Vom Bürgerbüro zum Internet

- Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung -

Die Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung wurden unter dem Vorsitz des Landes Nordrhein-Westfalen erarbeitet von

Brandenburg, Bayern, Bremen, Berlin, Hamburg, Hessen, Niedersachsen, Sachsen-Anhalt und Schleswig-Holstein.

Die redaktionelle Verantwortlichkeit liegt bei den Autorinnen und Autoren der einzelnen Beiträge.

zu 1. Berlin
zu 2. Hessen
zu 3. Bremen / Hamburg
zu 4. Niedersachsen
zu 5. Nordrhein-Westfalen
zu 6. Berlin
zu 7. Brandenburg
zu 8. Berlin

1 Einleitung

Die Modernisierung von Verwaltungsdienstleistungen ist eine Forderung, die seit vielen Jahren unter dem Stichwort „Verwaltungsreform" erhoben und inzwischen in der gesamten öffentlichen Verwaltung mehr oder weniger intensiv umgesetzt wird. Als Gründe werden z.B. genannt „zunehmende Bürokratie, Ohnmacht des Bürgers vor einer undurchschaubaren Verwaltungsapparatur, abnehmende Identifikation des Bürgers mit Verwaltungsentscheidungen" (von Mutius in: Stichwort „Verwaltungsreform" in: Verwaltungslexikon, Hg. von Eichhorn u.a., Baden-Baden 1985, S. 998). Eine wesentliche Reaktion auf diese Defizite ist die Bemühung, den Kontakt der Verwaltung mit den Bürgerinnen und Bürgern schneller und einfacher, aber auch transparenter zu machen.

Bereits in Zeiten, in denen sich die Nutzung der Elektronischen Datenverarbeitung auf wenige große Verwaltungsverfahren beschränkte, wurde in der Einrichtung von multifunktionalen Verwaltungsdienststellen ein Weg gesehen, diesen Zielen näherzukommen. Von der traditionellen kommunalen Verwaltungsgliederung abweichend, wurden Aufgabenbündelungen bei Stellen (Bürgerämter, Bürgerbüros o.ä.) propagiert, in denen an einem Ort Verwaltungsleistungen verschiedener Art entgegengenommen werden können. Mit zunehmender Technisierung der Verwaltung tritt das Bedürfnis hinzu, diese Stellen mit Informationstechnik auszustatten, insbesondere Zugriffe auf die verschiedensten Informationssysteme zu schaffen.

Es liegt auf der Hand, dass diese Entwicklung erhebliche datenschutzrechtliche Probleme aufwirft. Bereits die Bündelung verschiedener Aufgaben in einer Stelle steht im Konflikt mit der Forderung nach der Trennung von Datenbeständen, die unterschiedlichen Aufgaben zuzuordnen sind („informationelle Gewaltenteilung"). Dies wirkt sich insbesondere dann aus, wenn ein Teil der einbezogenen Aufgaben besonderen Geheimhaltungsvorschriften unterliegt (z.B. Sozial- oder Steuerverwaltung). Der Zugriff auf Informationssysteme, die unterschiedlichen Zwecken dienen, von einer Stelle aus verschärft die Risiken für das informationelle Selbstbestimmungsrecht.

Die 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Sitzung am 7. und 8. Oktober 1999 in Rostock deshalb den Beschluss gefasst, eine Arbeitsgruppe „Datenschutz in Bürgerbüros" zu konstituieren, „die sich auch mit der Modernisierung der Verwaltung allgemein und mit technischen Aspekten, wie der Verwendung der digitalen Signatur in der Verwaltung, befassen soll". Ziele sollten sein „die Analyse der Probleme und die Ausarbeitung von Vorschlägen für eine datenschutzgerechte Gestaltung der Bürgerbüros". Die Landesbeauftragte für den Datenschutz des Landes Nordrhein-Westfalen hat sich bereiterklärt, die Leitung der Arbeitsgruppe zu übernehmen, an der sich in der Folge auch die Länder Bayern, Berlin, Brandenburg, Hamburg, Hessen, Niedersachsen, Sachsen-Anhalt und Schleswig-Holstein beteiligten.

Erste Abstimmungen haben ergeben, dass es angesichts neuer Entwicklungen nicht sinnvoll ist, den Arbeitsauftrag auf Bürgerbüros zu beschränken. Vielmehr zeichnet sich zunehmend mehr der Wunsch ab, die Telekommunikation für Verwaltungsdienstleistungen zu nutzen, sei es in Form zentralisierter Telefondienstleistungen, sei es in Form der Nutzung des Internets („interaktive Verwaltung"). Sie ermöglicht ähnliche Effekte der Aufgabenbündelung, bietet jedoch im Hinblick auf zeitliche und räumliche Ressourcen erheblich Vorteile. Das „front office" wird in den persönlichen Lebensbereich der Bürgerinnen und Bürger verlagert, die Verwaltung selbst kann sich auf die „back office"-Funktionen konzentrieren. Hinzu kommen völlig neue Möglichkeiten etwa der Gewährleistung der Informationsfreiheit oder der anderweitigen Teilnahme am politischen Willensbildungsprozess.

Die Arbeitsgruppe war der Auffassung, dass der Begriff der „Serviceorientierung" alle diese Entwicklungen beschreibt und hat den Arbeitsauftrag entsprechend interpretiert. Das Arbeitsergebnis umfasst demzufolge die Datenschutzprobleme der „klassischen Bürgerbüros", der zentralisierten Nutzung von Telefondienstleistungen, der passiven und aktiven Nutzung des Internets einschließlich der für eine sichere Kommunikation erforderlichen Hilfsmittel bis hin zu elektronischer Auskunft, Akteneinsicht und Bürgerbeteiligung. Bei allen Aspekten spielt die Frage eine Rolle, wie die Auslagerung von Verwaltungsdienstleistungen einzuordnen ist; ein abschließender Teil behandelt daher die Fragen von Auftragsdatenverarbeitung und Funktionsübertragung unter besonderer Berücksichtigung des IuK-Rechts.

2 Multifunktionaler Service: Bürgeramt, Bürgerbüro, Bürgerladen und Kundencenter

2.1 Rechtliche Voraussetzung

Die Entwicklung zur serviceorientierten Verwaltung führt in immer mehr Städten und Gemeinden dazu, Aufgaben aus zentralen Fachämtern herauszunehmen und in dezentralen multifunktionalen Servicebüros (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) zu bündeln. Diese sollen den Bürgerinnen und Bürgern ermöglichen, verschiedene Behördengänge auf möglichst einen zu reduzieren. Außerdem kann das Recht, Anträge zur Niederschrift der Behörde zu stellen, aktualisiert werden. Multifunktional bedeutet dabei, dass möglichst viele Aufgaben an demselben Arbeitsplatz von ein und demselben Mitarbeiter erledigt werden sollen. Wenn dieses Ziel konsequent umgesetzt wird, bedeutet dies, dass einige wenige Mitarbeiter eines Bürgeramtes umfassende Informationen aus den verschiedensten Lebensbereichen einzelner Bürger erhalten. Die Verwaltung kann damit in Form des Bürgerbüros zu einer informationellen Einheit werden, und muss die vom Grundsatz der Zweckbindung gezogenen Grenzen überschreiten.

Die informationelle Einheit einer Stadtverwaltung wurde aus datenschutzrechtlicher Sicht aber bisher gerade verneint. Dies hat zur Folge, dass ein Datenaustausch („Datenübermittlung") zwischen verschiedenen Fachämtern nur unter den allgemeinen datenschutzrechtlichen Vorgaben wie Erforderlichkeit und Zweckbindung der Datenverarbeitung zulässig ist.

Folgende Organisationsformen von Bürgerämtern sind zum Teil realisiert oder werden geplant:

Informationszentrum mit Service-Angeboten

Informationsangebote in Verbindung mit Service-Leistungen, die keinen Datenschutzbezug haben, da es sich um Informationsangebote der Kommunen handelt: Verkauf von Eintrittskarten, Buskarten, Tarifinformationen der Stadtwerke, Grundstücksangebote für Wohn- und Gewerbebanken, kommunale Förderprogramme für Gewerbeansiedlung, Wasserbewirtschaftung, Solarenergie etc., Bereithalten von Antragsformularen.

Meldebehörde mit Service-Angeboten

Klassische Meldebehörde mit Service-Leistungen, insbesondere Antragsannahme und Weiterleitung zur sachlichen Bearbeitung an ein entsprechendes Fachamt sowie Ausgabe der bearbeiteten Anträge, Ausweise und Auskünfte.

Multifunktionales Bürgeramt

Multifunktionales Bürgeramt mit weiteren Aufgaben wie etwa KFZ-Zulassung, Gewerbeanzeigenannahme, Gewerbeauskunft, Hundesteuer, Grundsteuer,

Rundfunkgebührenbefreiung zur Endbearbeitung im Bürgerbüro bei einem Mitarbeiter.

Soweit in landesrechtlichen Bestimmungen eine Öffnungsklausel besteht, die eine Übertragung von Aufgaben auf die Kommunen zulässt, schafft diese Öffnung z.B. die Möglichkeit, die KFZ-Zulassung in den Kommunen durchzuführen; gerade diese Aufgabe wird auch in den Bürgerämtern erfüllt. Eine solche Öffnungsklausel schafft aber theoretisch auch die Möglichkeit, so sensible Bereiche wie Ausländerangelegenheiten und Sozialwesen auf die Kommunen zu übertragen. Eine Verlagerung auf Bürgerämter erscheint insofern problematisch, da eine zusätzliche Streuung sensibler Daten eintritt.

zu den einzelnen Service-Modellen:

Die als Informationszentrum ausgestattete Bürgeramtslösung ist datenschutzrechtlich völlig unproblematisch, wenn die räumlich – organisatorischen Maßnahmen angemessen sind (dazu unten).

Die Meldebehörde mit Service-Angeboten mit gebündelten Bearbeitungszuständigkeiten ist datenschutzrechtlich ebenfalls unproblematisch, soweit sie das Angebot beinhaltet, einen internen Beratungs- und Postdienst zu übernehmen, aber insgesamt das Fachamt für die Erledigung der Aufgabe zuständig bleibt. Damit haben die Bürgerinnen und Bürger weiterhin die Möglichkeit ohnehin direkt das Fachamt zu konsultieren.

Soll das Bürgeramt hingegen über die Meldeangelegenheiten hinaus auch bestimmte andere Aufgaben abschießend bearbeiten, ergeben sich aus dieser Aufgabenbündelung auch neue datenschutzrechtliche Anforderungen.

Datenschutzrechtlich problematisch wird es, wenn das Dienstleistungsangebot des Bürgeramtes Aufgaben einbezieht, bei denen die Verarbeitung von Daten, die besonderen Geheimhaltungsvorschriften unterliegen, erforderlich wird. Dies ist einmal bei der Verarbeitung von Steuerdaten, vor allem aber von Sozialdaten oder ähnlich sensiblen Daten der Fall (Grundsteuer, Rundfunkgebührenbefreiung, Sozialleistungen).

Im Vordergrund bei der Schaffung von Bürgerbüros steht aus kommunaler Sicht der Servicegewinn für die Bürgerinnen und Bürger. Die Datenschutzbeauftragten wollen die Verbesserung des Services keinesfalls behindern; sie haben allerdings dafür Sorge zu tragen, dass die Verbesserung des Serviceangebots nicht zu einer Gefährdung des Rechts auf informationelle Selbstbestimmung führt. So ist insbesondere darauf zu achten, dass eine Annahme des Angebotes für die Betroffenen freiwillig bleibt, d.h. dass sie jederzeit die Wahl haben ohne Nachteile befürchten zu müssen, das Angebot abzulehnen bzw. davon wieder Abstand zu nehmen. Auch darf für die Betroffenen aus der Annahme des Angebotes keine Verpflichtung erwachsen personenbezogene Daten gegenüber der Service-Stelle zu offenbaren. Eine exakte Vorgabe, welche kommunalen Aufgaben in einem Bürgerbüro zusammengeführt und organisiert werden können, kann den Datenschutzbeauftragten schon deshalb nicht gegeben werden, weil gerade

wegen der unterschiedlichen Größe von Kommunen, die Gegebenheiten höchst unterschiedlich ausfallen. Das Bedürfnis in einer kleinen Kommune mehr Aufgaben an einer Stelle zu bündeln, als in einer großen Kommune ist nicht zu leugnen.

Gleichwohl gibt es sensible Sachgebiete – wie etwa Sozialhilfe, Wohngeld, Steuerangelegenheiten - deren Abwicklung in einem Bürgerbüro durch ein und denselben Sachbearbeiter datenschutzrechtlich problematisch erscheinen mag. Deshalb sollte grundsätzlich empfohlen werden, diese Bereiche aus einem Bürgeramt auszugliedern.

Sollten sensiblere Bereiche dennoch in ein Bürgerbüro integriert werden, müssen hier verschärft folgende Anforderungen erfüllt werden:

- die Serviceleistungen des Bürgeramtes sind lediglich als Angebot zu verstehen
- es besteht keinerlei Verpflichtung für den Antragsteller, persönliche Daten aus diesen Zusammenhängen im Bürgeramt zu offenbaren (Einwilligung der Betroffenen)
- Anträge müssen nach wie vor in einem Fachamt gestellt werden können und müssen dort zweckgebunden bearbeitet werden
- Der Zugriff auf Daten des Fachamtes durch das Bürgeramt muss von der Einwilligung des Antragstellers abhängig gemacht werden; eine Speicherung der Daten außerhalb des Fachamtes muss unterbleiben (Vermeidung doppelter Datenspeicherung)

Grundsätzlich gilt: Je mehr Verwaltungsleistungen an einem Ort gebündelt werden, desto größer wird die Gefahr, dass Mitarbeiterinnen und Mitarbeiter in Bürgerbüros umfassend auf Daten aus verschiedenen Lebensbereichen der Bürgerinnen und Bürger Zugriff haben. Insofern bedarf es klarer gesetzlicher Regelungen, zumindest aber klarer Dienstanweisungen zum Umgang mit personenbezogenen Daten. Es sollte überlegt werden, dass bei umfassender Zuständigkeit eines Bürgeramtes für verschiedene Aufgaben wenigstens die Zuständigkeiten unter den Mitarbeitern aufgeteilt werden können und damit eine Einschränkung der Zugriffsbefugnisse in den EDV-Systemen möglich wird. Diese Zugriffsbeschränkungen dürften nur dann durchbrochen werden, wenn die Bürger sich damit ausdrücklich einverstanden erklären. Im übrigen muss durch Aufzeichnung von Zugriffslegitimationen sichergestellt sein, dass überprüft werden kann, ob und durch wen eine Zusammenführung von Daten vorgenommen wurde. Die Mitarbeiter sind besonders zur Geheimhaltung bekannt gewordener Lebensdaten zu verpflichten.

