Datenschutzgerechtes Electronic Government

Gutachten

im Auftrag des
Landesbeauftragten für den Datenschutz Niedersachsen -

Bearbeitet von: **Prof. Dr. Alexander Roßnagel**
Nuriye Yildirim

Stand: **15. Januar 2002**

Inhaltsverzeichnis

„Electronic Government“ ist zum neuen, international gebräuchlichen Schlagwort in der Diskussion um die Modernisierung des Staates avanciert.[1] Die Entwicklungen des Internets haben erheblich dazu beigetragen. Es stellt unter den Multimediadiensten bei einer immer leistungsfähigeren globalen Infrastruktur mehr als ein Kommunikationsinstrument für wirtschaftliche, kulturelle und öffentliche Anwendungen dar. Es ist Exponent der neuen Evolutionsstufe des technischen, wirtschaftlichen und kulturellen Phänomens der grenzüberschreitenden Datenflüsse.[2] Bei der Online-Übertragung digitaler Informationsinhalte werden die Informationsnetze, die ursprünglich nur das Medium für die Datenübertragung waren, selbst zu einem globalen Markt.[3] Die öffentliche Verwaltung in Städten und Gemeinden muss mit dieser Entwicklung von Multimedia und Internet Schritt halten, um ihre Gestaltungsaufgabe auch zukünftig wahrnehmen zu können.

Damit geht die Frage einher, welche Risiken mit einer derartigen Online-Realisierung verbunden sind. Neben einer Vielzahl von Vorteilen für Bürger, Verwaltung und Wirtschaftsakteure bestehen insbesondere datenschutzrechtliche Bedenken. Worin diese in Bezug auf konkrete Anwendungsfelder in der Verwaltung bestehen und wie sie behoben werden können, ist Gegenstand der vorliegenden Untersuchung. Bereits im Vorfeld ist jedoch klar, dass die Einführung von Electronic Government und die mit ihr Ergebnisse einer tiefgreifenden Verwaltungsreform sich erst langfristig einstellen werden.[4] Der Weg zum virtuellen Rathaus wird ein Lernprozess für alle Beteiligte sein.

1. E-Government - Vorteile für Bürger und Behörden

Die Zahl der Internetnutzer ist in den letzten Jahren rasant gestiegen: Während 1998 etwa nur 7,5 Millionen Deutsche das Internet nutzten, betrug die Zahl der Nutzer 1999 11,2 Millionen und für das laufende Jahr werden 16 Millionen erwartet.[5] Das Internet gehört für die meisten der 15- bis 25-Jährigen schon sehr lange zum Alltag. Es bietet einen hohen Nutzen, ist preiswert und leicht zugänglich. Daher sollte es auch zum Alltag der Verwaltung und ihrer Beschäftigten gehören.[6] So hat der Bundeskanzler im September 2000 eine Initiative der Bundesregierung gestartet: Mit “BundOnline 2005“ hat sich die Bundesregierung im Dezember 2001 verpflichtet, bis zum Jahr 2005 alle internetfähigen Dienstleistungen der Bundesverwaltung – ca. 1.200 – über das Internet anzubieten, und ein deutliches Signal gesetzt.[7] Damit jedoch die Bundesverwaltung mit

---

1 *Eifert*, ZG 2/2001, 116 m.w.N. für internationale Beispiele.

2 *Grewlich*, RiW 1988, 695, vgl. auch *Jessen* 2001, 11.

3 *Grewlich*, K&R 1998, 81 A.

4 *Kubicek/Hagen* 1999, 7.

5 *Roßnagel* 2000b, 257 ff.

6 *Zypries*, Kommune21 2/2001, 12.

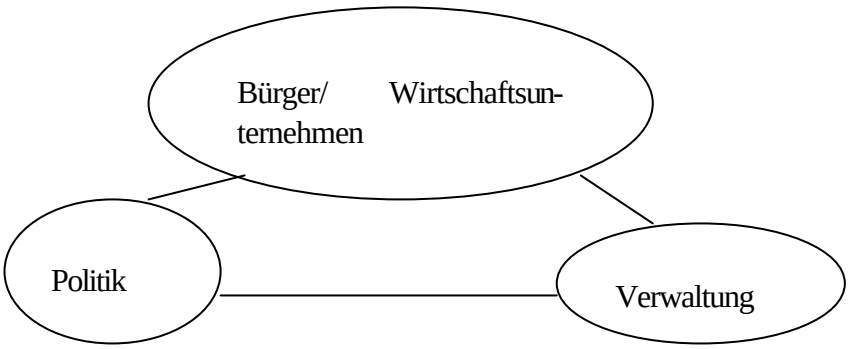
7 S. Beschluss der Bundesregierung vom 12.12.2001, http://www.staat-modern.de.

der Landes- und Kommunalverwaltung kooperieren kann, sind interoperable und kompatible elektronische Verfahren zwischen den Verwaltungsebenen erforderlich.[8] In den einzelnen Kommunen müssen dafür entsprechende Verfahren eingeführt werden.

1.1 Auf dem Weg zum Electronic Government

Die ersten Schritte für elektronische Verfahren und in Richtung virtuelles Rathaus liegen mehrere Jahre zurück. Bereits seit Anfang der neunziger Jahre wird in der Fachwelt vielfach darüber diskutiert, wie die Leistungsfähigkeit der Verwaltung an neue Herausforderungen und Rahmenbedingungen angepasst werden kann, um die einzelnen Verwaltungsabläufe zu verbessern. Die in diesem Bereich vorhandenen weltweiten Aktivitäten zur Organisations- und Managementreform sowie zur Vermarktlichung lassen sich unter der Bezeichnung „New Public Management" zusammenfassen. Niederländische Kommunen mit Tilburg an der Spitze setzten bereits die ersten Modernisierungsbausteine in diese Richtung (Tilburger Modell), an denen man sich auch in Deutschland seit 1990 orientierte. Es zeichnet sich immer mehr ein Übergang von einer am Bürokratiemodell orientierten Verwaltung auf eine Verwaltung ab, die nach den Grundsätzen des New Public Management oder der Neuen Steuerungsmodelle gestaltet wird. Es geht einerseits um die Neubestimmung der Rolle des Staates im Verhältnis zur Gesellschaft und zu seinen Bürgern, und andererseits um die Verbesserung der Leistungsfähigkeit staatlicher Institutionen durch eine Neugestaltung von Organisation und Management.[9]

Die Vorstellungen des Electronic Government gehen über das Konzept des „New Public Management" hinaus und entwickeln es weiter, indem sie den Fortschritt im IuK-Sektor in das Konzept integrieren.[10] Das Internet soll ein Forum für eine multimedial interaktive Kommunikation zwischen Verwaltung und Bürger (government-to-consumer) bzw. Verwaltung und Wirtschaft (government-to-buisness) bilden, ohne an räumliche, zeitliche und hierarchische Vorgaben gerichtet zu sein.[11]



Im Folgenden werden die Ziele und Vorteile des E-Government dargestellt:

---

8 *Zypries*, Kommune21 2/2001, 13; in Großbritannien soll ein einheitlicher Standard mit Interoperability Framework (e-GIF) geschaffen werden.

9 *Reichard*, VuF 2000, 171; Memorandum "Electronic Government", 6.

10 *Boehme-Neßler*, NVwZ 2001, 375.

11 Vgl. *Roßnagel* 2000b, 261; *Nedden*, DuD 2001, 64; Memorandum „Electronic Govemment", 2.

Bürger- oder Kundenfreundlichkeit

Der Bürger ist als Wähler und Steuerzahler daran interessiert, dass die öffentliche Hand Problemlösungen auf dem Stand des verfügbaren Wissens und der höchstmöglichen Produktivität zustande bringt. Soweit elektronische Netze dazu beitragen, haben sie auch einen positiven Einfluss auf Legitimation und Akzeptanz des Verwaltungshandelns.[12] Mit der elektronischen Verwaltung wird im Verhältnis Bürger und Verwaltung das Ziel verfolgt, Bürgern den Umgang mit der Verwaltung möglichst leicht und schnell zu ermöglichen und die Bürgerberatung über das Internet zu verbessern. Der Bürger wird in der Rolle des „Kunden", die Verwaltung in der Rolle des „Dienstleisters" betrachtet.[13] Der Bürger kann von zu Hause aus jeder Zeit das Verwaltungsangebot beanspruchen, ohne an bestimmte Öffnungszeiten gebunden zu sein. Der Einzelne ist also bei der Inanspruchnahme der Verwaltungsdienstleistungen weder orts- noch zeitabhängig: Nicht die Bürger, sondern die Daten sollen laufen.[14]

Durch die Netzpräsenz der Verwaltung kann der Bürger Informationen darüber bekommen, wer für welchen Verwaltungsvorgang zuständig ist, welche Unterlagen benötigt werden und wie der Stand der Bearbeitung ist. Neben dieser Leistungs- und Behördentransparenz wird darüber hinaus die Zahl der Anlaufstellen zum Verwaltungssystem erheblich reduziert.

Effizienzsteigerung

Das Internet bietet der Verwaltung eine Vielzahl von Möglichkeiten, ihre Arbeitsprozesse zu optimieren. Das elektronische Speichern von Daten ermöglicht einen jederzeitigen Zugriff durch jedermann, so dass die Mehrfacherfassung und Mehrfachaktualisierung von Daten obsolet wird. Im Gegensatz zu Papierdokumenten können zum Beispiel Änderungen ohne entscheidende Zeitverzögerungen vorgenommen werden und die Informationen somit auf dem aktuellen Stand gehalten werden. Durch die Vermeidung des mehrfachen Änderungsaufwandes können zugleich Fehler vermieden werden. Überdies entfällt das Warten auf Daten, weil sich die Akte etwa an einem anderen Arbeitsplatz befindet. Durch die Gewährleistung der Aktualität und Richtigkeit der Daten sowie des jederzeitigen Direktzugriffs auf diese dürfte ihre Nützlichkeit für die Mitarbeiter steigen, und damit auch deren Grad an Informiertheit sowie an Koordination.[15] Die Kommunikation mit dem Bürger kann in relativ kurzen Zeitabständen erfolgen, da zeitliche Verzögerungen durch Medienbruch, Suchen von Unterlagen sowie Transport entfallen. Der Verwaltungsmitarbeiter ist flexibel, weil er sich – genauso wie die Bürger – nicht an Öffnungszeiten orientieren muss.

Mit E-Government wird in den nächsten Jahren eine „Effizienzrevolution in der öffentlichen Verwaltung" erwartet, weil besonders günstige Bedingungen, nämlich „externer Druck, interner Zwang und technische Möglichkeiten", vorhanden seien.[16] Ziel ist es,

---

12 *Reinermann*, Verw. 1995, 12.

13 Dies kommt den Ideen des New Public Management sehr nahe.

14 Vgl. *Lenk* 2000, 84 ff.

15 *Reinermann*, Verw. 1995, 7.

16 *Rürup*, VM 2000, 266.

die unabdingbare Leistung, die nur durch Menschen erbracht werden kann, in höchstmöglichem Maße durch Informationstechnik zu unterstützen.[17]

Kostenersparnis

Die Effizienzsteigerung soll Kostenersparnisse auf Seiten der Verwaltung und der Bürger bringen. Denn in einer vernetzten Verwaltung entfällt eine Reihe von Kosten, die durch Papierdaten, Medienbrüche, durch Raumbedarf für Akten und Registraturen sowie für Boten- und weitere Hilfsdienste entstehen.[18] Darüber hinaus werden Kostenersparnisse durch die Reduzierung des Personalbestandes erwartet.[19] Allein 300.000 Papierformulare wurden im vergangenen Jahr falsch ausgefüllt oder einfach weggeworfen. Untersuchungen der Mummert + Partner Unternehmensberatung zufolge würde die Umstellung auf das Online-Formular eine Einsparung von bis zu 40 Mio. Mark ermöglichen.

Flexibilität der Behördenmitarbeiter

Ein großer Vorteil elektronischer Verwaltung besteht auch darin, dass sie die traditionellen Arbeitszeit-, Arbeitsort-, und Arbeitsteilungsregelungen auflockert. Der zeitunabhängige Zugriff und die zeitversetzte Kommunikation erfordern nicht die gleichzeitige Anwesenheit der Beschäftigten. Die Beschäftigten können sogar von beliebigen Orten aus auf die Datenbanken zugreifen und kommunizieren, so dass das Arbeiten in Außenstellen, zum Beispiel in Bürgerämtern, oder gar Teleheimarbeit möglich wird. Es ist zu erwarten, dass dadurch den Bedürfnissen aller Beteiligten weitgehend Rechnung getragen wird, da auf diesem Wege eine größere Individualisierung realisiert werden könnte.[20]

Demokratie

Durch die Nutzung des Internet kann der Einzelne stärker am politischen, sozialen und verwaltungstechnischen Geschehen beteiligt werden.[21] Die Vorstellungen hierzu erfassen nicht nur die Ersetzung der gegenwärtigen Wahlzettel oder der Briefwahl durch elektronische Stimmabgabe. Insoweit können schon derzeit die Wahlen zum Studierendenparlament der Universität Osnabrück beispielhaft erwähnt werden. Die Idee der E-Democracy geht weiter, da sie auch Elemente direkter Demokratie und neue Formen politischer Kommunikation (z.B. durch virtuelle Foren und Diskussionsräume für die Meinungsbildung) erfasst.[22] Inwieweit auf diese Weise materiell mehr Demokratie erreicht werden kann, werden gegenwärtige Pilotanwendungen zeigen.[23]

---

17 Memorandum “Electronic Government”, 11.

18 *Reinermann*, Verw. 1995, 7.

19 So jedenfalls *Kilian/Wind*, VerwArch 1997, 499 ff.; kritisch allerdings *Laux* 1997, 48 ff.

20 So jedenfalls *Reinermann*, Verw. 1995, 12.

21 *Boehme-Neßler*, NVwZ 2001, 375, der die nordschwedischen Stadt Kalix (www.kalix.se) als Beispiel aufführt.

22 BT-Drs. 13/11004, 83.

23 Zuversichtlich in dieser Hinsicht *Kubicek/Hagen* 1999, 234; *Rüß*, MMR 2000, 73 ff.; *Tauss* 1999, 291. Zustimmend und mit dem Hinweis auf damit verbundene Probleme *Eifert*, ZG 2/2001, 118. Nach *Noam* dagegen überwiegen die Gefährdungen und daher zweifelnd, vgl. Digitaler Schwindel,

Zusammenfassend können als Folgen der Internetnutzung der Verwaltung die Standortunabhängigkeit, die Zeitunabhängigkeit, die Vernetzung von Wissensressourcen und die Dynamisierung formaler Organisationsstrukturen genannt werden.

1.2 Erste Schritte zu einer elektronischen Verwaltung....

Die Möglichkeiten des Internets haben bereits zahlreiche Kommunen erkannt. Nach einer Studie der Mummert + Partner Unternehmensberatung verfolgen 91 Prozent der größten deutschen Kommunen das Ziel, E-Government-Verfahren zu realisieren oder setzen solche bereits ein.[24] Allerdings ist die Planung des elektronischen Bürgerservices so wenig konkret (47 Prozent verfügen über kein schriftliches Konzept), dass mit einer zeitnahen Realisierung nicht zu rechnen ist.[25]

Es gibt heute kaum noch eine Kommune, die sich nicht im Internet präsentiert.[26] Die bloße Präsenz im Internet stellt heute keine Aufwertung des Images der Stadt im Sinne der Fortschrittlichkeit dar.[27] Vielmehr gehört der Web-Auftritt der Kommune zu einem gängigen Standard und wird von den meisten Bürgern bereits vorausgesetzt. In den meisten Fällen (80 Prozent) handelt es sich allerdings um eine statische Homepage, die lediglich Informationen über Stadtgeschichte, Öffnungszeiten des Rathauses, Zuständigkeiten, Kontaktmöglichkeiten, Veranstaltungen und ähnliche Informationen anbietet. Kaum zu finden sind jedoch Angebote, die über eine solche einseitige Kommunikation hinausgehen.[28]

Die beidseitige Kommunikation zwischen Behörde und Bürger bzw. Unternehmen findet in der Regel über E-Mail statt, so dass einfache Bestellungen, zum Beispiel von Theaterkarten oder Mülltonnen somit möglich werden. Außerdem werden zur Beschleunigung der Verfahren Formulare zum Download bereit gestellt, die weiterhin ausgedruckt und auf dem Postweg geschickt werden müssen.

Die gegenwärtigen Internet-Angebote der Verwaltungen sind insoweit sehr weit von dem Konzept des E-Government entfernt.[29] Nach diesem sollen die vollständige Abwicklungen komplexer Verwaltungsdienstleistungen einschließlich der Signatur und der Bezahlfunktion erfasst werden.[30] Gemeint ist damit der gesamte „Workflow“ – also von der Antragstellung, über die Unterlagen, Beweisführung, Behörden- und Bürgerbeteiligung, die Aktenführung, die Verwaltungsentscheidung, die Zustellung bis hin zur be-

---

http://www.politik-digital.de/e-demokratie/forschung/digitalerschwindel.shtml, besucht im Juli 2001.

24 http://www.politik-digital.de/netzpolitik/egovernment/effiz_staat.shtml, besucht im Juli 2001.

25 Vgl. Studie “Kommunale Vorhaben der Verwatungsreform” von *Mummert + Partner*, www.mummert.de.

26 *Dieckmann* 1999, 68.

27 Nach den Informationen des DStGB haben von den rund 14.000 Städten zurzeit rund 2.5000 eine eigene Homepage.

28 *Lohmann*, VM 2001, 68.

29 So *Kubicek/Hagen* 1999, 19 ff.

30 In Bremen werden bereits erste Erfahrungen in diese Richtung im Bereich der An- und Ummeldung gemacht.

hördeninternen Dokumentation und Archivierung – ohne Medienbruch.[31] Dies bedeutet zugleich auch die Aufhebung der Papierakte und die Einführung der elektronischen Akte. In dem Wechsel von Papier auf elektronische Dokumente wird vielfach ein „Umbruch in der Verwaltungskultur" gesehen.[32] Die Umgestaltung auf die elektronische Akte muss aus rechtlicher Sicht verschiedenen Aspekten der Papierakte Rechnung tragen:

- Die elektronische Akte, ihre Verwaltung und Führung müssen sich an den Vorgaben der Papierakte orientieren, solange keine abweichenden Regelungen zur Führung von elektronischen Akten getroffen werden.

- Nach dem Gebot der Rechtsstaatlichkeit ist die gerichtliche Kontrolle eines- auch eines modernisierten- Verwaltungsverfahrens unabdingbar. Insoweit taucht die Frage auf, in welcher Form die „Unterlagen" auf einer Diskette zur gerichtlichen Kontrolle einzureichen sind.

- Der Rechtswirksamkeit eines elektronischen Dokuments steht dort, wo ausdrücklich eine eigenhändige Unterschrift vorgesehen ist, das Schriftformerfordernis de lege lata (noch) entgegen.

- Bedenken bestehen weiterhin hinsichtlich der Dokumentation von Verwaltungsabläufen zur nachträglichen Kontrolle. Eine vollständige, jederzeit verfügbare und fälschungssichere Dokumentation muss auch bei der elektronischen Akte gewährleistet sein.

1.3 Nicht ohne ausreichenden Datenschutz

Im Unterschied zur Offline-Welt bietet das Internet gerade auf der technischen Ebene zahlreiche Möglichkeiten, Informationen über den Betroffenen zu erhalten.[33] Jede Handlung hinterlässt Datenspuren, die grundsätzlich beobachtbar und registrierbar sind.[34] Die Nutzung der Informationstechnik erleichtert es, personenbezogene Daten von vielen Bürgern über alltägliches Verhalten, Einstellungen und Präferenzen sehr leicht und in großem Umfang zu sammeln.[35] Die bisher auf viele Fachämter (z.B. Meldewesen, Gesundheitsamt, Steueramt etc.) oder verschiedene Stellen (z.B. Kommunalverwaltung, Finanzamt, Banken) verstreuten Angaben zu einer Person können zusammengeführt und ein Persönlichkeitsprofil erstellt werden. Dadurch entsteht das Risiko, dass der Bürger durchsichtig, der Mensch gläsern wird.[36] Die Betroffenen haben nicht die Kenntnis und Kontrolle über Art, Umfang, Speicherort, Speicherdauer und Verwendungszweck der über sie erhobenen und gespeicherten Daten. Dies gewinnt an zusätzli-

---

31 Das Bundesverwaltungsamt sowie einige Dienststellen in Bayern stellen inzwischen grundsätzlich auf Workflow um.

32 *Roßnagel* 1999b, 160; *Reinermann* 2000, 14, *Hoffmann-Riem* 1998. 11 ff.

33 *Geis*, NJW 1997, 288.

34 *Köhntopp/Köhntopp*, CR 2000, 248 ff.; *Wiese* 1999, 9.

35 *Opaschowski* 1999, 184, spricht von Digitalvandalismus, Softwarepiraterie und Datendiebstahl.

36 *Lübking* 1992, 20.

chem Gewicht, wenn man sich vor Augen führt, dass eine Datenverarbeitung in einem grenzlosen Netz weltweit möglich ist.[37]

Zur Zeit scheitern tiefer greifende Transaktionen zwischen Verwaltung, Bürger und Wirtschaftsunternehmen bei Online-Abwicklungen im Verwaltungsverfahren noch an der fehlenden Rechtsverbindlichkeit und Vertraulichkeit, an dem mangelnden Datenschutz und der ungenügenden Datensicherheit. Sowohl Verwaltungen als auch die Bürger befürchten, dass vertrauliche Daten von Unbefugten eingesehen oder verfälscht werden können.

Einer Umfrage des Deutschen Instituts für Urbanistik zufolge liegt der Grund für die fehlenden Transaktionen u.a. in mangelndem Datenschutz und Datensicherheit.[38] Das Hamburger Freizeit-Forschungsinstitut stellte in einer Umfrage für den Bereich des E-Commerce[39] fest, dass sich 55 Prozent der deutschen Bevölkerung einen Ausbau des Datenschutzes wünschen.[40] Untersuchungen in den USA und Europa liefern ähnliche Ergebnisse.[41] Daraus ergibt sich, dass das Vertrauen in die Zuverlässigkeit der Infrastruktur, in die Vertraulichkeit der Kommunikation und den Schutz vor Missbrauch personenbezogener Daten unabdingbare Voraussetzungen für die Nutzung der Online-Angebote sind.[42] Beim Aufbau von E-Government-Verfahren sind daher nicht nur die technischen, organisatorischen, personalwirtschaftlichen, sozialen und politischen Anforderungen zu beachten, sondern insbesondere auch die rechtlichen.[43] Den Risiken der Datenverarbeitung in einem E-Government muss mit Datenschutz begegnet werden.[44]

Ziel und Aufgabe des Datenschutzrechts ist es nach § 1 Abs. 1 BDSG, „den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“. Das Bundesverfassungsgericht hat 1983 den Schutzzweck dahingehend präzisiert, dass jeder Betroffene grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten selbst zu bestimmen hat.[45] Dieses Grundrecht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht in seinem Volkszählungsurteil aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet. Das Gericht hat ferner den Grundsatz der Datenvermeidung durch Technik im Hinblick auf die sich drastisch ändernde Informations- und Kommunikationstechnik zum Ausdruck gebracht.[46] Danach ist bei der Erhebung von personenbezogenen Daten zu prüfen,

---

37 *Dix* 1999, 178 ff.

38 Dies gaben 80 Prozent der befragten Städte an, siehe *Floeting/Gaevert* 1997, 3.

39 Die Entwicklungen im Bereich des E-Commerce setzen für die Realisierungschance des E-Government ein deutliches Signal dafür, welche Bedeutung das Vertrauen der Bürger und Wirtschaftsakteure für die freie und ungehinderte Nutzung der Informations- und Kommunikationsmedien hat.

40 *Opaschowski*, DuD 1998, 654 ff.

41 *Fuhrmann 2000*, 132 m. w. Nachw.

42 *Dix* 1999, 178 m.w. N. für USA und Europa; *Gundermann*, K&R 2000, 225.

43 *Lübking* 1992, 20; *Büllesbach*, RDV 1997, 239.

44 *Wienholtz*, DuD 1995, 644; *Bäumler*, CR 1997, 174; *Mutius*, DuD 1995, 666.

45 BverGE 65, 1 (42 ff.).

46 Siehe ausführlich dazu, *Roßnagel*, NVwZ 2000, 622.

„ob das Ziel der Erhebung nicht auch durch anonymisierte Ermittlung erreicht werden kann“.[47]

Der Nutzer muss auch in einer Online-Welt kommunale Internetangebote ebenso spurlos beanspruchen können, wie jemand, der persönlich das Rathaus betritt.[48] Wenn der Bürger neben der Möglichkeit des konventionellen Verwaltungsverfahrens die Online-Variante wählt, müssen folgende Aspekte beachtet werden:

?? Personenbezogene Daten dürfen nur im erforderlichen Umfang verarbeitet werden. Soweit möglich, ist die Verarbeitung personenbezogener Daten zu vermeiden,

?? Personenbezogene Daten dürfen nur für die in den Erlaubnistatbeständen und in Einwilligungen genannten Zwecken verarbeitet werden. Diese Zweckbindung ist sicherzustellen.

?? Die personenbezogenen Daten müssen sicher und vertraulich verarbeitet werden.

?? Die Kontroll- und Korrekturrechte der Betroffenen sind zu gewährleisten.

Das Vertrauen in die Online-Welt kann aber nicht durch rechtliche Vorgaben allein gewährleistet werden. Vielmehr muss Datenschutz auch durch Technik garantiert werden.[49] Die Anforderungen an den Datenschutz durch Technik hat der Gesetzgeber im Teledienstdatenschutzgesetz (TDDSG) festgehalten.[50] Das TDDSG hat zum Einen bewährte Grundsätze des Datenschutzes an die neuen technischen Entwicklungen angepasst und zum Anderen erstmals neue Ansätze des Selbst- und Systemdatenschutzes umgesetzt.[51]

Datenschutz muss zu konstruktiven Lösungen für die Nutzung der Online-Verwaltung beitragen. Er darf nicht als reformfeindlich als Bremsklotz verstanden werden.[52] Aspekte des Datenschutzes müssen in den Reformprozess selbst integriert werden, weil dieses zur Kundenorientierung der umstrukturierten Verwaltungen gehört und zugleich einen Beitrag zur technischen Modernisierung darstellt. Datenschutz ist notwendiger Vertrauensfaktor bzw. entscheidender Akzeptanzfaktor für alle Formen des elektronischen Handelns und der elektronischen Verwaltung. Er kann das notwendige Vertrauen in die elektronische Kommunikation schaffen und verbreiteten Befürchtungen von Missbrauch personenbezogener Daten entgegenwirken.[53] Ein moderner und den neuen Technikanwendungen adäquater Datenschutz ist damit ein bedeutender Wettbewerbsfaktor und Standortvorteil.[54]

---

47 *Tinnefeld/Ehmann* 1998, 82.

48 *Dix* 1999, 180.

49 *Pfitzmann*, DuD 1999, 406; *Bizer*, DuD 2001, 276.

50 Ausführlich über die Entwicklung des Rechts der Multimediadienste siehe *Roßnagel*, NVwZ 1998, 1 ff. und NVwZ 2000, 622 ff.

51 *Roßnagel* 1999a, Einf. Rn. 52; *ders*., ZRP 1997, 26, *ders*. NVwZ 1998, 1 ff..

52 So auch *Bäumler*, CR 1997, 174; *Mutius*, DuD 1995, 666.

53 *Roßnagel/Pfitzmann,/Garstka*, DuD 2001, 253.

54 *Bizer*, DuD 2001, 250.

2. Beispiele für Electronic Government

Im Folgenden werden beispielhaft nur einige von vielen Anwendungsbereichen für Electronic Government dargestellt. Die Auswahl der Anwendungsbereiche ist im Hinblick auf ihre Präsenz innerhalb der laufenden Projekte sowie ihre Realisierungschance in der Online-Welt getroffen worden. Damit soll anderen als die hier untersuchten Verwaltungsbereichen der Durchbruch im E-Government nicht abgesprochen werden. Eine möglichst breite Palette der Anwendungen ist sogar wünschenswert, weil sie ein großer Schritt auf dem Weg zum virtuellen Rathaus bedeutet und das Ziel der interaktiven Verwaltung damit näher rückt.

2.1 Übersicht

Nahezu jede Kommune bietet Informationen im Internet an. Dagegen sind Transaktionen über das Internet kaum bzw. nur vereinzelt zu finden. Beispielhaft können die folgenden Verfahren genannt werden:

Die drei Media@Komm-Städte sind hinsichtlich der Transaktionen – unter Einsatz der elektronischen Signatur – besonders weit fortgeschritten:

Bremen setzt auf ein so genanntes Lebenslagenkonzept: Das bedeutet, dass der Nutzer von der Geburt über Einschulung, Ausbildung, Heirat bis hin zur Rente sowohl spezielle Informationen der Behörden als auch kommerzielle Angebote und Leistungen aus der Wirtschaft finden kann. An der Universität sowie an der Hochschule Bremen können die Adressänderung, die Exmatrikulation und Urlaubssemester elektronisch vorgenommen werden. Außerdem kann bei Umzug die Anmeldung online erfolgen. In Bremen wird im Bereich des KfZ-Wesens die Verlustanzeige von Pkw/Führerschein, die Abmeldung eines gestohlenen Pkw und die Anfrage nach dem Halter eines Pkw online realisiert. Auch das Grundbuch wird bereits elektronisch geführt.

Der Städteverbund Nürnberg strebt im Gegensatz zu Bremen eine dezentrale Lösung an. Eine Vielzahl von kommunalen und privatwirtschaftlichen Online-Dienstleistungen wird unter Einbeziehung der multifunktionalen Chipkarte geplant. Auf dieser Karte ist sowohl die Signaturfunktion, als auch die Bezahlfunktion integriert. Für alle Vorgänge ist also die Zahlung ebenfalls möglich. Die Ausstellung von Anwohnerparkausweisen wird bereits seit Mitte 2001 als Pilotprojekt durchgeführt. Dafür wurde einem kleinen Benutzerkreis die Signaturkarte ausgehändigt. Darüber hinaus ist die An- und Ummeldung im Einwohnerwesen , die Abwicklung von Bauanträgen, Buchung von Eintrittskarten für das Theater oder Oper etc., öffentliche Ausschreibeverfahren vorgesehen. Als nächstes zu realisierendes Anwendungsfeld ist die einfache Melderegisterauskunft angedacht. Als Public-Private-Projekt soll ein virtueller Marktplatz aufgebaut werden, der einen vereinfachten Einstieg ins Internet bieten soll. Auf dieser Plattform ist der Kauf von elektronischen Fahrscheinen möglich.

In Esslingen steht der marktwirtschaftliche Aspekt im Mittelpunkt des Projektvorhabens. Die in Esslingen entwickelte These „E-Business needs E-Government“ ist ein wesentlicher Aspekt, worin sich Esslingen von Bremen und dem Städteverbund Nürnberg unterscheidet. Ziel der Stadt ist die Entwicklung der Genehmigungsbehörde zum

Dienstleister. Auf der Homepage der Gemeinde ist ein virtueller Kleinanzeigemarkt vorhanden, Kinotickets können per Handy bestellt werden. Darüber hinaus sind kommunale Dienstleistungen wie die Gewerbeummeldung, die KfZ-Zulassung und der Anwohnerparkausweis vorgesehen. Für alle Anwendungsfelder ist der Einsatz von „Allsign", welches das Zertifikat sowohl von Sign Trust (Deutsche Post AG), als auch das der TeleSec (Deutsche Telekom AG) unterstützt, zur rechtsverbindlichen Abgabe der Willenserklärung geplant. Allsign ist eine Zwischenlösung für XML/OSCI.

Aber auch viele andere Städte haben bereits Konzepte für Internettransaktionen mit Bürgern und Wirtschaft konzipiert oder realisiert:

?? Die Stadt Mannheim ermöglicht ihren Einwohnern die elektronische An- und Ummeldung bei Wohnungswechsel. Die Daten werden dabei unverschlüsselt via Internet zur Meldebehörde übertragen.

?? In Karlsruhe können Wohnsitzanmeldung und Biotonnen-Abbestellung probeweise unter Verwendung von Verschlüsselungstechniken online abgewickelt werden. Allerdings muss der Antragsteller dann persönlich auf dem Meldeamt erscheinen, um den digital übertragenen Antrag zu unterschreiben. Insofern bieten die beiden Städte nur Vorbereitungshandlungen online an.

?? In Hagen kann derzeit eine einfache Melderegisterauskunft in einem automatisierten Abrufverfahren erteilt werden.

