Vision eines elektronischen Dokumentensafes[1]

Dr. Jörn von Lucke, Speyer

Elektronische Aktensysteme in der Verwaltung

Bei der Konzeption von Hochleistungsportalen für die öffentliche Verwaltung gilt es unter anderem zu klären, wie Bürgern der Zugang zu elektronischen Verwaltungsdokumenten und -akten ermöglicht werden soll. Traditionell führt in den Behörden eine aktenführende Stelle die Verwaltungsakten als Sach-, Verfahrens- oder Namensakten im Rahmen von Aktenverzeichnissen und Aktenplänen, die der Verwaltungsgliederung entspricht. Nach Abschluss des Verfahrens werden die Akten für die Dauer der gesetzlichen Aufbewahrungsfrist im Archiv gelagert. Akten dienen der Überprüfbarkeit und Dokumentation der Aufgabenerledigung, vom Beginn bis zum Abschluss eines Verwaltungsverfahrens. Dadurch lässt sich die Nachvollziehbarkeit des Verwaltungshandelns gewährleisten.[2] Akten bestehen aus Vorgängen in einer Verwaltungsangelegenheit, aus denen sich Inhalte und Ablauf des Verwaltungsverfahrens ergeben und die in einzelnen Dokumenten festgehalten werden. Sie beinhalten so das kollektive Wissen für eine unabhängige, arbeitsteilige und hochspezialisierte Bearbeitung von Verwaltungsverfahren ohne Ansehen der Person.[3] Die Bürger erhalten aus diesen Akten nur ausgewählte Dokumente, etwa Durchschläge eingereichter Formulare, Bescheinigungen, Auszüge und Bescheide. Diese nehmen sie zur Kenntnis, bevor sie sie in ihren persönlichen Ordnern zu Hause ablegen.

Die Einführung elektronischer Dokumentenmanagementsysteme in der öffentlichen Verwaltung stellt die bisherige Praxis der Aktenführung vor neue Herausforderungen. Dazu gehört

---

[1] Dieser Beitrag ist meinem Doktor- und Habilitationsvater Univ.-Prof. Heinrich Reinermann anlässlich seiner Emeritierung im Oktober 2003 gewidmet, der mir während unserer gemeinsamen Jahre am Forschungsinstitut für öffentliche Verwaltung bei der Deutschen Hochschule für Verwaltungswissenschaften Speyer (http://www.foev-speyer.de) immer wieder von seinen eigenen Überlegungen zur Funktionalität eines Dokumentensafes berichtete. Durch seine vielseitigen Ideen angeregt, erarbeitete ich im Rahmen unseres gemeinsamen Projektes „Hochleistungsportale für die öffentliche Verwaltung“ (http://www.foev-speyer.de/portale) die vorliegende Vision.

[2] Vgl. SAP 2002, S. 7 und Schreiber 2003, S. 175 ff.

[3] Vgl. Roßnagel 1999, S. 160 f. und Schreiber 2003, S. 175 ff.

die Anpassung der rechtlichen Rahmenbedingungen auf elektronische Dokumente, eine Reorganisation der Aktensystematik unter Berücksichtigung des Verwaltungsverfahrensrechts und des Datenschutzes sowie die Programmierung entsprechender Aktensysteme. Mit der Umstellung der bestehenden Akten- und Archivsysteme steht die aufwändigste Phase bevor. In diesem Moment bietet sich eine einzigartige Chance zur Neugestaltung des gesamten Aktenwesens in der Verwaltung. Elektronische Akten könnten künftig nicht nur aus Behördensicht, sondern auf Knopfdruck auch aus Bürgersicht zusammengestellt werden. Für Zugriffe auf Akten würden dann Portale ausreichen. Ausgehend von der Fragestellung, bei wem die elektronischen Akten, Vorlagen und Dokumente künftig gespeichert werden und wer welche Zugriffsrechte auf die in den Akten enthaltenen öffentlichen und nicht-öffentlichen Datenbestände[4] erhalten soll, eröffnen sich so grundsätzlich drei unterschiedliche Realisierungsansätze zur Speicherung von Bürgerdaten in der öffentlichen Verwaltung.

Verwaltungsakte, Bürgerakte und Dokumentensafe

Ausgangsbasis für neuartige Überlegungen sind die in Dokumentenmanagement- und Vorgangsbearbeitungssystemen eingebetteten **elektronischen Aktensysteme**, in denen sämtliche Daten, Unterlagen und Dokumente zu einem Verwaltungsverfahren gespeichert werden. Künftig wird jede Behörde über eigene Aktensysteme mit integrierter Vorgangsbearbeitung verfügen, entweder intern betrieben, outgesourct oder über netzbasierte Application Service Provider angemietet.[5] Diese mit Schnittstellen versehenen Systeme erlauben es, dass Akten auch über Behördengrenzen hinweg geführt, bearbeitet und zusammengeführt werden können. Und diese Funktionalität öffnet den Weg für die Einführung von elektronischen Verwaltungsakten, Bürgerakten und Dokumentensafes (Abbildung 1) als zentrale Verwaltungsportale im Informationszeitalter.

Bei einer bürgerbezogenen, **elektronischen Verwaltungsakte** handelt es eigentlich sich um eine virtuelle Zusammenstellung aller (im Ausnahmefall) oder ausgewählter, in der öffent-

---

[4] Elektronische Akten setzen sich aus öffentlich zugänglichen und aus nicht-öffentlichen Aktenbeständen zusammen. Nicht-öffentliche Datenbestände dienen etwa dem Schutz von personenbezogenen Daten, von Geschäftsgeheimnissen, der öffentlichen Sicherheit, der Verteidigung, von militärischen Belangen oder von internationalen Beziehungen.

[5] Vgl. hierzu Daum 2002, S. 263 ff.

lichen Verwaltung vorliegenden Akten zu einem Bürger, die zum Teil aus ganz verschiedenen Verwaltungsverfahren stammen. Nur Verwaltungsmitarbeiter bekommen einen solchen, ihrer Rolle angemessenen und zu einem Bürger passenden Auszug aus den verschiedenen Aktensystemen unterschiedlicher Behörden und Gebietskörperschaften. Der betroffene Bürger selbst darf nur unter gewissen Umständen eine Akteneinsicht[6] erhalten, jedoch kann er niemals diese Datenbestände selbständig ändern. Werden Aktensysteme zunächst nur innerhalb einzelner Behörden installiert, ist mittelfristig mit einer Vernetzung vieler Aktensysteme zu rechnen. Trotz des Grundsatzes der informationellen Gewaltenteilung[7] und damit verbundener datenschutzlicher Bedenken, sprechen vielfältige Erwägungen für eine (Wieder-)Herstellung der „virtuellen Einheit der Verwaltung“.[8] Behördenübergreifende Zusammenstellungen könnten etwa dazu dienen, Missbrauch und Betrug vorzubeugen, Schäden vom Staat und seinen Bürgern abzuwehren, die verwaltungsinterne Abstimmung zu vereinfachen und zu verbessern oder Entscheidungen besser abzusichern. Flankierende Datenschutzmaßnahmen werden dabei dafür sorgen, dass das Recht des Bürgers auf informationelle Selbstbestimmung[9] nicht beeinträchtigt wird.

Statt die Datenspeicherung und den Zugriff auf Bürgerdaten nur berechtigten Beschäftigten der öffentlichen Verwaltung zu eröffnen, verfolgt die **elektronische Bürgerakte** einen transparenteren Ansatz. Auch bei der Bürgerakte handelt es sich um eine auf Dokumentenmanagement- und Vorgangsbearbeitungssystemen basierende virtuelle Zusammenstellung aller oder ausgewählter, in der öffentlichen Verwaltung vorliegenden Akten zu einem Bürger, die zum Teil aus ganz verschiedenen Verwaltungsverfahren stammen. Diese Unterlagen können aber vom Bürger um eigene Anmerkungen und Dokumente ergänzt werden. Letztere sind als solche besonders kenntlich gemacht. Die Verwaltung hat auf diese persönlichen Unterlagen des Bürgers keine Zugriffsberechtigung. Sie fließen daher auch nicht in die Bearbeitung der Verwaltungsverfahren ein. Auf Wunsch kann der Bürger sie aber zum Verfahren nachreichen. Folglich handelt es sich bei der Bürgerakte um ein von der Verwaltung vorgehaltenes elektronisches Dokumentenmanagementsystem und -archiv für Verwaltung und Bürger. Nur

---

6 Rahmenbedingungen für eine Akteneinsicht werden im Informations- und Akteneinsichtsrecht geregelt.

7 Vgl. DIB 2000, S.6 und LfD NRW 1999, S. 92.

8 Vgl Ellwein 1973, S. 368; Beyer 1986, S. 136 ff., Denninger 2000, S. 71 ff. und Reinermann 2002b, S. 112.

9 Das Recht auf informationelle Selbstbestimmung des Bürgers als grundsätzlich geschützter Bereich des Persönlichkeitsrechts ergibt sich aus Art. 2, Abs. 1 in Verbindung mit Art.1, Abs. 1 des Grundgesetzes.