2.2 Räumliche Rahmenbedingungen:

Unabhängig davon, welche Aufgaben gebündelt werden, sind an die räumliche Gestaltung von Bürgerämtern besondere Anforderungen zu stellen. Bürgerbüros sind typischerweise Großraumbüros. Die Erfahrungen bei Überprüfungen haben gezeigt, dass es hier kaum möglich ist, ein vertrauliches Gespräch zu führen, da die einzelnen Arbeitsplätze häufig so nah beieinander stehen, dass mühelos Gespräche an den benachbarten Arbeitsplätzen mitgehört werden können. Es ist deshalb stets zu fordern, dass in Bürgerbüros den Bürgerinnen und Bürgern angeboten wird, dass jedes Gespräch auch unter vier Augen in einem separaten Raum geführt werden kann, dass Stellwände vorgesehen werden, dass Bildschirme uneinsehbar sind und dass Abstandsflächen ausreichend bemessen werden.

2.3 Fazit:

- Je nachdem für welches Service-Modell sich eine Kommune entscheidet, müssen die datenschutzrechtlichen Anforderungen in unterschiedlicher Intensität beachtet werden.

- Sachgebiete in denen regelmäßig sensible Daten anfallen, sollten nicht in einer Service-Stelle abgewickelt werden. Es sei denn, durch geeignete Maßnahmen kann der Schutz der personenbezogenen Daten gewährleistet werden.

- Die Annahme des Service-Angebotes außerhalb der Fachämter darf nur freiwillig sein

- Die Betroffenen sind nicht verpflichtet personenbezogene Daten außerhalb des Fachamtes zu offenbaren

- Die Mitarbeiterinnen und Mitarbeiter müssen im Vorfeld der Einrichtung des Bürgerbüros im Hinblick auf die besonderen auch datenschutzrechtlichen Anforderungen sorgfältig geschult werden.

- Die Einwohnerinnen und Einwohner müssen durch Informationsmaßnahmen über die Zuständigkeiten des Bürgeramtes und der Fachämter sowie über die Arbeitsabläufe unterrichtet werden. Sie müssen auf ihre Wahlmöglichkeit zwischen Fachamt und Bürgeramt aufmerksam gemacht werden.

- In Kommunen, die Bürgerämter einrichten, sollte die Stellung des behördlichen Datenschutzbeauftragten gestärkt werden; eine Beteiligung des behördlichen Datenschutzbeauftragten bereits bei der Einrichtung wird dringend angeraten.

3 Call-Center

3.1 Call-Center in der privaten Wirtschaft

Immer mehr Unternehmen bieten ihren Kunden ihre Dienste rund um die Uhr über das Telefon an, um ihren Kundenservice zu erhöhen. Dabei spricht der Anrufer oder die Anruferin häufig gar nicht mehr direkt mit dem Unternehmen, sondern mit einem externen Call-Center, das als selbständiger Auftragsdienst und selbstständiger Betrieb die telefonische Kundenbetreuung von einer oder auch mehreren Firmen komplett übernimmt. Dies betrifft Bereiche wie z.B. Service- und Bestellhotlines, die Responseannahme nach Anzeigen und TV-Spots oder auch die Vertriebsunterstützung.

Zwischen dem Call-Center und dem Auftraggeber besteht ein Vertragsverhältnis, das im einzelnen den Umfang der übertragenen Aufgaben, die Verpflichtung zur Wahrung von Betriebsgeheimnissen und des Datengeheimnisses bestimmt und die Speicherung, Übermittlung und Nutzung von Daten festlegt (siehe auch Kapitel 8.1). Call-Center haben in der Regel einen vertraglich definierten Zugriff auf die Datenbank des Auftraggebers mit der Möglichkeit, die Kundenwünsche online zu speichern, oder es werden die Daten in dem DV-System des Call-Centers zwischengespeichert und an den Auftraggeber entsprechend der vertraglichen Vereinbarungen weitergeleitet. In aller Regel erfährt der Kunde nichts davon, dass er mit einem Call-Center verbunden ist.

3.2 Kommunales Call-Center

Zunehmend nutzen Kommunen den Einsatz eines Call-Centers. Ausgelöst wurde diese Entwicklung durch die Diskussion über eine verstärkte Kundenorientierung der Verwaltung. Danach soll es kein Traum mehr sein, bei einem Anruf bei einer Behörde auf eine freundliche Telefonstimme zu stoßen, die hilfsbereit und stets erreichbar ist und die Fragen möglichst gebührenfrei unter einer 0800-Nummer beantwortet. Solche Fragen lauten häufig: Wer ist zuständig? Wie sind die Öffnungszeiten? Welche Dokumente muss ich mit zur Behörde bringen? Für die datenschutzrechtliche Betrachtung eines derartigen Serviceangebots kommt es darauf an, ob das Call-Center keine personenbezogenen Angaben der Anrufer und Anruferinnen benötigt oder ob die Verarbeitung personenbezogener Daten für die Dienstleistung erforderlich ist.

3.3 Ohne Verarbeitung personenbezogener Daten

In folgenden Beispielsfällen werden üblicherweise keine personenbezogenen Daten benötigt:

- Umfrage zur allgemeinen Zufriedenheit der Bürger oder zur Auswirkung konkreter Verwaltungsmaßnahmen, wie der Neugestaltung einer Straße.

- Entgegennahme von Anregungen, Wünschen und Hinweisen, wie das Aufstellen von Blumenkübeln, Beseitigung von Straßenschäden oder Nennung von verschmutzten Haltstellen.

- Beratung und Auskunft zu Öffnungszeiten, zur Erreichbarkeit von Mitarbeitern (Telefonnummer, Adresse, Zimmernummer) und zur Zuständigkeit.

- Einfache rechtliche Auskünfte (welche Unterlagen werden benötigt, welche Fristen sind zu beachten, wo finde ich die Rechtsvorschrift oder wie ist der Lauf des Antrags).

In all diesen Fällen, in denen keine personenbezogenen Daten erhoben und verarbeitet werden, können datenschutzrechtliche Bedenken gegen den Einsatz eines Call-Centers nicht geltend gemacht werden. Zu beachten ist dabei, dass auch Verbindungsdaten, wie z.B. die Rufnummernanzeige, nicht gespeichert werden dürfen.

3.4 Mit Verarbeitung personenbezogener Daten

Die öffentliche Verwaltung will aber einen weitergehenden Service anbieten, der ohne die Verarbeitung personenbezogener Daten nicht auskommt: So wird beispielsweise bei der Anforderung der Sperrmüllabfuhr zumindest der Name und die Adresse des Anrufers oder der Anruferin benötigt, bei einer denkbaren telefonischen Erläuterung eines Abwassergebührenbescheides müssten weitere Daten, wie z.B. das Buchungszeichen, genannt werden. Antragsformulare für verschiedene Verwaltungsleistungen können nur zugesandt werden, wenn der Bürger oder die Bürgerin Name und Adresse preisgibt. Falls eine Auskunft gewünscht wird, in welchem Bearbeitungsstadium sich gerade ein Antrag bei einer Behörde befindet, kann das erforderliche Datenvolumen, das genannt werden muss, weiter anwachsen.

Der Einsatz eines Call-Centers ist auch dann nicht grundsätzlich datenschutzrechtlich bedenklich, wenn personenbezogene Daten erhoben und verarbeitet werden. Allerdings muss vorher genau untersucht werden, welche personenbezogenen Daten dabei im einzelnen anfallen und welche Schutzvorkehrungen gegen eine missbräuchliche Verwendung getroffen werden müssen.

Handelt es sich um relativ unsensible Angaben, beispielsweise den Namen und die Adresse zur Vereinbarung eines Termins für die Sperrmüllabfuhr, reichen einfache Regelungen zur Datensicherheit aus. Hierunter fällt die Festlegung der Zweckbindung der Daten, deren Weiterleitung an das DV-System der Verwaltung, deren interne Nutzung für die Statistik und für Abrechnungszwecke sowie deren Löschung.

Höhere Schutzvorkehrungen verlangen die Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnis beeinträchtigen kann. Solche Daten können zum Beispiel im Rahmen

des Beschwerdemanagements anfallen. Deshalb muss in einem Datenschutzkonzept festgelegt werden, wie mit zentral und dezentral eingehenden Beschwerden umzugehen ist, an wen sie weiterzuleiten sind, welche personenbezogenen Daten (Anrufer, Mitarbeiter der Behörde, sonstige Dritte) gespeichert, weiter verarbeitet oder genutzt werden dürfen sowie zu welchem Zeitpunkt sie anonymisiert oder gelöscht werden müssen. Auch Auskünfte aus dem Melderegister könnten zukünftig, sofern die melderechtlichen Rahmenbedingungen entsprechend angepasst sind, über ein Call-Center (Stichwort „Bezahl-Telephonie") abgewickelt werden. Die dabei anfallenden Daten erfordern ebenfalls einen höheren Schutzstandard und die Erarbeitung eines Datenschutzkonzeptes. Dies gilt auch für die Fälle, in denen ein Call-Center Auskünfte über den Stand eines Verwaltungsverfahrens geben soll. Konkret gedacht werden kann an einen vereinbarten Code oder an einen Rückruf an eine bekannte Telefonnummer.

Die Erhebung und Verarbeitung personenbezogener Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen kann bzw. die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, ist grundsätzlich nicht einem Call-Center zu übertragen. Dazu gehören insbesondere Angaben, die sich auf gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen sowie arbeitsrechtliche, steuerliche oder soziale Rechtsverhältnisse beziehen. Grund hierfür ist, dass nach dem heutigen Stand der Technik zumindest die Vertraulichkeit und die Identität beim Einsatz der Telephonie nicht hinreichend sichergestellt werden kann.

3.5 Datenschutzvorkehrungen

Voraussetzungen für einen wirksamen Datenschutz sind:

- Transparenz
  Dem Bürger muss in jedem Fall eröffnet werden, dass er Kontakt mit einem Call-Center hat und nicht mit der Behörde.

- Alternative
  Es muss dem Bürger die Wahl bleiben, bei der Behörde direkt anzurufen oder dort vorzusprechen.

- Informiertheit
  Der Bürger muss darüber informiert werden, welche Daten über ihn bei dem Kontakt mit dem Call-Center verarbeitet werden und dass er seine datenschutzrechtlichen Betroffenen-rechte, wie z.B. auf Auskunft über die gespeicherten Daten, gegenüber der auftraggebenden Behörde geltend machen kann.

- Freiwilligkeit
  Wenn Daten über den Betroffenen nur mit seiner Einwilligung erhoben werden dürfen, ist er auf die Freiwilligkeit besonders hinzuweisen.

- Widerrufbarkeit
  Bis zum Abschluss des Kontaktes mit dem Call-Center muss der Bürger die Möglichkeit haben, den Kontakt abzubrechen und sein Anliegen direkt bei der zuständigen Stelle vorzutragen. Die bereits angefallenen Daten müssen unverzüglich gelöscht werden.

- Datenschutzvorkehrungen
  Im Vertragsverhältnis sind hinreichend die Festlegungen nach § 11 BDSG und die technischen und organisatorischen Maßnahmen nach § 9 BDSG oder den jeweiligen Landesdatenschutzgesetzen zu treffen sowie die Mitarbeiter des Call-Centers auf die Einhaltung des Datengeheimnisses zu verpflichten.

4 Informationsangebote öffentlicher Stellen im Internet

4.1 Inhaltsebene und Tele-/Mediendienste

Bei der Bereitstellung von Informationsangeboten öffentlicher Stellen im Internet und deren Nutzung werden auf vielfältige Weise personenbezogene Daten verarbeitet. Je nach Art bzw. Zweck der Verarbeitung sind unterschiedliche Regelungen zu beachten. Man unterscheidet

- Dienstedaten,
  - Bestandsdaten,
  - Nutzungsdaten,
  - Abrechnungsdaten,
- Inhaltsdaten.

Die Datenarten werden in der nachstehenden Tabelle näher erläutert. Bei Bestands-, Nutzungs- und Abrechnungsdaten handelt es sich überwiegend um Daten der Nutzer, die von der öffentlichen Stelle oder einem von ihr beauftragten Mediendienste- oder Telediensteanbieter verarbeitet werden, um ein entsprechendes Internet-Angebot zu realisieren. Bei der Bereitstellung von reinen Informationsangeboten fallen neben den Inhaltsdaten insbesondere Nutzungsdaten an. Auf die datenschutzrechtliche Regelungen zur Verarbeitung dieser Daten wird in Kap. 4.3 eingegangen.

Datenart		**Beschreibung**	**Beispiele**	**Rechtsgrundlage**
Dienstedaten	Bestandsdaten	Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich sind.	Name, Anschrift der Nutzer, statische IP-Nummer, Kontonummer, Kreditkarten-Nummer	TDDSG, MDStV
	Nutzungsdaten	Nutzerdaten, die für die Inanspruchnahme von Diensten erforderlich sind.	Name oder IP-Adresse des anfragenden Clients, Username, Anfrage und deren Status	TDDSG, MDStV
	Abrechnungsdaten	Nutzerdaten für die Abrechnung von Diensten	Zeitpunkt und Dauer von Verbindungen, Datenvolumen	TDG, TDDSG, MDStV
Inhaltsdaten		In den Internet-Angeboten zum Abruf bereitgestellte Informationen	Zeichen Bilder, Töne	Landesdatenschutzgesetze, BDSG,

			Fachgesetze

Inhaltsdaten sind die eigentlichen Informationen, die von der öffentlichen Stelle zum Abruf bereit gestellt werden. Die Zulässigkeit der Verarbeitung von Inhaltsdaten wird in Kap. 4.2 behandelt.

4.2 Inhaltsdaten: Was darf ins Internet?

Die Bereitstellung von personenbezogenen (Inhalts-)Daten im Internet hat sich in vielen Fällen nach bereichsspezifischen Regelungen zu richten (z.B. Sozialgesetzbuch, Meldegesetze). Fehlen solche Regelungen, so sind die jeweiligen Landesdatenschutzgesetze und bei Stellen des Bundes das Bundesdatenschutzgesetz einschlägig. Soweit die Bereitstellung von Daten im Internet ohne Einschränkungen erfolgt, also keine geschlossene Benutzergruppe durch z.B. ein Passwortverfahren gebildet wird, besteht weltweit die Möglichkeit zu einem Abruf. Da es Staaten gibt, in denen keine oder sehr schwach ausgeprägte Datenschutzbestimmungen existieren, können die schutzwürdigen Belange von Betroffenen durch die Einstellung ins Netz in besonderem Umfang beeinträchtig sein. Ein Bereithalten personenbezogener Daten im Internet ist daher nur zulässig, wenn die betroffenen Personen

- eingewilligt oder
- dies aufgrund einer Rechtsvorschrift hinzunehmen haben.

Einwilligung

Die Merkmale einer wirksamen Einwilligung sind:

- **Freiwilligkeit**
  Eine wirksame Einwilligung liegt nur vor, wenn diese freiwillig erteilt worden ist.

- **Informiertheit**
  Voraussetzung jeder Einwilligung ist, dass die Betroffenen umfassend über die Verarbeitung (Verwendungszweck, Beteiligte/Empfänger, Form der Verarbeitung, Anonymisierung) unterrichtet werden. Die Betroffenen sind darüber zu unterrichten, dass aus der Verweigerung einer Einwilligung keine Nachteile entstehen.