?? Auch die Stadt Rathenow hat sich die Umstellung auf elektronische Verfahren bei der einfachen und erweiterten Melderegisterauskunft als kurzfristiges, noch in diesem Jahr zu realisierendes Ziel gesetzt. In einer Pilotphase wird seit November 2001 Polizeibehörden die Möglichkeit des automatisierten Zugriffs auf das Melderegister eingeräumt. Die einfache Melderegisterauskunft im Außenverhältnis, also an private Stellen, wird als weiteren Umsetzungsschritt geplant.

?? In Warendorf können vier Anwendungsfelder vollständig elektronisch abgewickelt werden. Diese sind die Meldung von Fund- bzw. Verlustgegenständen, die Anmeldung eines Trödlerstandes, der Sperrmüllentsorgung sowie die Hundesteuererklärung.

?? In der niedersächsischen Stadt Hameln sollen die nächsten Kommunalwahlen digital durchgeführt werden.

?? In Hamburg ist das Grundbuch bereits auf elektronische Verfahren umgestellt.

Auf der Bundesebene kündigte die Staatssekretärin des Bundesministeriums des Inneren, Brigitte Zypries, an, dass alle öffentlichen Verwaltungen des Bundes, der Länder und Gemeinden über ein einziges Portal „Deutschland.de" im WWW erreichbar sein werden. Ein Beispiel für elektronische Verwaltung stellt das Antragsverfahren bei Führerscheinen dar, wobei die Antragsdaten, das digitalisierte Bild sowie die Unterschrift verschlüsselt zur Bundesdruckerei in Berlin gelangen.

Im Folgenden werden einige Anwendungsbereiche in ihrem rechtlichen und organisatorischen Kontext näher vorgestellt, von denen erwartet werden kann, dass sie als erste der anspruchsvolleren Transaktionen im Rahmen von Electronic Government realisiert werden. Bei ihnen handelt es sich durchweg um Anwendungen, die für die Verwaltung als auch für die nachfragenden Gruppen der Unternehmen und Bürger um Massenanwendungen handelt, bei denen ein hoher Nutzen der Online-Verwaltungsangebote erwartet werden kann.[55]

Für die folgenden Beispiele ist zu berücksichtigen, dass die Bundesregierung beabsichtigt, noch in diesem Jahr das Dritte Änderungsgesetz zum Verwaltungsverfahrensgesetz vom Gesetzgeber verabschieden zu lassen. In einem umfassenden Artikelgesetz sollen die rechtlichen Grundlagen für den elektronischen Rechtsverkehr im Verwaltungsbereich gelegt werden. Insbesondere sollen im VwVfG, im SGB und in der AO sowie in vielen bereichsspezifischen Gesetzen die elektronische Form eingeführt werden. Sie setzt ein elektronisches Dokument mit einer qualifizierten elektronischen Signatur voraus und vermag die Schriftform zu ersetzen.

2.2 Meldewesen

Das Meldewesen ist entsprechend Art. 75 Abs. 1 Nr. 5 GG rahmenrechtlich durch das Melderechtsrahmengesetz des Bundes geregelt. Die Ausfüllung dieses Rahmens liegt in der Gesetzgebungskompetenz der Länder und ist in Niedersachsen im NMG geregelt. Zweck des Melderechts ist es, die Registrierung bestimmter Grunddaten sicherzustellen, die für die Feststellung und den Nachweis der Identität und der Wohnungen der Einwohner erforderlich sind und zugleich einen wirksamen Persönlichkeitsschutz bei der Verwendung dieser Daten zu gewährleisten.

Meldebehörden sind die Kommunen, die ihre Aufgaben nach dem Meldegesetz gemäß § 2 NMG im übertragenen Wirkungskreis wahrnehmen. Ihre Aufgabe besteht nach § 1 Satz 1 NMG darin, die in ihrem Zuständigkeitsbereich wohnenden Einwohner zu registrieren, Melderegisterauskünfte zu erteilen und Daten an Behörden oder sonstige öffentliche Stellen zu übermitteln. Der Erfüllung dieser Aufgaben dient ein Melderegister, in dem die Daten gespeichert werden. Das Meldewesen ist keine polizeiliche, sondern eine eigenständige Aufgabe dieser Behörden.[56]

2.2.1 An- und Ummeldung

Nach § 9 Abs. 1 NMG hat sich eine Person innerhalb einer Woche bei der Meldebehörde an- oder abzumelden. § 10 Abs. 1 NMG sieht die allgemeine Meldepflicht als erfüllt an, wenn der Meldepflichtige einen Meldeschein ausfüllt, unterschreibt und der Meldebehörde zuleitet. In Niedersachsen sind für die An- und Ummeldung amtlich eingeführte Formblätter vorgesehen.[57] Für die Anmeldung ist nach § 9 Abs. 1 Satz 2 NMG weiterhin erforderlich, dass die Abmeldung durch Aushändigung des entsprechenden Pa-

---

55 Vgl. auch die KGSt-Empfehlungen in: Kommune und Internet, KGSt-Bericht Nr. 1/2000, 50 ff.

56 S. z.B. *Belz* 1987, § 36 Rn. 49.

57 Nds. Mbl. V. 23.7.1999, 510.

pierdokuments bestätigt wird. Für einen Umzug innerhalb derselben Gemeinde ist an Stelle des Anmeldescheins ein vereinfachter Umzugsmeldeschein zu verwenden, wenn mit dem Wohnungswechsel nicht der Status der Wohnung verändert wird.[58]

Zur Erfüllung der Meldepflicht ist die Unterschrift des Betroffenen erforderlich. Durch das Erfordernis der Abgabe eines Scheins und das Abholen eines Scheins ist derzeit noch das persönliche Erscheinen des Betroffenen oder eines Boten erforderlich.

Wer in Herbergen wohnt, hat besondere Meldepflichten zu erfüllen.[59] Nach § 18 Abs. 2 NMG hat die beherbergte Person am Tage der Ankunft einen besonderen Meldeschein handschriftlich auszufüllen und zu unterschreiben. Die ausgefüllten Meldescheine sind von dem Leiter der Beherbergungsstätte nach § 18 Abs. 3 NMG bis zum Ablauf des zweiten auf die Abreise folgenden Kalenderjahres aufzubewahren und der Meldebehörde sowie dem Polizeivollzugsdienst auf Verlangen vorzulegen oder zu übermitteln.

Für die Meldebehörden könnte ein besonderes Interesse an der elektronischen An-, Ab- und Ummeldung darin liegen, dass sie die Daten schon in der Weise erhalten, die sie für das Melderegister benötigen. Sie könnten die Formulare für die Meldungen in elektronischer Form abrufbar halten und die eingetragenen Daten nach einer Prüfung direkt in das Register übernehmen. Es bestehen keine Bedenken hinsichtlich der elektronischen Bereitstellung der vorgesehenen Formblätter. Die Meldebestätigung könnte automatisch erstellt und unmittelbar an den Sender zurückgesandt werden. Für die Meldebehörden könnten die Investitionen und Schulungen zur Verwendung der elektronischen Signatur vor allem auch deshalb interessant sein, weil sie ein wichtiger Knoten im Datenaustausch zwischen Behörden darstellen und viele Verpflichtungen zur Datenübertragung wahrnehmen müssen, in denen sie ebenfalls elektronische Signaturen einsetzen könnten und aus Sicherheitsgründen auch nutzen sollten.

Das Meldeformular müsste auf Seiten des Nutzers in jedem Fall am Bildschirm ausgefüllt und an den zuständigen Sachbearbeiter des Meldeamtes geschickt werden. Das elektronische Dokument müsste dafür verschlüsselt werden, um Unbefugten die Einsicht zu unterbinden. Nach der Annerkennung der elektronischen Signatur können die Meldescheine auch rechtsverbindlich elektronisch signiert werden.

Auf Seiten der Bürger ist nicht zu erwarten, dass diese sich zum Zwecke der An-, Ab- oder Ummeldung mit einem Schlüsselpaar und einem Zertifikat versehen. Aber soweit sie bereits für andere Zwecke, insbesondere auch andere Verwaltungszwecke elektronische Signaturen verwenden, könnte ein entsprechendes Angebot der Meldeämter die Attraktivität dieses Sicherungsmittels erhöhen. Von größerem Interesse könnte die Nutzung elektronischerer Signaturen für diejenigen sein, die wiederkehrende Kontakte zu den Meldebehörden haben. Dies gilt vor allem für die Stellen, die - wie etwa Anwaltsbüros, Banken, Versicherungen, Inkassobüros oder Auskunfteien - öfter Melderegisterauskünfte beantragen.

---

58 So jedenfalls in Niedersachsen, vgl. Nds. Mbl. V. 23.7.1999, 513.

59 S. § 16 Abs. 2 MRRG.

2.2.2 Melderegisterauskunft

Die Melderegisterauskunft unterscheidet sich in die einfache, erweiterte und Gruppenauskunft. Nach § 33 Abs. 1 NMG darf die Meldebehörde auf Antrag jedem eine einfache Auskunft erteilen; sie ist dazu nicht verpflichtet. Es besteht somit kein Rechtsanspruch des Anfragenden auf die Auskunftserteilung. Allerdings besteht ein Anspruch auf Ausübung des pflichtgemäßen Ermessens und eine über den Gleichbehandlungsgrundsatz zu begründende Selbstbindung der Verwaltung durch jahrelange Übung.

Zu dem auskunftsberechtigten Personenkreis zählen neben natürlichen Personen auch juristische Personen, nichtrechtsfähige Personenvereinigungen, privatrechtliche Religionsgesellschaften, Gewerkschaften sowie politische Parteien.[60]

Während die einfache Melderegisterauskunft über die zweifelsfreie Identifizierbarkeit des Betroffenen hinaus an keine weitere Voraussetzungen geknüpft ist, ist für die erweiterte Auskunft aus dem Melderegister zusätzlich die Glaubhaftmachung eines berechtigten Interesses erforderlich. Bei dem Begriff „berechtigtes Interesse“ handelt es sich um einen unbestimmten Rechtsbegriff. Zu den berechtigten Interessen gehört jedes von der Rechtsordnung als schutzwürdig anerkannte ideelle oder vermögenswerte Interesse, insbesondere ein rechtliches Interesse, aber auch ein wirtschaftliches Interesse wie die Ermittlung eines Schuldners oder ein privates Forschungsvorhaben. Demnach ist zur Feststellung eines berechtigten Interesses eine vernünftige Abwägung der jeweiligen, also auf den Einzelfall bezogenen Sachlage vorzunehmen. Die Meldebehörde hat zwischen dem Auskunftsinteresse des Anfragenden und dem Geheimhaltungsinteresse des Einwohners abzuwägen. Berechtigt ist das Interesse des Auskunftssuchenden, wenn dieses das Geheimhaltungsinteresse des Einwohners überwiegt. Das berechtigte Interesse ist für jedes erwünschte Datum glaubhaft zu machen und von den Meldebehörden zu überprüfen.

Die Meldebehörde hat nach § 33 Abs. 2 Satz 2 NMG den Betroffenen über die Erteilung einer erweiterten Melderegisterauskunft unter Angabe des Datenempfängers unverzüglich zu unterrichten. Die Unterrichtungspflicht entfällt bei Geltendmachung eines rechtlichen Interesses (§ 33 Abs. 2 Satz 2 NMG).

Im Unterschied zu der einfachen Auskunftserteilung kann eine erweiterte Auskunft verwaltungsrechtlich jedoch nicht in einem automatisierten Abrufverfahren erfolgen, da hier wegen des berechtigten Interesses eine Einzelfallprüfung durch den Sachbearbeiter vorgenommen werden muss.

Allerdings kann für diese Einzelfallprüfung eine Kommunikation über das Internet genutzt werden. In der Praxis ist es zur Glaubhaftmachung des berechtigten Interesses erforderlich, Dokumente (z.B. Gerichtsbeschluss, Behördenurkunden, Forderungsunterlagen) vorzulegen. Für die Glaubhaftmachung reicht aber in der Regel eine Kopie, die auch in der elektronischen Kopie eines digitalisierten Schriftstücks bestehen kann. Muss der Sachbearbeiter der Meldebehörde zur Feststellung dieses Interesses mit dem Auskunftssuchenden kommunizieren, kann er hierzu ebenfalls Dienste des Internet in An-

60 *Belz* 1987, § 32 Rn. 4.

spruch nehmen. Ein persönliches Erscheinen zur Übergabe der Kopien ist nicht notwendig.

Melderegisterauskünfte über eine Vielzahl von Einwohnern, die nicht namentlich bezeichnet, sondern lediglich nach abstrakten Merkmalen abgegrenzt sind (Gruppenauskünfte), dürfen nach § 33 Abs. 3 NMG nur erteilt werden, soweit dies im öffentlichen Interesse liegt. Was unter dem unbestimmten Rechtsbegriff „öffentliches Interesse" zu verstehen ist, ist bislang nicht geklärt. Es sind vielmehr einzelne Kriterien wie das Interesse der Allgemeinheit und der soziologisch-gesellschaftliche Bezug entwickelt worden.[61] Danach bildet die Markt-, Meinungs- und Sozialforschung, zumindest bei Ausstellung einer Unbedenklichkeitsbescheinigung durch das Innenministerium, regelmäßig einen Anwendungsfall des § 33 Abs. 3 NMG dar. Die Kunden- und Mitgliederwerbung liegt dagegen außerhalb des Anwendungsbereichs.

Nach § 35 Abs. 2 und 3 NMG kann eine Auskunft aus dem Melderegister nicht erteilt werden, wenn eine Auskunftssperre vorliegt. Eine Auskunftssperre liegt immer dann vor, wenn durch die Auskunftserteilung eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen glaubhaft gemacht werden kann. Ferner kann eine Auskunft nicht erteilt werden, wenn nach § 34 Abs. 5 NMG ein Widerspruch gegen die Weitergabe der dort genannten Daten eingelegt worden ist.

Nach der Meldedatenübermittlungsverordnung (MeldDüVO) konnten bislang Auskünfte aus dem Melderegister in einem automatisierten Verfahren nur an öffentliche Stellen erteilt werden. Der Entwurf des MRRG sieht eine Erteilung der *einfachen* Melderegisterauskunft im automatisierten Abrufverfahren auch an private Stellen vor. Gegen diese Art der Erteilung kann der Betroffene, über den eine Auskunft erteilt werden soll, ohne eine weitere Begründung der Online- Erteilung widersprechen. In diesem Fall darf die Meldebehörde eine Auskunft über das Internet nicht erteilen. Die Auskunftserteilung im analogen Verfahren ist von diesem Widerspruch allerdings nicht berührt. Dort hat der Betroffene nur die Möglichkeit einer Auskunftssperre unter Darlegung besonderer Umstände. Anders als im bisherigen Verfahren sieht der Entwurf des MRRG ferner die Angabe bestimmter Suchkriterien vor. Demnach ist der Name, Vorname sowie ein weiteres Kriterium zur Bestimmung des Betroffenen erforderlich. Auf die Frage, inwieweit die einfache Melderegisterauskunft auch nach dem geltenden Gesetz über das Internet automatisiert abgerufen werden kann, wird unter 6.3 eingegangen. Im Gegensatz zu der einfachen Auskunftserteilung scheidet die Erteilung einer erweiterten Melderegisterauskunft und der Gruppenauskunft im automatisierten Abrufverfahren nach der jetzigen Gesetzeslage jedoch von vornherein aus, da hierfür eine spezielle Einzelfallprüfung erforderlich ist. Auch der Entwurf zum MRRG sieht en solches Verfahren für diese Auskunftsformen nicht vor.

Die Online-Auskunft kann nicht anders als in der Offline-Welt lauten. Bei der Umsetzung sollte ein möglichst genauer Abgleich der Verfahren erfolgen, um Umstellungen zu vermeiden.

---

61 *Medert/Süßmuth* 1992, § 21 Rn. 49.

2.3 KfZ-Zulassung

Die Kraftfahrzeugzulassung wird immer wieder als „Paradebeispiel“ für interaktive elektronische Transaktionen zwischen Verwaltung, Bürgern und Wirtschaftsunternehmen genannt.[62] Pro Jahr werden 150.000 Vorgänge im Kfz- Zulassungswesen abgewickelt, 250 bis 400 Kunden werden pro Tag in einer mittelgroßen Stadt bedient. Da es sich um einen Massenvorgang handelt, bei dem - zumindest zu KfZ-Händlern - ein ständiger Verwaltungskontakt besteht, bietet sich die Kraftfahrzeugverwaltung tatsächlich für elektronische, durch elektronische Signaturen gesicherte Telekooperationen an.

Die Kraftfahrzeugverwaltung umfasst den Antrag auf KfZ-Zulassung durch Händler bzw. Kunde, Stillegung, Meldung bei Diebstahl, Wunschkennzeichenreservierung und Auskunftseinholung durch die Polizei und Versicherungen.

In dem Antrag sind sämtliche Daten über das Fahrzeug (§§ 34 Abs. 1, 33 Abs. 1 Satz 1 Nr. 1 StVG) sowie die nach § 33 Abs. 1 Satz 1 Nr. 2 StVG zu speichernden Halterdaten (Name, Vorname, Geburt, Geschlecht sowie Anschrift) zu nennen. Außerdem sind ein Versicherungsnachweis sowie der Fahrzeugbrief vorzulegen. Als Fahrzeugbrief dürfen nur die amtlich hergestellten Vordrucke mit einem für die Bundesdruckerei geschützten wasserzeichenähnlichen Sicherheitsmerkmal verwendet werden. Wird das Kraftfahrzeug veräußert, muss der neue Erwerber keinen neuen Kraftfahrzeugbrief, aber einen neuen Kraftfahrzeugschein und eine neue Zulassung beantragen. Aber auch er muss den übernommenen Kraftfahrzeugbrief vorlegen. Bei der Zulassung hat die Zulassungsstelle auch das ordnungsgemäße Ausfüllen des Briefes durch den Hersteller zu überprüfen und die Halter- und Kraftfahrzeugdaten in den Brief einzutragen und zu bestätigen. Dem Antragsteller wird ein Kennzeichen zugeteilt und mit einem amtlichen Stempel versehen. Der Zulassungsstelle ist nach § 27 Abs. 1 StVZO jede Änderung der im Kraftfahrzeugbrief, im Kraftfahrzeugschein oder in den Anhängerverzeichnissen enthaltenen Angaben, die Veränderung des Standortes des Kraftfahrzeugs, dessen Stillegung sowie dessen Veräußerung unverzüglich zu melden. Somit muss auch ein Wohnungswechsel oder eine Namensänderung durch Heirat der Zulassungsstelle gemeldet werden. Jede Änderung der Halterdaten oder KfZ-Daten ist im Kraftfahrzeugschein in jedem Fall, im Kraftfahrzeugbrief nur ausnahmsweise nachzutragen. Die Änderung ist mit dem Dienstsiegel der Zulassungsstelle, einem Handzeichen des Sachbearbeiters und einem Datumsstempel zu versehen. Nach § 27 Abs. 1 StVZO[63] müssen Änderungen im Fahrzeugbrief, im Fahrzeugschein und in den übrigen in der Vorschrift genannten Papieren der zuständigen Zulassungsbehörde erst gemeldet werden, wenn diese aus anderen Gründen mit den Fahrzeugpapieren befasst ist. Die Verordnung über die Entsorgung von Altautos und die Anpassung straßenverkehrsrechtlicher Vorschriften vom 4.7.1997[64] brachte mit der zum 1.4.1998 in Kraft getretenen Altauto-Verordnung für den Besitzer eines Autos, der sich dessen entledigen will oder muss, die Verpflichtung, das Fahrzeug einem von Herstellern oder Vertreibern eingerichteten anerkannten Ver-

---

62 S. z.B. bereits Enquete-Kommission Baden-Württemberg, LT-Drs. 11/6400, 35; *Habbel* 1998, 14 ff.

63 Eingeführt durch die 26. VO zur Änderung straßenverkehrsrechtlicher Vorschriften vom 12.8.1997, BGBl. I, 2051.

64 BGBl. I, 1666.

wertungsbetrieb zu überlassen (§ 3 AltautoV). Nach § 4 AltautoV müssen Betreiber von Annahmestellen, Verwertungsbetrieben und Schredderanlagen Altautos und Restkarossen nach Maßgabe des Anhangs zur AltautoV umweltverträglich behandeln, ordnungsgemäß und schadlos verwerten und gemeinwohlverträglich beseitigen.[65] Zugleich mit der AltautoV wurde in die StVZO eine neue Bestimmung über Verwertungsnachweis und Verbleibserklärung von Altautos aufgenommen. Nach § 27a StVZO sind Eigentümer und Halter näher bezeichneter PKW, wenn das Fahrzeug endgültig aus dem Verkehr gezogen wird oder als endgültig aus dem Verkehr gezogen gilt,[66] verpflichtet, der Zulassungsstelle einen Verwertungsnachweis oder eine Verbleibserklärung des Verwertungsbetriebs vorzulegen.[67] Verstöße sind nach § 69a Abs. 2 Nr. 12a StVZO ordnungswidrig.[68]

Die Einführung elektronisch signierter Dokumente in der Kraftfahrzeugverwaltung setzt keine Ergänzung einer Formvorschrift voraus. § 23 StVZO fordert nur einen Antrag auf Zuteilung des amtlichen Kennzeichens für ein Kraftfahrzeug, fordert hierfür aber keine bestimmte Form. Da elektronisch signierte Dokumente die funktionellen Voraussetzungen an die Integrität eines Antrags und den Nachweis seiner Urheberschaft erfüllen, kann bereits nach geltendem Recht der Antrag auch in Form eines signierten Dokuments gestellt werden. Die Zulassung selbst ist ein formbedürftiger Verwaltungsakt und ohnehin nicht durch elektronisches Handeln ersetzbar, so dass sich sowieso nur die Frage stellt, ob das Verwaltungsverfahren bis zu diesem Schlusspunkt durch ein elektronisches Verwaltungsverfahren vorbereitet werden könnte. Hierfür wären einige geringe Änderungen des Zulassungsverfahrens nach der StVZO erforderlich. Mit dem signierten Antrag auf Zulassung müssten bereits alle notwendigen Informationen übermittelt werden, unter anderem der Kraftfahrzeugbrief in gescannter Form und der Versicherungsnachweis, der von der Versicherung bereits elektronisch signiert ausgestellt werden könnte. Denn erst nach deren Prüfung kann die Zulassung erteilt werden. Bis zu dieser Änderung der StVZO könnte die Zulassungsbehörde die Zulassung unter dem Vorbehalt der Sichtprüfung vorbereiten, wenn ihr der Brief und der Versicherungsschein vorab gefaxt oder gescannt übermittelt werden. Zugleich mit dem Zulassungsantrag könnte ein formloser Antrag auf Zuteilung eines bestimmten Kennzeichens gestellt werden. Dem Antragsteller könnte unter dem Vorbehalt einer Sichtprüfung des Kraftfahrzeugbriefs elektronisch mitgeteilt werden, dass die Zulassung erteilt und ein bestimmtes Kennzeichen zugeteilt wird. Der Antragsteller kann daher alle Verwaltungsabläufe vor seinem Erscheinen in der Behörde elektronisch abwickeln und bereits das ihm zugeteilte Kennzeichen mitbringen. Zur Abstempelung des Kennzeichens ist nach § 23 Abs. 4 Satz 3 StVZO das Kraftfahrzeug vorzuführen, wenn die Zulassungsstelle nicht darauf verzichtet. Auch diese Entscheidung könnte dem Antragsteller elektronisch mitgeteilt werden. An diesem Punkt müsste dann das elektronische Verfahren in ein körperliches Verfahren übergehen. Die Einträge im Kraftfahrzeugbrief, das Ausstellen des Kraftfahrzeugscheins sowie das Anbringen des amtlichen Stempels auf das Kennzeichen erfordern die Vorlage dieser Gegenstände oder ihre körperliche Entgegennahme. Dies könnte

---

65 S. ausführlich *Kopp*, NJW 1997, 3292.

66 S. hierzu § 27 Abs. 6 Satz 2 StVZO.

67 S. *Hentschel*, NJW 1998, 650; *Kopp*, NJW 1997, 3292.

68 S. *Hentschel*, NJW 1998, 651.

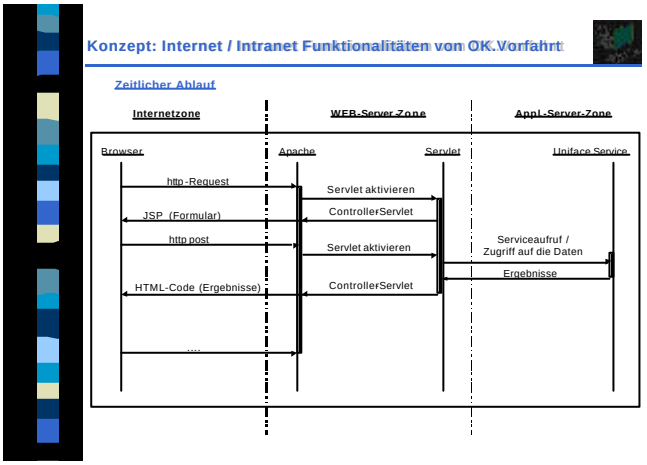
aber alles ohne Wartezeiten erfolgen, wenn alle sonstigen Verwaltungsvorgänge bereits durchgeführt sind.

Für die von § 27 StVZO geforderte Meldung einer Änderung der im Kraftfahrzeugbrief enthaltenen Angaben, für die Mitteilung über gestohlene oder abhanden gekommene Fahrzeuge und KfZ-Kennzeichen sowie für Verwertungsnachweise oder eine Verbleibserklärung des Verwertungsbetriebs ist ebenfalls keine besondere Form vorgeschrieben. Sie können daher auch mittels eines signierten Dokuments erfolgen.

Für das Electronic Government-Verfahren zur KfZ-Verwaltung gibt es bereits Software, deren Funktionalität am Beispiel der Software „OK.Vorfahrt“ beschrieben werden soll. Das Grundverfahren ist hierbei für alle Funktionalitäten gleich und muss in den einzelnen Bereichen um spezielle Software ergänzt werden.

Der Bürger muss sich über ein signiertes Applet mit seiner Signatur identifizieren. Er kann dann die erforderlichen Formulare vom Web-Server der Verwaltung laden und die Daten (z.B. Suchkriterien, Zulassungsdaten usw.) eingeben. Diese Daten werden an Servlets übertragen. Diese führen die notwendigen Überprüfungen durch und übermitteln die Daten an einen der OK.Vorfahrt-Netzdienste. Das Ergebnis der Verarbeitung geht wieder an das Servlet zurück und gelangt von dort aus an den Bürger.

Der Einsatz von Servlets auf dem Web-Server ermöglicht eine Schnittstelle zu OK.Vorfahrt. Die Verarbeitung erfolgt nur über diese Schnittstelle auf dem kommunalen Server und bleibt vor Beeinträchtigungen der Außenwelt geschützt.



Mit dieser Software können Wunschkennzeichen reserviert, Auskünfte erteilt und KfZ zugelassen und stillgelegt werden. Eine Spezial-Software existiert bereits. Das Verfahren soll am Beispiel der Händlerzulassung und -stillegung beschrieben werden:

Nach der Identifizierung kann der Händler zwischen den unterschiedlichen Anwendungen wählen und dann selber die erforderlichen Daten eingeben. Für die Händlerneuzulassung benötigt die Zulassungsstelle den Fahrzeugbrief, den Personalausweis bzw. eine Vollmacht und die Doppelkarte der Versicherung. Diese sind, solange die elektronische Signatur nicht anerkannt ist, auf konventionellem Postwege an die Zulassungsstelle zu

schicken. Bei Gleichstellung der elektronischen Signatur mit der Schriftform kann der digitalisierte Fahrzeugbrief und der bereits signiert ausgestellte Versicherungsnachweis elektronisch der Zulassungsstelle übermittel werden. Auch die nach Überprüfung der Daten fertig gestellten Dokumente müssen vom Händler abgeholt oder digitalisiert geschickt werden. Weder für die Neuzulassung noch für die Stillegung ist das Vorfahren mit dem Fahrzeug erforderlich. Das ist nur dann nötig, wenn das Fahrzeug aus einem Gebiet außerhalb des Landkreises stammt. In diesem Fall muss zur Anbringung der Plaketten das Fahrzeug bei der Zulassungsstelle z.B. durch einen Boten, so wie es bereits oft praktiziert wird, vorbeigefahren werden.

2.4 Pass- und Personalausweiswesen

Sowohl im öffentlichen als auch im privaten Bereich bedarf es häufig einer Identitätsfeststellung. Insoweit kommt Personalausweisen und Reisepässen als amtlichen Dokumenten zur Identitätsfeststellung zentrale Bedeutung zu. Einige Beispiele für die eindeutige Identifizierung der Person stellen die notarielle Beurkundung von Erklärungen gemäß § 10 Abs. 2 Beurkundungsgesetz, die Einrichtung von Kontrollstellen auf öffentlichen Straßen und Plätzen nach § 111 StPO oder der Abschluss von Verträgen mit Kredit- und Finanzdienstleistungsinstituten, Versicherungsunternehmen oder Spielbanken nach Maßgabe der Abgabenordnung und des Geldwäschegesetzes dar.
Nach § 4 PassG ist ein bestimmtes Muster für den Pass vorgesehen. Demnach ist neben der Seriennummer, dem Lichtbild und der Unterschrift des Passinhabers der vollständige Name, Doktorgrad, Ordensname, Künstlername, Geburtstag und -ort, Geschlecht, Größe, Augenfarbe, Wohnort und Staatsangehörigkeit in dem Pass anzugeben. Der Pass wird auf Antrag gestellt und sind 10 Jahre nach Ausstellung gültig. Nach § 1 Abs. 1 PAuswG müssen Personen über 16 Jahren und mit der deutschen Staatsangehörigkeit einen Personalausweis beantragen. Für die erstmalige Ausstellung fällt nach Abs. 4 des § 1 PAuswG eine Gebühr an. Auch die Personalausweise werden nach einem bestimmten Muster ausgestellt. Ihre Gültigkeit ist nach § 2 PAuswG unterschiedlich geregelt: Ausweise für Personen unter 26 Jahren haben eine Gültigkeitsdauer von 10 Jahren, andernfalls beträgt die Dauer 5 Jahre. In dem Gesetz zur Ausführung des Gesetzes über Personalausweise ist das Verfahren näher geregelt. So muss der Antragsteller nach § 5 Abs. 1 Nds. AGPAuswG persönlich erscheinen. Den Antrag muss der Betroffene im Einwohnermeldeamt stellen. Dafür muss er ein Formular ausfüllen und die Gebühr zahlen.

Im Online-Verfahren müssten die Abläufe an das analoge Verfahren angepasst werden. Es müssten einheitliche Formulare vorgesehen sein. Diese könnten dann online ausgefüllt, signiert mit dem ebenfalls signierten Lichtbild an die zuständige Stelle verschickt werden. Nach Gleichstellung der elektronischen Signatur könnten somit alle Vorgänge online abgewickelt werden. Der Betroffene müsste dann persönlich auf der Behörde erscheinen und seinen Pass bzw. Personalausweis sich aushändigen lassen.

Die Bundesdruckerei hat auf der Cebit 2000 ihr neues digitales Verfahren („Digant“) für die Beantragung von Personalausweisen, Pässen und Führerscheinen vorgestellt. Um die Verfahren zu beschleunigen, werden die Anträge nicht mehr per Post nach Berlin gesandt, sondern es werden Bild und Unterschrift bei den Meldestellen gescannt, digital

verschlüsselt und signiert und werden dann online nach Berlin geschickt. Durch dieses Verfahren kann die Bearbeitung der Vorgänge um etwa eine Woche beschleunigt werden.[69]

2.5 Bauwesen

Ein weiteres Anwendungsfeld für Electronic Government sind einige einfachere Verwaltungsvorgänge im Bauwesen wie Bauvoranfrage, Bauantrag und Baugenehmigung für Werbetafeln.

Ausgehend von einer Baumaßnahme, welche gemäß § 68 Abs. 1 NBauO der Genehmigung durch die Bauaufsichtsbehörde bedarf, ist grundsätzlich ein Antrag auf die Erteilung der Baugenehmigung zu stellen. Nach § 71 Abs. 1 NBauO ist der Bauantrag schriftlich bei der Gemeinde einzureichen. Ferner fordert § 1 Abs. 4 BauVorlVO, dass der Bauantrag vom Bauherrn und dem Entwurfsverfasser mit Tagesangabe eigenhändig unterschrieben wird. Hierfür sind spezifische Antragsformulare zu verwenden. Der Bauantrag und die Bauvorlagen sind in dreifacher Ausfertigung einzureichen. Das Bauantragsformular enthält eine Erklärung des Bauherrn zur Vollmachtserteilung an den Entwurfsverfasser. In dem Antrag hat der Entwurfsverfasser seine Qualifikation nach § 58 NBauO zu nennen. Des weiteren verlangt § 71 Abs. 2 NBauO zum Bauantrag das Vorlegen von allen für die Beurteilung der Baumaßnahmen und die Bearbeitung erforderlichen Unterlagen, also der Bauvorlagen. Nach §§ 74 Abs. 2, 71 Abs. 1 NBauO i.V.m. § 10 Abs. 2 BauVorlVO bedarf auch die Bauvoranfrage der Schriftform und der eigenhändigen Unterschrift. Gleiches gilt nach § 24 Abs. 1 Satz 1 NDenkmSchG für einen Antrag auf eine Genehmigung zur Vornahme einer in § 10 NDenkmSchG genannten Maßnahme hat nach schriftlich zu erfolgen.