der betroffene Bürger und die zum Zugriff berechtigten Verwaltungsmitarbeiter verfügen über einen Lesezugriff und in beschränkter Form auch einen Schreibzugriff auf die Objekte in der Bürgerakte. Eine automatisch integrierte Protokollfunktionalität informiert die Bürger über alle Zugriffe auf ihre Daten. Dadurch könnten die Bürger feststellen, wo in der Verwaltung ihre personenbezogenen Daten gespeichert und welche Stellen auf diese Daten für welche Zwecke zugreifen. Zur Speicherung der Datenbestände eignet sich neben einer Smartcard (Datenhandtasche) vor allem ein virtuelles Schließfach (im Sinne eines Postfachs mit zwei Schlüsseln), denkbar in zentraler oder verteilter Umsetzungsvariante.[10]

Der Ansatz des **elektronischen Dokumentensafes** verlagert die Speicherung und den Zugriff auf die Datenbestände aus dem Verantwortungsbereich der Verwaltung heraus zum Bürger beziehungsweise zu einem von ihm mit der Datenhaltung beauftragten Datentreuhänder. Der Bürger oder sein Treuhänder geben auf Anfrage oder im Rahmen eines Antrages ausgewählte öffentliche Datenbestände aus dem elektronischen Dokumentensafe an zum Zugriff berechtigte öffentliche Stellen weiter. Nur der Bürger kann und darf auf diese, seine persönlichen Daten zugreifen und sie verändern, ergänzen oder löschen. Mitarbeitern aus der Verwaltung bleibt der direkte Zugriff auf die im Safe gelagerten Datenbestände, lesend wie schreibend, verwehrt. Auf Anfragen erhalten sie nur Kopien der öffentlichen Datenbestände des Bürgers. Diese überführen sie dann in das elektronische Aktensystem der jeweiligen Verwaltungsbehörde.

Unabhängig von einer Realisierung im Detail stellt sich eigentlich nicht die Frage einer ausschließlichen Umsetzung eines dieser Ansätze. Alle drei Konzepte ergänzen sich im gemeinsamen Einsatz gegenseitig. Elektronische Verwaltungsakten könnten zu elektronischen Bürgerakten ausgebaut werden und so eine stärkere Bürgerorientierung der Verwaltung unterstreichen. Zugleich erleichtern sie eine Akteneinsicht. Ein Dokumentensafe erhält erst durch die Aufnahme der Funktionalität der Bürgerakten den Mehrwert, der für eine weite Marktdurchdringung erforderlich wäre. Trotz auf Bürgerseite vorhandener, elektronischer Dokumentensafes wird eine Verwaltung nicht auf eigene elektronische Verwaltungsakten verzichten wollen. Sie hätte aber durch flächendeckend verfügbare Dokumentensafes die Sicherheit, dass ihre elektronisch versandten Bescheide und sonstigen Dokumente auch zu-

---

[10] Vgl. Lenk 2002, S. 546.

stellbar wären, ohne dass sie sich selbst um die technische Abwicklung und die Bereitstellung von sicheren elektronischen Postfächern kümmern müssten.

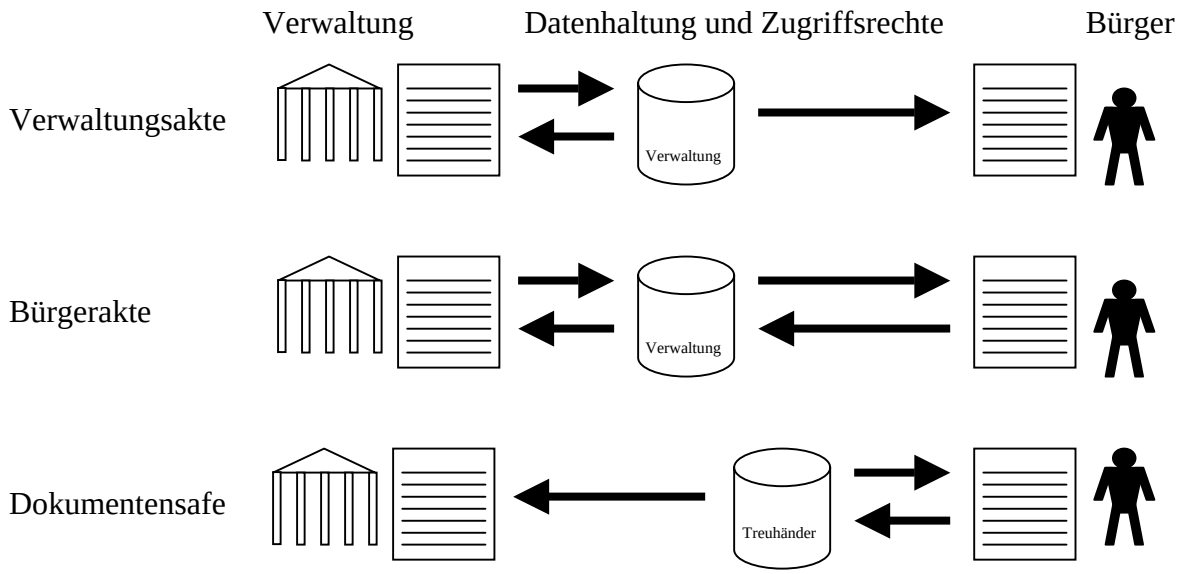

Abbildung 1: Verwaltungsakte, Bürgerakte und Dokumentensafe

In den folgenden Ausführungen wird die Vision eines elektronischen Dokumentensafes entwickelt. Dieser Ansatz bietet nicht nur aus Sicht der öffentlichen Verwaltung einen interessanten Business-Case. Auch für die Wirtschaft und den Dritten Sektor könnte dieser Ansatz von großem Interesse sein.

Elektronischer Dokumentensafe

Ausgangsbasis für Überlegungen zur Gestaltung elektronischer Dokumentensafes sind bereits vorhandene und bekannte Modelle realer Schließfächer und Safes. Dazu zählen der Geldtresor zu Hause oder im Büro, in dem Wertsachen verschlossen und nur nach Einführung eines Safeschlüssels oder nach Eingabe eines Freischaltcodes wieder zugänglich gemacht werden können. Weitere Anregungen bieten die verschiedenen Typen von Postschließfächern, etwa das Postfach im ehemaligen Postamt, der Postkorb am Arbeitsplatz, der Briefkasten an der Haustür oder die in ländlichen Regionen verbreiteten Postboxen an Abzweigungen zu abgelegenen Gehöften. Im Bankwesen gibt es zwei Arten von Schließfächern. Anleger richten sich Depots bei ihren Banken ein, in denen ihre Wertpapiere verwahrt werden. Zudem

besitzen Banken eigene Tresorräume, in denen ihre Kunden Schließfächer anmieten, auf die aber nur mit zwei gleichzeitig eingeführten Schlüsseln zugegriffen werden kann. Im Internet bieten Hostingdienste Webschließfächer (Webspace). Dieser Speicherraum auf Datenservern kann zur Ablage beliebiger Daten verwendet werden. Aus all diesen Überlegungen und Vorbildern heraus lassen sich zentrale Elemente der erforderlichen Funktionalität elektronischer Dokumentensafes ableiten.

Ein **elektronischer Dokumentensafe** sollte demnach ein auf modernen Informations- und Kommunikationstechnologien basierendes und über elektronische Medien erreichbares virtuelles Schließfach zur Ablage, Verwaltung, Versand und Empfang von elektronischen Dokumenten auf einem für diese Zwecke ausgerichteten Server sein. Der Safe steht unter ausschließlicher Verfügungsgewalt des Bürgers, vollkommen unabhängig vom Anbieter des Schließfaches, aber auch unabhängig von staatlichen Stellen oder sonstigen Dritten.

Im Grunde steckt hinter einem elektronischen Dokumentensafe die Basisfunktionalität für den Zugriff und die Verwaltung eines virtuellen Schließfachs mit ausreichendem Speicherplatz für die Ablage von Dateien auf einem angeschlossenen Fileserver. Auf diesem Fileserver können persönliche „Wertsachen“ in elektronischer Form sicher und auf Wunsch verschlüsselt verwahrt werden. Nur berechtigte Nutzer erhalten Zugriff auf diese Dateien. Sie können diese nach eigenen Vorstellen ordnen, sortieren und ablegen. Über eine Internetanbindung können Dritte dem Inhaber weitere Dokumente zukommen lassen. Diese werden in den Safe in einen separaten Bereich eingeworfen, ohne dass dabei ein Einblick in den Dokumentensafe gewährt wird. Safes sollten über das Internet von jedem Interessenten zu jeder Zeit eröffnet, gepflegt und gelöscht werden können. Zur Speicherung der Dateien bieten sich zwei Varianten an. Einerseits können die Dateien auf dem vom Anbieter des Dokumentensafes bereitgestellten Fileserver (und den davon gespiegelten Systemen) permanent gespeichert werden. Sollte der Nutzer aber eine lokale Speicherung seiner persönlichen Dateien in verschlüsselter Form vorziehen, würde der Safeinhalt beim Logout des Inhabers in verschlüsselter Form lokal gespeichert werden, etwa auf dem lokalen Rechner oder in einer Smartcard. Beim nächsten Login würden die Safedaten automatisch aus dieser Quelle hochgeladen, so dass die volle Funktionalität des Safes wieder hergestellt ist. Bei einer lokalen Speicherung bliebe der Dokumentensafe nur in seiner Grundfunktionalität erhalten, verfügt in ausgeloggten Zeiten über

keine Inhalte. Der Bürger kann so sicherstellen, dass niemand ohne sein Einverständnis auf seine Daten zugreift. Dafür verliert er räumliche Flexibilität beim Zugriff auf seine Daten.