- **Schriftlichkeit**
  Von der Schriftform kann nur abgewichen werden, wenn wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben. Die neuen Datenschutzgesetze sehen auch eine elektronische Form der Einwilligung vor.

- **Widerrufbarkeit**

Die Betroffenen sind darauf hinzuweisen, dass sie die Einwilligung verweigern oder in Zukunft widerrufen können.

Auch bei einer Verarbeitung mit Einwilligung sind die sonstigen Datenschutzvorkehrungen zu beachten.

Unabhängig hiervon ist der Grundsatz der Datenvermeidung zu beachten. Auch wenn die Verarbeitung von personenbezogenen Daten im Internet zulässig ist, sind alternative anonyme oder pseudonyme Verfahren zu wählen, wenn der Zweck der Verarbeitung so in gleicher Weise erreicht werden kann.

Diese allgemeinen Aussagen zur Zulässigkeit der Bereitstellung werden im Folgenden in einzelnen Teilbereichen verifiziert.

Bedienstetendaten

In Bund und Ländern ist die Verarbeitung von Bedienstetendaten der öffentlichen Stellen bereichsspezifisch geregelt (Sondervorschriften in den Datenschutzgesetzen, Beamtengesetze der Länder). Danach ist eine Übermittlung der Daten von Beschäftigten an Personen oder Stellen außerhalb des öffentlichen Bereichs nur zulässig, wenn der Dienstverkehr es erfordert oder die Betroffenen eingewilligt haben. Eine Veröffentlichung von Bedienstetendaten im Internet ist demnach zulässig, wenn der Dienstverkehr eine solche Veröffentlichung erfordert.

Diese Voraussetzungen sind in der Regel erfüllt für die Bekanntgabe des Namens, der dienstlichen Telefon- und Faxnummer, der E-Mail-Adresse und eines Hinweises auf den Aufgabenbereich von Bediensteten, die aufgrund ihres Aufgabenbereichs mit privaten oder anderen Dritten regelmäßig in Kontakt stehen, oder von herausgehobenen Funktionsträgern. Für Bedienstete, die in der Regel keinen unmittelbaren dienstlichen Kontakt mit Bürgerinnen und Bürgern haben (z.B. Angehörige interner Dienste wie des Schreib- oder Botendienstes), gilt dies nicht. Ob in diesem Zusammenhang eine Übermittlung von Vornamen und Amtsbezeichnung erforderlich ist, wird unterschiedlich beurteilt. In Zweifelsfällen sollte eine Einwilligung eingeholt werden oder auf eine Veröffentlichung ganz verzichtet werden. In Betracht kommt auch eine Regelung durch Abschluss einer Dienstvereinbarung. Auf jeden Fall müssen die Bediensteten in geeigneter Form vor der Bereitstellung der Daten im Internet informiert werden.

Weitere Daten über Beschäftigte mit Außenkontakten, wie private Telefonnummer, Fotos usw., dürfen nur mit Einwilligung der Betroffenen in Internet-Angeboten bereitgehalten werden. Die Bereitstellung von vollständigen Geschäftsverteilungsplänen oder Telefonverzeichnissen ist in aller Regel nicht erforderlich und damit ohne Einwilligung oder Dienstvereinbarung unzulässig.

Bürgerdaten

Grundsätzlich rechtlich zulässig ist die Bereitstellung von Informationen, die ohnehin rechtmäßig veröffentlicht sind oder werden dürfen. Hierzu gehören u.a.

- Publikationen der Presse,
- Tagesordnungen, Referenten, u.U. Gremienmitglieder öffentlicher Veranstaltungen,
- amtliche Bekanntmachungen.

Dabei ist allerdings zu beachten, dass auf diese Weise ein weltweiter Zugriff möglich ist und die bereitgestellten Daten automatisiert recherchierbar sind. Vor der Entscheidung einer Veröffentlichung im Internet sollten daher mögliche negative Konsequenzen für die Betroffenen untersucht und berücksichtigt werden. Bereits bestehende Widerspruchsrechte sind zu beachten. Außerdem sollten die Möglichkeiten zur Reduzierung der Recherchierbarkeit in geeigneter Weise genutzt werden (siehe Kasten).

Dürfen die Bürgerdaten nicht veröffentlicht werden, ist die Einwilligung der Betroffenen Voraussetzung für eine Bereitstellung im Internet. Dabei sollten pseudonyme Verfahren gewählt werden, wenn dies möglich und sinnvoll ist. Auch beim Vorliegen einer Einwilligung sollten die Möglichkeiten zur Einschränkung der Recherchierbarkeit in geeigneter Weise genutzt werden.

Einschränkung der Recherchierbarkeit von Webseiten

Der automatisierten Recherchierbarkeit von Webseiten kann begegnet werden, wenn die Daten nur über Downloads oder geeignete Datenbankabfragen übermittelt werden. Eingeschränkt gilt dies auch für Webseiten, die beim Zugriff aus Datenbankinhalten automatisch erstellt werden ("dynamisch generierte Webseiten"). Sie können zwar prinzipiell von Suchmaschinen indiziert werden; die meisten Anbieter von Suchmaschinen verzichten aber hierauf, weil so zu viele Fehleintragungen entstehen würden. Es besteht auch die Möglichkeit, durch die Aufnahme von geeigneten Metainformationen in das Internet-Angebot die automatische Recherche durch Suchmaschinen einzuschränken. So werden z.B. durch den html-Befehl

<META NAME="robots" CONTENT="noindex">

Suchmaschinen angewiesen, den Seiteninhalt nicht zu indizieren. Allerdings hängt es von der Gestaltung der jeweiligen Suchmaschine ab, ob diese Befehle unterstützt werden oder nicht.

Webcams

Es wird immer häufiger üblich, Kameras in öffentlichen und privaten Bereichen aufzustellen und deren Bilder im Internet abrufbar zu speichern. Öffentliche Stellen dürfen dies allenfalls dann tun, wenn die Kameras so aufgestellt sind, dass die anfallenden Bilder keine Daten mit Personenbezug enthalten. Ein Personenbezug ist auf jeden Fall herstellbar, wenn Gesichter, Autokennzeichen oder andere identifizierende Merkmale erkennbar sind oder durch Aufnahmesteuerung oder Bildbearbeitung seitens des Empfängers erkennbar gemacht werden können. In Frage kommen daher allenfalls Übersichtsaufnahmen, die die Herstellung eines Personenbezuges definitiv ausschließen. Dabei spielen Rahmenbedingungen wie Bildausschnitt, Bildschärfe oder Bildfrequenz eine wichtige Rolle.

Es sollte auch beachtet werden, dass die erwarteten Informationen oft auf andere, datensparsamere Weise übermittelt werden können. Z.B. können Informationen über die Verkehrslage in Schriftform ("Stau im Bereich...") oder über markierte Stadtpläne oft wirkungsvoller, schneller und völlig ohne personenbezogene Daten über das Internet weitergegeben werden.

4.3 Nutzungsdaten: Was darf wie verarbeitet werden?

Internet-Angebote öffentlicher Stellen sind entweder Teledienste, die im Teledienstegesetz (TDG) und im Teledienstedatenschutzgesetz (TDDSG) geregelt sind, oder Mediendienste, für die der Mediendienste-Staatsvertrag (MDStV) gilt. **Teledienste** sind 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. § 2 Abs. 2 TDG nennt einige Beispiele, wie etwa Telebanking, Datenaustausch, Datendienste (z. B. über Verkehrs- oder Wetterdaten), Angebote zur Nutzung des Internets oder weiterer Netze, Angebote zur Nutzung von Telespielen und Angebote von Waren- und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit. Zu den **Mediendiensten** gehören die an die **Allgemeinheit** gerichteten Informations- und Kommunikationsdienste wie z.B. Fernseheinkauf, Verbreitung von Messergebnissen in Text und Bild, Fernsehtext und vergleichbare Textdienste.

Da die Datenschutzregelungen für Tele- und Mediendienste in TDG/TDDSG und MDStV weitgehend identisch sind, kann die schwierige Unterscheidung zwischen Telediensten und Mediendiensten bei Internetangeboten öffentlicher Stellen in der Regel dahingestellt bleiben. Öffentliche Stellen haben folgende Anforderungen zu erfüllen:

- Nutzungsdaten sind frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen (soweit es sich nicht um Abrechnungsdaten handelt; § 6 Abs. 2 TDDSG bzw. § 15 Abs. 2 MDStV).

- Der Anbieter darf die Erbringung von Diensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung und Nutzung seiner Daten für andere Zwecke abhängig machen (§ 3 Abs. 3 TDDSG bzw. 12 Abs. 4 MDStV).

- Die Prinzipien der Datenvermeidung und der Datensparsamkeit sind zu beachten (§ 3 Abs. 4 TDDSG bzw. §12 Abs. 5 MDStV).

- Der Anbieter hat dem Nutzer die Inanspruchnahme von Diensten anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren (§ 4 Abs. 1 TDDSG bzw. § 13 Abs. 1 MDStV).

- Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig (§ 4 Abs. 4 TDDSG bzw. § 13 Abs. 4 MDStV).

Speicherung von Nutzungsdaten

Selbst wenn ein Nutzer im Internet keine Daten über seine Identität von sich aus offenbart (Ausfüllen von Formularen, E-Mail-Adressen usw.), fallen beim Anbieter Daten über den Nutzer an. Dazu gehören die IP-Adressen, über die der Datenaustausch vollzogen wird.

IP-Adresse

Die IP-Adresse (IP = Internet-Protokoll) ist die eindeutige Adresse eines Rechners im weltweiten Internet. Man schreibt sie meist als vier durch Punkte von einander getrennte Zahlen zwischen 0 und 255. Da Bezeichnungen leichter zu merken sind als Zahlen, sind den IP-Adressen sog. Domain-Namen zugeordnet. Die Zuordnung wird im Domain Name System (DNS) über bestimmte DNS-Server aufgelöst.

Während die Internet-Server feste IP-Adressen haben, gilt dies für die Rechner der meisten Nutzer nicht. Vielmehr erhält der Nutzer von seinem Access-Provider für die jeweilige Internet-Session eine IP-Adresse dynamisch zugeteilt. Es besteht die Gefahr, dass dynamische IP-Adressen außer vom Access-Provider auch von Außenstehenden (mit großem Aufwand) einem bestimmten Nutzer zugeordnet werden.

Es gibt außerdem Rechner, die über fest vergebene IP-Adressen verfügen. Dies können Rechner von Universitäten oder Firmen sein, die einen großen Bereich von IP-Adressen erworben haben, oder auch private Nutzer, die sehr früh im Internet präsent waren. In diesen Fällen lässt sich die IP-Adresse häufig auch ohne weitere Hilfsmittel einem bestimmten Nutzer zuordnen; sie ist deshalb als ein personenbezogenes Datum anzusehen. Allerdings ist nicht erkennbar, ob eine IP-Adresse statisch oder dynamisch ist. Öffentliche Stellen müssen darauf achten, dass vollständige IP-Nummern bei der Nutzung ihrer Informationsangebote nicht

dauerhaft protokolliert werden. Dies kann zum einen durch einen vollständigen Verzicht auf Protokollierungen erfolgen. Eine andere Möglichkeit besteht darin, nur die ersten drei Nummern der IP-Adresse zu speichern. Auch ist es denkbar, schon während der Verbindung den Besuch des Internetangebots durch Zuordnung zu einer größeren Nutzergruppe zu erfassen, um so eine gewünschte, anonyme Statistik zu erhalten.

Cookies

Die Verwendung von Cookies stellt einen Eingriff in die Datenverarbeitung auf dem persönlichen Rechner des Nutzers dar. Für den Nutzer ist in den meisten Fällen allenfalls die Tatsache einer Speicherung, nicht aber unmittelbar dessen Inhalt und Bedeutung erkennbar.

Cookies

Cookies sind kleine Dateneinheiten, die von Internet-Servern auf den Rechnern der Nutzer gespeichert werden. In den Cookies können Aktivitäten des Nutzers festgehalten werden. Cookies können zur Verbindungssteuerung während einer Sitzung ("Session Cookies") verwendet werden. In diesem Fall werden sie bei Beendigung der Sitzung wieder gelöscht. Häufig werden Cookies aber über viele Jahre gespeichert, um dem Anbieter beim nächsten Zugriff eine "bedarfsgerechte" Angebotsauswahl oder die Führung von Statistiken über das Nutzerverhalten zu ermöglichen bzw. Nutzerprofile zu bilden.

Die Verwendung von Cookies unterliegt dem TDDSG oder dem MDStV, wenn die Cookies bestimmten Personen zugeordnet werden können. Eine Zuordnung ist dann möglich, wenn - wie oben beschrieben - Nutzer statische IP-Adressen verwenden oder ihren Namen in Transaktionen preisgeben. In diesen Fällen ist die Verwendung von Cookies nur mit Einwilligung des Nutzers zulässig, wenn sie über das Sitzungsende hinaus gespeichert werden sollen. Dabei ist zu beachten, dass bei einer Preisgabe des Namens auch früher gesetzte Cookies zugeordnet werden können.

Wegen der damit verbundenen Risiken sollten öffentliche Stellen in ihren Informationsangeboten auf das Setzen von Cookies möglichst vollständig verzichten, soweit diese nicht zur Gestaltung des Angebots als sog. „Session Cookies" eingesetzt werden.

Active-X, Java, JavaScript, Plug-Ins

Active-X-Controls, Java-Applets und JavaScripts sind Programme, die beim Aufrufen von Angeboten auf den Rechner des Nutzers heruntergeladen und dort zur Ausführung gebracht werden. Eine Gefahr geht insbesondere von Programm-

Einheiten aus, die unter Ausnutzung von Sicherheitslücken Funktionen mit schädlichen Eigenschaften beinhalten. Diesen Gefahren kann der Nutzer durch Deaktivierung der Ausführbarkeit der Programme begegnen. Anbieter sollten daher damit rechnen, dass Nutzer beispielsweise Active-X-Controls, Java-Applets oder Plug-Ins (im Nutzerbrowser installierte Zusatztools) nicht ausführen können. Dies gilt insbesondere für Active X-Programme, von denen im Allgemeinen die weitreichendsten Gefährdungen für Internet-Nutzer ausgehen. Die Informationsangebote sollten dementsprechend ohne solche Programme gestaltet werden.

4.4 Gestaltung des Angebots

Datenschutzhinweise

§ 12 Abs. 6 MDStV und § 3 Abs. 5 TDDSG legen fest, dass der Nutzer vor einer Erhebung personenbezogener Daten über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten zu unterrichten ist. Diese Regelung lässt sich in vielen Fällen umsetzen, wenn im Informationsangebot der öffentlichen Stellen Datenschutzhinweise gegeben werden. Sie sollten immer dann veröffentlicht werden, wenn personenbezogene Daten online über die Web-Site gesammelt werden. Dies ist dann der Fall, wenn z.B. eine Online-Registrierung verlangt bzw. ermöglicht wird, wenn sonstige Formulare online ausgefüllt werden können oder wenn mittels E-Mail mit der öffentlichen Stelle kommuniziert werden kann. Auch wenn dies nicht der Fall ist, sollten entsprechende Datenschutzhinweise gegeben werden.
Die Datenschutzhinweise von Informationsangeboten sollten eine Erklärung zu Grundsätzen und Verfahrensweisen bei der Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten enthalten, die im Zusammenhang mit der Bereitstellung und Nutzung eines Informationsangebotes im Internet auftreten.