Die Baugenehmigung stellt einen Verwaltungsakt im Sinn des § 35 Abs. 1 VwVfG dar. Sie ist nach § 75 Abs. 3 NBauO schriftlich zu erteilen. Zwar kann nach § 37 Abs. 3 und 4 VwVfG die eigenhändige Unterschrift dadurch ersetzt werden, dass der Name des verantwortlichen Beamten wiedergegeben wird oder über Hinweise im Bescheid ermittelt werden kann. Doch muss die Erklärung der Behörde verkörpert sein, so dass ein elektronischer Bescheid ausscheidet.[70] Gleiches gilt für den Bescheid bei einer Bauvoranfrage. Dagegen kann die Abgabe einer Genehmigung durch die Behörde bereits heute elektronisch erfolgen, da nach den Vorschriften des NDenkmSchG dafür nicht einmal Schriftform verlangt wird.

In einer E-Government-Lösung des Baugenehmigungsverfahrens müsste versucht werden, alle End-User-Softwaresysteme miteinander zu verkoppeln: Der Architekt/Bauherr soll demnach in seinem Büro einen Bauantrag stellen, diesen, ohne ausdrucken und

---

69 FR vom 29.2.2000.

70 S. *Roßnagel*, DÖV 2001, 221; *Idecke-Lux* 2000, 107; a. A. *Knack* 1998 § 37 Rn. 5.3.; *Holznagel/Krahn/Werthmann*, DVBl 1999, 1482, nach denen es für das Schriftformerfordernis ausreicht, wenn die Willenserklärung in einer der Schriftform vergleichbaren Weise verkörpert werden kann. Dafür wird die Möglichkeit eines Ausdrucks auf der Empfängerseite als ausreichend angesehen. Allerdings verzichtet diese Ansicht auf wichtige Aspekte der Integritäts-, Identitäts-, Echtheits- und Nachweisfunktion der Schriftform und ist daher abzulehnen.

handschriftlich ausfüllen zu müssen, direkt via Internet in das EDV-System der zuständigen Baubehörde übermitteln. Diese setzt sich wiederum mit den anderen Fachbehörden direkt in Verbindung. Bei entsprechenden Schutzvorkehrungen soll der Verfahrensablauf von allen Beteiligten eingesehen werden können. Die Baugenehmigung als Ergebnis des Verfahrens wird ebenfalls über Internet an den Antragsteller übermittelt.

Grundsätzlich können alle rechtlich geforderten Funktionen elektronisch nachgebildet werden. Das Schriftformerfordernis nach § 71 Abs. 1 NBauO kann grundsätzlich mittels einer elektronischen Signatur erfüllt werden, wenn die Rechtsordnung dies zulässt. Bauvorlagen können als CAD-Datei oder in eingescannter Form mit elektronischer Signaturen der Behörde zugeleitet werden.

Beispielsweise ist das iNet-Modul der Firma PROSOZ Herten eine Schnittstelle zwischen den verwaltungsintern eingesetzten Fachverfahren und dem Internet. Mit entsprechender Software können alle Beteiligte in das Verfahren Zugang bekommen. Die Daten werden automatisiert und ohne Medienbrüche direkt in das Fachverfahren eingelesen und wieder dem Internet bereit gestellt, so dass die Beteiligten mit einem Passwort die Daten abfragen können. Das Sicherheitskonzept wird durch vorverlagerte Datenhaltung und den Einsatz einer Austauschdatenbank realisiert. Der gesamte Datenverkehr soll auf der Basis einer Sicherheitsplattform für den Einsatz elektronischerer Signatur organisiert werden. Als einheitliches Protokoll wird OSCI verwendet.[71]

2.6 „Wirtschaftliche Aktivität“ der Kommune am Beispiel des Freizeit- und Tourismusagenten

Außer für die hoheitlichen Tätigkeiten im übertragenen Wirkungskreis kann E-Government auch für die freiwilligen Aktivitäten der Kommune in ihrem eigenen Wirkungskreis interessant sein. Solche Tätigkeiten können zum Beispiel die Wirtschaftsförderung betreffen.

Der Freizeit- und Tourismusagent (im folgenden abgekürzt: FTA) der Stadtregion Nürnberg ist eine freiwillige Leistung der Kommune an die Bürger zu einer komfortabeln Freizeitgestaltung. Dies soll dazu dienen, das kommunale Portal für die Bevölkerung attraktiver zu machen und eine breite Nutzung der Angebote in der Bevölkerung sowohl seitens der Einwohner als auch seitens auswärtiger Besucher zu erreichen, indem vergleichsweise selten beanspruchte Leistungsangebote der Verwaltung mit privaten Angeboten kombiniert werden.

Die Angebote werden von den Veranstaltern über die Kommune bereit gestellt und sind für den Nutzer kostenfrei. Die Kommune dient quasi als Informationsvermittler. Die Kosten werden hauptsächlich von den Veranstaltern in Form einer Registrierungsgebühr getragen.

Fragt ein Kunde den FTA nach, ist in einem ersten Schritt ein Interessenprofil des Kunden zu erstellen. Um diesem auf seine individuellen Wünsche zugeschnittene Informati-

[71] OSCI: Online Services Computer Interfaces. Wird inzwischen durch HBCI ersetzt.

onen in Form eines Newsletters übermitteln zu können, werden dessen Interessen möglichst umfassend und detailliert erfragt. Die Erstellung eines derartigen Profils erfolgt in drei Stufen. Nach Festlegung der Kundeninteressen wird das erstellte Profil durch den FTA in einer serverseitigen Datenbank abgespeichert. Für die Zukunft ist geplant, die Profildaten zusätzlich auf einer multifunktionalen Chipkarte des Nutzers zu speichern, damit sie der ubiquitären Nutzung bereit stehen. Für die Nutzung der Online-Dienste, benötigt der Kunde eine Zugriffsberechtigung. Durch die Eingabe eines Loginnamens sowie Passwortes identifiziert er sich und weist somit seine Berechtigung nach.

Neben dem individualisierten Angebot bietet der FTA auch Angebote für alle Anwender. Hierzu wird ein allgemeiner Newsletter auf der kommunalen Homepage zur Verfügung gestellt. Diesen kann jedermann ohne Zugriffsberechtigung einsehen. Der allgemeine Newsletter kann unter Angabe einer E-Mail-Adresse abonniert werden.

Der Newsletter wird wöchentlich erstellt. Der allgemeine Newsletter enthält lediglich Empfehlungen der Redaktion mit kurzer Beschreibung der einzelnen Veranstaltungen. In dem auf die individuellen Wünsche angepassten Newsletter sind Informationen über Ort, Zeit und Inhalt der Veranstaltung mit einem Link auf vollständige Informationen sowie Stadtplan enthalten. Außerdem bekommt der Nutzer mit einem Link auf das Ticket- Büro die Möglichkeit, Eintrittskarten zu bestellen und zu zahlen. Bei Änderung der erteilten Angaben, wird der Empfänger des Newsletters automatisch über e-Mail benachrichtigt. Dafür muss protokolliert werden, wer welche Daten erhalten hat, und zwar in der Weise, dass entweder die Veranstaltungen oder die Empfänger gespeichert werden.

3. Infrastruktur des Electronic Government

Damit die Transaktionen im E-Government ihr Ziel erreichen, ist eine funktionierende informationstechnische Infrastruktur unabdingbar. Nur dann, wenn die Informationstechnik eine geeignete Basis zur Abwicklung der Verwaltungsdienstleistungen bietet, können die komplexen Anforderungen an eine Verwaltungsmodernisierung erfüllt werden. Eine sichere Informationstechnologie bildet das Instrument für alle beteiligten Akteure zur Nutzung von E-Government-Verfahren. Im Folgenden werden die einzelnen technischen Komponenten der Infrastruktur in einer abstrakten Form erläutert.

3.1 Zugang, Portale und Plattform

Der Zugang zum digitalen Stadttor kann über den PC, das Handy oder über betreute Kioske[72] an öffentlichen Stellen erfolgen. Der Zugang wird von Telekommunikationsdiensteanbietern oder Internet Service Providern ermöglicht.

Damit sich die Verfahren beim Bürger und bei der Verwaltung „verstehen“, muss eine von allen genutzte Plattform die Kompatibilität der unterschiedlichen Hard- und Soft-

[72] In Bremen wird der Zugang über betreute Kioske durch Bremen Online Services ermöglicht; ähnliche Einrichtungen in Hamburg, Berlin und Köln stellen diese ebenfalls zur Verfügung.

warekomponenten gewährleisten, so dass ein problemloser Austausch an Daten stattfinden kann. Die Plattform sollte ein schnelles und zuverlässiges System für den Nutzer darstellen. Sie sollte für die unterschiedlichsten Endnutzer zugänglich sein.

Kommt der Bürger am digitalen Stadttor an, so muss er sich orientieren können. Als ein solches Stadttor bieten Internet-Portale der Verwaltung einen Überblick und Informationen zu verschiedenen Verwaltungsbereichen, zu Dienststellen, Aufgabenverteilung, Verfahren und Formulare von einer zentralen Stelle. Von diesem Portal aus gelangt der Bürger auch an ein oder mehrere „Front-Offices". Auch kann seine Anfrage an die zuständige Stelle automatisiert weitergeleitet werden. Kann die Angelegenheit nicht automatisiert oder im „Front-Offices" erledigt werden, wird ein spezialisiertes „Back Office" eingeschaltet. Sofern die Zuordnung der Anfrage zur zuständigen Stelle problematisch ist, bietet sich die Einschaltung einer „Mid-Office genannten Plattform an, die das „Front Office" mit dem „Back Office" verbindet. Sie muss auch die Integration des Angebots, die Sicherheit und die Nachvollziehbarkeit gewährleisten.

Mit dieser Form der Neustrukturierung des Verwaltungszugangs entstehen neue, noch zu organisierende Strukturen. Derzeit geschieht der Aufbau von Plattformen in Deutschland in sehr unterschiedlicher Art und Weise. Gerade in der Verwaltung werden kommunale Leistungen auch durch andere Kommunen oder die Bundesverwaltung genutzt. Insoweit wird eine einheitliche Plattform notwendig.[73] Vor diesem Hintergrund gehen die Bestrebungen hin zu einem einheitlichen Modell.

Sowohl im Zugangsbereich als auch in den Plattform-Anwendungen und in den Portalen werden vielfältige und aussagekräftige personenbezogenen Daten verarbeitet. Diese drei „Gatekeeper" können von Kommunen selbst, von Privaten und auch in Public Private Partnership betrieben werden.

3.2 Bezahlverfahren

Um das gesamte Verwaltungsverfahren elektronisch abzuwickeln, muss auch die Zahlung der durch die vorgenommene Amtshandlung angefallenen Gebühr über das Internet vorgenommen werden können. Der Nutzer sollte nach Erhalt der erwünschten Verwaltungsleistung die fällige Gebühr synchron, also ohne nennenswerte zeitliche Verzögerung, ausgleichen können. Vor dem Hintergrund der Datensparsamkeit und der Datenvermeidung sollte auch das Bezahlen im Internet anonym oder unter Verwendung von Pseudonymen ermöglicht.[74] Dort, wo im Verwaltungshandeln eine Identifizierung nicht erforderlich ist, könnte die Zahlung anonym mit der Geldkarte erfolgen. In anderen Fällen kann durch eine Kreditkarte mit SET unter einem Pseudonym gezahlt werden.

---

73 Vgl. hierzu das in Österreich entwickelte nationale Portal unter www.help.gv.at oder VM 1998, 136 ff.

74 Vgl. zur prototypischen Umsetzung von Zahlungen im Internet unter Pseudonymen die Beschreibung des Projekts „DASIT" in: Jahrbuch Telekommunikation 2001, 422.

Insbesondere durch die Bewegungen im Bereich des E-Commerce haben sich in den letzten Jahren eine Vielzahl an Bezahlverfahren entwickelt. Allerdings hat sich nicht eine einzige von den vielen Erfindungen seit Mitte der Neunziger Jahre zu einem gängigen Zahlungssystem im Internet durchsetzen können.[75] Die Zahlung findet bei elektronischen Einkäufen nach wie vor auf konventionellem Wege statt.[76] Die Entwicklungen im Bereich des E-Government werfen jedoch ein anderes Bild auf: In den laufenden Pilotprojekten werden bereits für verschiedene Anwendungsfelder elektronische Zahlungsmethoden, nämlich die Geldkarte, eingesetzt.[77] Auf Seiten der Behörde muss ein Verfahren entwickelt werden, das die Zuordnung von Kassenzeichen und eingegangenen Zahlungen ermöglicht.[78]

3.3 Verschlüsselung

Die Kommunikation zwischen Bürgern, Mittlern, Unternehmen und Behörden ist gegenüber Dritten zu schützen. Zur Gewährleistung der Vertraulichkeit ist eine Vielzahl an Verschlüsselungsverfahren vorhanden. So wird beispielsweise mittels Secure Socket Layer (SSL) eine Kanalverschlüsselung zwischen den kommunizierenden Rechnern aufgebaut. Eine Verschlüsselung der elektronischen Dokumente ermöglichen asymmetrische Verschlüsselungsverfahren wie etwa Pretty Good Privacy (PGP).[79] In diesem Verfahren wird der öffentliche Schlüssel von Freunden für Freunde bestätigt. Soll der öffentliche Schlüssel vertrauenswürdig jedem zur Verfügung stehen, bietet sich der Einsatz einer vertrauenswürdigen dritte Stelle an, ein sogenanntes Trustcenter, die die Gültigkeit des öffentlichen Schlüssels zertifiziert.[80]

3.4 Signaturen

Gerade im öffentlichen Sektor werden an die sichere Identifizierung der Kommunikationspartner und an eine unverfälschte Übertragung der Dokumente hohe Anforderungen gestellt.[81] Vor diesem Hintergrund werden elektronische Signaturen zu notwendigem Werkzeug in der Behördenkommunikation. Sie sind die Basistechnologie des elektronischen Rechtsverkehrs.

Elektronische Signaturen[82] werden in vielen Verfahren des Electronic Government Anwendung finden, in denen auch personenbezogene Daten verarbeitet werden, und dort

---

75 First Virtual, CyberCash, Mondex und eCash zähle zu den ersten Verfahren und sind bereits eingestellt wurden.

76 *Grimm* 2001, 197.

77 In Hannover kann so z.B. für den Erhalt einer einfachen Melderegisterauskunft die Gebühr mit der Geldkarte gezahlt werden; in Bremen wird in Zusammenarbeit mit den Sparkassen insbesondere die Geldkarte in die Abwicklungsprozesse eingebunden.

78 *Hagen* 2001, 228.

79 *Hagen* 2001, 250.

80 Dies entspricht auch dem Modell des SigG für elektronische Signaturen.

81 *Roßnagel* 1999b, 158.

82 Ausführlich dazu *Roßnagel*, MMR 1999, 261.

vor allem zur sicheren Identifizierung eingesetzt werden. Dadurch kann das Aufkommen und die Nutzung personenbezogener Daten erhöht werden. Signaturverfahren ermöglichen aber auch Verbesserungen im Datenschutz, weil mit ihrer Hilfe in vielen Verfahren eine sichere Datenverarbeitung möglich ist, ohne dass für die verantwortliche Stelle der Personenbezug der Daten hergestellt werden muss. Insofern ergänzen sich elektronische Signaturen und pseudonyme Zertifikate. Eine sozialverträgliche Nutzung der Informations- und Kommunikationstechniken wird bei einer breiten Verwendung elektronischer Signaturen nur dann gewährleistet sein, wenn beide gleichberechtigt und gleichgewichtig zur Anwendung kommen.[83]

Für die Nutzung von Signaturverfahren zur Erzeugung rechtsverbindlicher Signaturen ist eine Sicherungsinfrastruktur notwendig, deren Knoten Instanzen sind, denen eine Reihe unverzichtbarer Funktionen zugeordnet werden, die diese verlässlich erfüllen müssen. Diese Instanzen verarbeiten für jede ihrer Funktionen personenbezogene Daten. Sie benötigen Datensammlungen zu ausgegebenen Zertifikaten, zur Identität der Zertifikatinhaber, zu deren bestätigten Eigenschaften, Nachweise zur Aushändigung von Chipkarten, Verzeichnisse der Zertifikate mit öffentlichen Schlüsseln und Namen, der Gültigkeitsdauer der Zertifikate, Listen zu Pseudonymen und deren Klarnamen, Listen gesperrter Zertifikate und ähnliche Sammlungen. Diese Daten müssen teilweise allgemein, teilweise auf berechtigte Nachfrage dem Rechtsverkehr zur Verfügung gestellt werden, damit rechtsverbindliche Telekooperation überhaupt möglich sein wird.[84]

Signaturverfahren und ihre Infrastruktur verursachen und lösen somit wesentliche Datenschutzprobleme eines E-Government. Die Nutzung von elektronischen Signaturen und die Organisation ihrer Infrastruktur innerhalb von E-Government-Anwendungen soll daher etwas ausführlicher beschrieben werden.

3.4.1 Unterschiede in den Signaturverfahren

Nach dem neuen SigG ist zwischen drei Stufen elektronischer Signaturverfahren mit unterschiedlichem Sicherheitsniveau zu unterscheiden:[85]

Nach § 1 Abs. 2 SigG sind *sonstige Signaturverfahren*, die nicht den Anforderungen des Signaturgesetzes entsprechen, weiterhin zulässig.

?? Sie können frei angeboten und genutzt werden und unterliegen keiner staatlichen Kontrolle.

?? Sie können aber mangels Kenntnis ihrer Qualität keine spezifische Handlungsform erfüllen und keine Beweiserleichterung genießen.

„*Qualifizierte" Signaturverfahren* entsprechen den europaweit geltenden Anforderungen der europäischen Richtlinie für elektronische Signaturen. Sie erfüllen jedoch nicht die Voraussetzungen, die das ursprüngliche SigG an elektronischee Signaturverfahren gestellt hat. Von diesen unterscheiden sie sich im Wesentlichen in drei Punkten:

---

83 S. *Roßnagel/Wedde/Hammer/Pordesch* 1990, 240 ff.; *Roßnagel*, DuD 1995, 582 (584 ff.); *Bäumler* 2001, 113 ff.

84 S. *Roßnagel*, DuD 1995, 584f.; *Greeenleaf/Clarke* 1997, Kap. 3.2.

85 S. hierzu näher *Roßnagel*, NJW 2001, 1820.

?? Qualifizierte Signaturverfahren müssen zwar die Anforderungen erfüllen, die §§ 4 bis 10 SigG an sie stellen. Die Einhaltung der Anforderungen wird jedoch nicht vorab überprüft. Vielmehr müssen Zertifizierungsdiensteanbieter nach § 4 Abs. 3 SigG die Aufnahme ihres Betriebs der Regulierungsbehörde mit der Betriebsaufnahme anzeigen. Gleichzeitig haben sie in geeigneter Form darzulegen, dass die Betriebsvoraussetzungen vorliegen. Sie unterliegen zwar der Aufsicht der Regulierungsbehörde, doch kann mangels systematischer Prüfung auch daraus nicht verlässlich geschlossen werden, dass jede Zertifizierungsstelle auch tatsächlich alle gesetzlichen Voraussetzungen erfüllt. Qualifizierte Signaturverfahren bieten somit keine geprüfte organisatorische Sicherheit.

?? Für qualifizierte Signaturverfahren, die nicht vorab überprüft werden, kann die Regulierungsbehörde nicht die Funktion der Wurzel-Zertifizierungsstelle übernehmen. Sie übernimmt daher für Zertifizierungsdiensteanbieter, die wegen Konkurs oder aus anderen Gründen ihren Betrieb einstellen, auch nicht die ausgestellten Zertifikate und die Verzeichnisse. In diesem Fall ist keine weitere Überprüfung der Zertifikate mehr möglich. Qualifizierte Signaturen bieten somit keine Gewähr für eine langfristige Verfügbarkeit.

?? Qualifizierte Signaturen müssen zwar mit einer „sicheren Signaturerstellungseinheit“ erzeugt worden sein. Nach § 17 Abs. 4 SigG sind für qualifizierte Signaturverfahren nur die Signaturerstellungseinheiten vorab zu überprüfen, nicht jedoch die Signaturprüf- und Signaturanwendungskomponenten und auch nicht die technischen Komponenten für Verzeichnis-, Sperr- und Zeitstempeldienste. Ob in qualifizierten Signaturverfahren ausreichend sichere Komponenten eingesetzt worden sind, kann nach dieser Rechtslage nicht unterstellt werden. Für Signaturprüf- und Signaturanwendungskomponenten wird es nach § 17 Abs. 2 SigG sogar dem Nutzer überlassen, ob er die dort beschriebenen sicheren Komponenten benutzt. Deren Einsatz ist ausdrücklich nicht Voraussetzung für qualifizierte elektronische Signaturen. Qualifizierte Signaturverfahren bieten somit keine umfassend geprüfte technische Sicherheit.

Nach § 15 SigG entsprechen *„akkreditierte“ Signaturverfahren* dem geprüften Sicherheitsniveau des ursprünglichen SigG. Nach den dort genannten Voraussetzungen werden sie nur in Deutschland akkreditiert. Doch können auch ausländische Anbieter die Akkreditierung erlangen, wenn sie die Voraussetzungen erfüllen. Im Gegensatz zu qualifizierten elektronischen Signaturverfahren bieten sie in folgenden drei Punkten weitergehende Sicherheit:

?? Akkreditierte Zertifizierungsdiensteanbieter werden von Prüf- und Bestätigungsstellen sowie der Regulierungsbehörde vor Betriebsaufnahme geprüft und können damit den „Nachweis der umfassend geprüften administrativen Sicherheit“ (§ 15 Abs. 1 SigG) erbringen.

?? Akkreditierte Signaturverfahren gewährleisten eine langfristige Verfügbarkeit der Zertifikate. Stellt ein akkreditierter Zertifizierungsdiensteanbieter seinen Betrieb ein, werden die von ihm ausgestellten Zertifikate von der Regulierungsbehörde übernommen. Dadurch ist sichergestellt, dass alle Zertifikate von akkreditierten Zertifizierungsdiensteanbietern mindestens 30 Jahre lang nach Ende der Gültigkeit des Zertifikats überprüft werden können.

?? Akkreditierte Signaturverfahren verfügen auch über den Nachweis umfassender technischer Sicherheit. Nach § 15 Abs. 7 SigG müssen alle technischen Komponenten für den Einsatz in akkreditierten Signaturverfahren vorab überprüft werden.

Für die Bewertung des organisatorischen und technischen Sicherheitsniveaus qualifizierter Signaturverfahren ist zu berücksichtigen, dass diesen nach § 23 SigG ausländische Signaturverfahren und Produkte gleichgestellt werden müssen.[86] Nach § 23 Abs. 1 SigG sind alle Signaturen mit Zertifikaten aus der EU oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, die Art. 5 Abs. 1 RLeS erfüllen, qualifizierten elektronischen Signaturen gleichgestellt. Für diese europäischen qualifizierten Signaturverfahren dürfte vielfach kein mit §§ 4 und 19 SigG vergleichbares Überwachungssystem bestehen. Noch weniger kann eine gleichwertige Sicherheit angenommen werden, wenn nach § 23 Abs. 2 SigG Signaturen, die auf Zertifikaten aus Drittstaaten beruhen, deshalb qualifizierten elektronischen Signaturen gleichgestellt werden müssen, weil ein in der EU niedergelassener Zertifizierungsdiensteanbieter für die Zertifikate seines internationalen Partners einsteht. Dies begründet nur einen zusätzlichen Haftungsschuldner, nicht aber einen Nachweis ausreichender Sicherheit. Nach § 23 Abs. 3 SigG müssen Produkte für elektronische Signaturen – dies betrifft vor allem Signaturerstellungseinheiten, weil nur diese nach Art. 3 Abs. 4 RLeS einer Vorabprüfung unterliegen – als für qualifizierte Signaturverfahren ausreichend anerkannt werden, wenn in einem anderen Mitgliedstaat der EU oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum festgestellt wurde, dass sie den Anforderungen der Richtlinie entsprechen. Umfang und Intensität der Überprüfung sind weder bekannt noch beeinflussbar.

Dagegen sind ausländische elektronische Signaturen mit Signaturen aus einem akkreditierten Signaturverfahren und ausländische Produkte mit geprüften Produkten für akkreditierte Signaturverfahren nach §§ 23 Abs. 2 und 15 Abs. 8 SigG nur dann gleichgestellt, wenn eine gleichwertige Sicherheit nachgewiesen worden ist.

Nach alledem erscheint es für die Verwaltung in vielen Anwendungszusammenhängen sinnvoll akkreditierte statt bloß qualifizierter Signaturverfahren zu nutzen. Wenn aber für Anwendungen, in denen sicher nachprüfbare oder langfristig verfügbare Signaturen genutzt werden sollen, akkreditierte Signaturverfahren verwendet werden müssen, macht es keinen Sinn, in anderen Zusammenhängen noch ein zweites Signaturverfahren zu verwenden, sondern es erscheint wirtschaftlicher, immer dann, wenn Signaturen gefordert werden oder sinnvoll erscheinen, mit den akkreditierten Signaturverfahren diejenigen mit dem höchsten Sicherheitsniveau zu verwenden.

3.4.2 Optionen zur Realisierung einer Sicherungsinfrastruktur

Grundsätzlich bestehen für die Verwaltung fünf unterschiedliche Möglichkeiten, sich an einer Publik Key Infrastruktur (PKI) zu beteiligen oder diese zu nutzen:

1. *Zertifizierung durch fremde Zertifizierungsdiensteanbieter*: Die Verwaltung betreibt keine eigene Zertifizierungsstelle. Bürger, Mitarbeiter der Wirtschaftsunternehmen und

86 S. hierzu und zum Folgenden näher *Roßnagel*, NJW 2001, 1817 ff.

die Mitarbeiter der Verwaltungsbehörden werden vielmehr Kunden bei einer oder verschiedenen Zertifizierungsdiensteanbietern. Sie verwenden im Kontakt mit den Behörden und untereinander die von diesem akkreditierten Zertifizierungsdiensteanbieter vergebenen Schlüssel. Zertifikate werden im Namen des Zertifizierungsdiensteanbieters erteilt, die Chipkarte tragen ihr Logo. Der Zertifizierungsdiensteanbieter betreibt selbst Registrierungsstellen. In diesem Fall haftet der Zertifizierungsdiensteanbieter nach § 11 SigG für ihr eigenes Handeln. Die Verwaltung ist ausschließlich Kunde der Zertifizierungsstelle, soweit ihre Mitarbeiter zertifiziert werden.

2. *Tätigwerden im Auftrag des fremden Zertifizierungsdiensteanbieters*: Die Verwaltung übernimmt im Auftrag des Zertifizierungsdiensteanbieters die Funktionen mit Kundenkontakt, nämlich Identifizierung, Unterrichtung und Kartenausgabe. Zertifikate werden im Namen des Zertifizierungsdiensteanbieters erteilt, die Chipkarte tragen ihr Logo. Dies ist nach § 4 Abs. 5 SigG zulässig. Allerdings haftet dann der Zertifizierungsdiensteanbieter nach § 11 Abs. 4 für die Registrierungsstelle wie für eigenes Verschulden. Dementsprechend ist diese nach § 4 Abs. 5 i.V.m. Abs. 2 Satz 4 SigG in das Sicherungskonzept der Zertifizierungsdiensteanbieter einzubinden. Der Zertifizierungsdiensteanbieter muss ihre Sicherheitspolitik auch gegenüber der Verwaltung durchsetzen können. Folgefragen sind: Wie ist die Registrierungsstelle in das Sicherheitskonzept des Zertifizierungsdiensteanbieters eingebunden? Welche Sicherheitsmaßnahmen sind in der Registrierungsstelle und in der Zertifizierungsdiensteanbieter vorgesehen? Wie erfolgt die Übermittlung der Daten, der Chipkarten? Wie erfolgt Registrierung und Ausgabe der Chipkarten?

Ein Beispiel einer Zusammenarbeit zwischen „Trustcenter“ und einer Meldebehörde besteht seit Januar 1998 in Hamburg. Dort übernimmt das Kundenzentrum des Bezirksamts Hamburg-Nord die Identitätsfeststellung der Antragsteller mit Hilfe des Melderegisters (http://www.trustcenter.de). Den „elektronischen Ausweis“ stellt dann die „TC TrustCenter for Security in Data Networks GmbH“ aus. Jeder Hamburger kann einen „elektronischen Ausweis“ beantragen, Privatpersonen erhalten ihn kostenlos. Er kann zum Verschlüsseln und zum Signieren benutzt werden.

3. *Zertifizierung im Auftrag der Verwaltung*: Ein privates Unternehmen betreibt eine Zertifizierungsstelle im Namen und im Auftrag der Verwaltung (virtuelles Trustcenter). Hierzu gibt es zwei Unteralternativen:

a) *Die Verwaltung tritt selbst als Zertifizierungsdiensteanbieter auf*: Sie beantragt bei der Regulierungsbehörde die Akkreditierung und weist alle Akkreditierungsvoraussetzungen selbst nach. Die Akkreditierung wird ihr erteilt. Diese Aufgaben müssen von der Verwaltung nur verantwortet, jedoch nicht technisch und wirtschaftlich umgesetzt werden. Für den Betrieb einer Zertifizierungsstelle kann sich die Verwaltung auch der Dienstleistungen eines privaten, nach dem Signaturgesetz akkreditierten Zertifizierungsdiensteanbieters bedienen. Außerdem könnte die Verwaltung innerhalb der in eigener Verantwortung aufgebauten PKI die Funktionen mit Kundenkontakt übernehmen und dem fremden Zertifizierungsdiensteanbieter die Zertifizierung, die Verzeichnisdienste, die Sperrdienste und eventuell die Schlüsselerzeugung und Personalisierung übertragen. Diese Alternative entspricht spiegelbildlich der Alternative 2. Sie ist nach § 4 Abs. 5 SigG zulässig. Allerdings haftet dann die Verwaltung nach § 11 Abs. 4 für den beauftragten Zertifizierungsdiensteanbieter wie für

eigenes Verschulden. Dementsprechend ist diese nach § 4 Abs. 5 i.V.m. Abs. 2 Satz 4 SigG in das Sicherungskonzept der Verwaltung einzubinden. Die Verwaltung muss ihre Sicherheitspolitik auch gegenüber dem Zertifizierungsdiensteanbieter durchsetzen können.

Diese Lösung haben die Bundesnotarkammer und einige Steuerberater- und Rechtsanwaltskammern gewählt. Sie sind als Zertifizierungsdiensteanbieter von der Regulierungsbehörde akkreditiert. Sie betrieben jedoch die Zertifizierungsstelle nicht selbst, sondern lassen sie in ihrem Namen von der Signtrust (Deutsche Post AG) oder der DATEV betreiben.

b) *Der fremde Zertifizierungsdiensteanbieter handelt im Auftrag der Verwaltung*: Bürger, Mitarbeiter der Wirtschaftsunternehmen und die Mitarbeiter der Verwaltungsbehörden erhalten ihre Zertifikate von der beauftragten Stelle im Auftrag der Verwaltung. Das fremde Unternehmen ist der akkreditierte Zertifizierungsdiensteanbieter nach § 15 SigG und erfüllt alle Pflichtdienstleistungen eines Zertifizierungsdiensteanbieters nach dem Signaturgesetz. Im Zertifikat muss der Name des Zertifizierungsdiensteanbieters aufgeführt sein. Allerdings kann die Chipkarte das Logo der Verwaltung tragen. Soweit die Verantwortung und Haftung des Zertifizierungsdiensteanbieters für den Nutzer klargestellt bleibt, kann deutlich gemacht werden, dass die Verwaltung den Zertifizierungsdiensteanbieter beauftragt hat. Grundsätzlich haftet der Zertifizierungsdiensteanbieter nach § 11 SigG. Sie kann aber eine interne Haftungsfreistellung, -beteiligung- oder -übernahme mit der Verwaltung vereinbaren. Die Verwaltung kann Teilaufgaben im Rahmen des Sicherheitskonzepts des Zertifizierungsdiensteanbieters entsprechend Alternative 2 übernehmen.