Die Basisfunktionalität des elektronischen Dokumentensafes stellt sicher, dass der Nutzer des Safes beliebige elektronische Objekte öffnen, speichern, versenden, weiterleiten, ausdrucken, herunterladen, hinaufladen, löschen, suchen, sortieren, kommentieren und auf mögliche Viren oder gültige Unterschriften überprüfen kann. Dies entspricht den Grundfunktionen eines elektronischen Dokumentenmanagementsystems. Sinnvoll ist auch die Integration einer E-Mail-Funktionalität, die Einbindung einer Terminverwaltung zu Fristabläufen und Fälligkeitsdaten[11] und die Anbindung der gespeicherten Objekte an vorhandene Anwendungen. Als Einziger verfügt nur der Inhaber des Safes über die Berechtigung, Daten zu öffnen, zu ändern oder zu versenden. Entsprechend der eigenen Vorlieben, Wünsche und Anforderungen können Unterschließfächer[12] und Datencontainer[13] eingerichtet werden. Hierbei ist zu berücksichtigen, dass Bürger künftig sicherlich über mehr als nur ein Schließfach verfügen. So wie viele Bürger auch Konten bei mehreren Banken besitzen, werden sie Schließfächer bei unterschiedlichen Anbietern von Dokumentensafes einrichten. Insofern sollte es den Inhabern von Dokumentensafes grundsätzlich möglich sein, ihre Daten auch aus verschiedenen Datencontainern und Safes hinweg zusammenzuführen.

In den elektronischen Dokumentensafe sollte der Bürger seine eigenen Dokumente ablegen können, entweder im elektronischen Original oder als elektronische Kopie des Originals. Dazu gehören sicherlich persönliche „Wertsachen“: Sparbücher und Wertpapiere, wichtige Briefe und E-Mails, Anwendungsprogramme und Sicherheitskopien, elektronische Reisetickets und Reservierungen. Ebenso bietet sich der Safe zur Ablage von Kopien der Identitätsdokumente wie Personalausweise, Reisepass und Kinderausweise an, die durch die Verwaltung ausgestellt werden. Im Falle eines Verlustes dieser Papiere könnte durch die virtuell vorhandenen und so über das Internet verfügbaren Kopien zumindest die eigene Identität nachgewiesen werden. Eine vergleichbarere Sicherheit bestände dadurch auch für weitere Ausweispapiere, wie etwa den Führerschein, das Schifferpatent, die Pilotenlizenz, den

---

11 Vgl. Reinermann 2002, S. 133.

12 Ein Unterschließfach im Datensafe entspricht einem Dateiverzeichnis auf einem Speichermedium.

13 Ein Datencontainer ist ein mobiles, aber in sich abgeschlossenes Schließfach für Daten, auf dessen Inhalte nur berechtigte Nutzer oder Nutzergruppen zugreifen dürfen. Im Datencontainer kann eine eigene Ordnungsstruktur bestehen. Datencontainer sind zwischen Systemen übertragbar.

Jagdschein, die Waffenbesitzkarte, den Fischereischein, den Behindertenausweis, die Sozialversicherungskarte, die Krankenversicherungskarte, Benutzerausweise, Dienstausweise oder den Studentenausweis. Denkbar wäre auch eine Speicherung der elektronischen Signatur mit allen Attributen und Zertifikaten sowie sonstiger elektronischer Identitätsprofile. Zu Ablage eignen sich aber auch Familienstandsurkunden (Familienstammbuch, Geburtsurkunde, Heiratsurkunden oder Sterbeurkunden)[14], Zeugnisse, der Lebenslauf (in Bewerbungsphasen), Ernennungsurkunden oder sonstige Bescheinigungen Dritter. Denkbar wäre auch die Ablage von Behördendokumenten. Dabei könnte es sich um Formulare handeln (blanko oder bereits ausgefüllte Formularanträge, die sich über Zusatzfunktionen signieren und verschlüsseln lassen), um Zwischenstatusmeldungen zu Anträgen, um zugestellte Bescheinigungen, um Registerauszüge oder um amtliche Bescheide. Überlegenswert wären auch die Ablage medizinischer Dokumente des Safeinhabers, etwa in Form des Gesundheitspasses, der elektronischen Patientenakte, von Attesten oder elektronischer Rezepte.[15]

An diesen ausgewählten Beispielen lässt sich erkennen, dass es vielfältige Ansatzpunkte zur Anbindung bestehender Anwendungen an einen virtuellen Safe gibt. Weitere Geschäftsmodelle ergeben sich aus der Verbindung des Dokumentensafes mit einem fortgeschrittenen E-Mail-Dienst, mit einem Identitätsmanagement zur Verwaltung des eigenen Profils, mit einem Verwaltungsaktensystem oder mit elektronischen Zahlungssystemen. Je mehr Anwendungen an einen elektronischen Datensafe angekoppelt werden, desto größer wird dessen Mehrwert und desto eher sind die Bürger oder Konsumenten bereit, ein solches Angebot zu nutzen und gegebenenfalls sogar dafür zu bezahlen. Eine grundsätzliche Zahlungsbereitschaft lässt sich aus den bereits verfügbaren kommerziellen Ange-

---

[14] Diese Aufzählung deutet auf eine mögliche Verknüpfung des Safes mit dem Lebenslagenprinzip hin. Die Ordnung innerhalb des Safes könnte ähnlich wie bei den Bürgerakten (etwa der Dortmunder DoMap: http://www.domap.de) um die Lebenslagen eines Bürgers gestaltet werden. Aus Verwaltungssicht könnte ein solcher persönlicher Safe mit der elektronischen Geburtsurkunde eröffnet und mit der elektronischen Sterbeurkunde geschlossen werden. Diese beiden Beispiel zeigen zugleich auf, dass zwar die Daten im Safe persönlicher Natur sind, aber auch ausgewählten Dritten, in diesem Falle den Eltern beziehungsweise den Erben, zugänglich sein sollten.

[15] Vgl. Mehlich 2002 S. 240 ff. und Reinermann 2002, S. 133.

boten zur elektronischen Patientenakte ableiten, für deren Nutzung jährliche Gebühren von rund 20 € für Einzelpersonen oder 50 € für Familien entrichtet werden müssen.[16]

Ausgestaltung der Verfügungsgewalt über die Safeinhalte

Der Zugang zum elektronischen Dokumentensafe muss für den Inhaber jederzeit möglich sein. Ihm darf der Zugriff weder verschlossen noch verwehrt werden. Ein Betreiber sollte dies im Regelbetrieb mühelos gewährleisten können. Dennoch sind Konstellationen denkbar, in denen der Betreiber oder Dritte ein durchaus berechtigtes Interesse haben können, dem Inhaber den Zugang zu seinen Dokumenten zu verweigern oder diese ihm gar zu löschen. Beispielsweise sei an die Nichtzahlung der vereinbarten Nutzungsgebühren, an (vom Safe unabhängige) juristische Streitigkeiten mit dem Betreiber, an eine Verwendung des Safes für illegale Aktivitäten, etwa zur Aufbewahrung und Verbreitung von Kinderpornographie, oder an eine Beschlagnahmung durch Strafverfolgungsbehörden zu denken. Somit sind bei der Einrichtung eines elektronischen Dokumentensafes auch Regelungen zum Umgang zwischen Betreiber, Nutzer und staatlichen Stellen in den allgemeinen Geschäftsbedingungen festzuhalten.

Die Regelung des Zugriffs auf die Datenbestände erweist sich als eine heikle Angelegenheit. Einerseits muss dem Nutzer garantiert werden, dass nur er und sonst niemand auf seine privaten Datenbestände zugreifen kann. Er kann selbstverständlich Teile seiner Bestände über Datencontainer der gesamten Öffentlichkeit oder ausgewählten Zielgruppen (etwa der Verwaltung, seinen Ärzten oder seinem Steuerberater) zur Verfügung stellen. In der Regel wird er aber sehr restriktiv mit der Vergabe eigener Daten umgehen wollen und keinen Zugriff Dritter zulassen. Die Sperrung des Zugriffs gilt aus Sicht des Inhabers für den Betreiber und den Superadministrator[17] des Safes ebenso wie für staatliche Stellen im Rahmen einer Strafverfolgung. Auch sollte es bei einer Nutzung im Betrieb dem Arbeitgeber technisch nicht möglich sein, auf den Dokumentensafe und seine Inhalte zuzugreifen. Lässt sich dieses dem Nutzer nicht zusichern, setzt er kaum Vertrauen in solche Angebote und nutzt sie ganz einfach nicht.

---

16 In Deutschland werden 2003 elektronische Patientenakten unter anderem von Avetana (AvetanaFile: http://www.avetana.de), von Careon (Gesundheitsakte: http://www.careon.de) und von der InterComponent Ware AG (Lifesensor: http://www.lifesensor.de) vermarktet.

17 Der Superadministrator verfügt in der Regel über alle Zugriffsrechte in einem IT-System.

Vergleichbar mit einem **Haustresor** könnte die Verfügungsgewalt über den Dokumentensafe ausschließlich beim Inhaber liegen. Es gibt nur **einen einzigen Schlüssel**[18] zum Zugriff auf die Inhalte des Safes. Deponierte Nachschlüssel sind nicht vorhanden. Bürger haben als Inhaber vollen lesenden und schreibenden Zugriff auf die Inhalte ihres Safes. Sonstigen Nutzern bleibt der Zugriff auf den Safe verwehrt. Dadurch kann der Bürger, entsprechend seiner Vorstellungen, die eigenen Daten oder Kopien dieser Daten gezielt an ausgewählte Empfänger weitergeben. Die Übertragung an Dritte geschieht verschlüsselt, so dass nur der Empfänger diese öffnen kann.