Beispiel für Datenschutzhinweise

Mit Ihrem Zugriff auf diese Web-Site werden Ihre um die letzte Zahl verkürzte IP-Adresse und weitere Angaben (Datum, Uhrzeit, betrachtete Seite) auf unserem Server für Zwecke der Datensicherheit für zwei Monate gespeichert. Die Daten werden außerdem für statistische Zwecke ausgewertet. Durch die Verkürzung der IP-Adresse ist ein Bezug der gespeicherten Daten auf Ihre Person ausgeschlossen.

Wir verwenden keine Cookies, Java-Applets oder Active-X-Controls.

Sollten Sie noch Fragen zum Datenschutz haben, so wenden Sie sich bitte an:
Name: ... E-Mail-Adresse: ... Telefon: ...

Darüber hinaus steht Ihnen auch der Landes/Bundesbeauftragte für den Datenschutz als Ansprechpartner zur Verfügung.

Web-Site: ... E-Mail-Adresse: ... Telefon: ...

Wenn Sie eine E-Mail mit schutzwürdigem Inhalt an uns senden wollen, so empfehlen wir dringend, diese zu verschlüsseln, um eine unbefugte Kenntnisnahme und Verfälschung auf dem Übertragungsweg zu verhindern. Unseren öffentlichen Schlüssel finden Sie unter ... unseres Informationsangebots.

Die Hinweise sollten an zentraler Stelle erfolgen, z.B. direkt auf der Begrüßungsseite oder durch einen Link über eine aussagekräftige Schaltfläche. Hier sollte erläutert werden, ob und inwiefern IP-Adressen für statistische Zwecke verarbeitet werden. Auch sollte darauf hingewiesen werden, ob Cookies verwendet werden. Soweit dies zutrifft, sollte dies begründet und über die Auswirkungen informiert werden. Wenn dies nicht der Fall ist, sollte hierauf hingewiesen werden, weil damit eventuell vorhandene Bedenken und Befürchtungen der Besucher zerstreut werden können.

Anbieterkennzeichnung, Impressum

Sowohl das Teledienstegesetz als auch der Mediendienstestaatsvertrag sehen eine Anbieterkennzeichnung vor (§ 6 TDG, § 6 MDStV). Diese muss Name und Anschrift, bei Personenvereinigungen und -gruppen auch Name und Anschrift des Vertretungsberechtigten enthalten. Die Anbieterkennzeichnung schafft auch aus Datenschutzsicht Transparenz und sollte dementsprechend zentral und vollständig in das Internet-Angebot eingestellt werden. Das Impressum sollte von jeder Webseite aus erreichbar sein.

Dienstanbieter sollten auch deutlich herausstellen, wenn ein Link des Angebots zu einer Seite führt, die nicht mehr im eigenen Verantwortungsbereich liegt (§ 4 Abs. 3 TDDSG, § 13 Abs. 3 MDStV).

Vorschlag für ein Impressum

Stadt <Name>
Verantwortlich: <Name>
<Straße>
<PLZ/Ort>
Telefon: <Telefonnummer>
Telefax: <Telefaxnummer>
E-Mail: <E-Mail-Adresse>

Hinweis zu externen Links

Die Stadt <Name> ist als Inhalteanbieter (Content provider) nach § 5 Abs.1 des Teledienstegesetzes (TDG) bzw. § 5 Mediendienstestaatsvertrag (MDStV) für die "eigenen Inhalte", die sie zur Nutzung bereithält, verantwortlich. Von diesen eigenen Inhalten sind Querverweise ("Links") auf die von anderen Anbietern bereitgehaltenen Inhalte zu unterscheiden. Durch Querverweise hält die Stadt <Name> "fremde Inhalte" zur Nutzung bereit, die durch den Hinweis

[LINK]

gekennzeichnet sind. Die Stadt <Name> hat bei der erstmaligen Verknüpfung die fremden Inhalte gesichtet. Bei Links handelt es sich allerdings stets um "lebende" (dynamische) Verweisungen; die fremden Inhalte können deshalb geändert worden sein, ohne dass die Stadt <Name> hiervon Kenntnis hat.

4.5 Technische Absicherung

Der Anschluss an das Internet ist mit erheblichen Gefährdungen der Datensicherheit und des Datenschutzes verbunden. Die Rechner und Übertragungswege dieses weltweiten Computernetzes sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht transparent. Denn das Internet wurde ursprünglich nur unter Verfügbarkeitsaspekten entwickelt – auch wenn neuere Entwicklungen versuchen, weiteren Sicherheitsbedürfnissen Rechnung zu tragen. Deshalb wird den Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit vielfach nicht in der gebotenen Weise begegnet. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen, manipulieren und zerstören. Dies ist besonders gravierend, weil angesichts von ca. 200 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Dieses Risiko ist bei den Informationsangeboten öffentlicher Stellen zu berücksichtigen. Die meisten Gefahren können durch eine geeignete Platzierung des Web-Servers beseitigt werden. Server sollten sich auf jeden Fall außerhalb der lokalen Netze der öffentlichen Stelle befinden. Dies kann durch eine Insellösung realisiert werden, bei der die Daten über das Internet oder durch direkte Eingabe gepflegt werden. Um einen Zugriff aus den lokalen Netzen in das Internet sowie eine Online-Pflege des Web-Servers zu ermöglichen und dennoch die lokalen Netze zu schützen, ist der Einsatz einer Firewall zwischen lokalen Netzen und Web-Server erforderlich. Zusätzlich muss der Web-Server selbst gegen Manipulationen aus dem Internet geschützt werden. Solche Sicherheitsvorgaben lassen sich durch den Aufbau einer doppelten Firewall erreichen, wobei der Web-

Server zwischen diesen in der sogenannten demilitarisierten Zone steht (siehe Abbildung).

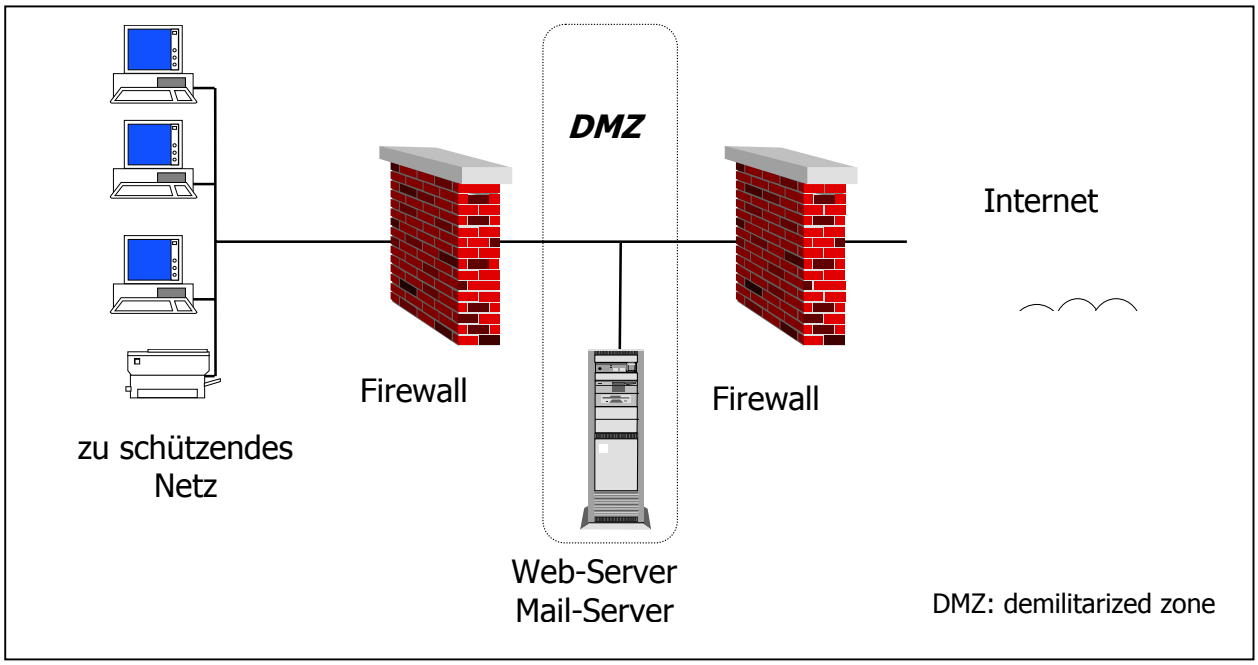
Dabei sollte auf Folgendes geachtet werden:

- Die Anschaffung eines Firewallsystems allein schafft noch keine ausreichende Sicherheit. Die Firewall muss in geeigneter Weise konfiguriert werden. Außerdem müssen die Verantwortlichen für die System- und Netztechnik die Internet-Systeme regelmäßig überprüfen. Auch ist organisatorisch sicher zu stellen, dass auf neue Risiken und bekannt werdende Sicherheitslücken sofort mit den geeigneten Maßnahmen reagiert wird.

- Der direkte Zugriff auf Datenbanken der öffentliche Stelle im LAN sollte nicht zugelassen werden. Soweit ein Datenbankzugriff erforderlich ist, sollten Kopien in Rechnern der entmilitarisierten Zone verwendet werden.

- Das Internet-Angebot ist durch geeignete Maßnahmen gegen unbefugte Manipulationen zu sichern. Hierzu gehören eine sichere Konfiguration der Rechteverwaltung und eine geeignete Protokollierung unerlaubter Zugriffe auf dem Webserver sowie eine geeignete Einstellung der äußeren Firewall.

- Besonderes Augenmerk ist auf die personenbezogenen Daten zu richten, die durch die Nutzung entstehen. Sie müssen gegen den Zugriff über das Internet geschützt werden und sollten nur kurzfristig im Web-Server gespeichert sein.



Unabhängig hiervon muss den Risiken begegnet werden, denen eigene Mitarbeiter bei der Nutzung des Internets ausgesetzt sind. Zusätzlich zur Firewall müssen z.B. Maßnahmen gegen Computerviren, schädliche ActiveX- und Java-Programme oder Plug-Ins, fehlerhafte Bedienung usw. getroffen werden.

Weitere Informationen zum Thema Datenschutz und Internet können z.B. den Orientierungshilfen der Datenschutzbeauftragten des Bundes und der Länder entnommen werden (Orientierungshilfe Internet des AK Technik der LfD-Konferenz unter www.datenschutz.de, Orientierungshilfen und Selbstschutz unter www.lfd. niedersachsen.de u.a.).

5 Interaktive Verwaltung

Im Zusammenhang mit den Informationsangeboten öffentlicher Stellen im Internet (unter 4.) wurden bereits grundlegende Vorgaben für die Gestaltung des Internetauftrittes angesprochen. Wollen die Verwaltungen auch eine interaktive Kommunikation mit den Bürgerinnen und Bürgern im Internet anbieten, sind darüber hinaus weitere Gesichtspunkte bei der Gestaltung des Angebotes zu berücksichtigen:

- Welche Verwaltungsvorgänge können über das Internet abgewickelt werden?
- Wie ist die internetbasierte Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung in das Datenschutzrecht einzuordnen?
- Müssen die Verwaltungen Verschlüsselungsverfahren anbieten?
- Ist der Einsatz von Signierverfahren erforderlich?
- Welche technischen und organisatorischen Maßnahmen sind für die Ausgestaltung des Verfahrens denkbar?

5.1 Welche Verwaltungsvorgänge können über das Internet abgewickelt werden?

Die Service-Orientierung der Verwaltung bedingt ein hohes Maß an Organisationsfreiheit der Verwaltung in der Ausgestaltung der Kommunikation mit den Bürgerinnen und Bürgern. Gerade auch Kommunen haben seit jeher auf ihre Organisationshoheit verwiesen, deren Grenzen lediglich in den bestehenden gesetzlichen Bestimmungen liegen dürften. Das bedeutet, dass öffentliche Stellen - wenn nicht etwas anderes ausdrücklich festgelegt ist - ein Verwaltungsverfahren so durchführen können, wie sie es für zweckmäßig halten. Das schließt auch die Wahl des Kommunikationsmediums ein. Wie internetbasierte Kommunikation mit der Verwaltung künftig aussehen könnte, zeigen folgende Beispiele:

Die elektronische Bestellung, den Sperrmüll abzuholen

Frau A möchte, dass ihr Sperrmüll abgeholt wird. Sie setzt sich an ihren Rechner, wählt die WWW-Adresse ihrer Gemeinde aus und ruft das entsprechende Formular auf der Homepage auf. Bevor sie das Dokument

absenden kann, wird mit SSL (Secure Socket Layer) ein „sicherer Kanal" aufgebaut, der von dem PC der Frau A bis zum Server der Kommune reicht. Der Aufbau erfolgt ohne weiteres Zutun von Frau A. Sie erhält lediglich den Browser-Hinweis, dass sie im Begriff ist, Daten über eine sichere Verbindung zu versenden und dass Dritte Informationen, die mit dieser Seite ausgetauscht werden, nicht sehen können. Sie weiß damit, dass ihre Daten geschützt übertragen werden, füllt das Formular mit den entsprechenden Angaben (Name und Anschrift) aus und sendet es ab. Auf dem gleichen Weg erhält sie auch die Mitteilung über den Abholtag.

Die elektronische Anmeldung zum Volkshochschulkurs

Frau A möchte einen Volkshochschulkurs besuchen. Sie informiert sich auf der Homepage der Volkshochschule über die Angebote und entscheidet sich dort für den Kurs: „Aggressivität und aggressive Kinder - ein Wochenende für Betroffene". Auf der Homepage befindet sich der Hinweis, dass sie die Anmeldung auch online durchführen kann, wenn sie die erforderlichen Angaben per E-mail übersendet. Da die Kommune ausdrücklich darauf hinweist, dass unverschlüsselte E-mails auf ihrem Weg durch das Internet viele Stationen durchlaufen und unbemerkt gelesen oder verändert werden können, will sie das Angebot wahrnehmen, die E-mail verschlüsselt zu übersenden. Hierzu installiert sie die erforderliche Software auf ihrem PC, lädt den öffentlichen Schlüssel der Kommune von der Homepage und überprüft ihn über den „Fingerprint". Anschließend verschlüsselt sie ihre Angaben mit dem heruntergeladenen Schlüssel und sendet sie an die Kommune. Diese kann die E-mail entschlüsseln und die Anmeldung entsprechend weiter leiten. Auf dem gleichen Weg - verschlüsselt - erhält sie auch die Anmeldebestätigung und die Rechnung.