4. *Eigene Zertifizierungsstelle der Verwaltung*: Die Verwaltung selbst betreibt eine eigene Zertifizierungsstelle. Sie erfüllt alle Pflichtdienstleistungen eines Zertifizierungsdiensteanbieters nach dem Signaturgesetz und hat die Akkreditierung nach § 15 SigG erhalten. Bürger, Mitarbeiter der Wirtschaftsunternehmen und die Mitarbeiter der Verwaltungsbehörden erhalten ihre Zertifikate von der Zertifizierungsstelle der Verwaltung. Im Unterschied zur Alternative 3a übernimmt die Zertifizierungsstelle der Verwaltung auch die Funktionen Zertifizierung, Verzeichnisdienste, Sperrdienste und eventuell Schlüsselerzeugung und Personalisierung. Sie haftet selbst nach § 11 SigG.

5. *Gemeinsame Zertifizierungsstelle*: Die Verwaltung schließt sich mit mehreren anderen Verwaltungen zusammen, um eine gemeinsame Zertifizierungsstelle zu betreiben, die alle Pflichtdienstleistungen eines Zertifizierungsdiensteanbieters nach dem SigG erfüllt. Bürger, Mitarbeiter der Wirtschaftsunternehmen und die Mitarbeiter der Verwaltungsbehörden erhalten ihre Zertifikate von der gemeinsamen Zertifizierungsstelle. Diese müsste eine eigene Rechtspersönlichkeit erhalten und ist akkreditierte Zertifizierungsstelle nach § 15 SigG. Sie haftet nach § 11 SigG. Sie muss im Zertifikat als Zertifizierungsdiensteanbieter genannt sein. Allerdings kann sie von den Verwaltungen beauftragt sein. Die Chipkarten können deren Logo tragen.

3.4.3 Datenschutzfragen der Verwaltung von Zertifikaten

Wird die Verwaltung Registrierungs- oder Zertifizierungsstelle sind mehrere Datenschutzanforderungen zu beachten. Werden die Daten ausschließlich von einem externen

Zertifizierungsdiensteanbieter erhoben, verarbeitet und genutzt, muss die Verwaltung als Auftraggeber darauf achten, dass die Datenschutzanforderungen bei diesem beachtet werden.

Erhebung, Verarbeitung und Nutzung personenbezogener Daten

Bei der *Registrierung* sind nach § 5 Abs. 1 SigG die Personen, die ein qualifiziertes Zertifikat beantragen, zuverlässig zu identifizieren. Hierzu sind zumindest die Daten aufzunehmen, die nach § 7 Abs. 1 für das Zertifikat erforderlich sind. Außerdem sind der Personalausweis oder Pass zu überprüfen, zu kopieren und die darin befindlichen Daten zu speichern. Soll das Zertifikat eine Vertretungsmacht für eine dritte Person, berufsbezogene oder sonstige Angaben (Attribute) enthalten, sind auch diese Daten zu erheben. Außerdem sind alle die Daten zu erheben, die für den Nachweis der Attribute notwendig sind, einschließlich der Bestätigung der bestätigenden Stelle. Nach § 14 Abs. 1 Satz 1 SigG sind die Daten ausschließlich beim Betroffenen selbst zu erheben und dürfen nicht von dritten Stellen bezogen werden. Auch die Einwilligung Dritter oder die Bestätigung der Inhalte des Attributs ist vom Antragsteller vorzulegen und nicht direkt von der bestätigenden Stelle anzufordern. Eine Datenerhebung bei Dritten ist nach § 14 Abs. 1 Satz 2 nur mit Einwilligung des Betroffenen zulässig. Diese ist nach § 4a Abs. 1 BDSG schriftlich oder nach §§ 126 Abs. 3, 126a BGB in elektronischen Form mit qualifizierter elektronischer Signatur zu erteilen.[87]

Der Umfang der erhobenen Daten muss sich nach § 14 Abs. 1 SigG auf das für die Zweck eine qualifiziertes Zertifikat Erforderliche beschränken. Diese Umschreibung des Erforderlichkeitsprinzips darf allerdings nicht allzu wörtlich genommen werden. Es dürfen nicht nur die Daten erhoben werden, die im engeren Sinn für den Inhalt des Zertifikats nach § 7 Abs. 1 SigG erforderlich sind, sondern auch alle die Daten, die im weiteren Sinn für das Erbringen der Pflichtdienstleistungen eines Zertifizierungsdiensteanbieters, wie sie im Signaturgesetz beschrieben sind, erforderlich sind. Als hierfür erforderlich können alle die Daten gelten, deren Erhebung andere Vorschriften des Signaturgesetz fordern oder voraussetzen.

Nach §§ 5 Abs. 3 und 7 Abs. 1 Nr. 1 SigG kann der Antragsteller auch verlangen, dass im Zertifikat anstelle seines Namens ein *Pseudonym* aufgeführt wird. Enthält das Zertifikat Angaben über eine Vertretungsmacht oder berufsbezogene oder sonstige Angaben, ist für die Verwendung des Pseudonyms die Einwilligung der dritten Person oder der zuständigen Stelle erforderlich.[88]

Bei der *Zertifizierung* sind Zertifikate mit dem Inhalt des § 7 Abs. 1 SigG oder Attributzertifikate nach § 7 Abs. 2 SigG entsprechend dem Antrag des Betroffenen nach § 7 Abs. 2 SigG auszustellen. Der Inhalt der Zertifikate ist entweder gesetzlich vorgegeben (§ 7 Abs. 1 SigG) oder müssen dem Antrag des Betroffenen entsprechen.[89]

---

87 S. hierzu näher *Roßnagel* 2002, Rn. 48 ff.

88 S. hierzu näher *Roßnagel* 2002, Rn. 61 ff.

89 S. hierzu näher *Roßnagel* 2002, Rn. 72 ff.

Bei der *Personalisierung* sind die Daten zu speichern, die erforderlich sind, um eine Chipkarte einer bestimmten Person zuordnen zu können. Hierzu ist eine Chipkarten-Identifizierungsnummer einem Zertifikat zuzuordnen. Hierfür kann es genügen, die laufende Nummer des Zertifikats nach § 7 Abs. 1 Nr. 4 SigG zu speichern.[90]

Bei der *Ausgabe* der Chipkarte an den Berechtigten ist zu protokollieren, dass der Berechtigte identifiziert wurde. Von ihm ist der Empfang der Chipkarte zu bestätigen.[91]

Für den *Verzeichnisdienst* sind die Zertifikate in das Verzeichnis aufzunehmen. Allerdings hat der Antragsteller die Möglichkeit zu entscheiden, ob die Zertifikate – mit allen Angaben – jedem Abfragenden zugänglich sein sollen (§ 5 Abs. 1 Satz 2 SigG: „abrufbar") oder ob dieser nur die Auskunft erhält, dass das Zertifikat zum Zeitpunkt der Erstellung der elektronischen Signatur gültig war (§ 5 Abs. 1 Satz 2 SigG „nachprüfbar"). Wird ein Sperrvermerk angebracht, darf der Verzeichnisdienst nur die Auskunft geben, dass das Zertifikat ab einem bestimmten Zeitpunkt gesperrt ist. Wurde das Zertifikat mit falschen Angaben ausgestellt, kann der Zertifizierungsdiensteanbieter dies nach § 8 Abs. 1 Satz 4 SigG zusätzlich kenntlich machen. [92]

Nach § 10 SigG hat der Zertifizierungsdiensteanbieter eine *Dokumentation* zu führen, aus der sich ergibt, dass die Anforderungen des Signaturgesetzes und der Signaturverordnung eingehalten worden sind. Die Dokumentation darf nicht nachträglich unbemerkt verändert werden können. Dies setzt ihre Signierung mit elektronischen Signaturen voraus. Nach § 10 Abs. 2 SigG ist dem Signaturschlüssel-Inhaber auf verlangen Einsicht in die ihn betreffenden Daten und Verfahrensschritte zu gewähren.[93]

Ergänzend zu diesen datenschutzrechtlichen Anforderungen an die Tätigkeit des Zertifizierungsdiensteanbieters sind weitere Anforderungen zu beachten, je nach dem welche Organisationsform von der Verwaltung gewählt worden ist.[94] Ist die Verwaltung Anbieter qualifizierter Zertifikate, gelten die Erlaubnistatbestände des SigG und die Datenschutzregeln des § 14 SigG. Ist die Verwaltung kein Zertifizierungsdiensteanbieter und auch keine Außenstelle des Zertifizierungsdiensteanbieters nach § 4 Abs. 4 SigG gelten die Vorschriften des BDSG und des NDSG. Außerdem hängen die zusätzlichen Anforderungen davon ab, wessen Daten verarbeitet werden, nämlich die der öffentlichen Bediensteten oder die der Bürger:

?? Zum Einen werden nämlich die personenbezogenen Daten der Bürger oder der Mitarbeiter der zugelassenen Unternehmen verarbeitet. Insofern sind die Erlaubnistatbestände des Signaturgesetzes und des NDSG oder des § 28 BDSG zu beachten.

?? Zum Anderen sind personenbezogene Daten von Mitarbeitern der Verwaltung zu erheben, zu verarbeiten und zu nutzen. Erfolgt dies durch die Verwaltung selbst, sind neben den allgemeinen Datenschutzregeln die Regelungen des Personaldatenschutzes

90 S. hierzu näher *Roßnagel* 2002, Rn. 70.

91 S. hierzu näher *Roßnagel* 2002, Rn. 71.

92 S. hierzu näher *Roßnagel* 2002, Rn. 80 ff.

93 S. hierzu näher *Roßnagel* 2002, Rn. 124 ff.

94 S. hierzu Kap. 3.4.2.

zu beachten. Wird ausschließlich der private Dienstleister tätig, gelten für diesen die Anforderungen des SigG und ergänzend das BDSG.

Für die personenbezogenen Daten, die für das Erbringen von Pflichtdienstleistungen des Zertifizierungsdiensteanbieters erhoben werden, gilt eine strikte *Zweckbindung*. Sie dürfen nach § 14 Abs. 1 Satz 3 SigG für andere Zwecke nur verwendet werden, wenn der das Signaturgesetz dies erlaubt oder der Betroffene eingewilligt hat. Beispielsweise darf keine Zweckentfremdung für Zwecke der Personaldatenverarbeitung oder Verwaltungszwecke erfolgen. Um dies zu gewährleisten, ist eine entsprechende Abschottung der Datenverarbeitung der Registrierungs- oder Zertifizierungsstelle sicherzustellen.

Pseudonyme

Werden in die Zertifikate statt des Namens Pseudonyme aufgenommen, gelten grundsätzlich die gleichen datenschutzrechtlichen Anforderungen. Zwar wirken die Pseudonyme gegenüber Dritten wie anonyme Daten und fallen damit aus dem Geltungsbereich des Datenschutzrechts heraus. Gegenüber dem Kenner der Zuordnungsregel zwischen Pseudonym und dessen Träger sind die Pseudonyme jedoch personenbezogene Daten und unterliegen voll den Anforderungen des Datenschutzrechts.[95]

Für die Verwendung von Pseudonymen dürfte zwischen Trägern öffentlicher Ämter und Privatpersonen zu unterscheiden sein.

?? Im Regelfall dürften die Träger öffentlicher Ämter hoheitliche Handlungen immer nur mit ihrem wahren Namen durchführen können. Insofern wären für diese keine pseudonymen Zertifikate vorzusehen.

?? Dagegen sollten Privatpersonen auch gegenüber der Verwaltung pseudonym handeln können, sofern nicht ihre Identifizierung zur Erfüllung der Verwaltungsaufgaben unabdingbar erforderlich ist.

Zu beachten ist allerdings, dass die zuständigen Stellen nach § 14 Abs. 2 SigG gegenüber dem Zertifizierungsdiensteanbieter einen Aufdeckungsanspruch haben, wenn dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist. In diesem Fall sind die Auskünfte zu dokumentieren und dem Betroffenen grundsätzlich mitzuteilen.

Während für die genannten Behörden ein Aufdeckungsanspruch besteht, ist dieser für Privatpersonen und die übrigen Behörden ausgeschlossen. Im neuen Signaturgesetz ist in § 14 Abs. 2 SigG insofern ein erster Schritt in Richtung auf ein Aufdeckungsverfahren unternommen worden, als auch Gerichte im Rahmen anhängiger Verfahren eine Aufdeckung anordnen können, der durch die neuen §§ 142, 144, 371 und 428 ZPO unterstützt wird. Dennoch ist ein eigener Aufdeckungstatbestand für Pseudonyme erforderlich.

---

95 S. *Roßnagel/Scholz*, MMR 2000, 721 ff.

Namenszusätze in Zertifikaten

Nach § 7 Abs. 1 Nr. 1 SigG ist im Zertifikat der Name des Signaturschlüssel-Inhabers bei einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen. Dies ermöglicht zwar eine Unterscheidung von mehreren Personen gleichen Namens, ermöglicht jedoch dem Empfänger einer signierten Nachricht noch keine Feststellung, um welche der Personen gleichen Namens es sich im jeweiligen Fall handelt.

Um in einem solchen Fall feststellen zu können, um welche Person es sich handelt, können im signierten Dokument oder einer ebenfalls signierten Anlage weitere Daten (z.B. Geburtsdatum, Geburtsort, Adresse oder Personalausweisnummer) angegeben oder diese Daten ins Zertifikat oder ein Attribut-Zertifikat aufgenommen werden. Dabei ist allerdings darauf zu achten, dass der Grundsatz der „Datensparsamkeit" sowie die Entscheidungsfreiheit des Antragstellers weitestmöglich beachtet werden. Dabei ist zu berücksichtigen, dass das Zertifikat in allen künftigen Kontakten des elektronischen Rechtsverkehrs benutzt werden wird, nicht nur im Kontakt mit einer bestimmten Behörde. Wenn die Behörde weitere Daten benötigt, kann sie diese vom Betroffenen einfordern und bei weiteren elektronischen Kontakten von dem bereits bekannten Namenszusatz auf diese Zusatzinformationen schließen.[96]

Beziehungen zwischen öffentlichen Bediensteten und Zertifizierungsdiensteanbietern

Je nach dem, welches Organisationsmodell die Verwaltung für die Sicherungsinfrastruktur wählt, ergeben sich unterschiedliche Probleme für die Beziehungen zwischen öffentlichen Bediensteten und dem Zertifizierungsdiensteanbieter.

Nach § 5 Abs. 1 SigG ist ein individueller Antrag des Bediensteten beim Zertifizierungsdiensteanbieter auf Ausstellung eines qualifizierten Zertifikats erforderlich. Er selbst ist Signaturschlüssel-Inhaber und kann nur in Person die Rechte eines Signaturschlüssel-Inhabers ausüben. Umgekehrt muss der Zertifizierungsdiensteanbieter den Antragsteller nach § 6 SigG unterrichten. Ihm muss die Chipkarte in sicherer Weise übergeben werden. Er kann die Sperrung seines Zertifikats beantragen. Außerdem dürfen die Daten für die Zertifizierung nach § 14 Abs. 1 SigG nur beim künftigen Signaturschlüssel-Inhaber erhoben werden. Daher setzt das Signaturgesetz eine eigene Rechtsbeziehung zwischen Bedienstetem und Zertifizierungsdiensteanbieter voraus.

Soll der Bedienstete im Rahmen des elektronischen Rechtsverkehrs das Signaturverfahren als Arbeitsmittel zur Erfüllung seiner Dienstaufgaben nutzen, kann die Antragstellung nicht seinem Belieben überlassen werden. Vielmehr setzt ein koordiniertes Angebot von Verfahren des Electronic Government einen ebenso koordinierten Einsatz von Signaturverfahren voraus. Hier ergeben sich nun unterschiedliche Probleme, je nach dem ob die Verwaltung selbst die Zertifizierungsdienste erbringt oder sie an private Unternehmen überträgt.

?? Bietet die Verwaltung selbst die Zertifizierungsdienste an, zertifiziert sie selbst ihre Bediensteten. Eigenständige Vertragsverhältnisse sind hierfür nicht erforderlich.

96 S. hierzu auch *Roßnagel* 2002, Rn. 52.

Vielmehr erfolgt die Antragstellung und das Angebot der Pflichtdienstleistungen eines Zertifizierungsdiensteanbieters im Rahmen des Beschäftigungsverhältnisses.

?? Nimmt dagegen die Verwaltung die Dienste eines privaten Unternehmens in Anspruch entstehen die Probleme, wie das Rechtsverhältnis zwischen Bediensteten und privatem Unternehmen zu qualifizieren ist, welcher Entscheidungsspielraum dem Bediensteten dabei verbleibt und ob der Dienstherr ihn zur Antragstellung und später zur Nutzung von Signaturverfahren verpflichten kann.

Es wird davon auszugehen sein, dass der öffentlich Bedienstete im Rahmen seiner Treuepflicht verpflichtet ist, auf Veranlassung des Dienstherrn ein qualifiziertes Zertifikat zu erwerben, soweit der Dienstherr die Kosten trägt und zusichert, eventuell daraus resultierende Haftungsansprüche abzudecken. Im Einzelnen bedarf dies allerdings noch näherer Untersuchungen.

Zur Einführung von Signaturverfahren, die für die Bediensteten verpflichtend sind, bedarf es aber wohl in beiden Konstellationen einer Dienstvereinbarung mit dem Personalrat.

3.4.4 Anforderungen an die technische Komponenten

Die konkreten technischen und organisatorischen Anforderungen sind im Detail davon abhängig, welche der aufgezeigten Organisationsmodelle gewählt werden.

Abstrakt ergibt sich die Antwort hinsichtlich

?? der einzusetzenden Technik aus § 17 SigG und § 14 SigV,

?? der zu treffenden organisatorischen Vorkehrungen aus §§ 5 ff SigG und der diese Regelungen konkretisierenden Vorgaben der §§ 2 bis 9 SigV.

Wird ein akkreditierter Zertifizierungsdiensteanbieter beauftragt oder einbezogen, ist es deren Aufgabe, die Anforderungen des Signaturgesetzes zu erfüllen. Die Verwaltung ist nur insoweit involviert als sie Aufgaben innerhalb der PKI übernimmt. Sie muss in ihren Anwendungen die Produkte des akkreditierten Zertifizierungsdiensteanbieters einbinden.

Alle Nutzer müssen zertifizierte Produkte einsetzen, die ihnen von dem akkreditierten Zertifizierungsdiensteanbieter angeboten werden.

3.4.5 Organisatorische Anforderungen an die Nutzung elektronische Signaturen

Das Signaturgesetz sieht nur Zertifikate für natürliche Personen vor. Allerdings besteht auch das Bedürfnis, dass Mitarbeiter für ihre Organisation handeln.

Die Organisationszugehörigkeit oder das Bestehen einer Vollmacht können in das Zertifikat aufgenommen und bestätigt werden. In diesem Fall ist die getrennte Nutzung des Zertifikats als Privatperson und als Beauftragter des Unternehmens nicht möglich. Für die unternehmensinterne Abrechnung müsste das Unternehmen eine eigene arbeitsver-

tragliche Lösung finden. Für die Verwaltung wäre immer das Unternehmen der Gebührenschuldner.

Organisationszugehörigkeit oder das Bestehen einer Vollmacht können aber auch Inhalt eines Attributzertifikats sein. Dies hätte den Vorteil, dass es von Verwendungsfall zu Verwendungsfall unterschiedlich genutzt werden kann. So könnte zum Beispiel der Mitarbeiter eines Unternehmens den geheimen Schlüssel ohne Attributzertifikat für private Zwecke nutzen, für ein Handeln im Auftrag des Unternehmens mit Attributzertifikat. Attributzertifikate müssen allerdings extra bezahlt werden und kosten derzeit als Einzelzertifikat etwa 40 DM. Bei Verwendung von Attributzertifikaten wäre eine getrennte Gebührenabrechnung gegenüber der Privatperson und dem Unternehmen möglich.

In qualifizierten Zertifikaten oder qualifizierten Attribut-Zertifikaten können auch Vertretungsrechte und Dienstbezeichnungen im öffentlichen Dienst aufgeführt werden. Auch Dienstsiegel können in qualifizierten Zertifikaten – im Form von Pseudonymen („Dienstsiegel der Ordnungsbehörde Hannover“) oder als Attribut zu einem Namen – abgebildet werden.

3.5 Organisatorische Infrastruktur

Damit der Behördenmitarbeiter seine Verwaltungstätigkeit über das Internet ausüben kann, benötigt er in jedem Fall einen PC mit einem Internetzugang. Ein PC-Netz als notwendige Basisinfrastruktur für den Internet- und Intranet-Zugang der Verwaltung und zur Verwaltung ist in allen Städten mit mehr als 50.000 Einwohnern inzwischen vorhanden. Im Durchschnitt sind heute 85 Prozent der Büroarbeitsplätze mit Rechnern ausgestattet, die meisten davon hängen auch an einem Verwaltungsnetz. In zwei Dritteln aller Städte existiert bereits ein kommunales Intranet, und fast jeder zweite Verwaltungsangestellte hat inzwischen Zugang zum Internet und ist per E-Mail erreichbar- bis zum Jahr 2001 sollen es bereits mehr als 80 Prozent sein.[97] Die Anbindung jedes Büroarbeitsplatzes an das Internet, die Schulung der Behördenmitarbeiter sowie die Umstrukturierung der Arbeitsprozesse in der Verwaltung unter Einbindung des Internets sind notwendig für den Aufbau eines E-Government. Der behördenübergreifende elektronische Datenaustausch zwischen den verschiedenen Verwaltungsebenen erfordert eine einheitliche Struktur. Neben den technischen Voraussetzungen ist ein Know-how des Sachbearbeiters im Umgang mit dem technischen Handwerk unumgänglich. Die Schulung der Behördenmitarbeiter in der Nutzung der neuen Technologien und in der Abwicklung der Arbeitsprozesse über das Internet gehört zu den ersten wesentlichen Schritten auf dem Weg zum Electronic Government. Der Einsatz der neuen Technologien in die Verwaltungsentwicklung trägt per se zur Veränderung der Verwaltungsabläufe bei. Diese Neustrukturierung in den Kommunalverwaltungen durch die Zusammenlegung von Bereichen, die Entstehung von Querschnittsaufgaben sowie von Fachbereichen statt der bisher üblichen Ämter, erlebt die öffentliche Verwaltung einen „Paradigmenwechsel“. Daraus geht nicht zuletzt eine Vielzahl neuer Organisationsmodelle

97 *Zypries*, Kommune21 2/2001, S. 13.

in den verschiedenen Verwaltungsbereichen sowie eine veränderte Verteilung der Zuständigkeiten von Stadt zu Stadt hervor.[98]

4. Herausforderungen für den Datenschutz

Die Zahl der Anbieter von Online-Diensten und deren Nutzer ist in den letzten Jahren drastisch gestiegen. Die Nutzung des Internets für die Verwaltung wird zur Erledigung ihrer Aufgaben immer attraktiver. Bei der Bereitstellung von Informationen sowie bei Transaktionen zwischen der Verwaltung und dem Bürger im Internet fallen auf vielfältige Weise personenbezogene Daten an. Datenschutzrechtlich unbedenklich ist es, wenn für diese Daten der Personenbezug vermieden wird. Zwar werden auch in der Papierwelt Daten verarbeitet. In der Online-Kommunikation ist jedoch die Art und Weise sowie der Umfang der Datenverarbeitung anders: Die Datenverarbeitung findet nicht mehr in einer Datenverarbeitungsanlage statt, sondern im Netz mit einer Vielzahl von Beteiligten, in dem die Kontrollmöglichkeiten des Nutzers erheblich eingeschränkt sind.[99] Trotz dieser erheblichen Risiken und durch den Einsatz der Informationstechnik entstehenden Gefährdungen sollten die neuen digitalen Technologien als willkommene Chance verstanden werden.[100] Denn der Datenschutz kann an diesen Herausforderungen wachsen, indem er Lösungen zu einer datenschutzgerechten Infrastruktur entwickelt. Für bestimmte Herausforderungen- wie die Globalisierung der Datenverarbeitung und die dynamische Entwicklung der Technik- wird es keine Lösungen, sondern allenfalls verbesserte Formen im Umgang mit diesen Herausforderungen geben können.[101]

4.1 Zunahme personenbezogener Daten

Sobald eine Verbindung mit einer Website hergestellt ist, hinterlassen Besucher Datenspuren im Netz. Jeder Rechner im Netz verfügt über eine eigene IP-Adresse (Internet Protokoll) und ist durch eine URL (Uniform Resource Locator) gekennzeichnet.[102] Eine Nutzung von Online-Diensten ist nur bei gemeinsamer Übertragung beider Daten möglich. Diese Steuerungsdaten werden sowohl bei dem Kommunikationspartner als auch bei den dazwischen liegenden Routern[103] gelesen.[104] Der Umfang der protokollierbaren Daten lässt sich noch erweitern auf Angaben über das Betriebssystem, den Typ und Version des Browsers, die Verwendung von Protokollen, Cookies und gewählte Sprache. Auf diese Weise lassen sich Reaktionen des Nutzers feststellen. Das Datum, insbesondere bei Zuordenbarkeit zu einer bestimmten Person, wird immer mehr zu einem wichtigen Produkt in einer Datawarehouse- und Datamining-Ära. Die Sammlung und

98 *Grabow/Floeting* 1999, 79.

99 *Engel-Flechsig*, DuD 1997, 10.

100 *Ulrich*, DuD 1996, 664.

101 *Roßnagel/Pfitzmann/Garstka* 2001, 14.

102 *Kesdogan* 2000, 5.

103 Darunter sind Rechner zu verstehen, die das eigene Netzprotokoll in das Transportnetzprotokoll übersetzt, damit die Daten weitergereicht werden; *Esser*, RDV 1996, 47.

104 *Schaar*, DuD 2001, 383.

Zusammenfügung von Daten kann mit niedrigem Kostenaufwand innerhalb kürzester Zeit ortsunabhängig erfolgen. Daten vermitteln jedoch nicht nur Informationen über eine bestimmte Person, sondern schaffen auch „Abbild sozialer Realität".[105]

Mit dem Internet erhalten die Bürger in steigendem Maße die Möglichkeit, sich umfassend zu informieren, Anträge auf eine Verwaltungsleistung zu stellen, eine Genehmigung zu erhalten, also zusammenfassend, Behördengänge virtuell zu beschreiten. Während eine telefonische Anfrage bei der Behörde nicht die Preisgabe personenbezogener Daten voraussetzt oder ein Behördengang nicht mit einer Identifizierung an der Rathaustür verbunden ist, fallen im Vergleich dazu in der elektronischen Verwaltung mehr Daten an. Denn bereits die Nutzung der Online-Angebote geht zwangsläufig mit dem Anfall datenschutzrechtlich relevanter Informationen einher. Hierfür und des weiteren für die Abrechnung sowie den Erhalt der angeforderten Informationen sind in der Regel Angaben zur eigenen Person erforderlich. Daher ist die Offenlegung eigener Daten in der Regel nicht vermeidbar.

Neben den leitungsgebundenen Kommunikationsübertragungen sind auch nicht leitungsgebundene Kommunikationsmöglichkeiten über Erd- oder Satellitenfunk zu beachten. Mit ihnen kann bei geeigneter Infrastruktur von jedem Ort aus kommuniziert werden, was zugleich eine Erhöhung der anfallenden Datenmenge bedeutet. Im Oktober 2000 waren 40 Millionen Mobilfunktelefone (Handys) registriert- mehr als ortsfeste Privatanschlüsse.[106] Geht man davon aus, dass sich künftig immer mehr WAP-fähige Handys durchsetzen und die Übertragungsrate von ca. 40 Kbit/s sich auf 2 Mbit/s über UMTS weiterentwickeln werden, kann ein verbreiteter Nutzen von Mobilfunktelefonen in absehbarer Zukunft angenommen werden.[107] Zwar wird in erster Linie die Verwendung von Mobilfunknetzen im Bereich des M-Commerce gesehen.[108] Dennoch bietet sie auch zur Inanspruchnahme von Online-Angeboten der Verwaltung eine schnelle und flexible Möglichkeit für den Bürger. Der Nutzer kann bequem orts- und zeitunabhängig seine „Behördengänge" machen. Der Trend zu einem Informationszugang „sofort, überall, zu allem" zeichnet sich immer deutlicher ab.[109] Er geht gar noch viel weiter: Durch in Alltagsgegenstände integrierte Prozessoren und Sensoren wird eine Kommunikation von Maschine zu Maschine möglich.[110]

Die Verarbeitung, Speicherung und Übertragung personenbezogener Daten stößt praktisch an keine technischen Grenzen mehr. Zum Einen können bei den heute verfügbaren Speichermedien bei vergleichbarer Kapazität viel größere Datenmengen aufbewahrt werden.[111] Zum Anderen steigt die Leistungsfähigkeit von Prozessoren immer mehr.[112]

---

105 BVerfGE 65, 1, (43).

106 *Pfitzmann*, DuD 2001, 195; die Zahl der Handybesitzer in anderen Ländern liefern ähnliche Ergebnisse, vgl. www.durlacher.com.

107 Vgl. *Pfitzmann*, DuD 1995, 195.

108 Schätzungen zufolge soll der Marktsanteil für Transaktionen mobile Endgeräte 66 Milliarden USD im Jahr 2003 betragen, vgl. www.radiccio.org

109 *Mattern* 2001, 52.

110 *Mattern* 2001; *Scholz*, Kap. 2, i.E.

111 Siehe Abbildung 1 bei *Pfitzmann*, DuD 1999, 194.

Ursache dafür ist die technische Entwicklung der Digitalisierung der Übertragungswege im Telekommunikationsbereich sowie die Datenkompression. Mit dem Einsatz von verdrillten Kupferkabeln bei 768 Kbit/s, Koaxialkabel bis zu 800 Kbit/s und Glasfasern bei 40.000 Mbit/s als Übertragungsleitungen werden dabei nicht nur Qualitätsverluste vollständig vermieden, sondern auch die Vermittlungs- und Übertragungsgeschwindigkeit im Vergleich zu analoger Übertragung erheblich verbessert.[113]

Während die Kommunikation herkömmlich über den Postweg, das Telefon und Fax erfolgte, stehen heute mit dem Internet und der Mobilkommunikation deutlich günstigere und effektivere Nutzungsmöglichkeiten zur Verfügung. Aufgrund der Bedienungsfreundlichkeit dieser Medien erscheint ihr vermehrter Einsatz sehr wahrscheinlich. Des weiteren setzen die herkömmlichen Kommunikationsmittel in der Regel die Fähigkeit zum Lesen und Schreiben voraus, so dass andernfalls der Sachbearbeiter oder Dritte Hilfe leisten müssten. Dagegen können Verwaltungsleistungen durch Videosequenzen oder die Möglichkeit, Bildschirmflächen durch Berühren zu bedienen, insoweit erheblich vereinfacht werden.[114] Diese Veränderungen in der Art und Weise der Kommunikation haben zur Folge, dass die Menge der anfallenden Daten ein unüberschaubares Ausmaß einnimmt, da über das Handy leicht der Standort ermittelt, personenbezogene Daten in großem Umfang ohne Kenntnis des Betroffenen ausgetauscht und sogar Datenbanken angelegt werden können. Insofern wächst die Menge der anfallenden Daten drastisch an.

Im Zuge der Privatisierung und des Outsourcing[115] werden die Aufgaben der öffentlichen Verwaltung auf private übertragen. Die Folge davon ist, dass neben öffentlichen Stellen immer mehr Private personenbezogene Daten erheben, verarbeiten und speichern. Mit der steigenden Anzahl privater Datenverarbeiter geht die Zunahme der anfallenden, personenbezogenen Daten einher.

4.2 Anfall personenbezogener Daten im Internet

Digitale Daten sind in elektronischen Netzen grundsätzlich ubiquitär, da sie sich an beliebigen Orten und zu beliebigen Zeiten gleichzeitig nutzen lassen.[116] Der Anfall von Daten und deren Weg im Netz erfolgt ohne nennenswerten Aufwand und sekundenschnell. Hinzu kommt, dass in fast allen Lebensbereichen Daten digitalisiert, in Computersystemen verarbeitet und über das Internet transportiert werden.[117]

Während der konventionelle Behördengang selbst nicht mit zusätzlichen Daten verbunden ist, erfordert der elektronische Weg zur Behörde oder zum Nutzer die Angabe wei-

---

112 Gordon Moore ging bereits Ende der 60er Jahre dabei von einer Verdoppelungsrate innerhalb von 18 Monaten aus. Für die chipherstellende Industrie stellt dieses „Gesetz“ eine Art self-fulling prophecy dar.

113 *Pfitzmann,* DuD 1999, 194.

114 *Kubicek/Hagen* 1999, 22.