Ausgehend vom Modell eines Banktresors könnte die Verfügungsgewalt eines Dokumentensafes auch wie bei einem **Banksafe mit zwei Schlüsseln** gelöst werden. Für den Zugriff auf die Inhalte seines Safes benötigt der Inhaber seinen eigenen Schlüssel und den Schlüssel des Safebetreibers, bei dem er sich authentifizieren muss. Die Authentifzierung dient der Überprüfung des Schlüsselinhabers und bedeutet für den Safeinhaber einen zusätzlichen Schutz vor der Vorspiegelung einer falschen Identität durch unbefugte Dritte. Die Safeverwaltung muss einer Öffnung eines Safes also explizit zustimmen. Dennoch verfügt nur der Bürger als Inhaber des Safes über die vollen lesenden und schreibenden Zugriffsrechte. Dem Safeverwalter blieben die Zugriffsrechte ebenso wie allen anderen Nutzern verwehrt.

Denkbar wäre auch eine Lösung in Form eines **Postfachs mit zwei oder mehreren Schlüsseln** unter geteilter Verfügungsgewalt. Zum Öffnen eines solchen Dokumentensafes, zu dem die Bezeichnung „virtuelles Schließfach“ besser passen würde, reicht ein Schlüssel oder ein Nachschlüssel. Jeder Nutzer eines Schlüssels hat vollen lesenden und schreibenden Zugriff auf die Inhalte dieses Safes. Sollte es für verschiedene Rollen verschiedene Arten von Schlüsseln geben, etwa einen Schlüssel für den Inhaber, einen für seinen Steuerberater und einen für die Steuerverwaltung, so könnten Zugriffsberechtigungen durch den Inhaber gezielt vergeben werden. Bei einem Dokumentensafe würde dann der Inhaber Lese- und Schreibrechte, berechtigte Dritte aber ihrer Rolle entsprechend lediglich Leserechte auf den Safe erhalten. Im Falle einer Bürgerakte, die nach diesem Zugriffsmuster gestaltet ist, verfügt der Bürger über Lese- und Schreibrechte auf selbsterstellte Dokumente, aber nur über Leserechte

---

[18] Der Terminus „Schlüssel“ wird im Folgenden im Sinne eines unbedingt erforderlichen Zugangsöffners zum Safe verwendet, ohne den der Zugriff auf den Safe nicht möglich wäre.

auf Dokumente der Verwaltung, während zugangsberechtigte Verwaltungsmitarbeiter zwar Lese- und Schreibrechte auf Verwaltungsdokumente, aber lediglich Leserechte auf Dokumente Dritter erhalten.

Aus Datenschutzerwägungen heraus ist der Postfachansatz, bei dem Bürger sämtliche Dokumente und Daten ihres Safes einem Dritten freigeben, als nicht realisierungsfähig einzuschätzen. Obwohl sich Zugriffe auf den Safe protokollieren lassen, könnten die Schlüssel auch ohne Einverständnis der Inhabers an Dritte weitergereicht werden. Dieser Ansatz eignet sich eher für die in Safes einlegbaren und zur Datenübermittlung einsetzbaren Datencontainer, auf die mehrere Personen entsprechend ihrer Rolle und mit vorhandener Zugriffsberechtigung zur Erfüllung bestimmter, vorher definierter Aufgaben, etwa die Bearbeitung einer Steuererklärung, zugreifen dürfen.

Potentielle Betreiber: Datennotare und Datentreuhänder

Entscheidend für die Akzeptanz solcher elektronischen Angebote ist die Person oder die Organisation des Betreibers. Nur wenn die Nutzer elektronischer Dokumentensafes einem Anbieter vertrauen und sich sicher sind, dass dieser in ihrem Sinne sorgsam und bedächtig mit den ihm anvertrauten elektronischen Dateien umgeht, werden sie solche Angebote für die Speicherung ihrer persönlichen wie öffentlichen Daten überhaupt nutzen. Dies macht vertrauensfördernde Maßnahmen auf Seiten des Safebetreibers erforderlich. Die Veröffentlichung von Richtlinien zum Umgang mit anvertrauten Kundendaten wäre dazu ein wesentlicher Schritt. In einer Datensicherheitsrichtlinie sollte festgehalten werden, mit welchen Maßnahmen die Sicherheit der Datenbestände bei potentiellen Gefährdungen zu gewährleisten ist. In der Datenschutzrichtlinie finden sich die Rahmenbedingungen und erforderlichen Aktivitäten des Anbieters zum Schutz der Privatsphäre und der persönlichen Daten der Kunden. Die Einrichtung passwortgeschützter Zugangssperren, die automatische Protokollierung jedes Zugriffs und Quittierungen erfolgreich über den Dokumentensafe durchgeführter Transaktionen zählen zu weiteren wichtigen funktionalen Ergänzungen. Große Bedeutung sollte auch der Nennung persönlicher Ansprechpartner und der Sicherstellung ihrer ständigen Erreichbarkeit zugemessen werden. Die Einhaltung dieser Maßnahmen kann

ein unabhängiges Institut zur Qualitätssicherung in regelmäßigen Abständen prüfen und durch ein Qualitätssiegel zertifizieren.[19]

Viele Informations- und Kommunikationstechnologieunternehmen kommen als Betreiber elektronischer Dokumentensafes in Betracht. Jedoch können nicht alle potentiellen Betreiber das erforderliche hohe Sicherheits- und Vertrauensniveau überhaupt anbieten. Unter Umständen muss sogar ein ganz neuer Typ von Safebetreiber geschaffen werden. Bei diesen, in ersten Überlegungen[20] **„Datennotare“** oder **„Datentreuhänder“** genannten Betreibern elektronischer Dokumentensafes könnte es sich um staatlich autorisierte, in ihrer Funktion wie Notare, Rechtsanwälte, Ärzte oder Steuerberater mit einem Vertrauens- und Geheimnisschutz ausgestattete Mittler handeln, die zwar vom Staat in Ihrer Funktion kontrolliert werden, auf deren Datenbestände öffentliche Stellen aber keinen Zugriff haben. Solche Modelle erfordern ein tragfähiges, rechtliches Fundament und eine ausgereifte technische Plattform, die allen Ansprüchen an elektronische Dokumentensafes gerecht wird.

Frühzeitig sollte von Überlegungen zu einer monopolartigen Situation eines einzigen Datentreuhänders Abstand genommen werden. Das Safekonzept besitzt für das Produktportfolio vieler Organisationen und Unternehmen einen hohen strategischen Stellenwert. Die öffentliche Verwaltung könnte über einen elektronischen Dokumentensafe Zustellung und Aufbewahrung elektronischer Verwaltungsdokumente sicherstellen. Der Datensafe wäre auch ein lukratives Geschäftsfeld für Telekommunikationsunternehmen, Banken und Sparkassen, Identitätsmanagementanbieter und Online-Dienste. Diese könnten ihre etablierten Geschäftsfelder um ein zusätzliches Angebot ergänzen, durch dessen Funktionalität sich Verbundeffekte realisieren lassen. Da Kunden mit der Einrichtung eines Safes, einem Portal ähnlich, erhebliche und nicht rückerstattbare Lern- und Anpassungs-aufwendungen[21] tätigen müssen, kommt für sie ein weiterer Anbieterwechsel eher seltener in Frage. Die so verstärkte Kundenbindung festigt die Marktposition des Anbieters gegenüber der Konkurrenz. Der Safe bietet weitere Mehrwerte. Rechnungen und Depotauszüge brauchen

---

19 Vgl. Gant/Gant 2002, S. 7 und S. 20.

20 Erste Anregungen und Überlegungen zu Datennotaren erhielt der Autor im Herbst 2002 in Gesprächen mit Hans-Joachim Heusler und Sayeed Klewitz-Hommelsen (Klewitz-Hommelsen 2003, S. 159). Sayeed Klewitz-Hommelsen führte im Sommersemester 2003 mit Heinrich Reinermann an der DHV Speyer und der Fachhochschule Bonn-Rhein-Sieg eine Arbeitgemeinschaft zum Thema „Neue Formen der Haltung persönlicher Daten - neues Datenschutzrecht“ durch.

21 Vgl. Fink 2002, S. 28 ff.

künftig nur noch in elektronischer Form und über den Safe zugestellt werden. Zugleich ließe sich die E-Mail- und Ablagefunktionalität qualitativ aufbessern.

