Unwirksamkeit noch mit der Nichteinbeziehung einer Klausel gleichzusetzen ist, scheidet die Inhaltskontrolle gem. §§ 305 ff. BGB zur dogmatischen Umsetzung der Pflicht, einen Datentransfer zu ermöglichen, aus.

Insofern besteht eine Schutzlücke, bei der man sich fragt, wie sie zu schließen ist. Einerseits kann man darüber nachdenken, ob hier der Gesetzgeber tätig werden und – im Rahmen der ggf. sachgerechten Regulierung bestimmter Cloud-Dienste (5.2) – eine Regelung treffen muss. Andererseits käme eine verfassungskonforme Auslegung der Nutzungsbedingungen anhand von Art. 2 Abs. 1 GG in Betracht. Eine solche ist nur dann möglich, wenn bzgl. der Verfahrensweise mit den Daten nach Beendigung des Vertrags keine Regelung (dann kommt eine ergänzende **verfassungskonforme Auslegung** in Betracht) oder nur eine auslegungsbedürftige Regelung getroffen worden ist. Liegt hingegen eine eindeutige Regelung in den SLA vor, die auf eine Löschung oder dauerhafte Sperrung der Daten hinausläuft, besteht tatsächlich eine Schutzlücke, die nur der Gesetzgeber schließen kann.

Aber auch dann, wenn das Nutzungsverhältnis nicht beendet ist, kann es vorkommen, dass der Anbieter eines Cloud-Service nicht verpflichtet ist, dem Nutzer weiterhin den Dienst anzubieten. Wenn der Datenbetroffene beispielsweise mit Zahlungen in Verzug gerät, steht dem Anbieter zunächst ein Zurückbehaltungsrecht aus § 273 BGB (gegebenenfalls analog) zu. Er muss seine Dienste somit nicht weiter anbieten, solange der Nutzer nicht seinen (Zahlungs-)Verpflichtungen nachkommt. Dies ist aufgrund der Interessen des Anbieters durchaus gerechtfertigt. Es ist kein Grund ersichtlich, warum dies nicht zulässig sein sollte.

Sobald der Cloud-Nutzer seinen Verpflichtungen aber wieder nachkommt, muss ihm der Zugang zur Cloud jedoch vor dem Hintergrund von Art. 2 Abs. 1 GG unverzüglich wieder eröffnet werden.

5.3.1.2 Langzeitverfügbarkeit

Die immer größere Anzahl verfügbarer elektronischer Dokumente und Urkunden erfordert eine entsprechende Archivierung, die diese Dokumente langfristig zur Verfügung stellt. Damit steht in Zusammenhang, dass die elektronischen Dokumente nach gesetzlichen Vorgaben revisionssicher, unverändert, vollständig wiederherstellbar und wiederauffindbar archiviert werden müssen. Dabei sind Aufbewahrungsfristen, wie sie der Gesetzgeber vorgesehen hat, zu beachten. Schon 2006 wurde eine erste Realisierung eines elektronischen Langzeitarchivs mit rechtssicherer Ablage von Dokumenten pilotiert. Das Projekt »ArchiSafe«[231] ist ein Praxisbeispiel, das im Rahmen der eGovernment-Initiative BundOnline mit der Physikalisch-Technischen Bundesanstalt realisiert wurde.

Durch die Umsetzung elektronischer Geschäftsprozesse, auch in der Verwaltung, unterliegen die elektronisch erzeugten Dokumente dem Erfordernis langfristiger Aufbewahrung, die sich aus der Anforderung der Aktenmäßigkeit des Verwaltungshandelns ergibt.

Die **Beweiskraft elektronischer Dokumente** muss nachhaltig rechtswirksam bleiben und wird durch elektronische Signaturen technologisch unterstützt. Durch die Verwendung elektronischer Signaturen ist die Integrität, Authentizität und eine beweissichere Unterschrift mit Zeitstempelfunktion gewährleistet. Darüber hinaus muss die Möglichkeit der Erhaltung der Beweiskraft durch Signaturerneuerung einbezogen werden. Mit kryptografischen Diensten wird die Erstellung und Verifikation elektronischer Signaturen unterstützt, die ebenfalls im Rahmen der BundOnline Initiative geförderten Projekts »ArchiSig«[232] pilotiert wurden. Darauf aufbauend hat das Bundesamt für Sicherheit in der Informationstechnik technische Richtlinien für die vertrauenswürdige elektronische Langzeitarchivierung erstellt[233]. Für die sichere Übermittlung, Speicherung und Archivierung der elektronischen Dokumente wird neben der elektronischen Signatur Verschlüsselungstechnologie verwendet.

Eine wesentliche Voraussetzung für die Archivierung von Dokumenten ist die **Unterstützung verschiedener Dokumentenformate.** Darüber hinaus muss sichergestellt werden, dass abhängig von der Aufbewahrungsfrist Dokumente gelöscht werden. Werden Dokumente in verwaltungsinterne Fachverfahren eingebunden, so müssen sie nach dessen Gebrauch automatisch gelöscht werden. In diesem Fall kann der Bürger sicher sein, dass seine Dokumente/Urkunden nur einmal im Langzeitarchiv existieren und die erzeugte Kopie nach Benutzung gelöscht wird.

Die Akzeptanz elektronischer Signaturen ist bei Bürgern wenig verbreitet, obwohl der neue Personalauswies diese Funktion optional zur Verfügung stellt. Da nicht alle Dokumente/Urkunden denselben Sicherheitsanforderungen genügen müssen, kann ein Dokument auch ohne elektronische Signatur bspw. in einem elektronischen Safe abgelegt werden. We-

---

231 Bundesministerium für Wirtschaft, Praxisbeispiel »Langzeitspeicherung mit ArchiSafe«, V. 1.1, 2006.

232 ArchiSig-Konzepte wurden am Universitätsklinikum Heidelberg und am Informatikzentrum Niedersachsen entwickelt und beschäftigen sich mit mathematischen Verfahren der Signaturerneuerung mit Hilfe von Hash-Bäumen und Zeitstempeln.

233 TR-03125.

sentlich ist dabei, dass der Gesetzgeber verschiedene Sicherheitslevel für elektronische Dokumente vorgibt, sodass auch elektronische Dokumente ohne Zertifikat (elektronische Signatur) anerkannt werden.

5.3.1.3 Ausfallsicherheit

Um jederzeit und von jedem Ort Zugriff auf die Daten zu haben, muss der Cloud-Anbieter dies technisch-organisatorisch durch Ausfallsicherheit realisieren. Ausfallsicherheit ist eine der Eigenschaften mit der gerade Cloud-Anbieter werben. Elastizität der Zugriffe und skalierbare Anwendungen sind wesentliche Eigenschaften des Cloud-Computings. Durch die Bereitstellung einer sehr großen Anzahl von Servern (Serverfarmen) und durch Virtualisierung können unendlich viele Ressourcen hochverfügbar bereitgestellt und bei Last entsprechend verteilt werden. Davon bekommt in der Regel der Kunde nichts mit.

Voraussetzung für eine redundante Bereitstellung der Daten sind standardisierte Dienste, die den hoch-verfügbaren Zugriff ermöglichen. Diese Dienste müssen bei Bedarf in einer anderen virtuellen Umgebung aufgesetzt werden können. Dies erfordert die Einhaltung standardisierter Schnittstellen, sodass Anwendungen auch bei verschiedenen Cloud-Anbietern, falls die eigenen Ressourcen nicht ausreichen, betrieben werden können. Die Standards unterstützen darüber hinaus die Portabilität, sodass auch der Nutzer jederzeit die Daten von einem Anbieter zu einem anderen übertragen kann. In diesem Fall hat der Ausfall eines Systems keine Auswirkung auf die Verfügbarkeit der Anwendung bzw. des Dienstes.

Kritisch wird es, wenn der Kunde an gesetzliche Rahmenbedingungen gebunden ist, die bspw. eine Speicherung der Daten außerhalb des Landes nicht erlauben. In diesem Fall muss der Cloud-Anbieter seinen Kunden informieren, damit er die Möglichkeit hat, ggf. unter diesen Rahmenbedingungen eine andere Lösung bzw. einen anderen Cloud-Anbieter zu finden. In jedem Fall ist es vertraglich abzusichern, wenn der Cloud-Anbieter einen Unterauftragnehmer zur Erbringung seiner Leistung hinzuzieht. Die rechtlichen Anforderungen bezüglich des Datenschutzes müssen an den Unterauftragnehmer weitergeleitet werden und der Kunde ist davon in Kenntnis zu setzen. Dabei ist besonders zu beachten, dass ggf. die Daten nur ortsgebunden gespeichert werden dürfen, der Cloud-Anbieter muss dies ebenfalls berücksichtigen.

Darüber hinaus ist ein wesentlicher Aspekt der Ausfallsicherheit auch der Schutz vor Angriffen, den ein Cloud-Anbieter garantieren muss. Dazu wird der Cloud-Anbieter, auch in eigenem Interesse, entsprechende Sicherheitsmechanismen einsetzen, die auch schon heute in jedem Datenzentren betrieben werden, um potentielle Angriffe möglichst schnell in den Griff zu bekommen.

5.3.2 Verfügungsbefugnis

Die Verfügungs*befugnis* ist – wie der Begriff zeigt – primär rechtlich zu erfassen. Dabei bestehen enge Verbindungen zur Sicherstellung der Vertraulichkeit, da jede Verfügung, die eine entsprechende Verfügungsbefugnis voraussetzt, auch die Vertraulichkeit beeinträchtigen kann. Dennoch lassen sich Fallgruppen extrahieren, in denen das Element der Verfügungsbefugnis nicht deckungsgleich mit dem Aspekt der Vertraulichkeit ist. Dies betrifft:

- Zugriffe (vor allem des Anbieters), die nicht auf die inhaltliche Kenntnisnahme der Daten gerichtet sind (also die Vertraulichkeit unberührt lassen). Denkbar ist dies bspw. in Form des **Löschens und Sperrens der Daten**, was in enger Verbindung

zur Forderung der (dauerhaften) Verfügbarkeit steht (5.3.1), sowie in Form des **Speicherns**, welches ebenfalls eine datenschutzrechtlich relevante Handlung darstellt (vgl. § 3 Abs. 4 BDSG).