Da gesetzliche Vorgaben, die die Wahl des Kommunikationsmediums einschränken, weder für die elektronische Bestellung der Sperrgutabfuhr noch für die Anmeldung zu einem Volkshochschulkurs bestehen, wäre in diesen Beispielsfällen eine internetbasierte Kommunikation zulässig.

Dagegen lässt sich eine ebenso eindeutige Aussage für einen anderen Beispielsfall - die Wohnsitzanmeldung - nicht treffen.

Die elektronische Wohnsitzanmeldung

Frau A ist umgezogen und möchte auf elektronischem Weg ihren Wohnsitz ummelden. Zu diesem Zweck ruft sie das elektronische Formular der entsprechenden Internetseite ihrer Kommune auf und gibt ihre Daten ein. Sie signiert das Meldeformular mit ihrem Signaturschlüssel und verschlüsselt das Dokument. Das Formular wird von den zuständigen Mitarbeiterinnen und Mit

arbeitern geöffnet und mit einem elektronischen Eingangsstempel versehen. Eine Bestätigung ihrer Anmeldung wird ihr übersandt.

Das Melderechtsrahmengesetz enthält keine Aussage dazu, wie die Meldepflicht konkret zu erfüllen ist. Regeln finden sich aber in den Meldegesetzen der Länder, die vorschreiben, dass die Meldepflichtigen einen Meldeschein auszufüllen, zu unterschreiben und bei der Meldebehörde abzugeben haben. Darüber hinaus sind - in der Regel durch Rechtsverordnung - Form und Inhalt des Meldescheins detailliert festgelegt. Zwar kann in den meisten Bundesländern vom Ausfüllen des Meldescheins abgesehen werden, falls das Melderegister automatisiert geführt wird. Dies gilt aber überwiegend nur dann, wenn die meldepflichtige Person bei der Behörde erscheint, um die erforderlichen Angaben zu machen. In einigen Ländern wird zusätzlich verlangt, dass die oder der Meldepflichtige die Richtigkeit und Vollständigkeit der Daten durch Unterschrift bestätigt. Ob dort, wo das Gesetz solche weitergehende Anforderungen stellt, internetbasierte Kommunikationsformen der Bürgerinnen und Bürger mit der Verwaltung rechtlich zulässig sind, lässt sich bislang nicht eindeutig beantworten.

Schriftliches Handeln setzt auch im Verwaltungs- bzw. Verwaltungsprozessrecht grundsätzlich eine eigenhändige Unterschrift auf einem Papierdokument voraus (vgl. m. w. N. BVerwGE 81, 32 (33)). Bezüglich der von der Verwaltung einzuhaltenden Formvorschriften gibt es gesetzliche Ausnahmen. So kann etwa beim Erlass eines schriftlichen Verwaltungsaktes, der mit Hilfe automatischer Einrichtungen erlassen wird, die Unterschrift fehlen, § 37 Abs. 4 Satz 1 VwVfG (daneben wird die Übermittlung eines Verwaltungsaktes durch E-mail allerdings mit dem Problem des Nachweises der Bekanntgabe bzw. des Zugangs zu kämpfen haben, wovon wiederum die Wirksamkeit desselben abhängt).

> Im Bereich der Kommunikation der Bürgerinnen und Bürger mit ihrer Verwaltung wäre es denkbar, unter Berufung auf die Rechtsprechung des Bundesverwaltungsgerichts im Zusammenhang mit dem Schriftformerfordernis (vgl. etwa BVerwGE 30, 274 ff.; 81, 32 ff.) weitere Ausnahmen zuzulassen.

Das Bundesverwaltungsgericht hat schon in der Vergangenheit zugunsten der Bürgerinnen und Bürger Ausnahmen vom eigenhändig unterschriebenen Dokument etwa bei der Klageerhebung (vgl. BVerwGE 81, 32 (38 ff.)) oder der Erhebung des Widerspruchs (vgl. BVerwGE 30, 274 (277 ff.)) zugelassen, wenn sich aus anderen Anhaltspunkten eine der Unterschrift vergleichbare Gewähr für die Urheberschaft und den Rechtsbindungswillen feststellen ließ. Fortentwickelt wird diese Auffassung, die maßgeblich auf die Rechtssicherheit und Verlässlichkeit als alleinige Zwecke der Schriftform abstellt, auch durch einen Beschluss des gemeinsamen Senates der obersten Gerichtshöfe des Bundes (Az.: GmS-OGB 1/98, NJW 2000, 2340 f.) vom 05.04.2000. Darin wird der technischen Entwicklung Rechnung getragen und ein Computerfax mit eingescannter Unterschrift als ausreichend angesehen. Es dürfte nicht mehr lange dauern bis auch die E-mail akzeptiert wird. Eine entsprechende Entschließung verbunden mit der Aufforderung an die Bundes

regierung, die elektronische Abwicklung von Verwaltungsdienstleistungen auch im Bereich der durch Bundesrecht vorgeschriebenen Formerfordernisse zuzulassen, hat der Bundesrat in seiner Sitzung am 09.06.00 bereits angenommen (BR-Drs. 231/00; Beschluss). Zeitdruck wird außerdem durch das Europarecht erzeugt, da die Richtlinie 1999/93 EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (Abl. EG L 13 vom 19.01.2000, Seite 12 ff.) bis zum 19.07.2001 in nationales Recht umzusetzen ist. Sie sieht in Art. 5 Abs. 1 a vor, dass die dort näher umschriebene digitale Signatur der eigenhändigen Unterschrift gleichzustellen ist. Gleichwohl sollte in den Beeichen, in denen eine eigenhändige Unterschrift für erforderlich gehalten wird, auf eine kostenintensive Projektierung internetbasierter Kommunikationsformen vorerst verzichtet werden.

Bis zur Klärung der rechtlichen Situation empfiehlt sich folgende Vorgehensweise: Wird die eigenhändige Unterschrift für erforderlich gehalten, so ist sie nachträglich einzuholen. Ergibt sich auf andere Weise eine der Unterschrift vergleichbare Gewähr für die Urheberschaft und den Rechtsbindungswillen, ist im Einzelfall zu entscheiden, ob ausnahmsweise auf die Unterschrift verzichtet werden kann. Gegebenenfalls ist dann jedoch immer auf die noch nicht eindeutig geklärte rechtliche Situation hinzuweisen.

5.2 Wie ist die internetbasierte Kommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung in das Datenschutzrecht einzuordnen?

Internetbasierte Kommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung lässt sich datenschutzrechtlich auf zwei Ebenen unterscheiden:

- Auf der Inhaltsebene sind die Vorgaben für die einzelnen Gegenstandsbereiche zu beachten, die spezialgesetzlich normiert oder den allgemeinen Datenschutzgesetzen zu entnehmen sind.

- Auf der Diensteebene gibt es Vorgaben für das Angebot von Informations- und Kommunikationsdiensten, die Pflichten speziell für die Diensteanbieterinnen enthalten.

Mit der Bestellung über das Internet hat Frau A in dem Beispielsfall 1 ihren Namen und ihre Adresse in das Formular eingegeben. Diese Angaben sind erforderlich, damit das Sperrgut abtransportiert werden kann. Die eingegebenen Daten unterliegen nicht der Diensteebene, weil sie unabhängig von der Art der Kommunikation sind. Sie gehören zur Inhaltsebene. So könnte Frau A die Sperrmüllabfuhr mit denselben Angaben schriftlich, durch einen Gang aufs Amt oder telefonisch anfordern. Genauso verhält es sich mit der Anmeldung zum Volkshochschulkurs. Auch hier sind die in der E-mail versandten Daten (Name, Adresse, Kursart etc.) der Inhaltsebene zuzuordnen. Für die Zulässigkeit der Erhebung der personenbezogenen Inhaltsdaten gilt nichts anderes als auf dem Medium Papier. Fehlt es z. B. schon an der Erforderlichkeit der Angaben, dürfen sie nicht verarbeitet werden.

Die für die Diensteebene maßgebenden rechtlichen Regelungen, nämlich der Mediendienstestaatsvertrag (MStV) und das Teledienstedatenschutzgesetz (TDDSG), enthalten Anforderungen, die erfüllt werden müssen, wenn die Kommunikation auf elektronischem Wege über das Internet geführt werden soll. Für die bei der Individualkommunikation zwischen den Bürgerinnen und Bürgern und der Verwaltung unabhängig von der Inhaltsebene anfallenden personenbezogenen Daten ist das Teledienstedatenschutzgesetz einschlägig. Nach § 6 Abs. 1 Nr. 1 TDDSG darf die Diensteanbieterin personenbezogene Daten über die Inanspruchnahme von Telediensten nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um den Nutzerinnen und Nutzern die Inanspruchnahme von Telediensten zu ermöglichen. Die IP-Nummer, die Aufschluss darüber geben kann, welche Rechner miteinander kommunizieren, stellt ein solches Nutzungsdatum im Sinne des Teledienstedatenschutzgesetzes dar, weil es sich hierbei um ein für den Verbindungsaufbau benötigtes Datum handelt. Die zunächst zulässig gespeicherten Nutzungsdaten sind aber frühestmöglich, spätestens nach dem Ende der jeweiligen Nutzung zu löschen (§ 6 Abs. 2 Nr. 1 TDDSG).

Bei der E-mail Kommunikation ist grundsätzlich zwischen dem Transport im Internet über die E-mail-Server und dem Empfang bzw. Versand über die Endgeräte zu unterscheiden. Im Folgenden soll lediglich auf die rechtlichen Vorgaben eingegangen werden, die die Verwaltungen beim Empfang bzw. Absenden einer E-mail-Nachricht zu beachten haben. In diesem Fall sind die Verwaltungen nicht Adressatinnen der Befugnisse und Pflichten aus dem Teledienstedatenschutzgesetz. Das in § 3 Abs. 1 TDDSG niedergelegte Verbot mit Erlaubnisvorbehalt personenbezogene Daten zu verarbeiten richtet sich an die Diensteanbieterinnen („vom Diensteanbieter"). Die Empfängerinnen und Empfänger einer E-Mail sind nicht Anbieterinnen und Anbieter des Informations- und Kommunikationsdienstes E-mail im Sinne des § 2 Nr. 1 TDDSG, da sie den Teledienst nicht zur Nutzung bereithalten, sondern selber Nutzerinnen und Nutzer des Dienstes sind. Als Diensteanbieterin kommt hier allenfalls die Betreiberin einer Mailbox in Betracht. Das kann im Einzellfall auch eine Kommune sein. Die Zulässigkeit der Speicherung der im Zusammenhang mit der E-mail-Kommunikation entstandenen Datensätze richtet sich daher auch für die über den Inhalt einer E-mail-Nachricht hinausgehenden Informationen nach den datenschutzrechtlichen Vorgaben auf der Inhaltsebene. Das bedeutet, dass personenbezogene Daten, wie etwa die Absenderadresse, das Sendedatum oder weitere Sendeinformationen zu löschen sind, wenn ihre Speicherung zur Erfüllung der jeweiligen Aufgabe nicht oder nicht mehr erforderlich ist.

Nutzungsdaten - wie etwa die IP-Nummer - sind spätestens nach dem Ende der jeweiligen Nutzung zu löschen. Auch andere Daten - wie etwa Routinginformationen - müssen gelöscht werden, wenn diese Daten nicht oder nicht mehr zu Erfüllung der jeweiligen Aufgabe der öffentlichen Stelle erforderlich sind.

5.3 Müssen die Verwaltungen Verschlüsselungsverfahren anbieten?

Anders als bei der Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem Informations- und Kommunikationsdienst E-mail sind die Verwaltungen aber Diensteanbieterinnen, wenn sie die Bürgerinnen und Bürger zu einer internetbasierten Kommunikation etwa im Rahmen einer Homepage einladen. Nach § 4 Abs. 2 Nr. 3 TDDSG hat die Diensteanbieterin durch technische und organisatorische Vorkehrungen sicherzustellen, dass Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch genommen werden können. Für die Nutzerinnen und Nutzer muss also die Möglichkeit - nicht die Verpflichtung - bestehen, sich durch technische Maßnahmen gegen unbefugte Kenntnisnahme und Verfälschung zu schützen (Schaar / Schulz in: Roßnagel, Recht der Multimediadienste, Stand: Januar 2000, Rdnr. 91 ff. zu § 4 TDDSG).

Die abstrakte Verpflichtung nach § 4 Abs. 2 Nr. 3 TDDSG regelt allerdings nicht, welcher Art die Anforderungen an die Verfahren zur Gewährleistung vertraulicher Kommunikation zu sein haben. Praktisch bedeutet das jedoch, dass die Verwaltungen Verschlüsselungsverfahren anzubieten haben. Das gilt unabhängig vom Inhalt für alle drei Beispielsfälle. Ein Warnhinweis kann zwar der nach § 3 Abs. 5 TDDSG erforderlichen Unterrichtung Rechnung tragen, vielleicht auch Grundlage einer Einwilligung sein. Einen wirksamen Schutz, wie er als technische oder organisatorische Maßnahme von den Diensteanbieterinnen nach dem Teledienstedatenschutzgesetz gefordert ist, stellt der Warnhinweis aber nicht dar, weil er keine vor der Kenntnisnahme Dritter geschützte Kommunikation sicherstellen kann.

Die Auswahl des konkreten Verschlüsselungsverfahrens richtet sich nach den allgemeinen Datenschutzgrundsätzen. Danach hat die Verwaltung diejenigen Verschlüsselungsverfahren anzubieten oder zu verwenden, die erforderlich sind, um die Vertraulichkeit zu gewährleisten. Vorschläge hierzu enthält die Tabelle unter Kap.5.5.

> Es gilt der Grundsatz, dass die Nutzerinnen und Nutzer Informations- und Kommunikationsdienste vor der Kenntnisnahme Dritter geschützt, z. B. durch angemessen sichere Verschlüsselung, in Anspruch nehmen können müssen. Ein bloßer Warnhinweis auf die Risiken unverschlüsselter Kommunikation im Netz reicht nicht aus.

5.4 Ist der Einsatz von Signierverfahren erforderlich?

Zum Schutz von Authentizität und Integrität ist der Einsatz von Signierverfahren zu empfehlen. Nach § 10 Abs. 2 Nr. 2 und 4 Datenschutzgesetz Nordrhein-Westfalen sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell (Integrität) bleiben und jederzeit ihrem Ursprung zugeordnet werden können (Authentizität). Eine technische Maßnahme zur Umsetzung dieser Verpflich

tung kann der Einsatz von Signierverfahren sein. Ob sich die Erforderlichkeit eines Einsatzes von Signierverfahren auch aus einer Zusammenschau verschiedener Gebote technischer und organisatorischer Maßnahmen, etwa der Zugriffs-, Übermittlungs-, Benutzer- oder der Transportkontrolle ergeben könnte, wird unterschiedlich beurteilt. Vorschläge für eine technische Umsetzung enthält die Tabelle unter 5.