Folgerichtig werden sich mehrere Anbieter mit eigenen, zum Teil vermutlich proprietären Lösungen am Markt positionieren. Ausgehend vom Konzept der Notare könnte es sogar viele, lokal tätige Datennotare geben, die sich die erforderliche Hard- und Softwareplattform bei einem Entwicklungspartner einkaufen oder mieten und selbst Kunden akquirieren. Lokalität würde dann wichtig sein, wenn gesetzliche Anforderungen eine einmalige persönliche Registrierung und Identifizierung des Nutzers beim Datennotar erforderlich machen oder Datennotare persönliche Kontaktstellen (Datenkanzleien, Kundenbüros) einrichten müssen. Unternehmen, die elektronische Datensafes entwickeln und programmieren, könnten ihr Konzept mit anderen Produkten (Hard- und Software, Netzwerke, Internetzugang oder sonstige Rechenzentrumskapazitäten) zu einem Paket zusammenschnüren und an mehrere, als Datennotare tätige Partner lizenzieren. Erreichen diese Datentreuhänder rasch die Gewinnschwelle, sichert sich der Entwickler eine regelmäßige Einnahmequelle. Das Lizenzmodell bietet sich insbesondere für Unternehmen in monopolähnlichen Marktpositionen an, die auf Grund öffentlich bekannt gewordener Sicherheitslöcher viel Vertrauen verloren haben oder bei denen sich direkte wirtschaftliche Aktivitäten auch in diesem Bereich als imageschädigend auswirken könnten. Denkbar wäre es allerdings, dass diese Unternehmen selbst als Datentreuhänder aktiv werden. Langfristig wird mit einer Konsolidierung der Datennotare zu rechnen sein. Daher ist davon auszugehen, dass sich vor allem führende IT-Unternehmen in diesem Bereich engagieren und durchsetzen werden.

Preismodelle für kommerzielle Dokumentensafes

Potentielle Nutzer werden sich in Zukunft zwischen verschiedenen Safeanbietern entscheiden können. Dank des zwischen den Anbietern herrschenden Wettbewerbs werden sich die elektronischen Dokumentensafes technisch und funktionell weiterentwickeln. Preis und Funktionalität spielen für die Akzeptanz eine wesentliche Rolle. Zu einer raschen und weiten Verbreitung wird erfahrungsgemäß die kostenlose Freigabe eines Safedienstes führen.[22]

---

[22] Beispiele für kostenlos verfügbare Software, um eine weite Verbreitung eines Produktes zu erreichen, sind die Webbrowser Netscape Navigator (http://www.netscape.com/computing/download) und der

Denkbar wäre eine Vollfinanzierung über Werbung oder Sponsoren. Alternativ eröffnet sich auch die Möglichkeit eines entgeltfreien Basisdienstes und eines kostenpflichtigen Premiumdienstes. Die zweite Variante würde lediglich über eine Basisfunktionalität mit wesentlichen Standarddiensten und einen begrenzten Speicherplatz von nur wenigen Megabytes verfügen. Ein solcher Basisdienst ließe sich im Sinne eines Add-Ons in Online-Angebote Dritter integrieren, die für diesen Dienst eine monatliche Lizenzgebühr an den Safebetreiber entrichten müssten. Umgekehrt könnten Unternehmen wie Telekommunikationsnetzbetreiber, Wertpapierhändler oder Banken dem Safebetreiber etwas dafür zahlen, wenn ihre Kundenkontenführung elektronisch über den Dokumentensafe abgewickelt und auf den Versand papierförmiger Dokumente verzichtet werden würde. Der Dokumentensafe wäre dann in eine Hard- und Softwareplattform aus Formularserver, Virtueller Poststelle, Statusverfolgungssystem, Akteneinsicht und Zustellserver einzubinden.

Für alle zusätzlichen Mehrwertdienste müssten die Nutzer selbst zahlen. Zur Sicherung langfristiger konstanter Einnahmen eignet sich vor allem eine monatliche Abonnementgebühr, die in Abhängigkeit zum Datenvolumen des Safes steht. Entsprechende Preismodelle werden von Hostinganbietern seit längerem verwendet, können daher als akzeptiert gelten und sollten entsprechend der Nachfrage und Zahlungsbereitschaft kalkuliert werden. Vorgefertigte Ordnungsmuster für den Safe oder Safeverzeichnisse (elektronische Patientenakte, elektronische Reisedokumente), die interessanterweise vom Betreiber nur einmalig zu erstellen und vielfach verkauft werden könnten, zugleich dem Nutzer einen immensen Mehrwert liefern, versprechen besonders überdurchschnittliche Erträge. Diese Spezialangebote könnten zu höheren monatlichen Festpreisen, dafür mit nahezu unbegrenztem Speicherplatz lanciert werden. Für die Einrichtung von speziellen Datencontainern zur Erledigung einer bestimmten Angelegenheit, etwa zur Steuererklärung, zum Bauantrag oder zum Umzug, ließe sich jeweils eine einmalige Gebühr verlangen. Ebenso wäre es denkbar, für Premiumdienste wie das Identitätsmanagement, die Bereitstellung von Signierfunktionen, von Zweitschlüsseln für Vertrauenspersonen, für zusätzlichen virtuellen Speicherplatz auf einem Webserver oder für Beratungsdienste gesonderte Preise festzusetzen.

Microsoft Internet Explorer (http://www.microsoft.com/windows/ie/default.asp), die Audioplayer RealPlayer (http://www.real.com), Windows MediaPlayer (http://www.microsoft.com/windows/windowsmedia/players.asp) und Apple's Quick Time (http://www.apple.com/quicktime) sowie das Betriebssystem Linux.

Chancen und Risiken elektronischer Safes

Die Akzeptanz solcher Preismodelle hängt stark vom Nutzen für die Konsumenten ab. Elektronische Dokumentensafes bringen in erster Linie Bürgern, aber auch der Verwaltung oder der Wirtschaft einen erheblichen Mehrwert. Bürger können ihre eigenen Dokumente im elektronischen Original oder als elektronische Kopie des papierförmigen Originals vor Verlust schützen, in dem sie diese in einen virtuellen Safe bei einem Spezialisten für die Aufbewahrung elektronischer Dokumente ablegen. Dieser verfügt nachweislich über ausreichende Serverkapazitäten und Sicherheitsmechanismen, durch die selbst bei technischen Ausfällen der Zugriff auf den Safe und seinen Inhalt jederzeit möglich wäre. Zugriffsberechtigungen können vom Safeinhaber für den ganzen Safe oder Teile davon frei vergeben werden. Gegen einen unbefugten Zugriff sind die Safes über eingebaute Sicherheitsmechanismen geschützt. Die Nutzer dieser Safedienste müssen sich nicht um technische Aspekte der Speicherung und der Aktualisierung der Speichermedien kümmern. Zugleich übernehmen sie wichtige Elemente des Datenschutzes eigenverantwortlich. Der Safeinhaber selbst entscheidet, welche seiner privaten, persönlichen und welche seiner öffentlichen Daten er welchen Stellen zur Verfügung stellt. Er bleibt sozusagen der „Herr über seine Daten“. Gleichzeitig verfügt er mit einer solchen Lösung über vielfältige Import- und Exportfunktionen. Mit einem elektronischen Dokumentensafe können die Vorteile elektronischer Dokumente richtig ausgeschöpft werden. Dazu zählen schnelles Durchsuchen und Wiederauffinden von Dokumenten, schnelle Übermittlung an Dritte, jederzeitige Verfügbarkeit unabhängig von Zeit und Raum und eine komfortable Handhabung. Dokumente müssten aus Sicherheits- und Nachweiserwägungen nicht mehr ausgedruckt und archiviert werden. Auch diese Aufgabe übernimmt der Safe.

Einen besonders hohen Mehrwert bietet die Einbindung des Dokumentensafes in die Abläufe der öffentlichen Verwaltung. Gerade elektronische Verwaltungsakten- und Bürgeraktensysteme erhalten durch den Dokumentensafe ein adäquates Gegenstück auf Seiten der Bürger. Der Dokumentensafe übernimmt quasi die Funktion eines Dokumentenmanagementsystems für jeden einzelnen Bürger. Seinem Safe kann der Bürger vertrauen, kann ihn selbst pflegen und nach seinen Vorstellungen einsetzen. Elektronische Anträge, Zwischenstatusmeldungen, Bescheinigungen, Registerauszüge und Bescheide lassen sich jederzeit im Safe ablegen. Auf sie könnte später zurückgegriffen werden. Der Dokumentensafe kann zudem zum Portal für

den Zugriff auf Bürgerakten werden, falls sich entsprechende Angebote der Verwaltung in Drittanwendungen integrieren lassen. Intelligente Zusatzfunktionen wie die kombinatorische Suche oder der Hinweis auf ablaufende Fristen und Fälligkeitstermine bringen zusätzlichen Mehrwert. Der Safe wird allein durch diese Funktionen und die damit gewonnene Transparenz einen wesentlichen Schritt dazu beitragen können, dass die Bürger stärkeres Vertrauen in elektronische Angebote der Verwaltung setzen und diese letztendlich nutzen werden. Zugleich haben die Bürger die Gewissheit, dass die Verwaltung im Gegensatz zur Bürgerakte nicht auf ihre persönlichen Datenbestände und Anmerkungen zugreifen könnte.