- Den **Umgang von Dritten mit »fremden« personenbezogenen Daten** und hier konkret die Frage, ob eine Verlagerung in Cloud-Anwendungen in Betracht kommt. Liegt die Datenhoheit weiterhin beim Betroffenen, gibt es eine geteilte Datenhoheit oder wird diese letztlich nur durch die datenhaltende Stelle ausgeübt? **Verfügungsbefugnis** (verstanden als Recht über den Speicherort zu entscheiden) und Datenhoheit (des Betroffenen) können daher auseinanderfallen.
- Und schließlich die etwas exotische Fragestellung, wem die Verfügungsbefugnis im Falle des **Versterbens des Datenbetroffenen** zukommt?

Ausgangspunkt: Verfügungsbefugnis des Datenbetroffenen

Unter dem Begriff »Verfügungsbefugnis« wird in der Rechtswissenschaft herkömmlicherweise die zuvörderst dem Eigentümer zustehende Befugnis verstanden, das Eigentum an einer Sache auf eine andere Person zu übertragen.[234] Hier ist mit der Verfügungsbefugnis (oder auch Verfügungsmacht) jedoch etwas anderes gemeint, da es sich bei Daten nicht um Eigentum in diesem Sine handelt und die Daten nicht übertragen werden sollen. »Verfügungsmacht« soll vielmehr so verstanden werden, dass es der Datenbetroffene allein in der Hand haben muss, was mit den seine Person betreffenden Daten geschieht. Diese Macht ist eine allumfassende. Es ist allein die Entscheidung des Datenbetroffenen, ob bzw. bei wem welche Daten gespeichert werden dürfen, ob die Daten verarbeitet werden dürfen bzw. wer die Daten verarbeiten darf und schließlich ob bzw. wann und in welchem Umfang Daten gelöscht werden dürfen.

Ausgehend von den Begriffsbestimmungen in § 3 Abs. 4 BDSG müssen die einzelnen Datenverarbeitungsvorgänge isoliert betrachtet werden – also das Speichern, Verändern, Übermitteln, Sperren und Löschen. Jeder Vorgang ist jeweils vom Datenbetroffenen zu legitimieren (soweit keine anderweitige gesetzliche Gestattung vorliegt). Sinn und Zweck eines Cloud-Vertrages sprechen dafür, dass das **Speichern** der Daten in der Cloud dem Provider ohne weiteres gestattet ist. Jeder anderweitige Zugriff auf die Daten (vor allem das **Verändern** bzw. die **inhaltliche Kenntnisnahme**) durch den Provider ist jedoch rechtfertigungsbedürftig und bedarf einer Legitimation durch den Träger der Datenhoheit. Letztlich muss er darüber entscheiden können, ob seine personenbezogenen Daten vom Provider oder gar Dritten verarbeitet werden dürfen oder nicht.

Es werden insoweit zwei Schutzrichtungen verbürgt. Einerseits ist es dem Datenbetroffenen in negativer Hinsicht zugesichert, dass er Zugriffe durch den Provider und Dritte untersagen darf. Andererseits wird in positiver Hinsicht gewährleistet, dass der Anbieter eines Cloud-Service den Vorgaben des Datenbetroffenen nachkommen muss. Die Freigabe der Daten an Dritte und die Verarbeitung der Daten durch den Provider oder Dritte unterliegt der alleinigen Weisung des Datenbetroffenen.

Auch das **Löschen** der Daten unterliegt allein dem Willen des Datenhoheitsträgers. Aus dem Recht auf Vergessenwerden gem. Art. 17 des Entwurfs der Europäischen Kommission für eine Europäische Datenschutz-Grundverordnung vom 25. 01. 2012 folgt, dass der Datenbetroffene jemanden, der seine Daten inne hat, verbindlich dazu veranlassen kann, alle ihn be-

[234] Oechsler, in: Münchener Kommentar zum BGB, Band 6, 5. Aufl. 2009, § 929 Rn. 43.

treffenden Daten zu löschen und deren weitere Verbreitung zu verhindern. Diesem Wunsch muss der Inhaber der Daten entsprechen und zwar vollumfänglich. Es genügt demnach nicht, einem Lösungswunsch des Datenbetroffenen in der Weise nachzukommen, dass die Daten (etwa Profilfotos in einem sozialen Netzwerk) für Dritte nicht mehr sichtbar sind (quasi ausgeblendet werden), diese aber gleichwohl beim Provider gespeichert bleiben. Vielmehr müssen die Daten auf Wunsch des jeweiligen Betroffenen in der Weise gelöscht werden, dass sie niemandem – auch nicht dem Anbieter – mehr zugänglich sind.

Auseinanderfallen von Verfügungsbefugnis und Datenhoheit

In Fällen, in denen nicht der originär Verfügungsberechtigte (der Träger der Datenhoheit) Daten in eine Cloud einstellt – die in eigener Entscheidung auch eine »unsichere« sein kann –, sondern wenn ein Dritter mit diesen personenbezogenen Daten umgeht, kann es zu einem **Auseinanderfallen von Datenhoheit und Verfügungsbefugnis** kommen:

- Die Berechtigung des Dritten, mit den Daten des Betroffenen umzugehen, ist immer nur eine **abgeleitete**, ihm kommt keinesfalls eine umfassende Datenhoheit hinsichtlich fremder Daten zu. Lediglich **ein Teil der** – grundsätzlich beim Datenbetroffenen verbleibenden – **Verfügungsbefugnis** wird transferiert. Damit dies nicht grenzenlos erfolgen kann, greifen die Schutzmechanismen der Auftragsdatenverarbeitung.
- Insofern stellen die Vorgaben zur Auftragsdatenverarbeitung gerade das **Fortbestehen der Verfügungsbefugnis beim Datenbetroffenen** sicher. Er kann seine datenbezogenen Rechte nämlich weiterhin von seinem Vertragspartner (Auftraggeber) einfordern; dieser muss sich vertraglich gegenüber seinen Auftragnehmern entsprechende Ingerenzrechte gesichert haben. Um »Anweisungen« des Datenbetroffenen, bspw. auf Löschung, gegenüber seinen Auftragnehmern durchsetzen zu können, müssen ihm gerade die die Verfügungsbefugnis kennzeichnenden Rechte zukommen.

Dem Umstand, dass sich der Betroffene gegenüber dem Anbieter nur auf einen mittelbaren Schutz berufen kann, wird also durch staatliche Maßnahmen begegnet, mit denen dieser der Schutz- und objektiven Gewährleistungsfunktion der Grundrechte nachkommt. Grundsätzlich ist dem Dritten, der mit »fremden« personenbezogenen Daten umgeht, nämlich die Weitergabe dieser Daten untersagt. In Betracht kommt lediglich eine Einwilligung (als Form der Ausübung der eigenen Verfügungsbefugnis des Datenbetroffenen), das Vorliegen der Voraussetzungen einer Auftragsdatenverarbeitung oder einer zulässigen Datenübermittlung. Kommt es bei der Nutzung Cloud-basierter Dienste zur Verarbeitung personenbezogener Daten, ist im Regelfall aber von einer Auftragsdatenverarbeitung i. S. d. § 11 BDSG auszugehen. Der **Auftraggeber bleibt datenschutzrechtlich verantwortlich**; er ist gem. § 11 Abs. 2 Satz 1 und 4 BDSG zur sorgfältigen Auswahl und Überwachung des Anbieters verpflichtet. Verarbeitungsprozesse des Auftragnehmers, technische und organisatorische Maßnahmen sowie etwaige Unterauftragsverhältnisse sind detailliert festzulegen.[235]

Gerade durch die exzessive Nutzung derartiger Unterauftragsverhältnisse treten Gefahren für den Schutz der personenbezogenen Daten ein – sie ist aber gerade für eine öffentliche Cloud prägend. Hinzu kommt, dass personenbezogene Daten nicht ohne Weiteres in Drittstaaten außerhalb der Europäischen Union übermittelt werden dürfen. Aber auch in Bereichen, wo personenbezogene Daten von den Verarbeitungsprozessen betroffen sind, erscheint eine Nutzung von Cloud-Angeboten nicht von vornherein ausgeschlossen. Das **Wechselverhältnis zwischen Technik und Recht** muss jeweils unter Berücksichtigung

---

[235] Simitis/Walz (Fn. 84), § 11 Rn. 50 ff.; s. auch Pohle/Ammann, CR 2009, 273 (276).

der Funktionsweise der eingesetzten Technologien betrachtet werden. So existieren mittlerweile **Verschlüsselungssysteme** und elektronische Daten- und Dokumentensafes, bei denen der Personenbezug vollständig aufgehoben werden kann – mit der Folge, dass auch ein Transfer in »unsichere« Drittstaaten bzw. auf dortige Server unproblematisch ist. Als Beispiel kann ein Produkt der trustedSafe GmbH, eines Spin-offs des Fraunhofer Instituts FOKUS, dienen.[236]

Der trustedSafe ist ein elektronischer Speicherplatz für die Ablage, die Verwaltung und den Austausch von Daten mit hohen Sicherheitsanforderungen. Grundkonzept sind die Verschlüsselung und Zerteilung der Daten im Client (also auf dem Endgerät des Nutzers) sowie die Speicherung der Daten bzw. von »Datenteilen« außerhalb des eigenen Endgeräts bei *verschiedenen* Providern. Dadurch wird eine höhere Datensicherheit und ein höherer Datenschutz erreicht als bei der herkömmlichen Speicherung bei *einem* Storage Provider oder auf dem eigenen Endgerät. Die rechtliche Analyse der Datenschutzkonformität eines solchen Systems muss die technische Funktionsweise, konkret die Auswirkungen der technischen Vorgänge des Verschlüsselns und Zerteilens auf den Personenbezug der verarbeiteten Daten, berücksichtigen. Während die Nutzung anderer Cloud-Dienste also an der weltweiten Verteilung der Daten und den entgegenstehenden strengen Vorgaben an eine Auftragsdatenverarbeitung scheitert, bieten Dienste wie der trustedSafe Abhilfe und können daher selbst im Zusammenhang mit besonders sensiblen Daten zum Einsatz kommen.