115 Auf die Begriffe wird in Kap. 4.8 näher eingegangen.

116 *Reinermann,* Verw. 1995, 6.

117 Vgl. *Kilian,* DuD 1993, 606.

terer Daten, sogenannter Teledienstedaten. Diese „Mehr-Daten“ in der Online-Welt fallen unabhängig von Inhalt, Zweck und Ausmaß der Kommunikation an. Sie existieren- vereinfacht ausgedrückt- nur deswegen, weil Informationen elektronisch über das WWW transportiert werden bzw. eine Kommunikation im WWW stattfindet. Darüber hinaus kann bei dem Online-Behördengang zum Beispiel registriert werden, welche Anfrage bei welchem Sachbearbeiter erfolgte. Im Folgenden wird dargestellt, welche Daten in einer vernetzten Verwaltung unabhängig von der jeweiligen Anwendung bei wem und wodurch anfallen. Zur Vermeidung von Wiederholungen erfolgt ihre Erläuterung abstrakt und nur beispielhaft an einzelnen Anwendungsfeldern im E-Government.

Jede Verbindungssuche und -herstellung, jeder Tastendruck und jeder Mausklick hinterlässt eine Datenspur.[118] Mit der Nutzung von Telediensten fallen unterschiedliche Arten von Daten an, die sich nach dem Zweck des Vertragsverhältnisses einer bestimmten Datengruppe wie folgt zuordnen lassen:

Inhaltsdaten

Jede Art von Online-Kommunikation der Behörde soll dazu dienen, Informationen an den Bürger zu übermitteln. Die Informationen über Kommunikationsinhalte jeglicher Art, die bei interaktiven Angeboten anfallen, stellen Inhaltsdaten dar. Dies sind die Daten, die grundsätzlich auch in herkömmlichen Kontakten ausgetauscht werden. Sie dürfen nur im Rahmen der Erforderlichkeit unter Beachtung der Zweckbestimmung verarbeitet werden.[119] Die Zulässigkeit ihrer Verarbeitung unterliegt den bereichsspezifischen Regelungen und subsidiär dem Landes- bzw. Bundesdatenschutzgesetz.[120] Inhaltsdaten fallen unabhängig davon an, ob die Verwaltungsleistung digitalisiert über das WWW oder konventionell erbracht wird. Sie sind für die Verwaltungsmaßnahme in der Regel erforderlich. Bei der einfachen Melderegisterauskunft handelt es sich zum Beispiel um die Angabe von Namen, Anschrift und Namensbestandteilen. Im Bauwesen geht es um die Daten, die im jeweiligen Formular benötigt werden.

Verbindungsdaten

Zur Nutzung eines Dienstleistungsangebots der Behörde muss der Nutzer eine Netzverbindung aufbauen und die Webseite der Behörde aufrufen. Dies geschieht durch Einwählen beim Zugangsrechner des Access-Providers (Zugangsvermittler)[121] und durch Anmeldung mittels Passwortes.[122] Nach der Legaldefinition des § 2 Nr. 4 TDSV sind Verbindungsdaten personenbezogene Daten eines an der Telekommunikation Beteiligten, die bei der Bereitstellung und Erbringung von Telekommunikationsdiensten erhoben werden. Durch den Verbindungsaufbau entstehen sowohl Daten bei dem Provider als auch Einträge in der Logdatei des Terminalservers. Die Verbindungsdaten werden

118 *Simitis*, NJW 1997, 1903; Wiese 2000, 12.

119 *Schaar*, DuD 1996, 136.

120 *Bizer*, in: RMD, § 3 TDDSG Rn. 4.

121 Zugangsvermittler können aus technischer Sicht mehrere Beteiligte wie z.B. der Internet-Service-Provider oder Online- Dienst-Anbieter und ggf. zusätzlich Zugangsvermittler sein, siehe *Köhntopp/Köhntopp*, CR 2000, 249.

122 *Scholz*, Kap. 3, i.E.

nicht vom TDDSG erfasst. Soweit bei der Inanspruchnahme von Telediensten Verbindungsdaten anfallen, finden die Vorschriften der TDSV Anwendung.

Bestandsdaten

Als Bestandsdaten sind personenbezogene Daten eines Nutzers zu verstehen, die im Zusammenhang mit der Begründung und Änderung eines Vertragsverhältnisses verarbeitet, erhoben oder genutzt werden.[123] Sie sind quasi Grunddaten eines Vertragsverhältnisses und ihre Verarbeitung zulässig, soweit sie für das Vertragsverhältnis benötigt werden.

Sofern die Verwaltung einen Teledienst anbietet und nicht nur nutzt, könnte dies zwischen ihr und dem Bürger oder einem Unternehmen in Form eines Teledienst-Vertrages erfolgen. Für dessen Abschluss könnten zum Beispiel Name, Vorname, Anschrift, Rufnummer, Teilnehmer- oder Anschlusskennung (User-ID), Kennwort oder Passwort (PIN), öffentlicher Schlüssel, Geburtsdatum, Kreditkartennummer, e-Mail-Adresse des Nutzers in Betracht kommen. Welche Daten konkret erhoben werden, hängt von dem jeweiligen Vertrag ab. Dieser könnte in Form eines einmaligen Basisvertrages für alle Online-Angebote der Behörde gestaltet sein. Er könnte aber auch für jedes Anwendungsfeld gesondert vereinbart werden. Die erst genannte Variante ist jedoch vorzuziehen, da sie nutzerfreundlich und mit weniger Kostenaufwand verbunden ist. Der vollständige Name sowie die Anschrift stellen Bestandsdaten jedenfalls dar, da sie für die Identifizierung des Nutzers erforderlich sind. Die persönliche Identifikationsnummer (PIN) und die User Identification (User-ID) fallen ebenfalls darunter, da sie der Authentifizierung des Nutzers dienen.[124] Das, wenn auch nur langfristige, Ziel bei E-Government ist eine multimedial interaktive Kommunikation zwischen Verwaltung und Bürger bzw. Wirtschaft, die auch die Bezahlung bei Vornahme von Amtshandlungen erfasst. Erfolgt die Zahlung für die Nutzung der Online-Angebote auf demselben Weg, also elektronisch, so kann die Kreditkartennummer ein Bestandsdatum sein. Allerdings sollte sie möglichst durch anonymes oder pseudonymes Handeln erfolgen. Für die Zugriffsberechtigung ist in jedem Fall die Identifizierung nötig, so dass die genannten Daten des Nutzers bereits aus diesem Grund erforderlich sind.

Nutzungsdaten

Als Nutzungsdaten sind solche Daten anzusehen, die dem Nutzer die Inanspruchnahme von Telediensten ermöglichen; es handelt dabei um solche Daten, die während der Nutzung eines Teledienstes entstehen.[125]

Abrechnungsdaten

---

123 *Dix*, in: RMD, § 5 TDDSG Rn. 1; der Begriff „Bestandsdaten" ergibt sich aus dem Telekommunikationsrecht und wird dort ohne dessen Benennung ähnlich in § 89 Abs. 2 Nr. 1a TKG geregelt. Darüber hinaus schreibt § 89 Abs. 1 TKG eine Konkretisierung durch Rechtsverordnung vor.

124 *Dix*, in: RMD, § 5 TDDSG Rn. 30.

125 *Engel-Flechsig*, DuD 1997, 14.

Abrechnungsdaten sind die für die Abrechnung der Inanspruchnahme der Teledienste erforderlichen Daten. Ihre Speicherung ist nur solange zulässig, wie sie für die Abrechnung erforderlich sind, so dass sie nach Erfüllung der Forderung zu löschen sind.[126]

Signaturdaten

Signaturdaten sind die Daten, die bei der Durchführung von Signaturverfahren entstehen. Sie wurden in Kap. 3.4.3 ausführlich beschrieben.

4.3 Personalisierte Angebote

Für die Werbewirtschaft ist das Internet ein großes Potenzial zur Vermarktung ihrer Angebote. Um das Angebot auf die Gewohnheiten, Interessen und Präferenzen des Kunden abstimmen zu können, ist die Erhebung seiner Daten unumgänglich. Oftmals erfolgt die Datenerhebung ohne die Kenntnis des Nutzers. Anders als in der analogen Welt bietet das Internet zur verdeckten Datenerhebung ein leichtes Spiel für den Anbieter.[127] Bereits beim Verbindungsaufbau fallen über die IP-Adresse eine Vielzahl von Daten wie zum Beispiel über den Browser, das Betriebssystem, die Uhrzeit und den Zugangsanbieter an. Darüber hinaus können mit Hilfe spezieller Software Informationen mit Personenbezug gespeichert werden. Beispielhaft hierfür sind Cookies zu nennen. Cookies werden in Verbindung mit Web-Bugs eingesetzt. Unter einem Cookie wird ein Datensatz verstanden, der von einem Web-Server erzeugt, an einen Web-Browser, der eine Verbindung mit dem Server aufgebaut hat, zur Ablegung der Datei auf dem Computer des Nutzers gesendet wird. Anhand von Cookies kann der Anbieter feststellen, ob der Nutzer schon einmal seine Page besucht hat. Eine verdeckte Datenerhebung ist im Bereich des E-Commerce für die privaten Anbieter besonders attraktiv.

Für den Bereich des E-Government könnte auch an personalisierte Angebote gedacht werden, wie dies in dem Beispiel des Freizeit- und Tourismusagenten in Nürnberg[128] bereits realisiert wurde. Vor allem aber werden personalisierte Angebote dort eine Bedeutung erlangen, wo private Stellen in die Datenverarbeitung involviert sind, also im Zusammenhang mit Outsourcing oder in Public Private Partnerships.

4.4 Vertraulichkeit und Integrität

Die Übermittlung der Daten im Internet ähnelt einer mit Bleistift in Druckbuchstaben geschriebenen Postkarte, wenn keine technischen Vorkehrungen zu ihrem Schutz getroffen wurden. Der Inhalt kann von Dritten eingesehen und verändert werden. In diesem Fall hätten der Absender sowie der Adressat der Nachricht nicht einmal Kenntnis über vorgenommene Manipulationen. In der analogen Papierwelt sind Änderungen nachvollziehbar. In der elektronischen Welt ist dies aufgrund der technischen Möglichkeiten kaum möglich. Elektronische Dokumente können täuschend echt verändert wer-

126 *Engel-Flechsig*, DuD 1997, 14.

127 *Hillenbrand-Beck/Greß*, DuD 2001, 390.

128 S. Kap. 2.6.

den. Es ist ohne einen nennenswerten Aufwand für jeden möglich, die elektronischen Inhalte einzusehen. Innerhalb weniger Sekunden lässt sich der ursprüngliche Text in einen neuen umwandeln, ohne dass es für den Empfänger ersichtlich wird. Hier liegt ein dem Internet immanentes Risiko für die Vertraulichkeit und Integrität personenbezogener Daten vor. Erst durch den Einsatz von Verschlüsselungstechniken kann festgestellt oder gar vermieden werden, dass Änderungen an elektronischen Dokumenten vorgenommen wurden bzw. werden.

4.5 Datenbanken und Aktenfindungssysteme

In der Papierwelt führt jede Behörde ihre eigene Papierakte. Dies ist zwar umständlich, gewährleistet aber die Zweckbindung durch informationelle Gewaltenteilung. Erstellt die Behörde elektronische Akten, entsteht der Wunsch nach einer multifunktionellen Verwendung dieser Daten. Dann könnten die Daten für alle Sachbearbeiter zugänglich sein. Dies kann entweder dadurch realisiert werden, dass die Daten in großen Datenbanken zentral gespeichert werden, oder aber auch dadurch, dass dezentral gespeicherte Daten durch die Vernetzung für alle interessierten Verwaltungsstellen zugänglich werden. Um verteilte Akten bei Bedarf zu finden, ist ein Aktenfindungssystem erforderlich, das die jeweils gewünschten Daten identifiziert und für unterschiedliche Behördenzwecke zum Abruf zur Verfügung stellt. Die Zusammenführung der Daten in Form einer realen oder virtuellen elektronischen Bürgerakte ähnelt dem im Bereich des E-Commerce zunehmend genutzten Konzept des Data Warehouse.

Eine solche Datenbank oder ein solches Aktenfindungssystem ermöglichen die systematische Erkundung und Dokumentation sämtlicher Äußerungen von Bürgern und Unternehmen im Internet. Im Vergleich dazu werden bei Data Mining auf der Basis vorhandener Data Warehouse Techniken verwendet, mit denen bisher unbekannte Daten aufgefunden und zu wissenswerten Zusammenhängen kombiniert werden.[129] Die Vorstellungen des Data Mining gehen auf ein Bild des „Daseinsvorsorgestaates“ zurück, der die allgemeine Bedürfnisbefriedigung durch seine Verwaltungstätigkeit sicherstellen sollte, indem elektronische Informationen über die Verhaltensweise der Gesellschaft zusammengeführt werden.[130] Insbesondere vor dem Hintergrund des „One-Stop-Government“ werden die Gedanken übergreifender Bestände personenbezogener Daten in der öffentlichen Verwaltung mit großer Wahrscheinlichkeit wieder aufleben.[131] In diesen Verfahren könnte die Verwaltung neue Möglichkeiten eines Datenabgleichs sehen.[132] Personenbezogene Daten, die in einer öffentlichen Verwaltung erhoben und gespeichert werden, sind in ihrer Zweckbestimmung grundrechtlich geschützt. Ihre Verarbeitung ist nach den datenschutzrechtlichen Vorgaben nicht erlaubt, soweit sie nicht zu einem bestimmten Zweck oder im gegenseitigen Einvernehmen erfolgt. Der Einsatz von Bürgerakten konfrontiert insoweit das Recht auf informationelle Selbstbestimmung.[133]

---

129 *Schweighofer*, DuD 1997, 459.

130 Siehe dazu ausführlicher *Forsthoff* 1959; *ders*. 1971.

131 Data Mining wird beispielsweise bei der Börsenaufsicht zur staatlichen Aufgabenerfüllung eingesetzt; vgl. *Möller*, DuD 1998, 557.

132 So jedenfalls *Möller*, DuD 1998, 557.

133 Vgl. *Möncke*, DuD 1998, 568.

4.6 Kontrolle für den Datenschutz

Die Rechtmäßigkeit der Datenverarbeitung wird über die datenschutzgesetzlichen Vorgaben hinaus durch die Betroffenenrechte sowie durch die Kontrollbefugnisse der Datenschutzbeauftragten und der Aufsichtsbehörden bestimmt. Die Notwendigkeit einer Datenschutzkontrolle hat das Bundesverfassungsgericht bereits 1983 festgestellt. In seinem Urteil heißt es unter anderem:

> „Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung“[134]

Datenschutzkontrolle ist demnach ein notwendiges Werkzeug zur Wahrung und Durchsetzung des Grundrechts auf informationelle Selbstbestimmung.

Eine zentrale, wenn auch nicht alleinige Aufgabe der Kontrollstellen besteht in der Überwachung der technisch- organisatorischen Maßnahmen öffentlicher und nicht öffentlicher Stellen zur Gewährleistung des Datenschutzes. Die Überwachung erfolgte auf der Basis einer praktischen Prüfung der Datenverarbeitungstechnik. Datenverarbeitung in geschlossenen und leicht überschaubaren Bereichen ließen eine Überwachung vor Ort zu. Unter den heutigen Bedingungen dagegen können personenbezogene Daten im Internet überall durch jedermann verarbeitet werden. Die in der Vergangenheit im Bereich proprietärer Großrechneranlagen repressive Kontrollen sind in offenen und globalen Netzen nicht realisierbar.[135] Auch neue Formen der Datenverarbeitung, wie zum Beispiel Data Mining oder Data Warehouse, ermöglichen personenbezogene Daten innerhalb kürzester Zeit und bequem zu erhalten, und zunehmende privatwirtschaftliche Datenverarbeitung, erschweren zusätzlich die nachträgliche Kontrolle des Datenverarbeitung. Obwohl mit der zunehmenden Integration der IuK-Technologie in verschiedene Lebensbereiche das Bewusstsein und die Sensibilität für Fragen des Datenschutzes, des Schutzes des Persönlichkeitsrechts und der Sicherung für die Informationsverarbeitungsprozesse erheblich gestiegen sind, genügen die bestehenden Kontrollmethoden nicht den Anforderungen eines effektiven Grundrechtsschutzes.[136] Die dynamische Entwicklung dieser Technologien und die damit einhergehende ubiquitäre Datenverarbeitung fordern daher eine Datenschutzkontrolle, die den Risiken des Internets hinreichend begegnen kann.

Diesen Herausforderungen kann mit den heute bestehenden Kontrollmechanismen nicht begegnet werden. Eine Zusammenlegung der Kontrollinstitutionen, etwa dadurch, dass die Aufsichtsbehörden für den nicht öffentlichen Bereich den Landesdatenschutzbeauftragten übertragen werden, könnte zu einer effizienten Datenschutzkontrolle erheblich beitragen. Außerdem ist eine Vereinheitlichung bereits aufgrund der Vorgaben der eu-

---

134 BVerfGE 65, 1 (46).

135 *Büllesbach* 1998, 100.

136 *Büllesbach*, RDV 1997, 241.

ropäischen Datenschutzrichtlinie geboten.[137] So fordert diese in Art. 28 Abs. 1 die Einrichtung völlig unabhängiger Stellen, ohne dass auch nur geringfügige Toleranz geduldet wird.[138] Die Vereinheitlichung und Unabhängigkeit der Kontrollstellen wird in Anlehnung an die europäische Richtlinie und an die höchstrichterliche Rechtsprechung für die zweite Novellierungsphase des BDSG gefordert.[139]

Eine effektive Kontrolle muss vor allem aber auf präventiver Ebene erfolgen.[140] Datenschutz muss vornehmlich in technischen Systemen realisiert werden. Erforderlich ist eine Ausgestaltung der Datenverarbeitung für Electronic Government nach den Grundsätzen des Systemdatenschutzes und eine Unterstützung der Betroffenen nach dem Prinzip des Selbstdatenschutzes.

4.7 Technisch-Organisatorische Herausforderungen

Das Internet als ein ständig anwachsendes, dezentrales und kooperatives System („cyberspace“) unterliegt keiner einheitlichen Rechtsordnung. Für die Anwendbarkeit des deutschen Datenschutzrechts ist es erforderlich, dass personenbezogene Daten auf dem Gebiet der Bundesrepublik Deutschland erhoben, verarbeitet oder gespeichert werden.[141] Gegenüber ausländischen Datenverarbeitern ist das deutsche Datenschutzrecht jedoch machtlos.[142] Um diesen Gefahren hinreichend begegnen zu können, sind daher neben rechtlichen Vorgaben ferner technische und organisatorische Maßnahmen erforderlich, um das materielle Recht abzusichern und dessen Einhaltung zu unterstützen. Der Zweck des Datenschutzes, den Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten zu schützen, kann durch gesetzliche Vorgaben und das Hoffen auf deren Beachtung allein nicht erreicht werden.

Die bisher in allen Datenschutzgesetzen des Bundes und der Länder einheitlich geltenden Maßnahmen, die sogenannten 10 Gebote der Datensicherung – jetzt 8 Gebote, gehen in ihrem Kern auf Diskussionen der siebziger Jahre zurück, das heißt auf einen technologischen Stand, der mehr als ein Vierteljahrhundert zurückliegt.[143] Die Unkontrollierbarkeit der Datenverarbeitung und ihre Verlagerung auf Private, die weltweite und jederzeitige Zugriffsmöglichkeit auf personenbezogene Daten sowie die immer leistungsfähigeren Rechner stellen für den Datenschutz inzwischen völlig neue Herausforderungen dar.

---

137 *Roßnagel/Pfitzmann/Garstka,* DuD 2001, 262.

138 *Garstka,* DVBl 1998, 987; *Lepper/Wilde,* CR 1997, 704; *Bizer,* DuD 1997, 482.

139 So jedenfalls *Roßnagel*, *Pfitzmann* und *Garstka* in einem Gutachten, zu welchem sie durch das Bundesinnenministerium beauftragt wurden. Siehe dafür umfassend *Roßnagel/Pfitzmann/Garstka,* DuD 2001, 253 ff; hinsichtlich der Kontrollstellen auch *Arlt* 1998, 278.

140 *Jacob* 1998, 120.

141 *Engels/Eimterbäumer,* K&R 1998, 197.

142 *Roßnagel*, ZRP 1997, 26; *Garstka,* DVBl 1998, 987; *Hoffmann-Riem,* DuD 1998, 686.

143 *Garstka,* DVBl 1998, 987.

Werden personenbezogene Daten zum automatisierten Abruf im Internet bereitgestellt, kann jedermann auf der Erde auf die gesamte Datensammlung zugreifen, ohne dass eine Kontrollstelle zwischengeschaltet wird. Weder das Erforderlichkeitsprinzip, wonach einem Nutzer nur die Daten zur Verfügung gestellt werden, die er für seine Aufgabenerfüllung braucht, noch die 1990 im BDSG aufgenommenen Vorgaben des § 10 Abs. 1 und 2 BDSG bei einem automatisierten Zugriff, also Angemessenheitsprüfung sowie die Dokumentations- und Protokollierungspflichten, tragen zu einer umfassenden Lösung des Problems bei. Im Gegensatz zu einer zentralistisch organisierten Datenverarbeitung in Rechenzentren werden heute Daten dezentral und in einer vernetzten Infrastruktur verarbeitet.

Zusammenfassend lässt sich also folgendes festhalten: Mit gesetzlichen Ge- oder Verboten kann ein umfassender Grundrechtsschutz für das informelle Selbstbestimmungsrecht des Einzelnen nicht gewährt werden. Die Risiken für die informationelle Selbstbestimmung lassen sich durch technische und organisatorische Lösungen minimieren, die Datenschutz bereits durch Systemdatenschutz sicherstellen.[144] Dem Datenschutzrecht obliegt es, Bestimmungen in dieser Hinsicht zu treffen; insofern ist das Datenschutzrecht gefordert. Eine Leitfunktion nehmen in dieser Hinsicht die Vorschriften des TDDSG ein, welche den Risiken des Internets weitgehend Rechnung tragen.[145]

4.8 Outsourcing und Privatisierung

Während in der Vergangenheit das Leitbild des Ordnungstaates prägend war, hat sich immer mehr das Bild des aktivierenden und gewährleistenden Staates herausgebildet. Zugleich werden immer mehr Aufgaben aus der staatlichen Obhut in private Hände gelegt. Private Stellen nehmen Aufgaben wahr, welche bisher zum staatlichen Tätigkeitsfeld gehören. Dabei baut der öffentliche Sektor zum Teil die Aufgaben entweder vollständig ab und überträgt sie an Private. Oder aber er bleibt weiterhin für die Aufgaben verantwortlich und lässt sie lediglich durch Private erfüllen. Im ersten Fall vollzieht er eine Privatisierung, im zweiten Fall verlagert er die Aufgaben nach Außen – auch Outsourcing genannt.[146] Die zunehmende Schwerpunktverlagerung in der Datenverarbeitung von öffentlichen auf nicht öffentliche Stellen erhöht das Gefährdungspotenzial für das informationelle Selbstbestimmungsrecht, da zusätzliche Interessen an der Verwertung eine Rolle spielen.

4.9 Datenschutz als Chance

Datenschutz bedeutet immer zugleich auch eine Einschränkung für die datenverarbeitende Stelle. Unabhängig davon, ob es sich um eine öffentliche oder nicht öffentliche Stelle handelt, können personenbezogene Daten nicht unbegrenzt erhoben, gespeichert

144 Das Konzept des Systemdatenschutzes ist auf den frühzeitigen Überlegungen von *Podlech* entstanden; siehe umfassend dazu *Podlech* 1982, 451 ff.

145 So auch wie viele andere: *Garstka*, DVBl 1998, 988.

146 Nach § 7 LDSG-BW zum Beispiel finden im Fall des Outsourcing die Vorschriften der Datenverarbeitung im Auftrag Anwendung.

oder genutzt werden. Dies gab für die betroffenen Stellen Anlass, den Datenschutz als Hindernis für wirtschaftlichen Fortschritt oder für die administrative Aufgabenerfüllung zu sehen.[147] Er wurde mit Bürokratie, Behinderung und kaum nachvollziehbaren Forderungen gleichgesetzt.[148] Die Befürchtungen der Bürger hinsichtlich der Verarbeitung ihrer Daten wurden durch entsprechende Sicherheitsvorkehrungen kaum oder gar nicht berücksichtigt. Würden diesen Befürchtungen der nötige Stellenwert beigemessen, so könnten die Online-Angebote für die Nutzer akzeptabel gemacht werden. Mit dem Eindringen der IuK-Technik in alle Lebensbereiche und somit auch in das Verwaltungsgeschehen, sind insbesondere in einer vernetzten Verwaltung automatisierte Datenverarbeitung notwendig. Das Datenschutzrecht sollte hierbei nicht „automationshemmend" wirken.[149] Datenschutz als Mittel zur Vertrauensgewinnung sollte als Motor zur Gestaltung und Nutzung von digitalisierten Behördengängen dienen. Er sollte als Mittel für konstruktive Lösungsansätze innerhalb der Behörden verstanden und akzeptiert werden.[150] Mit der sich zunehmend entwickelnden IuK-Technologie wird der Datenschutz die Informationsgesellschaft stets begleiten. Um so wichtiger ist es daher, den Datenschutz bei ihrem Aufbau als Wettbewerbsvorteil, als Beratungsgegenstand, als Dienstleistung, als Produktidee und als Aspekt der Selbstbestimmung zu verstehen und zu gestalten.[151] Der Datenschutz wird in jeder datenverarbeitenden Stelle, und nicht nur bei der Verwaltung, ein Qualitätsmerkmal darstellen.[152] Insofern ist er eine Chance, die Modernisierung der Verwaltung durch den Einsatz der Informationstechnologie voranzutreiben. Gleichzeitig bedeutet er auch einen Wettbewerbsvorteil gegenüber anderen Staaten.

5. Ziele des Datenschutzes

Dem Datenschutz kommt die Aufgabe zu, die informationelle Selbstbestimmung technikspezifisch und risikoadäquat zu gewährleisten.[153] Dabei müssen vor allem die verfassungsrechtlich unverzichtbaren Prinzipien der Zweckbindung, der Erforderlichkeit und der Transparenz realisiert werden.

5.1 Datenschutz durch Technik

Datenschutz wird vielfach die Rolle des Technikfeindes oder der Innovationsbremse zugewiesen, oft mit dem Hinweis, er würde die Überlebensfähigkeit der deutschen Industrie im Allgemeinen und die der IT-Industrie im Besonderen gefährden.[154] Dem kann nicht zugestimmt werden. Vielmehr muss Datenschutz mit Technik eine Allianz

147 Vgl. dazu *Garstka*, DVBl 1998, 983.

148 *Bäumler*, DuD 2001, 376.

149 Vgl. dazu *Garstka*, DVBl. 1998., 983.

150 Vgl. dazu *Hoffmann-Riem*, DuD 1998, 685, *Jacob*, DuD 2000, 5.

151 *Roßnagel* 2001, 241.

152 *Tauss/Özdemir* 2001, 232.

153 *Bizer*, 1997, 146 ff.

154 *Rannenberg* 1998, 190.

eingehen.[155] Er muss durch Technik, und nicht gegen Technik erreicht werden.[156] Die Einbindung der technischen Verfahren in den Datenschutz bietet eine Lösung bei den erläuterten Herausforderungen.[157] Technische Lösungen können befürchteten Datenmissbrauch weitgehend präventiv verhindern.[158] Außerdem ist technischer Datenschutz unabhängig vom individuellen Problembewusstsein und der persönlichen Aufmerksamkeitskapazität.

Hinsichtlich der Datensicherung sind statt der bisherigen 10, jetzt 8 Gebote die Ziele der Integrität, Vertraulichkeit, Verfügbarkeit und Zurechenbarkeit personenbezogener Daten zu verfolgen. Daneben sind soweit wie möglich personenbezogene Daten zu vermeiden und die Datenverarbeitungssysteme für die Betroffenen und die Kontrollstellen transparent zu gestalten.

5.2 Systemdatenschutz

Technische und organisatorische Gestaltung der Datenverarbeitung des Electronic Government soll Systemschutz ermöglichen. Erforderlichkeit, Zweckbindung und Transparenz sowie die Kontroll- und Korrekturrechte des Betroffenen sollen durch eine datenschutzgerechte Technikgestaltung sichergestellt werden.[159] Insbesondere die Anforderung des § 3a BDSG, „keine oder so wenige personenbezogene Daten wie möglich zu erheben, verarbeiten oder zu nutzen“, sollen auf diese Weise realisiert werden. Ergänzt wird diese Anforderung in § 4 Abs. 6 TDDSG durch die Verpflichtung der Diensteanbieter, die Inanspruchnahme durch anonymes und pseudonymes Handeln zu ermöglichen. Soweit eine Identifizierung, Wiedererkennung und Berechtigungsprüfung nicht erforderlich ist, kann auf das Konzept anonymen Handelns zurückgegriffen werden. Dort, wo eine Identifizierung zwar notwendig ist, aber der Betroffene anonym handeln möchte, bieten Pseudonyme eine Lösung. Der Systemdatenschutz soll schließlich sicherstellen, dass nur die rechtlich zulässige Datenverarbeitung durch die dazu ermächtigte Stelle erfolgt.[160]

5.3 Selbstdatenschutz

Systemdatenschutz muss durch Selbstdatenschutz ergänzt werden. Für einen umfassenden Persönlichkeitsschutz sollten dem Einzelnen selber die technischen Instrumente sowie notwendige Infrastrukturleistungen zur Verfügung gestellt werden.[161] Ein wichtiges Mittel des Selbstdatenschutzes ist die selbstbestimmte Nutzung von Anonymitätstechniken oder die Nutzung von Pseudonymen.

---

155 Vgl. *Bachmeier,* DuD 1996, 672.

156 *Bäumler,* RDV 1999, 5; *Bizer/Fox/Reimer,* DuD 1997, 2.

157 *Ohnsorge* 1995, 19 ff., *Ockenfeld/ Wetzel,* CR 1993, 386.

158 *Federrath/Pfitzmann* 2001, 252.

159 *Bizer* 1998, 45 ff.

160 *Bäumler,* DuD 2000, 257.

161 *Weichert* 1998, 225.

Ein weiteres Instrument des Selbstdatenschutzes ist die Möglichkeit, sich jederzeit ausreichende Transparenz über die Bedingungen des Datenverarbeitung zu verschaffen. Hier können Verfahren entsprechend des „Plattform for Privacy Preferences Project (P3P)“ helfen. P3P als universeller, technischer Standard erlaubt es, automatisiert weltweit im ganzen Internet Datenschutz-Policies für die Nutzer transparent zu machen, sofern die Anbieter P3P ebenfalls verwenden. Mit Hilfe von P3P wird dem Nutzer der Behördendienstleistung deutlich, welche seiner Daten zu welchem Zweck verarbeitet werden sollen. Dass die Verwaltung damit ihre Datenverarbeitungspraxis ausdrücklich offen legt, kann dem Nutzer einen Teil seiner Besorgnis nehmen.

5.4 Techniksicherung (Kommunikationssicherheit, Abschottung, Revisionsmöglichkeit)

Text von LfD Niedersachsen

5.5 Geheimnisschutz (Geschäfts- und Betriebsgeheimnis, Amtsgeheimnis), Vertraulichkeit

Text von LfD Niedersachsen

5.6 Betroffenenrechte

Das Volkszählungsurteil hat die Beteiligung der Bürger an Datenverarbeitung und Datenschutz gefordert, da andernfalls ein umfassender Schutz für das informationelle Selbstbestimmungsrecht nicht gewährleistet werden kann. Daher stehen dem Betroffenen Transparenz, Mitwirkungs- und Korrekturrechte zu.

5.6.1 Transparenzrechte

> „Wer nicht mit Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt sein, aus eigener Selbstbestimmung zu planen oder zu entscheiden“.[162]

Nur wenn die Datenverarbeitung der betroffenen Person bekannt ist, kann sie ihre Rechtmäßigkeit überprüfen und ihre Rechte gegebenenfalls geltend machen. Der Betroffene wird faktisch rechtlos, wenn er nicht in die Lage versetzt wird Informationen über die Erhebung, Verarbeitung und Nutzung seiner Daten zu bekommen. Die Pflicht zur Unterrichtung ist dann erfüllt, wenn der Nutzer erfährt, welche Angaben von ihm im

[162] BVerfGE 65, 1 (43).

konkreten Fall erwartet werden und für welche konkreten Zwecke diese erhoben, verarbeitet und genutzt werden.[163] Dazu gehört auch die Angabe, wie lange die Daten beim Anbieter vorgehalten werden und wann ihre Löschung erfolgt. Insoweit ist im Rahmen der Unterrichtung auch präzise anzugeben an wen und zu welchem Zweck welche Daten weitergegeben werden. Die Unterrichtung sollte darüber hinaus Informationen über die für die Datenverarbeitung verantwortliche Stelle, Rechtsgrundlage der Verarbeitung oder die Freiwilligkeit der Angaben, mögliche Folgen aus der Verweigerung der Angaben, Recht sowie Wahl- und Gestaltungsmöglichkeiten erfassen. Der Inhalt der Unterrichtung sollte von der betroffenen Person jederzeit abgerufen werden können.

Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Die betroffene Person muss die Möglichkeit haben zu entscheiden, ob sie das Nutzungsverhältnis unter den mitgeteilten Bedingungen fortsetzen oder abbrechen möchte. Um dies erreichen zu können, muss die Unterrichtung vollständig und leicht verständlich sein. So ist nach § 4 Abs. 1 TDDSG und § 12 Abs. 6 MDSTV der Nutzer von Telediensten zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten. Zu der Unterrichtungspflicht der Behörde gehören auch Hinweise auf das Recht zum Widerruf erteilter Einwilligungen nach § 4 Abs. 3 TDDSG. Die Behörde könnte ihrer Unterrichtungspflicht durch die Bereitstellung einer Datenschutzerklärung nachkommen. Diese (ähnlich wie die AGB's einer privaten Stellen) sollte dem Nutzer jederzeit und gut zugänglich sein.

Ferner sollte neben den genannten Inhalten auch die Systeme der Informationstechnik für die Betroffenen durchsichtig gestaltet werden. Die Behörde sollte über die Verwendung und der Funktionalität der jeweiligen Hardware, Betriebssysteme, Anwendungssoftware informieren. Dies sollte zumindest gegenüber der prüfenden Stelle geschehen, damit eine höhere Sicherheit gewährleistet werden kann. Würde eine Offenlegung auch gegenüber dem Betroffenen erfolgen, was wünschenswert ist, so könnte dieser selbst entscheiden, ob er das System nutzen möchte bzw. mit welchen Konsequenzen er zu rechnen habe.

Das Fundament aller Mitwirkungsrechte ist das Auskunftsrecht, das die Transparenz der Datenverarbeitung durch individuelle Unterrichtung und Datenschutzerklärung ergänzt. Die Auskunft erfasst inhaltlich die Information über die Speicherung und Herkunft der Daten, über den Zweck sowie Empfänger der Datenverarbeitung, über mögliche Korrekturdatenverarbeitungen wie Berichtigung, Löschung oder Speicherung und über die Einrichtung sowie Ablauf von automatisierten Abrufverfahren. Soweit die Informationen in der Unterrichtung oder in der Datenschutzerklärung enthalten ist, entfällt der Auskunftsanspruch. § 4 Abs. 7 TDDSG und § 16 MDSTV unterwerfen auch die Informationen über die Verwendung von Pseudonymen der Auskunftspflicht. Wird die Auskunft über Pseudonyme verlangt, muss der Auskunftssuchende die Informationen unter seinem Pseudonym verlangen, damit er sein Pseudonym nicht aufdeckt. Die Auskunft ist unentgeltlich, unverzüglich und vollständig zu erteilen.

---

163 Die Pflicht zur Information über den Zweck der Datenverarbeitung ist ein Grundsatz der Safe Harbor Principles; siehe dazu EG-ABL. L 215 vom 25.8.2001.

5.6.2 Berichtigung, Löschung und Sperrung

Der Betroffene hat grundsätzlich ein Recht zu wissen, wer was wann und bei welcher Gelegenheit über ihn weiß.[164] So räumt § 17 NDSG (vgl. §§ 6, 20, 35 BDSG) dem Betroffenen einen Anspruch auf Berichtigung. Löschung und Sperrung der zu seiner Person gespeicherten Daten ein. Die datenverarbeitende Stelle muss bei Unrichtigkeit der Daten diese von sich aus und unverzüglich berichtigen. Unrichtig können nur Tatsachen sein, da nur ihr Wahrheitsgehalt nachgewiesen werden kann. Werturteile fallen insofern nicht darunter. Die Berichtigungspflicht geht aus der Formulierung des § 17 Abs. 1 NDSG hervor, dass personenbezogene Daten zu berichtigen sind, wenn sie unrichtig sind. Diese Pflicht der datenverarbeitenden Stelle besteht unabhängig davon, ob der Betroffene einen Anspruch geltend macht.[165]

Die speichernde Stelle hat nach § 17 Abs. 2 NDSG die Daten zu löschen, wenn die Speicherung nicht zulässig, oder für die Aufgabenerfüllung nicht mehr erforderlich ist. Dabei bedeutet Löschung das Unkenntlichmachen von Daten, so dass sie für andere nicht mehr zugänglich sind. Die Löschung hat unverzüglich, das heißt ohne schuldhaftes Zögern, zu erfolgen. Anders dagegen, wenn Aufbewahrungspflichten bestünden oder wenn anzunehmen ist, dass schutzwürdige Interessen des Betroffenen durch die Löschung beeinträchtigt werden.[166] In dem Fall tritt an die Stelle der Löschung eine Sperrung nach § 17 Abs. 3 NDSG ein. Darüber hinaus ist eine Sperrung der Daten vorzunehmen, wenn ihre Richtigkeit nicht eindeutig ist oder die Sperrung von dem Betroffenen verlangt wird.

5.6.3 Widerspruchsrecht

?? Art. 14a und b EG-DSchRL räumt betroffenen Personen die Möglichkeit ein, eine an sich rechtmäßige Datenverarbeitung zu verhindern. Der Widerspruch kann im Regelfall in den Fällen geltend gemacht werden, in denen die Behörde eine Beeinträchtigung schutzwürdiger Interessen des Betroffenen nicht für möglich hält, weil die Daten zum Beispiel ohnehin veröffentlicht werden dürfen. Mit der Möglichkeit des Widerspruchs kann er diese Interessen durchsetzen**.** Eine entsprechende Regelung ist in § 17 a NDSG aufgenommen wurden. Soweit Rechtsregelungen wie § 34 Abs. 5 NMG und § 21a MRRG-E einen Widerspruch vorsehen, müssen die Electronic Government-Verfahren Möglichkeiten vorsehen, diesem Widerspruch – ohne Begrenzung durch technische Sachzwänge – zu entsprechen.

5.7 Elektronische Einwilligung

Fehlt es für die Datenverarbeitung an einem Erlaubnistatbestand, benötigt die Behörde die Einwilligung des Nutzers. Auf Grund des Erlaubnisvorbehalts setzt eine zulässige Datenverarbeitung eine wirksame Einwilligung voraus. Inhaltlich muss die Einwilli-

164 BVerGE 65, 1 (43).

165 *Tinnefeld/ Ehmann* 1998, 396.

166 *Tinnefeld/ Ehmann* 1998, 396.

gung freiwillig und in Kenntnis der gesamten Umstände, also über Art, Umfang und Ort und Zweck der Erhebung, Nutzung und Verarbeitung personenbezogener Daten, ergangen sein. An ihre Form werden strenge Maßstäbe gesetzt. Bei einer schriftlichen Einwilligung verlangt § 4a Abs. 1 BDSG die schriftliche Abgabe der Einwilligungserklärung, soweit wegen besonderer Umstände eine andere Form nicht angemessen ist. Außerdem kann die Einwilligung nach §§ 126 Abs. 3, 126a BGB in elektronischer Form erklärt werden.

Im Geltungsbereich des TDDSG kann die Einwilligung auch in erleichterter Form erteilt werden. Nach § 4 Abs. 2 TDDSG muss die Behörde als Diensteanbieter, wenn sie die elektronische Einwilligung anbietet, sicherstellen, dass sie nur durch eine eindeutige und bewusste Handlung des Nutzers erfolgen kann, die Einwilligung protokolliert wird und der Inhalt der Einwilligung vom Nutzer jederzeit abgerufen werden kann. Zum Nachweis ihrer Integrität und Authentizität bedürfen elektronische Einwilligungen mangels ihrer Verkörperung besonderer technischer Absicherung. Andernfalls könnten Dritte im fremden Namen Einwilligungen abgeben oder abgegebene Einwilligungen verfälschen. Die Nachweisführung darüber ist im Streitfall um so bedeutender, wenn es um die Beweisführung über das Bestehen oder die Reichweite der Einwilligung geht. Soweit Signaturverfahren verwendet werden, kann mit diesen in jedem Fall rechtswirksam und beweisbar eine elektronische Einwilligung erteilt werden. Rechtliche Anforderungen stellt § 4 Abs. 2 TDDSG hierzu aber nicht.

6. Datenschutzgerechte Gestaltung des Internetangebots- am Beispiel der einfachen Melderegisterauskunft bei der LHH

Im Folgenden wird die prototypische Umsetzung der datenschutzrechtlichen Anforderungen aus dem bereichs- und internetspezifischen sowie umsetzungsrelevantem Recht am Beispiel der einfachen Melderegisterauskunft dargestellt. Welche Rechtsvorschriften Vorrang haben, wie ihre Anforderungen auf die einfache Melderegisterauskunft maßgeschneidert umgesetzt werden können und welche Probleme mit der Realisierung einhergehen, war Gegenstand des Forschungsprojekts „Datenschutzgerechtes E-Government“, das von der Landeshauptstadt Hannover (LHH), dem Landesbeauftragten für den Datenschutz Niedersachsen und der Universität Kassel/provet gemeinsam durchgeführt wurde.

6.1 Vorhaben der LHH

Die LHH möchte Grunddaten der Melderegisterauskunft im Internet zum Abruf bereitstellen. Es handelt sich dabei ausschließlich um Daten der einfachen Melderegisterauskunft. Diese Form der Auskunft ist auch für die Behördenabfrage vorgesehen. Die einfache Melderregisterauskunft erfasst den vollständigen Namen mit Namensbestandteilen, Doktorgrad und Anschrift. Die Auskunft beinhaltet nur die aktuellen Daten des Betroffenen. Wird der Betroffene eindeutig identifiziert, so kann eine Auskunft erteilt werden. Im analogen Verfahren wurden Anfrage und Auskunft entweder telefonisch oder auf dem Postweg schriftlich bzw. durch Datenträgeraustausch erteilt. Das NMG

sieht keine besondere Formvorschrift für die Auskunftserteilung vor, so dass die Auskunft mittels Telekommunikation auch erteilt werden kann. Insoweit bestehen vor dem Hintergrund einer besonderen Form auch im Online-Verfahren keine Bedenken.

Für das automatisierte Verfahren stellt das Einwohnermeldeamt der Stadt Hannover auf einem separaten, gegen unbefugten Zugriff gesicherten Server Daten zur Verfügung, die auf diesen Server von dem „Mutterserver" *gespiegelt* werden. Der Spiegelserver stellt die Anfragedatenbank dar. Die Anfragedatenbank soll allerdings weniger Daten enthalten als das Melderegister. Auf diese Weise kann ausgeschlossen werden, dass der Anfragende durch Recherchieren mehr Informationen erhält, als er im Rahmen der einfachen Melderegister bekäme.

Der Nutzerkreis wird aufgeteilt in gelegentliche, regelmäßige (z.B. Großfirmen) und behördliche Nutzer. Außer die gelegentlichen Nutzer müssen sich alle übrigen, also auch die Mitarbeiter der Behörde oder der berechtigten Einrichtung ein elektronisches Signaturverfahren im Sinne des SigG bei einem Zertifizierungsdiensteanbieter besorgen, um auf die Anfragedatenbank zugreifen zu können. Für die regelmäßigen Nutzer ist ihre Authentifizierung erforderlich, da sie die Gebühr zyklisch per Rechnungsschreibung zahlen sollen. Auch die Identifizierbarkeit der behördlichen Nutzer ist für die LHH zwingend, denn diese erhalten die Auskunft im Rahmen der Amtshilfe nach § 29 Abs.1 NMG gebührenfrei. Das ergibt sich aus § 2 Abs.1 Ziff.2 VerwKostG. Demnach müssen sich diese im Vorfeld bei der LHH identifizieren und eine Zugriffsberechtigung besorgen. Die Registrierung soll in einem zweistufigen Verfahren erfolgen: In einem ersten Schritt soll der interessierte Großkunde bzw. die Behörde zugelassen werden. Bei den Großkunden handelt es sich in der Regel um Unternehmen mit mehreren Mitarbeitern, die ebenfalls eine Zugriffsberechtigung benötigen. Auch innerhalb einer Behörde werden Anfragen von unterschiedlichen Mitarbeitern gestellt. Unternehmen und Behörde ermächtigen ihre Mitarbeiter zum Abruf von Meldedaten. Zur Verwaltung der berechtigten Mitarbeiter soll in einem zweiten Verfahrensschritt eine Zulassung für einen sogenannten Kundenadministrator, eine Person aus dem jeweiligen Unternehmen oder der jeweiligen Behörde, erfolgen. Dieser soll die berechtigten Mitarbeiter online registrieren bzw. dafür sorgen, dass den nicht mehr berechtigten Mitarbeitern der Zugriff entzogen wird.

Die gelegentlichen Nutzer dagegen können die Daten abrufen, ohne sich zu authentifizieren. Eine Authentifizierung ist weder rechtlich noch im Hinblick auf die anfallende Gebühr notwendig, da in diesem Fall die Auskunft nur erteilt wird, wenn die Gebühr mittels Geldkarte entrichtet wurde. Diese Nutzergruppe kann also das Verfahren anonym nutzen, so dass dem Grundsatz der Datensparsamkeit und Datenvermeidung weitestgehend Rechnung getragen wird..

Die automatisierte Abrufbarkeit der einfachen Melderegisterauskunft kann nach der jetzigen Gesetzeslage nur in Form der Adressbuch-Lösung realisiert werden.[167] Die Abfrage soll nach der Vorstellung der Landeshauptstadt daher zunächst über zwei „Filter" erfolgen. Der zweite Filter dient der Reduzierung auf Adressbuchdaten und soll nach Inkrafttreten des künftig novellierten MRRG wegfallen.

---

[167] S. hierzu näher Kap. 6.3.

In der folgenden Tabelle werden die mit der Nutzung eines automatisch abrufbaren Melderegisters verbundenen Vorstellungen erläutert.

Benutzergruppe:	Gelegentliche private Nutzer	Regelmäßige Nutzer	Behörden
Registrierung	Keine	Eine Registrierung sowohl der Organisation, als auch der berechtigten Mitarbeiter ist erforderlich	Die Behörde selbst und die berechtigten Mitarbeiter sind zu registrieren
Authentifizierung	Für den Erhalt der Melderegisterauskunft nicht erforderlich	Mittels Signaturkarte	Mittels Signaturkarte
Gebühr	Vorherige Zahlung mit Geldkarte. Andernfalls wird Auskunft nicht erteilt.	Sammelrechnung	Keine Gebührenerhebung
Datenerhebung:			
Bestandsdaten:	Keine Datenerhebung, da anonyme Nutzung.	Es werden der Kunden-/Firmenname, die Kundenanschrift und Kundennr., der Ansprechpartner, die Rechnungsadresse, Kontoverbindung, der Abrechnungszeitraum sowie User-ID erhoben. Es sind keine Argumente gegen die Erhebung dieser Daten ersichtlich.	Nur erforderliche Daten der Behörde.
Nutzungsdaten:	Es werden keine Nutzungsdaten bei Verbindungsabbau gespeichert.		
Gebührdaten.	Keine Datenerhebung, da anonyme Nutzung.	Transaktions-ID, Positionsnummer, Leistungsart, Art der Anfrage, Kommune/ Fachamt, Kassenzeichen, Haushaltsstelle, Datum, Uhrzeit, ID des Anfragenden, Kundennr., Verarbeitungsstatus- und datum, Gesamtbetrag. Diese Daten sind für die Rechungsschreibung erforderlich. Inwieweit die Speicherungsdauer von 180 Tagen erforderlich ist, bedarf einer Klärung.	Keine Datenerhebung.

6.2. Datenschutzrechtliche Bewertung

Vor der datenschutzrechtlichen Bewertung des Projektvorhabens ist die Frage nach der Anwendbarkeit der Rechtsvorschriften zu klären. Für die rechtliche Bewertung kommen Regelungen aus folgenden Rechtsbereichen in Betracht.

6.2.1 Zu berücksichtigende Rechtsbereiche

Die Online-Melderegisterauskunft ist in der Realität zwar ein einheitlicher Vorgang. Für ihre datenschutzrechtliche Bewertung sind aufgrund der Besonderheiten des deutschen Datenschutzrechts jedoch grundsätzlich drei unterschiedliche Rechtsbereiche zu beachten.

a) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Verwaltungszwecke unterliegt dem Verwaltungsdatenschutzrecht. Dieses unterscheidet nicht danach, in welcher Form und auf welchem Weg die Melderegisterauskunft erteilt wird. Auch für die Online-Auskunft sind somit alle Anforderungen an die Offline-Auskunft, wie sie schon bisher schriftlich erfolgt ist, zu beachten.

b) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für den Zweck, die Auskunftserteilung über das Internet zu ermöglichen, unterliegt dem Online-Datenschutzrecht. Dies gilt aber nur für die Datenverarbeitung, die erfolgt, um diese spezifische Form der Auskunftserteilung zu ermöglichen.

c) Um über das Internet Auskünfte zu erhalten, muss eine Telekommunikationsverbindung zwischen dem Anfragenden und dem Auskunftsserver aufgebaut werden. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für das Herstellen und Aufrechterhalten von Telekommunikationsverbindungen unterliegt dem Telekommunikationsdatenschutzrecht.

Für die Melderegisterauskunft über das Internet müssen somit folgende drei Aktionsebenen und deren unterschiedlichen Rechtsgrundlagen beachtet werden:

Ebene	**Rechtsgrundlagen**	**Beispiel**
Inhaltsebene (Auskunftserteilung, Suchkriterien, Auskunftssperre, Widerspruch)	"Offline-Recht": Niedersächsisches Melde- und Datenschutzgesetz	Erhalt einer einfachen Melderegisterauskunft
Transportbehälterebene (Teledienste, Mediendienste)	"Online-Recht": Teledienstedatenschutzgesetz, Mediendienste-Staatsvertrag	Bereitstellen des automatisierten Abrufverfahrens

Transportebene (Telekommunikation)	Telekommunikationsrecht: TKG, TDSV	Netzbetrieb, Zugangsvermittlung

6.2.2 Anzuwendende Rechtsregeln

Damit die einfache Melderegisterauskunft über das Internet datenschutzgerecht erteilt wird, ist zu klären, welche der Datenschutzregelungen aus diesen Bereichen konkret zur Anwendung kommen.

6.2.3 Verwaltungsdatenschutzrecht

Für die Landesverwaltung gelten grundsätzlich die Regelungen des Niedersächsischen Landesdatenschutzgesetzes (NDSG). Dieses ist jedoch gegenüber bereichsspezifischen Datenschutzregelungen subsidiär. Daher gehen die Regelungen des Niedersächsischen Meldegesetzes (NMG) dem Landesdatenschutzgesetz vor. Das NDSG kommt nur insoweit zur Anwendung, als in ihm Rechtsfragen geregelt sind, die nicht Gegenstand des NMG sind.

6.2.4 Online-Datenschutzrecht

Für das Online-Datenschutzrecht enthalten das TDDSG sowie der MDStV (vgl. §§ 12, 17 MDStV) ausführliche - nahezu wortgleiche - **bereichsspezifische Regelungen** zum **Datenschutz**, die für ihren Anwendungsbereich den Landesdatenschutzgesetzen und dem Bundesdatenschutzgesetz vorgehen. Die Unterscheidung zwischen Tele- und Mediendiensten hat ihre Ursache im föderativen Aufbau der Bundesrepublik Deutschland. Während Teledienste der Regelungskompetenz des Bundes zugeordnet sind, unterliegen die Mediendienste der Zuständigkeit der Länder.

Welche dieser Regelungen eingreift, hängt davon ab, ob die Auskunftserteilung einen Tele- oder Mediendienst darstellt. § 2 Abs. 1 TDG enthält eine generelle Umschreibung des Begriffs „Teledienst“. Danach sollen alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt, erfasst werden. Wesentliches Merkmal eines Teledienstes ist die individuelle Nutzung, also die Individualkommunikation. Dagegen handelt es sich bei einem Mediendienst um eine Massenkommunikation, wobei das Angebot an die Allgemeinheit gerichtet ist. Als ein wichtiges Abgrenzungskriterium zwischen Tele- und Mediendienst kann die „redaktionelle Gestaltung zur Meinungsbildung“ bezeichnet werden.

Eine Auskunft aus dem Melderegister kann zwar grundsätzlich jedermann erteilt werden. Doch die Auskunft wird jeweils erst nach einer individuellen Abfrage erteilt. Ferner kann die Auskunft im Online-Verfahren nur nach einem Antrag und nach Erhalt einer Zugriffsberechtigung, die im Offline-Verfahren erteilt wird, gegeben werden. Schließlich dient die Auskunft nicht der Meinungsbildung, sondern einem individuellen Auskunftsinteresse. Es handelt sich bei dem Abruf somit um eine individuelle Nutzung

des Melderegisters, so dass die Individualkommunikation im Vordergrund steht. Folglich stellt die Auskunftserteilung einen Teledienst dar, für den sich die datenschutzrechtlichen Anforderungen allein aus dem TDDSG ergeben.

6.2.5 Telekommunikationsdatenschutzrecht

Von dem inhaltlichen Informations- und Kommunikationsangebot ist der technische Telekommunikationsvorgang, der das Übermitteln von Signalen ermöglicht, zu unterscheiden. Die Verwendung personenbezogener Daten, die diesem Zweck dient ist in § 85 ff. TKG und der Teledienstedatenschutzverordnung (TDSV) geregelt. Unter das Telekommunikationsrecht fällt der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern und Tönen mittels Telekommunikationsanlagen. Adressat der Regelungen ist aber nur derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt. Nicht erfasst werden vom TKG und der TDSV inhaltliche Aspekte der Kommunikationsbeziehungen der Nutzer der Telekommunikationstechnik. Da die LHH für die Melderegisterauskunft über das Internet nicht selbst Telekommunikationsdienste erbringt, sondern nur nutzt, muss sie keine Anforderungen nach dem TKG und der TDSV erbringen. Anforderungen nach dem Telekommunikationsdatenschutzrecht können für den geplanten Internetdienst somit unberücksichtigt bleiben.

6.3 Verwaltungsrechtliche Zulässigkeit

Um eine einfache Melderegisterauskunft in einem automatisierten Abrufverfahren erteilen zu können, ist eine gesetzliche Grundlage erforderlich. Allein § 33 NMG ermächtigt die Behörde zu einer Melderegisterauskunft an private Stellen, es sei denn, schutzwürdige Interessen des Betroffenen stehen der Auskunftserteilung entgegen (vgl. § 4 NMG). Im Offline-Verfahren wird die Behörde also durch § 33 Abs. 1 NMG zur Auskunftserteilung ermächtigt. Ob § 33 Abs. 1 NMG die Meldebehörde ermächtigt, auch in einem automatisierten Verfahren über das Internet eine einfache Melderegisterauskunft zu erteilen, ist nicht ausdrücklich geregelt, hängt also davon ab, ob die Internetauskunft den gleichen Zweck erfüllt. § 33 Abs. 1 NMG ermächtigt nur zu einer Einzelauskunft. Im Fall eines automatisierten Abrufverfahrens dagegen könnte der einmal Zugriffsberechtigte jederzeit und ohne einen bestimmten Zweck beliebig über die Daten der Einwohner verfügen. Dies kommt einer regelmäßigen Datenübermittlung in einem automatisierten Abrufverfahren, wie sie zwischen öffentlichen Stellen erfolgt, gleich. **Regelmäßige** Melderegisterauskünfte, die den regelmäßigen Datenübermittlungen zwischen den öffentlichen Stellen entsprechen, sind nach § 33 NMG nicht zulässig. Dass der Gesetzgeber die Meldedatenübermittlung durch ein automatisiertes Verfahren nur zwischen den öffentlichen Stellen in einer Verordnung geregelt hat, deutet darauf hin, dass ein solches Verfahren für nicht öffentliche Stellen von dem Willen des Gesetzgebers nicht erfasst ist.

Fraglich ist, ob das Online-Bereithalten von Daten für Zugriffsberechtigte nach § 34 Abs. 4 NMG zulässig ist. Nach § 34 Abs. 4 NMG darf die Meldebehörde Adressbuchverlagen Auskunft über die Daten im Umfang einer einfachen Melderegisterauskunft erteilen, wenn der Einwohner über 18 Jahre alt ist, in Hannover wohnt, eine Auskunftssperre nicht vorliegt und nicht widersprochen hat.

Die Adressbuchverlage stellen diese Daten in Papierform gegen Entgelt jedermann zur Verfügung. § 34 Abs. 4 NMG sieht ferner eine bestimmte Form zur Veröffentlichung der Daten nicht vor. Daher könnten die Daten durch Adressbuchverlage auch im Internet veröffentlicht werden. Indem die Meldebehörde Grunddaten aus dem Melderegister übermittelt, stellt sie dadurch indirekt Daten, wenn auch in eingeschränktem Umfang, jedermann zur Verfügung.

Aus der Sicht der Betroffenen und damit aus der Sicht des Datenschutzes macht es keinen Unterschied, ob die Behörde die Daten mittelbar über Adressbuchverlage oder unmittelbar selbst der Allgemeinheit zur Verfügung stellt. Dass die Daten in dem von der LHH gewählten Verfahren nur den Personen, die hierfür von der Verwaltung ausdrücklich zugelassen sind, und nicht für die Allgemeinheit zum Abruf zur Verfügung gestellt werden, spricht nicht dagegen. Entscheidend ist, dass sich gegebenenfalls jedermann eine Zugriffsberechtigung holen könnte und der Benutzerkreis nicht durch Zugangseigenschaften eingeschränkt wird. Der Betroffene würde in beiden Fällen derselben Gefährdungslage ausgesetzt, gleichgültig, ob eine private oder eine öffentliche Stelle seine Daten veröffentlicht. Der Veröffentlichung seiner Daten kann er allerdings mit einem Widerspruch (vgl. § 34 Abs. 5 NMG und § 21 Abs. 1 a MRRG-E) entgegenwirken. Dass die Vorschrift ausgehend vom Wortlaut nur Adressbuchverlage zur Veröffentlichung ermächtigt, basiert auf wettbewerbsrechtlichen Überlegungen, dass die Gemeinde nur bedingt wirtschaftlich tätig werden darf. Datenschutzrechtliche Aspekte liefern jedoch keine Begründung für die eingeschränkte Ermächtigung der Behörde, da es vor dem Hintergrund der Gefahr für das informationelle Selbstbestimmungsrecht keinen Unterschied macht, ob die Behörde über Adressbuchverlage oder selber die Daten veröffentlicht. Daher kann die Behörde die Grunddaten auch selber veröffentlichen.

Zwar ist zu bedenken, dass die Veröffentlichung von Daten einen besonders starken Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt. Veröffentlichte Daten sind in der Regel auf unbestimmte Zeit für jedermann zugänglich und unterliegen faktisch keiner Zweckbindung oder sonstigen Verwendungsbeschränkung mehr. Daher könnte eingewendet werden, dass ein solcher Eingriff einer ausdrücklichen Ermächtigung bedürfe, aus der sich die Voraussetzungen und der Umfang der Beschränkung klar und für den Bürger erkennbar ergeben. Eine solche fehlt in § 34 NMG für den Internetabruf.

Allerdings kann § 12 Abs. 1 NDSG ergänzend herangezogen werden. Nach dieser Vorschrift kann ein automatisiertes Verfahren dann eingerichtet werden, wenn eine Rechtsvorschrift dies zulässt. Eine Verordnung, welche eine Datenübermittlung in einem automatisierten Abrufverfahren zulässt, ist die Niedersächsische Meldedatenübermittlung zwischen *öffentlichen Stellen*. Weder diese noch eine andere Verordnung sieht eine Datenübermittlung an Private in dieser Form vor. Ferner wird in § 12 Abs. 4 NDSG ausdrücklich erwähnt, dass personenbezogene Daten nicht zum Abruf durch Stellen außerhalb des öffentlichen Bereichs bereitgehalten werden dürfen. Allerdings gelten nach § 12 Abs. 5 NDSG die Absätze 1 bis 4 nicht, wenn die automatisiert abrufbaren Daten solche Daten sind, die jeder Person offenstehen oder deren Inhalt veröffentlicht werden darf. Diese Anforderung ist in dem vorgesehenen Verfahren erfüllt, da die einer einfachen Melderegisterauskunft unterliegenden Daten nach § 34 Abs. 4 NMG durch Adressbuchverlage veröffentlicht werden dürfen, solange kein Widerspruch des Betroffenen vorliegt.

Ferner heißt es in der Amtlichen Begründung zu § 12 LDSG: Die besonderen Anforderungen an die Einrichtung von automatisierten Abrufverfahren sind nicht gerechtfertigt, wenn es sich um den Anschluss an Datenbestände handelt, die jedermann zur Benutzung offenstehen. Dabei ist es ohne Bedeutung, ob der Benutzer einer besonderen Zulassung bedarf oder nicht. Entscheidend ist vielmehr, dass jedermann gegebenenfalls die besondere Zulassung erhalten kann, es sich also nicht um einen geschlossenen Benutzerkreis mit besonderen Zulassungseigenschaften handelt, über die nicht jedermann verfügen kann. Die einfache Melderegisterauskunft kann jeder ohne Preisgabe seiner Identität erhalten. Sie steht daher jedermann zur Verfügung.

Die hier gefundene Wertung entspricht auch der künftig ausdrücklich geregelten Ermächtigung. Nach § 21 Abs. 1a des Entwurfs zum MRRG dürfen einfache Melderegisterauskünfte in einem elektronischen Verfahren erteilt werden. Die landesrechtlichen Vorschriften müssten den rahmenrechtlichen Regelungen des MRRG angepasst werden. Eine Authentisierung des Auskunftssuchenden ist nach dem Entwurf zum MRRG nicht erforderlich. Dies entspricht der bisherigen Praxis. In der Begründung zum Entwurf des MRRG heißt es: Das vorgesehene Verfahren stelle nicht einen automatischen Abruf im Sinne eines freien, an keinerlei Voraussetzungen gebundenen Zugangs zum Melderegister dar. Vielmehr erfolge die Auskunftserteilung dann, wenn die Angaben des Auskunftssuchenden den Betroffenen eindeutig identifizieren und eine Gebühr gezahlt worden ist.

6.4. Konkretisierung der datenschutzrechtlichen Anforderungen hinsichtlich der einfachen Melderegisterauskunft

Soll die einfache Melderegisterauskunft im automatisierten Abrufverfahren über das Internet erteilt werden, so muss sie insbesondere im Einklang mit dem Datenschutzrecht stehen. Die Erteilung einer einfachen Melderegisterauskunft im Weg automatisierten Abrufverfahrens über das Internet muss daher zunächst die Anforderungen aus dem TDDSG, die an die Meldebehörde gestellt werden, umsetzen. Dabei ist zu beachten, dass die an dem Verfahren Beteiligten in verschiedenen Rollen auftreten:

Die Meldebehörde tritt im Rahmen des Auskunftsverfahrens als verantwortliche Stellen für die Verarbeitung der Daten der Antragsteller und der im Register Erfassten auf. Zugleich ist sie Anbieter eines Teledienstes und muss in dieser Rolle die Anforderungen des TDDSG erfüllen.

Die Antragsteller sind zugleich verantwortliche Stellen und Betroffene: Verantwortliche Stelle insofern, als sie Daten über die im Register Erfassten bereits verarbeiten, die Übermittlung personenbezogener Daten beantragen und die übermittelten Daten ebenfalls verarbeiten. Zugleich sind sie ihm Rahmen der Signaturverfahren, des Teledienstes und der Gebührendatenverarbeitung Betroffene.

Die im Register Erfassten sind Betroffene im Rahmen der Melderegisterauskunft.

Die unterschiedlichen Rollen der Akteure sowie die einzelnen Handlungsabschnitte sind klar voneinander zu differenzieren, um eine datenschutzrechtliche Untersuchung sinnvoll durchführen zu können. Dies ist nur dann möglich, wenn die Transportbehälterebe-

ne von der Inhaltsebene strikt getrennt wird. Anhand einzelner Szenarien werden im Folgenden die datenschutzrechtlichen Anforderungen dargestellt.

Im Folgenden werden die Datenschutzanforderungen und die Gestaltungsmöglichkeiten an Hand von Szenarien dargestellt, die sich am Ablauf der Anmeldung und Durchführung einer Melderegisterauskunft orientieren.