Manchmal erweist sich die Verwendung von Signierverfahren auch aus anderen Erwägungen als sinnvoll. Die Signatur eines Dokumentes als obligatorische Voraussetzung für eine elektronische Bestellung der Sperrgutabfuhr kann notwendig sein, um die Identität der Betroffenen zweifelsfrei sicherzustellen und einer Verbreitung unrichtiger Daten über die Betroffenen, wie etwa bei scherzhaften Massenbestellungen unter einem falschen Namen vorzubeugen. Zwar ist dies auch derzeit per Telefon möglich. Die unsichere Identifizierung der anrufenden Person ist jedoch auch der angerufenen Person bekannt. Demgegenüber lässt sich im Internet der tausendfache Versand einer E-mail unter einer Schein-Identität mit wenigen Mausclicks initiieren!

5.5 Welche technischen und organisatorischen Maßnahmen sind für die Ausgestaltung des Verfahrens denkbar?

Die nachfolgende Tabelle soll einer ersten Orientierung über den Umfang der erforderlichen technischen und organisatorischen Maßnahmen dienen. Sie weist auf den Zusammenhang hin, der je nach der konkreten Datenverarbeitungssituation im aktuellen Verwendungszusammenhang entsprechend der unterschiedlichen Sensitivität der Daten unterschiedliche technische und organisatorische Maßnahmen fordert.

Die Anwendung der Tabelle darf nicht schematisch erfolgen. Die Einordnung der einzelnen Daten hängt entscheidend von dem Sachzusammenhang ab, in dem diese Daten verarbeitet werden. Wegen der Kontextabhängigkeit der Sensitivität von Daten müssen besondere Risiken individuell berücksichtigt werden. Sind die Daten eines Datensatzes unterschiedlichen Stufen zuzuordnen, so sind jeweils für den genannten Datensatz die Anforderungen der höchsten Stufe für das einzelne Datum zu wählen. Ebenso wenig darf die Tabelle genutzt werden, um sich der Verpflichtung zu entziehen, ein ausreichendes Sicherheitskonzept zu erstellen.

Die öffentlichen Stellen haben zu gewährleisten, dass – verglichen mit konventionellen Formen des Austausches von Informationen – durch die neuen Kommunikationswege nicht zusätzliche Beeinträchtigungen des Grundrechts auf Datenschutz eintreten können.

Kategorien pb. Daten	Technische und organisatorische Maßnahmen	Technische Umsetzung
Kategorie 1: Personenbezogene Daten oder Verwendungszusammenhänge, die wegen ihrer Sensitivität in dem konkreten Datenverarbeitungszusammenhang einen besonderen Datenschutz erfahren müssen. Dieses Schutzniveau ist i. d. R. insbesondere bei Berufs- und Amtsgeheimnissen (z. B. Sozialdaten) und bei personenbezogenen Daten, die nach Art. 8 der EG-Datenschutzrichtlinie als besondere Kategorie eingestuft worden sind (z. B. Daten über die Gesundheit) zu fordern. Ferner personenbezogene Daten oder Verwendungszusammenhänge, deren Missbrauch zu einer Beeinträchtigung von weiteren Grundrechten oder in der Folge zu sonstigen besonders schwerwiegenden Nachteilen führen kann.	Es ist sicher zu stellen, dass nur Befugte die personenbezogenen Daten zur Kenntnis nehmen können (Wahrung der Vertraulichkeit). Erforderlich sind außerdem Maßnahmen, die geeignet sind, dass personenbezogene Daten während der Verarbeitung unversehrt und vollständig bleiben (Integrität) sowie jederzeit ihrem Ursprung zugeordnet werden können (Authentizität).	Die Kommunikationspartnerinnen und Kommunikationspartner müssen eine hinreichende Verschlüsselung der Daten vornehmen und eine digitale Signatur einsetzen, die auf dem Signaturgesetz i.V. m. der Signaturverordnung basiert.
Kategorie 2: Personenbezogene Daten, deren Missbrauch in ihrem Verwendungszusammenhang geeignet ist, die Betroffenen in ihrer gesellschaftlichen Stellung oder in ihren wirtschaft	Es sind grundsätzlich die gleichen Maßnahmen wie in Kategorie 1 erforderlich. Allerdings sind an die Ausgestaltung der Sicherungsinfrastruktur keine besonderen (über einen geregelten RZ-Betrieb hinausgehenden) Anforderungen zu	Eine Umsetzungsmöglichkeit besteht darin, allgemein verbreitete Verschlüsselungs- und Signatursoftware einzusetzen. Notwendige Voraussetzung für einen vertrauenswürdigen

lichen Verhältnissen nicht besonders gewichtig zu beeinträchtigen.	stellen. Betroffene und öffentliche Stellen können Zertifikate oder vergleichbare Authentifizierungsmaßnahmen nach eigenen festgesetzten Regeln verwenden.	Umgang mit einem derartigen Produkt ist die Einrichtung von Zertifizierungsstellen, bei denen die Bürgerinnen und Bürger ihren öffentlichen Schlüssel hinterlegen und digital bestätigen, also zertifizieren lassen können.
Kategorie 3: Personenbezogene Daten, die den Kategorien 1 und 2 nicht zugeordnet werden können.	Es sind Schutzmaßnahmen zu treffen, die einen sicheren Übertragungskanal zwischen den beteiligten Endsystemen mit ausreichender Verschlüsselung ermöglichen. Zusätzliche Maßnahmen sind dann erforderlich, wenn der Verwendungszusammenhang dies erfordert.	Eine Möglichkeit der Kommunikation öffentlicher Stellen mit Bürgerinnen und Bürgern über einen „sicheren Kanal“ besteht darin, Secure Socket Layer einzusetzen. Secure Socket Layer (SSL) legt, wie der Name andeutet, eine zusätzliche Schicht zwischen die Transport-Ebene TCP/IP und die Anwendungsebene (HTTP, Telnet, FTP,...) einer Datenübertragung. Von „oben“ gesehen ist sie transparent, d.h. die Anwendungsprogramme können ohne große Modifikation auf eine sichere Übertragung zugreifen.

6 Bürgerkarte

6.1 Digitale Signatur und Bürgerkarte

Soweit die Verwaltung ihre Dienstleistungen über elektronische Medien anbietet, stellt sich die Frage, wie die Berechtigung der Klienten nachgewiesen werden kann. Zum Abruf allgemeiner Informationen oder für das Herunterladen von Dateien ist eine Identifizierung der Bürger entbehrlich, diese Angebote können anonym wahrgenommen werden. Anders ist dies allerdings beim Übergang zur interaktiven Verwaltung: Die Bürger sollen dabei die Möglichkeit erhalten, Anträge zu Verwaltungsleistungen (z.B. Kindergartenplätze, Wohnberechtigungsscheine, Wohngeld, Sozialhilfe, Baugenehmigung u.v.a.m.) über das Internet zu stellen, ihren gesetzlichen Pflichten den Behörden gegenüber (z.B. Meldepflicht, Steuererklärungen, statistische Erhebungen) über das Internet nachzukommen oder ihre staatsbürgerlichen Rechte über das Internet wahrnehmen (z.B. Wahlrecht, Beteiligungsrechte, Auskunft nach dem Datenschutzrecht, Akteneinsichtsrechte)

Für diese interaktiven Vorgänge ist sowohl die sichere Authentifikation des Antragstellers sowie seine verbindliche Willensbekundung erforderlich. Während die Authentifikation auf verschiedenen Wegen mit unterschiedlichen Sicherheitsgrad erreicht werden kann, kann die verbindliche Willensbekundung nur mit einer elektronischen Unterschrift nachgewiesen werden. Diese kann gleichzeitig die Identität des Bürger und die Integrität der übertragenen Daten auf dem Wege zur Verwaltung sicherstellen.

Die elektronische Unterschrift ist im Gesetz zur digitalen Signatur (Signaturgesetz) vom 22. Juli 1997 geregelt, das demnächst an die Europäische Richtlinie über gemeinsamen Rahmenbedingungen für elektronische Signaturen angepasst wird (die den Mitgliedstaaten gestattet, im öffentlichen Bereich zusätzliche Anforderungen an die Zertifizierung zu stellen). Mit Hilfe zweier Signaturschlüssel und geeigneter Software wird zu den in Frage kommenden Dokumenten ein elektronisches Siegel erzeugt, aus dem man Inhaber des Schlüssels und Unverfälschtheit der Dokumente erkennen kann. Die Schlüssel selbst werden von Zertifizierungsstellen (Trustcenters) ausgegeben, die die korrekte Zuordnung zwischen den Schlüsseln und deren Inhabern gewährleisten sollen. Eine begleitende Gesetzgebung wird demnächst gewährleisten, dass digital signierte Dokumente das Schriftlichkeitserfordernis erfüllen.

Die digitale Signatur erfolgt mit asymmetrischen Verschlüsselungsverfahren. Einer der beiden Schlüssel, die dem Bürger dazu von einem Trustcenter zugewiesen werden, ist öffentlich und wird vom Trustcenter in einem Schlüsselverzeichnis zur Überprüfung bereitgehalten und kann im Internet selbst aufgenommen werden. Der andere Schlüssel fungiert als privater Schlüssel, der nur ihm selbst bekannt sein darf. Wegen seiner Länge muss der streng vertraulich zu behandelnde Schlüssel auf einem Datenträger gespeichert sein. Aus Sicherheitserwägungen kommen dazu nur Prozessorchipkarten in Frage, die die erforderliche

Sicherheitsumgebung bieten können. Von der permanenten Speicherung der Schlüssel auf der Festplatte des heimischen PCs ist wegen des Risikos, dass diese unbefugt über das Internet ausgelesen werden kann, ebenso abzuraten wie von der Speicherung auf Disketten, die anders als Chipkarten keinen aktiven Beitrag zur Sicherheit der Vertraulichkeit des privaten Schlüssels leisten können.

Wer interaktive Verwaltungsdienstleistungen in Anspruch nehmen will, muss demnach künftig über eine derartige Chipkarte verfügen. Verwendet werden könnten Karten, die von den normalen Zertifizierungsstellen für beliebige Zwecke ausgegeben werden. Es wird diskutiert, dass für die Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern spezielle Karten ausgegeben werden, für die der Begriff „Bürgerkarte" (international: CITY-CARD) üblich geworden ist (Deutscher Städtetag: Digitale Signatur auf der Basis multifunktionaler Chipkarten - Ein Leitfaden. Köln 1999).

6.2 Funktionen der Bürgerkarte

Die Bürgerkarte als speziell gewidmete Signaturkarte eröffnet die Möglichkeit, sie über die Möglichkeit der digitalen Signatur hinaus mit weiteren Funktionen auszustatten. Die zusätzlichen Anwendungen sind dabei nicht notwendig auf Verwaltungszwecke beschränkt, auch verwaltungsferne Anwendungen können auf einer derartigen multifunktionalen Chipkarte integriert werden. Diskutiert werden z.B. folgende Sekundäranwendungen der Bürgerkarte:

- Bereitstellung öffentlicher Schlüssel von Verwaltungen zur Entschlüsselung von vertraulichen Nachrichten der Verwaltungen an die Bürgerinnen und Bürger, eine Voraussetzung etwa dafür, dass elektronische Bescheide zugesandt werden können;

- Elektronische Ausweisfunktionen (z.B. Zugangsberechtigungen zu kommunalen Einrichtungen)

- Zahlungsmittel für Gebühren und andere Forderungen der öffentlichen Hand (theoretisch sogar Steuern) auf der Grundlage von Prepaid- oder Netzgeld-Verfahren. Eine Prepaid-Zahlungsfunktion kann auch für die anonyme Bezahlung von öffentlichen oder privaten Infrastrukturdienstleistungen herangezogen werden (Telekommunikation, Strom, Gas, Wasser, öffentlicher Nahverkehr, Parkgebühren).

Als zusätzliche (tertiäre) Anwendung im privaten Bereich käme vor allem die Integration der allgemeinen GeldKarte des deutschen Kreditwesens in Betracht.

Im Hinblick auf Stellen, die einen Zugriff auf verschiedene Datenbestände der Verwaltung erhalten sollen, bietet die Bürgerkarte darüber hinaus eine interessante Möglichkeit: Sie kann als Authorisierungsmittel für den Zugriff auf personenbezogene Daten dienen, wenn die Einwilligung oder zumindest die

Beteiligung bzw. Kenntnisnahme des Bürgers erforderlich ist. Dieses sei am Beispiel eines Berliner Projekts zur Vereinheitlichung und Zusammenführung von Datenstrukturen (VeZuDa) erläutert: Wenn ein Bürger einen Antrag in einer Behörde stellt, dann sollen bestimmte Grunddaten zur Person nicht mehr direkt beim Bürger erhoben, sondern als Datenobjekte aus dem Einwohnerwesen abgerufen werden. Obwohl diese Vorgehensweise durch die einheitliche Darstellung Fehlerrisiken reduziert und Bearbeitungszeiten verkürzen kann, steht sie einerseits im Widerspruch zum Gebot, dass in der Regel Daten des Bürgers bei ihm direkt zu erheben sind und erzeugt andererseits die Gefahr unberechtigter, weil nicht dienstlich begründeter Zugriffe. Die „Bürgerkarte" könnte dazu dienen, der Verwaltung unter Beteiligung des Bürgers eine datenschutzgerechte Vorgehensweise zu ermöglichen. Das Verfahren ist vergleichbar mit dem Einsatz einer Patientenkarte, die vom Arzt in Verbindung mit der eigenen Health Professional Card für den Zugriff auf Patientendaten über Datennetze herangezogen werden muss.

Derartige multifunktionale Chipkarten bringen allerdings erhebliche datenschutzrechtliche Probleme mit sich.

Bei Chipkarten im allgemeinen steht im Vordergrund die wirksame Entscheidung der Betroffenen über die Verwendung dieser Zusatzfunktionen einschließlich der jederzeitigen Widerrufsmöglichkeit. Hierzu gehört eine umfassende Information der Betroffenen über die verantwortliche Stelle, die Verwendungszwecke, mögliche Verarbeitungsbeschränkungen, Löschungsregelungen und Maßnahmen zur Sperrung bzw. Regenerierung der Daten bei Verlust oder Diebstahl. Bei der Nutzung der Daten muss erkennbar sein, welche Daten jeweils genutzt werden. Den Betroffenen muss die Möglichkeit eröffnet werden, sich jederzeit über den Inhalt der Karte zu informieren und auf den Inhalt der Karte Einfluss zu nehmen, soweit dies mit der jeweiligen Funktion vereinbar ist.

Grundvoraussetzung für die Zulässigkeit *multifunktionaler* Bürgerkarten ist die Abschottung der einzelnen Funktionsbereiche voneinander. Nur wenn dies technisch sichergestellt werden kann, ist die Hinzunahme weiterer Funktionen hinnehmbar. Auch mit Einwilligung der Betroffenen kann hierbei keine Abschwächung des Schutzes hingenommen werden.

Funktionen, die zur Verarbeitung von Daten führen, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen und/oder zu sensiblen Daten nach Art. 8 der Europäischen Datenschutzrichtlinie gehören, dürfen mit einer Bürgerkarte nicht verbunden werden, da sie besonderen Anwendungsbedingungen unterliegen. Dies betrifft insbesondere die Aufnahme medizinischer Daten.