Die Kombination zahlreicher Sicherheitsmechanismen führt nicht nur zur Aufhebung des Personenbezugs, sondern bietet darüber hinaus zusätzliche Sicherheit, sodass die vom deutschen Datenschutzrecht formulierten Anforderungen zum Teil »übererfüllt« werden. Entscheidend ist neben den Vorgängen des Verschlüsselns der Dokumente und deren Zerteilung der Umstand, *wo* diese Vorgänge erfolgen – nämlich ausschließlich innerhalb des Clients des Nutzers. Denjenigen Datenteilen, Schlüsseln und Transportcontainern, die dieses System verlassen, fehlt es schon am Personenbezug, sodass dieser Vorgang als datenschutzrechtlich unbedenklich zu bewerten ist. Mit der Verschlüsselung auf dem System des Nutzers findet eine **Aufhebung des Personenbezugs** statt. Es kommt zu einer Anonymisierung, die nur dann nicht ausreichend wäre, den Personenbezug aufzuheben, wenn die Verschlüsselung unter Rückgriff auf öffentlich bekannte Verfahren oder öffentlich verfügbare Schlüssel erfolgt. Wird der notwendige Schlüssel aber bei Installation des Systems initial auf dem Rechner des Nutzers erzeugt und kann auf ihn ausschließlich mithilfe des nur dem Nutzer bekannten Passworts zugegriffen werden, kommt es zu einer Beseitigung des Personenbezugs. Im zweiten Schritt kommt es durch eine Zerteilung der – verschlüsselten – Datei in mehrere Teile nicht nur zu einer (weitergehenden) Aufhebung des Personenbezugs, sondern auch zur **Beseitigung des Aussagegehalts des Dokuments**.

Verfügungsbefugnis nach dem Tod

Interessante rechtliche Fragen stellen sich darüber hinaus im Zusammenhang mit dem Tod des Datenbetroffenen. Insbesondere bedarf einer Klärung, wem die Verfügungsbefugnis über die den Verstorbenen betreffenden, in der Cloud abgelegten, personenbezogenen Daten zusteht. Der Verstorbene scheidet erkennbar als Verfügungsbefugter aus. Zu untersuchen ist, ob die Datenhoheit seinen Erben, dem Cloud-Provider, sonst einem Dritten oder gar niemandem mehr zukommt. Es geht damit um die Frage, wer nach dem Tod die Macht über die in Clouds oder allgemein in Web 2.0-Angeboten abgelegten personenbezogenen Daten des Verstorbenen hat, wer also über sie bestimmen und festlegen darf, was mit ihnen

[236] Weitere Informationen unter www.trustedsafe.de/.

geschieht. Wer »erbt« beispielsweise nach dem Tod eines Nutzers dessen Facebook-Account und die darin enthaltenen personenbezogenen Daten, quasi den »digitalen Nachlass«?[237]

Klar ist zunächst, dass Daten nicht im Sinne des BGB vererbt werden können, wenn sie nicht zugleich vermögensrechtlichen Charakter haben (vgl. § 1922 Abs. 1 BGB). Bei personenbezogenen Daten ohne Vermögenscharakter wird einer Ansicht zufolge danach differenziert, ob diese frei zugänglich sind, etwa im Rahmen eines Blogs, oder nicht, wie es bei zugangsgeschützten Online-Accounts der Fall ist.[238] Die Zugangsdaten zu Online-Accounts sollen aufgrund des postmortalen Persönlichkeitsrechts vom Provider nicht an die Erben des Nutzers herausgegeben werden dürfen, da dieser sich sonst zu Lebzeiten in seiner Persönlichkeitsentfaltung eingeschränkt fühlen könnte. Der Schutz des BDSG solle darum nach dem Tod des Datenbetroffenen fortwirken und eine Preisgabe seiner Daten an die Erben verhindern. Dagegen spricht jedoch ein Vergleich mit der analogen Welt: Auch hier kommt es vor, dass sich in der Erbmasse hochsensible Daten befinden. Diese fallen regelmäßig in die Hände der Erben. Niemand würde auf die Idee kommen, den Erben unter Hinweis auf das postmortale Persönlichkeitsrecht zu verbieten, einen Blick in das Tagebuch des Erblassers zu werfen. Zudem könnten die Erben möglicherweise ein (wirtschaftliches, soziales oder ideelles) Interesse an den in einem Online-Account hinterlegten Daten haben. Bei frei zugänglichen Internetdaten über den Erblasser sollen dessen Erben nach der zuvor zitierten Auffassung die Rechte auf Auskunft, Berichtigung, Löschung und Sperrung aus § 13 Abs. 7, § 12 Abs. 3 TMG i. V. m. §§ 19, 20, 35 BDSG wahrnehmen können.[239] Das ist zwar innerhalb der skizzierten Auffassung wenig konsequent, erscheint vor dem Hintergrund der Tatsache, dass die Erben richtigerweise auch sonst die Verfügungsbefugnis über die personenbezogenen Daten des Erblassers erhalten müssen als richtig.

Die Fragen rund um den »digitalen Nachlass« sind weitgehend ungeklärt, was nicht zuletzt mit fehlenden rechtlichen Regelungen in diesem Bereich und den faktischen Problemen (Welcher Erbe weiß schon von allen Online-Accounts des Erblassers bzw. kennt alle seine Online-Identitäten?) zusammenhängen dürfte.

5.3.3 Identitätsmanagement

Ein wesentlicher Faktor für ein sicheres Identitätsmanagement ist der Authentisierungsprozess und seine Relevanz in Bezug auf Vertrauen.[240] Um Vertrauen in einer Kommunikationsbeziehung herzustellen, ist es notwendig, zu wissen, mit wem man kommuniziert. Der Authentisierungsprozess verifiziert die Authentizität einer Entität (Darstellung einer Person, eines Gegenstands, eines Computerprograms, etc.) und stellt deren »Echtheit« sicher. Identitäts- und Rechteverwaltung ist ein wesentlicher Baustein und dient der Zugangskontrolle in Cloud-Systemen. Neben einer sicheren Identifikation des Kunden selbst muss der Cloud-Anbieter auch sicherstellen, dass die eigenen Administratoren denselben Sicherheitsbedingungen unterliegen, damit sie nicht auf fremde Daten zugreifen können.

---

237 So genannt von Martini, JZ 2012, 1145 ff.

238 Vgl. dazu und zum Folgenden Martini, JZ 2012, 1145 (1147 ff.).

239 Martini, JZ 2012, 1145 (1152 f.).

240 ISO/IEC JTC 1 SC 27/WG 5 »A framework for IdM«.

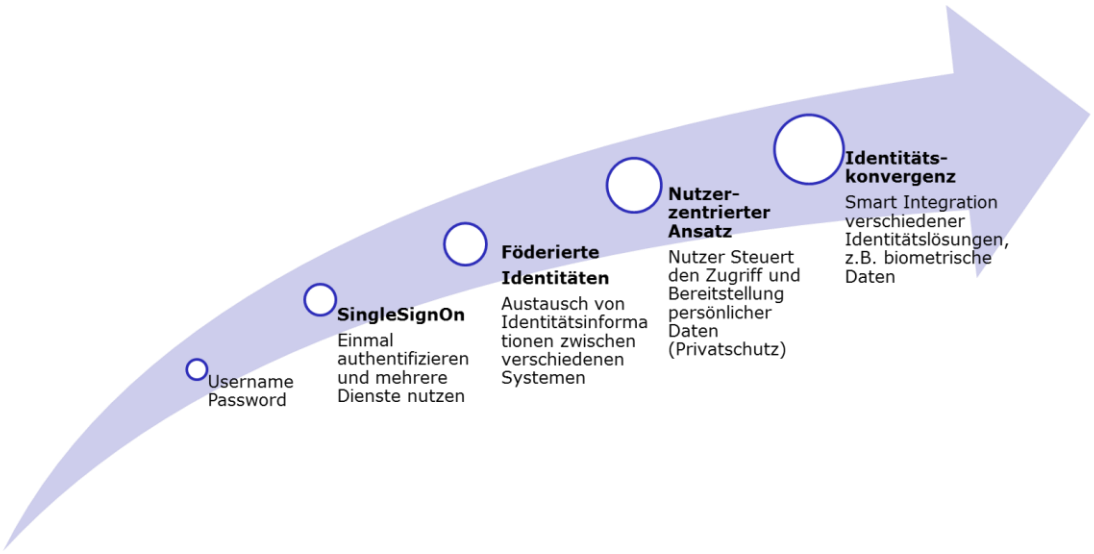

ABBILDUNG 15: EVOLUTION DIGITALER IDENTITÄTEN

Das Identitätsmanagement bietet dem Nutzer die Möglichkeit, seine Identitäten zu verwalten und entsprechende Profile (Teilidentitäten) zusammenzustellen. Für die Teilidentitäten werden Pseudonyme als Identifikatoren verwendet, die sowohl den Umgang mit den Teilidentitäten als auch deren Wiederverwendung[241] erleichtern.

Der Kunde sollte aus Sicherheitsgründen eine Zwei-Faktor-Authentisierung fordern, die ein höheres Sicherheitslevel bietet als Username/Password. Der elektronische Personalausweis bietet hier eine Unterstützung, da er entsprechende Credentials (eID) als Basisfunktion beinhaltet.

Der Cloud-Anbieter muss die Zugriffe auf die Konten der Nutzer protokollieren und den Kunden zur Verfügung stellen, damit der Kunde überprüfen kann, wer auf sein Konto zugegriffen hat.