Aus Verwaltungssicht sprechen weitere Gründe für eine rasche Einführung. Eine integrierte Empfangsfunktionalität im Safe vereinfacht die elektronische Zustellung und stellt diese sogar ortsunabhängig sicher. Ein vollständiger elektronischer Zugang zu Verwaltungsleistungen und Verwaltungsdiensten ließe sich durch eine gemeinsame Installation des Safes mit elektronischen Formularservern, Aktenmanagement- und Vorgangsbearbeitungssystemen erzielen, eine wesentliche infrastrukturelle Voraussetzung für einen breiten Einsatz von Electronic Government. Anträge könnten dann vollständig elektronisch entgegen genommen, bearbeitet und beschieden werden, ohne dass im Verwaltungsverfahren noch Papier unbedingt erforderlich wäre. Über spezielle Datencontainer ließe sich ein geschützter Datenaustausch zwischen Bürger und Verwaltung sicherstellen. In diesen, für verschiedene Zwecke normierten Containern könnten jene Dokumente oder Stammdaten abgelegt werden, die für die Bearbeitung eines Verfahrens aus Sicht der Verwaltung und des Bürgers erforderlich wären. Nur die mit einer Zugriffsberechtigung ausgestatteten Verwaltungsbeschäftigten dürfen auf die beim Datennotar gelagerten Container zugreifen, die für die Bearbeitung eines Verwaltungsverfahrens erforderlichen Daten oder Dokumente entnehmen und in die Verwaltungsakte einfügen. Ein solches Vorgehen vereinfacht die Kommunikation zwischen Verwaltung und Bürger erheblich, reduziert den gemeinsamen Abstimmungsaufwand und könnte so die Durchlaufzeiten der Verfahren senken.

Visionäre wie Heinrich Reinermann können sich sogar vorstellen, dass die Speicherung der Bürgerdaten in öffentlichen Datenbanken und Registern durch die Möglichkeit der Datensafes vollständig in die Verantwortung der Bürgern übertragen werden könnte. Der Staat wäre dann von der Datenhaltung befreit und riefe nur noch im Bedarfsfall die erforderlichen Angaben aus einem, für diesen Zweck bereit gestellten öffentlichen Datencontainer des Bürgers ab.

Pflege und Aktualisierung der Daten lägen in der Verantwortung des Bürgers. Dies klingt einerseits und insbesondere aus Datenschutzaspekten verlockend.[23] Andererseits stellt sich rasch die Frage, ob Staat und Verwaltung bei Entscheidungen auf in eigener Regie gesammelte und aufbereitete Entscheidungsgrundlagen verzichten möchten oder dürfen. Wichtige Anforderungen an Aktensysteme, etwa in den Bereichen Zuverlässigkeit, Verfügbarkeit und Verständlichkeit, könnten in ungünstigen Fällen nicht mehr gewährleistet werden. Daher müssen bei einer vollständigen Verlagerung sehr hohe Anforderung an die zu verwendenden elektronischen Dokumentensafes gestellt werden.

Elektronische Datensafes bergen in sich aber auch Risiken. Ausgehend von der Fragestellung, was geschehen kann, falls Unbefugte auf die Inhalte des Safes zugreifen können, müssen in die Konzeption vielfältige Sicherheitserwägungen einfließen. So ist zu klären, wie gewährleistet werden kann, dass nur der Nutzer einen Schlüssel zum Safe hat und Nachschlüssel nicht angefertigt werden können.[24] Ebenso muss geklärt sein, wie dem rechtmäßigen Inhaber eines Dokumentensafes bei Verlust des Schlüssels ein angemessener Zugang zu seinen Datenbeständen wieder ermöglicht werden kann.[25] Die Zentralisierung von persönlichen Datenbeständen steigert zudem die Gefahr, als Anbieter elektronischer Dokumentensafes schnell ins Visier weltweiter Hackergruppen zu geraten. Diese werden mit diversen Ansätzen und Techniken versuchen, die vorhandenen Sicherheitsmechanismen und Firewalls zu überwinden. Schließlich gilt es aus ihrer Sicht zu beweisen, dass doch noch Sicherheitslöcher in der eingesetzten Firewall bestehen und dass aus Datenschutzerwägungen die Speicherung persönlicher Daten in öffentlichen und ungesicherten Netzen wie dem Internet immer noch als „sehr leichtsinnig“ einzustufen sei. In der Tat kann trotz aller ergriffener Sicherheitsmaßnahmen niemals ein hundertprozentiger Schutz vor unbefugten Zugriffen gewährleistet werden. Durch geeignete Maßnahmen sollte daher sichergestellt werden, dass die Aufwendungen für Hacker, bestehende Schutzmechanismen auszuhebeln, in keinem Verhältnis zu den möglichen Vorteilen einer unbefugten Einsichtnahme stehen. Aus diesem Grund ist der Sicherheits-

---

23 Der betroffene Bürger müsste sich eigenverantwortlich um den Umgang mit seinen persönlichen Daten kümmern, würde quasi vom Objekt des Datenschutzes zum handelnden Subjekt mutieren. Vgl. Gerhold/Heil 2001, S. 382 f. Im Sinne eines möglichst weitreichenden Selbstdatenschutzes hätte er so stets die Verfügungsgewalt über seine Daten inne. Vgl. Hansen/Rost 2002, S. 265. Allerdings sollte auch berücksichtigt werden, dass aus technischen, intellektuellen oder sonstigen Gründen nicht jeder Bürger zu einem Selbstdatenschutz in der Lage ist.

24 Vgl. BigBrother Awards 2001.

25 Vgl. Posch/Menzel 2002, S. 146.

technologie innerhalb des Angebots besondere Bedeutung beizumessen. Diese Thematik darf auf keinen Fall unterschätzt werden, denn mit jeder aufgedeckten Sicherheitslücke entsteht ein erheblicher Vertrauensverlust, der in den seltensten Fällen wieder zu beheben ist.

Weitere Risiken aus der langfristigen Perspektive birgt der Konkurs beziehungsweise die Geschäftseinstellung eines Datennotars, eine Betriebseinstellung des dahinterliegenden externen Rechenzentrums und die Einstellung des Softwaresupports durch das Entwicklungsteam. Für alle diese Szenarien müssen im Vorfeld Notfallpläne mit Handlungsanleitungen vorbereitet werden, um allen in virtuellen Schließfächern befindlichen Dokumenten Datenschutz und Datensicherheit garantieren zu können. Explizit sind Anweisungen vorzubereiten, damit eine Überführung der Datenbestände in ein standardisiertes Drittsystem selbst bei völliger Zahlungsunfähigkeit des Betreibers gewährleistet werden kann.

Vorhandene, aber lösbare Problemfelder

Wie diese aufgezeigten Problemdimensionen zeigen, sind derzeit noch einige Fragen rund um den elektronischen Dokumentensafe ungeklärt und verlangen nach Lösungen. Zum Teil müssen noch die rechtlichen Rahmenbedingungen geschaffen, datenschutzrechtliche Erwägungen in die Konzeption miteingebaut, die Technologie weiterentwickelt, das Interesse bei potentiellen Anwendern geweckt und geeignete Betreiber gefunden werden.

Sollte das Konzept des Datennotars auf politischer Ebene breite Zustimmung erhalten, gilt es, über das Gesetzgebungsverfahren die Rahmenbedingungen für die Tätigkeit der Datentreuhänder derart zu gestalten, dass sich Aktivitäten aus wirtschaftlichen Erwägungen heraus rentieren. Dabei sind auch die berechtigten Interessen des Datenschutzes mit einzubeziehen. Datenschützer stehen dem Konzept eines ausschließlich vom Bürger gesteuerten Safes in Kombination mit Datencontainern durchaus aufgeschlossen gegenüber.[26] Zu überlegen wäre beispielsweise, ob die Safes, die über einen längeren Zeitraum nicht genutzt werden, nach einem Hinweis an den Inhaber automatisch gelöscht werden dürfen. Dies würde Datenfriedhöfe vermeiden, andererseits den Komfort mindern und eine Form der Überwachung implizieren.[27]

---

[26] Vgl. Accenture 2002b, S. 13 und Klewitz-Hommelsen 2003, S. 159.
[27] Vgl. KDBL 2003, S. 41.

Auch die Sperrung des Zugangs durch den Betreiber, etwa im Falle von Rechtstreitigkeiten, illegalen Aktivitäten des Safeinhabers mit seinem Safe oder Zahlungsversäumnissen des Nutzers, bedarf gesetzlicher Grundlagen. Zudem sind Lösungsansätze erforderlich, wie nach dem Tod des Inhabers (und dem damit unter Umständen verbundenen Verlust des Schlüssels) seinen Erben der Zugang zum Safe gewährleistet werden kann.