6.4.1 Szenario I: Zulassung zum automatisierten Abrufverfahren

Jeder ist berechtigt, ohne Angabe von Gründen eine einfache Melderegisterauskunft zu beantragen. Eine Identifizierung und Authentifizierung des Anfragenden ist für den Erhalt der Melderegisterauskunft aus rechtlicher Sicht nicht erforderlich. Insofern kann der gelegentlich Anfragende bei einem Anruf im Online-Verfahren anonym bleiben. Hierbei werden keine personenbezogenen Daten gespeichert.

Anders ist der Fall, wenn ein Abruf bei Bezahlen nach Sammelrechnung oder eine gebührenfreie Behördenauskunft nach § 29 NMG gewollt wird. In diesem Fall muss vor der automatisierten Auskunft die Berechtigung des Nutzers für dieses Verfahren geprüft werden. Die Behörde kann das Auskunftsverfahren auf diejenigen beschränken, die sich bei ihr hierfür angemeldet haben und für die dadurch die Kompatibilität der technischen Verfahren zur Authentisierung, zum Abruf und zur Gebührenentrichtung sichergestellt ist. Zu diesem Zweck sieht auch die LHH die Anmeldung und Zulassung zum automatisierten Abrufverfahren vor.

6.4.1.1 Anfall personenbezogener Daten: Bestandsdaten und Verwaltungsdaten

Mit Unternehmen, die regelmäßig eine Abfrage machen und die Gebühr zyklisch per Rechnung erhoben wird, wird die LHH eine Rahmenvereinbarung treffen. In einem öffentlichen-rechtlichen Vertrag werden u.a. die Abstände für die Rechnungsschreibung sowie der berechtigte Nutzerkreis, eine Erklärung der Abfrageberechtigten darüber, dass sie über einen eventuellen Einzelverbindungsnachweis aufgeklärt wurden, festgehalten. Insoweit werden Informationen über die berechtigten Mitarbeiter des Unternehmens bekannt gegeben. Dies geschieht mit der Einwilligung der Betroffenen in die Erhebung seiner Daten und ist daher datenschutzrechtlich unbedenklich.

Bestandsdatenverarbeitung

Als Bestandsdaten sind personenbezogene Daten eines Nutzers zu verstehen, die im Zusammenhang mit der Begründung und Änderung eines Vertragsverhältnisses verarbeitet, erhoben oder genutzt werden. Sie sind quasi Grunddaten eines Vertragsverhältnisses und ihre Verarbeitung ist zulässig, soweit sie für das Vertragsverhältnis benötigt werden. Da sie der Identifikation des Netznutzers dienen, sind sie dauerhaft zu speichern. In § 5 Abs. 1 TDDSG ist kein bestimmter Katalog der Bestandsdaten enthalten. Der Zweck des jeweiligen Vertragsverhältnisses bestimmt, welche Daten als Bestandsdaten gelten. Die konkrete Datenerhebung hängt von dem jeweiligen Teledienst ab und ist daher nicht von vornherein zu bestimmen.

Soweit keine besondere Berechtigung erforderlich ist und eine Bezahlung auf andere Weise (durch Geldkartenzahlung) sichergestellt ist, müssen und werden in dem Pilotprojekt auch keine Bestandsdaten erhoben werden.

Für eine Abfrage auf Sammelrechnung oder für Behördenauskünfte ist eine Berechtigung erforderlich. Daher werden der vollständige Name sowie die Anschrift als Bestandsdaten verarbeitet werden. Weiterhin können Rufnummer, Teilnehmer- oder Anschlusskennung (User-ID), Kennwort oder Passwort (PIN), öffentlicher Schlüssel und die E-Mail-Adresse des Nutzers in Betracht kommen. Die persönliche Identifikationsnummer (PIN) und die User Identification (User-ID) fallen ebenfalls darunter, da sie der Authentifizierung des Nutzers dienen.

Verwaltungsdatenverarbeitung

Gemäß § 10 NDSG können zur Vorbereitung der Gebührenerhebung und des Gebühreneinzugs personenbezogene Daten erhoben, gespeichert und verarbeitet werden. Vorliegend werden die Transaktions-ID, die Positionsnummer, die Leistungsart, die Art der Anfrage, die zuständige Kommune bzw. Fachamt, das jeweilige Kassenzeichen, die Haushaltsstelle, das Datum, die Uhrzeit, das ID des Anfragenden, die Kundennummer, Verarbeitungsstatus und -datum und der Gesamtbetrag der betätigten Anfrage gespeichert. Allerdings werden diese Daten nur bei den Großkunden, also den regelmäßigen Nutzern erhoben. Denn die Geldkartenzahler bleiben anonym und bei Abfragen durch eine Behörde fallen keine Gebühren an.

6.4.2 Szenario II: Bereitstellen des Angebots

Auf der Homepage der Behörde wird ein Fenster bereitgestellt, das der Nutzer für seine Anfrage startet. Dieser Vorgang betrifft die Anforderungen aus dem TDG.

Datentyp: Verbindungsdaten

Nach der Legaldefinition des § 2 Nr. 4 TDSV sind Verbindungsdaten personenbezogene Daten eines an der Telekommunikation Beteiligten, die bei der Bereitstellung und Erbringung von Telekommunikationsdiensten erhoben werden.

§ 89 TKG ermächtigt Unternehmen zur Erhebung personenbezogener Daten, die geschäftsmäßig Telekommunikationsdienste anbieten oder hieran mitwirken. Die Unternehmen treten in diesem Fall als Access Provider (Zugangsvermittler) auf, indem sie dem Nutzer ermöglichen, sich über Telekommunikationsverbindungen in das Internet einzuwählen, oder aber eine Verbindung über Standleitungen zur Verfügung stellen. Die LHH sieht eine Zugangsvermittlung weder über Modem noch Standleitungen vor. Die LHH tritt daher nicht als Access Provider auf.

Zur Nutzung eines Dienstleistungsangebots der Behörde muss der Nutzer eine Netzverbindung aufbauen und die Webseite der Behörde aufrufen. Die Netzverbindung muss der Nutzer durch Einwählen bei einem beliebigen Zugangsrechner herstellen.

Er übermittelt an die Behörde nur seine IP-Adresse. Die IP-Adresse weist dann einen Personenbezug auf, wenn die LHH den Nutzer durch die übermittelte Adresse identifizieren kann. Bei dynamischen IP-Adressen, die nach einem Zufallsprinzip von dem Access-Provider für jede einzelne Sitzung neu vergeben werden, hat nur der Zugangsvermittler Kenntnis darüber, welche Adresse wem zugeordnet ist. Der Teleddiensteanbieter, also die LHH, kann ohne zusätzliche Merkmale den Betroffenen nicht identifizieren, es sei denn der Access-Provider übergibt der LHH die durch den Verbindungsaufbau

erhobenen Daten. Die LHH kann allenfalls feststellen, dass die Nummer zu einem bestimmten Provider gehört, aber nicht die Person des Anfragenden. Daher sind dynamische IP-Adressen keine personenbezogenen Daten.

In größeren Unternehmen wird es jedoch üblich sein, dass die Nutzer über feste IP-Adressen verfügen. In diesem Fall lässt sich die IP-Adresse einem konkreten Rechner und mithin regelmäßig einer konkreten Person zuordnen. Grundsätzlich kann bei statischen IP-Adressen ein Personbezug hergestellt werden, so dass diese datenschutzrechtlich relevant sind. Für die Frage, ob ein Personenbezug hergestellt werden kann oder nicht, ist die Perspektive des Empfängers, also die der LHH, entscheidend. Allerdings verhindern technische Vorkehrungen (etwa Firewalls) in der Regel die Aufdeckung des Personenbezugs. In dem Fall ist es für die LHH nicht möglich, einen Personenbezug herzustellen. Daher kann bei derartigen technischen Vorkehrungen der Personenbezug bei statischen IP-Adressen ebenfalls verneint werden.

Anbieterkennzeichnung

Für den Nutzer muss erkennbar sein, mit welchen natürlichen oder juristischen Personen er es auf der Seite des Diensteanbieters zu tun hat. Dadurch soll ermöglicht werden, dass individuelle Rechte oder eine im Interesse der Allgemeinheit bestehende Rechtslage gegenüber dem Anbieter durchgesetzt werden können. Da die Melderegisterauskünfte in einem automatisierten Abrufverfahren Teledienste sind, tritt die Melderegisterbehörde als Diensteanbieter auf und muss die Anbieterkennzeichnung des § 6 TDG erfüllen.

Aus dieser müssen der vollständige Name sowie die Postanschrift des Anbieters, Angaben zu zuständigen Aufsichtsbehörde sowie Angaben zur schnellen elektronischen Kommunikation und der elektronischen Post hervorgehen. Die Information muss so präzise sein, dass die Betroffenen bei der Ausübung ihrer Rechte auf Auskunft, Berichtigung und Löschung keine Probleme haben, gleichgültig ob sie den herkömmlichen Postweg nutzen oder online agieren. Die Informationen für den Nutzer sollten leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein.

6.4.3 Szenario III: Nutzer trifft Auswahl zum Abruf der Auskunft

Der Nutzer entscheidet sich für eine einfache Melderegisterauskunft und startet den Vorgang zum Abruf einer einfachen Melderegisterauskunft im automatisierten Abrufverfahren.

Unterrichtung des Nutzers

Bevor ein Nutzer die Anfrage startet, muss er bestätigen, dass er die rechtlichen Hinweise akzeptiert. Bei registrierten Nutzern geschieht dies einmalig und bereits im Vorfeld bei der Registrierung. Die Nutzer ohne eine vorherige Registrierung, also die gelegentlichen Nutzer, müssen durch das Anklicken des Buttons „Hinweise zur Registrierung“ die Kenntnisnahme der rechtlichen Hinweise bestätigen.

Datentyp: Nutzungsdaten

Nach § 6 Abs. 1 TDDSG können Nutzungsdaten erhoben, verarbeitet und genutzt werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen. Als Nutzungsdaten sind solche Daten anzusehen, die dem Nutzer die Inanspruchnahme von Telediensten ermöglichen; es handelt sich dabei um solche Daten, die während der Nutzung eines Teledienstes entstehen. Beispielhaft werden Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über den vom Nutzer in Anspruch genommenen Teledienst aufgeführt. Nutzungsdaten werden in der LHH nicht außerhalb der aktuellen Nutzung des Teledienstes verarbeitet und danach sofort gelöscht.

Elektronische Einwilligung

Soweit kein Registrierungsverfahren erfolgt, also im Falle der Geldkartenbezahlung, oder nach einem Registrierungsverfahren nachträglich eine Einwilligung notwendig erscheint, kommt vor allem eine elektronische Einwilligung in Betracht. Nach § 4 Abs. 2 TDDSG muss der Diensteanbieter, wenn er die elektronische Einwilligung anbietet, sicherstellen, dass sie nur durch eine eindeutige und bewusste Handlung des Nutzers erfolgen kann, die Einwilligung protokolliert wird und der Inhalt der Einwilligung vom Nutzer jederzeit abgerufen werden kann. Dies ist allerdings nur möglich, wenn die beabsichtigte Datenverarbeitung nur den Teledienst und nicht das mit ihm ermöglichte Verwaltungsverfahren betrifft. Die LHH möchte im Zusammenhang mit der Nutzung des Teledienstes keine personenbezogene Daten verarbeiten, für die eine Einwilligung erforderlich ist.

Technische und organisatorische Vorkehrungen

Nach § 7 NDSG müssen technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung getroffen werden. Nach geltendem Recht stellt das Melderegister als solches kein öffentliches, jedermann zugängliches Register dar. Die LHH kommt diesen Anforderungen durch den Einsatz von Firewall und zwei Filter nach. Das Melderegister wird nicht eins-zu-eins in die Abfragedatenbank übernommen. Vielmehr wird die Abfragedatenbank ein Teilduplikat aus dem Melderegister sein, so dass zwei Datenbanken nebeneinander bestehen werden. Beide Datenbanken müssen grundsätzlich den gleichen Aktualitätsstand haben. Die Amtspflicht der Meldebehörden gemäß § 25 NMG zur Berichtigung und Ergänzung von Daten besteht auch bezüglich der Abfragedatenbank. Die Aktualität beider Datenbanken wird durch die LHH in gleichen, kurzen regelmäßigen Abständen vorgenommen.

Bei Erbringung eines Teledienstes fallen per se Nutzungsdaten an. Zur Sicherung dieser Daten sieht § 4 Abs. 4 TDDSG weitere technische und organisatorische Vorkehrungen vor. Demnach muss der Diensteanbieter, also die LHH, sicherstellen, dass der Nutzer jederzeit seine Verbindung abbrechen kann, die anfallenden personenbezogenen Daten unmittelbar nach Beendigung des Nutzungsvorgangs gelöscht oder gesperrt werden, das Datengeheimnis gewahrt wird, so dass die Daten für Unbefugte nicht zugänglich sind. Bei Inanspruchnahme verschiedener Teledienste müssen die Daten ferner getrennt verarbeitet werden. Die LHH muss die Anforderungen des § 4 Abs. 4 TDDSG erfüllen.

6.4.4 Szenario IV: Aufforderung zur Identifizierung

Der Nutzerkreis wird in drei Gruppen unterteilt: Gelegentliche Nutzer, gewerbliche (regelmäßige) Nutzer und Behörden. Eine Unterscheidung ist notwendig, da für sie unterschiedliche Bezahlverfahren und Anforderungen an die Authentifizierung vorgesehen ist.

Gelegentliche Nutzer

Anfragende, die gelegentlich das Angebot der Meldebehörde in Anspruch nehmen, bedürfen nicht einer vorherigen Registrierung. Ihre Identifizierung ist melderechtlich nicht vorgesehen. Sie ist auch für die Gebührenerhebung nicht vorgesehen, da für diese Nutzergruppe die Zahlung mit der Geldkarte vorgesehen ist. Der Erhalt der Auskunft ist ferner an die vorausgehende Entrichtung der Gebühr gekoppelt. Insoweit bedarf es bei dem gelegentlichen Nutzer nicht einer Identifizierung und er kann anonym bleiben.

Regelmäßige Nutzer

Gewerbliche Kunden, die regelmäßig Anfragen stellen, müssen sich als „registrierte private Stelle“ anmelden. Ihre Authentifizierung wird mittels einer Signaturkarte über ein Zertifikat/MFC erfolgen.

Behörden

Auch bei Anfragen durch eine Behörde erfolgt die Authentifizierung ebenfalls über ein Zertifikat.

6.4.5 Szenario V: Eingabe der Suchkriterien

Nachdem der Identifizierungsvorgang abgeschlossen ist, ruft der Nutzer den Anfragekorb zur Eingabe der Suchkriterien auf, um die Person, über die er eine Auskunft haben möchte, zu identifizieren. Welche und wie viele Daten als Suchkriterien einzugeben sind, bestimmt sich nach dem NMG. Auf dieser Ebene geht es nicht mehr um die Nutzung eines Teledienste, sondern um die inhaltliche Gestaltung des über den Teledienst vermittelten Verwaltungsverfahrens. Auf dieser Inhaltsebene finden die Vorschriften des TDDSG keine Anwendung.

Datentyp: Inhaltsdaten

Inhaltsdaten fallen unabhängig davon an, ob die Verwaltungsleistung digitalisiert über das WWW oder konventionell erbracht wird. Bei der einfachen Melderegisterauskunft handelt es sich um die Suchkriterien auf der einen und um die Angabe von Namen, Anschrift und Namensbestandteilen auf der anderen Seite.

Bestimmen des Betroffenen

Zu dem auskunftsberechtigten Personenkreis zählen neben natürlichen Personen auch juristische Personen, nichtrechtsfähige Personenvereinigungen, privatrechtliche Religionsgesellschaften, Gewerkschaften sowie politische Parteien.

Der Auskunftssuchende muss nach § 33 Abs. 1 Satz 1 NMG den Einwohner, über den er eine Auskunft erteilt haben möchte, „bestimmen“. Darüber hinaus ist die einfache Melderegisterauskunft - abgesehen von der allgemeinen Vorschrift § 4 NMG - nicht an weitere Voraussetzungen gebunden. Unter „Bestimmen“ ist die zweifelsfreie Identifizierbarkeit des Betroffenen zu verstehen. Die zweifelsfreie Identifizierbarkeit ist notwendig, da bei Auskünften, die auf Personenverwechslungen infolge von Namensgleichheit beruhen, gravierende rechtliche, wirtschaftliche oder immaterielle Nachteile (z.B. ungerechtfertigte Zwangsvollstreckung) entstehen können. Besteht eine Verwechslungsgefahr, hat der Auskunftssuchende weitere Kriterien (z.B. die Angabe des Geburtsdatums) zur eindeutigen Bestimmung der von ihm gesuchten Person zu machen.

Der Antragsteller hat den Betroffenen namentlich zu bezeichnen. Allerdings muss der vollständige Name nicht genannt werden. Vielmehr kann eine eindeutige Identifizierung auch durch Namensteile, frühere Namen oder die Angabe der gegenwärtigen oder einer früheren Anschrift ermöglicht werden. Die Angabe der Suchkriterien kann nach der jetzigen Gesetzeslage fragmentarisch erfolgen. Dabei muss die frühere Anschrift nicht gleichzeitig die letzte Anschrift vor dem Umzug sein. Vielmehr kann es sich dabei um eine sehr viel länger zurückliegende Anschrift handeln.

Die LHH sieht als Haupt-Suchkriterien (Mussfelder) den Vornamen, Familiennamen und Namensbestandteile und als zusätzliche Suchkriterien das Geburtsdatum, die Anschrift und das Geschlecht vor. Nach der gegenwärtigen Gesetzeslage ist die Angabe bestimmter Suchkriterien nicht vorgeschrieben. Diese Bestimmung ist dennoch vor dem Hintergrund, dass die Suchanfrage automatisiert und unbegrenzt erfolgt, zulässig. Denn dadurch kann der Erhalt von über die einfache Melderegisterauskunft hinausgehenden Informationen durch Ausforschungen der Suchkriterien vermieden werden. Außerdem werden andere als die vorgesehenen Kriterien für die Suche in dem analogen Verfahren praktisch sehr selten genutzt. Sollte die Angabe weiterer Kriterien dennoch erforderlich werden, steht das bisherige Verfahren weiterhin zur Verfügung.

Nach der künftig zu erwartenden Gesetzeslage (§ 21a MRRG-E) hat der Auskunftsersuchende den vollständigen Namen sowie zwei weitere Kriterien anzugeben, um eine Auskunft zu erhalten. Welche weiteren Kriterien es sein müssen, kann der Gesetzgeber auf Landesebene im Rahmen seiner zugeteilten Kompetenz konkretisieren. Ob auch nach dem künftigen MRRG eine Suche mit Teilangaben möglich sein wird, ist dem MMRG-E nicht eindeutig zu entnehmen. Es bleibt daher abzuwarten, ob hier noch Klarheit durch den Gesetzgeber geschaffen wird.

Die LHH plant sowohl Einzelabfragen als auch Mehrabfragen in Form eines “Anfragekorbs”, in dem mehrere Anfragen gesammelt und abgeschickt werden, zu ermöglichen. Bei dem „Anfragekorb“ handelt es sich um eine Unterform der einfachen Melderegisterauskunft, nämlich um eine Sammelauskunft. Auch bei einer Sammelauskunft ist jede Auskunft wie eine Einzelauskunft zu behandeln, das heißt, jede Auskunft ist einzeln zu bewerten und abzurechnen. Gegen die Sammlung mehrerer Anfragen in einem Anfragekorb bestehen keine datenschutzrechtlichen Bedenken.

Umfang der Datenbank

Damit die betroffene Person, über die eine Auskunft verlangt wird, zweifelfrei identifiziert wird, muss ein umfangreiches Angebot an Suchkriterien ermöglicht werden. Im bisherigen Offline-Verfahren wurde auf den Datenbestand des Melderegisters in der nach § 2 Abs. 1 MRRG vorgesehenen Form zugegriffen. Auch der Entwurf des MRRG erlaubt eine Suche aus dem Bestand der nach dieser Vorschrift gespeicherten Daten. § 21 Abs. 1a MRRG-E sieht vor, dass bei einer Online-Auskunft der Betroffene mit Vor- und Familiennamen sowie mindestens zwei weiteren der aufgrund von § 2 Abs. 1 MRRG gespeicherten Daten bezeichnet werden muss. Die Formulierung des § 21 Abs. 1a Nr. 2 MRRG-E ist so zu verstehen, dass alle in § 2 Abs. 1 genannten Daten als Suchkriterien zur Bestimmung einer Person zulässig sind, wobei Vor- und Familiennamen zwingend vorgeschrieben sind. Die LHH beabsichtigt, nur die bisher im Meldebereich verwendeten Suchstrategien zuzulassen. Die folgenden Daten sollen als Suchkriterien verwendet werden:

1. Familiennamen
2. Vornamen
3. frühere Namen
4. Doktorgrad
6. Tag der Geburt (nicht Ort)
7. Geschlecht
12. gegenwärtige, frühere und zukünftige Anschriften, Haupt- und Nebenwohnungen

Die nachfolgenden Merkmale könnten nach dem derzeitigen Stand des § 21 Abs. 1a MRRG-E als Suchkriterien für die Personenidentifikation als zulässig angesehen werden. Sie sind jedoch geeignet, durch Ausprobieren (mehrfache Einzelabfragen zu einer Person) mittels Eingabe der wenigen Ausprägungen der entsprechenden Merkmale Informationen zu erhalten, die in der einfachen Melderegisterauskunft nicht vorgesehen sind, zum Teil auch in der Meldeauskunft für Behörden nicht vorgesehen sind (Religionszugehörigkeit). Gegen die Verwendung dieser Suchkriterien bestehen deshalb erhebliche rechtliche Bedenken:

8. Erwerbstätig / nicht erwerbstätig (2 Ausprägungen, soll nach E-MRRG entfallen)
10. Staatsangehörigkeiten (größere Anzahl Ausprägungen, bei Vermutung oder Kenntnis des Herkunftsbereichs aber leicht einzuschränken)
11. Rechtliche Zugehörigkeit zu einer Religionsgesellschaft (6 Ausprägungen)
14. Familienstand (4 Ausprägungen)
18. Übermittlungssperren (je 2 Ausprägungen)

Diese Datenfelder werden daher im Pilotprojekt nicht als Suchkriterien verwendet.

Bei den verbleibenden Feldern bestehen die genannten Bedenken nicht; sie wären damit grundsätzlich zur Bestimmung der gesuchten Personen geeignet. Dies sind:

5. Ordensnamen/ Künstlernamen
6. Ort der Geburt

9. Gesetzliche Vertreter

13. Tag des Ein- und Auszugs

14. (Familienstand) bei Verheirateten zusätzlich Tag und Ort der Eheschließung

17. Ausstellungsbehörde, -datum, Gültigkeitsdauer des Personalausweises und Passes.

Diese Felder haben jedoch für die Personenbestimmung zur Erteilung einer "Einfachen Melderegisterauskunft" durch die Meldebehörde derzeit keinerlei praktische Bedeutung. Dies wird sich auch bei der Online-Auskunft nach unserer Auffassung nicht verändern. Ihre Aufnahme in die Suchmasken würde nach Einschätzung der LHH vielmehr nur zur Verunsicherung der Nutzer führen, zusätzlichen Aufwand bei der Entwicklung bedeuten und dabei keinerlei positiven Effekt erzielen.

Eine umfangreiche Datenbank ist in Hinblick darauf, den Betroffenen eindeutig zu identifizieren und eine Verwechslungsgefahr auszuschließen, zu empfehlen. Gegen einen umfangreichen Datenbestand in der Abfragedatenbank spricht jedoch, dass dem Anfragenden auf diese Weise ermöglicht wird, durch die Angabe unterschiedlicher Suchkriterien in beliebigen Versuchen indirekt mehr über den Betroffenen in Erfahrung zu bringen als er im Rahmen der einfachen Melderegisterauskunft erfahren würde. Insoweit ist ein kleinerer Datenbestand vorzuziehen.

Nach dem Entwurf zum MRRG kann der Betroffene der Auskunftserteilung im automatisierten Abrufverfahren, und zwar auch nur dieser Form der Auskunftserteilung, widersprechen. In diesem Fall ist die Auskunftserteilung über das Internet grundsätzlich nicht zulässig. Auch die Behördenauskunft muss bei Widerspruch des Betroffenen unterbleiben. Den Kriterien der Datensparsamkeit und Risikovorsorge würde es eher entsprechen, wenn die Daten des Widersprechenden gar nicht in die Abfragedatenbank aufgenommen würden. Sie sind für die Abfrage nicht erforderlich. Allerdings fordert der Wortlaut des § 21 MRRG-E nur die „Abrufbarkeit" zu unterbinden. Er bezieht sich nur auf eine spezifische Phase der Datenverarbeitung und regelt somit nicht die andere Phase der Speicherung der Daten. Soweit nur eine Datenbank vorhanden wäre, die das Melderegister und die Abfragedatenbank enthielte, wäre diese Frage ohnehin obsolet. Daher erscheint es vertretbar, die Abfrage durch andere Mittel zu verhindern als den Verzicht auf die Speicherung der Daten.

6.4.6 Szenario VI: Erhalt der Auskunft

Ist die Voraussetzung des „Bestimmens" erfüllt, kann die Behörde eine einfache Auskunft aus dem Melderegister erteilen. Diese Auskunft umfasst nach § 33 Abs. 1 NMG die Angaben des Vor- und Familiennamens mit den jeweiligen Namensbestandteilen, den Doktorgrad sowie die Anschriften. Nach dem Wortlaut des § 33 Abs. 1 NMG ist das Sterbedatum nicht Bestandteil der einfachen Melderegisterauskunft (enumerative Aufzählung). Allerdings stellt seine Erteilung keine Einschränkung des Rechts auf informationelle Selbstbestimmung dar. Seiner Erteilung im Rahmen der einfachen Melderegisterauskunft ist nichts entgegenzusetzen.

Die Auskunft bezieht sich lediglich auf die aktuellen Daten des Einwohners. Dies ergibt sich aus dem Umkehrschluss des § 33 Abs. 2 NMG, da hier die Erteilung der früheren

Daten nur im Rahmen der erweiterten Melderegisterauskunft ausdrücklich erwähnt wird. Ferner betrifft es die Daten von Personen über 18 Jahren (Adressbuchdaten).

Nach dem die eingegebenen Daten mit den im Melderegister enthaltenen Daten abgeglichen werden und eine Übereinstimmung festgestellt wird, sollte in einem Auskunftsfenster die begehrte Auskunft unter entsprechenden Sicherheitsvorkehrungen „mitgeteilt“ werden.

Ergebnis der Suche:	**Zulässige Auskunft:**	**Unzulässige Auskunft:**
Keine Auskunftsmöglichkeit, da Person nicht gefunden	„Eine Auskunft kann nicht erteilt werden.“	
Der Betroffene ist unbekannt verzogen	„Unbekannt verzogen“	
Es besteht nur eine einzige Auskunftsmöglichkeit	Auskunft über die o.g. Daten	Mehr oder weniger als die genannten Daten
Mehrere Auskunftsmöglichkeiten	„Die Auskunft kann nicht erteilt werden, da mehrere Treffer. Die Suche bedarf einer Einschränkung“ (wie viele Einschränkungsversuche?)	Auskunft über alle Betroffenen oder einen beliebigen Betroffenen
Es ist eine Auskunftssperre eingetragen	„Eine Auskunft kann nicht erteilt werden.“	Hinweise und nicht mehr neutrale Auskünfte auf die Auskunftssperre; Betroffene ermittelt, aber Auskunft aus rechtlichen Gründen nicht möglich..
Es ist ein Widerspruch eingetragen	„Eine Auskunft kann nicht erteilt werden.“	Wie das zur Auskunftssperre Gesagte
Der Betroffene ist zwar ermittelt, aber bereits verstorben	„Der Betroffene ist verstorben“	Auskunft über Sterbetag und –ort.
Trotz fehlerhafter Angaben, z.B. falsche Schreibweise, gibt es nur **eine** Auskunftsmöglichkeit	Eine Auskunft kann erteilt werden, indem die betroffenen Daten aufgeführt werden.	
Es sind mehrere Anschriften eingetragen und der Anfragende möchte alle erfahren	Die Meldebehörde ist im Rahmen ihres Ermessens befugt, grundsätzlich die Anschrift der Hauptwohnung zu erteilen, wenn nicht eine Auskunft über sämtliche Anschriften *erwünscht* wird. Aus der Verwendung des Plurals "Anschriften" geht eindeutig hervor, dass auf Anfrage die Anschriften sämtlicher Wohnungen mitgeteilt werden dürfen.	Der Status der Wohnung als einzige Wohnung, Haupt- oder Nebenwohnung ist ein selbständiges Datum, das nicht im Rahmen einer einfachen Melderegisterauskunft mitgeteilt werden kann. Dies wird insofern durch § 22 Abs. 1 Nr. 12 NMG bestätigt. Eine Auskunft darüber muss unterbleiben.

6.4.7 Szenario VII: Gebührabrechnung und -bezahlung

Nach § 1 Abs. 1 Niedersächsisches Verwaltungskostengesetz (NVwKostG) kann für Amtshandlungen eine Gebühr erhoben werden. Für die elektronisch beantragte und erteilte einfache Melderegisterauskunft ist eine Gebühr in Höhe von 8,- DM pro Abfrage vorgesehen, wenn besondere Ermittlungen nicht erforderlich sind. Dies ist in der Niedersächsischen Allgemeinen Gebührenordnung (AllGO) Nr. 63 geregelt. Wenn mehrere Auskünfte gleichzeitig erteilt werden, kann eine Ermäßigung der Gebühr für die zweite und weitere Auskunft erfolgen. Nach § 5 Abs. 1 NVwKostG ist Schuldner der Kosten derjenige, der Anlass zur Vornahme der Amtshandlung gegeben hat. Der Auskunftssuchende ist demnach der Kostenschuldner. Die Kosten werden auch dann erhoben, wenn die Vornahme der Amtshandlung abgelehnt wurde. Die Kosten entstehen nach § 6 Abs. 1 NVwKostG mit der Beendigung der Amtshandlung oder der Rücknahme des Antrags und werden nach § 7 NVwKostG mit der Bekanntgabe des Gebührenbescheids an den Kostenschuldner fällig. Eine besondere Form ist für die Gebührenerhebung nicht vorgesehen. Demnach kann die Gebührenerhebung auch online erfolgen.

Zahlung über die Geldkarte

Nutzer, die gelegentlich privat oder geschäftlich, eine Auskunftserteilung aus dem Melderegister im Online-Verfahren wünschen, können, ohne besondere Voraussetzungen wie etwa eine Vorabregistrierung erfüllen zu müssen, diese bekommen. Sie müssen mit der Geldkarte die zu entrichtende Gebühr im Voraus zahlen und erhalten anschließend die Auskunft aus dem Melderegister. Die einzige Bedingung für die Teilnahme an diesem Verfahren ist, dass der Nutzer über die technische Ausstattung verfügt. Die Zahlungsaufforderung stellt einen Gebührenbescheid dar, der in der Online-Form lediglich bei den anonymen Nutzern mit Geldkarte vorkommt. Bei dem Online-Gebührenbescheid handelt es sich um einen feststellenden Verwaltungsakt im Sinne des § 35 Abs. 1 VwVfG. Nach dem VwVfG ist eine Rechtsbehelfsbelehrung vorliegend nicht zwingend vorgesehen, weil die Erteilung der Rechtsmittelbelehrung für die Frist, nicht aber für das Zustandekommen des Verwaltungsakts von Bedeutung ist. Zur Beschleunigung von Verwaltungsverfahren gilt der Grundsatz der Formfreiheit. Demnach können Verwaltungsakte grundsätzlich formfrei erlassen werden, es sei denn Spezialgesetze sehen eine bestimmte Form vor. In dem NVwKostG ist eine Formvorschrift nicht ersichtlich. Daher erübrigen sich eventuellen Anforderungen an eine qualifizierte Signatur.

Zahlung über Sammelabrechnung

Für die Auskunftserteilung an regelmäßige Nutzer zu geschäftlichen Zwecken soll die Abrechnung im Wege einer Rechnungsstellung auf dem Papierweg erfolgen. Die Rechnung soll in bestimmten Perioden ausgestellt und per Post dem Kostenschuldner zugestellt werden. Für diese Verfahren ist eine Identifizierung der Institution wie der ihr angehörenden Mitarbeiter, die zum Abruf berechtigt werden sollen, erforderlich.