Um eine Profilbildung seitens des Cloud-Anbieters zu vermeiden, sollte der Kunde darauf bestehen, dass Pseudonyme verwendet werden können.

5.3.4 Vertraulichkeit

Die Vertraulichkeit der in der Cloud mit Freigabemöglichkeit gelagerten Daten wird nach der herrschenden Meinung von Art. 10 GG gewährleistet, weil die Daten durch die Möglichkeit der Freigabe eine Nachrichtenähnlichkeit erhalten. Fehlt eine Freigabemöglichkeit, so ist der Schutzbereich der informationellen Selbstbestimmung eröffnet. Demgegenüber sollte vorzugswürdig zwischen System- und Inhalts- bzw. Datenschutz differenziert werden, sodass der Schutz der in der Cloud gespeicherten Daten stets aus dem Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 GG zu entnehmen wäre (3.2.3.2).

Die Absicherung der Vertraulichkeit der in der Cloud gelagerten Daten muss aus drei denkbaren Richtungen erfolgen, aus denen ein Zugriff auf diese Daten erfolgen kann, obwohl der Datenbetroffene nicht damit einverstanden ist. Hinsichtlich der **Zugriffe staatlicher Stellen** kann weitgehend auf die Ausführungen zum Rechtsrahmen verwiesen werden (3.2.3), da

[241] Einführungstutorium Datenschutz- und Identitätsmanagement www.prime-project.eu/tutorials/gpto/.

sich die verfassungsrechtlichen Schutzpositionen aus Art. 10 und Art. 2 Abs. 1 GG primär gegen staatliche Zugriffe wenden. Sollten Zugriffe des Safeanbieters auf die gespeicherten Daten nicht vollständig – z. B. durch eine Verschlüsselung und Aufteilung in Datenteile– ausgeschlossen sein, erscheint es einfachgesetzlich vorzugswürdig, die staatlichen Zugriffsrechte abschließend, normklar und bereichsspezifisch im Rahmen der erforderlichen Regulierung von sicheren Cloud-Angeboten zu normieren, da ansonsten das allgemeine Regime des Strafverfolgungs- und Gefahrenabwehrrechts zur Anwendung gelangt,[242] welches weit weniger geeignet ist, die besondere Schutzbedürftigkeit elektronischer Safes abzubilden.

Hinsichtlich der **Zugriffe des Providers** ist – wie bereits ausgeführt – zwischen den Zugriffsformen zu unterscheiden; das Speichern ist seine originäre vertragliche Aufgabe, das Löschen und Sperren ggf. dem Element der Verfügbarkeit zuzuordnen, sodass vor allem eine **inhaltliche Kenntnisnahme** zu betrachten bleibt.

Bei der »Abwehr« von Zugriffen Dritter dürften vor allem technische Maßnahmen im Vordergrund stehen, die einerseits vor externen Zugriffen schützen, andererseits sicherstellen, dass im Rahmen von Freigabefunktionen wirklich nur Berechtigte zugreifen.

5.3.4.1 Gegenüber (unberechtigten) Zugriffen Dritter

Der Vertraulichkeitsschutz bezüglich der vom Bürger in eine Cloud-Anwendung eingebrachten personenbezogenen Daten folgt aus verfassungsrechtlicher Sicht aus Art. 2 Abs. 1 GG. Weitergehend stellt sich die Frage, wie dieser Aspekt der Datenhoheit in der Praxis abgesichert werden kann. Das Recht auf informationelle Selbstbestimmung gewährleistet die Befugnis des jeweiligen Grundrechtsträgers, selbst über die Veröffentlichung und Verwendung seiner personenbezogenen Daten zu bestimmen. Daraus folgt, dass nur er festlegen darf, wer auf seine in der Cloud gelagerten Daten zugreifen darf. Die Absicherung dieses Selbstbestimmungsrechts und der daraus abgeleiteten Befugnis kann zum einen rechtlich, zum anderen technisch-tatsächlich erfolgen.

5.3.4.1.1 Tatsächliche Maßnahmen

Cloud-Anbieter, die ein Identitätsmanagement anbieten bzw. einen Drittanbieter einbeziehen, schützen die Privatsphäre der Kunden. Darüber hinaus sind IT-Sicherheitsmaßnahmen erforderlich, die Sicherheitslücken schnell und effizient aufdecken und beseitigen. Diese IT-Sicherheitsmaßnahmen sind nicht cloud-spezifisch, sondern gelten allgemein im Rahmen der IT-Sicherheit. So können Cloud-Anbieter mit einer ISO 27001-Zertifizierung zumindest auf Basis der IT-Sicherheit ein vertrauenswürdiges Zertifikat erwerben und sich von anderen, nicht-zertifizierten Cloud-Anbietern, unterscheiden.

In Zukunft wird das nachweisbare Löschen erforderlich sein, also die physische Zerstörung personenbezogener Informationen, um eine weitere Verarbeitung zu verhindern. Wie Cloud-Anbieter das realisieren, bleibt derzeit noch offen; auch ein rechtlicher Anspruch auf auf "Vergessen im Internet"[243] bleibt in seinem Gehalt vage.

Durch Anonymisierung kann der Kunde selbst seine personenbezogenen Daten vor einer Profilierung seitens des Cloud-Anbieters schützen, da er selbst die Identitätsattribute anonymisiert und diese vom Cloud-Anbieter nicht zusammengeführt werden können. Der An-

---

[242] Schulz/Hoffmann, CR 2010, 131 ff.

[243] Vgl. zu entsprechenden Überlegungen im Rahmen der EU-Datenschutzgrundverordnung Hornung/Hofmann, JZ 2013, 163 ff.; Koreng/Feldmann, ZD 2012, 311 ff.; Kalabis/Selzer, DuD 2012, 670 ff.

bieter muss allerdings einen entsprechenden Dienst zur Verfügung stellen, beispielsweise einen Identitätsmixer (Idemix von IBM[244]), der es ermöglicht, persönliche Daten so zu anonymisieren, dass der Anwender sich sicher digital zertifizieren kann, ohne jedoch seine Identität preiszugeben.

5.3.4.1.2 Rechtliche Maßnahmen

Neben diesen technischen Möglichkeiten existiert aber auch eine rechtliche Handhabe zur Absicherung der Vertraulichkeit gegenüber unberechtigten Zugriffen Dritter.

Vertragliche Verpflichtung des Cloud-Providers

In Betracht kommt zunächst, dass der Anbieter von Cloud-Anwendungen vertraglich ausdrücklich dazu verpflichtet wird, sicherzustellen, dass der Nutzer allein Zugriff auf seine Daten in der Cloud hat. Hat die Cloud eine Freigabefunktion, muss er es allein in der Hand haben, die berechtigten Dritten festzulegen. Das Interesse des Cloud-Anbieters, eine derartige Verpflichtung freiwillig einzugehen, dürfte angesichts der Haftungsrisiken gering sein. Insofern ist es auch nicht weiter verwunderlich, dass die Anbieter von Cloud-Services in der Regel keine Verpflichtung eingehen, die Datenvertraulichkeit zu gewährleisten.[245] Dabei stellt sich allerdings die Frage, wie der Nutzer einer Cloud-Anwendung geeignete Maßnahmen ergreifen soll, um die Vertraulichkeit seiner Daten sicherzustellen. Denn technische Maßnahmen wird er kaum ergreifen können, weil er an die technischen Vorgaben der Software gebunden ist und er diese nicht verändern kann. Schon vor diesem Hintergrund dürfte es gerechtfertigt sein, die Ergreifung von geeigneten Maßnahmen zur Absicherung der Datenvertraulichkeit als Angelegenheit des Cloud-Anbieters zu erachten. Er sollte selbst dafür Sorge tragen müssen, dass sich unbefugte Dritte den Zugang zur Cloud und den darin enthaltenen Daten nicht erschleichen können.

Vor diesem Hintergrund ist zu untersuchen, ob die entsprechenden Klauseln in den Nutzungsbedingungen der Cloud-Anbieter AGB-rechtlich zu beanstanden sind. In Betracht kommt die **Unwirksamkeit nach § 307 Abs. 2 Nr. 2 BGB**. Das wäre der Fall, wenn die Bestimmung wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrages ergeben, so einschränkt, dass die Erreichung des Vertragszwecks gefährdet ist. Dabei muss es um Hauptpflichten (Kardinalpflichten) des jeweiligen Vertrags gehen.[246] Da dies von Vertrag zu Vertrag verschieden ist, bedarf es zunächst einer Untersuchung, was für ein Vertragstyp vorliegt, wenn ein Vertrag über die Nutzung einer Cloud-Anwendung geschlossen wird. Daraus lassen sich dann in einem zweiten Schritt die vom Anbieter zu erfüllenden Kardinalpflichten ableiten.

Rechtsnatur eines »Cloud-Vertrags«

Nach Auffassung des Bundesgerichtshofs ist die Zurverfügungstellung von Speicherkapazitäten auf dem Server des Anbieters zur Speicherung von Daten mietvertraglich zu qualifizieren.[247] Demzufolge ist die Zurverfügungstellung von Speicherplatz in einer Cloud-

---

[244] Pressemitteilung 2007, IBM stellt eine neue Software vor, die es Internetanwendern erlaubt, ihre persönlichen Informationen bei Online-Transaktionen besser zu schützen und so Datenmissbrauch und Identitätsdiebstahl vorzubeugen.

[245] Vgl. nur Nr. 3.1 Satz 3 der Amazon Cloud Drive Nutzungsbedingungen, www.amazon.de/gp/feature.html/ref=sa_menu_acd_lrn1?ie=UTF8&docId=1000655923/.

[246] Wurmnest, in: Münchener Kommentar zum BGB, Band 2, 6. Aufl. 2012, § 307 Rn. 70.

[247] BGH, NJW-RR 1993, 178; NJW 2007, 2394 (2395).