6.3 Informationssicherheit

Entscheidende Voraussetzung für den Einsatz der Bürgerkarte ist die Beachtung der Anforderungen an die informationstechnische Sicherheit. Im Gegensatz zu anderen mobilen Datenträgern (z.B. Disketten) bietet diese Technik auf Grund der integrierten Verarbeitungsfunktionen die Möglichkeit, auch hohe datenschutzrechtliche Anforderungen technisch umzusetzen.

Als Grundschutzmaßnahmen unerläßlich sind die fälschungssichere Ausstattung, die Sicherheitsmechanismen gegen die unbefugte Ausspähung gespeicherter Daten und die Authentifizierung zwischen Chipkarte und Benutzer sowie zwischen Chipkarte und Rechner. Bei multifunktionalen Karten ist die technische Abschottung unterschiedlicher Anwendungen auf der Karte von zentraler Bedeutung. Je nach Anwendung und angestrebtem Sicherheitsniveau sind darüber hinaus weitere Schutzmaßnahmen erforderlich.

Von besonderer Bedeutung sind bei multifunktionalen Chipkarten die Abschottungen zwischen den verschiedenen Anwendungsbereichen. Wie sicher diese Abschottungen erfolgen können, hängt vom eingesetzten Chipkartenbetriebssystem ab. Die meisten Chipkartenbetriebssysteme folgen der Normenserie ISO/IEC 7816. Aufgrund der hierarchischen Struktur der Dateisysteme erlauben sie es, die Anwendungsbereich streng von einander abzuschotten und mit jeweils eigenen Sicherheitsumgebungen zu versehen. Dies bedeutet, dass Anwendungen mit geringen Sicherheitsanforderungen neben Anwendungen mit höchsten Sicherheitsanforderungen auf einer Chipkarte untergebracht werden können, ohne dass die höheren Sicherheitsbedürfnisse beeinträchtigt werden.
(Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Entschließung der 50. Konferenz am 9./10. November 1995 zu Datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen; Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Anforderungen zur informationstechnischen Sicherheit bei Chipkarten. In: DuD 21 (1997), S. 254 ff)

7 Elektronische Auskunft, Akteneinsicht und Bürgerbeteiligung

Eine serviceorientierte Verwaltung wird im Verhältnis zu Bürgerinnen und Bürgern neben der Möglichkeit von internetgestützten Transaktionen auch die Möglichkeit der elektronischen Auskunft und der elektronischen Akteneinsicht prüfen müssen. Dabei ist zu unterscheiden zwischen der Auskunft und Akteneinsicht an und durch Betroffene im Sinne des Datenschutzrechts (7.1), der Akteneinsicht durch Beteiligte an einem Verwaltungsverfahren und der Akteneinsicht für alle im Sinne der neueren Akteneinsichts- und Informationszugangsgesetze (Brandenburg, Berlin und Schleswig-Holstein) bzw. - für die übrigen Bundesländer und den Bund - nach allgemeinen rechtsstaatlichen Grundsätzen (7.2.).
Wenn den Bürgerinnen und Bürgern die Möglichkeit eröffnet wird, online mit der Verwaltung Kontakt aufzunehmen und sich an Verwaltungsverfahren zu beteiligen, liegt es nahe, auch weitergehende Formen der Partizipation wie Beteiligung an öffentlichen Anhörungen im Planfeststellungsverfahren unter Nutzung des Internets in Betracht zu ziehen (7.3.).

In all diesen Fällen kann es nur darum gehen, zusätzliche Kommunikations- und Beteiligungsmöglichkeiten mit Hilfe der neuen Informations- und Kommunikationstechniken zu eröffnen, indem per e-mail kommuniziert wird oder Informationen zum eigenständigen Abruf durch die Bürgerinnen und Bürger bereitgehalten werden. Ein - rechtlicher oder faktischer - "Anschluss- und Benutzungszwang" darf nicht entstehen.

7.1 Elektronische Auskunft und Akteneinsicht für Betroffene

Das allgemeine Datenschutzrecht privilegiert in einigen Bundesländern den Online-Zugriff der Betroffenen auf "ihre" Daten, indem es diesen Vorgang vom Verbot des Online-Abrufs durch Private ausdrücklich ausnimmt (so z. B. § 9 Abs. 5 2. Halbsatz Brandenburgisches Datenschutzgesetz - BbgDSG -). Materiellrechtlich ist in der (auch automatisierten) Weitergabe personenbezogener Daten an die Betroffenen keine Übermittlung zu sehen.

Für die Auskunftserteilung an die Betroffenen sieht das Datenschutzrecht keine besonderen Formvorschriften, insbesondere nicht die Schriftform vor. Lediglich die Benachrichtigung der Betroffenen von der Tatsache der automatisierten Verarbeitung ihrer personenbezogenen Daten hat schriftlich zu erfolgen (z.B. § 18 Abs. 2 BbgDSG.). Andererseits gehen einige Datenschutzgesetze noch davon aus, dass Betroffene ein Recht auf Einsicht nur in Akten und andere nicht automatisiert geführte Datensammlungen haben (z.B. § 18 Abs. 4 Satz 1 BbgDSG). Mithin ist eine elektronische Akteneinsicht hiernach bisher nicht möglich, weil sie gerade automatisierte (digitalisierte) Aktenbestände voraussetzt.

Insgesamt spricht aber rechtspolitisch viel dafür, den Bürgerinnen und Bürgern die Ausübung ihres wichtigsten datenschutzrechtlichen Einzelanspruchs ("Magna Charta des Datenschutzes") auch online zu ermöglichen, zumal das Multimedia-Recht von Bund und Ländern den Nutzern von Tele- und Mediendiensten dieses Recht ausdrücklich einräumt (§ 7 S.2 TDDSG; 16 Abs.1 S.2 MDStV). Dabei kann es stets nur um eine Ergänzung der vorhandenen Auskunfts- und Einsichtsmöglichkeiten gehen. Eine ausschließlich elektronische Auskunft oder Akteneinsicht für die Betroffenen würde bestimmte Zielgruppen, die keinen Internetzugang haben oder sich von der Technik an öffentlichen Internet-Kiosken überfordert fühlen, systematisch ausschließen (Problem des "digital divide" bzw. der "digitalen Kluft").

Im Einzelnen könnte eine elektronische Auskunft bzw. Akteneinsicht nur unter folgenden technischen Voraussetzungen erteilt bzw. gewährt werden:

- Die Betroffenen, die Online-Auskunft über die zur ihrer Person gespeicherten Daten erlangen, müssten sich eindeutig identifizieren, um zu verhindern, dass personenbezogene Daten an Unbefugte übermittelt oder von ihnen abgerufen werden. Dies wäre mit Hilfe einer elektronischen Signatur möglich. Auch die Verwendung von entsprechenden Pseudonymen ist denkbar, wenn die Betroffenen Auskunft über die zu ihrem Pseudonym gespeicherten Daten verlangen (§§ 7 Satz 1 TDDSG, 16 Abs. 1 Satz 1 MDStV). Bei übertragbaren oder von mehreren Menschen verwendeten Pseudonymen dürfte sich die Auskunft nur auf die eigenen personenbezogenen Daten erstrecken.

- Die Behörde würde nach Eingang des Antrages zunächst prüfen, ob die materiell-rechtlichen Voraussetzungen der Auskunftserteilung (unabhängig vom Medium, offline wie online) vorliegen. Bei einem (ganz oder teilweise) positiven Bescheid würde sie die gewünschten Informationen verschlüsselt per e-mail übermittelt oder auf einem abgesetzten Server zum Abruf bereithalten. Als Schutz gegen etwaige Zugriffe auf die personenbezogenen Daten Dritter sollten die Betroffenen in keinem Fall Zugriff auf die Verwaltungsrechner erhalten. Auch verschlüsselte Informationen über den Betroffenen sollten nicht unbefugt abgerufen werden können, da diese später beispielsweise aufgrund entstandener Sicherheitslücken auch von Unberechtigten entschlüsseln werden könnten. Gegen solche unberechtigten Zugriffe auch auf verschlüsselte Daten des Betroffenen sollte sich dieser bei Abruf authentisieren. Diese Authentisierung ist unabhängig von der Identifikation in Punkt 1 und lässt sich auch mit Pseudonymen realisieren. Tritt die Verwaltung als Anbieterin von Tele- oder Mediendiensten auf, so hat sie den Nutzerinnen und Nutzern auf deren Wunsch jederzeit auch elektronisch Auskunft über die zu ihrer Person oder ihrem Pseudonym gespeicherten Bestands-, Nutzungs- und Abrechnungsdaten zu erteilen. (§§ 7 Satz 2 TDDSG, 16 Abs.2 Satz 2 MDStV).

- Den Betroffenen wird per verschlüsselter und elektronisch signierter E-Mail die (Nicht-) Bereitstellung der Information mitgeteilt, wenn sie diese Form der Informationsübermittlung wählen. Bei dieser Mitteilung handelt es sich um einen Verwaltungsakt, für den keine besonderen Formvorschriften bestehen. er kann gemäß §37 Abs. 2 und 4 VwVfG auch "in anderer Weise" und ohne Unterschrift erlassen werden.

- Nach erfolgtem Abruf, spätestens nach Ablauf einer vorgegebenen Frist, sollten die auf dem abgesetzten Server gespeicherten personenbezogenen Daten automatisch gelöscht werden. Die Betroffenen sollten vorab auf dieses Verfahren hingewiesen werden.

- Das gesamte Szenario setzt den Einsatz qualifizierter elektronischer Unterschriften (entsprechend dem bisherigen Signaturgesetz), sichere kryptographische Verfahren zur Verschlüsselung des Inhalts der Nachrichten (z. B. Triple-DES, IDEA, RSA mit mindestens 1024 Bit Schlüssellänge), die Protokollierung der Zugriffe auf die abgesetzten Informationsserver und deren Abschottung vom Internet durch Firewalls voraus. Im Einzelnen wären die technischen und organisatorischen Fragen im Zusammenhang mit der Datensicherheit, z. B. zum Schlüsselmanagement, noch weiter zu konkretisieren.

7.2 Elektronische Akteneinsicht für alle

Die neuen Akteneinsichts- und Informationsfreiheitsgesetze setzen zum Teil einen schriftlichen Antrag der Informationsinteressenten voraus (§ 6 Abs.1 Brandenburgisches Akteneinsichts- und Informationszugangsgesetz (AIG); offener § 6 Abs. 1 Informationsfreiheitsgesetz (IFG) Schleswig-Holstein: "soll schriftlich gestellt werden"; § 13 Abs. 1 Berliner Informationsfreiheitsgesetz: "schriftlich oder mündlich"). Für die Geltendmachung des Anspruchs auf Zugang zu Umweltinformationen nach dem Umweltinformationsgesetz (UIG) wie auch des ungeschrieben Anspruchs auf ermessensfehlerfreie Entscheidung über den Informationszugang für alle, die ein berechtigtes Interesse geltend machen können (vgl. BVerwGE 30, 154 (160); OVG Schleswig NVwZ 1996, 408 (409)), besteht keine besondere Formvorschrift. Ob für andere, bereichsspezifische Ansprüche die Schriftform vorgeschrieben ist, muss im Einzelfall geprüft werden. Beteiligte an Verwaltungsverfahren können ebenfalls formlos Akteneinsicht verlangen(§ 29 VwVfG).

Für gesetzliche Schriftformerfordernisse bei der Antragstellung auf Akteneinsicht gilt das bereits im Zusammenhang mit interaktiver Verwaltung (unter 5.1) Ausgeführte entsprechend.

Andererseits ist z.B. in Brandenburg die Erteilung der Akteneinsicht in elektronischer Form (per eMail) ausdrücklich zugelassen(§ 7 Satz 3 Nr. 3 AIG -

mit Zustimmung des Antragstellers). Auch eröffnen einige neuere Datenschutzgesetze (z.B. in Brandenburg, Schleswig-Holstein und Nordrhein-Westfalen) den Betroffenen die Möglichkeit, ihre evtl. erforderliche Einwilligung in die Akteneinsicht durch Dritte elektronisch zu erteilen, wenn sichergestellt ist, dass sie nur durch eine eindeutige und bewusste Handlung des oder der Betroffenen erfolgen kann, nicht unbemerkt verändert werden kann, ihre Urheberin oder ihr Urheber erkannt werden kann, die Einwilligung protokolliert wird und die betroffene Person den Inhalt der Einwilligung jederzeit ohne unverhältnismäßigen Aufwand zur Kenntnis nehmen kann.

Außerdem kann der Antragsteller auf Veröffentlichungen der zuständigen Behörden z. B. im Internet verwiesen werden (§ 7 Satz 4 AIG). Soweit die Verwaltung sogar zur Veröffentlichung bestimmter Informationen (z.B. Verwaltungsvorschriften, Aktenverzeichnisse, Kataster, Pläne) ohne entsprechende Anträge auf Akteneinsicht verpflichtet ist (vgl. z.B. nach § 17 Berliner IFG), kann und sollte diese Veröffentlichung natürlich auch elektronisch erfolgen.

Für die Durchführung der elektronischen Akteneinsicht für alle gelten zunächst dieselben technischen Voraussetzungen wie bei der Online-Auskunft und elektronischen Akteneinsicht durch Betroffene (s. oben I.). Insbesondere gilt auch hier, dass die Informationen auf einem abgesetzten Server vorgehalten werden sollten, um einen direkten Zugriff außenstehender Personen auf die Verwaltungsrechner auszuschließen.

Ob wie bei der Auskunftserteilung an Betroffene bei der allgemeinen Akteneinsicht auch ein Bedarf besteht, die Inhaltsdaten zu verschlüsseln und eine Authentisierung des Informationsabrufs vorzusehen, hängt von den konkreten Bedingungen ab, unter denen Akteneinsicht den Nicht-Betroffenen gewährt wird. Wird die Akteneinsicht beliebigen Bürgerinnen und Bürgern gewährt und haben die datenschutzrechtlich Betroffenen eingewilligt, dass ihre Akte von allen eingesehen werden darf, oder wenn es aus Rechtsgründen auf die Einwilligung der Betroffenen nicht ankommt (z.B. weil das öffentliche Interesse an der Offenlegung überwiegt), dann kann auf die Verschlüsselung verzichtet werden, weil der Inhalt der Akte von allen gelesen werden darf. Machen dagegen die Bürgerin oder der Bürger, um deren Daten es in der Akte geht, ihre erforderliche Einwilligung davon abhängig, dass nur einem bestimmten Dritten Einsicht gewährt wird (und gerade nicht allen), dann ist der Akteninhalt auch hier zu verschlüsseln und kann nicht unbeschränkt zugänglich gemacht werden. Ähnlich verhält es sich schließlich bei der Akteneinsicht durch Verfahrensbeteiligte, die allein aufgrund ihrer besonderen Stellung gesetzlich befugt sind, Daten Dritter einzusehen.

Namen von Betroffenen und von beteiligten Verwaltungsbediensteten (außer herausgehobenen Funktionsträgern) müssen in jedem Fall in geeigneter Weise vor einer internetweiten Recherchierbarkeit geschützt werden (s.o. Informationsangebote öffentlicher Stellen im Internet unter 4.2 Informationsangebote in der Verwaltung).