Die LHH plant mit der registrierten Einrichtung in Form eines öffentlich-rechtlichen Vertrages eine Vereinbarung zu treffen, in der die Rechte und Pflichten konkretisiert, Abrechnungsperioden festgelegt, Zahlungsweisen und Umfang der Rechnungslegung vereinbart werden. Die Vorschriften des NVerwKostG enthalten Regelungen zu diesen

Maßnahmen. Nach der modifizierten Subjektstheorie handelt es sich um öffentlich-rechtliches Verwaltungshandeln, da die streitentscheidenden Normen aus dem öffentlichen Recht stammen. Für einen öffentlich-rechtlichen Vertrag nach § 54 ist eine gesetzliche Ermächtigung im Einzelfall nicht erforderlich. Soweit gesetzliche Vorschriften oder allgemeine Rechtssätze dem öffentlich-rechtlichen Vertrag nicht entgegenstehen, kann die Behörde diese Handlungsweise auch wählen. Auch im Gebührenrecht ist grundsätzlich das allgemeine Verwaltungsrecht anwendbar. In den Vorschriften des LGebG ist keine Vorschrift enthalten, die den Abschluss solcher Verträge verbietet. Öffentlich-rechtliche Verträge sind demnach auch im Gebührenrecht zulässig.[168]

Datenerhebung bei dem Bezahlverfahren mittels Geldkarte

Das TDDSG fordert die Gestaltung von Zahlungsmodellen, bei denen so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden. Die Nutzung des Teledienstes „Zahlungssystem" soll, wenn dies technisch möglich und zumutbar ist, anonym oder pseudonym erfolgen. Pseudonyme Zahlung sollte erfolgen, wenn die Identifizierung des Gebührenschuldigen rechtlich vorgesehen oder zwecks Gebührenerhebung erforderlich ist. Wie bereits erläutert, besteht keine Notwendigkeit etwa aus dem NMG zur Authentifizierung des Anfragenden, so dass der Nutzer dieses Verfahrens durchaus anonym bleiben kann. Eine Authentifizierung ist ferner auch aus Gründen der Gebührenerhebung nicht erforderlich, da die Auskunft von einer tatsächlich erfolgten Zahlung abhängig gemacht wird. Daher werden bei der anonymen Zahlung mittels Geldkarte keine personenbezogenen Daten verarbeitet.

Datenerhebung bei dem Bezahlverfahren mittels Sammelrechnung

Bei den Nutzern, die eine regelmäßige Abfrage aus dem Melderegister machen, wird die Gebühr über eine Sammelrechnung erhoben. Dabei werden Informationen über Transaktions-ID, Positionsnummer, Leistungsart, Art der Anfrage, Kommune/ Fachamt, Kassenzeichen, Haushaltsstelle, Datum, Uhrzeit, ID des Anfragenden, Kundennummer, Verarbeitungsstatus und -datum sowie Gesamtbetrag gespeichert. Ihre Erhebung ist für die Rechungsschreibung erforderlich. Um im Streitfall einen Nachweis über die erteilte Auskunft erbringen zu können bzw. ein Mahnverfahren abschließen zu können, ist eine Speicherungsdauer von 180 Tagen vorgesehen. Nach Ausgleich der Gebührenschuld ist die Speicherung dieser Daten nach § 17 Abs. 2 Nr. 2 NDSG nicht mehr zulässig, da ihre Kenntnis für die Aufgabenerfüllung der Behörde nicht mehr erforderlich ist.

Da die Gebührenerhebung die Verwaltungshandlung und nicht den Internetdienst betrifft, gelten nicht die Anforderungen zur Datensparsamkeit des § 4 Abs. 6 TDDSG. Auch § 3a des neuen BDSG ist nicht einschlägig. Doch können die dort explizit ausgewiesenen Anforderungen auch aus dem Erforderlichkeitsprinzip entnommen werden. Da jeder Auskunftsbegehrende, der für eine Sammelrechnung registriert ist, auch jederzeit die Abfrage mittels Geldkarte durchführen kann, bietet die LHH auch diesem Personenkreis die Möglichkeit einer anonymen Abfrage und Bezahlung.

168 So auch: VGH BW, B.v. 15.2.1993- 2 S 2674/92- VBlBW 1993, 257.

Die LHH könnte auch Pseudonyme in ihr Verfahren einbinden. Für sie ist bei der Auskunft auf Sammelrechnung nur entscheidend, dass die Auskunft einem Sammelkonto zugerechnet werden kann und hierfür die Einrichtung und Autorisierung eines Abfragers durch den Koordinator des Kunden erfolgt ist. Daher kann der Abfrager auch mit einem Zertifikat agieren, das entsprechend § 7 Abs. 1 Nr. 1 SigG auf ein Pseudonym lautet. Das Pseudonymzertifikat wird von dem Zertifizierungsdienstanbieter ausgegeben und enthält die gleichen Einträge wie ein Zertifikat mit vollem Namen. Die LHH müsste es nur akzeptieren, um der Anforderung des § 4 Abs. 6 TDDSG auch in dieser Hinsicht gerecht werden zu können.

Das Pseudonym wirkt gegenüber der LHH und allen anderen Beteiligten, nicht aber gegenüber dem Koordinator, da er die von ihm zu autorisierende Person kennt.

Die LHH sollte der Nutzungsvereinbarung mit den Kunden ein Merkblatt (besser viele) beifügen, in dem sie ausdrücklich auf die Möglichkeit der pseudonymen Abfrage hinweist und erläutert, dass bei der Beantragung des Zertifikats beim Zertifizierungsdiensteanbieter auch ein Zertifikat auf ein Pseudonym beantragt werden kann.

6.4.8 Szenario VIII: Rechte der Betroffenen

Auskunft

§ 4 Abs. 7 TDDSG gibt dem Nutzer das Recht auf unentgeltliche und unverzügliche Auskunft über die zu seiner Person oder seinem Pseudonym gespeicherten Daten bei dem Diensteanbieter. Die Auskunft ist gemäß § 4 Abs. 7 Satz 2 TDDSG auf Verlangen des Nutzers auch elektronisch zu erteilen. Da über den Zeitraum der Erbringung des Teledienstes keine Nutzungsdaten und auch keine Abrechnungsdaten für den Teledienst gespeichert werden, könnte sich der Anspruch nur auf die Bestandsdaten erstrecken. Diese werden aber nur von den Anfragenden, die eine Sammelrechnung und von abfrageberechtigten Behördenmitarbeitern erhoben. Diese haben außerdem für die Verwaltungsdaten einen umfassenden Auskunftsanspruch nach § 17 NDSG. Die Auskünfte über Stamm- und Verwaltungsdaten kann die LHH erfüllen. Sie seiht jedoch keine elektronische Auskunftserteilung vor.

Sperre

Nach § 5 NMG stehen jedem Einwohner und jeder Einwohnerin gegenüber der Meldebehörde verschiedene Rechte zur Verfügung. Dazu zählt die Einrichtung von Übermittlungssperren. Dieser Anforderung kommt die LHH durch die Einrichtung entsprechender technischer Vorkehrungen nach.

Berichtigung

Sind die gespeicherten Daten über die betroffene Person nicht richtig, hat der Betroffene ein Recht auf Berichtigung der unrichtigen Daten. Dieses Recht kann im Verfahren der LHH problemlos umgesetzt werden.

Löschung

Wenn die Daten für die Aufgabenerfüllung nicht mehr erforderlich sind oder ihre Speicherung nicht mehr zulässig sind, besteht ein Recht des Betroffenen auf die Löschung der zu ihrer Person gespeicherten Daten. Auch dieses Recht ist problemlos erfüllbar.

Widerspruch nach § 21a MRRG-E

Tritt das MRRG in der bisher geplanten Form in Kraft, so muss die Behörde dem Betroffenen künftig ein Widerspruchsrecht einräumen. Anders als im geltenden Gesetz, wonach der Betroffene unter substantiierter Darlegung seines berechtigten Interesses eine Auskunftssperre durchsetzen kann, sieht der Entwurf des MRRG in § 21a MRRG-E eine Widerspruchsrecht vor. Demnach kann der Betroffene der Erteilung einer einfachen Melderegisterauskunft über die zu seiner Person gespeicherten Daten im Wege des Widerspruchsverfahrens verhindern. Dafür bedarf es nicht der Glaubhaftmachung eines besonderen Interesses. Vielmehr kann er ohne jegliche Voraussetzungen der Auskunftserteilung auf dem Online-Wege, und auch nur diesem, widersprechen.

7. Ausblick

Die Entwicklung zu einem Electronic Government ist notwendig und wünschenswert. Der Weg dorthin wird länger sein als manche Politiker sich dies heute vorstellen und die erhofften Wirkungen werden sich erst langfristig einstellen. Der Weg zum virtuellen Rathaus wird sich nicht in wenigen Jahren realisieren lassen und vielmehr ein lang anhaltender Lernprozess für alle Beteiligte sein. Um so wichtiger ist es, dass vermehrt kommunale Dienstleistungen über das Internet angeboten werden, die auch rechtsverbindlich sind und tatsächlich eine spürbare Erleichterung für Bürger und Unternehmen mit sich bringen. Zu hoffen ist, dass der dadurch angestoßene Prozess zu einer nachhaltigen Verwaltungsreform führt, die eine effektive bürgernahe Dienstleistungsverwaltung hervorbringt.

Electronic Government und andere gesellschaftliche Formen der Nutzung weltweiter Netze wird zu einem deutlichen Wandel in der Rolle des Staates führen.[169] Immaterialisierung und Globalisierung der Informationsströme durch das Internet verhindern, dass der Staat und Gemeinwohlbelange nicht mehr in dem Umfang durchsetzen und die Grundrechte seiner Bürger seine Bürger nicht so effektiv schützen kann wie bisher. E-Government bringt einen Struktur- und Aufgabenwandel des Staates bei der Erfüllung seiner verfassungsrechtlichen Pflichten von der Erfüllung zur Gewährleistungs- und Infrastrukturverantwortung mit sich. Er muss den Einzelnen in die Lage versetzen, sich auch – besser als bisher – selbst zu schützen, soweit dadurch sozialverträgliche Verhältnisse erhalten bleiben. Und er muss technische und rechtliche Rahmenbedingungen schaffen, die Selbstschutz und die Gewährleistung von Grundrechten unterstützen. Hierzu gehört sicher auch die Einführung eines Datenschutzaudits.[170] Viele der genannten datenschutzrechtlichen Anforderungen werden nur zu erreichen sein, wenn die verantwortlichen Stelle ein Eigeninteresse an diese erkennt und eine Eigeninitiative entwi-

169 S. ausführlich dazu *Roßnagel* 2000b, 257 ff., *ders.* DuD 1997, 505.

170 S. hierzu ausführlich *Roßnagel* 2000a, 5 f.

ckelt, sie umzusetzen. Dies wird sie nur tun, wenn sie dafür Anerkennung erhält und mit dieser um Vertrauen für ihre Datenverarbeitung werben kann.

Literaturverzeichnis

Arlt, U.	Künftige Rechtssprechung der Kontrollstellen für den Datenschutz, in: Bäumler, H. (Hrsg.), Der neue Datenschutz, Berlin 1998, 271.
Bachmeier, R.	Vorgaben für datenschutzgerechte Technik, DuD 1996, 672.
Bäumler, H..	Der neue Datenschutz, RDV 1999, 5.
Bäumler, H.	Wie geht es weiter mit dem Datenschutz?, DuD 1997, 446.
Bäumler, H.	New Public Management und Persönlichkeitsschutz, CR 1997, 169.
Bäumler, H.	Datenschutz als Wettbewerbsvorteil, DuD 2001, 376.
Bäumler, H.	Der neue Datenschutz in der Realität, DuD 2000, 257.
Bäumler, H.	Eine sichere Informationsgesellschaft?, DuD 2001, 348.
Belz, R	Kommentar zum Meldegesetz für Baden-Württemberg, 3. Auflage, Stuttgart [u.a.] 1987.
Bizer, J.	Technikfolgenabschätzung und Technikgestaltung im Datenschutzrecht, in: Bäumler, H. (Hrsg.), Der neue Datenschutz, Berlin 1998, 45.
Bizer, J.	Unabhängige Datenschutzkontrolle, DuD 1997, 481.
Bizer, J./Fox, D./Reimer, H.	Recht und Technik, DuD 1997, 2.
Bizer, J.	Datenschutz in neuen Medien, in: Kubicek, H./Braczyk, H.-J./Müller, G./Neu, W./Raubold, E./Roßnagel, A. (Hrsg.), Die Ware Information auf dem Weg in eine Informationsökonomie, Jahrbuch Telekommunikation und Gesellschaft 1997, Heidelberg 1997, 146.
Bizer, J.	Datenschutz verkauft sich- wirklich!, DuD 2001, 250.
Bizer, J.	Ziele und Elemente der Modernisierung des Datenschutzes, DuD 2001, 274.
Boehme-Neßler, V.	Electronic Government: Internet und Verwaltung, NVwZ 2001, 374.
Borking, J.	Der Identity-Protector, DuD 1996, 654.
Bull, H.-P.	Zeit für einen grundlegenden Wandel des Datenschutzes?, CR 1997, 711.
Büllesbach, A.	Datenschutz bei Data Warehouses und Data Mining, CR 2000, 11.

Büllesbach, A.	Neue Anforderungen an die Datenschutzkontrolle nach den Multimediagesetzen, in: Bäumler, H. (Hrsg.), Der neue Datenschutz, Berlin 1998, 99.
Büllesbach, A.	Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsfaktor, RDV 1997, 239.
Deutscher Städtetag	Schritte auf dem Weg zum digitalen Rathaus, Berlin 2000.
Dieckmann, J.	Herausforderungen der Kommunen durch das Internet, in: Kubicek, H/Braczyk, H./Klumpp, D./Müller, G./Neu, W./Raubold, E./Roßnagel, A. (Hrsg.), Multimedia@Verwaltung, Heidelberg 1999, 67.
Dix, A.	Verwaltung und Internet aus der Sicht des Datenschutzes, in: Kubicek/ H., Braczyk, H.-J./ Müller, G./ Neu, W./Raubold, E./ Roßnagel, A. (Hrsg.), Multimedia@Verwaltung, Jahrbuch Telekommunikation und Gesellschaft Heidelberg 1999, 178.
Dix, A.	Digitale Signaturen im Verwaltungsverfahren: Besondere Sicherheitsanforderungen erforderlich?, K&R 2000 Beilage 2, 20.
Eifert, M.	Electronic Government als gesamtstaatliche Organisationsaufgabe, ZG 2001, 115.
Engel-Flechsig, S.	Datenschutz in Telediensten, DuD 1997, 8.
Engel-Flechsig, S.	Die datenschutzrechtlichen Vorschriften im IuK-Gesetz, RDV 1997, 59.
Engels, S./Entenbäumer, E.	Sammeln und Nutzen von e-Mail-Adressen zu Werbezwecken, K&R 1998, 196.
Esser, M.	Internet: Begriffe und Erläuterungen, RDV 1996, 46.
Federrath, H./Pfitzmann, A.	Neues Datenschutzrecht und die Technik, in: Kubicek, H./Klumpp, D./Fuchs, G./Roßnagel, A. (Hrsg.), Internet @Future, Jahrbuch Telekommunikation und Gesellschaft 2001, Heidelberg 2001, 252.
Forsthoff, E.	Der Staat der Industriegesellschaft: Am Beispiel der BRD, München 1971.
Forsthoff, E.	Rechtsfragen der leistenden Verwaltung, Stuttgart 1959.
Fuhrmann, H.	Vertrauen im Electronic Commerce, Baden-Baden 2001.
Floeting, H./Gaevert, S.	Städte im Netz: Elektronische Bürger-, Stadt-, und Wirtschaftsinformationssysteme der Kommunen; Ergebnisse einer Difu-Städteumfrage, Berlin 1997.

Garstka, H.-J.	Empfiehlt es sich, Notwendigkeit und Grenzen des Schutzes personenbezogener-auch grenzüberschreitender-Informationen neu zu bestimmen?, DVBL 1998, 981
Geis, I.	Internet und Datenschutzrecht, NJW 1997, 288.
Gesellschaft für Informatik e.V.	Electronic Government als Schlüssel zur Modernisierung- Memorandum des Fachausschusses Gesellschaft im VDE (Hrsg.) Verwaltungsinformatik der Gesellschaft der Informatik e.V. und des Fachbereichs 1 der Informationstechnischen Gesellschaft im VDE, Bonn/Frankfurt 2000.
Grabow, B./Floeting, H.	Wege zur telematischen Stadt, in: Kubicek/ H., Braczyk, H.-J./ Müller, G./ Neu, W./Raubold, E./ Roßnagel, A. (Hrsg.), Multimedia@Verwaltung, Jahrbuch Telekommunikation und Gesellschaft 1999, Heidelberg 1999, 75.
Greenleaf, G./Clarke, R.	Privacy Implications of Digital Signatures, http://www.anu.edu.au/people/Roger.Clarke/DV/PKI2000.html, besucht im Januar 2002.
Grewlich, K.W.	Wirtschaftsvölkerrechtliche Ordnung für das Internet, K&R 1998, 81 A.
Grewlich, K.W.	Wirtschaftsvölkerrecht kommunikationstechnisch gestützter Dienstleistungen, RIW 1988, 694.
Grimm, R.	Elektronische Zahlungssysteme im Überblick, in: Kubicek, H./Klumpp, D./Fuchs, G./Roßnagel, A. (Hrsg.), Internet@Future, Jahrbuch Telekommunikation und Gesellschaft 2001, Heidelberg 2001, 197.
Gundermann, L.	E-Commerce trotz oder durch Datenschutz?, K&R 2000, 225.
Habbel, F.-R.	Computer für die Stadt der Zukunft: Internationale Fallbeispiele für Entscheider [cities of tomorrow, international network for better local government], Gütersloh 1998.
Hagen, M.	Ein Referenzmodell für Online-Transaktionssysteme im Electronic Government, München 2001.
Hentschel, P.	Die Entwicklung des Straßenverkehrsrecht im Jahre 1997, NJW 1998, 649.
Hillenbrand-Beck, R./Greß, S.	Datengewinnung im Internet, DuD 2001, 389.
Holznagel, B./Krahn, C./	Electronic Government auf kommunaler Ebene
Werthmann, C.	Die Zulässigkeit von Transaktionen im Internet, DVBl. 1999, 1477.
Hoffmann-Riem, W.	Weiter so im Datenschutzrecht?, DuD 1998 684.

Hoffmann-Riem, W.	Informationelle Selbstbestimmung als Grundrecht kommunikativer Entfaltung, in: Bäumler, H. (Hrsg.), Der neue Datenschutz, Berlin 1998, 11.
Idecke-Lux, S.	Der Einsatz von multimedialen Dokumenten bei der Genehmigung von neuen Anlagen nach dem Bundesimmissionsschutz-Gesetz, Baden-Baden 2000.
Jacob, J.	Perspektiven des neuen Datenschutzrechts, DuD 2000, 5.
Jacob, J.	Datenschutzkontrollen über die Grenzen hinweg, in: Bäumler, H. (Hrsg.), Der neue Datenschutz, Berlin 1998, 109.
Jessen, E.	Die Zukunft des Internet- und insbesondere der Wissenschaftsnetze, in: Kubicek, H../ Klumpp, D./ Fuchs, G. und Alexander R. (Hrsg.), Internet@Future, Jahrbuch Telekommunikation und Gesellschaft 2001, Heidelberg 2001, 11.
Kesdogan, D.	Privacy im Internet, Braunschweig, Wiesbaden 2000
Kilian, W.	Möglichkeiten und zivilrechtliche Probleme eines rechtswirksamen elektronischen Datenaustauschs, DuD 1993, 606.
Kilian, W./Wind, M.	Vernetzte Verwaltung und zwischenbehördliche Beziehungen, VerwArch 1997, 499.
Knack, H.-J.	Verwaltungsverfahrensgesetz, Kommentar, 6. Auflage, Köln [u.a.] 1998.
Konferenz der Datenschutzbeauftragten derLänder und des Bundes	Vom Bürgerbüro zum Internet, Hannover 2000.
Köhntopp, M./Köhntopp, K.	Datenspuren im Internet, CR 2000, 248.
Kopp, A.	Altautoentsorgung, NJW 1997, 3292.
Kubicek, H./ Hagen, M.	Internet und Multimedia in der öffentlichen Verwaltung, Bonn 1999.
Laux, E.	Probleme der Verwaltungsmodernisierung, in: Miller, M./Morlok, M./Windisch, R. (Hrsg.), Rechts- und Organisationsprobleme der Verwaltungs- Staats- und Verwaltungsmodernisierung, Berlin 1997, 48.
Lenk, K.	Ausserrechtliche Grundlagen für das Verwaltungsrecht in der Informationsgesellschaft: Zur Bedeutung von Information und Kommunikation in der Verwaltung, in: Hoffmann-Riem, W./Schmidt-Assmann, E. (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft Baden-Baden 2000, 59.

Lepper, U./Wilde, Ch.-P.	Unabhängigkeit der Datenschutzkontrolle zur Rechtslage im Bereich der Privatwirtschaft, CR 1997, 703.
Lohmann, J.	Schritte zur Modernisierung der Landesverwaltung, VM 2001, 68.
Lübking, U.	Datenschutz in der Kommunalverwaltung: Rechtsgrundlagen – Organisation - Datensicherung, Berlin 1992.
Mattern, F.	Ubiquitous Computing, in: Kubicek, H./Klumpp, D./Fuchs, G./Roßnagel, A. (Hrsg.), Internet@Future, Jahrbuch Telekommunikation und Gesellschaft 2001, Heidelberg 2001, 52.
Medert,, K./Süßmuth, W.	Pass- und Personalausweisrecht, Kommentar, Köln 1992.
Mutius, A.	Resümee der Sommerakademie 1995, DuD 1995, 666.
Möncke, U.	Data Warehouses- eine Herausforderung für den Datenschutz?, DuD 1998, 561.
Möller, Frank	Data Warehouse als Warnsignal an die Datenschutzbeauftragten, DuD 1998, 555.
Mummert+Partner Unternehmensberatung AG	Kommunale Vorhaben der Verwaltungsreform, Studie, Hamburg 2000.
Nedden, B.	E-Government- Innovationsbündnis für ein digitales Rathaus in Hannover; DuD 2001, 64.
Noam, E.	Digitaler Schwindel, http://www.politik-digital.de/netzpolitik/egovernment/effiz_staat.shtml, besucht Juli 2001.
Obermeyer, K.	Kommentar zum Verwaltungsvefahrensgesetz [VwVfG], 3.Auflage, Neuwied 1999.
Ockenfeld, M./Wetzel, E.	Grundlagen und Perspektiven der Multimedia-Techniken, CR 1993, 385
Ohnsorge, H.	Die Weiterentwicklung der Basistechnologien für die Telekommunikation, in: Kubicek, H./ Müller, G./ Neumann, K.-H./ Raubold, E./ Roßnagel, A. (Hrsg.), Multimedia- Technik sucht Anwendung, Jahrbuch Telekommunikation und Gesellschaft 1995, Heidelberg 1995, 19.
Opaschowski, H.	Datenschutz aus der Sicht des Nutzers, in: Kubicek/ H., Braczyk, H.-J./ Müller, G./ Neu, W./Raubold, E./ Roßnagel, A. (Hrsg.), Multimedia@Verwaltung, Jahrbuch Telekommunikation und Gesellschaft 1999, Heidelberg 1999, 184.
Opaschowski, H.	Quo vadis, Datenschutz?, DuD 1998 654.

Podlech, U.	Individualdatenschutz- Systemdatenschutz, in: Festgabe Grüner, H., Percha 1982, 451.
Pfitzmann, A.	Datenschutz durch Technik, DuD 1999, 405.
Pfitzmann, A.	Entwicklungen der Informations- und Kommunikationstechnik, DuD 2001, 194.
Provet/GMD (Hrsg.)	Die Simulationsstudie Rechtspflege - Eine neue Methode zur Technikgestaltung für Telekooperation, Darmstadt 1993.
Raunenberg, K.	Datenschutz als Innovationsmotor statt als Technikfeind in: Bäumler, H. (Hrsg.), Der neue Datenschutz, Berlin 1998, 190.
Reichard, C.	Staats- und Verwaltungsmodernisierung im „aktivierenden Staat“, VuF 1999, 117.
Reinermann, H.	Die vernetzte Verwaltung, Die Verwaltung 1995, 1.
Reinermann, H.	Der öffentliche Sektor im Internet, Speyer 2000.
Roßnagel, A.	Datenschutz in Sicherungsinfrastrukturen offener Telekooperation, DuD 1995, 582.
Roßnagel, A.	Datenschutz-Audit, DuD 1997, 505.
Roßnagel, A.	Globale Datennetze: Ohnmacht des Staates - Selbstschutz der Bürger, ZRP 1997, 26.
Roßnagel, A.	Neues Recht für Multimediadienste, NVwZ 1998, 1.
Roßnagel, A. (1999a)	Kommentar zum Recht der Multimedia-Dienste, München 1999.
Roßnagel, A.	Europäische Signatur-Richtlinie und Optionen ihrer Umsetzung, MMR 1999, 261.
Roßnagel, A. (1999b)	Die elektronische Signatur in der öffentlichen Verwaltung, in: Kubicek H./ Braczyk, H.-J./ Müller, G./ Neu, W./Raubold, E./ Roßnagel, A. (Hrsg.), Multimedia @Verwaltung, Jahrbuch Telekommunikation und Gesellschaft 1999, Heidelberg 1999, 158.
Roßnagel, A.	Recht der Multimediadienste 1998/1999, NVwZ 2000, 622.
Roßnagel, A. (2000a)	Datenschutzaudit, Braunschweig / Wiesbaden
Roßnagel, A. (2000b)	Möglichkeiten für Transparenz und Öffentlichkeit im Verwaltungshandeln – unter besonderer Berücksichtigung des Internet als Instrument der Staatskommunikation, in: Hoffmann-Riem, W./ Schmidt-Aßmann, E. (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000, 257.
Roßnagel, A.	Das neue Recht elektronischer Signaturen, NJW 2001, 1817.

Roßnagel, A.	Die elektronische Signatur im Verwaltungsrecht, DÖV 2001, 221.
Roßnagel, A.	Ansätze zur Modernisierung des Datenschutzrechts, in: Kubicek, H./Klumpp, D./Fuchs, G./Roßnagel, A. (Hrsg.), Internet@Future, Jahrbuch Telekommunikation und Gesellschaft 2001, Heidelberg 2001, 241.
Roßnagel, A.	Datenschutz in Signaturverfahren, in: *ders*. (Hrsg.), Handbuch des Datenschutzrechts, Kap. 7.7, München 2002, i.E.
Roßnagel, A./ Wedde P./ Hammer V./ Pordesch, U.	Digitalisierung der Grundrechte?, Opladen 1990.
Roßnagel, A./ Bizer, J.	Multimediadienste und Datenschutz, Gutachten im Auftrag der Akademie für Technikfolgenabschätzung in Baden-Württemberg, Stuttgart 1995.
Roßnagel, A./Schroeder, U. (Hrsg.)	Multimedia im immissionsschutzrechtlichen Genehmigungsverfahren, Köln 1999.
Roßnagel, A./Scholz, P.	Datenschutz durch Anonymität und Pseudonymität, MMR 2000, 721.
Roßnagel, A./Pfitzmann, A./ Garstka, H.-J.	Modernisierung des Datenschutzrechts, DuD 2001, 253.
Roßnagel, A./Pfitzmann, A./ Garstka, H.-J.	Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Heidelberg 2001.
Rürup, B.	Effizienzrevolution in der öffentlichen Verwaltung, VM 2000, 265.
Rüß, O.	Wahlen im Internet, MMR 2000, 73.
Schaar, P.	Persönlichkeitsprofile im Internet, DuD 2001, 383.
Schaar, P.	Datenschutzrechtliche Probleme von Online-Diensten, DuD 1996, 134.
Scholz, P.	Datenschutz in Telediensten, 2002, i.E.
Schweighofer, E.	Data Mining und Datenschutz, DuD 1997, 458.
Simitis, S.	Privatisierung und Datenschutz, DuD 1995, 648.
Simitis, S.	Die EU-Datenschutzrichtlinie- Stillstand oder Anreiz?, NJW 1997, 281.
Simitis, S.	Daten- oder Tatenschutz- ein Streit ohne Ende?, NJW 1997, 1902.
Tauss, J.	E-Vote: Die „elektronische Briefwahl“ als ein Beitrag zur Verbesserung der Partizipationsmöglichkeiten, in: Kubicek/ H., Braczyk, H.-J./ Müller, G./ Neu, W./Raubold, E./ Roßnagel, A. (Hrsg.), Multimedia@Verwaltung, Jahrbuch Telekommunikation und Gesellschaft 1999, Heidelberg 1999, 285.

Tauss, J./Özdemir, C.	Umfassende Modernisierung des Datenschutzrechts, in: Kubicek, H./Klumpp, D./Fuchs, G./Roßnagel, A. (Hrsg.), Internet@Future, Jahrbuch Telekommunikation und Gesellschaft 2001, Heidelberg 2001, 232.
Tinnefeld, M.-T./Ehmann, E.	Einführung in das Datenschutzrecht, 3. Auflage München 1998.
Ulrich, O.	Leitbildwechsel, DuD 1996, 664.
Weichert, T.	Datenschutzberatung - Hilfe zur Selbsthilfe, in: Bäumler, H. (Hrsg.), Der neue Datenschutz, Berlin 1998, 213.
Wienholtz, E.	Modernisierung der öffentlichen Verwaltung, DuD 1995, 642.
Wiese, M.	Unfreiwillige Spuren im Netz, in: Bäumler, H. (Hrsg.), E-Privacy, Braunschweig, Wiesbaden 2000, 9.
Zypries, B.	Zentraler Zugang, Kommune21 2001, 12.

Abkürzungsverzeichnis

A

a.A	andere Ansicht
Abs.	Absatz
AGB	Allgemeine Geschäftsbedingung
AllGO	Allgemeine Gebührenordnung
AöR	Archiv für öffentliches Recht (Zeitschrift)
Art.	Artikel

B

BauVorlVO	Bauvorlagenverordnung
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
BT-Drs.	Bundestags Drucksache
BVerGE	amtliche Sammlung der Entscheidungen des Bundesverfassungs-gerichts
BW	Baden-Württemberg

C

CR	Computer und Recht (Zeitschrift)

D

d.h.	das heißt
DASIT	Projekt: Datenschutz in Telediensten
ders.	derselbe
DÖV	Die öffentliche Verwaltung (Zeitschrift)
DSRL	Datenschutzrichtlinie
DStGB	Deutschen Städte- und Gemeindebundes
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt (Zeitschrift)

E

EG	Europäische Gemeinschaft
Einl.	Einleitung

F

ff.	folgende
Fn.	Fußnote

G

GG	Grundgesetz

H

Hrsg.	Herausgeber

I

i.E.	im Erscheinen
i.S.d.	im Sinne des
i.V.m.	in Verbindung mit
IT-Industrie	Information und Technologie
IP-Adressen	Internet Protocol
IuKDG	Informations- und Kommunikationsdienste-Gesetz

K

Kap.	Kapitel
K&R	Kommunikation und Recht

L

LDSG	Landesdatenschutzgesetz
LGebG	Landesgebührengesetz

M

m.w.N.	Mit weiteren Nachweisen
MDStV	Mediendienstestaatsvertrag
MeldDüVO	Meldedatenübermittlungsverordnung
MMR	Multimedia und Recht (Zeitschrift)
MRRG	Melderechtsrahmengesetz

N

Nds. AGPAuswG	Niedersächsisches Gesetz zur Ausstellung von Personalausweisen
NBauO	Niedersächsische Bauordnung
NDSG	Niedersächsisches Datenschutzgesetz
NJW	Neue Juristische Woche (Zeitschrift)
NMG	Niedersächsisches Meldegesetz
Nr.	Nummer
NVwKostG	Niedersächsisches Verwaltungskostengesetz
NVwZ	Neue Zeitschrift für Verwaltungsrecht

P

P3P	Plattform for Privacy Preferences
PassG	Passgesetz
PersAuswG	Personalausweisgesetz
Provet	Projektgruppe für verfassungsverträgliche Technikgestaltung

R

RDV	Recht der Datenverarbeitung
RiW	Recht internationaler Wirtschaft
RMD	Recht der Multimedia-Dienste, Kommentar zum Informations- und Kommunikationsdienste-Gesetz und Mediendienstestaats-vertrag, A. Roßnagel (Hrsg.)
Rn.	Randnummer

S

s.	siehe
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
sog.	sogenannte(r)

T

TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TDSV	Teledienstedatenschutzverordnung
TKG	Telekommunikationsgesetz

U

u.a.	unter anderem

V

VerwArch	Verwaltungsarchiv
Verw.	Die Verwaltung (Zeitschrift)
vgl.	vergleiche
VM	Verwaltung und Management
VuF	Verwaltung und Forum
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz

W

WWW	World Wide Wide

Z

Z.B.	Zum Beispiel
ZG	Zeitschrift für Gesetzgebung (Zeitschrift)
ZRP	Zeitschrift für Rechtspolitik (Zeitschrift)