Anwendung grundsätzlich ebenfalls als **Mietvertrag** anzusehen. Dies wird in der Literatur mit dem Argument befürwortet, dass die Interessenlage mit der Nutzung eines real existierenden Schließfachs oder der Überlassung von Speicherplatz auf einem Großrechner in einem Rechenzentrum vergleichbar sei.[248] Diese Einordnung ist aber nur dann als richtig anzusehen, wenn der Nutzungsvertrag eine irgendwie geartete **Entgeltpflicht** des Nutzers vorsieht (vgl. § 535 Abs. 2 BGB). Sofern dies der Fall ist, gilt bzgl. der Überlassung von Speicherplatz in einer Cloud das mietvertragliche Pflichtenprogramm der Vertragsparteien. Der Vermieter ist gem. § 535 Abs. 1 Satz 2 BGB dazu verpflichtet, dem Mieter die vermietete Sache in einem zum vertragsmäßigen Gebrauch geeigneten Zustand zu überlassen und sie während der Mietzeit in diesem Zustand zu erhalten.[249] Der zum vertragsgemäßen Gebrauch geeignete Zustand in diesem Sinne liegt aber nur dann vor, wenn der Mieter die Mietsache **frei von Störungen durch Dritte** nutzen kann. Insofern besteht eine Pflicht des Vermieters, Störungen von dritter Seite abzuwehren.[250] Übertragen auf den Nutzungsvertrag über Speicherplatz in einer Cloud bedeutet dies, dass der Cloud-Provider dazu verpflichtet ist, dafür zu sorgen, dass unbefugte Dritte nicht auf die in der Cloud gespeicherten Daten der Nutzer zugreifen können. Diese Pflicht des Providers stellt auch eine **Hauptpflicht** dar. Enthalten die Nutzungsbedingungen eine Klausel, wonach der Cloud-Anbieter von einer entsprechenden Verpflichtung freigestellt und die Gewährleistung der Datenvertraulichkeit auf den Nutzer abgewälzt wird, so ist eine wesentliche Pflicht des Anbieters eingeschränkt. Dies gefährdet den Vertragszweck, weil der Nutzer – gerade vor dem Hintergrund der Entgeltlichkeit – erwarten kann, dass seine Daten seitens des Anbieters vor unbefugtem Zugriff Dritter gesichert werden. Folglich sind vergleichbare Klauseln gem. § 307 Abs. 2 Nr. 2 BGB unwirksam. Entsprechende individualvertragliche Klauseln sind hingegen gem. § 138 Abs. 1 BGB unwirksam, weil sie gegen die guten Sitten verstoßen.[251]

Wird der Speicherplatz hingegen **unentgeltlich** zur Verfügung gestellt, so kann man nicht davon ausgehen, dass ein Mietvertrag vorliegt, weil der Nutzer hier nicht zur Entrichtung der Miete verpflichtet ist. Dies ist jedoch für den Mietvertrag ein wesentliches Merkmal. Hier spricht vielmehr einiges dafür, den Vertrag als **Leihvertrag** gem. § 598 BGB über den zur Verfügung gestellten Speicherplatz anzusehen. Hier ist der Entleiher jedoch – anders als der Vermieter – nicht dazu verpflichtet, Störungen des Gebrauchs der entliehenen Sache durch Dritte abzuwehren. Dies korrespondiert mit dem Interesse des Anbieters kostenloser Cloud-Services, dass ihm kein weitreichendes Pflichtenprogramm mit entsprechenden Haftungsrisiken aufgebürdet wird. Bei rein bürgerlich-rechtlicher Betrachtung besteht also keine Pflicht des Cloud-Providers, Maßnahmen zur Gewährleistung der Datenvertraulichkeit zu ergreifen. Die Unwirksamkeit entsprechender Klauseln in den Nutzungsbedingungen gem. § 307 Abs. 2 Nr. 2 BGB kommt nicht in Betracht.

Datenschutzrechtliche Verpflichtung des Cloud-Providers

Eine Pflicht zur Ergreifung von Maßnahmen zur Sicherung der Datenvertraulichkeit könnte sich jedoch – sowohl bei unentgeltlichen als auch bei entgeltlichen Cloud-Nutzungsverträgen – aus § 9 BDSG, mithin einer öffentlich-rechtlichen Vorschrift, ergeben.[252]

---

248 Vgl. Hoffmann (Fn. 34), S. 233.

249 Wurmnest (Fn. 246), § 307 Rn. 73.

250 Häublein, in: Münchener Kommentar zum BGB, Band 3, 6. Aufl. 2012, § 535 Rn. 133.

251 Vgl. Hoffmann (Fn. 34), S. 237.

252 An dieser Stelle sei unterstellt, dass deutsches Datenschutzrecht anzuwenden ist. Denn es sind durchaus Fallgestaltungen denkbar, in denen die Beteiligten und der zugrunde liegende Sachverhalt nach deutschem

Gem. § 9 Satz 1 BDSG haben öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Nach der Anlage zu § 9 Satz 1 BDSG sind unter anderem Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle), zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle), dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger 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 (Weitergabekontrolle). Nach Satz 2 der Anlage zu § 9 Satz 1 BDSG sind solche Maßnahmen vor allem die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Durch die **Zugangs-, Zugriffs-, und Weitergabekontrolle** wird die Vertraulichkeit der personenbezogenen Daten gewährleistet. § 9 Satz 1 BDSG schützt somit in Verbindung mit der Anlage die Datenvertraulichkeit.

Es stellt sich daher die Frage, ob § 9 Satz 1 BDSG die Lagerung von Daten in einer Cloud durch den Bürger erfasst. Der private Cloud-Provider ist eine nicht-öffentliche Stelle im Sinne von § 2 Abs. 4 Satz 1 BDSG. Eine Datenverarbeitung ist gem. § 3 Abs. 4 Satz 1, 2 Nr. 1 BDSG das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten, wobei das Speichern ungeachtet der dabei angewendeten Verfahren das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung ist. Werden Daten in einer Cloud-Anwendung abgelegt, so werden diese zumindest auf einem Datenträger aufbewahrt. Das gilt trotz der Tatsache, dass nicht alle Daten eines Nutzers in demselben Rechenzentrum bzw. auf demselben Speichermedium fixiert werden. Fraglich ist, *wer* die Speicherung der Daten vornimmt. Einerseits könnte man davon ausgehen, dass der Nutzer selbst die Speicherung seiner Daten initiiert und verantwortet, weil der Provider nur den Speicherplatz zur Verfügung stellt und er an dem Vorgang des Speicherns nicht beteiligt ist. Dann läge seitens des Providers kein Speichern und folglich auch keine Datenverarbeitung vor, sodass ihn die Pflicht aus § 9 Satz 1 BDSG zur Ergreifung technisch-organisatorischer Maßnahmen nicht träfe. Andererseits soll eine Speicherung im Sinne von § 3 Abs. 4 Satz 1, 2 Nr. 1 BDSG aber nicht nur dann vorliegen können, wenn von der »verantwortlichen Stelle« erhobene oder ihr sonst bekannte Informationen wie auch immer »nachlesbar« fixiert werden, sondern auch dann, wenn die Daten von einem Dritten gespeichert und vom Provider nur vorrätig gehalten werden.[253] Dieser Ansicht zufolge ist unabhängig davon, dass der Provider nur den Speicherplatz zur Verfügung stellt und der Nutzer die eigentliche Handlung des »Ablegens« vornimmt, davon auszugehen, dass der Provider die Daten speichert und somit eine Datenverarbeitung vornimmt. Für diese Auslegung spricht der Schutzzweck des § 9 Satz 1 BDSG. Diese Norm soll dem Schutz der informationellen Selbstbestimmung dienen. Diese soll möglichst umfassend geschützt werden. Um dies zu erreichen, ist eine **weite Auslegung des**

Recht zu beurteilen sind. Dies gilt vor allem, wenn zukünftig das in der Europäischen Datenschutz-Grundverordnung enthaltene »Marktortprinzip« maßgeblich ist.

253 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 3 Rn. 27.

Begriffs des Speicherns geboten. Insofern liegt eine Speicherung und somit auch eine Verarbeitung der Daten durch den Provider vor, sodass ihn die Pflichten aus § 9 Satz 1 BDSG treffen. Er hat also technisch-organisatorische Maßnahmen zur Gewährleistung der Datenvertraulichkeit vorzunehmen. Zu beachten ist dabei jedoch, dass der Provider gem. § 9 Satz 1 und 2 BDSG nur **erforderliche Maßnahmen**, also solche, deren Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht, ergreifen muss.[254]

Auswirkungen auf das Vertragsgefüge

Fraglich ist, wie sich diese öffentlich-rechtliche Pflicht im Bereich der unentgeltlichen Cloud-Angebote auf das dahinter stehende vertragliche Gefüge auswirkt. Einerseits könnte man es als Wertungswiderspruch ansehen, ein unentgeltliches Cloud-Angebot als Leihe einzuordnen, womit keinerlei Pflichten zur Gewährleistung der Vertraulichkeit einhergehen und dann dem Provider gleichwohl die öffentlich-rechtliche Pflicht aufzuerlegen, Maßnahmen zur Gewährleistung der Vertraulichkeit zu ergreifen. Damit würde das von den Parteien gewollte und (zivil-)rechtlich gebilligte Pflichtenprogramm durch eine öffentlich-rechtliche Vorschrift überlagert. Vor allem den Provider träfe es, wenn er einen kostenlosen Service anbietet und ihm »durch die Hintertür« erhebliche Pflichten auferlegt werden, die zu erfüllen einen hohen Aufwand und hohe Kosten bedeuten. Hinzu kommt ein erhebliches Haftungsrisiko bei Verletzung der Pflichten aus § 9 Satz 1 BDSG, da diese Vorschrift ein Schutzgesetz im Sinne von § 823 Abs. 2 BGB darstellt und diese Vorschrift eine Schadensersatzanspruchsgrundlage für den Betroffenen bietet.[255] Insofern könnte man es als nicht angemessen ansehen, dem Provider auch bei unentgeltlichen Cloud-Services die Ergreifung technisch-organisatorischer Maßnahmen im Sinne von § 9 Satz 1 BDSG aufzuerlegen. Damit ist es auf den ersten Blick – und rein zivilrechtlich betrachtet – interessengerecht, dass bei unentgeltlicher Zurverfügungstellung von Speicherplatz keine Pflicht des Anbieters besteht, den Zugriff unbefugter Dritter auf die Daten zu verhindern.