Für eine praktische Umsetzung des virtuellen Dokumentensafes und seiner Funktionalitäten wird die grundlegende Technologie zunächst entwickelt und programmiert werden müssen. Dies ist eng mit der Entwicklung elektronischer Dokumente und elektronischer Urkunden verbunden. Darüber hinaus sollte im Sinne eines Mehrkanalansatzes sichergestellt werden, dass der Bürger nicht nur über den direkten elektronischen Kanal, also über das Internet, das interaktive Digitalfernsehen oder UMTS-Dienste, auf den Safe zugreifen kann. Ebenso notwendig wäre ein sprachtelefonischer Zugang, beispielsweise über einen Sprachcomputer, der im Safe befindliche Dokumente vorlesen kann und sich mittels Sprachbefehlen steuern lässt, und ein persönlicher Zugang über die „Kundenbüros“ oder „Datenkanzleien“ der Datennotare. Für die Übermittlung von Dokumenten an und aus einem Safe werden eigene technische Standards erforderlich sein. Falls zwischen zwei Safes Dateien oder Datencontainer nicht direkt über das FTP-Protokoll ausgetauscht werden können, steht jedem Anwender immer noch eine manuelle Zwischenspeicherung auf dem eigenen Rechner als temporäre Zwischenlösung für Down- und Upload zur Verfügung. Problematischer wird es, wenn der Safe als Briefkasten verwendet werden soll. Neben neuartigen, zunächst aber proprietären Adressierungssystemen für elektronische Dokumentensafes könnte auch die E-Mail-Adresse bei Zustellungen eine wichtige Rolle spielen, da sie sich als Adressierungselement in der elektronischen Korrespondenz bereits bewährt hat. Denkbar wäre ebenso ein EDI- oder XML-basierter Datenaustausch zwischen den Dokumentensafes. Benötigt werden hier nicht viele bilaterale Austauschprotokolle zwischen jeweils zwei Safeanbietern, sondern ein weltweiter einheitlicher Standard für eine vom Anbieter unabhängige Zustellung. Ebenso wird erheblicher Aufwand in die Programmierung und Integration von Verschlüsselungs- und Signierfunktionen, in das Identitätsmanagementsystem, in die Protokollierung von Zugriffen, in (anonyme) Bezahlverfahren und die Datencontainer zu stecken sein. Große Anstrengungen erfordern Konzeption und Umsetzung der Berechtigungskonzepte für den Zugriff auf die Safes. Aufwändig wird die Verwaltung der Berechtigungen sein, da es durch Kündigungen,

Versetzungen, Urlaubs- und Krankheitsvertretungen zu einer hohen Fluktuation auf Seiten der zum Zugriff berechtigten Organisationen kommen kann.[28]

Zur Steigerung des Interesses bei den potentiellen Nutzern eines elektronischen Dokumentensafes sind Marketingmaßnahmen erforderlich. Schließlich darf nicht erwartet werden, dass Bürger ihre persönlichen Daten bei einem, ihnen unbekannten Unternehmen oder Datennotar hinterlegen, in die sie bisher kein Vertrauen gefasst haben. Dieses Vertrauen muss über zielgerichtete, vertrauensfördernde Maßnahmen geschaffen und mit Hilfe einer Werbekampagne in die Öffentlichkeit kommuniziert werden. Ebenso sollten potentielle Nutzer über die Vorzüge eines elektronischen Datensafes für ihr persönliches Umfeld informiert werden. Dazu eignen sich Fallbeispiele zu bereits umgesetzten Anwendungen, etwa der Verlust der Brieftasche, eine internationale Flugreise mit Hotelreservierung, ein Bauantrag, eine Steuererklärung oder die elektronische Patientenakte. Bedenken, Blockaden, Misstrauen und Desinteresse in den Köpfen der Bevölkerung müssen abgebaut werden. Eine frühe Einbindung der Datenschützer in die Entwicklung von Dokumentensafes würde helfen, weitere, bisher noch nicht artikulierte Bedenken bereits frühzeitig zu erkennen.

Für den technischen und organisatorischen Betrieb virtueller Datensafes gibt es verschiedene Optionen. Staatliche Auftrags- und Fördermittel könnten bei einem Anbietermangel die Programmierung eines Dokumentensafes anstoßen. Sobald sich eine Organisation für ein (wirtschaftliches) Engagement im Geschäftsfeld „elektronischer Dokumentensafe“ entschlossen und ein Produkt am Markt positioniert hat, entscheidet die Nachfrage über Erfolg und Misserfolg. Fehlendes Vertrauen der Bürger in solche Angebote könnte sich aber als fatal auswirken. Insofern würde gerade die erforderliche Unabhängigkeit eines Betreibers von Dritten unter gleichzeitiger staatlicher Aufsicht für das Konzept der Datennotare sprechen. Ob es aber gelingen würde, ein flächendeckendes Netz aus Datentreuhändern aufzubauen und dieses langfristig am Leben zu halten, ist gegenwärtig nicht abzusehen.

---

[28] Vgl. Eifert/Püschel/Stapel-Schulz 2003, S. 87 ff.

Erste Umsetzungen zu elektronischen Dokumentensafes

Die öffentliche Verwaltung sollte aus dem Blickwinkel der sicheren Zustellung ihrer Dokumente ein erhöhtes Interesses an der Einführung elektronischer Dokumentensafes haben. Vorschläge zur Einrichtung kamen bereits im Jahr 2000 aus Österreich (Amtshelfer Online)[29] und im Folgejahr aus Frankreich (Mon.Service-Public.fr)[30]. In Frankreich erntete das Konzept, das eine Umsetzung bis 2005 vorsieht, erheblich Kritik. Dem Initiator wurde 2001 der „Big Brother Award France“[31] verliehen, da mit einem solchen vorgeschlagenen Konzept erhebliche Unsicherheiten verbunden seien. Auch im irischen Konzept des Public Services Brokers/Reach ist ein „Personal Data Vault“ enthalten.[32] Diese bisher noch konzeptionellen Ansätze gehen über die Funktionalität einfacher Zustellserver oder Bürgeraktensysteme hinaus und setzen auf den Dokumentensafe als Kern des Identitätsmanagementsystems zur Stammdatenpflege. Die dänische Post bietet mit e-Boks seit 2001 eine komplette Safeinfrastruktur zum Empfang und Versand von elektronischen Dokumenten innerhalb Dänemarks an.[33] In Deutschland kam der entscheidende Entwicklungsantrieb zu einem sogenannten „Netsafe“ dagegen aus der Privatwirtschaft, bemerkenswerter Weise unter dem Aspekt elektronischer Dokumente. Im Juni 2000 wurde von der Bayerischen Hypo- und Vereinsbank AG, der Mannesmann AG (später Vodafone AG) und der IXOS Software AG das Unternehmen memIQ AG[34] mit dem Zweck einer intelligenten, webbasierten Dokumentenverwaltung und -zustellung gegründet. Zunächst sollten Kontoführungsbelege und Telefonrechnungen elektronisch versandt werden. In zwei Jahren konnten über 26.000 Kunden gewonnen werden. Das Unternehmen musste im August 2002, nach der Rücknahme von Finanzierungszusagen durch die Investoren, Insolvenz anmelden.[35] Die Deutsche Telekom AG[36] übernahm die entwickelte Technologie aus der Insolvenzmasse. Von Seiten der öffentlichen Verwaltung wird der Ansatz eines elektronischen Dokumentensafes in

---

29 Amtshelfer Online: http://www.help.gv.at. Vgl. Winter 2000, S. 55.
30 Service-public.fr: http://www.service-public.fr.
31 Big-Brother Awards France: http://www.bigbrotherawards.eu.org/2001/nomines/monservicepublic.html.
32 Reach – Personal Data Vault: http://www.reach.ie/about/psb/personal_data.htm. Vgl. Accenture 2002, S. 35.
33 E-Boks: http://www.e-boks.dk. Vgl. Accenture 2003, S. 36.
34 MemIQ AG: http://www.memiq.de. Diese Domain wurde mittlerweile eingestellt. Kopien des Web-Angebots sind über das Internet-Archiv verfügbar: http://web.archive.org/web/*/http://www.memiq.de.
35 Insolvenz im Heise.de Forum: http://www.heise.de/newsticker/foren/go.shtml?list=1&forum_id=32963.
36 Deutsche Telekom AG: http://www.telekom.de.

Deutschland bisher noch nicht verfolgt. Stattdessen haben die Einführung elektronischer Aktensysteme und die Generierung von Bürgerakten (etwa die „domap“[37] als Sieger des 6. Speyerer Qualitätswettbewerbes 2002)[38] eine höhere Priorität. Dies könnte sich aber in naher Zukunft ändern, wenn das Thema „Zustellserver“[39] auf die Agenda vieler E-Government-Aktivisten kommt und nach Alternativen zur elektronischen Verwaltungs- und Bürgerakte gesucht wird.

Obwohl die Vision eines echten elektronischen Dokumentensafes noch Zukunftsmusik darstellt, können sich interessierte Bürger bereits heute mit am Markt verfügbaren Dienstangeboten eigene Datensafes zusammenstellen. Beispielsweise lässt sich der verfügbare Webspace internetbasierter Anbieter von Hosting-, E-Learning oder Diskussionsforendiensten zur sicheren Ablage von Dateien verwenden. Über ein integriertes Mitgliedermanagement kann der Moderator solcher Dienste anderen Nutzern gezielt Zugriffsberechtigungen auf gespeicherte Daten erteilen oder entziehen. Sicherlich werden diese Angebote den Anforderungen an elektronische Dokumentensafes noch nicht gerecht, aber sie bedeuten einen ersten wichtigen Schritt zur Schaffung einer Nachfrage für Safeangebote.

Die bereits vorliegenden Erfahrungen kommerzieller Anbieter sollten genutzt werden, um die Entwicklung des Datensafes weiter zu forcieren und um dabei das Marktpotential sorgfältig abzuschätzen. Für eine Umsetzung der Vision in ein marktfähiges Produkt sprechen viele Gründe. Da Vertrauen für die Existenz der Dokumentensafes elementar ist, dürfen nach dem offiziellen Vertriebsbeginn allerdings weder technische Fehler noch prozedurale Mängel auftreten. Diese würden das Ende für das Produkt bedeuten. Somit sollte der offizielle Markteintritt nur mit einem wirklich ausgereiften Prototypen erfolgen. Ein Durchbruch des Konzeptes wird dann nicht lange auf sich warten lassen.