Fraglich ist, ob bei der allgemeinen Akteneinsicht eine strenge Identifizierung der Informationsinteressenten in der gleichen Weise geboten ist wie beim

Informationszugang durch Betroffene. Soweit und solange die allgemeinen Informationszugangsgesetze (z. B. Brandenburgs) die Schriftform bei der Antragstellung voraussetzen und wenn die Betroffenen nur einer Akteneinsicht durch bestimmte Personen zugestimmt haben, wird man dies bejahen müssen. Dasselbe gilt, wenn der Informationsinteressent sich nicht auf ein allgemeines Informationszugangsgesetz stützen kann, sondern nach allgemeinen rechtsstaatlichen Grundsätzen ein berechtigtes oder nach besonderen Rechtsvorschriften sogar ein rechtliches Interesse seiner Person darlegen muss. Es ist aber beispielsweise vorstellbar, dass der Zugriff auf Daten der Verwaltung, für die kein schutzwürdiges Geheimhaltungsinteresse besteht und die von allgemeinem öffentlichen Interesse sind, auch anonym oder unter Pseudonym abgerufen werden können. Das gilt jedenfalls für den Abruf von Verwaltungsinformationen, die ohne entsprechenden Antrag im Internet bereitgestellt werden. Hier ist schon jetzt eine anonyme oder pseudonyme Ausgestaltung der Zugriffe datenschutzrechtlich sogar geboten (§§ 4 Abs. 1 TDDSG, 13 Abs. 1 MDStV).

Auch die Gebührenpflicht des allgemeinen Informationszugangs (z. B. auch nach Umweltinformationsgesetz des Bundes) setzt nicht zwingend voraus, dass die Informationsinteressenten sich identifizieren. Sobald anonyme Bezahlverfahren im Internet verfügbar sind, wäre es vorstellbar, dass die abgefragten Informationen zeitgleich anonym über das Netz bezahlt werden. Insgesamt wird beim allgemeinen Informationszugang eine zunehmende elektronische Übermittlung von Akteninhalten dazu beitragen, dass die Gebührenschwelle völlig an Bedeutung verliert, die bei konventioneller Akteneinsicht noch prohibitiven Charakter haben kann. Dieser Gesichtspunkt spielt dagegen bei der Auskunftserteilung an und Akteneinsicht durch Betroffene bei öffentlichen Stellen keine Rolle, weil sie gebührenfrei zu erfolgen haben.

Ein Personenbezug könnte allerdings notwendig sein, wenn der Informationszugang ganz oder teilweise abgelehnt wird, weil darin ein anfechtbarer Verwaltungsakt liegt, der dem Interessenten bekannt gegeben werden muss. Ein Personenbezug wird häufig auch in den Fällen hergestellt werden müssen, in denen Antragsteller ein besonderes (persönliches) Interesse etwa an der politischen Mitgestaltung darlegen müssen, um auf diese Weise der Behörde eine Abwägung mit entgegenstehenden Interessen Betroffener, deren personenbezogene Daten in den Akten enthalten sind, zu ermöglichen. In beiden Fällen wäre aber auch der Einsatz von bestimmten (adressierbaren) Pseudonymen vorstellbar. Wird der beantragte Informationszugang unter Zurückstellung der Interessen des Drittbetroffenen gewährt, liegt darin die weitere Besonderheit, dass (konkludent) ein belastender Verwaltungsakt ergeht, der seinerseits durch den Dritten angefochten werden muss (vgl. VG München, NVwZ 1996, 410,412).

7.3 Online-Partizipation im Verwaltungsverfahren

Wie bei der elektronischen Ausübung von Auskunfts- und Einsichtsrechten ergeben sich auch bei der internet-gestützten Beteiligung an Anhörungen im Planfeststellungsverfahren und anderen Formen der elektronischen Bürgerbeteiligung Fragen der notwendigen Identifikation. Das geltende Verwaltungs

verfahrensrecht setzt nicht ausdrücklich eine namentliche Identifizierung der Einwender und anderer Beteiligter an Erörterungsterminen im Planfeststellungsverfahren voraus. In der Praxis wird aber eine Identifikationspflicht vorausgesetzt, da der Planfeststellungsbeschluss Rechtswirkungen für und gegen jeden einzelnen Einwender entfaltet. Soweit man dieser Praxis folgt, muss auch eine "online-Einwendung" dem Rechnung tragen, d.h. sie muss nach denselben Regeln unter Einsatz einer elektronischen Signatur den Einwender identifizierbar machen wie bei der online-Auskunft an Betroffene.

Datenschutzfreundlicher und mit dem geltenden Recht auch vereinbar wäre aber ein Verfahren, bei dem der Planfeststellungsbeschluss - wie ein Bescheid über Auskunft oder Akteneinsicht - über ein adressierbares Pseudonym bekannt gegeben wird. Dies würde es dem Einwender ermöglichen, seine Identität bei der Anhörung nicht offenzulegen. In Betracht käme dies vor allem bei allgemeinen (z. B. umwelt- oder gesundheitsbezogenen) Einwendungen. Eine Identifikation der Einwender bleibt allerdings erforderlich bei grundstücksbezogenen Einwendungen, da insoweit eine Überprüfung anhand des Grundbuchs erfolgt.

Relevant für die internet-gestützte Beteiligung an Planungsverfahren ist darüber hinaus die Rechtsprechung des Bundesverfassungsgerichts, wonach die unverschlüsselte und personenbezogene Veröffentlichung der Einwendungen die Zweckbindung dieser Daten unterläuft und in unverhältnismäßiger Weise in das informationelle Selbstbestimmungsrecht der Einwenderinnen und Einwender eingreift (BVerfG 77, S. 121; BVerfG Computer und Recht 1990, S. 798 ff.). Dem hat die technische Gestaltung einer "online-Anhörung" durch den Einsatz von sicheren Verschlüsselungsverfahren Rechnung zu tragen.

8 Auslagerung von Verwaltungsfunktionen

8.1 Auftragsdatenverarbeitung und Funktionsübertragung

Viele Formen serviceorientierter Verwaltung sind dadurch gekennzeichnet, dass die zuständige Behörde einzelne Arbeitsabläufe oder gar ganze Aufgaben auf eine andere Stelle überträgt (Outsourcing). Dies wirft die Frage auf, wie dieser Vorgang datenschutzrechtlich zu beurteilen ist, insbesondere, welche Voraussetzungen für eine rechtmäßige Übertragung vorliegen müssen und ob es Grenzen für eine derartige Übertragung gibt.

Das Datenschutzrecht unterscheidet hierzu zwischen der Datenverarbeitung im Auftrag und der Funktionsübertragung. Während bei der Auftragsdatenverarbeitung die Verantwortlichkeit bei der zuständigen Stelle bleibt und der Auftragnehmer die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten darf, geht bei der Funktionsübertragung die datenschutzrechtliche Verantwortlichkeit auf den Funktionsnehmer über. Im ersten Fall stellt die Datenweitergabe eine Nutzung im rechtlichen Sinne dar. Im zweiten Fall müssen bei der Datenweitergabe die strengen Voraussetzungen der Datenübermittlung vorliegen.

Für eine Auftragsdatenverarbeitung spricht

- das Fehlen einer Entscheidungsbefugnis des Auftragnehmers über die Daten,
- ein Auftragsschwerpunkt, der auf die praktisch technische Durchführung einer Datenverarbeitung gerichtet ist,
- das Fehlen einer eigenständigen rechtlichen Beziehung des Auftragnehmers zu Betroffenen.

Für eine Funktionsübertragung spricht andererseits

- die Nutzung der herausgegebenen Daten für eigene Zwecke des Funktionsnehmers,
- eine Dienstleistung, die über die praktisch technische Datenverarbeitung hinausgeht,
- das Fehlen der Möglichkeit des Funktionsgebers, auf einzelne Phasen der Verarbeitung oder Nutzung Einfluss zu nehmen,
- die auf den Funktionsnehmer abgewälzte Verantwortlichkeit für die Zulässigkeit und Richtigkeit der Datenverarbeitung.

Die Funktionsübertragung durch einen öffentlichen Funktionsgeber kann auf dem Wege einer Delegation oder der Erteilung eines Mandates erfolgen. Bei der Delegation tritt der Funktionsnehmer in eigener Zuständigkeit und unter eigenem Namen auf. Er ist Normadressat für die datenschutzrechtlichen Regelungen; Widerspruch und Klagen richten sich gegen den Delegationsempfänger. Anders beim Mandat. Auch hier entscheidet der Funktionsnehmer selbständig, ohne Weisungen für die Datenverarbeitung erhalten zu haben, tritt aber nach außen unter dem Namen des Funktionsgebers auf, der damit für die Datenverarbeitung verantwortlich bleibt. Der Mandatsnehmer ist damit im Ergebnis als Organisationseinheit der speichernden Stelle zu betrachten.

Serviceorientierte Verwaltung bedient sich der Auslagerung der Datenverarbeitung in unterschiedlichen Formen, die zu einer differenzierten datenschutzrechtlichen Einordnung führen.

Nimmt eine Bürgerberatungsstelle nur Antragsdaten der Betroffenen entgegen, ohne selbst auf diese Daten Einfluss zu nehmen, handelt es sich um Datenverarbeitung im Auftrag, und zwar um Datenerhebung im Rahmen der Aufgabenstellung der auftraggebenden Behörde.

Ebenso klar stellt sich die Rechtslage dar, wenn der Auftragnehmer eigene Entscheidungsbefugnisse erhält oder sogar selbst Verwaltungsakte für die auftraggebende Behörde erlässt. In diesem Fall müssen zum einen die gesetzlichen Voraussetzungen einer derartige Aufgabenübertragung vorliegen (gesetzliche Ermächtigung, bei Übertragung auf nicht-öffentliche Stellen Beleihung mit entsprechender Rechtsgrundlage und Publizitätsakt), andererseits müssen die Voraussetzungen der Datenübermittlung von der auftraggebenden an die auftragnehmende Stelle und umgekehrt vorliegen. Für Datenschutzgesetze, die wie in Berlin hierfür keine Generalklausel vorsehen oder als Rechtsgrundlage nur die Erforderlichkeit im Rahmen einer *gesetzlichen* Aufgabenüberweisung anerkennen, bedeutet dies, dass für den Funktionsnehmer eine eigene Rechtsgrundlage geschaffen werden muss (wie dies in Berlin für Bürgerbüros geschehen ist).

Problematisch ist die Einordnung in den Fällen, in denen dem Funktionsnehmer zwar die Zuständigkeit für die Letztentscheidung nicht übertragen ist, in denen aber der Funktionsnehmer Beratungsleistungen übernimmt, die Umfang und Inhalt der erhobenen Daten, gegebenenfalls auch deren Verarbeitung beeinflussen. Häufig wird hierbei auch auf bereits vorhandene Datenbestände zugegriffen werden.

Für derartige Beratungen kennzeichnend ist, dass vom Funktionsgeber Weisungen, die den Verlauf der Beratung präzise bestimmen, nicht gegeben werden können. Dies führt dazu, dass auch hier die Voraussetzungen der Funktionsübertragung vorliegen müssen. Soweit nicht wegen der bestehenden Rechtslage ohnehin eine gesetzliche Regelung erforderlich ist, muss aus diesem Grund die Einwilligung der Betroffenen eingeholt werden. Dies setzt vor allem bei telefonischer Beratung oder gar Online-Beratung eine hinreichende Information

der Betroffenen sowie die Erteilung einer (elektronischen) Einwilligungserklärung voraus.

Materielle Grenzen der Aufgabenübertragung als solche kennt das bestehende Datenschutzrecht nicht. Soweit jedoch personenbezogene Daten verarbeitet werden sollen, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, oder die zu den sensiblen Daten nach der Europäischen Datenschutzrichtlinie zählen, müssen hierfür die jeweils besonderen Zulässigkeitsvoraussetzungen vorliegen; insbesondere müssen sich die Einwilligungserklärungen ausdrücklich auf diese Daten beziehen (vgl. hierzu auch den Entwurf BDSG 2000).

8.2 Anbieterfunktion nach dem Multimediarecht

Eine besondere Form der Auslagerung von Verwaltungsfunktionen liegt dann vor, wenn sich die öffentlichen Stellen beim Gang ins Internet der Hilfe Dritter bedienen. Eine solche Hilfe Dritter kann vom Bereithalten der Homepage z. B. auf dem Server eines Rechenzentrums bis hin zum Erstellen und der Entgegennahme ausgefüllter Formulare im Falle der interaktiven Verwaltung reichen.

Auf der sog. Inhaltsebene (vgl. dazu unter 5.2) handelt es sich bei der Entgegennahme ausgefüllter Formulare im Regelfall um eine Datenverarbeitung im Auftrag. Regelmäßig soll dem etwa mit der Datenverarbeitung beauftragten Rechenzentrum weder eine Entscheidungsbefugnis über die Verarbeitung personenbezogener Daten zustehen, noch steht der mit der technischen Durchführung betraute Dritte auf der Inhaltsebene in einer rechtlichen Beziehung zum Betroffenen. Vielmehr erfolgt die Verarbeitung der übersandten Informationen im Regelfall im Interesse und im Auftrag der jeweiligen öffentlichen Stelle.

Auf der Diensteebene (vgl. dazu unter 5.2) sind die öffentlichen Stellen als sog. Inhaltsanbieter neben dem beauftragten Rechenzentrum für die Einhaltung der datenschutzrechtlichen Vorschriften des Multimediarechts verantwortlich (vgl. m.w.N. zu der Frage, ob der Inhaber einer Homepage Anbieter eines Informations- und Kommunikationsdienstes ist, Spindler in: Roßnagel (Hrsg.), Recht der Multimediadienste, München 1999, Rdnr. 53 f. zu § 5 TDG).

Für eine solche Auslegung der Definition des Anbieters sprechen

- die Vorschriften zur Verantwortlichkeit des Diensteanbieters für „eigene Inhalte" (so die Formulierung in § 5 Abs. 1 TDG; § 5 Abs. 1 MDStV) und

- die Vorschriften zur Anbieterkennzeichnung (§ 6 TDG; § 6 MDStV), die nach ihrem Sinn und Zweck nicht lediglich auf den mit der technischen Durchführung beauftragten Dritten, sondern auf die öffentliche Stelle zielen, die sich mit einer Homepage im Netz präsentiert und in diesem Rahmen die Bürgerinnen und Bürger zu interaktiven Formen der Kommunikation über das Netz einlädt.

Neben dem mit dem Bereithalten von Informations- und Kommunikationsdiensten beauftragten Dritten sind auch die öffentlichen Stellen Anbieter im Sinne der §§ 2 Nr. 1 TDDSG, 3 Nr. 1 MDStV. Das bedeutet, dass die öffentlichen Stellen auch auf der Diensteebene für die Einhaltung der datenschutzrechtlichen Vorschriften des Multimediarechts verantwortlich sind.