Andererseits differenziert § 9 Satz 1 BDSG nicht zwischen entgeltlichen und unentgeltlichen Angeboten. Der Wortlaut der Norm lässt insofern keinen Spielraum für eine Befreiung der Anbieter kostenloser Cloud-Services. Dies entspricht auch dem **Schutzzweck von § 9 BDSG,** der auch bei unentgeltlichen Angeboten zur Geltung gelangen muss. Des Weiteren ist zu bedenken, dass es dem Provider aufgrund der aus Art. 2 Abs. 1 GG abgeleiteten Privatautonomie[256] frei steht, einen für ihn nachteiligen Vertrag abzuschließen. Darüber hinaus bietet das Anbieten unentgeltlicher Cloud-Services auch Vorteile wie etwa eine verstärkte Kundenbindung oder Prestige und somit Wettbewerbsvorteile gegenüber den Konkurrenten. Im Übrigen besteht für den Provider die Möglichkeit, dem Nutzer kostenpflichtige Zusatzangebote zu unterbreiten. Folglich erscheint es nicht unangemessen, auch dem Anbieter kostenloser Cloud-Services die Pflicht zur Ergreifung technisch-organisatorischer Maßnahmen im Sinne von § 9 Satz 1 BDSG aufzuerlegen.

Weiter ist fraglich, wie vor diesem Hintergrund eine Klausel in den Nutzungsbedingungen zu beurteilen ist, die den Anbieter kostenloser (und kostenpflichtiger) Cloud-Services davon befreien, die entsprechenden technisch-organisatorischen Maßnahmen zu ergreifen, oder diese Pflicht auf den Nutzer abwälzen. In Betracht kommt eine Unwirksamkeit entsprechender Klauseln aus § 307 Abs. 2 Nr. 1 BGB. Dies wäre der Fall, wenn eine unangemessene Benachteiligung in der Form vorläge, dass diese Bestimmung mit wesentlichen Grundge-

---

254 Vgl. dazu Gola/Schomerus (Fn. 253), § 9 Rn. 7 ff.

255 Dazu Gola/Schomerus (Fn. 253), § 1 Rn. 4.

256 Dazu Di Fabio, in: Maunz/Dürig (Fn. 30), Art. 2 Rn. 101 ff.

danken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist. Dabei stellt sich die Frage, ob das Tatbestandsmerkmal »der gesetzlichen Regelung« auch **öffentlich-rechtliche Vorschriften** erfasst. Der Wortlaut der Norm enthält keine Beschränkung auf privatrechtliche Normen. Daher wird in Literatur und Rechtsprechung davon ausgegangen, dass sich § 307 Abs. 2 Nr. 1 BGB auch auf andere als vertragsrechtliche Gesetze, insbesondere das BDSG bezieht, weil sich der Gesetzgeber grundsätzlich für den Schutz perso-personenbezogener Daten entschieden habe.[257] Insofern ist § 9 Satz 1 BDSG im Rahmen von § 307 Abs. 2 Nr. 1 BGB zu berücksichtigen. Es ist auch ein wesentlicher Grundgedanke von § 9 Satz 1 BDSG, dass die datenverarbeitende Stelle technisch-organisatorische Maßnahmen im Sinne der Vorschrift zu treffen hat. Dies ergibt sich aus dem Schutzzweck der Norm – Absicherung der grundrechtlich verbürgten Datenvertraulichkeit. Ein Ausschluss dieser Pflicht in Allgemeinen Geschäftsbedingungen stellt eine unangemessene Benachteiligung dar. Eine entsprechende Klausel wäre somit gem. § 307 Abs. 2 Nr. 1 BGB unwirksam. Ein individualvertraglicher Ausschluss der Pflichten aus § 9 Satz 1 BDSG dürfte gem. § 138 Abs. 1 BGB nichtig sein.

Sonstige Rechte des Datenhoheitsträgers

Hält sich der Anbieter entgeltlicher Cloud-Services nicht an die Vorgaben des § 9 Satz 1 BDSG zur Ergreifung technisch-organisatorischer Maßnahmen zur Gewährleistung der Datenvertraulichkeit, so kann der Nutzer einen vertraglichen Anspruch auf deren Einhaltung geltend machen.

Gelingt es einem unbefugten Dritten, auf die in der Cloud gelagerten Daten zuzugreifen, so steht dem Datenbetroffenen ein **Unterlassungsanspruch analog § 1004, § 823 Abs. 1 BGB** zu.[258] Die Rechtsdurchsetzung erscheint jedoch schwierig, da der Anspruchsteller in der Regel nicht weiß, ob ein Zugriff erfolgen soll, wann dieser stattfinden soll, geschweige denn, wer diesen initiiert.

Zudem kommen **Schadensersatzansprüche** sowohl gegen den Cloud-Betreiber als auch gegen den zugreifenden unbefugten Dritten in Betracht,[259] stellen aber eher nachgelagerten Schutz dar und können nicht dafür sorgen, dass ein Zugriff auf die Daten unterbleibt. Auch hier besteht im Übrigen bzgl. des Dritten aus tatsächlichen Gründen ein Durchsetzungsproblem. Hinsichtlich des Cloud-Betreibers kommt es darauf an, ob das Nutzungsverhältnis als Miete oder als Leihe ausgestaltet ist. Nur im Fall der Miete besteht ein Pflichtenprogramm, welches den Schutz der Vertraulichkeit umfasst und bei dessen Verletzung Schadensersatzansprüche aus Vertrag gegen den Betreiber ausgelöst werden können.

Rechtliche Handhabe bei staatlichen Cloud-Angeboten

Betreibt der Staat einen Cloud-Service oder hält er einen bestimmten Datenbestand zum Abruf durch andere (staatliche) Stellen bereit, so darf er nur im Rahmen seiner gesetzlichen Bindungen handeln. Er hat seine Schutzpflicht für das Recht auf informationelle Selbstbestimmung zu wahren, indem er entsprechende (Schutz-)Maßnahmen ergreift. Einfachgesetzlich betrachtet trifft auch staatliche Stellen die Pflicht aus § 9 Satz 1 BDSG zur Vornahme technisch-organisatorischer Maßnahmen zum Schutz der Datenvertraulichkeit. Kommt er dieser nicht nach und entsteht dem Bürger dadurch ein Schaden, so kommt ein **Amtshaftungsanspruch aus § 839 BGB i. V. m. Art. 34 GG** in Betracht. Treten auf Seiten

---

[257] Vgl. Wurmnest (Fn. 246), § 307 Rn. 69.

[258] Vgl. Polenz, in: Kilian/Heussen (Hrsg.), Computerrecht, Loseblatt (Stand: 31. Erg.-Lfg. 05/2012), 1. Abschn., Teil 13, Betroffenenrechte, Rn. 36.

[259] Vgl. Polenz (Fn. 258), Rn. 38.

des Datenbetroffenen andere (tatsächliche) Folgen auf, so könnte er ein Verlangen nach Rückgängigmachung auf der Grundlage des Folgenbeseitigungsanspruchs geltend machen. Diese Ansprüche stellen freilich nur einen nachgelagerten Schutz dar und können die Verletzung der Vertraulichkeit nicht verhindern. Hat der Bürger Kenntnis von der Verletzung der Pflichten aus § 9 Satz 1 BDSG, so kann er die Einhaltung dieser Anforderungen in Form eines Leistungsbegehrens durchsetzen.

Fazit

Festhalten lässt sich, dass es aufgrund der geringen Einflussmöglichkeiten des Cloud-Nutzers interessengerecht ist, dem Provider die Pflicht aufzuerlegen, Maßnahmen zur Sicherung der Datenvertraulichkeit zu ergreifen. Die rechtliche Verpflichtung dazu folgt bei entgeltlichen Cloud-Services aus dem zugrundeliegenden Vertragsverhältnis und bei entgeltlichen wie unentgeltlichen Angeboten aus § 9 Satz 1 BDSG. Von dieser Verpflichtung kann sich der Provider nicht entledigen – und zwar weder individualvertraglich noch durch allgemeine Geschäftsbedingungen. Auch den Staat treffen die Pflichten aus § 9 Satz 1 BDSG, wenn er einen Cloud-Service anbietet oder zentrale Datenbestände vorhält.