---

37 DoMap: http://www.domap.de. Dortmunder Systemhaus: http://www.dortmunder-systemhaus.de.

38 6. Speyerer Qualitätswettbewerb 2002: http://www.dhv-speyer.de/Qualitaetswettbewerb/6.%20Speyerer%20Qualitaetswettbewerb/6Qual.htm

39 Ein Zustellserver ist ein Server zur Sicherstellung der Zustellung eines elektronisch verschlüsselten Datencontainers mit darin enthaltenen elektronischen Dokumenten (Zustellstück) an einen Empfänger. Der Absender erhält bei erfolgreicher Zusendung eine Quittung in Form einer Zustellbestätigung.

Literaturverzeichnis

Accenture 2002: Accenture: eGovernment Leadership - Realizing the Vision, North Sydney 2002. Online: http://www.accenture.com/xdoc/en/industries/government/eGov_April2002_3.pdf [Stand: 29. April 2002].

Accenture 2002b: Accenture: Technology in Government – Riding the Waves of Change, The Government Executives Series, North Sydney 2002.

Accenture 2003: Accenture: eGovernment Leadership - Engaging the Customer, Washington 2003. Online: http://www.accenture.com/xdoc/en/industries/government/gove_capa_egov_leadership.pdf [Stand: 17. Juni 2003].

Beyer 1986: Beyer, Lothar: Wandel der Strategien und Kontinuität der Folgeprobleme – Automation im Einwohnerwesen, in Grimmer, Klaus (Hrsg.): 1986, Informationstechnik in öffentlichen Verwaltungen – Handlungsstrategien ohne Politik, Birkhäuser Verlag, Basel, Boston Stuttgart 1986, S. 122 – 232.

Big Brother Awards 2001: Big Brother Awards France: Mon service Public, Bigbrotherawards.eu.org, Paris 2001. Online: http://www.bigbrotherawards.eu.org/2001/nomines/monservicepublic.html [Stand: 22. Mai 2003].

Daum 2002: Daum, Ralf: Die Rolle öffentlicher Unternehmen im Application Service Providing, in: ZögU - Zeitschrift für öffentliche und gemeinwirtschaftliche Unternehmen, Band 25, Heft 3, Nomos Verlag, Baden-Baden 2002, S. 263 – 276.

Denninger 2000: Denninger, Erhard: Nahtloser öffentlicher Sektor? Rechtsfragen der Informationsgesellschaft, in: Reinermann, Heinrich (Hrsg.): Regieren und Verwalten im Informationszeitalter – Unterwegs zur virtuellen Verwaltung, Schriftenreihe Verwaltungsinformatik, Band 22, R. v. Decker Verlag, Heidelberg 2000. S. 68 – 80.

DIB 2000: Arbeitsgruppe “Datenschutz in Bürgerbüros“: Vom Bürgerbüro zum Internet - Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung, Der Landesbeauftragte für den Datenschutz Niedersachsen, Hannover 2001. Online: http://www.lfd.niedersachsen.de/dokumente/bürgerbüro.pdf [Stand: 23. Oktober 2001].

Eifert/Püschel/Stapel-Schulz 2003: Eifert, Martin; Püschel, Jens-Ole und Stapel-Schulz, Claudia: Rechtskonformes E-Government – Antworten auf Kernfragen beim Bau eines virtuellen Rathauses, Bundesministerium für Wirtschaft und Arbeit und Hans-Bredow-Institut, Berlin und Hamburg 2003. Online: http://www.bmwi.de/Homepage/download/infogesellschaft/Rechtsratgeber.pdf [Stand: 3. April 2003].

Ellwein 1973: Ellwein, Thomas: Das Regierungssystem der Bundesrepublik Deutschland, Westdeutscher Verlag, 3. Auflage, Opladen 1973.

Fink 2002: Fink, Lars-Rüdiger: Economies of Aggregation – Internetportale als Informationsgüterbündel und die Zahlungsbereitschaft der Nachfrager, Dissertation, Universität Köln, Köln 2002.

Gant/Gant 2002: Gant, Diana Burley und Gant, Jon P.: Enhancing E-Service Delivery, in: Johnson, Craig L.; Gant, Diana Burley und Gant, Jon P.: State Web Portals – Delivering and Financing E-Service, Grant Report, The PricewaterhouseCoopers Endowment for the Business of Government und Indiana University, Bloomington 2002. Online: http://endowment.pwcglobal.com/pdfs/JohnsonReport.pdf [Stand: 30. Juli 2002].

Gerhold/Heil 2001: Gerhold, Diethelm und Heil, Helmut: Das neue Bundesdatenschutzgesetz 2001, in: DuD - Datenschutz und Datensicherheit, 25. Jahrgang, Heft 7, Vieweg Verlag, Wiesbaden 2001, S. 377 - 382.

Hansen/Rost 2002: Hansen, Marit und Rost, Martin: Datenschutz durch computergestütztes Identitätsmanagement, in: Kubicek, Herbert et al.: Innovation@Infrastruktur : Informations- und Dienstleistungsstrukturen der Zukunft - Jahrbuch Telekommunikation und Gesellschaft 2002, Hüthig Verlag, Heidelberg 2002, S. 255 – 268. Online: http://www.netzservice.de/Home/maro/mr_dsidman.html [Stand: 31. Januar 2003].

KDBL 2003: Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Datenschutzgerechtes eGovernment, Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Hannover 2003. Online: http://www.lfd.niedersachsen.de/functions/downloadObject/0,,c1358174_s20,00.pdf [Stand: 19. März 2003].

Klewitz-Hommelsen 2003: Klewitz-Hommelsen, Sayeed: Recht auf Anonymität – Oder Anspruch auf Transparenz?, in: DuD - Datenschutz und Datensicherheit, 27. Jahrgang, Heft 3, Vieweg Verlag, Wiesbaden 2003, S. 159.

Lenk 2002: Lenk, Klaus: Datenschutzprobleme bei integriertem Zugang zu Verwaltungsleistungen, in: DuD - Datenschutz und Datensicherheit, 26. Jahrgang, Heft 9, Vieweg Verlag, Wiesbaden 2002, S. 542 – 546.

LfD NRW 1999: Landesbeauftragte für Datenschutz Nordrhein-Westfalen: 14. Datenschutzbericht 1999, Landesbeauftragte für Datenschutz Nordrhein-Westfalen, Düsseldorf 1999.

Mehlich 2002: Mehlich, Harald: Electronic Government – Die elektronische Verwaltungsreform, Grundlagen – Entwicklungsstand – Zukunftsperspektiven, Betriebswirtschaftlicher Verlag Dr. Th. Gabler GmbH, Wiesbaden 2002.

Posch/Menzel 2002: Posch, Reinhard und Menzel, Thomas: Elektronische Signatur und Zustellung, in: Wimmer, Maria A. (Hrsg.): Impulse für e-Government – Internationale Entwicklungen, Organisation, Recht, Technik, Best Practices, Tagungsband zum ersten e|Gov Day des Forums e|Gov.at, Band 158, Österreichische Computergesellschaft, Wien 2002, S. 139 - 149.

Reinermann 2002: Reinermann, Heinrich: Internetportale in der öffentlichen Verwaltung - Die Neuordnung von Informationen und Geschäftsprozessen, in: Karl-Peter Sommermann und Jan Ziekow (Hrsg.): Perspektiven der Verwaltungsforschung - Beiträge zur Wissenschaftlichen Arbeitstagung aus Anlass des 25-jährigen Bestehens des Forschungsinstituts für öffentliche Verwaltung vom 8. bis 10. Oktober 2001 in Speyer, Schriftenreihe der Hochschule Speyer, Band 154, Duncker & Humblot, Berlin 2002, S. 127 - 137.

Reinermann 2002b: Reinermann, Heinrich: Transformation zu Electronic Government, in: Reinermann, Heinrich und von Lucke, Jörn (Hrsg.): Electronic Government in Deutschland, Ziele – Stand – Barrieren – Beispiele – Umsetzung, Speyerer Forschungsbericht, Band 226, Forschungsinstitut für öffentliche Verwaltung, Speyer 2002, S. 104 – 117.

Roßnagel 1999: Roßnagel, Alexander: Die digitale Signatur in der öffentlichen Verwaltung, in: Kubicek, Herbert et al.: Multimedia@Verwaltung - Jahrbuch Telekommunikation und Gesellschaft, Hüthig Verlag, Heidelberg 1999, S. 158 - 171.

SAP 2002: SAP Deutschland AG & Co. KG: IT-gestützte Vorgangsberarbeitung mit mySAP Public Sector, SAP White Paper, SAP Deutschland AG & Co. KG, Walldorf 2002.

Schreiber 2003: Schreiber, Lutz: Elektronisches Verwalten – Zum Einsatz der elektronischen Signatur in der öffentlichen Verwaltung, in Hoffmann-Riem, Wolfgang (Hrsg.): Schirften zur rechtswissenschaftlichen Innovationsforschung, Band 6, zugleich Dissertation an der Universität Hamburg, Nomos Verlagsgesellschaft, Baden-Baden 2003.

Winter 2000: Winter, Arthur: @mtshelfer online - www.help.gv.at - Das Portal zur öffentlichen Verwaltung, in: Reinermann, Heinrich und von Lucke, Jörn (Hrsg.): Portale in der öffentlichen Verwaltung, Forschungsbericht, Band 205, 2. Auflage, Forschungsinstitut für öffentliche Verwaltung, Speyer 2000, S. 54 – 70.