5.3.4.2 Gegenüber Zugriffen durch den Provider

Zuweilen enthalten die Nutzungsbedingungen von Cloud-Services eine Klausel, wonach der Nutzer dem Anbieter in den Zugriff auf die in der Cloud gelagerten Daten sowie deren Verarbeitung einwilligt.[260] Aus technischer Sicht sind derartige Zugriffe für den Nutzer in der Regel nicht verhinderbar (vgl. aber auch 5.3.2.2 zur Möglichkeit, nicht nur den Personenbezug, sondern auch den Aussagegehalt der Daten aufzuheben), zumal der Provider es in der Hand hat, die Benutzeroberfläche so zu gestalten, dass er selbst von Sicherheitseinstellungen ausgenommen ist. Aus rechtlicher Sicht stellt sich die Frage, ob derartige Klauseln wirksam sind.[261]

Einfachgesetzliche Zugriffsrechte

Zunächst könnte sich das Recht des Cloud-Anbieters zum Zugriff und zur Verarbeitung der in der Cloud gelagerten personenbezogenen Daten bereits aus dem Gesetz ergeben. Bei entgeltlichen Cloud-Nutzungsverhältnissen liegt ein **typengemischter Vertrag mit primär mietvertraglichen Elementen** vor. Insofern bietet es sich an, die mietvertraglichen Regelungen des BGB nach vergleichbaren Zugriffsrechten des Vermieters auf das Mietobjekt zu analysieren und deren Übertragbarkeit auf die hier vorliegende Situation zu prüfen. Das BGB kennt an verschiedenen Stellen das Recht des Vermieters zum Betreten der von ihm vermieteten Wohnung. Relevante Vorschriften sind insoweit die §§ 554, 562 ff. und § 242 BGB. So folgt aus § 554 Abs. 1 BGB ein Betretungsrecht des Vermieters zwecks Mängelbeseitigung und aus § 554 Abs. 2 BGB ein Recht zum Betreten der Wohnung zum Zwecke der Ausführung von Modernisierungsmaßnahmen. Übt der Vermieter sein Vermieterpfandrecht gem. §§ 562 ff. BGB aus, so muss er dafür zwangsläufig die Wohnung betreten können. Darüber hinaus ist dem Vermieter nach richtiger Auffassung aus § 242 BGB ein periodisches Betretungsrecht zuzubilligen, um seiner Pflicht zur Instandhaltung der Wohnung aus §§ 536 ff. BGB nachkommen und eine mögliche Haftung gegenüber dem Mieter abwenden zu können.[262] Aus der Zusammenschau dieser Vorschriften ergibt sich, dass dem Vermieter ein Be-

---

[260] So etwa Nr. 3.3 der Amazon Cloud Drive-Nutzungsbedingungen; www.amazon.de/gp/feature.html/ref=sa_menu_acd_lrn1?ie=UTF8&docId=1000655923/.

[261] Bei der Beantwortung dieser Frage soll hier unterstellt werden, dass deutsches Recht anwendbar ist.

[262] Dazu Dittman/Reichhart, JA 2011, 173.

tretungsrecht einerseits zum Zwecke der Instandhaltung und andererseits zum Zwecke der Durchsetzung seiner Ansprüche aus dem Mietverhältnis zusteht.

Diese Grundgedanken lassen sich auf Cloud-Services übertragen. Hier besteht die Pflicht des Anbieters, für Datenvertraulichkeit und Datenverfügbarkeit zu sorgen. Tut er dies nicht, besteht ein Haftungsrisiko. Zudem muss dem Anbieter ein wirksames Mittel zur Durchsetzung seiner Ansprüche zustehen. Im Rahmen eines Zurückbehaltungsrechts etwa muss der Provider auf die Daten zugreifen können, um dieses wirksam, bspw. in Form des Sperrens auszuüben. Die Interessenlage bei Cloud-Services und der Wohnraummiete ist auch deshalb vergleichbar, weil der Bürger, wenn er personenbezogene Daten in einer Cloud ablegt, für diese einen privaten und damit vertraulichen Aufbewahrungsort anlegt. Nicht anders verhält es sich, wenn er für sich selbst als die Person, auf die sich die Daten beziehen, einen privaten Rückzugsort schafft. Datenverarbeitungsvorgänge durch den Cloud-Anbieter zum Zwecke der Erhaltung und Ermöglichung der Weiternutzung der Daten müssen somit zulässig sein. Dies gilt jedenfalls dann, wenn sich dies nicht ohne Verletzung der Vertraulichkeit gewährleisten lässt, weil die Vertraulichkeitsverletzung ansonsten nicht erforderlich und damit unverhältnismäßig wäre. Derartige Maßnahmen dienen letztlich auch dem Interesse des Datenbetroffenen an der **Datenverfügbarkeit**. Andere Maßnahmen – etwa die Löschung oder die Verarbeitung der Daten, um personalisierte Werbung an die Nutzer zu versenden – sind vom Sinn und Zweck dieser Vorschriften nicht erfasst. Bei unentgeltlichen Cloud-Services, die als Leihe einzuordnen sind, bestehen keine Instandhaltungspflichten. Ein Betretungsrecht oder Ähnliches besteht hier nicht. Somit fehlt es an einer gesetzlichen Grundlage für einen anbieterseitigen Zugriff auf die Daten des Nutzers.

Vertraglich eingeräumte Zugriffsrechte

Daneben könnte das Recht des Cloud-Anbieters zum Zugriff und zur Verarbeitung der in der Cloud gelagerten personenbezogenen Daten vertraglich, insbesondere durch Allgemeine Geschäftsbedingungen, vereinbart werden. Auf diese Weise könnte bei unentgeltlichen Nutzungsverhältnissen ein Zugriffsrecht erstmals begründet und – auch bei entgeltlichen Cloud-Services – möglicherweise um Zugriffsrechte zu weiteren Zwecken erweitert werden. Dabei stellt sich zunächst die Frage, ob Einwilligungen zu Datenverarbeitungsvorgängen in Allgemeinen Geschäftsbedingungen wirksam enthalten sein können. Dies ist nur der Fall, wenn die entsprechende Klausel gem. § 4a Abs. 1 Satz 4 BDSG besonders hervorgehoben ist.[263] Liegt eine besondere Hervorhebung vor, ist also eine Einwilligung zur Datenverarbeitung in Allgemeinen Geschäftsbedingungen wirksam zu vereinbaren. Vorgänge, die von dieser Einwilligung umfasst werden, sind aus datenschutzrechtlicher Sicht unbedenklich. Gleichwohl bedeutet dies nicht zugleich, dass die entsprechenden Klauseln auch aus AGB-rechtlicher Sicht nicht zu beanstanden sind. Insoweit ist zwischen der datenschutzrechtlichen und der AGB-rechtlichen Wirksamkeit der Klauseln zu unterscheiden.

Demnach ist zu untersuchen, inwieweit sich der Provider durch AGB überhaupt Zugriffsrechte einräumen lassen darf und wie weit diese gehen dürfen. Als unproblematisch wirksam dürften solche Klauseln anzusehen sein, die der Erhaltung und Ermöglichung der fortwährenden **Speicherung** der Daten dienen. Datenverarbeitungsvorgänge, die diesem Zweck dienen, fördern den Zweck von Cloud-Anwendungen, nämlich die externe Speicherung von Daten. Sie sind also weder überraschend im Sinne von § 305c Abs. 1 BGB noch aus inhaltlichen Gründen gem. §§ 307 ff. BGB als unwirksam anzusehen. Diese Maßnahmen dienen letztlich der Datenverfügbarkeit und liegen daher auch im Interesse des Datenbetroffenen. Durch eine solche Klausel in den Nutzungsbedingungen kann bei unentgeltlichen

[263] Vgl. dazu weiterführend Redeker, in: Hoeren/Sieber, (Hrsg.), Handbuch Multimedia-Recht, Loseblatt-Sammlung (Stand: 32. Erg.-Lfg. 03/2012), Teil 12 Rn. 111 ff.

Cloud-Services die rechtliche Grundlage für Datenverarbeitungsvorgänge, die der Erhaltung und Ermöglichung der fortwährenden Speicherung der Daten dienen, geschaffen werden.

Neben Datenverarbeitungsvorgängen, die der Erhaltung und Speicherung der Daten dienen, sind weitere denkbar, wie etwa das **Löschen** oder die **Auswertung** der in der Cloud gespeicherten Daten, um bspw. dem Nutzer personalisierte Werbung zukommen zu lassen. Auch hier wäre hinsichtlich der Zulässigkeit derartiger Klauseln danach zu differenzieren, ob in diese Maßnahmen datenschutzrechtlich wirksam eingewilligt worden ist. Selbst wenn dies der Fall ist, ist damit jedoch über die AGB-rechtliche Zulässigkeit noch keine Aussage getroffen. Bei Klauseln, die auf über die reine Datenspeicherung hinausgehende Datenverarbeitungsvorgänge abzielen, stellt sich aus AGB-rechtlicher Sicht zunächst die Frage, ob diese als **überraschende Klauseln im Sinne von § 305c Abs. 1 BGB** zu qualifizieren sind. Überraschend ist eine Klausel, wenn sie so ungewöhnlich ist, dass der Vertragspartner des Verwenders mit ihr nicht zu rechnen braucht. Ob dies anzunehmen ist, wird in drei Schritten geprüft. »Zunächst ist festzustellen, welche Vorstellungen und Erwartungen der Kunde vom Inhalt des abgeschlossenen Vertrages nach den Umständen hatte und haben durfte. Sodann ist der Inhalt der streitigen AGB-Klausel zu ermitteln. Schließlich ist zu fragen, ob die Diskrepanz zwischen den Vorstellungen des Kunden und dem Inhalt der AGB-Klausel so groß ist, dass sich die Annahme rechtfertigt, es handele sich um eine überraschende Klausel im Sinne des § 305c Abs. 1.«[264] Der Klausel muss ein **Überrumpelungseffekt** innewohnen, der dann anzunehmen ist, wenn der Vertragspartner mit dieser nach den Umständen vernünftigerweise nicht rechnen musste.[265] Der Nutzer einer Cloud erwartet, dass er seine Daten in dieser ablegen kann und der Anbieter dafür Sorge trägt, dass die Daten verfügbar bleiben und kein Dritter unbefugt auf die Daten zugreift. Dass der Provider selbst die Daten in irgendeiner Form – vor allem wirtschaftlich motiviert – auswertet, um daraus Profit zu schlagen, erwartet der Nutzer hingegen nicht. Schon gar nicht erwartet er ein Löschungsrecht des Anbieters, ohne dass es hierfür einen begründeten Anlass gäbe. Wenn Nutzungsbedingungen derartige Rechte des Anbieters trotzdem vorsehen, so sind diese als überraschend anzusehen, da der Nutzer einerseits mit einer wirtschaftlichen Nutzung nicht zu rechnen braucht, wenn das Angebot keinen kommerziellen Hintergrund hat, der über die reine Speicherung der Daten hinausgeht. Andererseits stünde ein Löschungsrecht in krassem Widerspruch zum Vertragszweck.[266]

Selbst wenn man dies anders bewerten sollte, so könnte sich die **Unwirksamkeit** entsprechender Klauseln gleichwohl aus § 307 Abs. 1 Satz 1 BGB oder § 307 Abs. 2 Nr. 2 BGB ergeben. Gem. § 307 Abs. 1 Satz 1 BGB sind nämlich Klauseln in Mietverträgen unwirksam, wenn sie dem Vermieter ein jederzeitiges Betretungsrecht der vermieteten Wohnung einräumen.[267] Übertragen auf Cloud-Nutzungsverträge dürften Klauseln, wonach der Provider jederzeit auf die Daten zugreifen darf, um sie zu verwerten und für sich zu nutzen, unwirksam sein. Gem. § 307 Abs. 2 Nr. 2 BGB sind Bestimmungen in Allgemeinen Geschäftsbedingungen unwirksam, wenn sie wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrags ergeben, so einschränken, dass die Erreichung des Vertragszwecks gefährdet ist. Dafür spricht hier die Tatsache, dass Nutzungen der Daten, die über den Vertragszweck, also die

---

264 Basedow, in: Münchener Kommentar zum BGB (Fn. 246), § 305c Rn. 5.

265 Basedow (Fn. 264), § 305c Rn. 10.

266 Eine ähnliche Ansicht vertritt wohl Berberich, MMR 2010, 736 (737), für die Einräumung von Urheberrechten an den Betreiber sozialer Netzwerke für den dort eingestellten urheberrechtsfähigen Content.

267 Vgl. Eisenschmidt, in: Schmidt-Futterer (Hrsg.), Mietrecht, 10. Aufl. 2011, § 535 BGB Rn. 187.

Speicherung der Daten, hinausgehen, kaum vom beiderseitig zugrunde gelegten Vertragszweck gedeckt sein dürften und inhaltlich überflüssige Rechte davon nicht gedeckt sind.[268]

Wird das Cloud-System hingegen von der **öffentlichen Hand** betrieben, so sind deren rechtsstaatliche Bindungen zu beachten. In erster Linie muss daher für jeglichen Zugriff auf die in der Cloud gelagerten Daten eine verfassungskonforme Rechtsgrundlage existieren, die den **Zweckbindungsgrundsatz** achtet und zudem rechtmäßig zur Anwendung gebracht werden muss. Die Rechtsgrundlage muss so gestaltet sein, dass durch sie das Recht auf informationelle Selbstbestimmung nicht verletzt wird. Zugriffe auf die Daten zu Zwecken der Erhaltung und Speicherung der Daten stellen zwar einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Dieser ist jedoch gerechtfertigt, weil er letztlich nur der Erhaltung der Daten dient und somit die Verfügbarkeit der Daten für den Nutzer sicherstellen soll.

5.3.5 Integrität

Integrität ist neben Verfügbarkeit und Vertraulichkeit eines der klassischen drei Schutzziele der Informationssicherheit. Integrität bezeichnet die **Vollständigkeit und Unveränderbarkeit** von Daten und Informationen. Eine wesentliche Anforderung an vertrauenswürdige Cloud-Anbieter ist die Bereitstellung technischer Werkzeuge, die die Integrität sicherstellen bzw. unterstützen.

Schutz vor der Manipulation von Daten bieten **kryptografische Verfahren.** Da kryptografische Verfahren häufig kompromittiert werden, ist eine ständige Risikobewertung des Schutzniveaus beim Cloud-Anbieter vorzunehmen. Dies kann zur Folge haben, dass Verfahren oder Verschlüsselungsschlüssel ausgetauscht werden müssen.

Eine wichtige Maßnahme, die vom Cloud-Anbieter gefordert wird ist die **Protokollierung** aller Aktionen, die das Konto eines Nutzers betreffen. Diese Protokollierungsdaten sollten dem Nutzer online zur Verfügung gestellt werden.

Des Weiteren ist **Mandantentrennung** eine Forderung zum Schutz vor Zugriff anderer Kunden auf eigene Daten. Schließlich sollte vom Cloud-Anbieter gefordert werden, Angriffe bekannt zu machen, da in diesem Fall Manipulationen auf Kunden-/Nutzerkonten und deren Daten erfolgt sein könnten.

Darüber hinaus sind organisatorische Maßnahmen beim Cloud-Anbieter hilfreich, die das Personal betreffen und sicherstellen müssen, dass das Personal keinen Zugriff auf Kundendaten hat. Eine anerkannte Zertifizierung der Informationssicherheit nach ISO 27001 könnte hilfreich sein, obwohl damit hohe Kosten beim Cloud-Anbieter verbunden sind.

---

[268] Vgl. Berberich, MMR 2010, 736 (738).

6 Ausblick

Mit der Einordnung des Begriffs Datenhoheit ist ein konzeptioneller Rahmen erstellt worden, der neben den Elementen der Verfügbarkeit die rechtlichen Elemente der Verfügungsbefugnis, Vertraulichkeit und Integrität beinhaltet. Dieser Rahmen kann mittels organisatorischer Maßnahmen seitens eines Cloud-Dienstanbieters eingehalten und durch technische Realisierungen unterstützt werden.

Grundlage für die Datenhoheit ist ein elektronisches Archiv, das personenbezogene Informationen langfristig speichert und zur Verfügung vorhält. Dies kann ein Cloud-Dienst sein, der einen elektronischen Safe realisiert, aber auch – soweit verfügbar – ein elektronischer Safe aus dem De-Mail-Angebot. Wesentliche Funktionen, die von einem elektronischen Safe gefordert werden, sind:

- Die Möglichkeit einer **Freigabefunktion**, um Daten bzw. Dokumente aus dem Safe anderen Benutzern zur Verfügung zu stellen.
- Die Möglichkeit, die Dokumente als Originale abzuspeichern, was durch eine **elektronische Signatur** gegeben ist.
- Die Möglichkeit, eine Kopie des Originals zu erzeugen und nach Gebrauch zu löschen.
- Die Möglichkeit, die Dokumente langfristig zu archivieren, nach dem Prinzip der revisionssicheren elektronischen Langzeitarchivierung.

Bei der Nutzung einer Public Cloud sind die unterschiedlichen Konstellationen zu berücksichtigen, die einerseits den Cloud-Anbieter und seine Kunden und andererseits den Cloud-Anbieter und seine Unterauftragnehmer umfassen.

Ist der Kunde, der den Archiv-Dienst in Anspruch nimmt, ein staatliches Unternehmen, so ist dieser verpflichtet, beim Cloud-Anbieter zu überprüfen, ob dieser die rechtlichen Rahmenbedingungen einhält, die mit der Speicherung und Verarbeitung personenbezogener Daten einhergehen. In diesem Fall der Auftragsdatenverarbeitung obliegt die Datenhoheit der staatlichen Stelle, die darauf zu achten hat, dass solche Daten nur zweckgebunden erhoben werden. Der Cloud-Anbieter muss den IT-Sicherheitsanforderungen des Kunden genügen und ggf. durch Audits testieren lassen. Nach IT-Grundschutz zertifizierte Cloud-Anbieter werden es leichter haben, den staatlichen Anforderungen zu entsprechen.

Ist der Kunde hingegen ein privates Unternehmen, muss er sich zwar an die Datenschutzgesetze halten, hat aber mehr Freiheit in Bezug auf das Sammeln und Auswerten von Daten als der öffentliche Sektor. Privatunternehmen haben somit die Verpflichtung, entsprechende

Auskunftsfunktionen für den Endverbraucher bereitzustellen. Dazu muss eine Auskunftsfunktion als Dienst vom Cloud-Anbieter gefordert werden.

Für den Schutz der Privatsphäre kann der Kunde einen elektronischen Safe für die Ablage der Daten und Dokumente als Cloud-Dienst benutzen. Ein *Trusted Safe*-Gütesiegel kann dabei behilflich sein, einen nach sicherheitsrelevanten Kriterien geprüften elektronischen Safe als vertrauenswürdigen Dienst einzustufen. Für die Rechtsgültigkeit der Dokumente, die im Safe abgelegt werden, sorgt die elektronische Signatur. Dokumente, die anderen zur Verfügung gestellt werden, sollten nur als Kopie des Originals verwendet werden und nach Gebrauch sofort gelöscht werden. Es wird davon ausgegangen, dass die in einem elektronischen Safe gespeicherten Dokumente eine langfristige Gültigkeit haben. Aus diesem Grunde ist zu empfehlen, den elektronischen Safe um die Funktion der Langzeitarchivierung zu erweitern. Da sich Dokumentenformate an die Standards zur Dokumenteninteroperabilität anpassen, ist zumindest abzusehen, dass Dokumente auch langfristig einsehbar sind, selbst wenn sie nicht als XML-Dokumente gespeichert sind. Dokumente, die noch nicht elektronisch erfasst sind, könnten durch einen Notardienst beglaubigt werden und dann rechtssicher im Safe abgelegt werden.

Damit der Cloud-Anbieter sowohl den "Eigentümer" als auch den Nutzer, beispielsweise die staatliche Stelle, authentifizieren kann ist ein entsprechendes Identitätsmanagement vom Cloud-Anbieter bereitzustellen.

Grundlegende Voraussetzung für ein Vertrauensverhältnis zwischen Kunde und Cloud-Anbieter ist die vertragliche Gestaltung dieser Beziehung. Da sich die Vertragsbedingungen aus einer Risikoabschätzung ergeben, sind in der Regel die Verträge sehr spezifisch und komplex. Für eine Vereinfachung soll zum einen die allgemeine Datenschutzverordnung sorgen, die die Behandlung personenbezogener Daten europaweit regelt, und zum anderen sollen Musterverträge dafür Sorge tragen, dass die Bedingungen auch verständlich und in vereinheitlichter Form zur Verfügung stehen. Dies wird in Zukunft die Auswahl der Cloud-Anbieter vereinfachen und die Angebote auch vergleichbar machen. Initiativen aus EU, nationalen Programmen und der Industrie arbeiten daran, diesen Prozess zu beschleunigen.